



# Citrix Endpoint Management

## Contents

<b>Endpoint Management</b>	<b>3</b>
<b>What's new</b>	<b>10</b>
<b>Third-party notices</b>	<b>18</b>
<b>Deprecation</b>	<b>18</b>
<b>System requirements</b>	<b>30</b>
<b>Endpoint Management compatibility</b>	<b>43</b>
<b>Supported device operating systems</b>	<b>44</b>
<b>Language support</b>	<b>46</b>
<b>FIPS 140-2 compliance</b>	<b>48</b>
<b>About Endpoint Management</b>	<b>49</b>
<b>Citrix Endpoint Management integration with Microsoft Endpoint Manager</b>	<b>64</b>
<b>Onboarding and resource setup</b>	<b>100</b>
<b>Scale and size considerations for Cloud Connectors</b>	<b>114</b>
<b>Prepare to enroll devices and deliver resources</b>	<b>115</b>
<b>Certificates and authentication</b>	<b>131</b>
<b>Upload, update, and renew certificates</b>	<b>139</b>
<b>Citrix Gateway and Endpoint Management</b>	<b>152</b>
<b>Domain or domain plus security token authentication</b>	<b>163</b>
<b>Client certificate or certificate plus domain authentication</b>	<b>169</b>
<b>PKI entities</b>	<b>192</b>
<b>Credential providers</b>	<b>231</b>
<b>APNs certificates</b>	<b>239</b>
<b>SAML for single sign-on with Citrix Files</b>	<b>248</b>

<b>Authentication with Azure Active Directory through Citrix Cloud</b>	<b>257</b>
<b>Authentication with Okta through Citrix Cloud</b>	<b>261</b>
<b>Authentication with an on-premises Citrix Gateway through Citrix Cloud</b>	<b>263</b>
<b>Derived credentials</b>	<b>266</b>
<b>User accounts, roles, and enrollment</b>	<b>285</b>
<b>Enrollment profiles</b>	<b>301</b>
<b>Notifications</b>	<b>306</b>
<b>Configure roles with RBAC</b>	<b>319</b>
<b>Licenses</b>	<b>339</b>
<b>Device management</b>	<b>339</b>
<b>Alexa for Business</b>	<b>371</b>
<b>Migrate from device administration to Android Enterprise</b>	<b>385</b>
<b>Android Enterprise</b>	<b>390</b>
<b>Android for Workspace</b>	<b>440</b>
<b>Distribute Android Enterprise and Android for Workspace (Preview) apps</b>	<b>449</b>
<b>Legacy Android Enterprise for Google Workspace (formerly G Suite) customers</b>	<b>478</b>
<b>Android OS</b>	<b>515</b>
<b>Firebase Cloud Messaging</b>	<b>521</b>
<b>Android SafetyNet</b>	<b>525</b>
<b>Samsung</b>	<b>530</b>
<b>Samsung Knox bulk enrollment</b>	<b>535</b>
<b>Network Access Control</b>	<b>541</b>
<b>iOS</b>	<b>547</b>
<b>macOS</b>	<b>563</b>

<b>Deploy devices through the Apple Deployment Programs</b>	<b>570</b>
<b>Enroll Apple devices in bulk</b>	<b>585</b>
<b>Integrate with Apple Education features</b>	<b>590</b>
<b>Shared iPads</b>	<b>606</b>
<b>Distribute Apple apps</b>	<b>618</b>
<b>Network Access Control</b>	<b>644</b>
<b>Chrome OS</b>	<b>650</b>
<b>Windows Desktop and Tablet</b>	<b>660</b>
<b>Windows Phone</b>	<b>670</b>
<b>Enroll Windows devices in bulk</b>	<b>673</b>
<b>Workspace hub device management</b>	<b>678</b>
<b>Device policies</b>	<b>690</b>
<b>AirPlay mirroring device policy</b>	<b>721</b>
<b>AirPrint device policy</b>	<b>724</b>
<b>App permissions device policy</b>	<b>724</b>
<b>APN device policy</b>	<b>726</b>
<b>App access device policy</b>	<b>729</b>
<b>App attributes device policy</b>	<b>730</b>
<b>App configuration device policy</b>	<b>731</b>
<b>App inventory device policy</b>	<b>735</b>
<b>Application Guard device policy</b>	<b>737</b>
<b>App lock device policy</b>	<b>739</b>
<b>Apps notifications device policy</b>	<b>743</b>
<b>App restrictions device policy</b>	<b>745</b>

<b>App uninstall device policy</b>	<b>748</b>
<b>App uninstall restrictions device policy</b>	<b>750</b>
<b>Automatically update managed apps device policy</b>	<b>750</b>
<b>BitLocker device policy</b>	<b>751</b>
<b>Browser device policy</b>	<b>757</b>
<b>Calendar (CalDav) device policy</b>	<b>758</b>
<b>Cellular device policy</b>	<b>759</b>
<b>Connection scheduling device policy</b>	<b>760</b>
<b>Contacts (CardDAV) device policy</b>	<b>762</b>
<b>Content device policy</b>	<b>764</b>
<b>Copy Apps to Samsung Container device policy</b>	<b>765</b>
<b>Credentials device policy</b>	<b>765</b>
<b>Custom XML device policy</b>	<b>773</b>
<b>Defender device policy</b>	<b>775</b>
<b>Device Guard device policy</b>	<b>777</b>
<b>Device Health Attestation device policy</b>	<b>778</b>
<b>Device name device policy</b>	<b>779</b>
<b>Education Configuration device policy</b>	<b>780</b>
<b>Endpoint Management options device policy</b>	<b>783</b>
<b>Endpoint Management uninstall device policy</b>	<b>785</b>
<b>Enterprise Hub device policy</b>	<b>786</b>
<b>Exchange device policy</b>	<b>787</b>
<b>Files device policy</b>	<b>795</b>
<b>FileVault device policy</b>	<b>797</b>

<b>Firewall device policy</b>	<b>800</b>
<b>Font device policy</b>	<b>802</b>
<b>Home screen layout device policy</b>	<b>803</b>
<b>Import Device Configuration device policy</b>	<b>805</b>
<b>Import iOS &amp; macOS Profile device policy</b>	<b>806</b>
<b>Keyguard Management device policy</b>	<b>808</b>
<b>Kiosk device policy</b>	<b>812</b>
<b>Knox Platform for Enterprise device policy</b>	<b>819</b>
<b>Launcher configuration device policy</b>	<b>820</b>
<b>LDAP device policy</b>	<b>821</b>
<b>Location device policy</b>	<b>823</b>
<b>Lock screen message device policy</b>	<b>829</b>
<b>Mail device policy</b>	<b>830</b>
<b>Managed bookmarks device policy</b>	<b>833</b>
<b>Managed configurations policy</b>	<b>834</b>
<b>Managed domains device policy</b>	<b>844</b>
<b>Maps device policy</b>	<b>846</b>
<b>Maximum resident users device policy</b>	<b>847</b>
<b>MDM options device policy</b>	<b>847</b>
<b>Network device policy</b>	<b>849</b>
<b>Network usage device policy</b>	<b>866</b>
<b>Office device policy</b>	<b>866</b>
<b>Organization information device policy</b>	<b>868</b>
<b>OS Update device policy</b>	<b>868</b>

<b>Passcode device policy</b>	<b>883</b>
<b>Passcode lock grace period device policy</b>	<b>897</b>
<b>Personal hotspot device policy</b>	<b>897</b>
<b>Power management device policy</b>	<b>898</b>
<b>Profile Removal device policy</b>	<b>899</b>
<b>Provisioning profile device policy</b>	<b>900</b>
<b>Provisioning profile removal device policy</b>	<b>901</b>
<b>Proxy device policy</b>	<b>901</b>
<b>Public session device policy</b>	<b>903</b>
<b>Restrictions device policy</b>	<b>905</b>
<b>Roaming device policy</b>	<b>960</b>
<b>Samsung MDM license key device policy</b>	<b>961</b>
<b>SCEP device policy</b>	<b>963</b>
<b>Siri and dictation policies</b>	<b>967</b>
<b>SSO account device policy</b>	<b>968</b>
<b>Storage encryption device policy</b>	<b>969</b>
<b>Store device policy</b>	<b>970</b>
<b>Subscribed calendars device policy</b>	<b>971</b>
<b>Terms and conditions device policy</b>	<b>972</b>
<b>Tunnel device policy</b>	<b>972</b>
<b>VPN device policy</b>	<b>974</b>
<b>Wallpaper device policy</b>	<b>1023</b>
<b>Web content filter device policy</b>	<b>1025</b>
<b>Web clip device policy</b>	<b>1027</b>

<b>Windows Agent device policy</b>	<b>1028</b>
<b>Windows GPO Configuration device policy</b>	<b>1032</b>
<b>Windows Hello for Business device policy</b>	<b>1035</b>
<b>Windows Information Protection device policy</b>	<b>1036</b>
<b>Add apps</b>	<b>1041</b>
<b>App connector types</b>	<b>1092</b>
<b>Citrix Launcher</b>	<b>1093</b>
<b>Add apps using Apple volume purchase</b>	<b>1096</b>
<b>Deploy Microsoft Store for Business apps from Endpoint Management</b>	<b>1104</b>
<b>Use Citrix Content Collaboration with Endpoint Management</b>	<b>1108</b>
<b>SmartAccess for HDX apps</b>	<b>1124</b>
<b>Upgrade MDX or enterprise apps</b>	<b>1141</b>
<b>Add media</b>	<b>1143</b>
<b>Deploy resources</b>	<b>1147</b>
<b>Macros</b>	<b>1161</b>
<b>Automated actions</b>	<b>1196</b>
<b>Monitor and support</b>	<b>1207</b>
<b>Connectivity checks</b>	<b>1215</b>
<b>Mobile Service Provider</b>	<b>1222</b>
<b>Reports</b>	<b>1223</b>
<b>Endpoint Management Analyzer</b>	<b>1231</b>
<b>REST APIs</b>	<b>1239</b>
<b>ActiveSync Gateway</b>	<b>1240</b>
<b>Endpoint Management connector for Exchange ActiveSync</b>	<b>1243</b>



<b>Citrix Gateway connector for Exchange ActiveSync</b>	<b>1293</b>
<b>Advanced concepts</b>	<b>1308</b>
<b>Endpoint Management deployment</b>	<b>1308</b>
<b>Management modes</b>	<b>1309</b>
<b>Device requirements</b>	<b>1313</b>
<b>Security and user experience</b>	<b>1313</b>
<b>Apps</b>	<b>1330</b>
<b>User communities</b>	<b>1338</b>
<b>Email strategy</b>	<b>1345</b>
<b>Endpoint Management integration</b>	<b>1352</b>
<b>Integrating with Citrix Gateway and Citrix ADC</b>	<b>1359</b>
<b>SSO and proxy considerations for MDX apps</b>	<b>1365</b>
<b>Authentication</b>	<b>1370</b>
<b>Server properties</b>	<b>1384</b>
<b>Device and app policies</b>	<b>1397</b>
<b>Client properties</b>	<b>1408</b>
<b>User enrollment options</b>	<b>1419</b>
<b>App provisioning and deprovisioning</b>	<b>1422</b>
<b>Dashboard-based operations</b>	<b>1424</b>
<b>Role-based access control and Endpoint Management support</b>	<b>1426</b>
<b>Citrix Support process</b>	<b>1428</b>
<b>Sending group enrollment invitations in Endpoint Management</b>	<b>1429</b>
<b>Configuring certificate-based authentication with EWS for Secure Mail push notifications</b>	<b>1431</b>
<b>Configuring an on-premises Device Health Attestation server</b>	<b>1434</b>

## Endpoint Management

October 27, 2021

Citrix Endpoint Management is a solution for managing endpoints, offering mobile device management (MDM) and mobile application management (MAM) capabilities. With Endpoint Management, you manage device and app policies and deliver apps to users. Your business information stays protected with strict security for identity, devices, apps, data, and networks.

### Citrix and customer responsibilities

Citrix Cloud Operations handles various infrastructure and monitoring tasks. As a result, you can focus on the user experience and on managing devices, apps, and policies.

Citrix responsibilities:

- Endpoint Management server nodes
- Citrix Gateway (service or on-premises) initial integration and configuration
- Citrix Gateway Load Balancer
- Database
- Cloud Connector software configuration
- SAML authentication integration with Citrix Content Collaboration
- Endpoint Management site monitoring: Instance, database, enterprise connectivity (LDAP), VPN tunnel (if applicable), public SSL certificate, Endpoint Management licensing

Customer responsibilities:

- Citrix Gateway (on-premises) management and updates
- Machines where Cloud Connectors and Gateway Connector (for Citrix Gateway service) are installed
- LDAP/Active Directory
- DNS
- Citrix Content Collaboration: Initial Citrix Content Collaboration configuration, on-premises storage zones controller installation, Citrix Files updates
- Endpoint Management configuration: Devices, policies, apps, delivery groups, actions, and client certificates

### Integration with Citrix Workspace experience

Endpoint Management customers can opt to integrate Endpoint Management with the Citrix Workspace experience. You make that choice in **Citrix Cloud > Workspace Configuration > Service Integrations**. By default, Workspace integration is disabled.

Currently, this integration is publicly available for the Android platform. It's available as a preview for Windows 10 desktops and tablets.

### **About the integration**

Citrix hosts the Cloud environment in data centers located throughout the world to deliver high performance, rapid response, and support. With Endpoint Management, you pay a subscription fee instead of purchasing and managing licenses.

Endpoint Management integration with Citrix Workspace differs for new and existing customers.

#### **For new Endpoint Management customers (as of August 27, 2018)**

- If you enable the integration, the Citrix Workspace app aggregates resources. Those resources come from Endpoint Management and other configured sources. Your users access resources from the Citrix Workspace app. Other configured sources might include Citrix Content Collaboration and Citrix Virtual Apps and Desktops.
- If you leave the integration disabled, Citrix Secure Hub aggregates mobile apps. Your users access apps from Secure Hub.

#### **Important:**

After you configure your integration choice and enroll users: If you later change your integration choice, re-enrollment is required for all users.

Endpoint Management supports auto-enrollment of any desktop and tablet running Windows 10 or Windows 11 using the Citrix Workspace app. This support means that you can enroll any desktop or tablet running Windows 10 or Windows 11, regardless of hardware. For more information about the Citrix Workspace app, see [Citrix Workspace app for Windows](#).

#### **For customers who onboarded before August 27, 2018**

You can enable Workspace integration (**Citrix Cloud > Workspace Configuration > Service Integrations**). Devices that are already enrolled in Secure Hub continue to use Secure Hub.

New devices enroll in Workspace. However, if you prefer to enroll only selected devices in Workspace, you must create a delivery group called Workspace.

- For devices already enrolled in Secure Hub and then added to the Workspace delivery group, a user must re-enroll the device. The user then accesses resources from the Citrix Workspace app.
- For new devices added to the Workspace delivery group, users enroll in Workspace.

- If you move a device from the Workspace delivery group to any other delivery group, a user must re-enroll the device. The user then accesses resources from Secure Hub.
- Citrix notifies you when migration to Workspace is supported without requiring re-enrollment.

To enable Citrix Workspace integration with Citrix Endpoint Management:

1. Sign in to [Citrix Cloud](#).
2. Click **Manage** on the Endpoint Management tile. You can request a 30-day trial if the **Manage** tab is unavailable.
3. In the upper-left menu, navigate to **Workspace Configuration > Service Integration**.
4. Click **Enable** to integrate Citrix Workspace app with Endpoint Management.

Endpoint Management supports auto-enrollment of any desktop and tablet running Windows 10 or Windows 11 by using the Citrix Workspace app. This support means that you can enroll any desktop or tablet running Windows 10 or Windows 11, regardless of hardware. For more information about the Citrix Workspace app, see [Citrix Workspace app for Windows](#).

### Single sign-on support

Endpoint Management integration with Citrix Workspace supports mobile single sign-on (SSO). MDM enrolled iOS and Android devices support SSO to native SaaS apps. See [Configure mobile SSO \(preview\)](#).

### Mobile SSO to native SaaS apps (preview)

A preview of mobile SSO to native SaaS apps is now available for customers who meet these requirements:

- Citrix Workspace Premium license
- Your identity provider configured in Citrix Cloud
- The following services configured:
  - Workspace service with Endpoint Management enabled. For information about enabling service integration, see [Configure Workspaces](#).
  - Citrix Endpoint Management service
  - Citrix Gateway service

Single sign-on to native SaaS apps is available for iOS and Android devices that are enrolled into MDM. For more information, see [Configure mobile SSO \(preview\)](#).

### Citrix Gateway service

The Citrix Gateway service is now publicly available for customers who meet these requirements:

- Citrix Workspace experience enabled

- Citrix Gateway service subscription
- Android for Workspace configured

The Citrix Gateway service is available as a preview for customers who meet the listed requirements but don't use Android for Workspace.

If you already use on-premises Citrix Gateway and want to switch to Citrix Gateway service, contact your Citrix Support representative. For more information, see [Configure Citrix Gateway use with Endpoint Management](#).

### **Integration with Microsoft Endpoint Manager**

Endpoint Management integrates with Microsoft Endpoint Manager (MEM). That integration adds the value of Endpoint Management micro VPN to Microsoft Intune aware apps, such as Microsoft Edge browser. With the integration, you can:

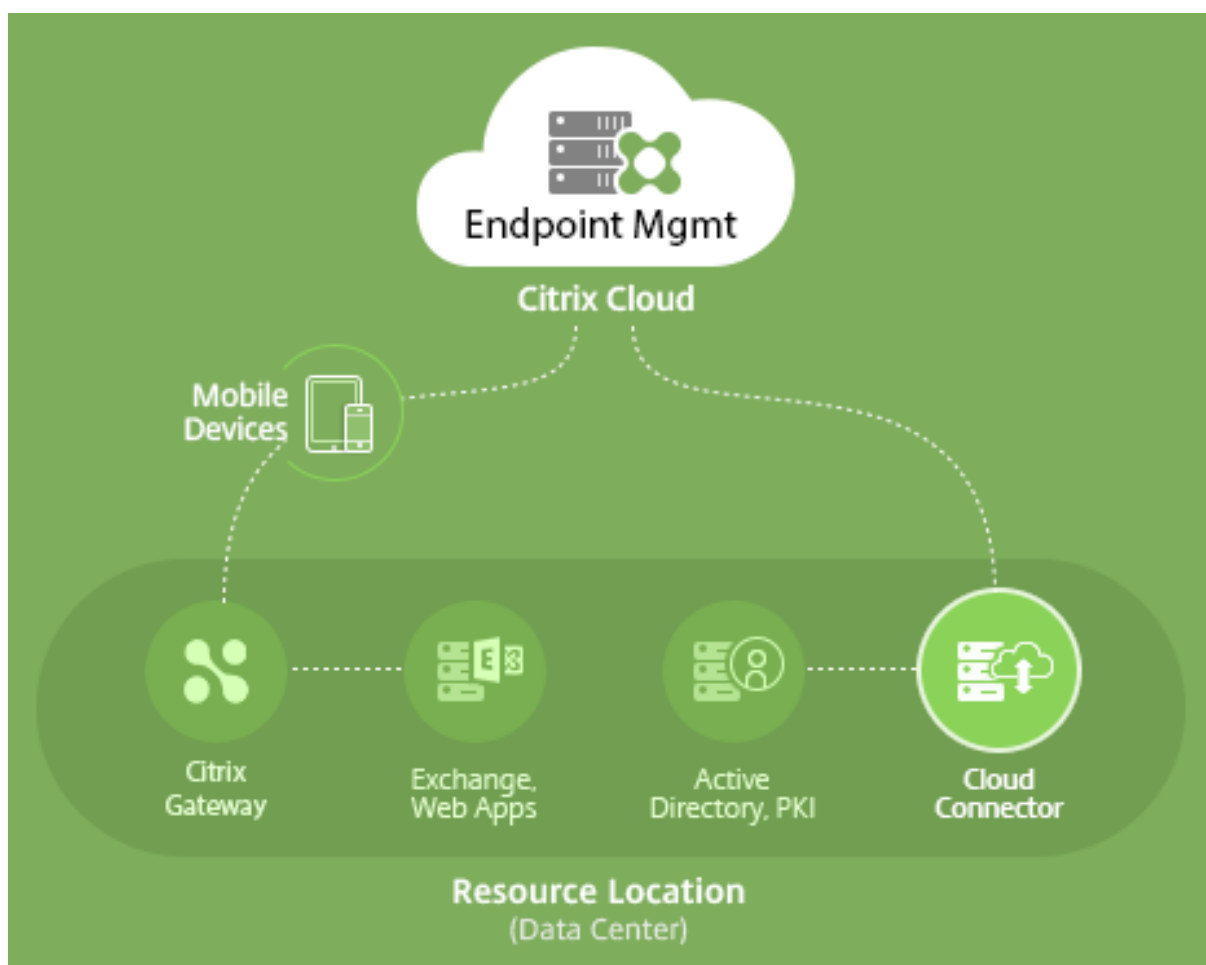
- Secure Office 365 applications with conditional access with Azure AD. For more information, see [Integrate with Azure AD Conditional Access](#).
- Wrap your own line of business apps with Intune and Citrix to provide micro VPN capabilities inside an Intune mobile app management (MAM) container.
- Manage and deliver Office 365 apps, line of business apps, and Citrix Secure Mail in one container. This management method provides ultimate security and productivity. For example, you can:
  - Block individual devices or operating systems
  - Customize ActiveSync policies based on devices, users, or user groups
  - Quarantine at the device level
  - Monitor individual connections or devices
  - Avoid the security risks of credential and data caching

Use Endpoint Management MDM+MAM or Intune MDM to manage devices. For more information, see [Citrix Endpoint Management integration with Microsoft Endpoint Manager](#).

### **Cloud Connector and resource locations**

You connect to Endpoint Management through Cloud Connector. Cloud Connector serves as a channel for communication between Citrix Cloud and your resource locations. Cloud Connector enables cloud management without requiring any complex networking or infrastructure configuration such as VPNs or IPsec tunnels.

Resource locations contain the resources required to deliver services to your subscribers. For Endpoint Management, resource locations are your Citrix Gateway, LDAP, DNS, and PKI servers.



For more information about Cloud Connector and resource locations, see [About Endpoint Management](#).

## Get started with Endpoint Management

### Tip:

XenMobile Migration Service

If you're using XenMobile Server on premises, our XenMobile Migration Service can get you started with Endpoint Management. Migration from XenMobile Server to Citrix Endpoint Management doesn't require you to re-enroll devices.

For more information, contact your local Citrix salesperson, Systems Engineer, or Citrix Partner.

To learn more about our migration service, see [3 reasons to move to Citrix Endpoint Management service](#).

To see why to migrate, how to migrate, and the benefits of migrating to Citrix Endpoint Management, visit the [CEM Migration Service Course Catalog](#).

When you are evaluating or purchasing Endpoint Management, the Endpoint Management Operations team provides ongoing onboarding help. The Operations team also communicates with you to ensure that the core Endpoint Management services are running and configured correctly. This figure shows the onboarding steps.



To sign up for a Citrix account and request an Endpoint Management trial, contact your Citrix Sales Representative. When you're ready to proceed, go to <https://onboarding.cloud.com>.

For a quick overview of Endpoint Management onboarding and configuration, watch this video.

[This is an embedded video. Click the link to watch the video](#)

Want to learn more before starting? Try these resources:

**Endpoint Management documentation:** Provides full Endpoint Management documentation, from onboarding to initial configuration to advanced configuration. A “What’s new” article describes new features and fixes. Citrix notifies you when that article is available for a new release.

**Citrix Endpoint Management Onboarding Handbook:** Consolidates all the available information around Endpoint Management, so you can proceed in smoothly enabling and onboarding Endpoint Management. You can use the document to record changes for your internal processes and to document your high-level and functional designs.

**Endpoint Management Deployment Handbook:** Planning an Endpoint Management deployment involves many considerations. The handbook includes recommendations, common questions, and use cases for your Endpoint Management environment.

**SalesIQ:** More resources for our Citrix Partners.

### Next steps

For information about the Endpoint Management onboarding process, see [Onboarding and resource setup](#).

After you complete onboarding, see [Prepare to enroll devices and deliver resources](#).

## Deprecation announcements

For advanced notice of the Citrix Endpoint Management features that are being phased out, see [Deprecation](#).

## Endpoint Management support

For details on how to access supported related information and tools in the Endpoint Management console, see [Monitor and support](#).

Rolling updates to the Endpoint Management release occur approximately every two weeks. To you, the customer, this process is transparent. Initial updates are applied to Citrix internal sites only, and are then applied to customer environments gradually. We deliver updates incrementally in waves to ensure product quality and to maximize availability.

Endpoint Management customers receive updates and communications directly from the Endpoint Management Cloud Operations Team. Those updates keep you current with new features, known issues, fixed issues, and so on.

The Citrix Cloud Operations team maintains the Endpoint Management environments with the latest Endpoint Management rolling patches. To obtain specific patches or fixes that are required before the rolling patch, contact Citrix Technical Support.

If you have any issues with your environment, contact Citrix Technical Support or your Citrix Account Team. Such issues might include mobile device enrollment, Endpoint Management console access, or Secure Mail issues.

If you need any integration or changes made on Citrix Gateway in the Cloud or Endpoint Management, submit a request through Citrix Technical Support.

Examples of changes that you might request are:

- Citrix Files integration with Citrix Gateway in the Cloud
- Change Citrix Gateway authentication type
- Validate connectivity to customer data center resources
- Change split tunnel configuration for micro VPN
- Restart Endpoint Management components due to some server configuration changes

## Service level agreement

Citrix Endpoint Management uses industry best practices to achieve cloud scale and a high degree of service availability.

For complete details about Citrix's commitment for availability of Citrix Cloud services, see the [Service Level Agreement](#).



## What's new

October 28, 2021

Citrix aims to deliver new features and product updates to Endpoint Management customers when they're available. New releases provide more value, so there's no reason to delay updates.

- Rolling updates to Endpoint Management release approximately every two weeks.
- These updates don't result in any downtime for your instance or device users.
- Not every release has new features and some updates include fixes and performance enhancements.

To you, the customer, this process is transparent. We apply initial updates to Citrix internal sites only, and then to customer environments gradually. Delivering updates incrementally in waves helps to ensure product quality and to maximize availability.

You also receive Endpoint Management updates and communications directly from the Endpoint Management Cloud Operations Team. Those updates keep you current with new features, known issues, fixed issues, and so on.

For more details, including cloud scale and service availability, see the Endpoint Management [Service Level Agreement](#). To monitor service interruptions and scheduled maintenance, see the [Service Health Dashboard](#).

### **Continued support for the Classic policies deprecated from Citrix ADC**

Citrix recently announced the deprecation of some Classic policy-based features starting with Citrix ADC 12.0 build 56.20. The Citrix ADC deprecation notices have no impact to existing Endpoint Management integrations with Citrix Gateway. Citrix Endpoint Management continues to support the Classic policies and no action is needed.

### **Before upgrading endpoints to iOS 14.5**

Before upgrading any endpoint to iOS 14.5, Citrix recommends that you perform the following actions to mitigate app crashes:

- Upgrade Citrix Secure Mail and Secure Web to 21.2.X or higher. See [Upgrade MDX or enterprise apps](#).
- If you use the MDX Toolkit, wrap all third-party iOS applications with MDX Toolkit 21.3.X or higher and upgrade those apps in the Endpoint Management console. Check the MDX Toolkit [download page](#) for the latest version.

## **Before you upgrade an on-premises Citrix ADC to 13.0-64.35+**

If you use the on-premises version of Citrix ADC and upgrade to version 13.0–64.35+: Perform the workaround described in [Known issues in Endpoint Management 20.10.1](#).

## **Endpoint Management 21.10.1**

The following features are now rolling out to commercial customers. Releases to US government customers begin within three months. For feature differences between the commercial and US government offerings, see [Endpoint Management service for US Government](#).

**Lock device after inactivity extension.** The maximum amount of time of inactivity before a device locks has been increased to 15 minutes. For more information, see [Passcode device policy](#).

**Added the restriction setting for pasting content from iOS apps.** The restrictions device policy now supports **Require managed pasteboard** for iOS. With this restriction setting, you can block or allow the pasting of content from managed apps to unmanaged apps, and the opposite way.

This setting applies to iOS 15 and later. For more information, see [Restrictions device policy for iOS](#).

## **Fixed issues in Endpoint Management 21.10.1**

The network policy fails to deploy to iOS and macOS devices using WPA2 and WPA3 network security types. [CXM-96166]

## **Endpoint Management 21.10.0**

The following features are now rolling out to commercial customers. Releases to US government customers begin within three months. For feature differences between the commercial and US government offerings, see [Endpoint Management service for US Government](#).

**Assign custom roles for cloud administrators in Citrix Cloud.** New Endpoint Management customers onboarded after October 4, 2021 can now assign custom roles to cloud administrators in Citrix Cloud. Before, you had to assign custom roles in Endpoint Management. This feature lets you perform your administrator-related customizations without having to switch between Citrix Cloud and Endpoint Management. In addition, the **COSU devices enroller** and **Shared devices enroller** templates were removed from Endpoint Management. **COSU devices enroller** is now handled through enrollment profiles and **Shared devices enroller** is handled at the platform level with kiosk mode or Citrix Launcher.

**Support for Windows 11 devices.** You can now use Endpoint Management to manage Windows 11 devices. For more information, see [Operating system support list](#).

**iOS User Enrollment mode is now available as a public preview.** You can now take advantage of Apple User Enrollment features on iOS and iPadOS devices. User Enrollment integrates Managed Apple

IDs to create a user identity on devices. For more information about User Enrollment, see [Managed Apple IDs](#).

**Updated maximum value for tracking iOS device location.** You can now configure the location policy to track the location of an iOS device for up to 10 hours. See [Location device policy](#).

### **Fixed issues in Endpoint Management 21.10.0**

When updating an administrator role in the Citrix Cloud console, the change is not reflected in the Citrix Endpoint Management console. This is strictly a user interface issue and does not impact any functionality. Only customers onboarded in version 21.10.0 or later are affected. [CXM-101044]

### **Endpoint Management 21.9.1**

The following features are now rolling out to commercial customers. Releases to US government customers begin within three months. For feature differences between the commercial and US government offerings, see [Endpoint Management service for US Government](#).

**Configure Azure AD or Okta as an identity provider to enroll and manage user devices without a Cloud Connector (Preview).** If you configure an identity provider through Citrix Cloud, you don't need a Cloud Connector to establish communication between Endpoint Management and Citrix Cloud. Endpoint Management still requires a Cloud Connector for the following:

- LDAP
- PKI Server
- Internal DNS queries
- Citrix Virtual Apps

For more information about this feature, see [Identity provider authentication without a Cloud Connector](#).

**Support for iOS 15 and macOS 12 devices.** You can now use Endpoint Management to manage iOS 15 and macOS 12 devices. For more information, see [Operating system support list](#).

**Always-on VPN for Android Enterprise.** You can now enable an always-on VPN for Android Enterprise devices. You can choose to enable a lockdown feature as well. Apps require a VPN connection to access the network unless you exclude them from the lockdown. For more information, see [VPN device policy](#).

**Fully managed Android 11+ devices enroll in work profile on corporate-owned devices mode.** The new mode further separates the personal and work profiles on a device. This change offers an organization greater control on the managed profile and offers users more privacy on their personal profile. For more information, see [Android Enterprise](#).

**Ability to set global consent for client apps.** You can now set global consent so that users don't need to provide consent on each device. For details, see [Configure Endpoint Management for Azure AD compliance management](#).

**Azure AD permissions changes now detected.** When a change occurs in Azure AD permissions, Endpoint Management now warns automatically about the change so you can approve it using the **Azure AD compliance management** setting. Follow the consent link and click **Approve** to accept the changes. Previously, you had to initiate this approval manually. For more information, see [Configure Endpoint Management for Azure AD compliance management](#).

### **Fixed issues in Endpoint Management 21.9.1**

If you add deployment rules to a delivery group, any new or existing deployment rules at the resource level (policies, apps, actions) no longer apply. [CXM-98013]

The Export Data feature of Endpoint Management doesn't export complete sets of data. Use these workarounds to retrieve data about managed devices:

- Export data from the console by navigating to **Analyze > Reporting > Device Enrollment**.
- Export data by using the reporting API. For information about the reporting API, see the [developer documentation](#). [CXM-99906]

If accessing Endpoint Management through Citrix Cloud, adding an enterprise app for macOS causes an authorization error to occur. As a workaround, contact support and request direct access to your Endpoint Management console. You can then add enterprise apps for macOS devices. [CXM-100046]

## **Current known issues**

### **Known issues in Endpoint Management 21.10.0**

The following device policies don't work properly on managed Windows 11 devices:

- App inventory
- Kiosk
- VPN

We reported these issues to Microsoft and are working with Microsoft to resolve them. We will keep you updated on any progress.

### **Known issues in Endpoint Management 21.9.1**

When creating an enrollment profile for Android devices to enroll in the work profile on corporate-owned devices mode, you must enable the **BYOD work profile** setting. If you don't enable this setting, the devices fail to enroll. [CXM-100418]

On Android devices enrolled in work profile on corporate-owned devices mode: If users see errors saying that they can't install or search apps on their personal profile, update the Google Play Store app and try again. [CXM-100678]

Intermittently, when you click **Export Configuration Script** from the **Settings > Citrix Gateway** page, you receive a corrupt CSV file. As a workaround, download the configuration script while adding or editing a Citrix Gateway configuration. [CXM-100908]

### **Known issues in Endpoint Management 21.5.0**

Users can't authenticate to Azure Active Directory (AAD) if they:

1. Enroll their device in Endpoint Management using AAD credentials.
2. Launch an Office 365 app and complete the AAD registration.
3. Remove their account from the Microsoft Authenticator app.
4. Launch an Office 365 app and sign out.

As a workaround, unenroll the device from Endpoint Management and re-enroll. [CXM-90235]

### **Known issues in Endpoint Management 21.4.0**

Re-enrollment fails on iOS devices if the user trying to re-enroll is a different Azure Active Directory user than the user originally enrolled on the device. As a workaround, unregister the original user from the Microsoft Authenticator app on the device before re-enrolling. [CXM-90218]

When you use a package ID to search for a Google Play app to add to the Endpoint Management console, the mandatory **Name** field displays as empty. You can still enter the app name manually. [CXM-93655]

### **Known issues in Endpoint Management 21.2.0**

When adding Secure Web as an MDX app for Android Enterprise, Managed Google Play can't find the app using the app identifier. If you search for "Secure Web" instead of the app identifier, Managed Google Play can find the app. This issue is a Google bug. [CXM-91991]

Importing the SSL Listener certificate might fail. Repackage the certificate keystore by following the steps in [CTX-297153](#). [XMHELP-3346]

### **Known issues in Endpoint Management 21.1.1**

Accessing the new Endpoint Management console may result in a 401 error. Your account may not be added to Endpoint Management properly. For steps to resolve the issue, see [Citrix Endpoint Management console error "Failed to retrieve"](#). [CXM-92007]

### Known issues in Endpoint Management 20.12.0

In the **Monitor** tab, devices don't appear as assigned to enrolled Active Directory users and you can't perform security actions. To see the policies and apps assigned to those users and perform all security actions, go to **Manage > Devices**. [CXM-90210]

You can't access the Endpoint Management console by clicking **Manage** from the **Citrix Cloud** tile on Internet Explorer 11. Access the console from another browser. Internet Explorer 11 is no longer supported for console use. [CXM-90540]

You can't wrap iOS apps developed on macOS 10.14 and later using the MDX Service. To add iOS apps with MAM SDK or MDX functionality, prepare the app with the MAM SDK or wrap the apps using the on-premises MDX Toolkit. [XMHELP-3174]

### Known issues in Endpoint Management 20.10.1

If you upgrade on-premises Citrix ADC to 13.0-64.35 or later, and Endpoint Management isn't Workspace-enabled: Single sign-on to Citrix Files or the ShareFile domain URL in a browser with the **Company Employee Sign in** option results in an error. The user is unable to sign in.

To work around this issue: If you haven't already run the following commands from the ADC CLI on Citrix Gateway, run them to enable global SSO:

```
set vpn parameter SSO ON  
bind vpn vs <vsName> -portalTheme X1
```

For more information, see:

- [Citrix ADC Release](#)
- [Impacted SSO configurations](#)

After you complete the workaround, users can authenticate to Citrix Files or the ShareFile domain URL using SSO in a browser with the **Company Employee Sign in** option. [CXM-88400]

### Known issues in Endpoint Management 20.5.0

At the beginning of June 2020, the Google Play EMM API had an outage. During the outage, if you went to **Settings > Android Enterprise**, Endpoint Management removed the Android Enterprise configuration from the console. As a result, currently enrolled devices don't receive the policy and app updates. To fix the issue, contact Citrix Technical Support for assistance. [XMHELP-2811]

### Known issues in Endpoint Management 20.4.1

When you install multiple LDAP Active Directories (AD) on Endpoint Management using Citrix Cloud Connector, only the first installed AD populates in the Endpoint Management settings. As a

workaround, you can check Citrix Cloud. If those domains are marked as unused, manually mark **Used**. Marking the domain as used makes it available in Endpoint Management. [CXM-81697]

### **Known issues in Endpoint Management 20.2.1**

For customers using a cloud hosting service and the new Citrix enhanced enrollment profiles: New devices may not successfully enroll. As a work-around, create a default enrollment profile that includes all delivery groups. See [To create an enrollment profile](#). You might see an enrollment profile titled “FactoryDefault”. We use this enrollment profile for special logic. If you see the “FactoryDefault” enrollment profile, don’t modify or delete it. [CXM-79019]

After configuring Citrix Content Collaboration with a ShareFile URL in the Citrix Endpoint Management console, clicking the **Test Connection** button results in an error. To resolve this issue, disable multi-factor authentication for ShareFile. Learn more about this issue and the workaround on this [support page](#). [CXM-79240]

Sorting devices by **Last access** or **Inactivity days** results in a 500 internal server error. [CXM-79414]

### **Known issues in Endpoint Management 20.1.0**

You can’t delete duplicate certificate files from **Settings > Certificates**. [CXM-72630]

When adding users to a library in Citrix Cloud, Endpoint Management reports success, but the users aren’t added. [CXM-73726]

### **Known issues in Endpoint Management 19.11.0**

MDX and Public apps can’t be deleted from the console. As a workaround, select the app you want to delete and then click **Edit**. Deselect **Android Enterprise** and select any other platforms from the platform list. Save the app. You can then delete the app. [CXM-74468]

For sites with Workspace Environment Management (WEM) integrated with Endpoint Management: A Windows GPO configuration device policy created with User Configuration doesn’t deploy to user devices. A policy created with Device Configuration deploys as expected. [CXM-74762, WEM-6319]

### **Known issues in Endpoint Management 19.9.0**

The **Settings > Apple Deployment Program** page doesn’t include skip options for the new iOS 13 Setup Assistant screens. During enrollment, users must click through screens for Express Language, Preferred Language, Get Started, and Appearance. [CXM-71370]

### **Known issues in Endpoint Management 19.5.0**

On macOS, enterprise apps pushed from Endpoint Management remain in a pending state. This third-party issue is Apple bug #50311461 and is fixed in macOS 10.14.4. [CXM-65957]

When enrolling a Citrix Ready workspace hub device, define the Ethernet (eth0) MAC address in the allow list to avoid failed enrollment. [CXM-43141]

### **Known issues in Endpoint Management 19.4.1**

The **Monitor** tab doesn't appear. [DIR-7483]

When tabbing through options in the Windows GPO device policy, radio buttons and check boxes get skipped. [CXM-58277]

### **Known issues in Endpoint Management 19.2.1**

If you unenroll an Android Enterprise enterprise by deleting it through the Google admin console: Attempts to re-enroll the enterprise might fail. Always use the Endpoint Management console to unenroll an Android Enterprise enterprise, as described in [Unenroll an Android Enterprise enterprise](#). Google Workspace customers, follow the instructions in [Unenrolling an Android Enterprise enterprise](#). [CXM-62709] [CXM-62950]

### **Known issues in Endpoint Management 19.2.0**

When creating a public store app in Endpoint Management 10.18.3: On the iPad App Settings page, if you click **Back** without searching for apps, and then you click **Next**, the following issue occurs. The navigation buttons appear unresponsive and don't allow you to search for apps. The issue occurs when creating public store apps for both iOS or Android. [CXM-46820]

### **Known issues in Endpoint Management 10.19.1**

After you complete the registration process on the **Settings > Android Enterprise** page, the following error message appears: "A configuration error occurred. Please try again". When you close the error message, your Android Enterprise configuration is saved, however **Enable Android Enterprise** is **Off**. To work around this issue, reduce the number of app categories to 30 or fewer. [CXM-60899]

### **Known issues in Endpoint Management 10.18.19**

When tabbing through options in the Windows GPO device policy, radio buttons and check boxes get skipped. [CXM-58277]



### **Known issues in Endpoint Management 10.18.5**

When a Chrome app is configured as a required app for Chrome OS devices: Users might need to log off and log back on to install the app. This third-party issue is Google bug ID #76022819. [CXM-48060]

### **Known issues in Endpoint Management 10.18.3**

After you delete a Citrix Cloud administrator who has a device enrolled: Endpoint Management doesn't update the User Role in the Endpoint Management console until after the administrator logs in again from Secure Hub or the Self-Help Portal. [CXM-45730]

### **Known issues in Endpoint Management 10.7.4**

If you configure Endpoint Management for single sign-on using the Citrix identity provider with Azure Active Directory: When an Endpoint Management administrator or user gets redirected to the Azure Active Directory sign-in screen, the screen includes the message "Sign-in page for Citrix Secure Hub." The correct message is "Sign-in page for Citrix Endpoint Management console." [CXM-42309]

### **Known issues in Endpoint Management 10.7.3**

For devices running Windows 10 RS3 Version 1709 build 16299.19: App Configuration device policies created by importing a Citrix Receiver ADMX file might fail when pushed to those devices. This third-party issue is Microsoft bug ID #14280113. [CXM-40521]

## **Third-party notices**

April 3, 2020

Citrix Endpoint Management might include third-party software licensed under the terms defined in the following document:

[Citrix Endpoint Management Third-Party Notices](#)

## **Deprecation**

October 22, 2021

The announcements in this article are advanced notice of the Citrix Endpoint Management features that are being phased out, so that you can make timely business decisions. Citrix monitors customer

use and feedback to determine when they are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality. For details about product lifecycle support, see the [Product Lifecycle Support Policy](#) article.

## Deprecations and removals

The following list shows the Citrix Endpoint Management features that are deprecated or removed.

*Deprecated* items are not removed immediately. Citrix continues to support a deprecated item until removing it in a future release.

*Removed* items are either removed, or are no longer supported, in Citrix Endpoint Management.

For information about the mobile productivity apps that reached End of Life, see [EOL and deprecated apps](#).

Item	Description	Deprecation announced	Removed	Alternative
MDX Toolkit	Deprecate support for the MDX Toolkit in favor of the Mobile App Management (MAM) SDK. During the transition period, you can use both MDX wrapped apps and MAM SDK developed apps.	March 2020	Target: March 2022	To continue managing your enterprise applications, use the MAM SDK.

Item	Description	Deprecation announced	Removed	Alternative
RBAC Role - Shared devices enroller and COSU devices enroller	Deprecate support for predefined Role Based Access Control settings for both Shared devices enroller and COSU devices enroller	July 2021	Target Q4 2021	Configure iOS devices through <a href="#">Apple School Manager</a> or <a href="#">Apple Business Manager</a> . Configure Android COSU (dedicated) devices through <a href="#">enrollment profiles</a> .
Allow auto-connect to Wi-Fi sense hotspots restriction for Windows devices.	Remove support for the Allow auto-connect to Wi-Fi sense hotspots restriction for Windows 10 devices. Windows 10 no longer supports this feature. For information, see <a href="#">Microsoft documentation</a> .	October 2021	Target: Q1 2022	No alternative
MDX: Alternative Gateway Server	Deprecate step-up authentication for iOS and Android devices.	March 2020	Target: September 2021	No alternative

Item	Description	Deprecation announced	Removed	Alternative
MDX: Micro VPN (full tunnel mode)	Deprecated a full virtual private network (VPN) tunnel for iOS and Android devices.	March 2020	Target: September 2021	Use the MAM SDK Web SSO mode or create a per-app VPN policy with the Citrix SSO connection type.
MDX: PAC file support	Deprecated support for a Proxy Automatic Configuration (PAC) file with a full VPN tunnel deployment for iOS and Android devices.	March 2020	Target: September 2021	Use Citrix Gateway to connect through a proxy server for access to internal networks.
MDX shared device support	Deprecated shared device support for MDX apps.	March 2020	Target: June 2021 for new deployments. September 2021 for existing deployments using the feature.	For Android Enterprise, use shared devices enrolled as dedicated devices. For iOS, use Apple School Manager or GroundControl.
Android - Sony	Deprecated support for Android Sony devices and Sony-specific policies.	January 2021	Target: Q3 2021	Use Android Enterprise

Item	Description	Deprecation announced	Removed	Alternative
Android - HTC	Deprecated support for Android HTC devices and HTC-specific policies.	January 2021	Target: Q3 2021	Use Android Enterprise
Knox Mobile Enrollment (legacy DA)	Deprecated support for Knox Mobile Enrollment (KME) in the legacy Device Administrator mode on all Android versions.	May 4, 2021	Target: Q3 2021	Use KME to enroll in Android Enterprise mode. Android 8, 9, 10, 11 support Android Enterprise.
High Security enrollment mode	Deprecated support for generating enrollment invitations with the <b>High Security</b> enrollment security mode.	July 2021	Target: Q3 2021	See <a href="#">Enrollment invitations</a> for a list of supported enrollment security modes.
Derived credentials	Deprecated support for derived credentials and the Citrix Derived Credential Manager app.	March 25, 2021	Target: October 2021	See <a href="#">iOS</a> for a list of authentication types supported for iOS.

Item	Description	Deprecation announced	Removed	Alternative
APNs outgoing ports	Apple support for the APNs legacy binary protocol ends as of March 31, 2021. Apple recommends that you use the HTTP/2-based APNs provider API instead. As part of this change, we are deprecating support for ports 2195 and 2196, used to send APNs notifications to <a href="https://*.push.apple.com">*.push.apple.com</a> .	October 2020	Target: March 31, 2021	Use port 443 instead. See <a href="#">Network and firewall requirements</a> .
MDX Service	Deprecated support for the MDX Service in favor of the Mobile App Management (MAM) SDK. During the transition period, you can use both MDX wrapped apps using MDX toolkit and MAM SDK developed apps.	March 2020	September 2021	To continue wrapping your enterprise applications, use the MDX toolkit.

Item	Description	Deprecation announced	Removed	Alternative
Enrollment invitation setup in the Self-Help Portal	Deprecated support for users to generate enrollment invitations from the Self-Help Portal.	July 2021	July 2021	Contact your administrator to generate enrollment invitations in the Endpoint Management console.
Enrollment invitation setup	Deprecated support for using a device IMEI, serial number, and UDID to create an enrollment invitation.	April 2021	July 2021	When you create an enrollment invitation, configure the available settings under <b>Manage &gt; Enrollment Invitations</b> in the Endpoint Management console.
Certificate-based authentication signature algorithms (non-FIPS and weak ciphers)	Deprecated support for the following signature algorithms: SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA/ SHA1withDSA, RIPEMD160withRS RIPEMD128withRS RIPEMD256withRS	May 2020	June 2021	When you create a CSR for a credential provider in the Endpoint Management console ( <b>Settings &gt; Credential Providers &gt; Certificate Signing Request</b> ), choose a stronger cipher.

Item	Description	Deprecation announced	Removed	Alternative
Citrix mobility apps and Workspace apps for Android 7.x and iOS 12.x	Deprecated support for the Android 7.x and iOS 12.x versions of Secure Hub, Secure Mail, Secure Web, and Citrix Workspace app.	April 2021	June 2021	Use, at a minimum, the current and prior version of each major operating system platform. Older devices remain enrolled. However, Citrix doesn't test or support the legacy devices.
RSA soft token support for Android	Deprecated support for the direct import of RSA soft tokens into Secure Hub for Android.	January 2021	February 2021	You can import the RSA soft token inside the RSA secure ID app available in Google Play. You can then use the token for Citrix Gateway authentication.
Internet Explorer 11	Deprecated support of Internet Explorer use with the Endpoint Management console.	January 2021	January 2021	Use the latest version of these web browsers: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari



Item	Description	Deprecation announced	Removed	Alternative
Gateway configuration checks in Endpoint Management Analyzer	Deprecated support for the Gateway configuration check option.	November 2020	November 2020	Use the Citrix Insight Services check in Analyzer to check your Citrix ADC configurations for Endpoint Management deployment readiness. See <a href="#">Endpoint Management Analyzer</a> .
Apps published for the legacy Device Administrator mode on Android Enterprise devices	We no longer deliver apps published for the legacy DA platform to devices enrolled in Android Enterprise.	October 2020	November 2020	For Android Enterprise devices, publish apps for the Android Enterprise platform. To continue to publish legacy DA apps to devices in DA mode, create a separate delivery group for those apps.

Item	Description	Deprecation announced	Removed	Alternative
Legacy Device Administrator mode for Android 10 devices	Google deprecated some Device Administrator APIs. Citrix doesn't support Android 10 devices enrolled into Device Administrator mode as of the upgrade to Citrix Secure Hub that targets Android API level 29.	February 2020	November 2020	Migrate Android 10 devices to Android Enterprise.
Android TouchDown	DigiCert stopped supporting Android TouchDown. Citrix removed the Android TouchDown platform page from the Exchange device policy.	July 2018	November 2020	Recommendation: Use Citrix Secure Mail.

Item	Description	Deprecation announced	Removed	Alternative
New Device Administrator enrollments for Android 10	Deprecated support for new enrollments or re-enrollments into the legacy Device Administrator mode on Android 10 devices. Already enrolled devices continue to work.	February 2020	September 2020	Enroll new Android 10+ devices into Android Enterprise.
MDX encryption	Deprecated MDX encryption and the MDX encryption feature in the Endpoint Management console.	October 2019	September 2020	Enable iOS or Android platform encryption using our Encryption Management feature with added compliance checking. Ensure you have tested and planned for migration off MDX encryption by July 2020.
Windows Mobile/CE	Deprecated support for Windows Mobile/CE devices.	April 2018	September 2020	Use Windows 10 Desktop and Laptop.

Item	Description	Deprecation announced	Removed	Alternative
Samsung SEAMS container	Deprecated support for the Samsung SEAMS container.	June 2020	August 2020	Use the Samsung Knox Service Plugin (KSP) app for Android Enterprise. See <a href="#">Add the Knox service plug-in app</a> .
Remote Support	Deprecated the Remote Support client.	January 2019	August 2020	No alternative
Citrix mobility apps and Workspace apps for Android 6.x and iOS 11.x	Deprecated support for the Android 6.x and iOS 11.x versions of Secure Hub, Secure Mail, Secure Web, and Citrix Workspace app.	April 2020	June 2020	Use, at a minimum, the current and prior version of each major operating system platform. Older devices remain enrolled. However, Citrix doesn't test or support the legacy devices.
Secure Hub Network Extensions for iOS	Deprecated the Network Extension framework that allowed you to customize networking features for iOS devices. Secure Hub release 20.3.0.	October 2018	March 2020	No alternative

Item	Description	Deprecation announced	Removed	Alternative
API sign in using local accounts	Administrators will no longer be able to sign in to the REST API using a local account.	October 2020		Administrators can log in using a Citrix Cloud account. See <a href="#">REST API</a> .
Self-signed Secure Sockets Layer (SSL) certificates	Deprecated support for self-signed SSL certificates for all device platforms.	May 2020		Replace your existing self-signed certificate with a trusted SSL certificate from a well-known certificate authority (CA).

## System requirements

July 28, 2021

While waiting for Citrix to provision Endpoint Management, be sure to prepare for your Endpoint Management deployment by installing Cloud Connector. Although Citrix hosts and delivers your Endpoint Management solution, some communication and port setup is required. That setup connects the Endpoint Management infrastructure to corporate services, such as Active Directory.

### Cloud Connector requirements

Citrix uses Cloud Connector to integrate the Endpoint Management architecture into your existing infrastructure. Cloud Connector integrates the following resource locations to Endpoint Management securely over port 443: LDAP, PKI Server, internal DNS queries, and Citrix Workspace enumeration.

- At least two dedicated Windows Server machines that are joined to your Active Directory domain. The machines can be virtual or physical. The machine where you are installing the Connector must be in sync with UTC time for proper installation and operation. For a full list of the latest requirements, see the deployment materials provided by your Citrix Account Team.

The onboarding wizard guides you through installing Cloud Connector on those machines.

- For more platform system requirements, see [Citrix Cloud Connector](#).

### Supported Active Directory functional levels

For use with Endpoint Management, the Citrix Cloud Connector supports the following forest and domain functional levels in Active Directory.

Forest Functional Level	Domain Functional Level	Supported Domain Controllers
Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2016	Windows Server 2016
Windows Server 2012	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2016	Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012 R2	Windows Server 2016	Windows Server 2016
Windows Server 2016	Windows Server 2016	Windows Server 2016

### Citrix Gateway requirements

Endpoint Management requires a Citrix Gateway installed in your resource location for the following scenarios:

- You require a micro VPN for access to internal network resources for line-of-business apps. Those apps are wrapped with Citrix MDX technology. The micro VPN needs Citrix Gateway to

connect to internal back-end infrastructures.

- You plan to use Citrix mobile productivity apps, such as Citrix Secure Mail.
- You plan to integrate Endpoint Management with Microsoft Endpoint Manager.

The requirements:

- Domain (LDAP) authentication
- Citrix Gateway 12.1 or above, with a Platform/Universal license

For details, see [Licensing](#).

- Public SSL Certificate.

For details, see [Create and Use SSL Certificates on a Citrix ADC Appliance](#).

- Unused public IP address for Citrix Gateway Virtual Server
- Publicly resolvable Fully Qualified Domain Name (FQDN) for Citrix Gateway Virtual Server
- Cloud-hosted Endpoint Management Intermediate and Root certificates (provided in the script bundle)
- Unused internal private IP address for the proxy load balancer IP
- For port requirements, see Citrix Gateway port requirements later in this article.
- [Citrix Endpoint Management integration with Microsoft Endpoint Manager](#)
- [Deploy Citrix ADC VPX instance on Microsoft Azure](#)

For information about Citrix Gateway requirements, see the deployment materials provided by your Citrix Account Team.

For information about Android Enterprise requirements, see the [Android Enterprise](#) section.

### **Citrix Files requirements**

Citrix Files file sync and sharing services are available in the Endpoint Management Premium Service offering. Storage zones controller extends the Citrix Files software as a service (SaaS) cloud storage by providing your Citrix Files account with private data storage.

Storage zones controller requirements:

- A dedicated physical or virtual machine
- Windows Server 2012 R2 or Windows Server 2016
- 2 vCPUs
- 4 GB RAM
- 50 GB hard disk space
- Server roles for Web Server (IIS):
  - Application Development: ASP.NET 4.5.2

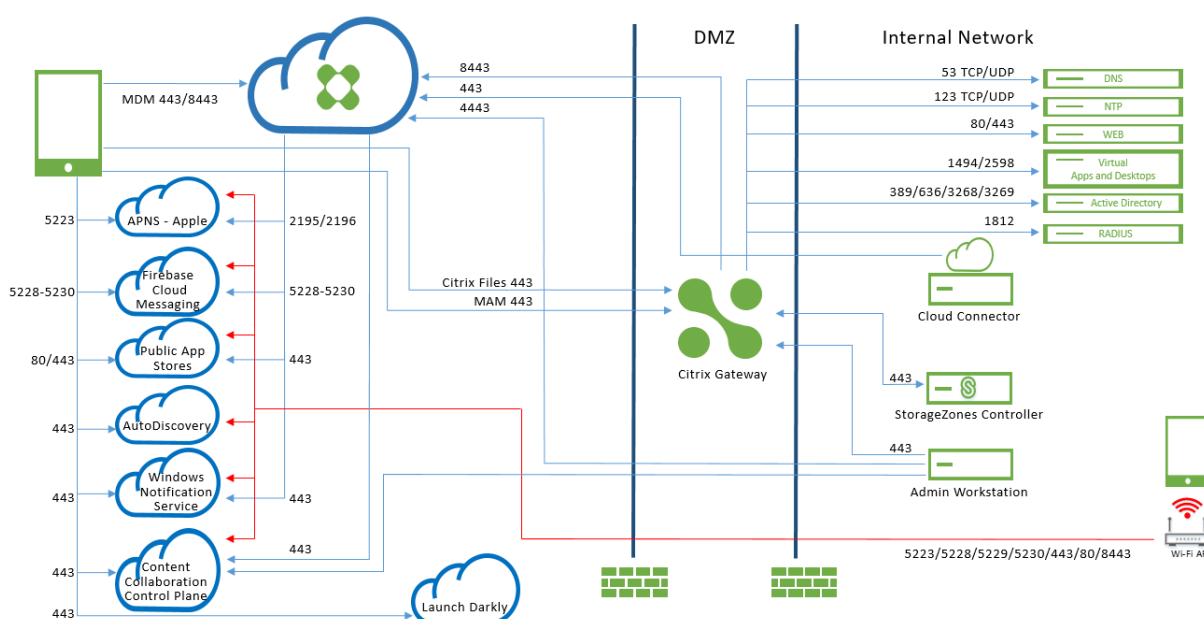
- Security: Basic Authentication
- Security: Windows Authentication

Citrix Files platform requirements:

- The Citrix Files installer requires administrative privileges on the Windows Server
- Citrix Files Admin user name

## Port requirements

To enable devices and apps to communicate with Endpoint Management, you open specific ports in your firewalls. The following diagram shows the traffic flow for Endpoint Management.



The following sections list the ports that you must open. For information about the URLs that mobile productivity apps use, see [Feature flag management](#).

## Citrix Gateway port requirements

Open ports to allow user connections from Citrix Secure Hub and Citrix Workspace through Citrix Gateway to:

- Endpoint Management
- StoreFront
- Other internal network resources, such as intranet websites

For more information about Citrix Gateway, see [Configuring Settings for your Citrix Endpoint Management Environment](#) in the Citrix Gateway documentation. For information about IP addresses, see [How Citrix Gateway uses IP addresses](#) in the Citrix Gateway documentation.



TCP Port	Description	Source	Destination
53 (TCP and UDP)	Used for DNS connections.	Citrix Gateway SNIP	DNS server
80/443	Citrix Gateway passes the micro VPN connection to the internal network resource through the second firewall.	Citrix Gateway SNIP	Intranet websites
123 (TCP and UDP)	Used for Network Time Protocol (NTP) services.	Citrix Gateway SNIP	NTP server
389	Used for insecure LDAP connections.	Citrix Gateway NSIP (or, if using a load balancer, SNIP)	LDAP authentication server or Microsoft Active Directory
443	Used for connections to StoreFront from Citrix Workspace to Citrix Virtual Apps and Desktops.	Internet	Citrix Gateway
443	Used for connections to Endpoint Management for web, mobile, and SaaS app delivery.	Internet	Citrix Gateway
443	Used for Cloud Connector communication – LDAP, DNS, PKI & Citrix Workspace enumeration	Cloud Connector Servers	<a href="https://*.citrixworkspacesapi.net">https://*.citrixworkspacesapi.net</a> , <a href="https://*.cloud.com">https://*.cloud.com</a> (commercial), <a href="https://*.cloud.us">https://*.cloud.us</a> (government), <a href="https://*.blob.core.windows.net/">https://*.blob.core.windows.net/</a> , <a href="https://*.servicebus.windows.net">https://*.servicebus.windows.net</a>

TCP Port	Description	Source	Destination
443	Used for accessing the Endpoint Management Self-Help Portal, if enabled, through the browser.	Access point (browser)	Endpoint Management ( <a href="https://&lt;sitename&gt;/zdm/shp">https://&lt;sitename&gt;/zdm/shp</a> )
636	Used for secure LDAP connections.	Citrix Gateway NSIP (or, if using a load balancer, SNIP)	LDAP authentication server or Active Directory
1494	Used for ICA connections to Windows-based applications in the internal network. Citrix recommends keeping this port open.	Citrix Gateway SNIP	Citrix Virtual Apps and Desktops
1812	Used for RADIUS connections.	Citrix Gateway NSIP	RADIUS authentication server
2598	Used for connections to Windows-based applications in the internal network using session reliability. Citrix recommends keeping this port open.	Citrix Gateway SNIP	Citrix Virtual Apps and Desktops
3269	Used for Microsoft Global Catalog secure LDAP connections.	Citrix Gateway NSIP (or, if using a load balancer, SNIP)	LDAP authentication server or Active Directory
4443	Used for accessing the Endpoint Management console by an administrator through the browser.	Access point (browser)	Endpoint Management

TCP Port	Description	Source	Destination
8443	Used for enrollment, app store, and mobile app management (MAM).	Citrix Gateway SNIP	Endpoint Management
8443	Secure Ticket Authority (STA) port used for Secure Mail authentication token	Citrix Gateway SNIP	Endpoint Management

### **Network and firewall requirements**

To enable devices and apps to communicate with Endpoint Management, you open specific ports in your firewalls. The following tables list those ports.

Open ports from the internal network to Citrix Cloud:

TCP port	Source IP	Description	Destination	Destination IP
443		Cloud Connector	<a href="https://*.citrixworkspac.net">https://*.citrixworkspac.net</a> , <a href="https://*.cloud.com">https://*.cloud.com</a> (commercial), <a href="https://*.cloud.us">https://*.cloud.us</a> (government), <a href="https://*.sharefile.com">https://*.sharefile.com</a> , <a href="https://cwsproduction.blob.core.windows.net/downloads">https://cwsproduction.blob.core.windows.net/downloads</a> , <a href="https://*.servicebus.windows.net">https://*.servicebus.windows.net</a>	
443		Administrative Console	<a href="https://*.citrixworkspacesapi.net">https://*.citrixworkspacesapi.net</a> , <a href="https://*.cloud.com">https://*.cloud.com</a> (commercial), <a href="https://*.cloud.us">https://*.cloud.us</a> (government), <a href="https://*.citrix.com">https://*.citrix.com</a> , <a href="https://cwsproduction.blob.core.windows.net/downloads">https://cwsproduction.blob.core.windows.net/downloads</a>	

TCP port	Source IP	Description	Destination	Destination IP
443		Endpoint Management Self-Help Portal access through a browser (if the portal is enabled)	Endpoint Management	
4443		Endpoint Management console access through a browser	Endpoint Management	

Open ports from the Internet to the DMZ:

TCP port	Description	Source IP	Destination	Destination IP
443	Endpoint Management Client Device		Citrix Gateway	
443	Endpoint Management Client Device		Citrix Gateway VIP	
443	Citrix Files Public IP	<a href="#">CTX208318</a>	Citrix Gateway VIP	

Open ports from the DMZ to the internal network:

TCP port	Description	Source IP	Destination	Destination IP
389 or 636	Citrix Gateway NSIP		Active Directory	
53 (UDP)	Citrix Gateway NSIP		DNS Server IP	
443	Citrix Gateway SNIP		Exchange (EAS) Server IP	

TCP port	Description	Source IP	Destination	Destination IP
443	Citrix Gateway SNIP		Internal Web Apps/Services	
443	Citrix Gateway SNIP		Storage zones controller IP	

Open ports from the internal network to the DMZ:

TCP port	Description	Source IP	Destination	Destination IP
443	Admin Client		Citrix Gateway NSIP	

Open ports from the internal network to the Internet:

TCP port	Description	Source IP	Destination	Destination IP
443	Exchange (EAS) Server IP		Endpoint Management Push Notification Listeners (1)	
443	Storage zones controller IP		Citrix Files Control Plane	<a href="#">CTX208318</a>

(1)[us-east-1.mailboxlistener.xm.citrix.com](#), [eu-west-1.mailboxlistener.xm.citrix.com](#), [ap-southeast-1.mailboxlistener.xm.citrix.com](#)

Open ports from the corporate Wi-Fi to the Internet:

TCP port	Description	Source IP	Destination	Destination IP
8443 / 443	Endpoint Management Client Device		Endpoint Management	
5223	Endpoint Management Client Device		Apple APNS Servers	17.0.0.0/8

TCP port	Description	Source IP	Destination	Destination IP
5228	Endpoint Management Client Device		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
5229	Endpoint Management Client Device		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
5230	Endpoint Management Client Device		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
443	Endpoint Management Client Device		Firebase Cloud Messaging	fcm.googleapis.com
443	Endpoint Management Client Device		Windows Push Notification Service	*.notify.windows.com
443 / 80	Endpoint Management Client Device		Apple iTunes App Store	ax.apps.apple.com, *.mzstatic.com, vpp.itunes.apple.com

TCP port	Description	Source IP	Destination	Destination IP
443 / 80	Endpoint Management Client Device		Google Play	play.google.com, android.clients.google.com, android.l.google.com, android.com, google-analytics.com
443 / 80	Endpoint Management Client Device		Microsoft App Store	login.live.com, *.notify.windows.com
443	Endpoint Management Client Device		Endpoint Management AutoDiscovery service for iOS and Android	discovery.cem.cloud.us
443	Endpoint Management Client Device		Endpoint Management AutoDiscovery service for Windows	enterpriseenrollment.mycompany.com, discovery.cem.cloud.us
443	Storage zones controller IP		Citrix Files Control Plane	CTX208318
443	Endpoint Management Client Device		Google Mobile Management, Google APIs, Google Play Store APIs	*.googleapis.com



TCP port	Description	Source IP	Destination	Destination IP
443	Endpoint Management Client Device		Connectivity checks for CloudDPC versions earlier than v470. Android connectivity checks starting with N MR1 requires <a href="https://www.google.com/generate_204">https://www.google.com/generate_204</a> to be reachable, or for the given Wi-Fi network to point to a reachable PAC file)	<a href="https://connectivitycheck.android.com">connectivitycheck.android.com</a> , <a href="https://www.google.com">www.google.com</a>

### Port requirement for AutoDiscovery service connectivity

This port configuration ensures that Android devices connecting from Secure Hub for Android can access the Endpoint Management AutoDiscovery service (ADS) from within the internal network. The ability to access the ADS is important when downloading any security updates made available through the ADS.

#### Note:

ADS connections might not support your proxy server. In this scenario, allow the ADS connection to bypass the proxy server.

If you want to enable certificate pinning, complete the following prerequisites:

- **Collect Endpoint Management server and Citrix Gateway certificates:** The certificates must be in PEM format and must be a public certificate and not the private key.
- **Contact Citrix Support and place a request to enable certificate pinning:** During this process, you are asked for your certificates.

Certificate pinning requires that devices connect to ADS before the device enrolls. This requirement

ensures that the latest security information is available to Secure Hub. For Secure Hub to enroll a device, the device must reach the ADS. Therefore, opening ADS access within the internal network is critical to enabling devices to enroll.

To allow access to the ADS for Secure Hub for Android/iOS, open port 443 for the following FQDN :

FQDN	Port	IP and port usage
<code>discovery.cem.cloud.us</code>	443	Secure Hub - ADS Communication via CloudFront

For information on supported IP addresses, see [Cloud-based storage centers from AWS](#).

### **Android Enterprise network requirements**

For information about the outbound connections to consider when setting up network environments for Android Enterprise, see the Google support article, [Android Enterprise Network Requirements](#).

## **Endpoint Management compatibility**

October 7, 2021

To use the new features, fixes, and policy updates, Citrix recommends that you install the most recent version of the following:

- Citrix recommends that you integrate the Mobile Application Management (MAM) SDK with enterprise iOS and Android apps to apply MDX capabilities to the apps.

The MDX toolkit is scheduled to reach EOL in March 2022. To continue managing your enterprise apps, you must incorporate the MAM SDK.

- Mobile productivity apps

This article summarizes the versions of the supported Endpoint Management components that you can integrate.

The latest versions of Secure Hub, MDX Toolkit, and mobile productivity apps are compatible with the latest version and the two prior versions of Endpoint Management.

## Mobile productivity apps

Users access the mobile productivity apps from the public app stores. The latest version of the mobile productivity apps requires the latest version of Secure Hub. The two previous versions of the apps are compatible with the latest Secure Hub.

For more information about the mobile productivity apps two-week phased release cadence, see [Release timeline](#). For support details, see [Support for mobile productivity apps](#).

## MAM SDK

The MAM SDK provides MDX functionality that isn't covered by the iOS and Android platforms. You make those apps available in either an internal store or public app stores. See [MDX App SDK](#).

## MDX Toolkit

The MDX toolkit is scheduled to reach EOL in March 2022. To continue managing your enterprise applications, you must incorporate the MAM SDK.

Citrix supports the latest three releases (n.n.n) of the MDX Toolkit. See [What's new in the MDX Toolkit](#).

## Browser support

The Endpoint Management console requires one of the following supported web browsers:

- Latest version of Google Chrome
- Latest version of Mozilla Firefox
- Latest version of Microsoft Edge
- Latest version of Apple Safari

## Supported device operating systems

September 9, 2021

This article covers supported devices for enterprise mobility management with Endpoint Management. Because of platform restrictions and security features, Endpoint Management doesn't support all functionality on all platforms.

For the latest versions of the mobile productivity apps, see [Support for mobile productivity apps](#).

### Note:

Citrix supports, at a minimum, the current and prior version of each major operating system

platform. Not all features of the newer version of Endpoint Management work on older platform releases.

For deprecation announcements, see [Deprecation](#).

### Operating system support list

Citrix Endpoint Management supports the following operating systems:

#### Note:

Support ended for the Android 7.x and iOS 12.x versions of Secure Hub, Secure Mail, Secure Web, and Citrix Workspace app in April 2021.

- **Android:** 8.x, 9.x, 10.x, 11.x, 12.x

For Android 10+, see [Android considerations](#).

- **Chrome OS:** Chromebook

- **iOS:** 13.x, 14.x, 15

Endpoint Management and Citrix mobile apps are compatible with iOS 14.x and iOS 15, but don't currently support all new features available for iOS 14.x and iOS 15.

- **iPadOS:** 13.x, 14.x

Endpoint Management and Citrix mobile apps are compatible with iPadOS 14.x, but don't currently support all new iPadOS 14.x features.

- **macOS:** 10.13x, 10.14x, 10.15x, 11.x, 12

Endpoint Management and Citrix mobile apps are compatible with macOS 11 and macOS 12, but don't currently support all new features available for macOS 11 and macOS 12.

- **tvOS:** 10.2, 11.x, 12.x, 13.x. Requires 4th generation Apple TV devices enrolled using Apple Deployment Program.

- **Windows 10 and Windows 11 Desktops and Tablets:** (MDM only)

- Windows 10 Professional and Windows 11 Professional
- Windows 10 Enterprise and Windows 11 Enterprise
- Windows 10 Education and Windows 11 Education
- Windows IoT Enterprise

Refer to Microsoft documentation for the level of support for a specific operating system.

- **Windows Phone:** (MDM only). Windows Phone 8.1, Windows Phone 10, Windows 10 RS4, and Windows 10 RS5.

- **Raspberry Pi platform:** Citrix Ready workspace hub, built on the Raspberry Pi 3 platform. For more information about Workspace hub requirements, see [Citrix Ready workspace hub](#).

- **Samsung SAFE and Knox:** On compatible Samsung devices, Endpoint Management supports and extends both Samsung for Enterprise (SAFE) and Samsung Knox policies. Endpoint Management requires that you enable the SAFE APIs before you deploy SAFE policies and restrictions. To do that, deploy the built-in Samsung Enterprise License Management (ELM) key to a device. See [Samsung MDM license key device policy](#).

## Android considerations

Before upgrading to Android 10 or later: For information about how the deprecation of Google Device Administration APIs impacts devices running Android 10+, see [Migrate from device administration to Android Enterprise](#). Also see this [Citrix blog](#).

- Citrix recommends that you avoid enrolling Android 10 devices in legacy device administration mode. Google is deprecating Device Administration APIs, which impact devices running Android 10+. After the APIs get deprecated, enrollment of Android 10+ devices in legacy device administration mode will fail. Citrix doesn't support enrolling Android 11 devices in device administration mode.
- Citrix recommends using Android Enterprise for Android 10+ devices. For more information, see [Migrate from device administration to Android Enterprise](#).
- The Google API change doesn't impact devices enrolled in MAM-only mode.
- Also see this [Citrix blog](#).

Before upgrading:

- Ensure that your server infrastructure is compliant with security certificates that have a matching host name in the subjectAltName (SAN) extension.
- To verify a host name, the server must present a certificate with a matching SAN. Citrix trusts certificates only if they contain a SAN that matches the host name.

## Language support

September 16, 2020

Citrix mobile productivity apps and the Endpoint Management console are adapted for use in languages other than English. The support includes non-English characters and keyboard input even when the app is not localized in the preferred language of a user. For more information about globalization support for all Citrix products, see <https://support.citrix.com/article/CTX119253>.

This article lists the supported languages in the latest release of Endpoint Management.

## Endpoint Management console and the Self-Help Portal

- French
- German
- Spanish
- Japanese
- Korean
- Portuguese
- Simplified Chinese

## Citrix mobile productivity apps

An X indicates that the app is available in that particular language.

### iOS and Android

Language	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
Japanese	X	X	X	X	X	X
Simplified Chinese	X	X	X	X	X	X
Traditional Chinese	X	X	X	X	X	X
French	X	X	X	X	X	X
German	X	X	X	X	X	X
Spanish	X	X	X	X	X	X
Korean	X	X	X	X	X	X
Portuguese	X	X	X	X	X	X
Dutch	X	X	X	X	X	X
Italian	X	X	X	X	X	X
Danish	X	X	X	X	X	X
Swedish	X	X	X	X	X	X
Hebrew	X	X	X	X	X	iOS only
Arabic	X	X	X	X	X	X
Russian	X	X	X	X	X	X

Language	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
Turkish	X	X	Android only	-	-	-
Polish	X	X	X	-	-	-

### Right-to-left language support

The following table summarizes support for text in Middle Eastern languages for each app. An X indicates that the feature is available for that platform. Right-to-left language support is not available for Windows devices.

App	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
QuickEdit	X	X

### FIPS 140-2 compliance

September 24, 2021

The Federal Information Processing Standard (FIPS) is issued by the US National Institute of Standards and Technologies (NIST). FIPS specifies the security requirements for cryptographic modules used in security systems. FIPS 140-2 is the second version of this standard. For more information about NIST-validated FIPS 140 modules, see the [NIST Computer Security Resource Center](#).

All data-at-rest and data-in-transit cryptographic operations on iOS use FIPS-validated cryptographic modules. On Android, all data-at-rest cryptographic operations use FIPS-validated cryptographic modules provided by Citrix or the platform's crypto modules provided by the device manufacturer. Contact your Citrix representative for more information on device manufacturer's modules.

All data-at-rest and data-in-transit cryptographic operations for Mobile Device Management (MDM) on supported Windows devices use FIPS-validated cryptographic modules.

All data-at-rest and data-in-transit cryptographic operations for Citrix Endpoint Management MDM use FIPS-validated cryptographic modules. All data-at-rest and data-in-transit for MDM flows use FIPS-compliant cryptographic modules end-to-end. That security includes the cryptographic operations

described above for mobile devices, plus the cryptographic operations between mobile devices and Citrix Gateway.

The MDX Vault encrypts MDX-wrapped apps and associated data-at-rest on both iOS and Android devices using FIPS-validated cryptographic modules.

## About Endpoint Management

October 7, 2021

Citrix Endpoint Management is a unified endpoint management (UEM) solution that brings every app and endpoint into one unified view to increase security and improve productivity. For an overview of UEM, see the Citrix Tech Zone technical brief, [Citrix Endpoint Management](#).

Endpoint Management provides Mobile Device Management (MDM) and Mobile App Management (MAM).

MDM features of Endpoint Management let you:

- Deploy device policies and apps.
- Retrieve asset inventories.
- Carry out actions on devices, such as a device wipe.

MAM features of Endpoint Management let you:

- Secure apps and data on BYO mobile devices.
- Deliver enterprise mobile apps.
- Lock apps and wipe their data.

With a combination of MDM and MAM features, you can:

- Manage a corporate-issued device by using MDM
- Deploy device policies and apps
- Retrieve an asset inventory
- Wipe devices
- Deliver enterprise mobile apps
- Lock apps and wipe the data on devices

The following table summarizes the Endpoint Management features supported for MDM, MAM, or MDM+MAM.

Feature (by platform)	MDM (1)	MAM (2)	MDM+MAM
<b>Android Enterprise:</b>			



Feature (by platform)	MDM (1)	MAM (2)	MDM+MAM
Device enrollment support	Yes	Yes	Yes
Domain authentication support	Yes	No	Yes
Domain plus security token authentication support	No	No	Yes
Client certificate authentication support	No	Yes	Yes
Client certificate plus domain authentication support	No	No	Yes
Client certificate plus security token support	No	No	Yes
Azure AD identity provider support	Yes	No	Yes
Okta identity provider support	Yes	No	Yes
Single sign on to native SaaS apps	Yes	No	Yes
Citrix Content Delivery Network support for enterprise apps	Yes	Yes	Yes
Citrix Content Delivery Network support for MDX apps	Yes	Yes	Yes

Feature (by platform)	MDM (1)	MAM (2)	MDM+MAM
Shared device support by provisioning dedicated Android Enterprise (COSU) devices	Yes	No	Yes
<b>Android (legacy):</b>			
Device enrollment support	Yes	Yes	Yes
Domain or domain plus security token authentication support	No	No	Yes
Client certificate authentication support	No	Yes	Yes
Client certificate plus domain authentication support	No	No	Yes
Client certificate plus security token support	No	No	Yes
Azure AD and Citrix identity provider support	Yes	No	Yes
Okta identity provider support	Yes	No	Yes
Single sign on to native SaaS apps	Yes	No	Yes
Citrix Content Delivery Network support for enterprise apps	Yes	Yes	Yes

Feature (by platform)	MDM (1)	MAM (2)	MDM+MAM
Citrix Content Delivery Network support for MDX apps	Yes	Yes	Yes
<b>Chrome:</b>			
Device enrollment support	Yes	No	Yes
User name and password authentication support	Yes	No	Yes
<b>iOS:</b>			
Device enrollment support	Yes	Yes	Yes
Domain or domain plus security token authentication support	No	No	Yes
Client certificate authentication support	No	Yes	Yes
Client certificate plus domain authentication support	No	No	Yes
Azure AD and Citrix identity provider support	Yes	No	Yes
Okta identity provider support	Yes	No	Yes
Single sign on to native SaaS apps	Yes	No	Yes
Citrix Content Delivery Network support for enterprise apps	Yes	Yes	Yes

Feature (by platform)	MDM (1)	MAM (2)	MDM+MAM
Citrix Content Delivery Network support for MDX apps	Yes	Yes	Yes
Apple Education integration	Yes	No	Yes
<b>macOS:</b>			
Device enrollment support	Yes	No	No
Domain or domain plus one-time password support	Yes	No	No
Invitation URL plus one-time password support	Yes	No	No
<b>Windows:</b>			
Device enrollment support	Yes	No	No
Automatic enrollment of Windows 10 and Windows 11 devices through Citrix Workspace app	Yes	No	No
Domain or domain plus security token authentication support	Yes	No	No
Client certificate authentication support	Yes	No	No
Client certificate plus domain authentication support	Yes	No	No

Feature (by platform)	MDM (1)	MAM (2)	MDM+MAM
Federated authentication through Azure AD or Citrix identity provider	Yes	No	No
Citrix Content Delivery Network support for enterprise apps	Yes	No	No
Workspace Environment Management integration (3)	Yes	No	No

**Notes:**

- (1) Deployment ordering applies only to devices in a delivery group that has an enrollment profile configured for MDM.
- (2) MAM enrollment requires Citrix Gateway.
- (3) Workspace Environment Management (WEM) integration provides access to MDM features on a wide spectrum of Windows operating systems.

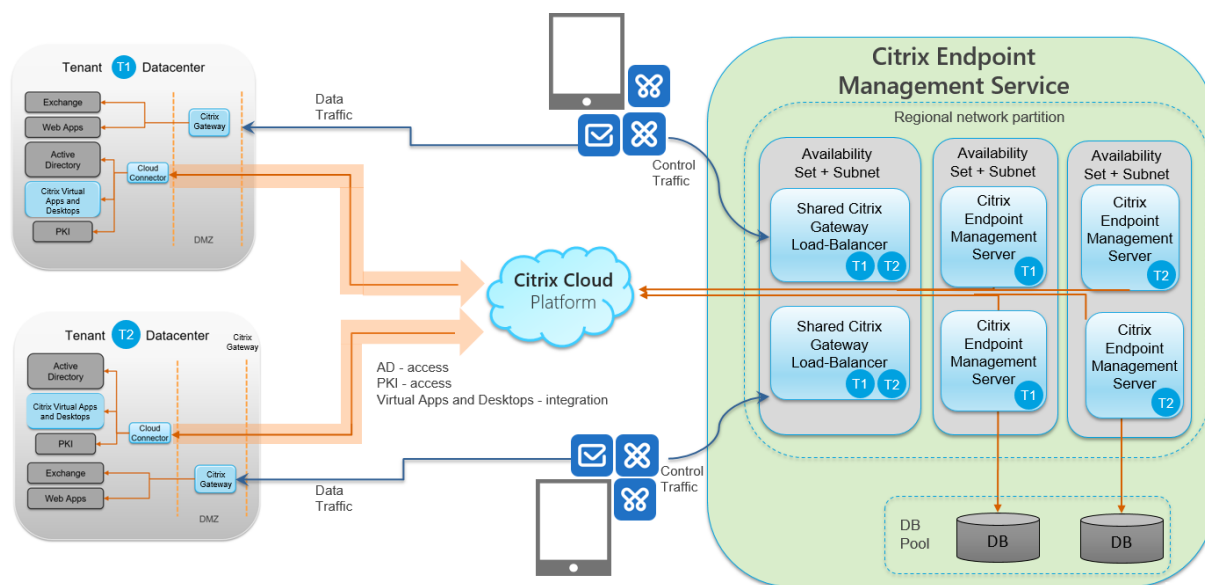
For more information, see [Management modes](#).

**Architecture**

The device and app management requirements of your organization determine the Endpoint Management components in your Endpoint Management architecture. The components of Endpoint Management are modular and build on each other. For example, your deployment includes Citrix Gateway:

- Citrix Gateway gives users remote access to mobile apps and tracks user device types.
- Endpoint Management is where you manage those apps and devices.

The following diagram shows a general architectural overview of an Endpoint Management cloud deployment and its integration with your data center.



The following subsections contain reference architecture diagrams for:

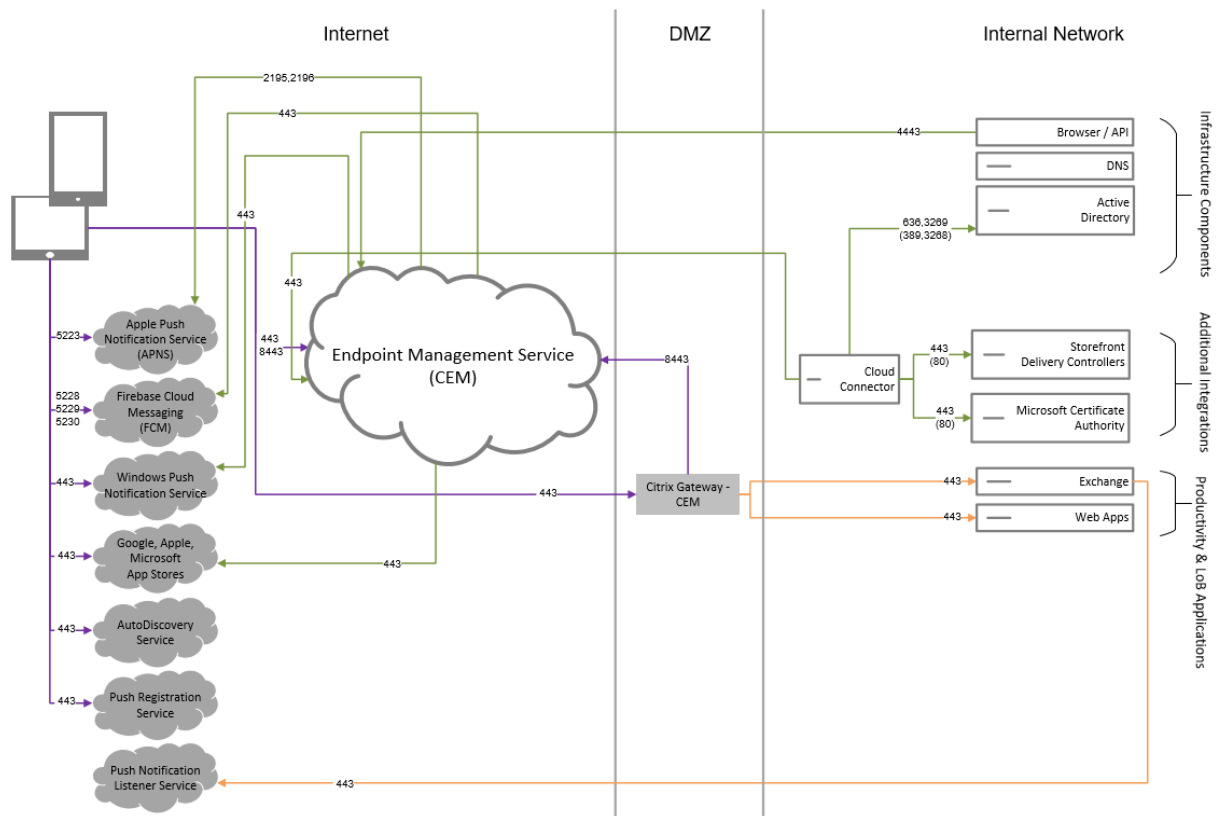
- Endpoint Management
- Optional components such as an external Certificate Authority, Endpoint Management connector for Exchange ActiveSync, and Endpoint Management MDM+MAM and Intune MAM traffic flow.

For more information about Citrix ADC and Citrix Gateway requirements, see the Citrix product documentation at <https://docs.citrix.com/>.

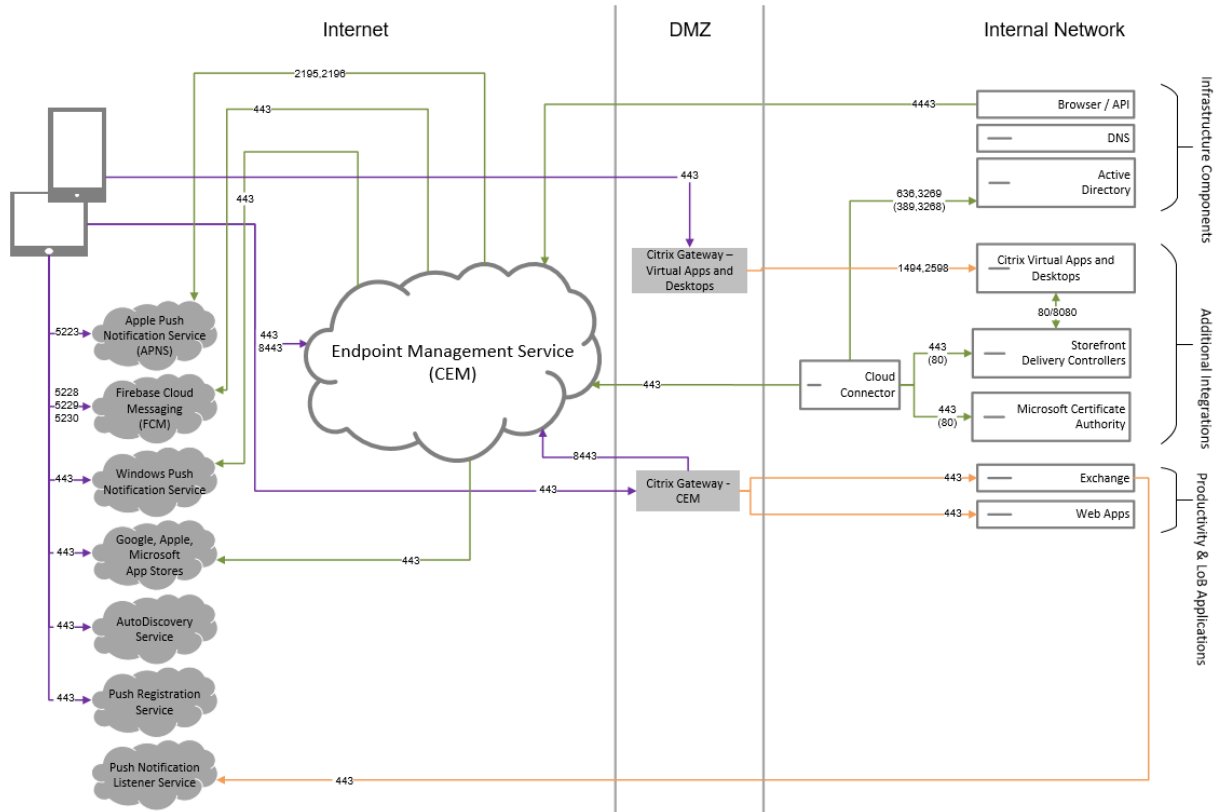
## Core reference architecture

For details about port requirements, see [System requirements](#).

# Citrix Endpoint Management

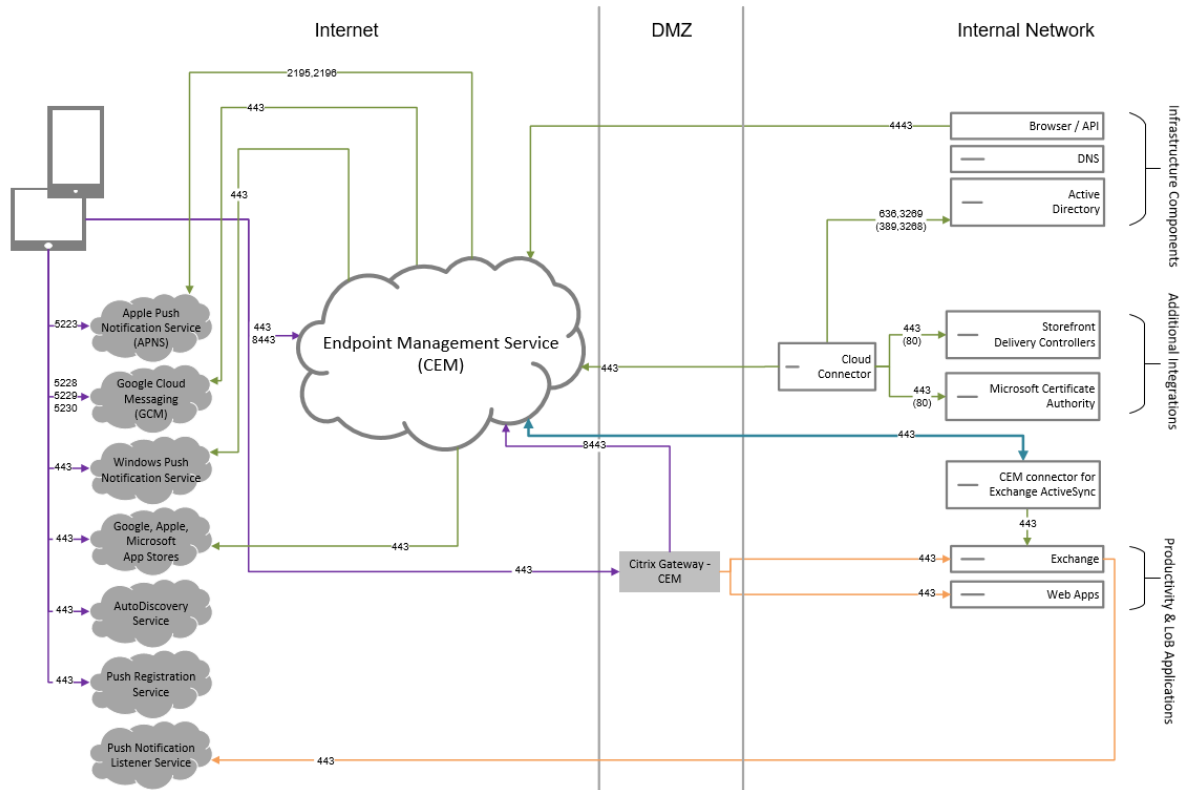


**Reference architecture with Citrix Virtual Apps and Desktops**

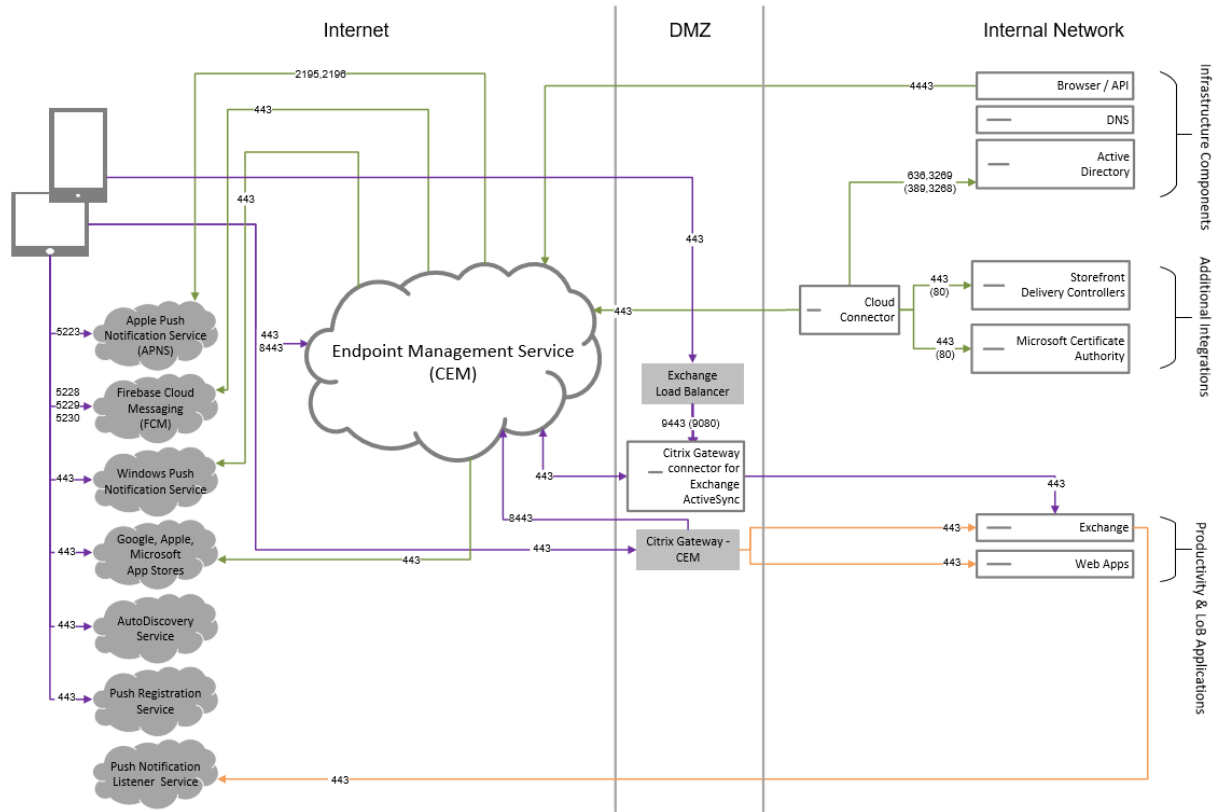




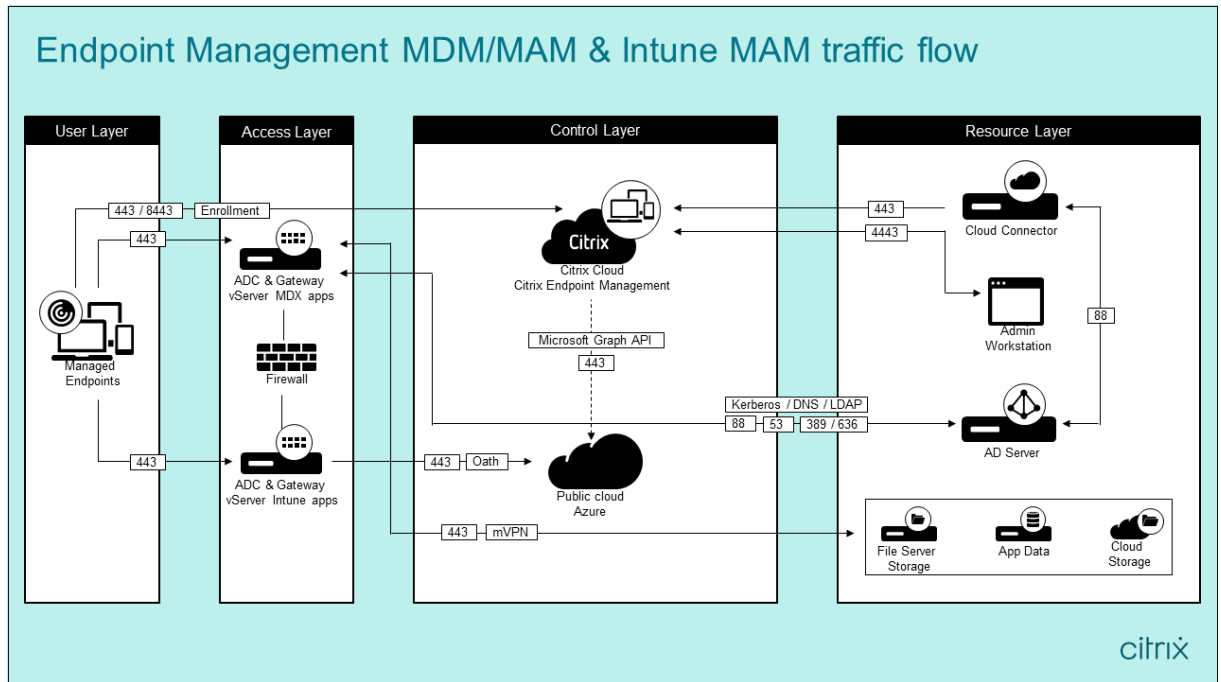
**Reference architecture with Endpoint Management connector for Exchange ActiveSync**



**Reference architecture with Citrix Gateway connector for Exchange ActiveSync**



**Reference architecture with Endpoint Management MDM+MAM and Intune MAM**



### Resource locations

Place resource locations where they best meet your business needs. For example, in a public cloud, in a branch office, private cloud, or a data center. Factors that determine the choice of location include:

- Proximity to subscribers
- Proximity to data
- Scale requirements
- Security attributes

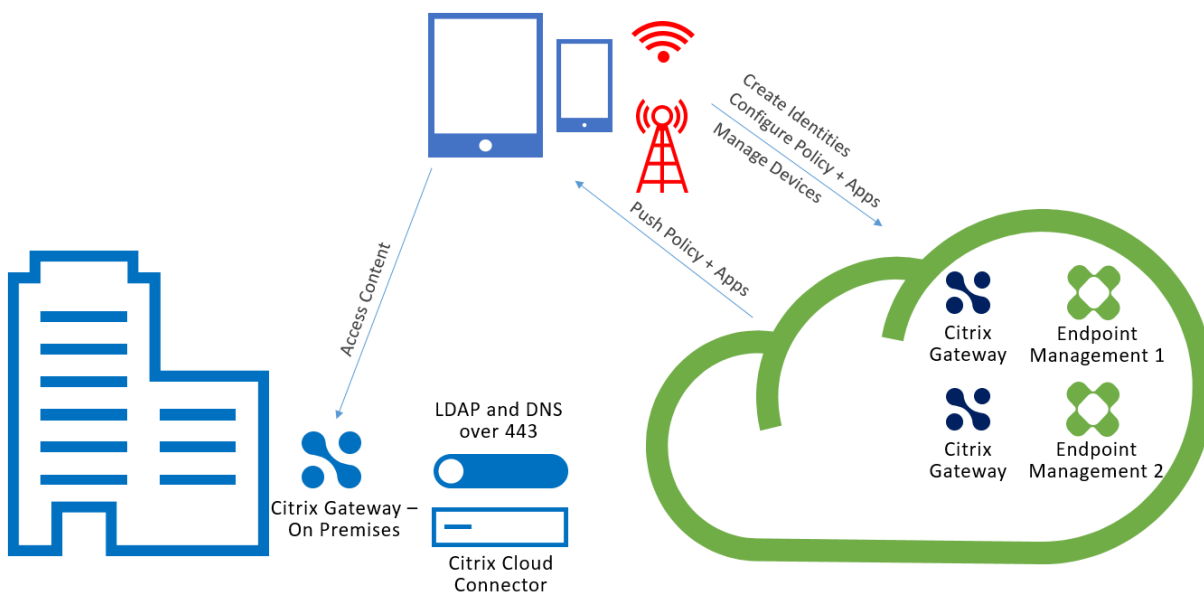
You can build any number of resource locations. For example, you might:

- Build a resource location in your data center for the head office, based on subscribers and applications that require proximity to the data.
- Add a separate resource location for your global users in a public cloud. Alternatively, build separate resource locations in branch offices to provide the applications best served close to the branch workers.
- Add a further resource location on a separate network that provides restricted applications. This setup provides restricted visibility to other resources and subscribers without the need to adjust the other resource locations.

### Cloud Connector

Cloud Connector authenticates and encrypts all communication between Citrix Cloud and your resource locations. Cloud Connector is required to access the following services: LDAP, IdPs, PKI Server, internal DNS queries, Citrix Virtual Apps, Citrix Gateway, Citrix Workspace, and Microsoft Endpoint Manager.

The following diagram shows the traffic flow for Cloud Connector.



Cloud Connector establishes connections to Citrix Cloud. Cloud Connector doesn't accept incoming connections.

Cloud Connector is under load only during device enrollment. For more information, see [Scale and size considerations for Cloud Connectors](#).

A solution that includes Mobile App Management (MAM) requires a micro VPN that is provided by an on-premises Citrix Gateway. In this scenario:

- The following components reside in your data center:
  - Cloud Connector
  - Citrix Gateway
  - Your servers for Exchange, web apps, Active Directory, and PKI
- Mobile devices communicate with Endpoint Management and your on-premises Citrix Gateway.

### Endpoint Management components

**Endpoint Management console.** You use the Endpoint Management administrator console to configure Endpoint Management. For details about using the Endpoint Management console, see the articles under [Endpoint Management](#). Citrix notifies you when the What's new articles for Endpoint Management are updated for a new release.

Note these differences between the Endpoint Management service and the on-premises releases:

- The Remote Support client is not available for Endpoint Management.
- Citrix does not support syslog integration in Endpoint Management with an on-premises syslog server. Instead, you can download the logs from the **Troubleshooting and Support** page in the Endpoint Management console. When doing so, you must click **Download All**.

**MAM SDK.** The MDX toolkit is scheduled to reach EOL in March 2022. To continue managing your enterprise applications, you must incorporate the MAM SDK.

- The Mobile Application Management (MAM) SDK provides MDX functionality that isn't covered by the iOS and Android platforms. You can MDX-enable and secure iOS or Android apps. You make those apps available in either an internal store or public app stores. See [MDX App SDK](#).

**Mobile productivity apps.** Citrix-developed mobile productivity apps provide a suite of productivity and communication tools within the Endpoint Management environment. Your company policies secure those apps. For more information, see [Mobile productivity apps](#).

**Endpoint Management connector for Exchange ActiveSync.** Endpoint Management connector for Exchange ActiveSync provides secure email access to users who use native mobile email apps. The connector for Exchange ActiveSync provides ActiveSync filtering at the Exchange service level. As a result, filtering only occurs once the mail reaches the Exchange service, rather than when it enters the Endpoint Management environment. The connector doesn't require the use of Citrix Gateway.

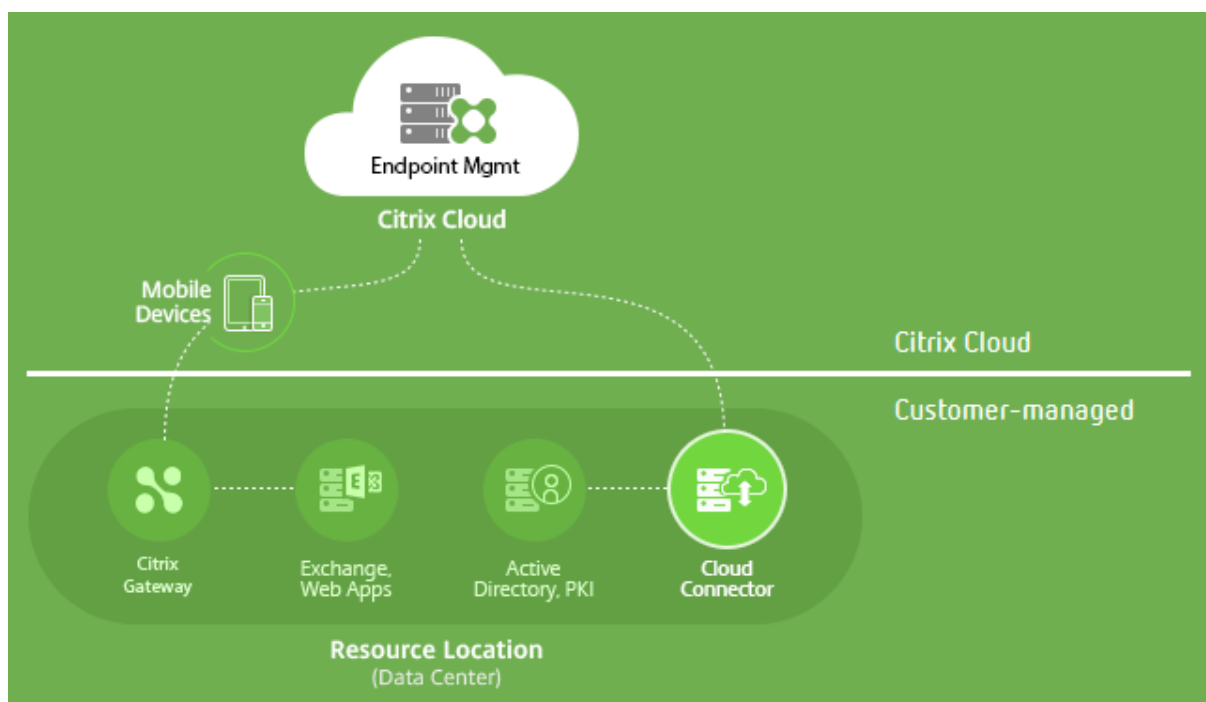
You can deploy the connector without changing routing for the existing ActiveSync traffic. For more information, see [Endpoint Management connector for Exchange ActiveSync](#).

**Citrix Gateway connector for Exchange ActiveSync.** Citrix Gateway connector for Exchange ActiveSync provides secure email access to users who use native mobile email apps. The connector for Exchange ActiveSync provides ActiveSync filtering at the perimeter. The filtering uses Citrix Gateway as a proxy for ActiveSync traffic. As a result, the filtering component sits in the path of mail traffic flow, intercepting mail as it enters or leaves the environment. The connector for Exchange ActiveSync acts as an intermediary between Citrix Gateway and Endpoint Management. For more information, see [Citrix Gateway connector for Exchange ActiveSync](#).

### Endpoint Management technical security overview

Citrix Cloud manages the control plane for Endpoint Management environments. The control plane includes the Endpoint Management server, Citrix ADC load balancer, and a single-tenant database. The cloud service integrates with a customer data center using Citrix Cloud Connector. Endpoint Management customers who use Cloud Connector typically manage Citrix Gateway in their data centers.

The following figure illustrates the service and its security boundaries.



The information in this section:

- Provides an introduction to the security functionality of Citrix Cloud.
- Defines the division of responsibility between Citrix and customers for securing the Citrix Cloud deployment.

- Isn't configuration or administration guidance for Citrix Cloud or any of its components or services.

For information about the technology used by Endpoint Management to deliver comprehensive, end-to-end security, see the Citrix whitepaper, [Citrix Endpoint Management Security Overview](#).

### **Data flow**

The control plane has limited read access to user and group objects. Those objects reside in your directory, DNS, and similar services. The control plane accesses those services over Citrix Cloud Connector through secure HTTPS connections.

Company data, such as email, intranet, and web-app traffic, flows directly between a device and the application servers over Citrix Gateway. Citrix Gateway is deployed in the customer data center.

### **Data isolation**

The control plane stores metadata needed for managing user devices and their mobile applications. The service itself consists of a mix of multi- and single-tenant components. However, per the service architecture, customer metadata is always stored separately for each tenant and secured by using unique credentials.

### **Credential handling**

The service handles the following types of credentials:

- **User credentials:** User credentials are transmitted from the device to the control plane over an HTTPS connection. The control plane validates these credentials with a directory in the customer directory over a secure connection.
- **Administrator credentials:** Administrators authenticate against Citrix Cloud, which uses the sign-on system from Citrix Online. This process generates a one-time signed JSON Web Token (JWT), which gives the administrator access to the service.
- **Active Directory credentials:** The control plane requires bind-credentials to read user meta-data from Active Directory. These credentials are encrypted using AES-256 encryption and saved in a per-tenant database.

### **Deployment considerations**

Citrix recommends that you consult the published best practices documentation for deploying Citrix Gateway within your environments.

### More resources

See the following resources for more security information:

- Citrix Security Site: <https://www.citrix.com/security>
- Citrix Cloud Documentation: [Secure Deployment Guide for the Citrix Cloud Platform](#)
- [Secure Deployment Guide for Citrix ADC](#)

### Integration with Mobile Threat Defense software

Mobile Threat Defense (MTD) software detects, analyzes, and helps prevent advanced cyberattacks against enterprise mobile devices. The combination of MTD and Unified Endpoint Management (UEM) increases security and visibility for your organization.

MTD software provides threat data that Endpoint Management uses to:

- Protect against malware, phishing, network attacks, and man-in-the-middle attacks
- Determine device compliance status
- Determine risk levels
- Take policy-based actions to protect your apps, data, devices, and mobile network

Citrix Endpoint Management integrates with the following MTD vendors:

- [Check Point](#)
- [Lookout](#)
- [Wandera](#)
- [Zimperium](#)

For more information or to request a demo, contact our MTD partners or your Citrix Sales Representative.

## Citrix Endpoint Management integration with Microsoft Endpoint Manager

October 22, 2021

Endpoint Management integration with Microsoft Endpoint Manager (MEM) adds the value of Endpoint Management micro VPN to Microsoft Intune aware apps, such as Microsoft Edge browser.

**To activate the integration**, contact the Citrix Cloud Operations team.

This release supports the following use cases:

- Intune MAM with Endpoint Management MDM+MAM.

This article focuses on the Intune MAM + Endpoint Management MDM+MAM use case. After you add Citrix as your MDM provider, configure Intune managed apps for delivery to devices.

### Important:

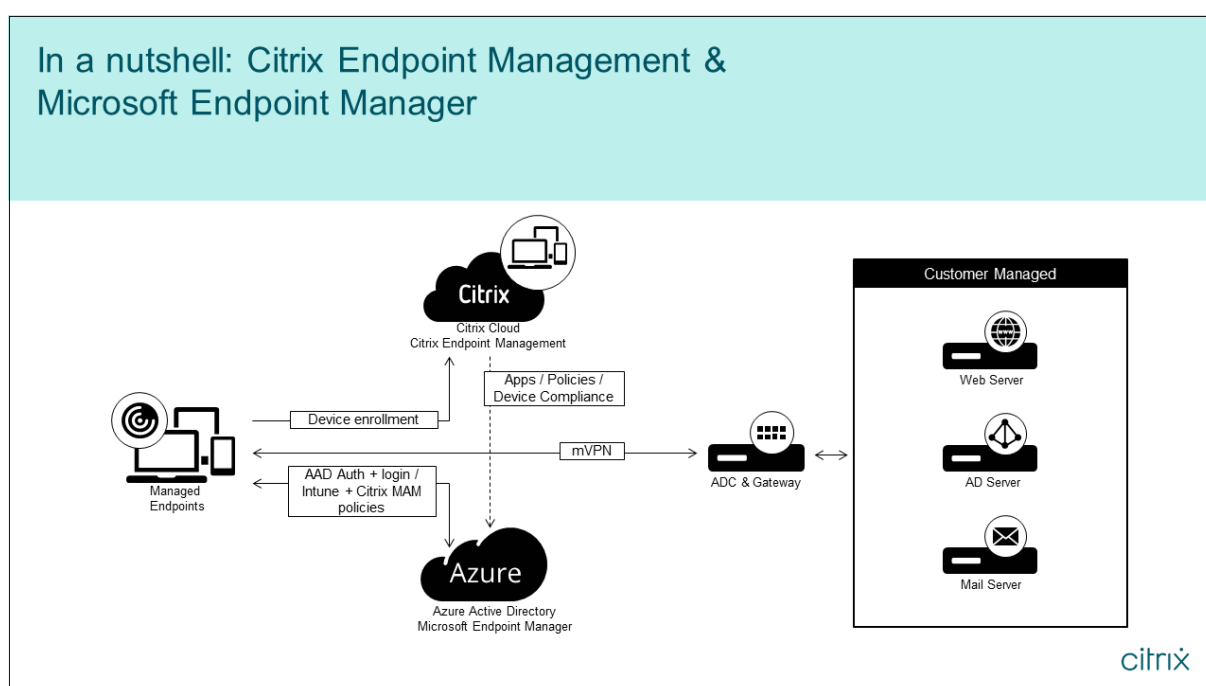
For this use case, Secure Mail doesn't support integration with Intune. Secure Mail only works for devices enrolled in MDX mode.

- Intune MAM and Endpoint Management MDM.
- Intune MAM.
- Intune MAM and Intune MDM. Secure Mail for iOS supports single sign-on for this use case.

For an easy-to-follow, graphical guide to setting up Endpoint Management integration with MEM, see [Getting Started Guide](#).

For information on integrating with Azure AD Conditional Access, see [Integrate with Azure AD Conditional Access](#).

The following diagram provides an overview of Citrix Endpoint Management integration with Microsoft Endpoint Manager.



## System requirements

### MDX-enable

- [MAM SDK](#)

or



- [MDX Toolkit](#)

## Microsoft

- Azure Active Directory (AD) access (with Tenant Admin privileges)
- Intune-enabled tenant

## Firewall rule

- Enable a firewall rule to allow DNS and SSL traffic from a Citrix Gateway subnet IP to \*.manage.microsoft.com, <https://login.microsoftonline.com>, and <https://graph.windows.net> (port 53 and 443)

## Prerequisites

- **Microsoft Edge browser:** The Mobile Apps SDK is integrated within the Microsoft Edge browser app for iOS and Android. For more information about Microsoft Edge, see the [Microsoft Edge documentation](#).
- **Citrix Cloud account:** To sign up for a Citrix account and request a Citrix Endpoint Management trial, contact your Citrix Sales Representative. When you're ready to proceed, go to <https://onboarding.cloud.com>. For more information on requesting a Citrix Cloud account, see [Sign up for Citrix Cloud](#).

### Note:

The email you supply must be an address that is not associated with Azure AD. You can use any free email service.

- **APNs certificates for iOS:** Ensure that you configure APNs certificates for iOS. To learn more about setting up these certificates, see this Citrix blog post: [Creating and Importing APNs Certificates](#).
- **Azure AD sync:** Set up synchronization between Azure AD and on-premises Active Directory. Do not install the AD sync tool on the domain controller machine. For more information on setting up this sync, see the Microsoft documentation on [Azure Active Directory](#).

## Configuring Citrix Gateway

If you are setting up a new Endpoint Management deployment, install one of these Citrix Gateway appliances:

- NetScaler Gateway VPX 3000 series or greater
- NetScaler Gateway MPX or dedicated SDX instance

To use Citrix Gateway with Endpoint Management integration with MEM:

- Configure Citrix Gateway with a management interface and a subnet IP.
- Use TLS 1.2 for all client to server communication. For information about configuring TLS 1.2 for Citrix Gateway, see [CTX247095](#).

If you are using Endpoint Management integration with MEM with an Endpoint Management MDM+MAM deployment, configure two Citrix Gateways. MDX app traffic is routed through one Citrix Gateway. Intune app traffic is routed through the other Citrix Gateway. Configure:

- Two public IPs.
- Optionally, one network address translated IP.
- Two DNS names. Example: <https://mam.company.com>.
- Two public SSL certificates. Configure certificates that match the reserved public DNS name or use wildcard certificates.
- A MAM load balancer with an internal non-routable RFC 1918 IP address.
- An LDAP Active Directory service account.

### Consenting to delegated permission prompts

For managed apps that require users to authenticate, the apps request application permissions exposed by Microsoft Graph. By consenting to these permission prompts, the app can access the required resources and APIs. Some apps require consent by the global administrator for Microsoft Azure AD. For these delegated permissions, the global administrator must grant Citrix Cloud permission to request tokens. The tokens then enable the following permissions. For more details, see the [Microsoft Graph permissions reference](#).

- **Sign in and read user profile:** This permission allows users to sign in and connect to Azure AD. Citrix can't view user credentials.
- **Read all users' basic profiles:** The app reads profile properties on behalf of users in the organization. The properties include the display name, first and last name, and email address and photo of users in the organization.
- **Read all groups:** This permission enables Azure AD groups to be enumerated for app and policy assignment.
- **Access directory as the signed-in user:** This permission verifies the Intune subscription and enables Citrix Gateway and VPN configurations.
- **Read and write Microsoft Intune apps:** The app can read and write the following:
  - Microsoft-managed properties
  - Group assignments and the status of apps
  - App configurations

- App protection policies

Also, during the Citrix Gateway configuration, the Azure AD global administrator must:

In addition, during the Citrix Gateway configuration, the Azure AD global administrator must approve the Active Directory chosen for micro VPN. The global administrator must also generate a client secret that Citrix Gateway uses to communicate with Azure AD and Intune.

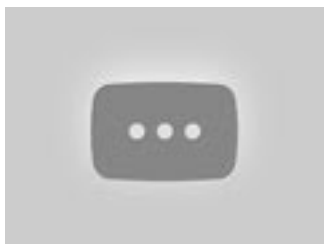
The global administrator must not have the role of Citrix administrator. Instead, the Citrix administrator assigns Azure AD accounts to users with appropriate Intune application admin privileges. The Intune administrator then serves the role of a Citrix Cloud admin to manage Intune from within Citrix Cloud.

**Note:**

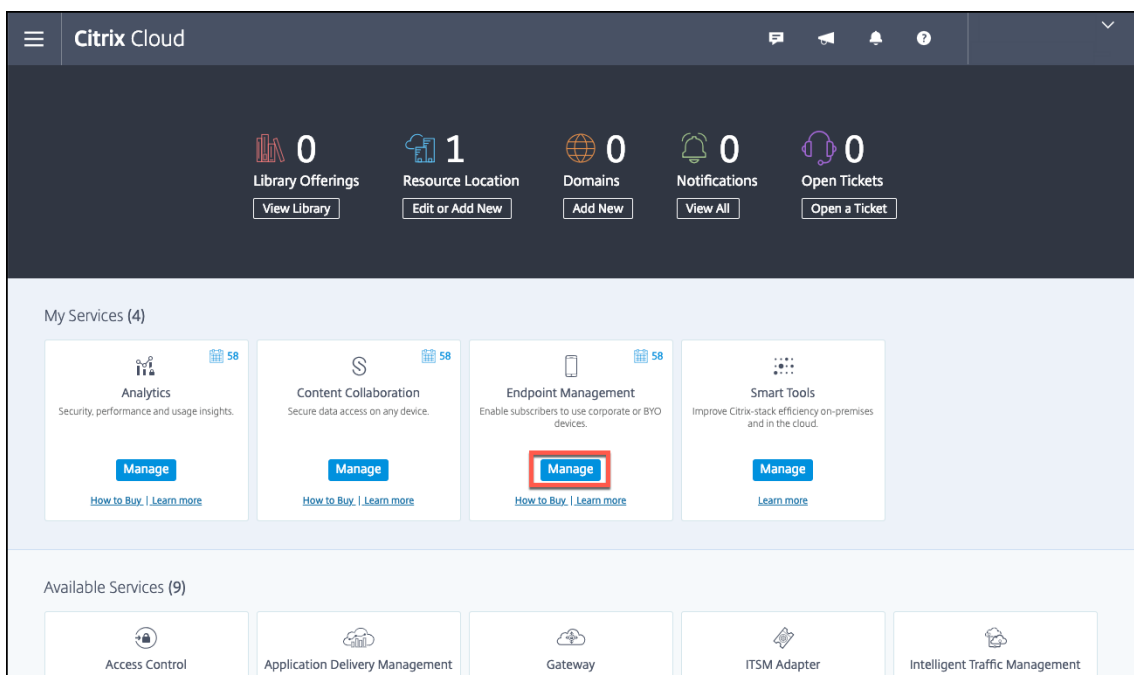
Citrix only uses the Intune Global Administrator password during setup and redirects the authentication to Microsoft. Citrix can't access the password.

### To configure Endpoint Management integration with MEM

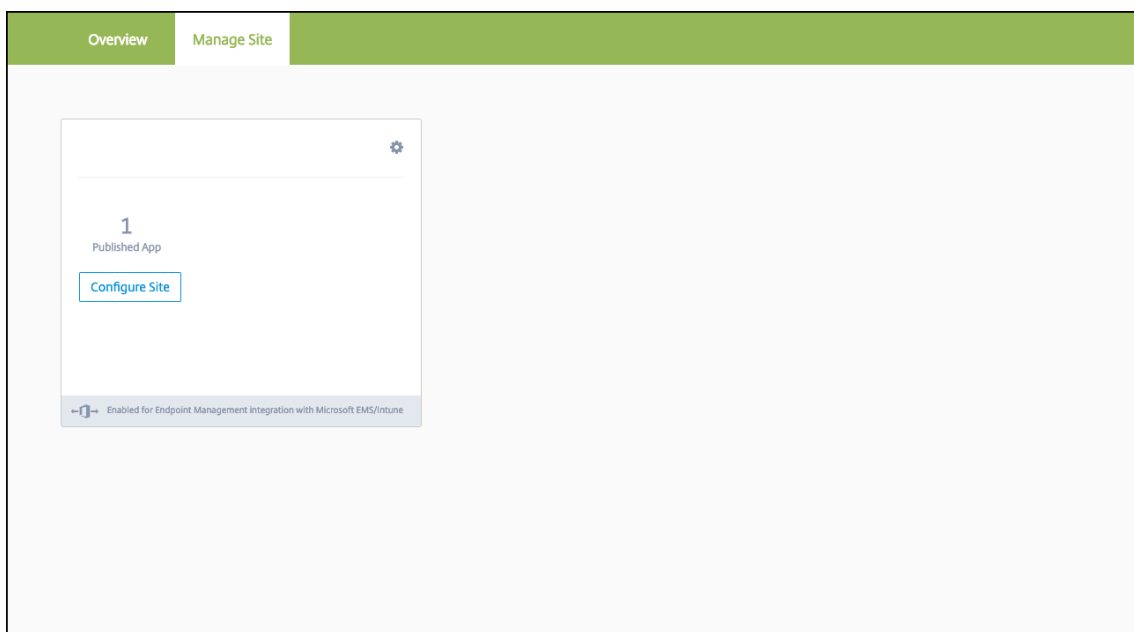
For a video summary of the integration, watch:



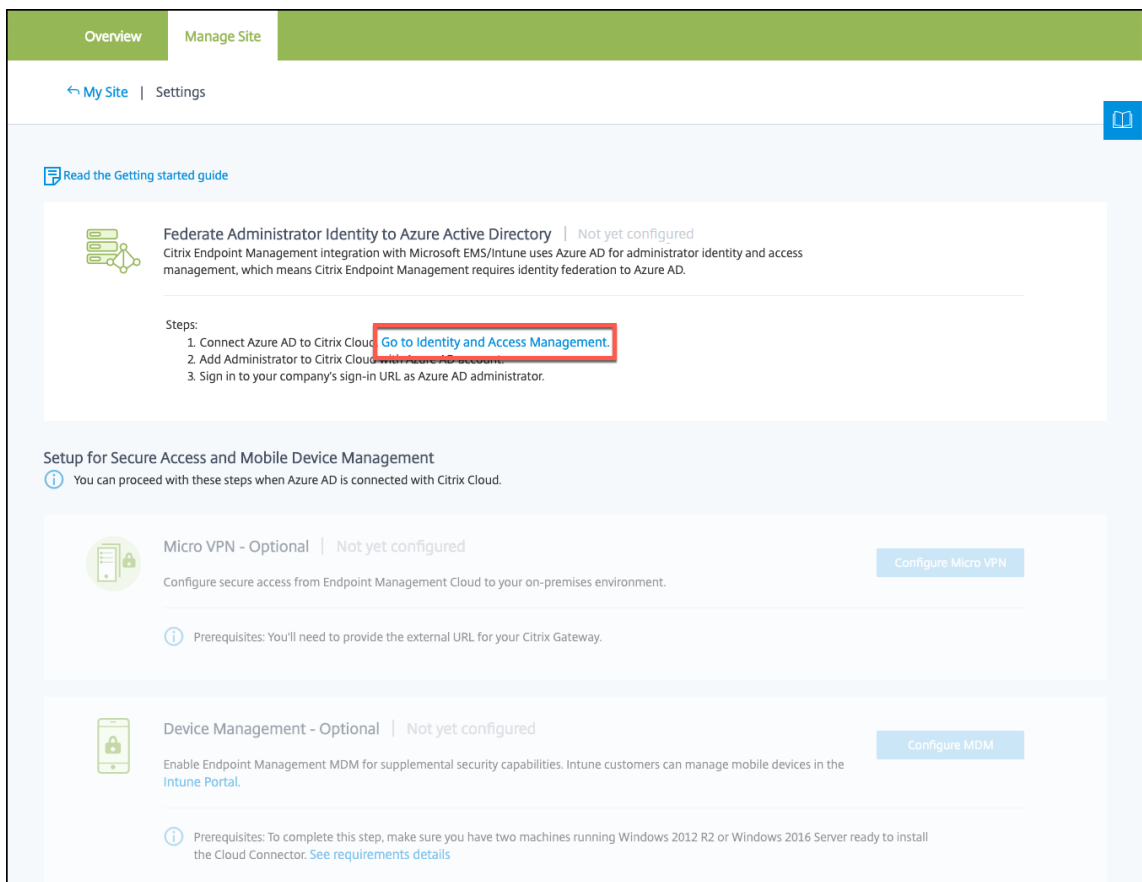
1. Log on to the Citrix Cloud site and request a trial for Endpoint Management.
2. A sales engineer schedules an onboarding meeting with you. Let them know that you want Endpoint Management integration with MEM. When your request is approved, click **Manage**.



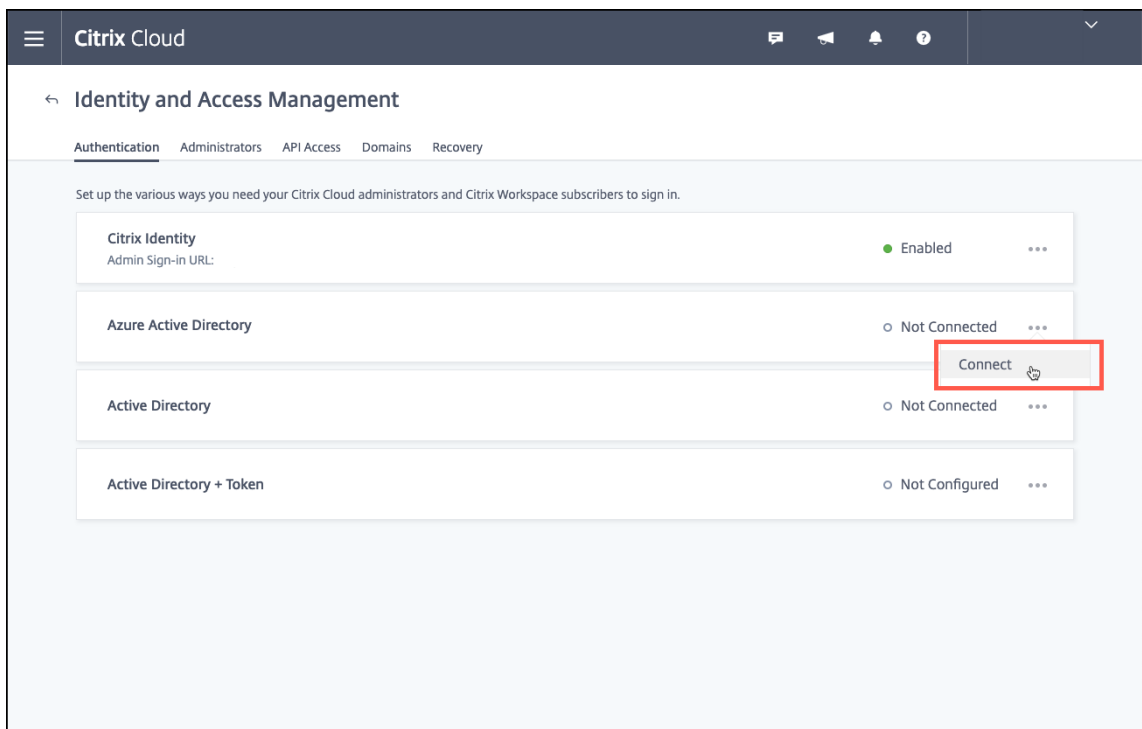
3. From here you can click the cog in the upper right of your site or you can click **Configure Site**.



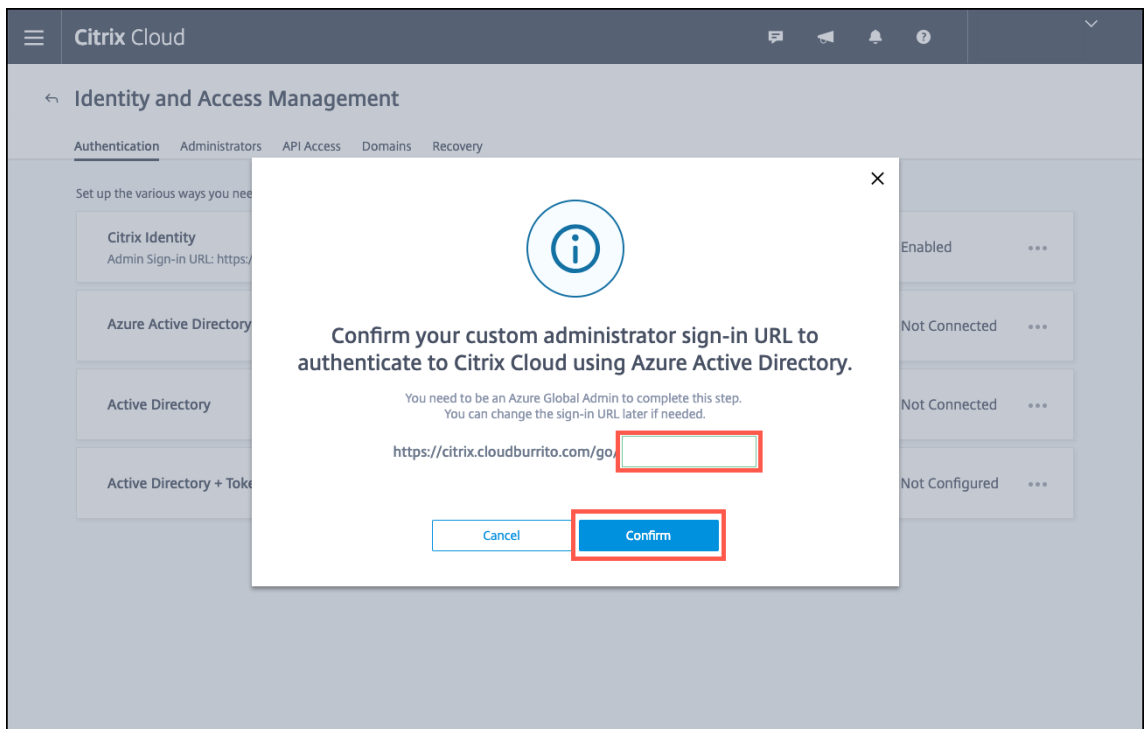
4. Follow the link in the first step to the **Identity and Access Management** page.



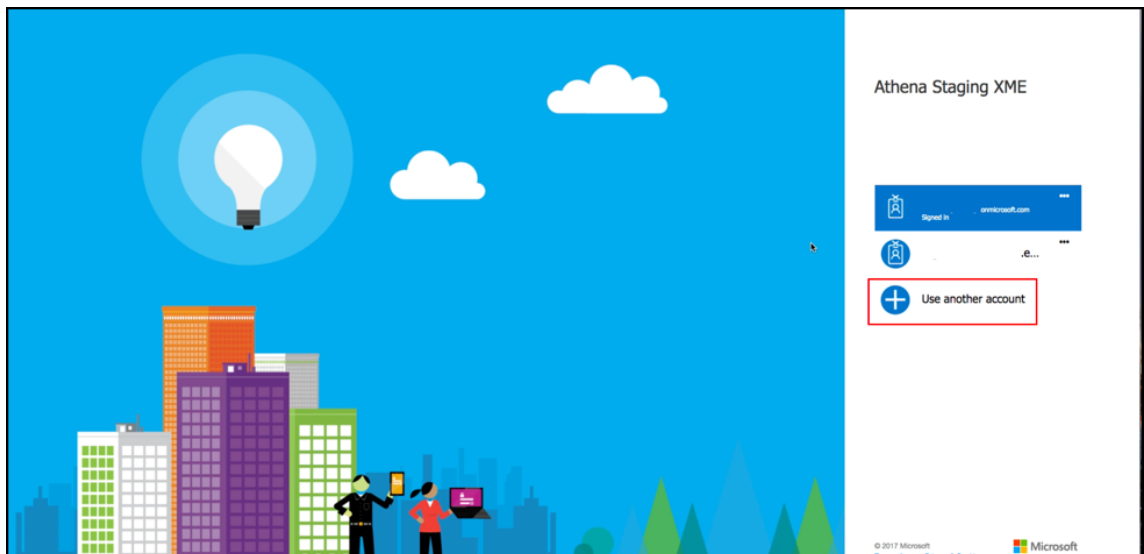
5. Click **Connect** to connect your Azure AD installation.

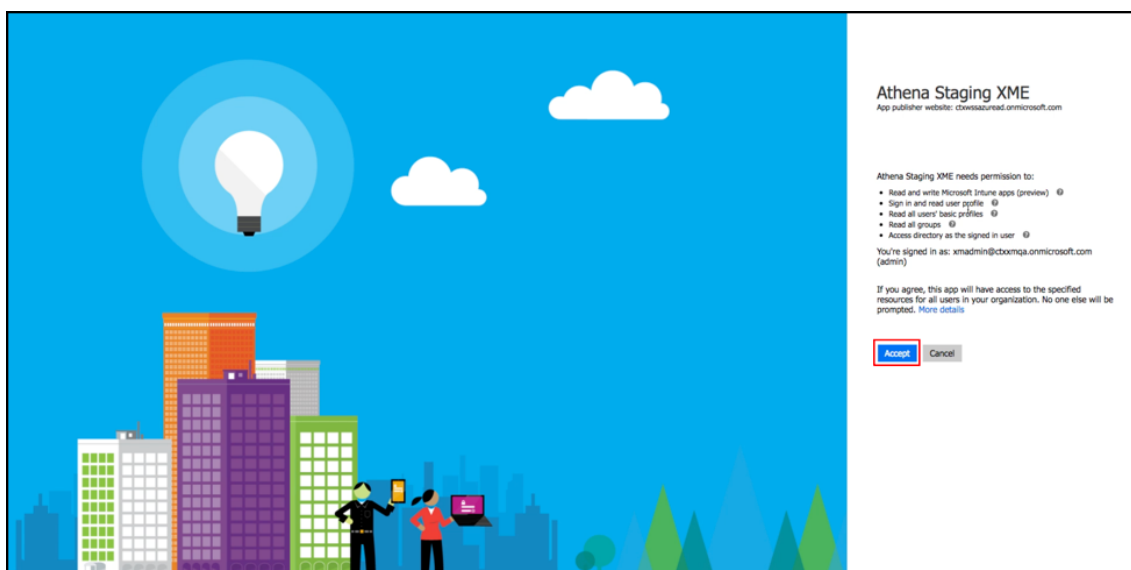


6. Enter a unique logon URL that the Azure AD administrator uses to log on and then click **Confirm**.

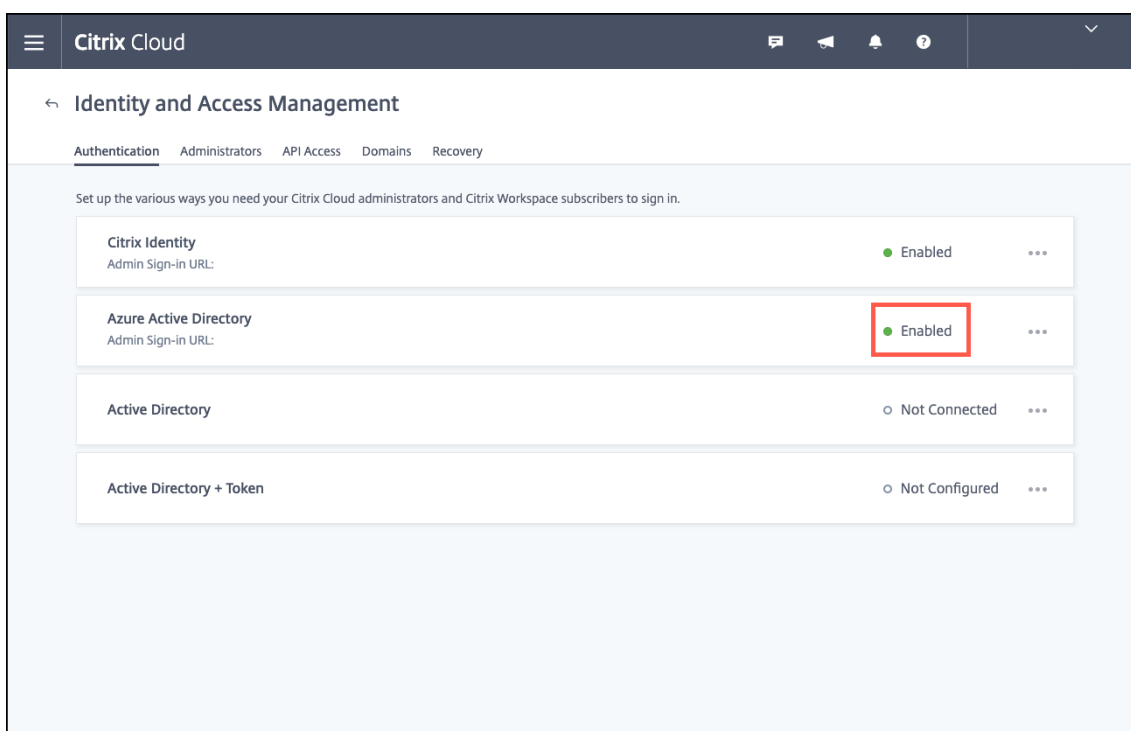


7. Add an Azure AD global administrator account and then accept the permissions request.





- Confirm that your Azure AD instance connects successfully. To indicate a successful connection, the **Not Connected** text changes to say **Enabled**.



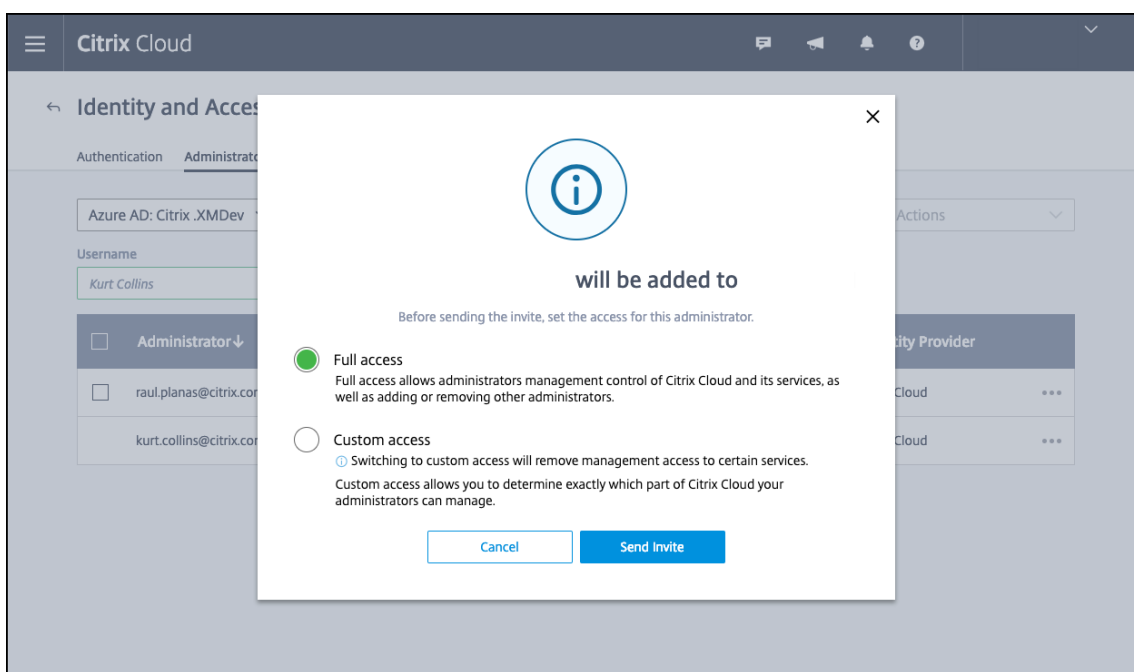
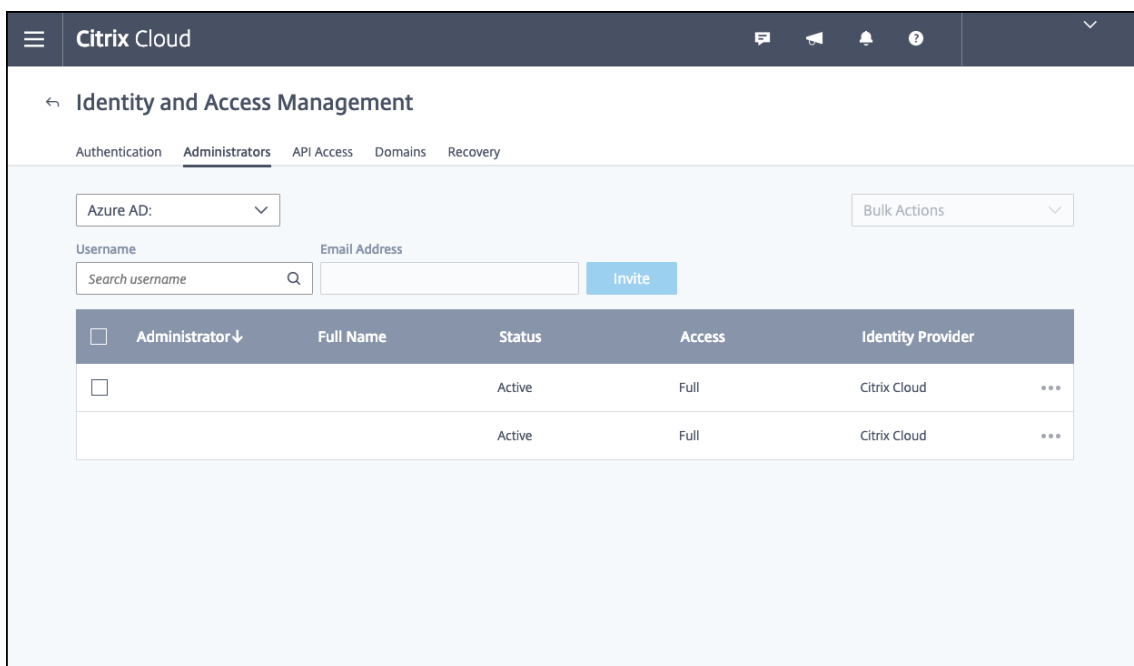
- Click the **Administrators** tab and then add your Azure AD Intune administrator as a Citrix Cloud administrator. Select Azure AD or Citrix Identity from the drop-down menu, and then search for the user name you want to add. Click **Invite** and then grant the user **Full Access** or **Custom Access** before clicking **Send Invite**.

**Note:**

Endpoint Management requires the following rules for **Custom Access:** Library and Citrix Endpoint Management.

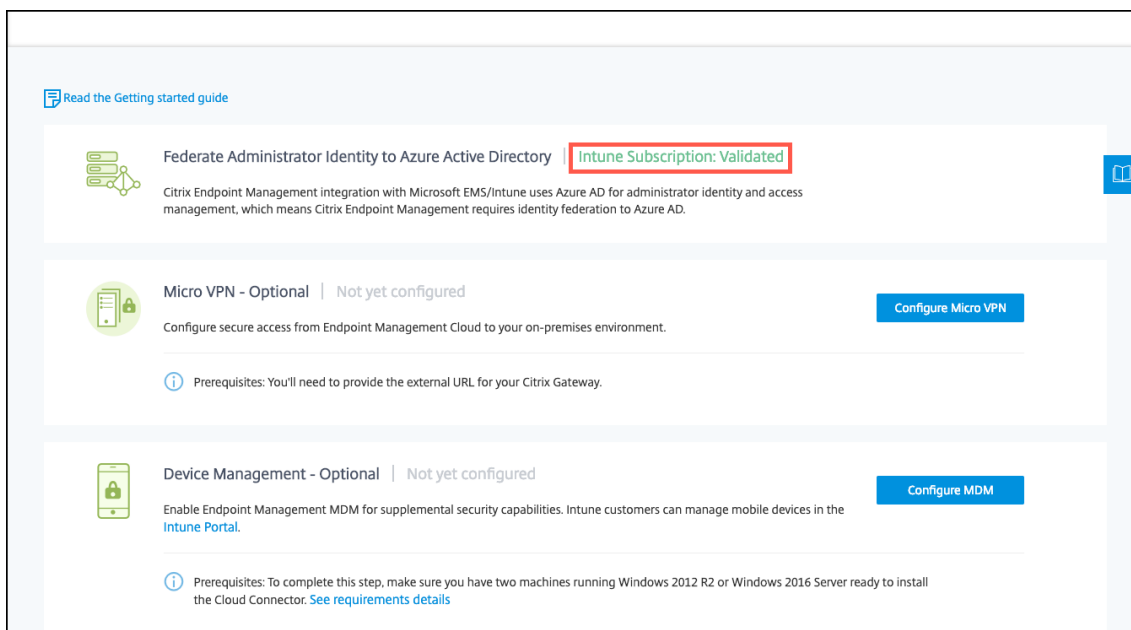
As a result, the Azure AD Intune administrator receives an email invitation to create a password and sign in to Citrix Cloud. Before the administrator signs in, ensure that you sign out of all other accounts.

The Azure AD Intune administrator must follow the remaining steps in this procedure.





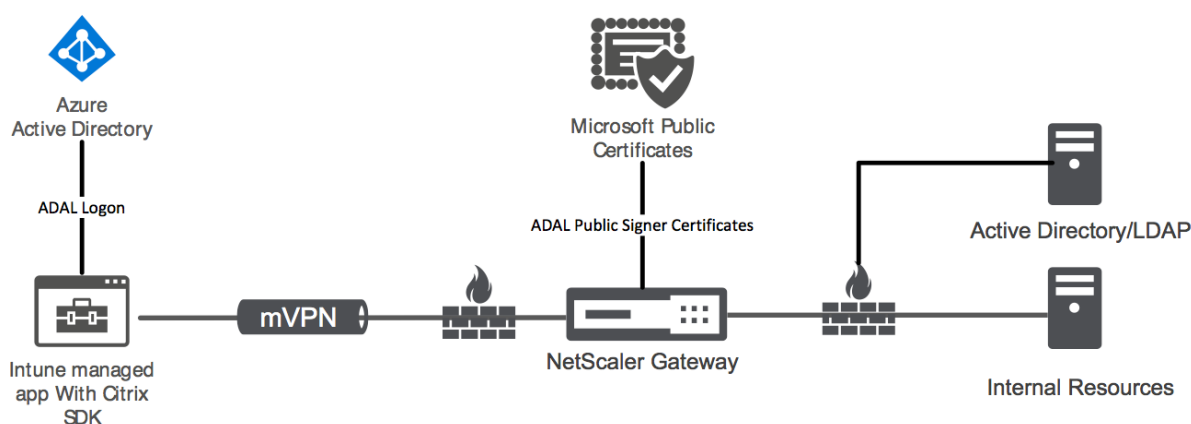
- After signing in with the new account, under **Endpoint Management**, click **Manage**. If you configure everything correctly, the page shows that the Azure AD administrator is signed in and that your Intune subscription is valid.



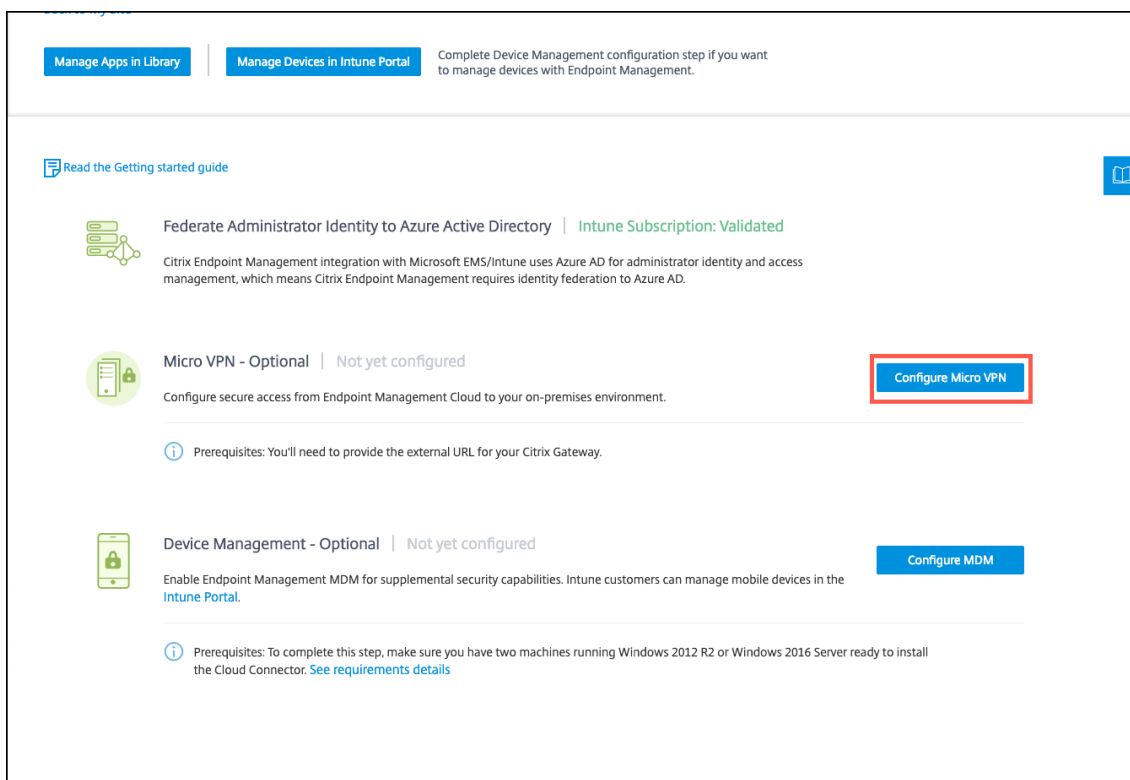
## To configure Citrix Gateway for micro VPN

To use micro VPN with Intune, you must configure Citrix Gateway to authenticate to Azure AD. An existing Citrix Gateway virtual server does not work for this use case.

First, configure Azure AD to sync with the on-premises Active Directory. This step is necessary to ensure that authentication between Intune and Citrix Gateway occurs properly.

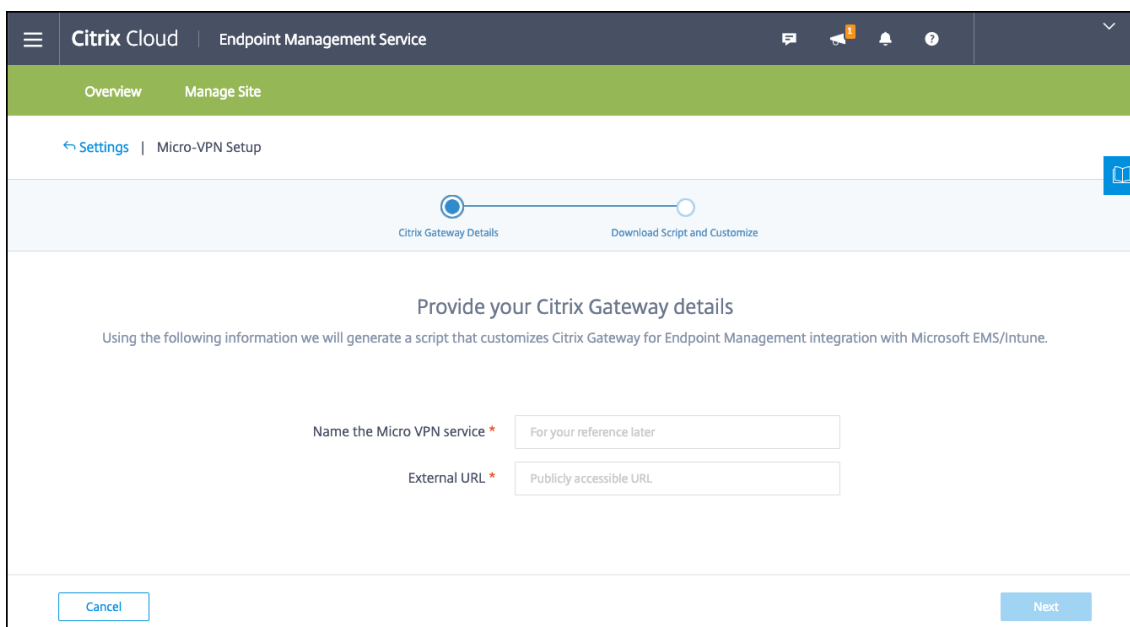


- From the Citrix Cloud console, under **Endpoint Management**, click **Manage**.
- Next to **Micro VPN**, click **Configure Micro VPN**.



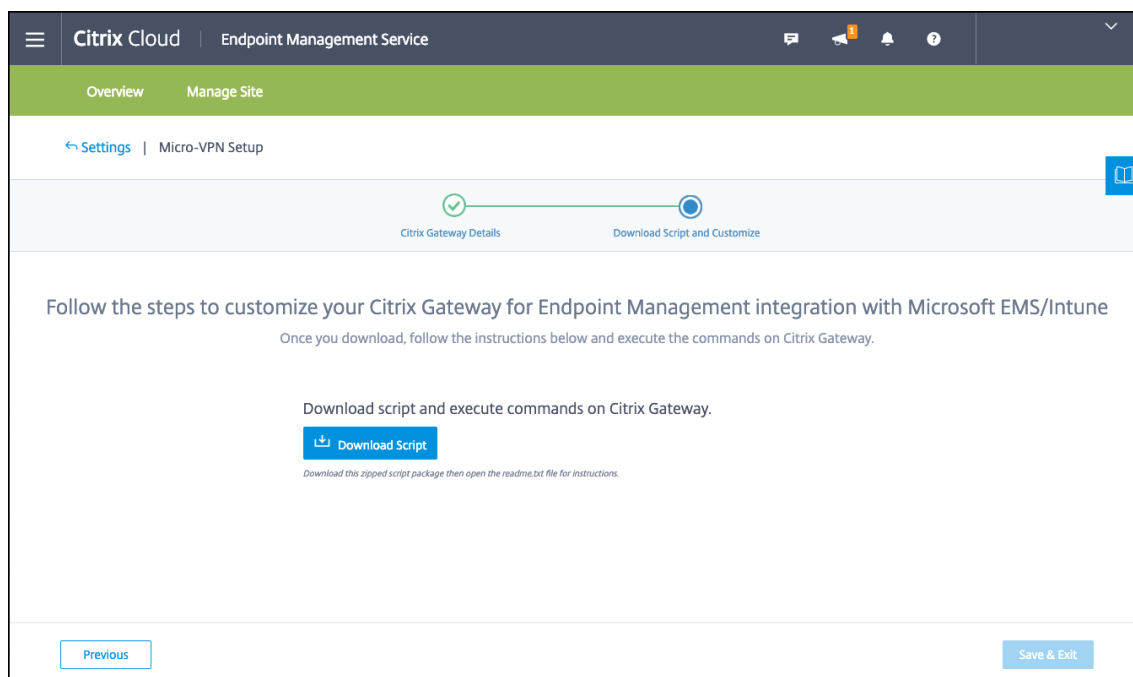
3. Enter a name for the micro VPN service and the external URL for your Citrix Gateway and then click **Next**.

This script configures Citrix Gateway to support Azure AD and the Intune apps.



4. Click **Download Script**. The .zip file includes a readme with instructions for implementing the script. Even though you can Save and Exit from here, the Micro VPN is not set up until you run

the script on your Citrix Gateway installation.



**Note:**

When you finish the Citrix Gateway configuration process, if you see an OAuth Status other than COMPLETE, see the Troubleshooting section.

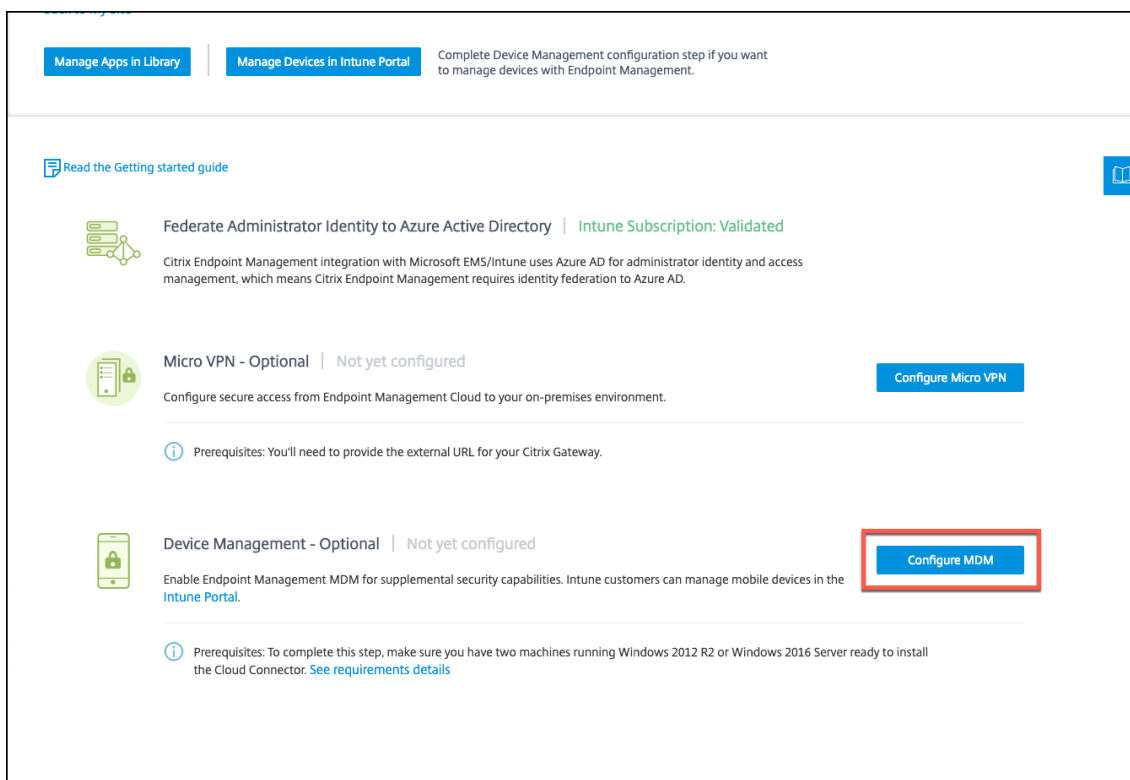
### To configure device management

If you want to manage devices in addition to apps, choose a method of device management. You can use Endpoint Management MDM+MAM or Intune MDM.

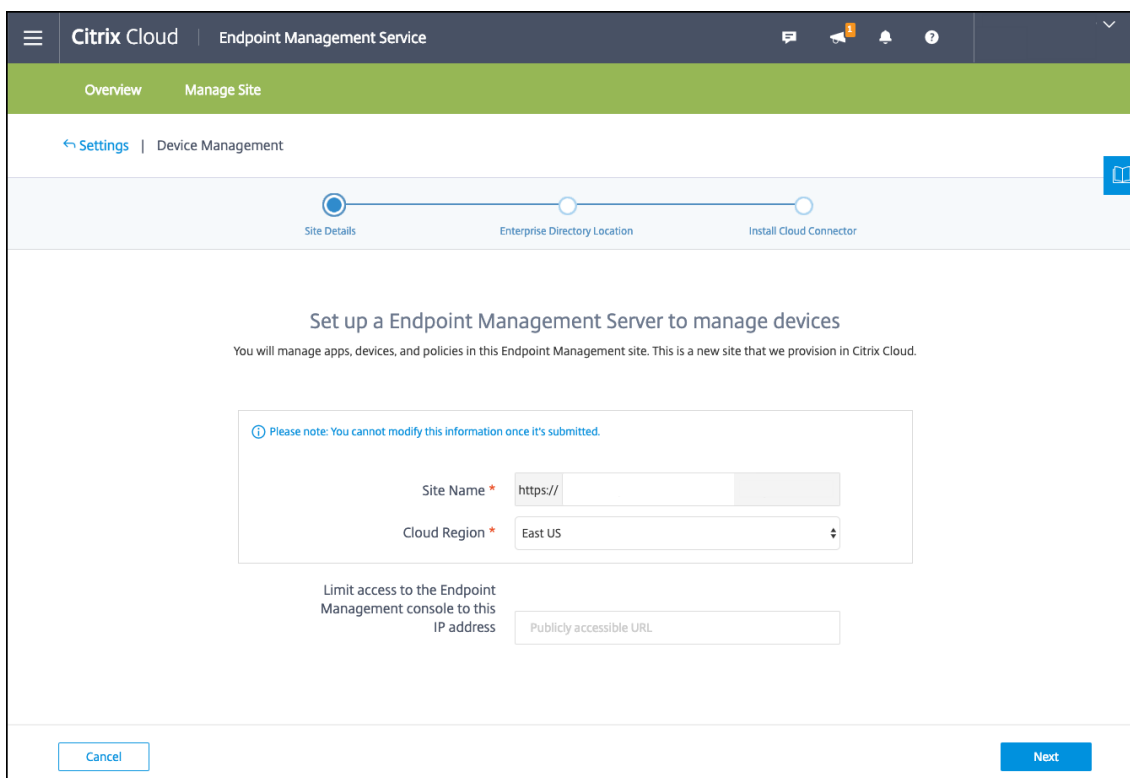
**Note:**

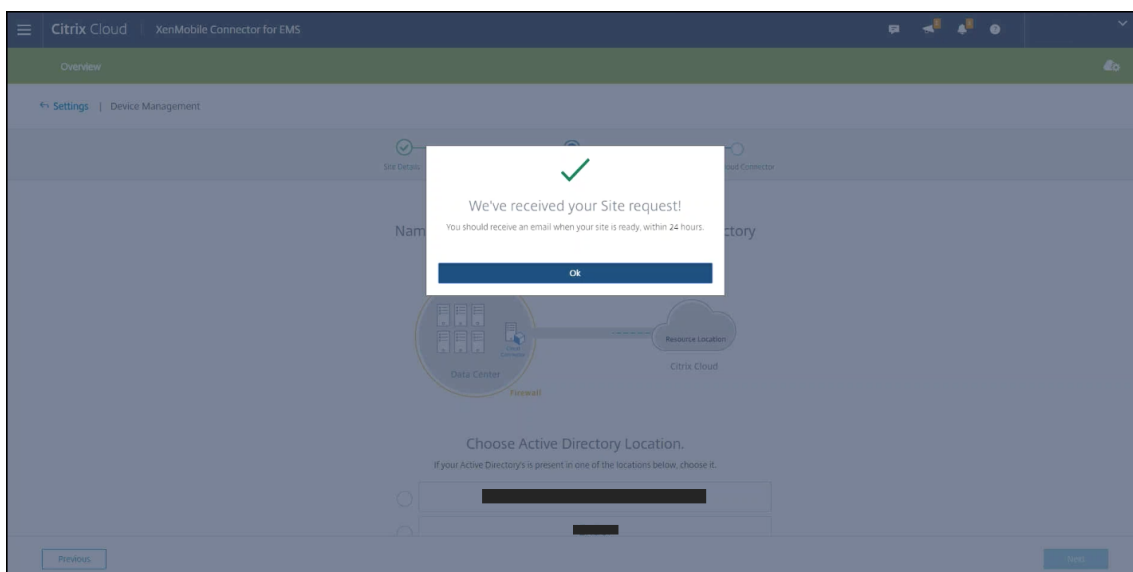
The console defaults to Intune MDM. To use Intune as your MDM provider, see the [Microsoft Intune documentation](#).

1. From the Citrix Cloud console, under Endpoint Management integration with MEM, click **Manage**. Next to **Device Management - Optional**, click **Configure MDM**.

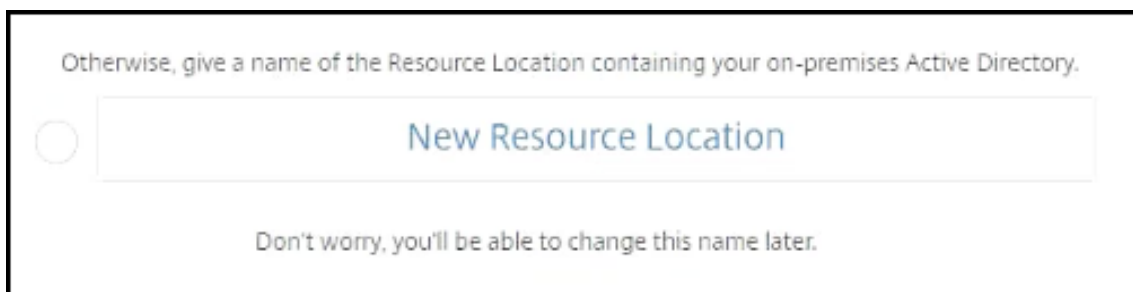
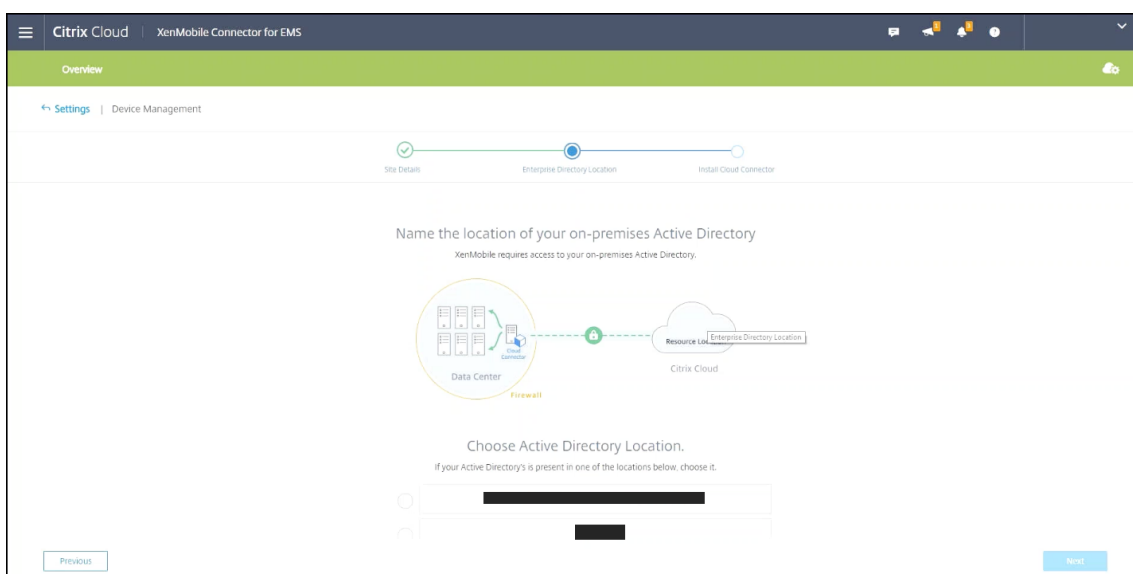


2. Enter a unique site name, select the Cloud region closest to you and then click **Request a Site**. A prompt lets you know that you receive an email when your site is ready.

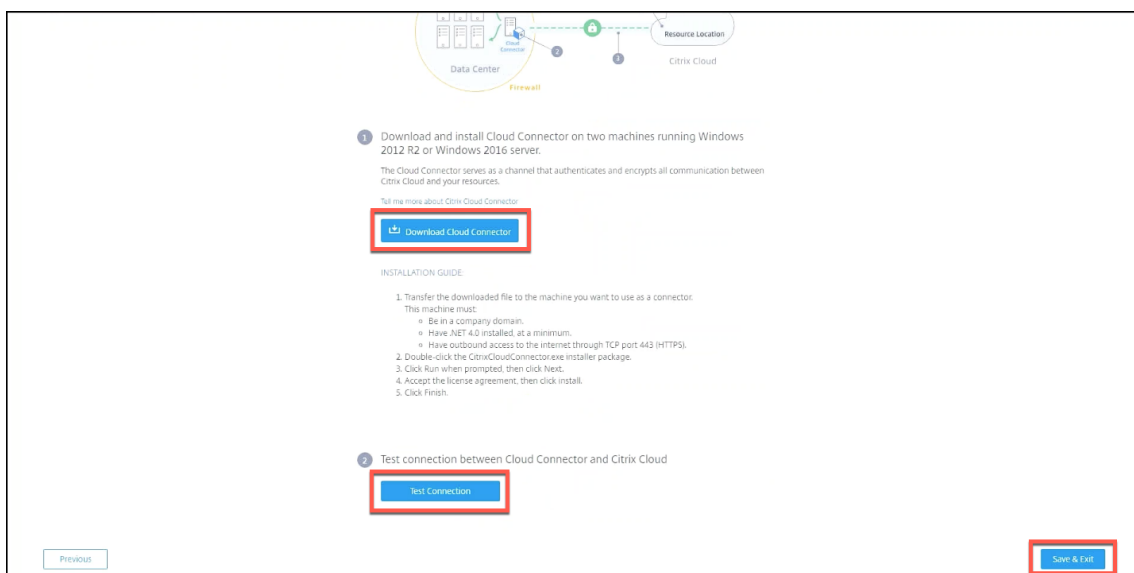
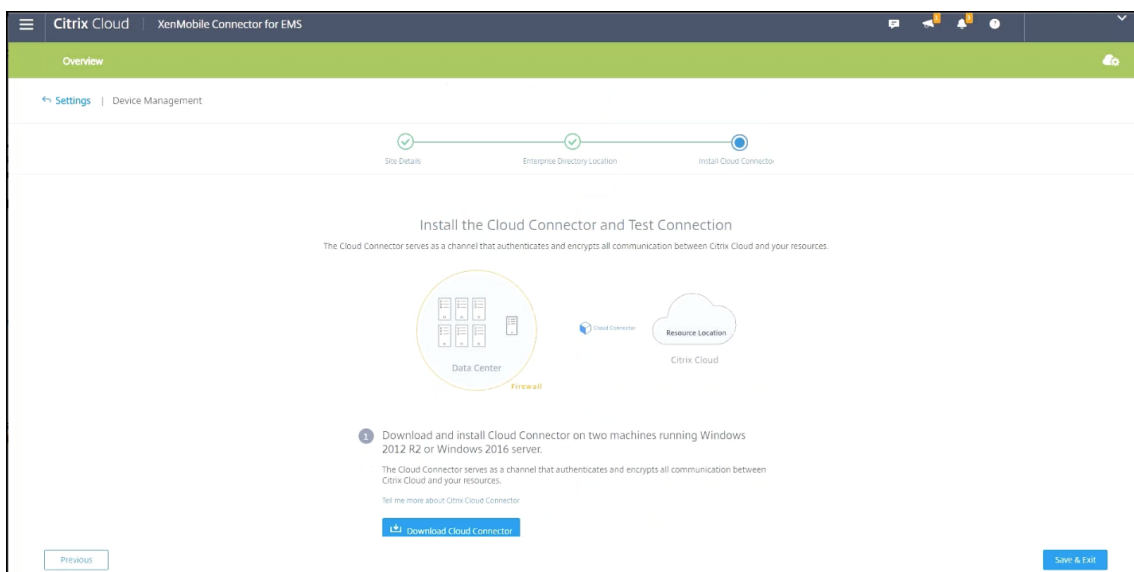




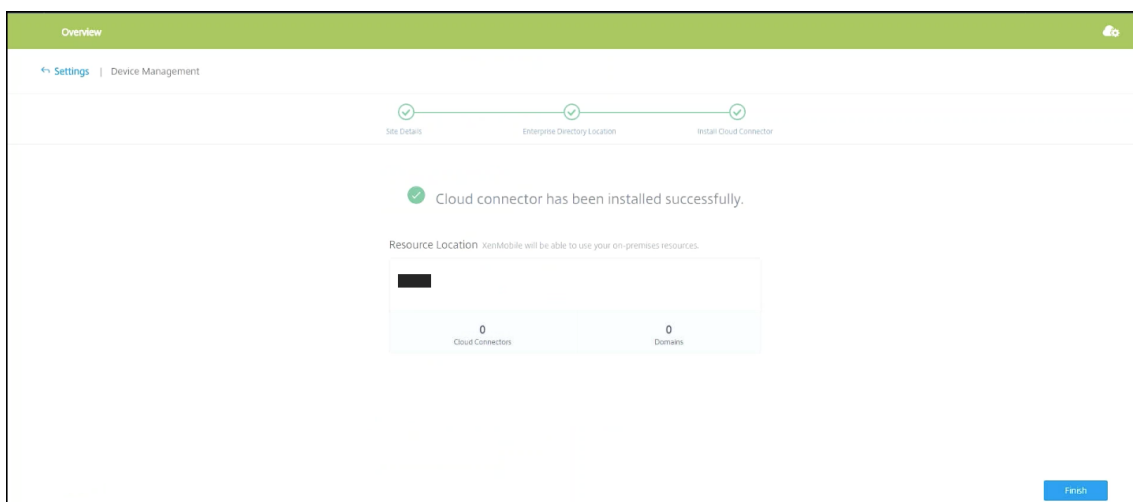
3. Click **OK** to close the prompt. Select an Active Directory Location to associate with your site or create a resource location and then click **Next**.



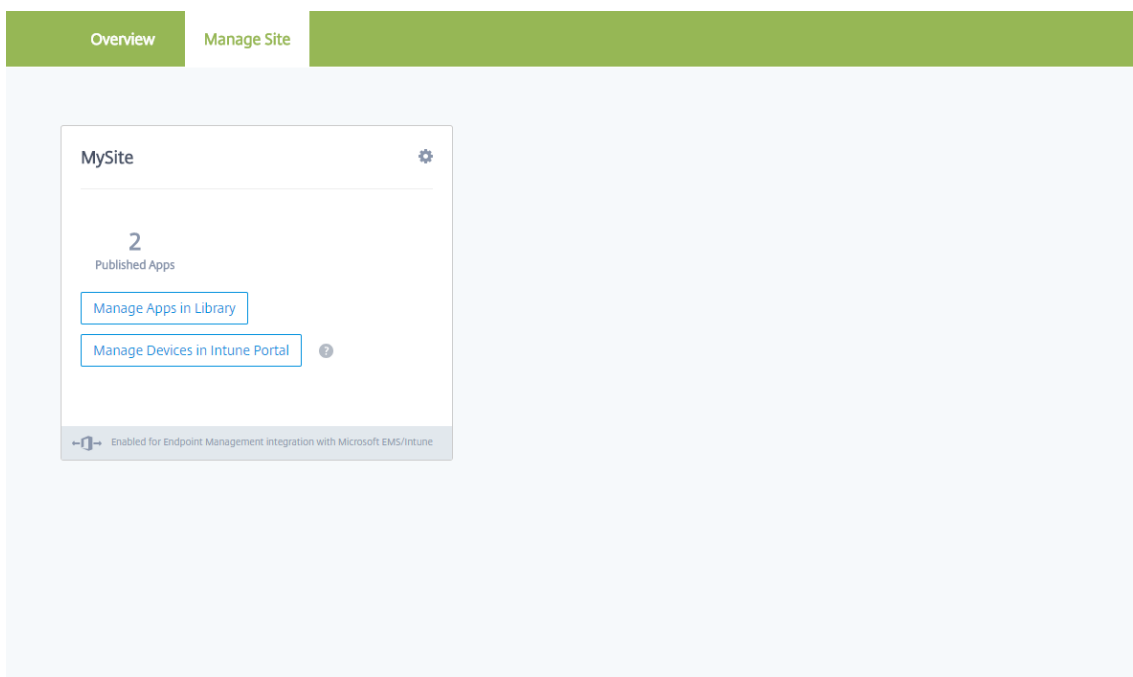
4. Click **Download Cloud Connector** and follow the on-screen instructions to install the cloud connector. After installation, click **Test Connection** to verify the connection between Citrix Cloud and the Cloud Connector.



5. Click **Save & Exit** to finish. Your resource location appears. Clicking **Finish** takes you back to the settings screen.



6. You can now access the Endpoint Management console from your site tile. From here, you can perform MDM management tasks and assign device policies. For more information on device policies, see [Device Policies](#).



### Configure Intune managed apps for delivery to devices

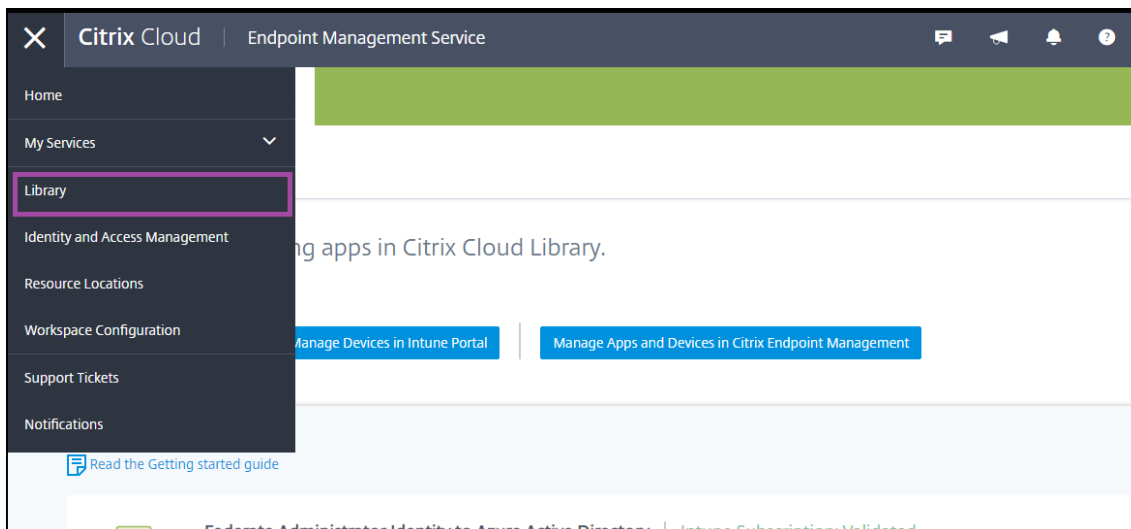
To configure Intune managed apps for delivery:

- Add the apps to the Citrix Cloud library
- Create Endpoint Management device policies to control the flow of data
- Create a delivery group for the apps and policies

## Add Microsoft Intune apps to the Citrix Cloud library

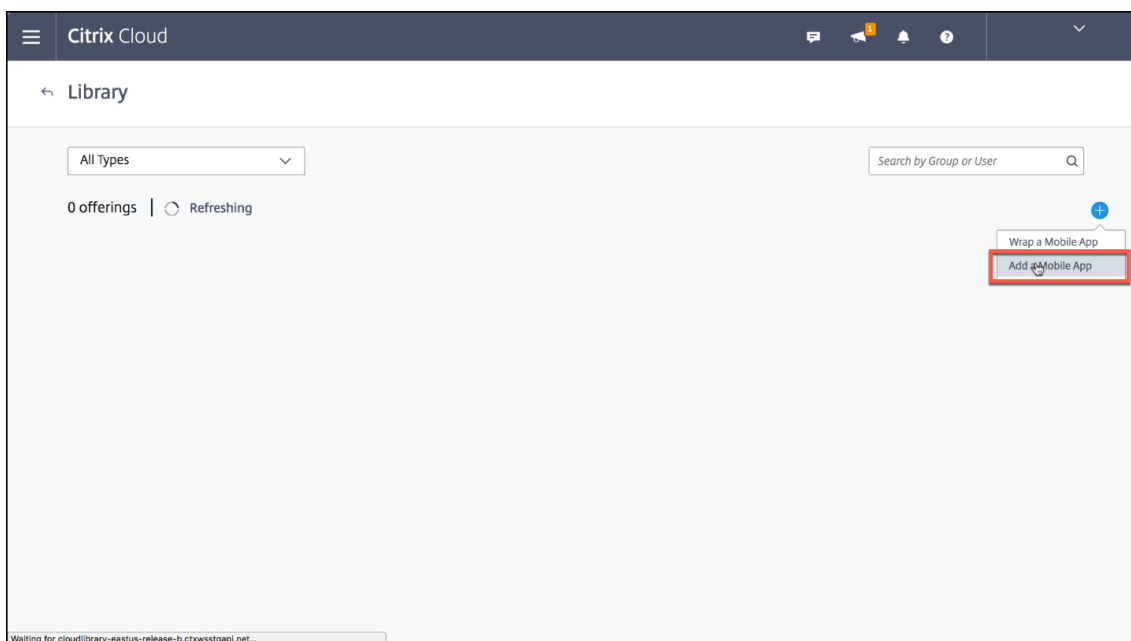
For each app you want to add:

1. From the Citrix Cloud console, click the menu icon and then click **Library**.



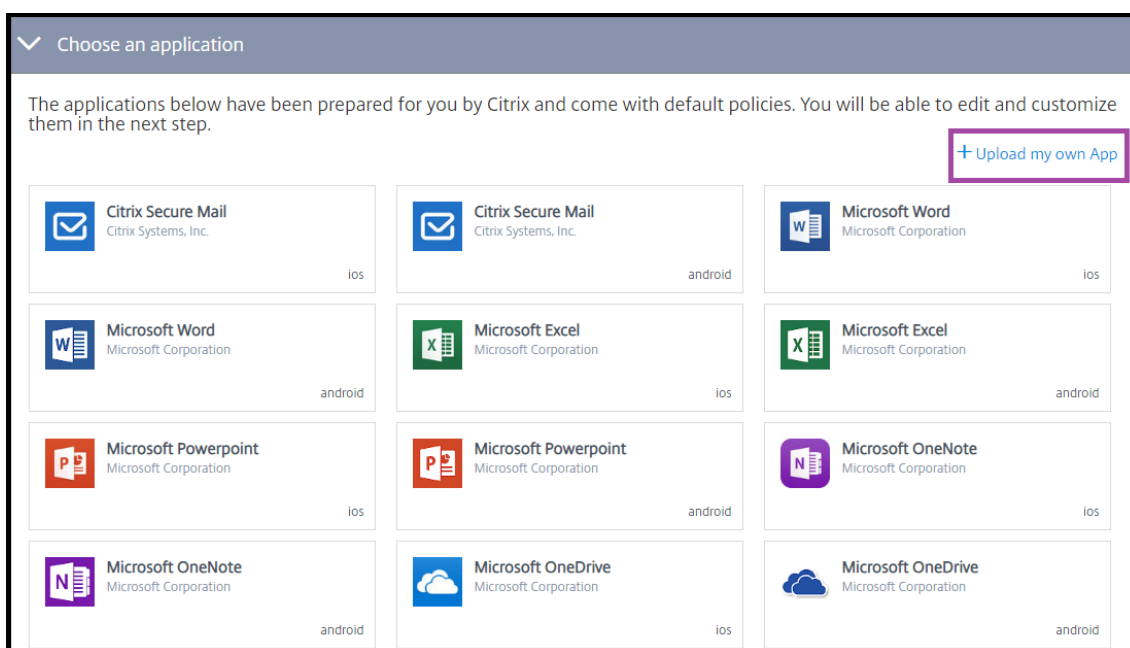
2. Click the plus sign icon on the upper-right, and then click **Add a Mobile app**.

You might need to wait a minute for the options to populate the list.



3. If you have Android Enterprise configured in the Endpoint Management console, select **Microsoft Intune Apps** under **Choose an application**. Select an app template to customize or click **Upload my own App**.





Citrix supplies the existing app templates, each of which comes with a set of preconfigured default policies. For apps that customers upload, the following policies apply:

- **MDX Files:** Includes MAM SDK enabled apps or MDX-wrapped apps, such as:
  - Intune app protection policies and the default MDX policies contained in the package
  - Public store apps, such as Intune app protection policies and default MDX policies that match the bundle ID or package ID
- **IPA Files:** Intune app protection policies.
- **APK Files:** Intune app protection policies.

**Note:**

If the app is not wrapped with Intune, Intune app protection policies do not apply.

4. Click **Upload my own App** and upload your .mdx or Intune wrapped file.

Upload my own MDX wrapped app

Add an app wrapped using the MDX Toolkit or the Intune wrapping tool to include application policies. You can deploy MDX apps obtained internally and from the public store. Example: Secure Mail

Instructions to wrap [Back to app list](#)

Upload an MDX or Intune wrapped app package:

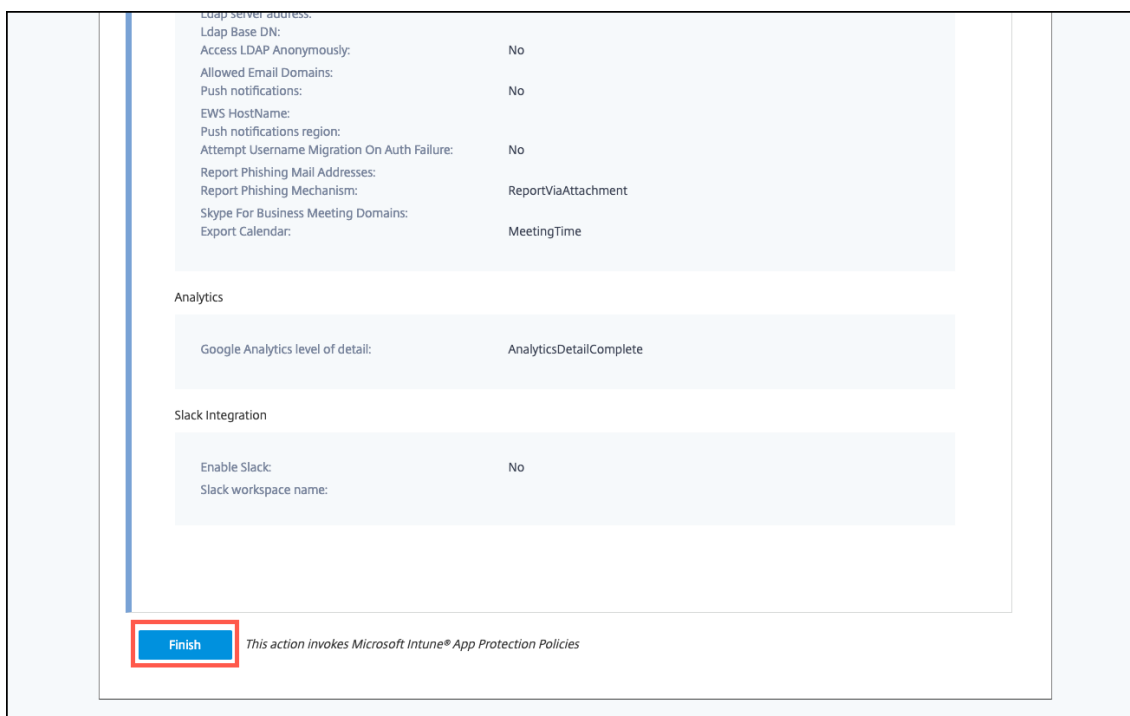
.mdx file or Intune wrapped file  [Browse](#)

[Next](#)

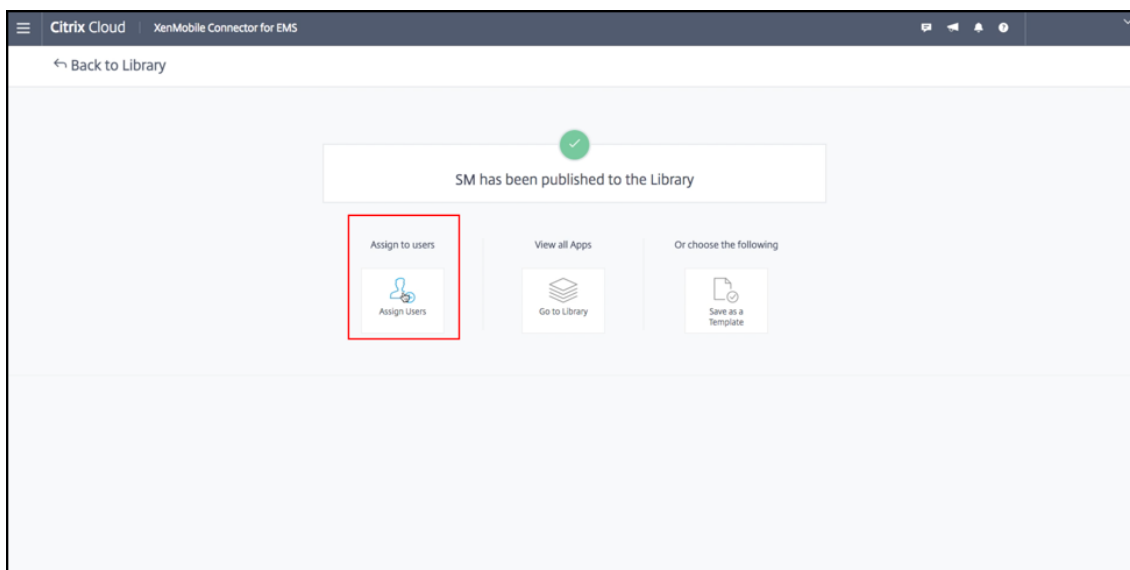
- > Application details
- > Configure application policies
- > Summary

5. Enter a name and description for the app, choose whether the app is optional or required, and then click **Next**.
6. Configure the application settings. The following configurations enable Endpoint Management and Intune containers to transfer data to each other.
  - **Allow apps to receive data from other apps:** Select **Policy managed apps**.
  - **Allow app to transfer data to other apps:** Select **All apps**.
  - **Restrict cut, copy, paste with other apps:** Select **Policy managed apps**.
7. Configure the storage repositories for saved data. For **Select which storage services corporate data can be saved to**, select **LocalStorage**.
8. Optional: Set Data Relocation, Access, and PIN policies for the app. Click **Next**.
9. Review the summary of the app, and then click **Finish**.

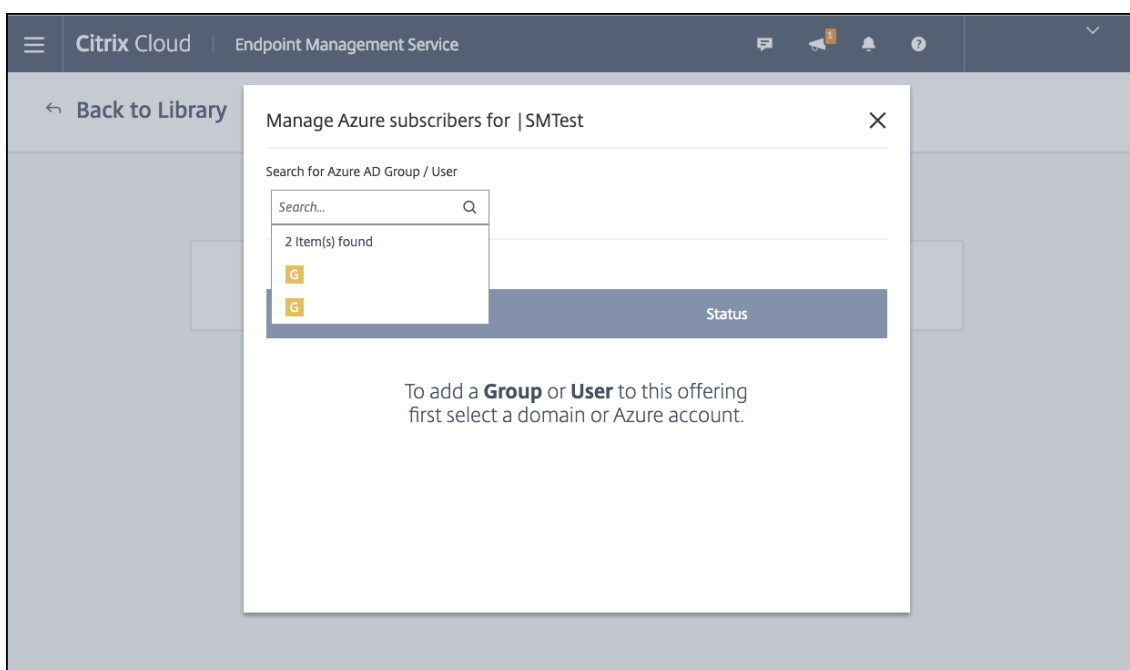
The app configuration process might take a few minutes. When the process completes, a message indicates that the app has been published to the library.



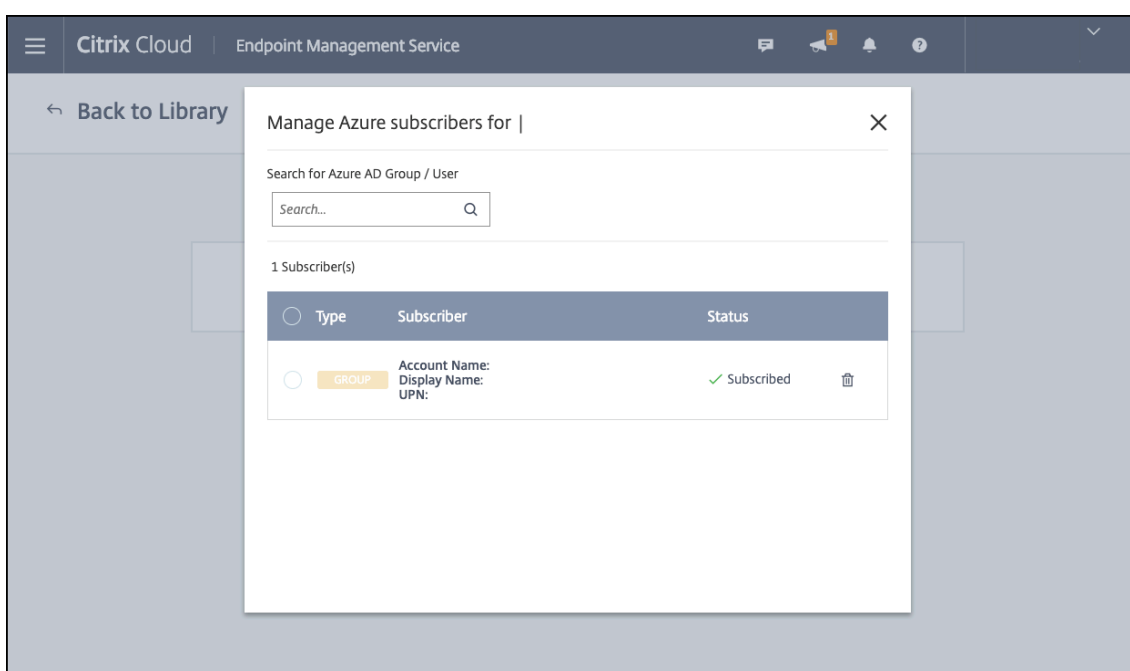
10. To assign user groups to the app, click **Assign Users**.



11. In the search box, search for user groups and click to add them. You cannot add individual users.



12. When you have added all the groups you want, close the window by clicking the X.



You might encounter an error when adding user groups. This error occurs when the user group has not been synchronized to the Local Active Directory.

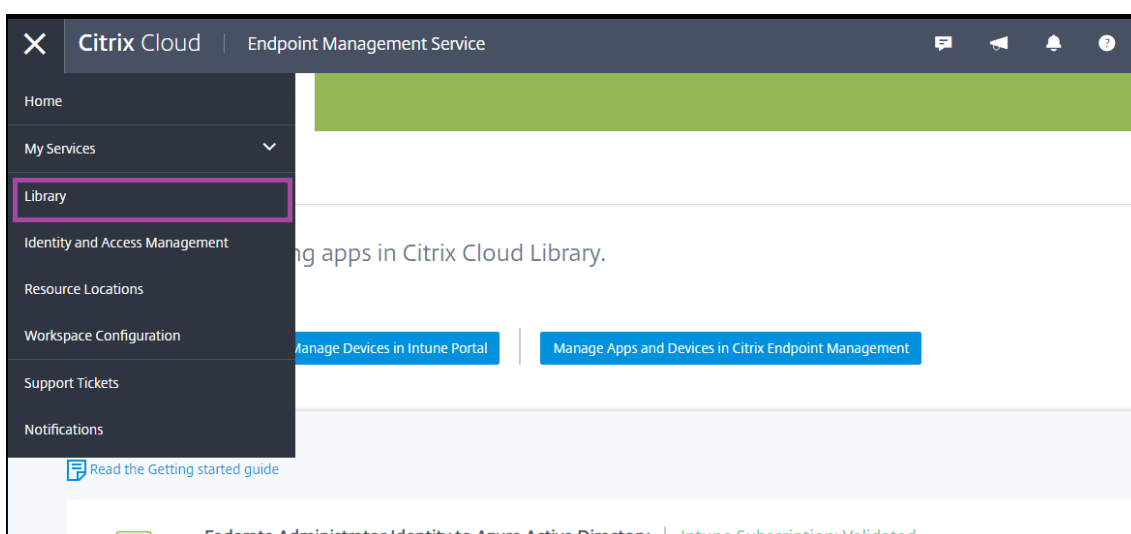
### Add Android Enterprise apps to the Citrix Cloud Library

In order to add Android Enterprise apps to the Citrix Cloud Library and set Intune app protection policies, configure your cloud environment with the following:

- Federate Citrix Cloud with your Azure Active Directory (AAD) account. See [Connect Azure Active Directory to Citrix Cloud](#).
- Configure LDAP and Cloud Connector in Endpoint Management.
- Set up Android Enterprise in Endpoint Management. Ensure that Android Enterprise devices enroll in MDM+MAM. To set up Android Enterprise, see [Android Enterprise](#).

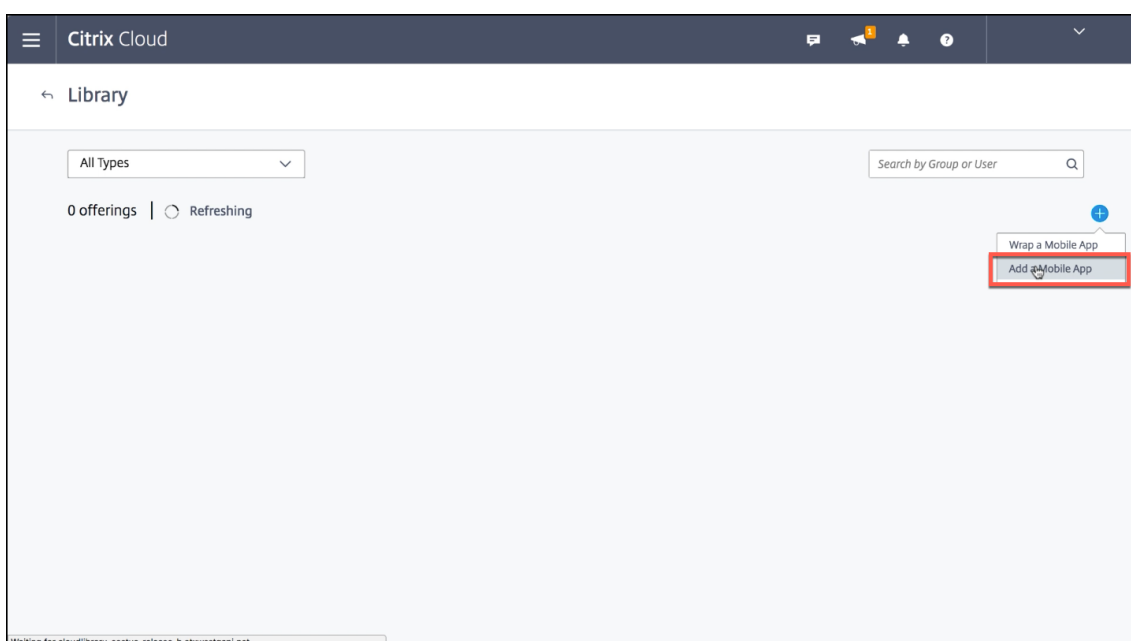
Following this procedure adds Android Enterprise apps to the Endpoint Management console and Intune console simultaneously. For each Android Enterprise app you want to add:

1. From the Citrix Cloud console, click the menu icon and then click **Library**.

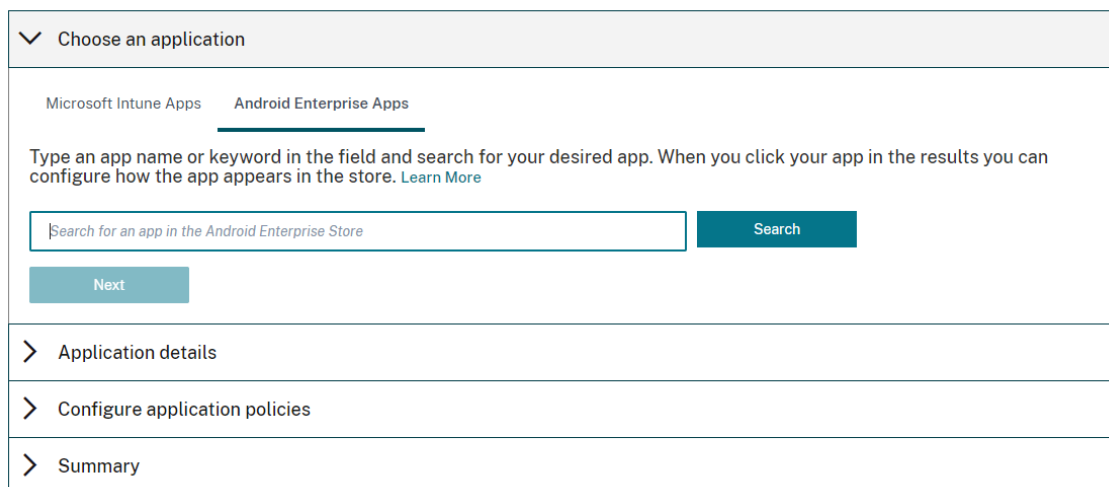


2. Click the plus sign icon on the upper-right, and then click **Add a Mobile app**.

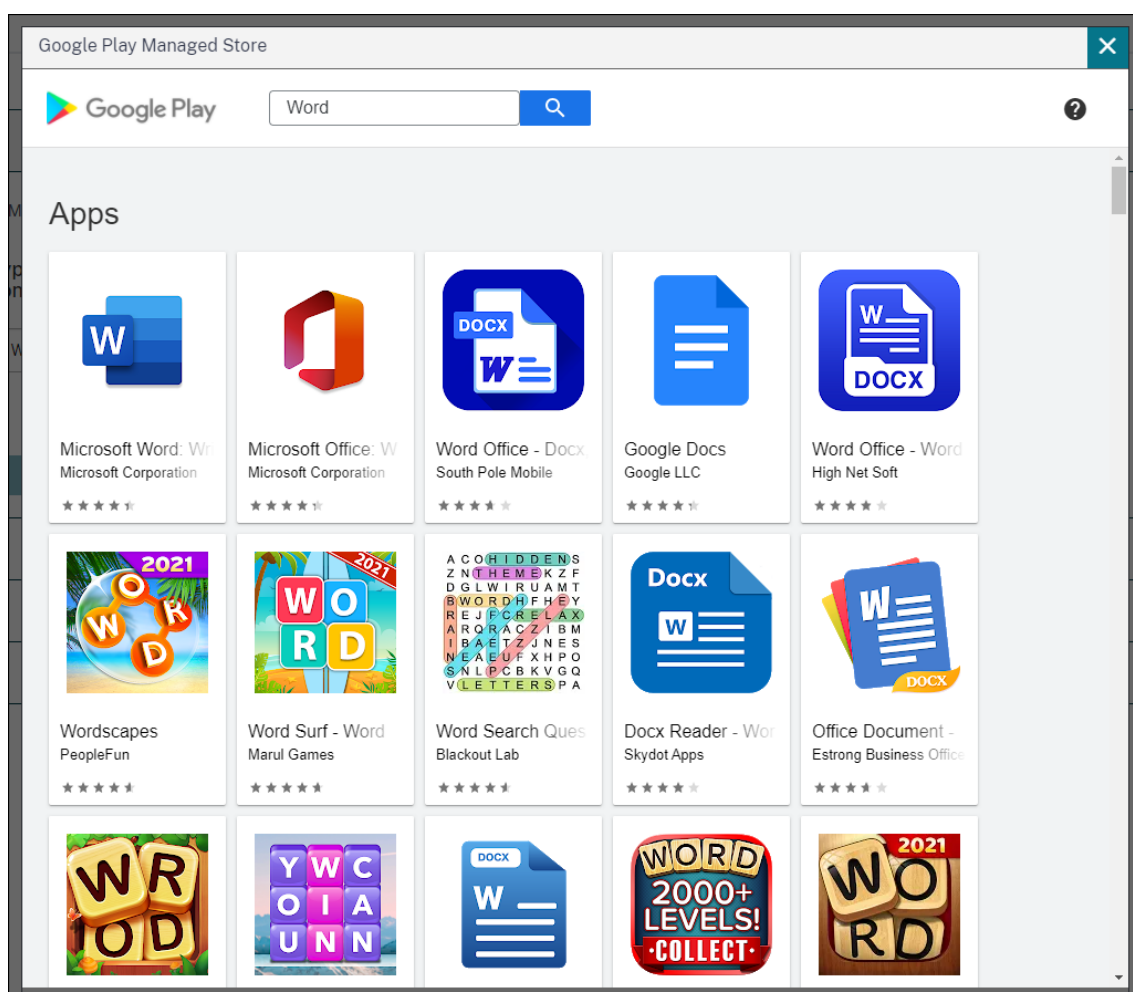
You might need to wait a minute for the options to populate the list.



3. Under **Choose an application**, select **Android Enterprise Apps**.



4. Search for an app and approve it in the Managed Google Play store window. After the Google window closes, click **Next**.



▼ Choose an application

Microsoft Intune Apps
Android Enterprise Apps

Type an app name or keyword in the field and search for your desired app. When you click your app in the results you can configure how the app appears in the store. [Learn More](#)

Search

You selected the following Managed Google Play App:

**Microsoft Word: Write, Edit & Share**  
 Docs on the Go  
 Version: 16.0.13628.20214  
 For Android

Next

> Application details

> Configure application policies

> Summary

5. Add application details, and then click **Next**.

> Choose an application ✓

▼ Application details

You can name this based on who will receive this app or what helps you for reference later.

**Microsoft Word: Write, Edit & Share**  
 Docs on the Go  
 Android

Name this published app

Custom Name

Description

Custom description ...

Highlight app in store

Show app in the 'Featured' section of the Intune app store.

Required app

This is a required app and should be automatically installed on the user's device.

Previous

Next

> Configure application policies

6. If you searched for and selected a Citrix mobile productivity app, you can configure Micro VPN policies. After you configure those policies, click **Next**.

> Choose an application	✓
> Application details	✓
<b>▼ Configure Micro VPN policies</b>	
<p>Enable Micro-VPN if you would like this app to access your on premises resources.</p> <p><a href="#">Apply recommended default settings</a></p> <p>Network access  <input type="text" value="Unrestricted"/></p> <p>micro VPN session required  <input type="text" value="No"/></p> <p>Exclusion List  <input type="text"/></p> <p><a href="#">Previous</a>   <a href="#">Next</a></p>	
> Configure application policies	
> Summary	

7. Configure Intune app protection policies. Click **Next**.

> Choose an application	✓
> Application details	✓
<b>▼ Configure application policies</b>	
<p><b>Intune app protection policies</b></p> <ul style="list-style-type: none"> <li>Data relocation</li> <li>Access</li> <li>PIN</li> </ul> <p><a href="#">Apply recommended default settings</a></p> <p>Allow app to receive data from other apps  <input type="text" value="All apps"/></p> <p>Allow app to transfer data to other apps  <input type="text" value="All apps"/></p> <p>Restrict cut, copy, and paste with other apps  <input type="text" value="Any apps"/></p> <p>Prevent Android backups  <input checked="" type="radio"/> Yes   <input type="radio"/> No</p> <p>Block managed apps from running on jailbroken or rooted devices  <input checked="" type="radio"/> Yes   <input type="radio"/> No</p> <p>Restrict web content transfer with other apps  <input type="text" value="Any App"/></p>	



8. Configure the application settings. The following configurations enable Endpoint Management and Intune containers to transfer data to each other.
  - **Allow apps to receive data from other apps:** Select **Policy managed apps**.
  - **Allow app to transfer data to other apps:** Select **All apps**.
  - **Restrict cut, copy, paste with other apps:** Select **Policy managed apps**.
9. Configure the storage repositories for saved data. For **Select which storage services corporate data can be saved to**, select **LocalStorage**.
10. Optional: Set Data Relocation, Access, and PIN policies for the app. Click **Next**.
11. Review the summary of the app, and then click **Finish**.

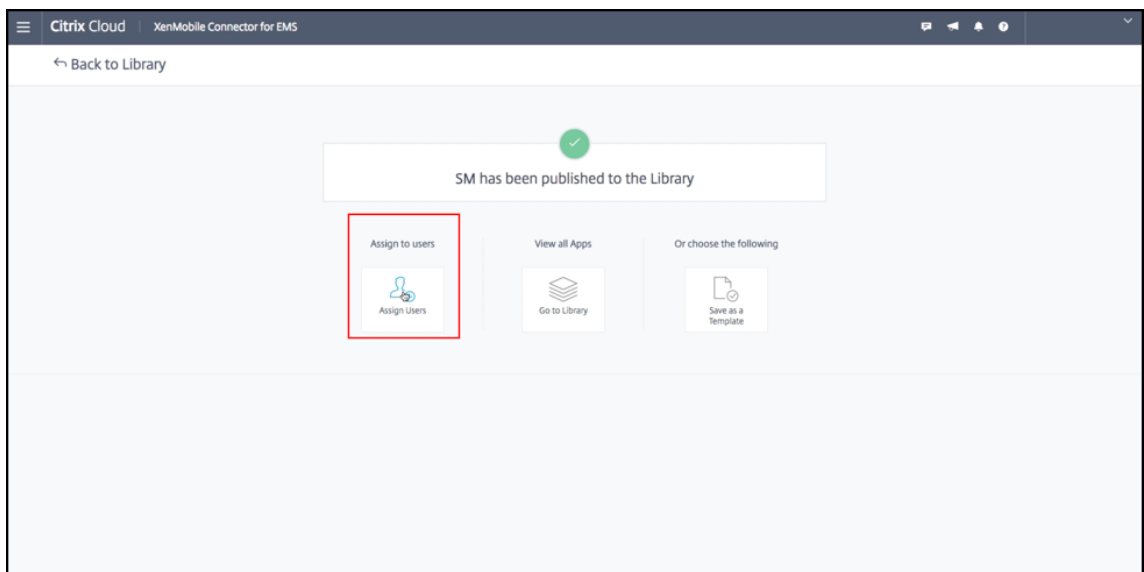
The app configuration process might take a few minutes. When the process completes, a message indicates that the app has been published to the library. The app is available in the Endpoint Management and Intune consoles. In the Endpoint Management console, the app is part of a new delivery group and is identified as a public app store app.

The screenshot displays the configuration summary for an application. It is organized into several sections:

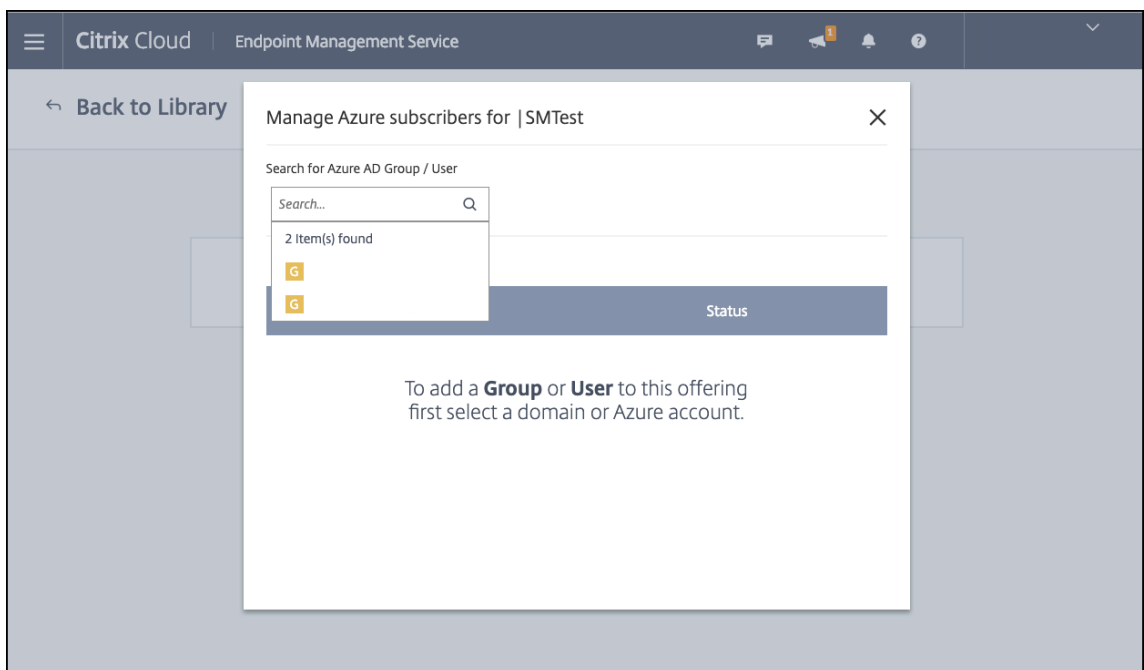
- LDAP Settings:**
  - Ldap server address: (empty)
  - Ldap Base DN: (empty)
  - Access LDAP Anonymously: No
  - Allowed Email Domains: (empty)
  - Push notifications: No
  - EWS HostName: (empty)
  - Push notifications region: (empty)
  - Attempt Username Migration On Auth Failure: No
  - Report Phishing Mail Addresses: (empty)
  - Report Phishing Mechanism: ReportViaAttachment
  - Skype For Business Meeting Domains: (empty)
  - Export Calendar: MeetingTime
- Analytics:**
  - Google Analytics level of detail: AnalyticsDetailComplete
- Slack Integration:**
  - Enable Slack: No
  - Slack workspace name: (empty)

At the bottom left, there is a blue **Finish** button, which is highlighted with a red rectangular box. A tooltip next to it states: "This action invokes Microsoft Intune® App Protection Policies".

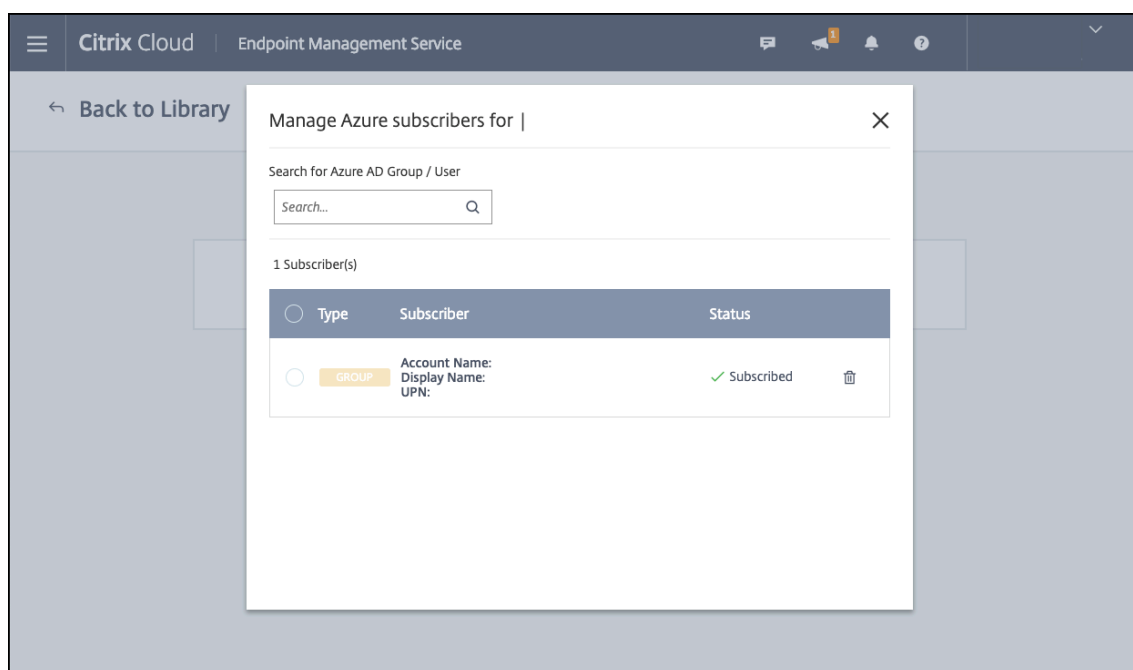
12. To assign user groups to the app, click **Assign Users**.



13. In the search box, search for user groups and click to add them. You cannot add individual users.



14. When you have added all the groups you want, close the window by clicking the X.



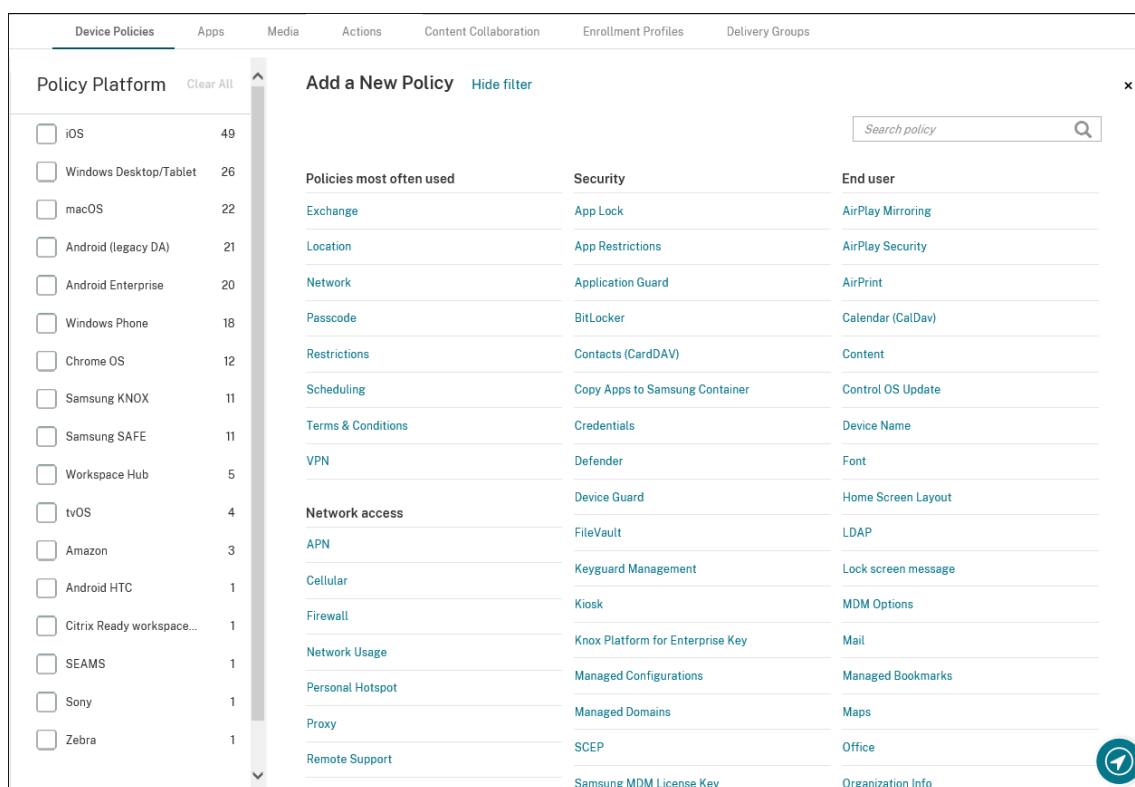
You might encounter an error when adding user groups. This error occurs when the user group has not been synchronized to the Local Active Directory.

### Control the type of data transferred between managed apps

Control the type of data that can transfer between managed apps within the Endpoint Management or Intune containers using Endpoint Management device policies. You can configure a Restrictions policy to allow only data tagged as “corporate”. Configure an App Configuration policy to tag the data.

To configure the Restrictions device policy:

1. In the Endpoint Management console, click **Configure > Device Policies**.
2. On the **Device Policies** page, click **Add**. The **Add a New Policy** page appears.



3. Click **Restrictions** from the list of policies.
4. On the **Policy Information** page, type a name and (optionally) a description for the policy. Click **Next**.
5. To create a device policy for iOS apps, select **iOS** in the **Platforms** pane.
6. Under **Security - Allow**, set **Documents from managed apps in unmanaged apps** to **Off**. Turning this setting **Off** also sets **Unmanaged apps read managed contacts** and **Managed apps write unmanaged contacts** to **Off**. Click **Next**.
7. Click **Next** until the **Save** button appears. Click **Save**.

Configure the App Configuration device policy for each app:

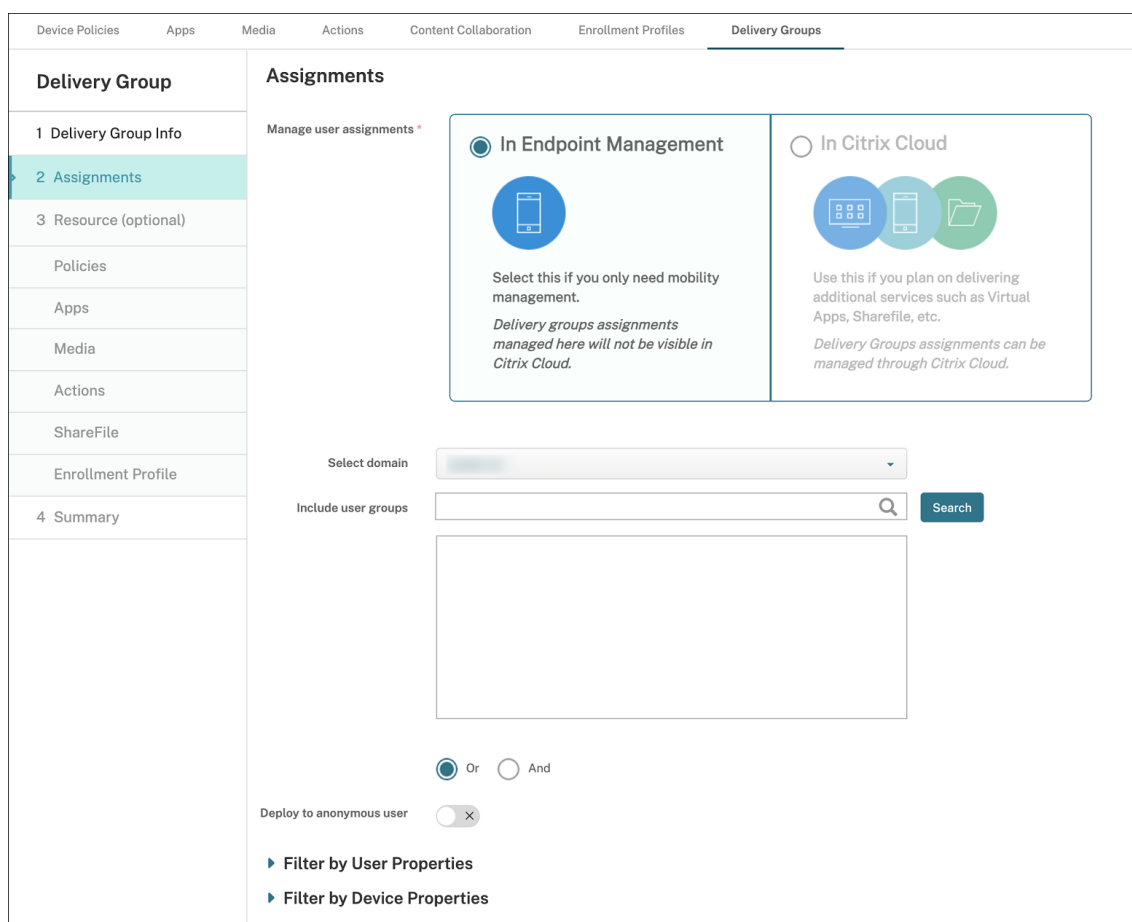
1. In the Endpoint Management console, click **Configure > Device Policies**.
2. Click **Add**. The **Add a New Policy** page appears.
3. Click **App Configuration** from the list of policies.
4. On the **Policy Information** page, type a name and (optionally) a description for the policy. Click **Next**.
5. To create a device policy for an iOS app, select **iOS** in the **Platforms** pane.
6. Select the identifier for the app to be configured.
7. For iOS apps, add the following text to **Dictionary content**:

```
1 <dict>
2   <key>IntuneMAMUPN</key>
3   <string>${
4   user.userprincipalname }
5 </string>
6 </dict>
7 <!--NeedCopy-->
```

8. Click **Check Dictionary**.
9. Click **Next**.
10. Click **Save**.

### **Configure delivery groups for the apps and device policies**

1. In the Endpoint Management console, click **Configure > Delivery Groups**.
2. On the **Delivery Groups** page, click **Add**. The **Delivery Group Information** page appears.
3. On the **Delivery Group Information** page, type a name and (optionally) a description for the delivery group. Click **Next**.
4. On the **Assignments** page, specify how you want to deploy the delivery group: Choose **In Endpoint Management** or **In Citrix Cloud**.



5. If you chose **In Endpoint Management**:

- **Select domain:** From the list, select the domain from which to choose users.
- **Include user groups:** Do one of the following:
  - In the list of user groups, click the groups you want to add. The selected groups appear in the **Selected user groups** list.
  - Click **Search** to see a list of all user groups in the selected domain.
  - Type a full or partial group name in the search box, and then click **Search** to limit the list of user groups.

To remove a user group from the **Selected user groups** list, do one of the following:

- In the **Selected user groups** list, click the **X** next to each of the groups you want to remove.
- Click **Search** to see a list of all user groups in the selected domain. Scroll through the list and clear the check box of each of the groups you want to remove.
- Type a full or partial group name in the search box, and then click **Search** to limit the list of user groups. Scroll through the list and clear the check box of each of the groups you want to remove.

6. Click **Next**.
7. In the **Policies** page, drag the Restrictions policy and the App Configuration policy you create from the left to right. Click **Next**.
8. In the **Apps** page, drag the apps you want to deliver from the left side of the page to **Required Apps** or **Optional Apps**. Click **Next**.
9. Optional, configure the settings on the **Media** page, **Actions** page, and **Enrollments** page. Or accept the defaults on each page and click **Next**.
10. On the **Summary** page, review the delivery group settings and click **Save** to create the delivery group.

When publishing the app in the Intune console, select **Force apps to be managed**. Users on unsupervised devices are prompted to allow management of the app. If users accept the prompt, the app is managed on the device. If users decline the prompt, the app is not available on the device.

## Configure Secure Mail

Secure Mail now supports various configurations. You can wrap Secure Mail in an Intune MAM container connecting to an on-premises Exchange Server. You can connect Secure Mail to hosted Exchange or Office 365 accounts. This release does not support certificate-based authentication, however, so use LDAP instead.

### Important:

To use Secure Mail in MDX mode, you must use Citrix Endpoint Management MDM+MAM.

Secure Mail also automatically populates user names. To enable this feature, you must configure the following custom policies first.

1. From your Endpoint Management console, go to **Settings > Server Properties** and then click **Add**.
2. In the list, click **Custom Key** and then in the **Key** field, type `xms.store.idpuser_attrs`.
3. Set the value to **true** and then in **Display name**, type `xms.store.idpuser_attrs`. Click **Save**.
4. Click **Client Properties** and then click **Add**.
5. Select **Custom Key** and then type **SEND\_LDAP\_ATTRIBUTES** in the **Key** field.
6. Type `userPrincipalName=${ user.userprincipalname } ,email=${ user.mail } ,displayname=${ user.displayname } ,sAMAccountName=${ user.samaccountname } ,aadupn=${ user.id_token.upn } ,aadtid=${ user.id_token.tid }` in the **Value** field, enter a description and then click **Save**.

The following steps only apply for iOS devices.

7. Go to **Configure > Device Policies**, click **Add**, and then select the **App Configuration** policy.
8. Enter a policy name and then click **Next**.

In the Identifier list, click **Add new**. In the text box that appears, enter the bundle ID for your Secure Mail app.

9. In the **Dictionary** content box, type the following text.

```
1 <dict>
2
3 <key>XenMobileUserAttributes</key>
4
5 <dict>
6
7 <key>userPrincipalName</key>
8
9 <string>${
10 user.userprincipalname }
11 </string>
12
13 <key>email</key>
14
15 <string>${
16 user.mail }
17 </string>
18
19 <key>displayname</key>
20
21 <string>${
22 user.displayname }
23 </string>
24
25 <key>sAMAccountName</key>
26
27 <string>${
28 user.samaccountname }
29 </string>
30
31 <key>aadupn</key>
32
33 <string>${
34 user.id_token.upn }
35 </string>
36
37 <key>aadtid</key>
```



```
38
39 <string>${
40   user.id_token.tid }
41 </string>
42
43 </dict>
44
45 <key>IntuneMAMUPN</key>
46
47 <string>${
48   user.id_token.upn }
49 </string>
50
51 </dict>
```

10. Clear the **Windows Phone** and **Windows Desktop/Tablet** check boxes and then click **Next**.
11. Select the user groups to which you want the policy deployed and then click **Save**.

## Troubleshooting

### General issues

**Issue:** When opening an app, the following error message appears: App Policy Required.

**Resolution:** Add policies in the Microsoft Graph API.

**Issue:** You have policy conflicts.

**Resolution:** Only a single policy per app is allowed.

**Issue:** Your app can't connect to internal resources.

**Resolution:** Ensure that the correct firewall ports are open, you use the correct tenant ID, and so on.

### Citrix Gateway issues

The following table lists common issues with Citrix Gateway configurations and their solutions. For troubleshooting, enable more logs and check them by doing the following:

1. In the command-line interface, run the following command: `set audit syslogParams - logLevel ALL`
2. Check the logs from the shell using `tail -f /var/log/ns.log`

Issue	Solution
The permissions required to be configured for the Gateway App on Azure are unavailable.	Check if a proper Intune license is available. Try using the <a href="https://manage.windowsazure.com">manage.windowsazure.com</a> portal to see if the permission can be added. Contact Microsoft support if the issue persists.
Citrix Gateway cannot reach <a href="https://login.microsoftonline.com">login.microsoftonline.com</a> and <a href="https://graph.windows.net">graph.windows.net</a> .	From NS Shell, check if you are able to reach the following Microsoft website: <code>curl -v -k https://login.microsoftonline.com</code> . Then, check whether DNS is configured on Citrix Gateway and that the firewall settings are correct (in case DNS requests are firewalled).
An error appears in ns.log after you configure OAuthAction.	Check if Intune licensing is enabled and the Azure Gateway app has the proper permissions set.
Sh OAuthAction command does not show OAuth status as complete.	Check the DNS settings and configured permissions on the Azure Gateway App.
The Android or iOS device does not show the dual authentication prompt.	Check if the Dual Factor Device ID logonSchema is bound to the authentication virtual server.

### OAuth error condition and status

Status	Error Condition
COMPLETE	Success
AADFORGRAPH	Invalid secret, URL not resolved, connection timeout
MDMINFO	* <a href="https://manage.microsoft.com">manage.microsoft.com</a> is down or unreachable
GRAPH	Graph endpoint is down unreachable
CERTFETCH	Cannot talk to "Token Endpoint: <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> because of a DNS error. To validate this configuration, go to shell and type <code>curl https://login.microsoftonline.com</code> . This command must validate.

## Limitations

The following items describe some limitations of using MEM with Citrix Endpoint Management.

- When you deploy apps with Citrix and Intune to support micro VPN: When users provide their user name and password to access digest sites, even though their credentials are valid, an error appears. [CXM-25227]
- After changing **Split tunnel** from **On** to **Off** and waiting for the current gateway session to expire: External traffic passes directly on without going through Citrix Gateway until the user launches an internal site in Full VPN mode. [CXM-34922]
- After changing the Open-in policy from **Managed apps** only to **All apps**, users cannot open documents in unmanaged apps until they close and relaunch Secure Mail. [CXM-34990]
- When split tunneling is **On** in Full VPN mode, and the split DNS changes from local to remote, internal sites fail to load. [CXM-35168]

## Known issues

When the mVPN policy **Enable http/https redirection (with SSO)** is disabled, Secure Mail does not function. [CXM-58886]

## Third-party known issues

On Secure Mail for Android, when a user taps **Create New Event**, the new event creation page does not display. [CXM-23917]

When you deploy Citrix Secure Mail for iOS with Citrix and Intune to support micro VPN: The app policy that obscures the Secure Mail screen when users move the app to the background is not enforced. [CXM-25032]

## Onboarding and resource setup

October 20, 2021

If you are new to Citrix, Citrix Cloud, or to Endpoint Management, this article guides you through onboarding. Learn about workflow and the details you need to get started.

- **Where do I start?**

- If you haven't purchased an Endpoint Management subscription, see [For new Citrix customers](#).
- If you have an Endpoint Management subscription, skip to [When the Manage button is available](#).

- If your Endpoint Management site is provisioned, skip to [Configure authentication](#).
- **Does the configuration order matter?** This article follows a recommended configuration sequence. You can work in a different order. The Endpoint Management console lets you know if prerequisites are missing, through messages such as “Set up after provisioning”.
- **What do I do after onboarding?** After you complete the onboarding and resource configuration described in this article, continue your configuration in the Endpoint Management console. For information about next steps, see [Prepare to enroll devices and deliver resources](#).

Provide us with your feedback for the new console experience in Endpoint Management using the [Citrix Endpoint Management Console Feedback](#) link.

### For new Citrix customers

For Citrix Cloud customers new to Endpoint Management:

If you already purchased an Endpoint Management subscription, skip to [When the Manage button](#) is available.

If you haven't set up a Citrix Cloud account, see [Sign up for Citrix Cloud](#).

If you already set up a Citrix Cloud account, but haven't purchased Endpoint Management, request a service demo.

1. Use your Citrix Cloud administrator credentials to sign in to your Citrix Cloud account. The Citrix Cloud home page appears.

All Citrix Cloud administrator accounts are created as follows:

- Citrix Cloud administrators are Endpoint Management administrators by default.
  - Citrix Cloud administrators created with customer access must have Endpoint Management selected for them to administrate Endpoint Management.
2. On the Citrix Cloud home page, locate the Endpoint Management service tile and click **Request Demo**.
  3. Complete and submit the demo request form. The button on the Endpoint Management services tile changes to **Demo Requested**.

If you click the Endpoint Management services tile before your request is handled, a screen appears advising you to contact your representative or partner. A Citrix sales representative can provide more information and detail about the service.

While waiting for the trial, be sure to prepare for your Endpoint Management deployment by reviewing [System requirements](#). Although Citrix hosts and delivers your Endpoint Management solution, you must handle some communication and port requirements.

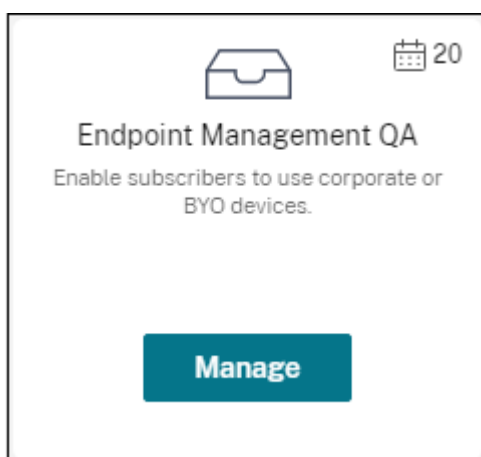
Continue with the next section.

## When the Manage button is available

This video guides you through onboarding:

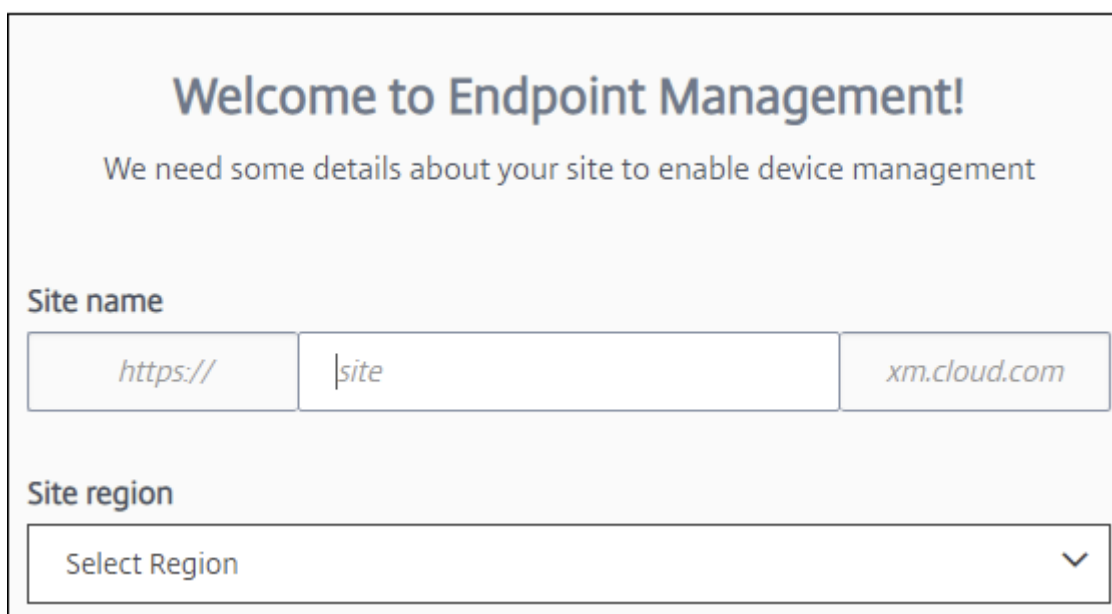
[This is an embedded video. Click the link to watch the video](#)

When your Endpoint Management service is available, the button on the Endpoint Management services tile changes to **Manage**.



To start setup:

1. Sign in to your Citrix Cloud account using your Citrix Cloud administrator credentials.
2. Click **Manage** in the Endpoint Management tile to access the Endpoint Management console.
3. Type your site name and select a region. Then select **Save & Continue**.

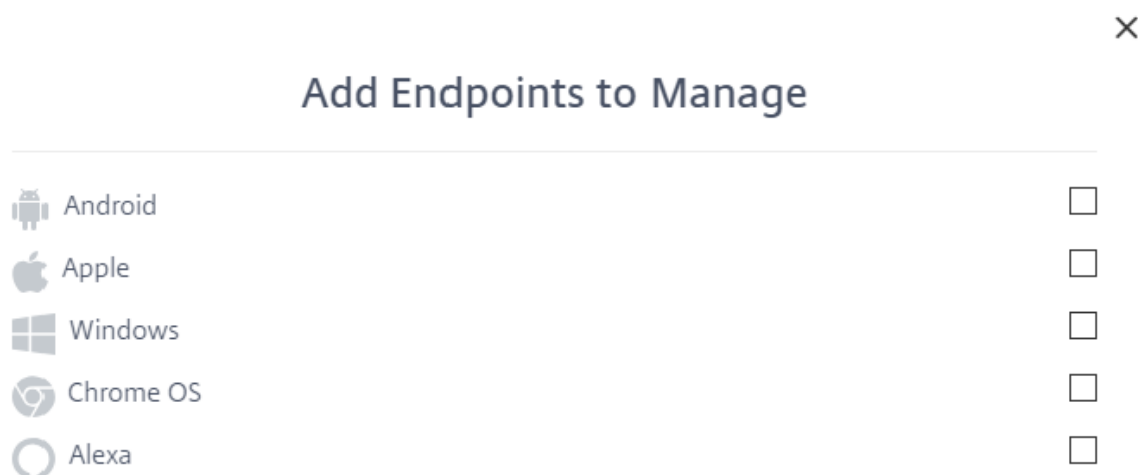
A screenshot of the 'Welcome to Endpoint Management!' setup screen. The title is 'Welcome to Endpoint Management!' and the subtitle is 'We need some details about your site to enable device management'. Under the heading 'Site name', there are three input fields: the first contains 'https://', the second contains '|site', and the third contains 'xm.cloud.com'. Under the heading 'Site region', there is a dropdown menu with the text 'Select Region' and a downward-pointing chevron icon.

**Note:**

To request the IPs to allow, contact the Citrix Support representative.

The Endpoint Management console then opens with a message saying that we are provisioning your suite and that some Endpoint Management functions are locked during provisioning.

1. In the **Welcome** screen, click **Start setup**.
2. Select the endpoints you want to manage and click **Save**. You can add or clear endpoints at any time to show or hide them in the console. Showing and hiding endpoints doesn't affect your configuration.



We send you an email when provisioning completes.

### Resource Center



Click the **Resource Center** icon to watch how-to videos without leaving the console.

### During provisioning

While we provision Endpoint Management, you can get started with configuration.

### Configure resource locations

You need resource locations before you can configure Lightweight Directory Access Protocol (LDAP) connections for Endpoint Management. Resource locations contain the resources required to deliver cloud services to your subscribers. You need one resource location per domain. For help, see the Citrix Cloud article, [Resource Locations](#).

While waiting for the trial, be sure to prepare for your Endpoint Management deployment by reviewing [System requirements](#). Although Citrix hosts and delivers your Endpoint Management solution, some

communication and port requirements are required. That setup connects the Endpoint Management infrastructure to corporate services, such as Active Directory. The information that you must provide is included in the [Onboarding Handbook](#) under “Endpoint Management Trial Sales Engineer engagement.”

After you are authorized to access the trial, the button for **Endpoint Management** changes to **Manage**. Click **Manage** to open the Citrix Endpoint Management console.

## Configure authentication

After your site is provisioned, you can continue with configuration. We recommend that you set up a cloud-hosted identity provider (IdP) or Lightweight Directory Access Protocol (LDAP) to import groups, user accounts, and related properties.

### To configure IdP

Endpoint Management supports authentication with identity providers, such as Azure Active Directory, Okta, and on-premises Citrix Gateway.

To configure an IdP in Citrix Cloud and set it up for Endpoint Management:

- [Authentication with Azure Active Directory through Citrix Cloud](#)
- [Authentication with Okta through Citrix Cloud](#)
- [Authentication with an on-premises Citrix Gateway through Citrix Cloud \(Preview\)](#)

You can configure Azure AD and Okta identity providers (IdPs) through Citrix Cloud to manage devices that enroll in MDM through Citrix Secure Hub without a Cloud Connector. Endpoint Management requires a Cloud Connector for LDAP, PKI Server, internal DNS queries, Citrix Virtual Apps, Citrix Gateway, Citrix Workspace, and Microsoft Endpoint Manager. For information, see [Identity provider authentication without a Cloud Connector \(Preview\)](#).

### To configure LDAP

You can configure a connection in Endpoint Management to one or more LDAP-compliant directories for domain-based authentication. Endpoint Management supports groups that are nested in LDAP. Nested groups synchronize daily at 12 AM local time.

As a part of configuring LDAP, you must install at least one Cloud Connector.

For a quick overview, watch this video.

[This is an embedded video. Click the link to watch the video](#)

To set up LDAP:

1. On the **Settings** page, scroll to the **LDAP** tile and then click **Set Up**.

2. Follow the on-screen guidance to download and install a Cloud Connector. Cloud Connectors are required for enabling communication between Citrix Cloud and your resources. For help, see [Citrix Cloud Connector](#).

If you have the LDAP configuration and you add Azure AD or Okta as an identity provider, Endpoint Management synchronizes IdP-specific information for your Active Directory groups in the Endpoint Management database. This configuration doesn't affect your existing delivery groups and user enrollments. However, you can't add LDAP settings in Endpoint Management afterwards. For more information, see [Identity provider authentication without a Cloud Connector \(Preview\)](#).

If you change the **Domain alias** or **User search by** settings after enrollment, users must re-enroll. For more information about LDAP configuration, see [Domain or domain plus security token authentication](#).

After setting up LDAP, you can continue with the authentication configuration or set up a specific platform.

## Configure Citrix Gateway

When integrated with Endpoint Management, Citrix Gateway provides remote device access to your internal network and resources.

Endpoint Management requires Citrix Gateway for the following scenarios:

- You require a micro VPN for access to internal network resources for line-of-business apps. Those apps are wrapped with Citrix MDX technology. The micro VPN needs Citrix Gateway to connect to internal back-end infrastructures.
- You plan to use Endpoint Management to manage apps (MAM or MDM+MAM). Citrix Gateway isn't required to manage devices only (MDM).
- You plan to integrate Endpoint Management with Microsoft Endpoint Manager. (Requires an on-premises Citrix Gateway.)

Citrix offers both cloud-based and on-premises Citrix Gateway solutions. However, only customers with the Citrix Gateway service entitlement can configure the cloud-based service.

For a quick overview, watch this video.

[This is an embedded video. Click the link to watch the video](#)

### **Important:**

After you configure a Citrix Gateway solution, switching to another solution requires that you reenroll devices. If you already use on-premises Citrix Gateway and want to switch to Citrix Gateway service, contact your Citrix Sales representative. For prerequisites, see [To use Citrix Gateway service](#) in this article.



The following table summarizes the features supported by the cloud-based and on-premises Citrix Gateway solutions.

Supported features	Citrix Gateway service	Citrix Gateway on-premises
Secure Mail (STA)*	yes	yes
Tunneled - Web SSO (web single sign-on)	yes	yes
Full VPN (not available for Citrix Mobile productivity apps for iOS)	no	yes
Per-app VPN	no	yes
Mobile single sign-on (access control)	yes	no
High Availability	yes	yes**
Multi-POP deployment	yes	yes***
Proxy support	yes	yes
Split-tunneling	no	yes
Split DNS	no	yes

\* Citrix Cloud Secure Ticket Authority (STA) service configuration

\*\* On-premises configuration

\*\*\* Global Server Load Balancing configuration

### **Citrix Gateway service use cases**

Use the cloud-based Citrix Gateway service with Endpoint Management when:

- You want to use the unified authentication experience provided by Citrix Cloud. Citrix Gateway service uses the Citrix identity provider to manage the identity information for all users in your Citrix Cloud account.
- You plan to use Citrix mobile productivity apps, such as Citrix Secure Mail or Secure Web. Citrix Gateway provides an on-demand application VPN connection that allows mobile devices to access corporate network sites or resources.

This variation of a clientless VPN is also known as Tunneled – Web single sign-on (SSO). Connections such as web traffic that tunnel to the internal network use Tunneled - Web SSO. We recommend Tunneled - Web SSO for connections that require single sign-on.

### How Citrix Gateway service works

MDM and MAM control traffic go directly to Citrix Endpoint Management, without going through Citrix Gateway service. All traffic sent to Citrix Gateway gets directed to the on-premises Gateway Connector.

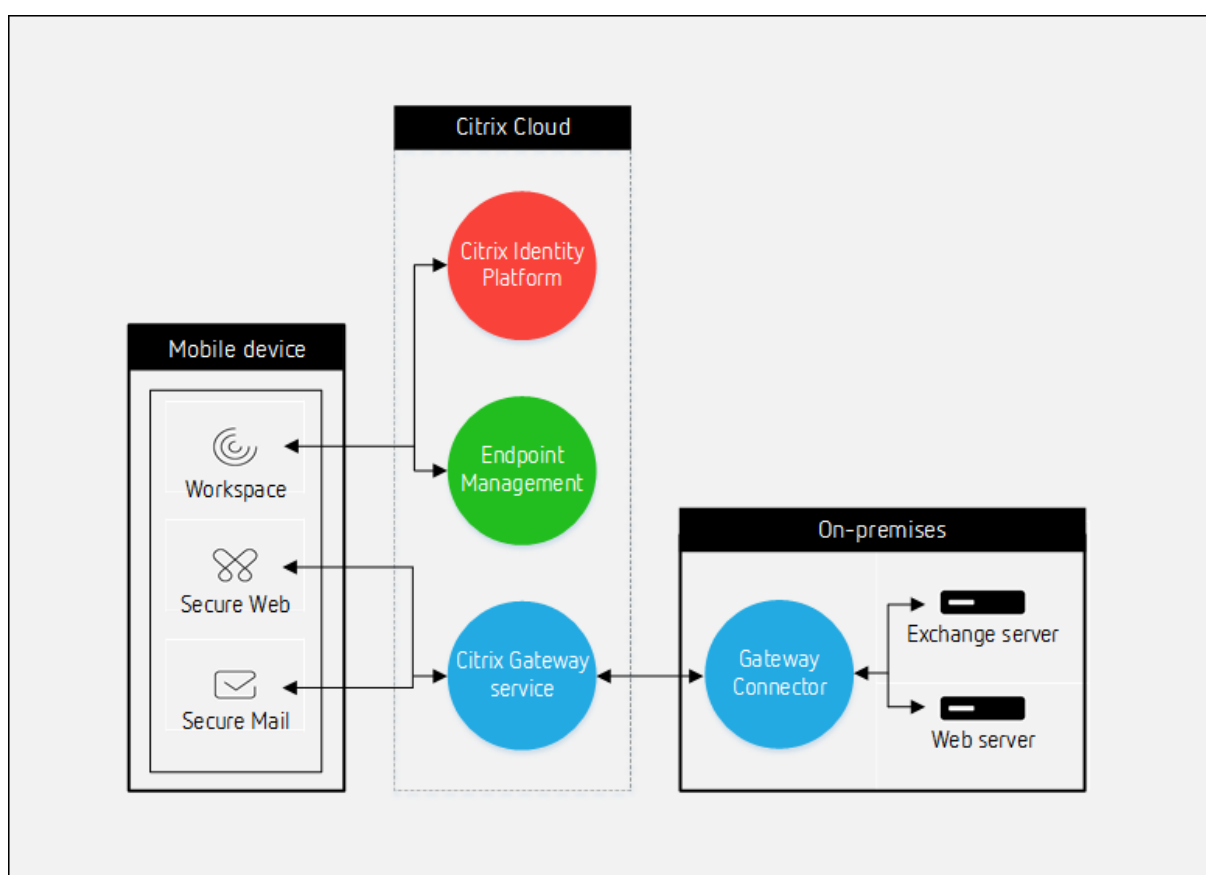
Citrix Gateway service isn't used during device enrollment in Endpoint Management. For Citrix mobile productivity apps:

- Secure Mail uses the Citrix Cloud Secure Ticket Authority (STA) service.

**Note:**

Citrix Gateway service uses the primary resource location.

- Citrix Gateway provides an on-demand application VPN connection.



Citrix Gateway service isn't used during device enrollment in Endpoint Management. After enrollment, MDM control traffic goes directly to Citrix Endpoint Management, without going through Citrix Gateway service. MAM control traffic goes through the Citrix Gateway service. All traffic sent to Citrix Gateway gets directed to the on-premises Gateway Connector.

For a more detailed diagram of the traffic flow, see [Support for Citrix Endpoint Management](#). For Gateway Connector port requirements, see [Gateway Connector](#).

The following authentication types are supported for Citrix Gateway service integration with Endpoint Management:

- Basic, Digest, NTLM
- Kerberos Constrained Delegation (KCD) single sign-on
- Form-based single sign-on
- SAML single sign-on

### Prerequisites

- Citrix Workspace experience enabled
  - On Android devices, users enroll through the Citrix Workspace app only.
  - For other platforms, user enrollment starts with the Workspace app. When Secure Hub detects the Workspace entitlement, Secure Hub completes enrollment. Secure Hub then opens Citrix Workspace, where users can access their apps and other resources. For more information about using Citrix Workspace with Android, see [Android for Workspace](#).
- Citrix Gateway service subscription
  - If you already use on-premises Citrix Gateway and want to switch to Citrix Gateway service, contact your Citrix Sales representative. Switching from on-premises Citrix Gateway to the Citrix Gateway service requires that you reenroll devices.
  - New Endpoint Management customers: Select the Citrix Gateway service during Endpoint Management onboarding.
- Gateway Connector installed on-premises in a resource location
  - Endpoint Management uses the resource location for Gateway Connector only for STA tickets for Secure Mail. Citrix Gateway sends STA traffic to the Gateway Connector in the resource location.
  - You can install one or more Gateway Connectors in any resource location. Endpoint Management doesn't support Gateway Connectors installed in multiple resource locations.
  - You can install Gateway Connector in the same or a different resource location than Active Directory. The only role of Active Directory is to use Citrix Cloud authentication to authenticate users to Citrix Gateway service. Citrix Gateway service creates session connections to the Gateway Connector for authenticated users. You can have multiple Active Directories.
  - If the connector isn't available during Citrix Endpoint Management onboarding, you can install it after onboarding.

For more information, see [Citrix Gateway Connector](#) and [System requirements](#).

Citrix recommends that new Endpoint Management customers configure Citrix Gateway service rather than on-premises Citrix Gateway.

### Set up Citrix Gateway service

1. On the **Settings** page, scroll to the **Citrix Gateway** tile and then click **Set Up**.
2. Select **Citrix Gateway service (cloud)** as the type. Only customers with the Citrix Gateway service entitlement can view this setting.
3. Follow the on-screen guidance. For information, see [Configure on-premises Citrix Gateway for use with Endpoint Management](#).

### On-premises Citrix Gateway use cases

Use one or more on-premises Citrix Gateway appliances with Endpoint Management when:

- You require per-app VPN capabilities.
- You require full tunneling, split tunneling, reverse split tunneling, or split DNS. We recommend full VPN tunnel for connections that use client certificates or end-to-end SSL to a resource in the internal network.
- You use Citrix Endpoint Management integration with Microsoft Endpoint Manager.

The usage of on-premises Citrix Gateway involves significant configuration and maintenance. After you configure LDAP and Citrix Gateway in the Endpoint Management console, you export a script from that console. You then run the script on the Citrix Gateway.

1. On the **Settings** page, scroll to the **Citrix Gateway** tile and then click **Start setup**.
2. Select **Citrix Gateway (on-premises)** as the type.
3. Follow the on-screen guidance. For information, see [Configure on-premises Citrix Gateway for use with Endpoint Management](#).

### Configure notification server

To send notifications, you must configure a gateway and a notification server. A notification server ensures connectivity and the possibility of communication between end users and the administrator. To set up a notification server in Endpoint Management, see [Notifications](#).

### Configure an Apple Push Notification service (APNs) certificate for Apple devices

Endpoint Management requires an Apple Push Notification service (APNs) certificate from Apple to enroll and manage Apple devices. Endpoint Management also requires an APNs certificate if you plan to use push notifications for Secure Mail for Apple. For information about Endpoint Management and APNs, see [Push Notifications for Secure Mail for iOS](#).

To obtain a certificate from Apple requires an Apple ID and developer account. For details, see the [Apple Developer Program](#) website.

For a quick overview, watch this video.

[This is an embedded video. Click the link to watch the video](#)

To configure APNs with a Citrix Certificate Signing Request:

1. On the **Settings** page, expand the **Apple** tile.
2. On the **APNs Certificate** tile, click **Set Up** and then follow the on-screen guidance.

For more information, see [Certificates and authentication](#).

## Configure Android Enterprise

Endpoint Management is fully configured after you create delivery groups and assign users to the delivery groups through the Cloud Library. From this point on, Endpoint Management administration takes place within Citrix Cloud. The combined interface simplifies switching between Citrix Cloud and Endpoint Management.

You can set up Android Enterprise for Endpoint Management with either Google Play or Google Workspace.

1. **If your organization does not use Google Workspace:** You can use managed Google Play to register Citrix as your EMM provider. If you use managed Google Play, you provision managed Google Play Accounts for devices and end users. Managed Google Play Accounts provide access to managed Google Play, allowing users to install and use work apps you make available. If your organization uses a third-party identity service, you can link managed Google Play Accounts with your existing identity accounts.

Because this type of enterprise isn't tied to a domain, you can create more than one enterprise for a single organization. For example, each department or region within an organization can enroll as a different enterprise. That setup enables you to use different enterprises to manage separate sets of devices and apps.

2. **If your organization already uses Google Workspace to provide users access to Google apps:** You can use Google Workspace to register Citrix as your EMM. If your organization uses Google Workspace, it has an existing enterprise ID and existing Google Accounts for users. To use Endpoint Management with Google Workspace, you sync with your LDAP directory and retrieve Google Account information from Google using the Google Directory API.

This type of enterprise is tied to an existing domain. Therefore, each domain can only create one enterprise. To enroll a device in Endpoint Management, each user must manually sign in with their existing Google Account. The account gives users access to managed Google Play and to other Google services through your Google Workspace plan.

For a quick overview, watch this video.

[This is an embedded video. Click the link to watch the video](#)

To get started:

1. On the **Settings** page, expand the **Android** tile.
2. On the **Android Enterprise** tile, click **Set Up**.
3. Choose **Google Play** or **G Suite**, according to how you provide users access to Google applications.  
If you previously configured the Android Enterprise platform with Google Play, the UI takes you to the Google Play store to reenroll. Click **Re-enroll**, return to the CEM console, and refresh the page.
4. Follow the on-screen guidance.

See:

- [Create an Android Enterprise Account](#)

## Configure Firebase Cloud Messaging

Citrix recommends that you use Firebase Cloud Messaging (FCM) to control how and when Android devices connect to Endpoint Management. Endpoint Management sends connection notifications to Android devices that are enabled for FCM. Any security action or deploy command triggers a push notification to prompt the user to reconnect to the Endpoint Management server. See [Firebase Cloud Messaging](#).

## Integrate with Microsoft Endpoint Manager

Endpoint Management integration with Microsoft Endpoint Manager adds the value of the Endpoint Management micro VPN to Microsoft Intune aware apps, such as Microsoft Edge browser.

Endpoint Management integration with MEM also allows enterprises to wrap their own line of business apps with Intune and Citrix. The app wrapping provides micro VPN capabilities inside an Intune mobile app management (MAM) container. Endpoint Management micro VPN enables your apps to access on-premises resources. You can manage and deliver Office 365 apps, line of business apps, and Citrix Secure Mail in one container. A single container provides ultimate security and productivity.

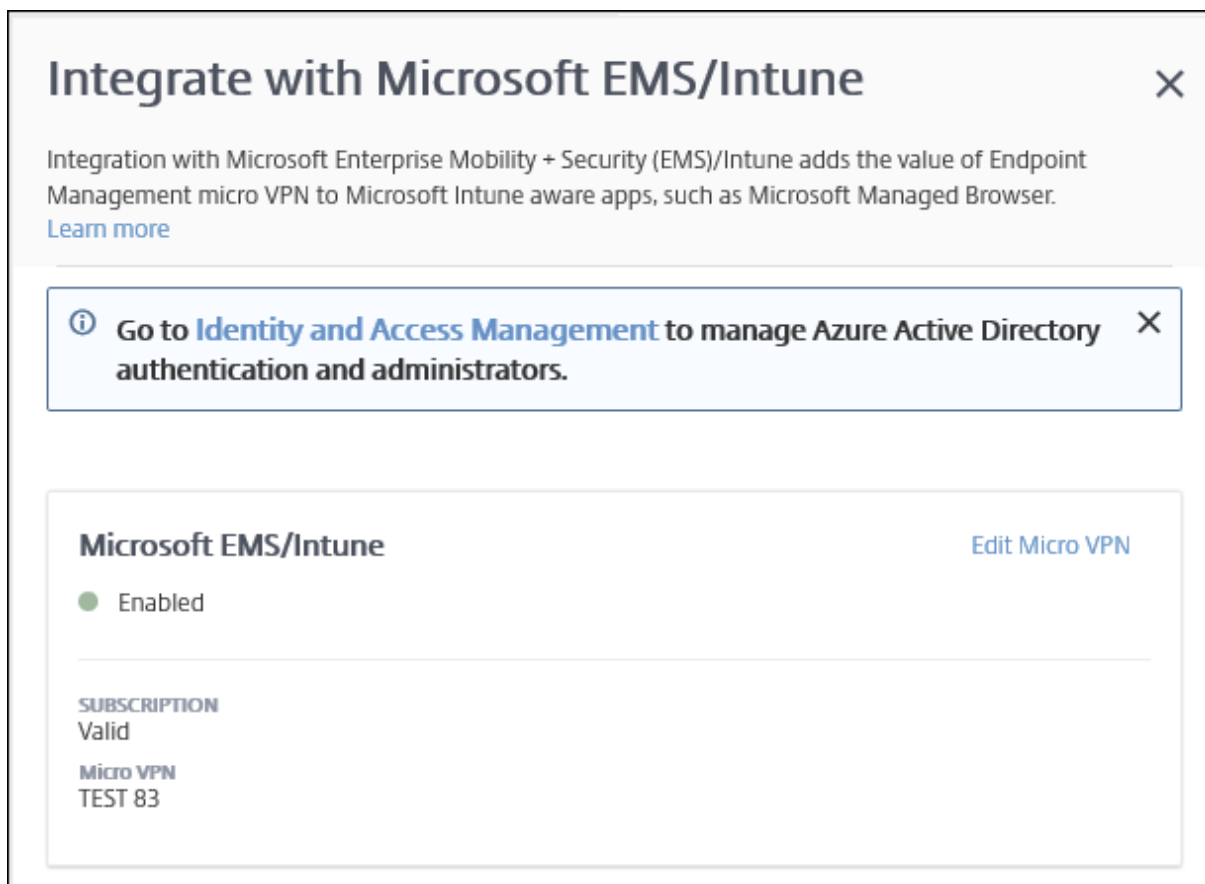
- Citrix Cloud administrators are Endpoint Management administrators by default.
- Citrix Cloud administrators created with customer access must have Endpoint Management selected for them to administrate Endpoint Management.

In the Endpoint Management console, you can change only the role and membership of a user. To change a role at any time, access the Endpoint Management console from the Citrix Cloud dashboard. Go to the **Manage** tab and click **Users**. Select a specific user and click **Edit** to change the role. For more information, see [Configure roles with RBAC](#).

To integrate with MEM, see [Citrix Endpoint Management integration with Microsoft Endpoint Manager](#).

After you complete configuration in Citrix Cloud, return to the Endpoint Management console as follows: Go to the Citrix Cloud **Home** page and then click **Manage** on the **Endpoint Management** tile. Then you can verify if you signed in to Endpoint Management with your Azure Active Directory account.

1. On the **Settings** page, scroll to the **Integrate with Microsoft EMS/Intune** tile.
2. Click **See more**. The UI indicates if you successfully enabled the connection.

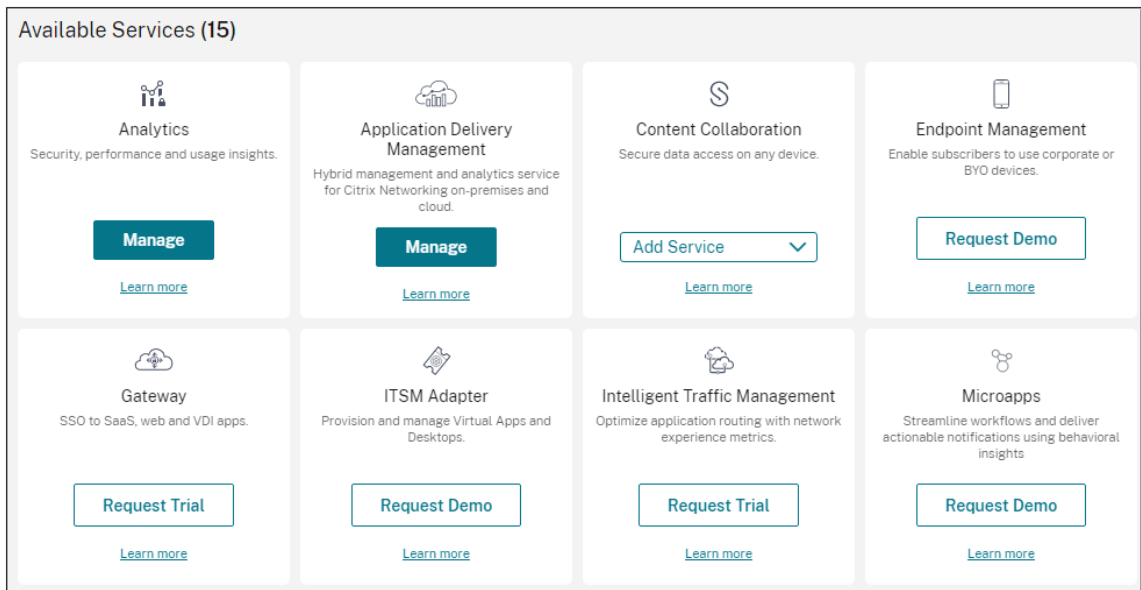


In the Citrix Cloud console, you can also change user names or passwords, and delete or edit local users. See [Identity and access management](#).

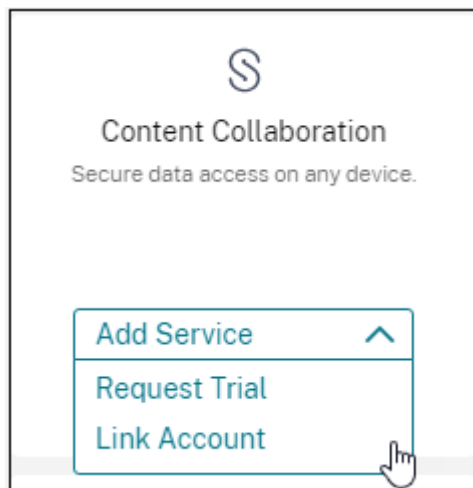
### Link an existing Citrix Content Collaboration account to Citrix Cloud

If you had a Citrix Content Collaboration account before you signed up with Citrix Cloud, you must link that account to Citrix Cloud. To link your account, your email address must be an administrator of the Citrix Content Collaboration account. When you're ready to proceed, go to <https://onboarding.cloud.com>.

1. After you log in, a screen similar to the following appears.



2. In the **Citrix Content Collaboration** tile, choose **Link Account**.



3. After we confirm your Citrix Content Collaboration account, the following page appears:



**Add Content Collaboration Account**

Request Trial Link Account

**GEO Location**  
Select the geographical location for the account.

USA  EU

I understand that I cannot change the region after set up.

**Select a subdomain**  
Your subdomain is your unique URL for your Content Collaboration account. You can change this later.

https://  sharefile.com

Cancel Request Trial

4. Click the **Link Account** tab to complete the process. You can immediately manage your Citrix Content Collaboration account from Citrix Cloud.

### Verify your setup

To ensure that everything is set up correctly, you can use the Endpoint Management Analyzer. From the Troubleshooting and Support page, click **Endpoint Management Analyzer** to access this tool. For information on using the Endpoint Management Analyzer, see [Endpoint Management Analyzer](#).

## Scale and size considerations for Cloud Connectors

June 5, 2020

When evaluating the Citrix Endpoint Management service for sizing and scalability, research and test the configuration of the Cloud Connectors for your specific requirements. Cloud Connector is under load only during device enrollment. Undersizing the machines can impact system performance negatively.

Citrix requires two Cloud Connectors per resource location. Install Cloud Connector on a dedicated

server that doesn't share responsibilities with any other components or products. In our testing, Cloud Connectors were deployed in HA sets (**they are not load-balanced**).

### Test configuration

- Two dedicated Windows Server 2019, 2 vCPU, 4 GB memory
- Android and iOS device enrollments into MDM+MAM, split evenly over an 8-hour period
- Endpoint Management configured to enroll 125 devices per hour per 1,000 devices
  - 1,000 devices (125 device enrollments per hour)
  - 5,000 devices (625 device enrollments per hour)
  - 10,000 devices (1250 device enrollments per hour)
  - 20,000 devices (2500 device enrollments per hour)

### Test results

Cloud Connector	1,000 devices	5,000 devices	10,000 devices	20,000 devices
CPU average	2%	2%	4%	4%
CPU maximum	8%	8%	10%	11%
Memory average	73%	73%	75%	75%
Memory maximum	76%	76%	76%	79%

## Prepare to enroll devices and deliver resources

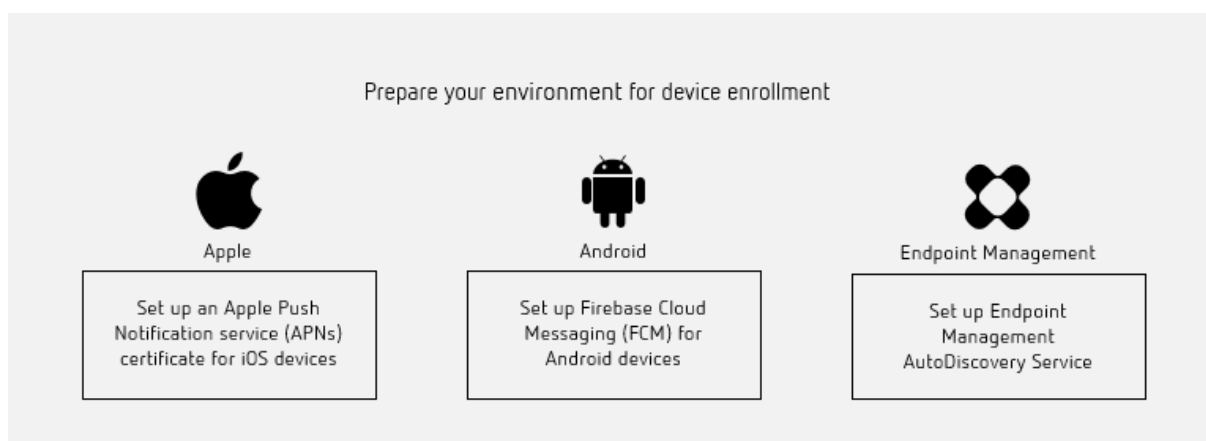
October 26, 2021

#### Important:

Before proceeding, be sure to complete all the tasks described in [Onboarding and resource setup](#).

Keep your users informed about upcoming changes. See [Welcome to your Citrix Endpoint Management User Adoption Kit](#).

Endpoint Management supports various enrollment options. This article covers the basic setup required to enable all supported devices to enroll. The following diagram summarizes the basic setup.



For a list of supported devices, see [Supported device operating systems](#).

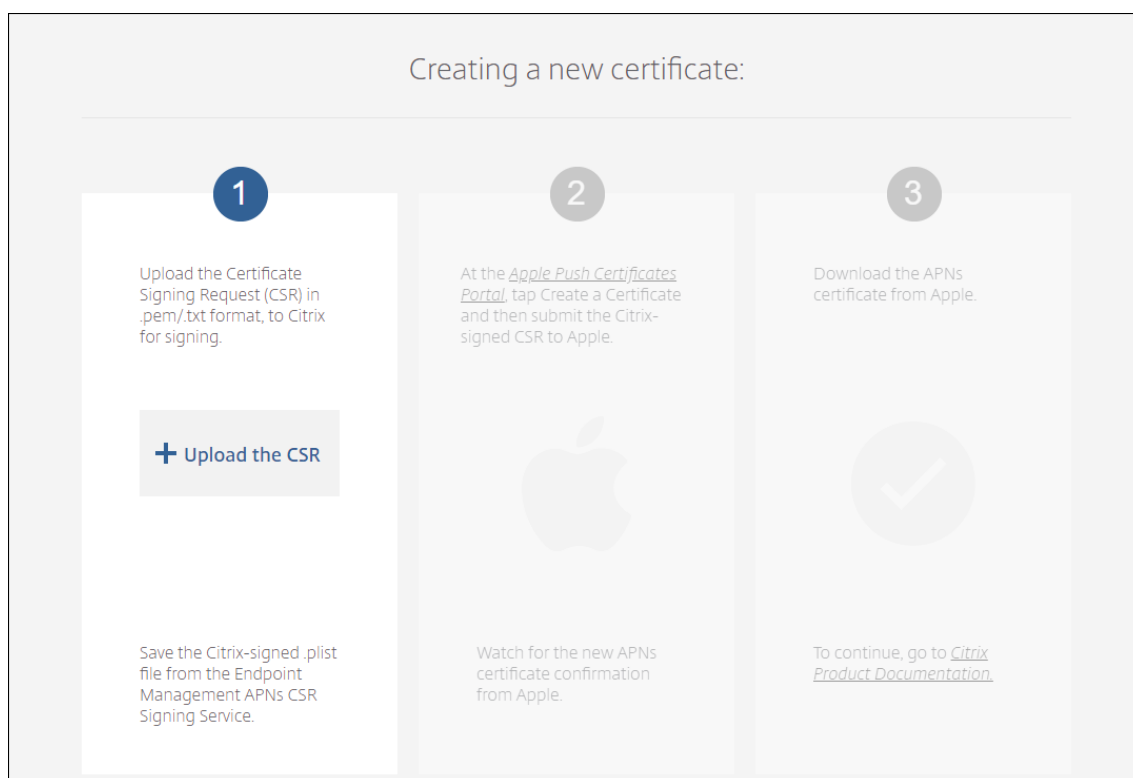
### Set up an Apple Push Notification service (APNs) certificate for iOS devices

**Important:**

Apple support for the APNs legacy binary protocol ends as of March 31, 2021. Apple recommends that you use the HTTP/2-based APNs provider API instead. As of release 20.1.0, Citrix Endpoint Management supports the HTTP/2-based API. For more information, see the news update, “Apple Push Notification Service Update” in <https://developer.apple.com/>. For help with checking connectivity to APNs, see [Connectivity checks](#).

Endpoint Management requires an Apple Push Notification service (APNs) certificate from Apple to enroll and manage iOS devices. Endpoint Management also requires an APNs certificate for Secure Mail for iOS push notifications.

- To obtain a certificate from Apple requires an Apple ID and developer account. For details, see the [Apple Developer Program](#) website.
- To obtain an APNs certificate and import it into Endpoint Management, see [APNs certificates](#).



- For more information about Endpoint Management and APNs, see [Push Notifications for Secure Mail for iOS](#).

### Set up Firebase Cloud Messaging (FCM) for Android devices

Firebase Cloud Messaging (FCM) controls how and when Android devices connect to the Endpoint Management service. Any security action or deployment command triggers a push notification. The notification prompts users to reconnect to Endpoint Management.

- FCM setup requires that you configure your Google account. To create Google Play credentials, see [Manage your developer account information](#). You also use Google Play to add, buy, and approve apps for deployment to the Android Enterprise workspace on a device. You can use Google Play to deploy your private Android apps, public apps, and third-party apps.
- To set up FCM, see [Firebase Cloud Messaging](#).

### Set up Endpoint Management AutoDiscovery service

The AutoDiscovery service simplifies the enrollment process for users through email-based URL discovery. The AutoDiscovery service also provides features such as enrollment verification, certificate pinning, and other benefits for Citrix Workspace customers. The service, hosted in Citrix Cloud, is an important part of many Endpoint Management deployments.

With the AutoDiscovery service, users:

- Can use their corporate network credentials to enroll their devices.
- Don't need to enter details about the Endpoint Management server address.
- Enter their user name in user principal name (UPN) format. For example, `user@mycompany.com`.

We recommend that you use the AutoDiscovery service for high-security environments. The AutoDiscovery service supports public key certificate pinning, which prevents man-in-the-middle attacks. Certificate pinning ensures that the certificate signed by your enterprise is used when Citrix clients communicate with Endpoint Management. To configure certificate pinning for your Endpoint Management sites, contact Citrix Support. For information about certificate pinning, see [Certificate pinning](#).

To access the AutoDiscovery service, navigate to <https://adsui.cloud.com> (commercial) or <https://adsui.cem.cloud.us> (government).

### Prerequisites

- The new AutoDiscovery service in Citrix Cloud requires the latest version of Secure Hub:
  - For iOS, Secure Hub version 21.6.0 or later
  - For Android, Secure Hub version 21.8.5 or laterDevices running on earlier versions of Secure Hub might experience interruptions in service.

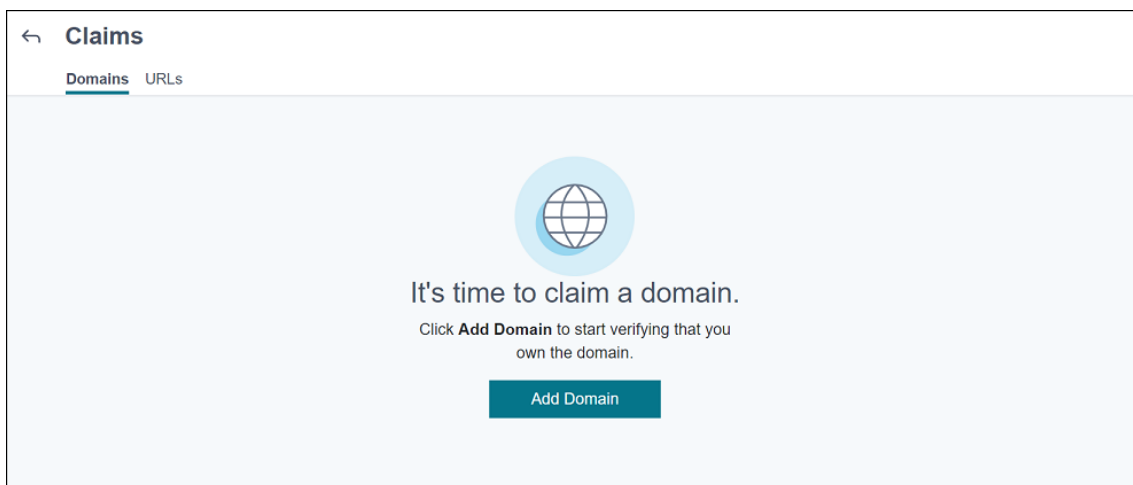
- To access the new AutoDiscovery service, you must have a Citrix Cloud administrator account with full access. The AutoDiscovery service doesn't support administrator accounts with custom access. If you don't have an account, see [Sign up for Citrix Cloud](#).

Citrix migrated all existing AutoDiscovery records to Citrix Cloud without a disruption in service. The migrated records don't automatically appear in the new console. You must reclaim domains in the new AutoDiscovery service to prove ownership. For more information, see [CTX312339](#).

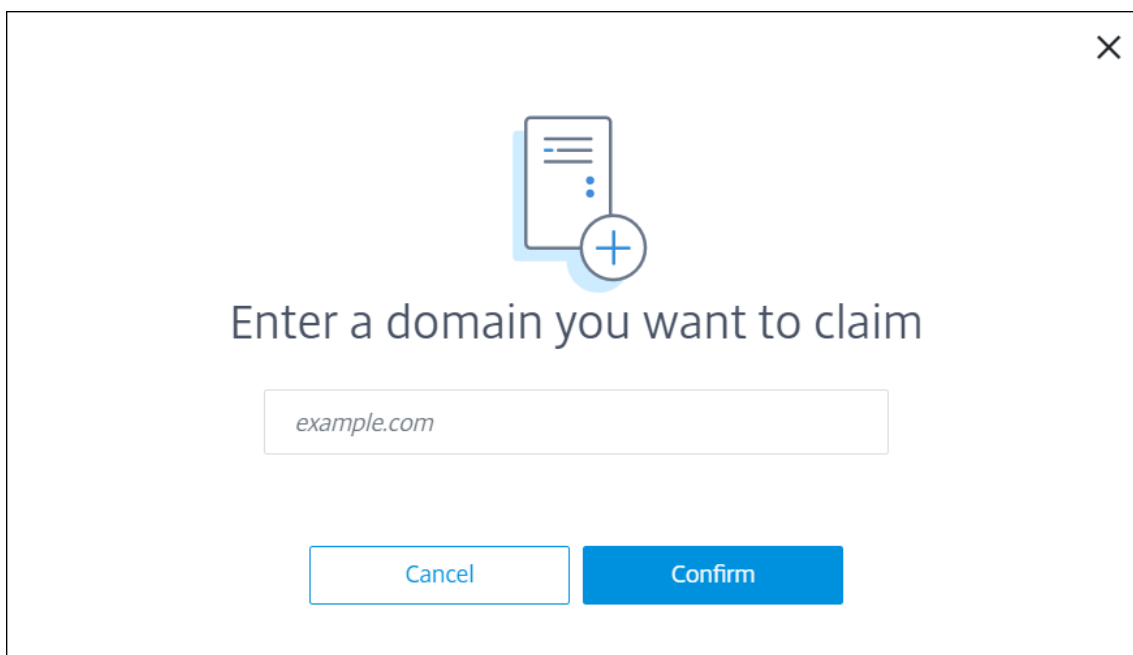
- Before starting using the AutoDiscovery service for your Endpoint Management deployments, verify and claim your domain. You can claim up to 10 domains. The claim associates the verified domain with the AutoDiscovery service. To claim more than 10 domains, open an SRE ticket or contact Citrix Technical Support.
- Use the MAM Port setting instead of Citrix Gateway FQDN to direct MAM traffic to your data center. If you enter a fully qualified domain name along with the port of your Citrix Gateway, the client device uses the configuration from the **MAM Port** setting.
- If an ad blocker prevents the site from opening, ensure that you disable the ad blocker for the entire website.

## Claim a domain

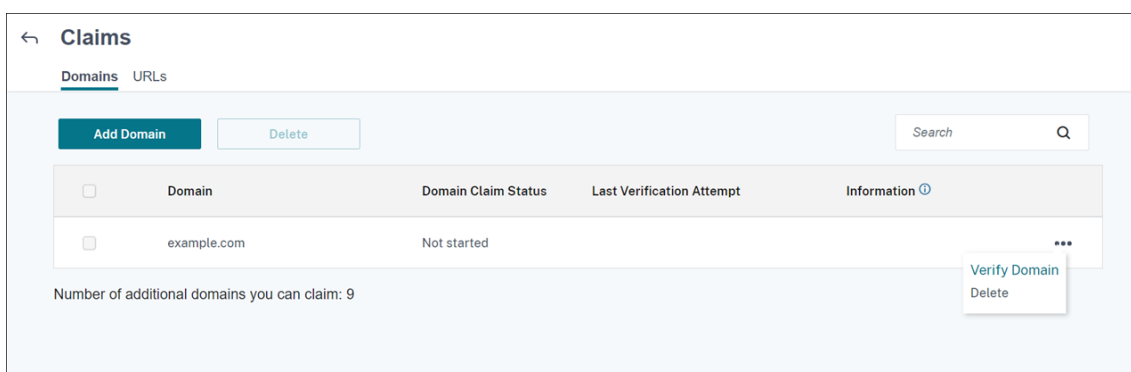
1. On the **Claims > Domains** tab, click **Add Domain**.



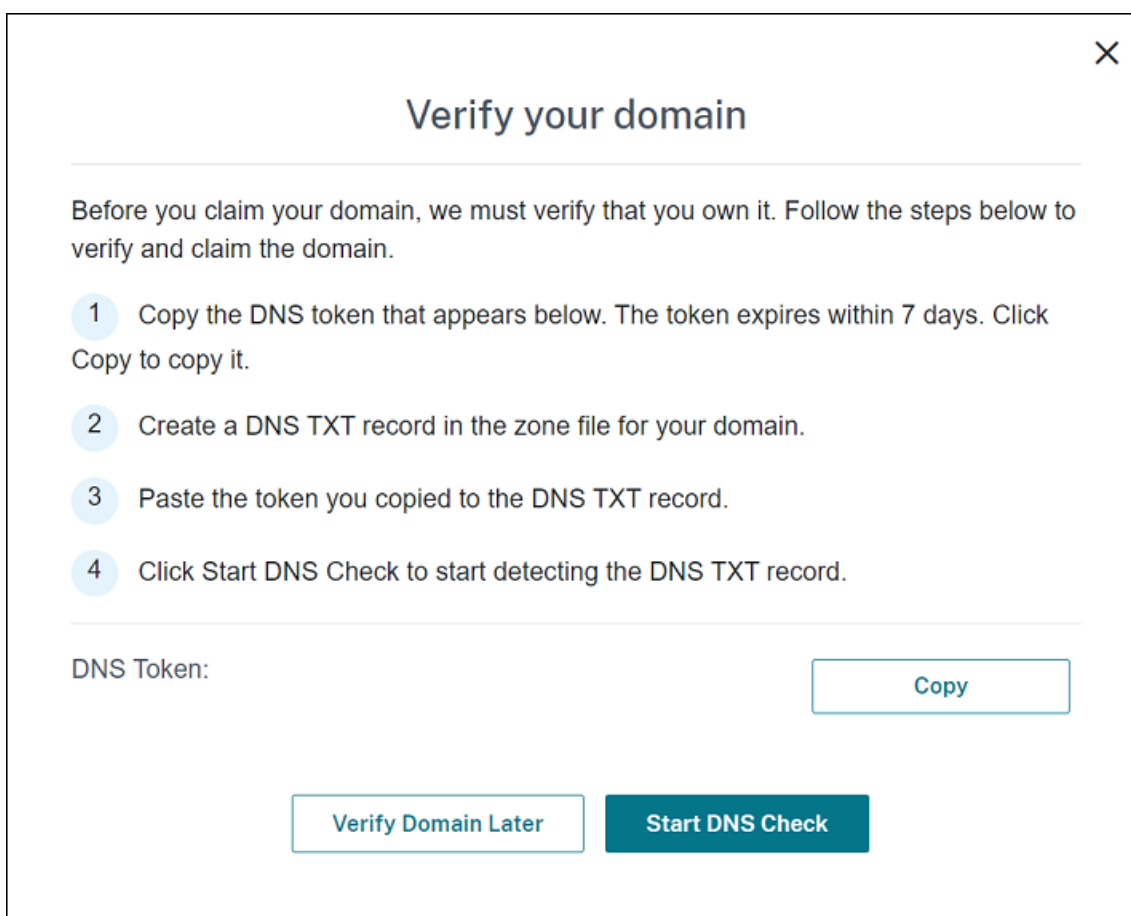
2. In the dialog box that appears, enter the domain name of your Endpoint Management environment and then click **Confirm**. Your domain appears in **Claims > Domains**.



3. On the domain you added, click the ellipsis menu and select **Verify Domain** to start the verification process. The **Verify your domain** page appears.



4. On the **Verify your domain** page, follow the instructions to verify that you own the domain.



- a) Click **Copy** to copy the DNS token to the clipboard.
- b) Create a DNS TXT record in the zone file for your domain. To do so, go to your domain hosting provider portal and add the DNS token you copied.

The following screenshot shows a domain hosting provider portal. Your portal may look different.

- c) In Citrix Cloud, on the **Verify your domain** page, click **Start DNS Check** to start detecting your DNS TXT record. If you want to verify the domain later, click **Verify Domain Later**.

The verification process generally takes about an hour. However, it can take up to two days to return a response. It is OK for you to log out and log in again during the status check.

After the configuration completes, the status of your domain changes from **Pending** to **Verified**.

5. After you claim your domain, provide information about the AutoDiscovery service. Click the ellipsis menu on the domain you added and then click **Add Endpoint Management Info**. The **AutoDiscovery Service Information** page appears.
6. Enter the following information and then click **Save**.
  - **Endpoint Management Server FQDN:** Enter the fully qualified domain name of the Endpoint Management server. For example: `example.xm.cloud.com`. This setting is used for MDM and MAM control traffic.
  - **Citrix Gateway FQDN:** Enter the fully qualified domain name of Citrix Gateway, in the form FQDN or FQDN:port. For example: `example.com`. This setting is used to direct MAM traffic to your data center. For MDM-only deployments, leave this field blank.

**Note:**

Citrix recommends that you use the **MAM Port** setting instead of **Citrix Gateway**



**FQDN** to control MAM traffic. If you enter a fully qualified domain name along with the port of your Citrix Gateway, the client device uses the configuration from the **MAM Port** setting.

- **Instance Name:** Enter the instance name of the Endpoint Management server you configured above. If you are unsure about your instance name, leave the default value, **zdm**.
- **MDM Port:** Enter the port used for MDM control traffic and MDM enrollment. For cloud-based services, the default is 443.
- **MAM Port:** Enter the port used for MAM control traffic, MAM enrollment, iOS enrollment, and app enumeration. For cloud-based services, the default is 8443.

### Request AutoDiscovery for Windows devices

If you plan to enroll Windows devices, do the following:

1. Contact Citrix Support and create a support request to enable Windows AutoDiscovery.
2. Obtain a publicly signed, non-wildcard SSL certificate for `enterpriseenrollment.mycompany.com`. The `mycompany.com` portion is the domain that contains the accounts that users use to enroll. Attach the SSL certificate in .pfx format and its password to the support request created in the previous step.

To use more than one domain to enroll Windows devices, you can also use a multi-domain certificate with the following structure:

- A SubjectDN with a CN that specifies the primary domain it serves (for example, `enterpriseenrollment.mycompany1.com`).
  - The appropriate SANs for the remaining domains (for example, `enterpriseenrollment.mycompany2.com`, `enterpriseenrollment.mycompany3.com`, and so on).
3. Create a canonical name (CNAME) record in your DNS and map the address of your SSL certificate (`enterpriseenrollment.mycompany.com`) to `autodisc.xm.cloud.com`.

When a Windows device user enrolls using a UPN, the Citrix enrollment server:

- Provides the details of your Endpoint Management server.
- Instructs the device to request a valid certificate from Endpoint Management.

At this point, you can enroll all supported devices. Proceed to the next section to prepare to deliver resources to devices.

### Integrate with Azure AD Conditional Access

You can configure Endpoint Management to apply Azure AD Conditional Access support to Office 365 applications. This feature lets you deploy the Zero Trust methodology to device users when deploying

Office 365 applications. You can use device state, risk score, location, and device protections to apply automated actions and define access to the Office 365 applications on managed Android Enterprise and iOS devices.

To enforce Azure AD device compliance, you must configure Conditional Access policies for individual Office 365 applications. You can restrict user access to specific Office 365 applications on non-managed and non-compliant devices and permit access to individual applications only on managed and compliant devices.

### Prerequisites

- For this integration, you must have a valid Azure AD premium subscription, including Intune and Microsoft Office 365 licenses.
- Secure Hub version 21.4.0 and later
- Configure Azure AD as an identity provider (IdP) in Citrix Cloud, and then set Citrix identity as the IdP type for Endpoint Management. For information, see [Authentication with Azure Active Directory through Citrix Cloud](#).
- Consent to the Citrix Multi-tenant AAD application to allow mobile applications to authenticate with the AAD client app. Only required if the Azure Global Administrator set the value for **Users can register applications** to **No**. Configure this setting in the Azure portal under **Azure Active Directory > Users > User Settings**. To provide consent, see Configure Endpoint Management for Azure AD Compliance Management.
- Install the Microsoft Authenticator application on the device before starting the Azure AD device registration process.
- For the Android Enterprise platform, configure a web browser app as the required public store app.
- Disable the **Security defaults** setting in the Azure AD console. When you start Azure AD configuration, you will replace security defaults with more granular Azure AD Conditional Access policies. For more information about security defaults, see the [Microsoft documentation](#).

### Configure device compliance through Azure AD Conditional Access policies

The general steps to configure device compliance through Azure AD Conditional Access policies are as follows:

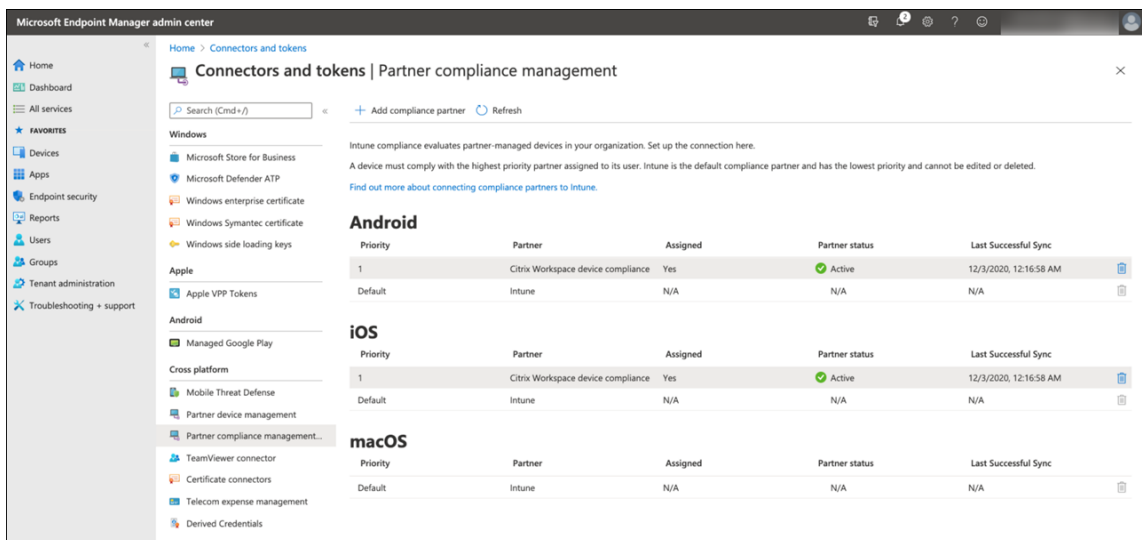
#### 1. Endpoint Management configuration:

- In the Microsoft Endpoint Manager admin center, add **Citrix Workspace device compliance** as the compliance partner for each device platform and assign user groups.
- In Endpoint Management, synchronize information from the Microsoft Endpoint Manager admin center.

2. **Azure AD configuration:** In the Azure AD portal, set Conditional Access policies for individual Office 365 apps.
3. **Endpoint Management configuration:** After configuring Conditional Access policies for Office 365 apps, add the Microsoft Authenticator app and Office 365 apps as public app store apps in Endpoint Management. Assign these public apps to the delivery group and set them as required apps.

### Configure Endpoint Management for Azure AD compliance management

1. Sign in to the [Microsoft Endpoint Manager admin center](#) and navigate to **Tenant administration > Connectors and tokens > Device compliance management**. Click **Add compliance partner** and choose **Citrix Workspace device compliance** as the compliance partner for each device platform. Then assign user groups.




2. In Endpoint Management, go to **Settings > Azure AD compliance management**.
3. Optionally, set global consent so that users don't need to provide consent on each device. Next to **Client App consent**, click **Provide consent**. Enter your global admin Azure AD credentials and follow the prompts to provide global consent for the client apps.
4. Click **Connect** to sync information from the Microsoft Endpoint Manager admin center.

Settings > Azure AD Compliance Management

### Azure AD compliance management

Configure Endpoint Management to enable device compliance through Azure AD conditional access. This feature requires that you configure Azure Active Directory in [Citrix Cloud Identity and Access Management](#). Select Azure AD as the IDP in the [Identity Provider](#) setting page.


 Before configuring this page, go to [Intune Partner compliance management](#) page. Add **Citrix Workspace device compliance** as the compliance partner for each device platform and assign user groups. Then, on this page, click **Connect** to sync information from Intune. [Learn more](#)

IDP Configuration Citrix Identity Platform with AzureAd

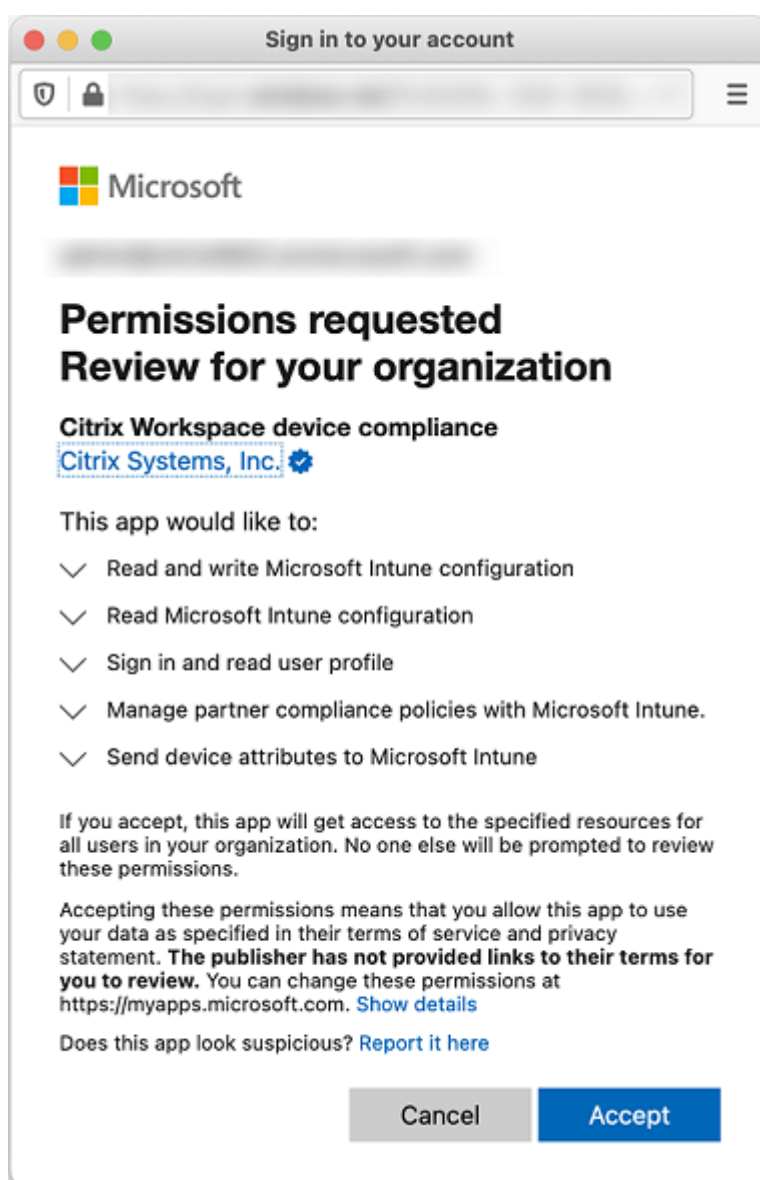
Compliance Partner name Citrix Workspace Device Compliance

Client App consent [Provide consent](#)

Platform	Included Groups	Excluded Groups
No results found.		

[Connect](#) [Close](#) 

A dialog box prompts you to accept the permissions for this configuration. Click **Accept**. After the configuration completes, synchronized device platforms appear in the list.



### Configure Conditional Access policies in Azure AD

In the Azure AD portal, configure Conditional Access policies for Office 365 apps to enforce device compliance. Go to **Devices > Conditional Access > Policies > New policy**. For more information, see the [Microsoft documentation](#).

To configure device compliance for Intune managed apps:

- [Configure Intune managed apps for delivery to devices](#)
- [Require approved client apps](#)
- [Require app protection policy and an approved client app for cloud app access](#)

## Configure apps in Endpoint Management

After configuring Conditional Access policies for Office 365 apps, add the Microsoft Authenticator app and Office 365 apps as public app store apps in Endpoint Management. Assign these public apps to the delivery group and set them as required apps. For information, see [Add a public app store app](#).

### User authentication workflow

1. A new user must enroll a device into Endpoint Management using Azure AD credentials. Users, who previously enrolled with Azure AD credentials, don't need to re-enroll their devices.
2. Endpoint Management pushes Microsoft Authenticator and configured Office 365 apps to a device as required apps. If you configured a web browser app as the required public store app for Android platform, Endpoint Management pushes it to the user device as well.
3. Secure Hub automatically installs and displays all apps managed through Endpoint Management.
4. When a user tries to sign in to any available Office 365 app, the device prompts the user to tap the **Azure AD registration** link to start the registration process.
5. After the user taps the registration link, the Microsoft authenticator app opens. The user enters Azure AD credentials and agrees to the device enrollment terms. Then the Microsoft authenticator app closes and Secure Hub reopens.
6. Secure Hub displays a message that Azure AD device registration is complete. The user can now use Microsoft apps to access their cloud resources.

After the registration completes, Azure AD marks the device as managed and compliant in the console.

### Default device policies and mobile productivity apps

If you onboard starting with Endpoint Management 19.5.0 or later, we preconfigure a few device policies and mobile productivity apps. That configuration enables you to:

- Immediately deploy basic functionality to devices
- Start with the recommended baseline configurations for a secure workspace

For the Android, Android Enterprise, iOS, macOS, and Windows Desktop/Tablet platforms, your site contains these preconfigured device policies:

- **Passcode device policy:** The Passcode device policy is **On**, with all default passcode settings enabled.
- **App inventory device policy:** The App inventory device policy is **On**.

- **Restrictions device policy:** The Restrictions device policy is **On**, with all default restrictions settings enabled.

Those policies are in the **AllUsers** delivery group, which contains all Active Directory and local users. We recommend that you use the AllUsers delivery group only for initial testing. Then, create your delivery groups and disable the AllUsers delivery group. You can reuse the preconfigured device policies and apps in your delivery groups.

All Endpoint Management device policies are documented under [Device policies](#). That article includes information about how to use the console to edit device policies. For information about some commonly used device policies, see [Device policies and Use Case Behavior](#).

For the iOS and Android platforms, your site contains these preconfigured mobile productivity apps:

- **Secure Mail**
- **Secure Web**
- **Citrix Files**

Those apps are in the **AllUsers** delivery group.

For more information, see [About mobile productivity apps](#).

## Continue your Endpoint Management configuration

After you complete the basic setup for device enrollment, how you configure Endpoint Management varies widely based on your use cases. For example:

- What are your security requirements and how do you want to balance those requirements with user experience?
- Which device platforms do you support?
- Do users own their devices or use corporate-owned devices?
- What device policies do you want to push to devices?
- What types of apps do you provide users?

This section helps you navigate through the many configuration choices by directing you to articles in this documentation set.

As you complete configuration in third-party sites, make note of the information and its location, for reference when you configure Endpoint Management console settings.

- Security and authentication. Endpoint Management uses certificates to create secure connections and authenticate users. Citrix provides wildcard certificates for your Endpoint Management instance.
  - For a discussion of authentication components and recommended configurations by security level, see the “Advanced concepts” article, [Authentication](#). See also, [Security and user experience](#).

- For an overview of the authentication components used during Endpoint Management operations, see [Certificates and authentication](#).
- You can choose from the following types of authentication. Configuring authentication includes tasks in the Endpoint Management and Citrix Gateway consoles.
  - \* [Domain or domain plus security token authentication](#)
  - \* [Client certificate or certificate plus domain authentication](#)
- To deliver certificates to users, configure:
  - \* [PKI entities](#)
  - \* [Credential providers](#)
- Device enrollment security modes. Device enrollment security modes specify the credential types and use enrollment steps required for users to enroll their devices in Endpoint Management. For information, see [Configure enrollment security modes](#).
- To allow users to authenticate with Azure Active Directory credentials, see [Authenticate with Azure Active Directory through Citrix Cloud](#).
- Device enrollment
  - Programs are available to enroll large numbers of devices:
    - \* [Deploy devices through Apple Deployment Program](#)
    - \* [Bulk enrollment of Apple devices](#)
    - \* [Samsung Knox Bulk Enrollment](#)
    - \* [Enroll Windows devices in bulk](#)
  - To enroll Android devices, create an Android Enterprise administrator account. See [Android Enterprise](#). Or, see [Legacy Android Enterprise for Google Workspace Customers](#).
  - To configure Google Workspace for Chrome OS device enrollment from your Google Workspace account, see [Chrome OS](#).
  - To enroll a Citrix Ready workspace hub, see [Workspace hub device management](#)
  - You can use enrollment invitations or send notifications for enrollment.
    - \* [Enrollment invitations](#).
    - \* [Notifications](#).
  - For more information about enrollment, see [Device management](#) and articles under that node.
- Device policies and management
  - Device (MDM) policies. All Endpoint Management device policies are documented under [Device policies](#). For information about some commonly used device policies, see [Device Policies and Use Case Behavior](#).



- Client properties. Client properties contain information that is provided directly to Secure Hub on user devices. See [Client properties](#) and [Endpoint Management client properties](#).
- Delivery groups. For a sample use case related to delivery groups, see [User Communities](#) and [Add a delivery group](#).
- Prepare apps for deployment
  - For information about the apps supported by Endpoint Management, see [Add apps](#).
  - You can manage iOS app licensing by using Apple volume purchase. For information, see [Apple Volume Purchase](#).
  - You can use Endpoint Management to deploy iBooks that you obtain through Apple volume purchase. See [Add media](#).
  - You can connect Citrix Endpoint Management to the Microsoft Store for Business. See [Deploy Microsoft Store for Business apps from Endpoint Management](#).
  - Citrix provides mobile productivity apps, including Secure Mail and Secure Web. See [About mobile productivity apps](#).
  - As an alternative to Secure Mail, you can deliver native mail to devices. See:
    - \* [Email strategy](#)
    - \* [Endpoint Management connector for Exchange ActiveSync](#)
    - \* [Citrix Gateway connector for Exchange ActiveSync](#)
  - To allow users to securely transfer docs and data to Microsoft Office 365 apps, see [Allowing Secure Interaction with Office 365 Apps](#) and [Office device policy](#).
  - For general information about app policies, see [App Policies and Use Case Scenario](#).
  - The MDX Toolkit is an app wrapping technology that prepare enterprise apps for secure deployment with Endpoint Management. The MAM SDK replaces the MDX Toolkit. The MDX toolkit is scheduled to reach EOL in March 2022.  
  
For information about the MAM SDK, see [MAM SDK overview](#).
  - For more information about apps, see other articles under [Add apps](#).
- The Role-Based Access Control (RBAC) feature in Endpoint Management lets you assign predefined roles, or sets of permissions, to users and groups. These permissions control the level of access users have to system functions. For information, see [Configure roles with RBAC](#).
- You create automated actions in Endpoint Management to specify the action to take in reaction to events, certain settings, or the presence of apps on user devices. For information, see [Automated actions](#).

## Certificates and authentication

October 13, 2021

Several components play a role in authentication during Endpoint Management operations:

- **Endpoint Management:** The Endpoint Management server is where you define enrollment security and the enrollment experience. Options for onboarding users include:
  - Whether to make the enrollment open for all or by invitation only.
  - Whether to require two-factor authentication or three-factor authentication. Endpoint Management client properties allow you to enable Citrix PIN authentication and configure the PIN complexity and expiration.
- **Citrix Gateway:** Citrix Gateway provides termination for micro VPN SSL sessions. Citrix Gateway also provides network in-transit security, and lets you define the authentication experience used each time a user accesses an app.
- **Secure Hub:** Secure Hub and Endpoint Management work together in enrollment operations. Secure Hub is the entity on a device that talks to Citrix Gateway: When a session expires, Secure Hub gets an authentication ticket from Citrix Gateway and passes the ticket to the MDX apps. Citrix recommends certificate pinning, which prevents man-in-the-middle attacks. For more information, see this section in the Secure Hub article: [Certificate pinning](#).

Secure Hub also facilitates the MDX security container: Secure Hub pushes policies, creates a session with Citrix Gateway when an app times out, and defines the MDX timeout and authentication experience. Secure Hub is also responsible for jailbreak detection, geolocation checks, and any policies you apply.

- **MDX policies:** MDX policies create the data vault on the device. MDX policies direct micro VPN connections back to Citrix Gateway, enforce offline mode restrictions, and enforce client policies, such as time-outs.

Citrix Endpoint Management authenticates users to their resources using the following authentication methods:

- Mobile device management (MDM)
  - Cloud-hosted identity providers (IdPs)
  - Lightweight Directory Access Protocol (LDAP)
    - \* Invitation URL + Pin
    - \* Two-factor authentication
- Mobile application management (MAM)
  - LDAP
  - Certificate

- Security token

MAM authentication requires Citrix Gateway.

For other configuration details, see the following articles:

- [Upload, update, and renew certificates](#)
- [Citrix Gateway and Endpoint Management](#)
- [Domain or domain plus security token authentication](#)
- [Client certificate or certificate plus domain authentication](#)
- [PKI entities](#)
- [Credential providers](#)
- [APNs certificates](#)
- If your site isn't Workspace enabled: [SAML for single sign-on with Citrix Files](#)
- [Authentication with Azure Active Directory through Citrix Cloud](#)
- [Authentication with Okta through Citrix Cloud](#)
- [Authentication with an on-premises Citrix Gateway through Citrix Cloud](#)
- To authenticate to a Wi-Fi server, send a certificate to the devices: [Network device policy](#)
- To push a unique certificate not used for authentication, such as an internal root certificate authority (CA) certificate, or a specific policy: [Credentials device policy](#)
- To enable certificate management on Android devices, watch this video:



## Certificates

Endpoint Management generates a self-signed Secure Sockets Layer (SSL) certificate during installation to secure the communication flows to the server. Replace the SSL certificate with a trusted SSL certificate from a well-known certificate authority.

Endpoint Management also uses its own Public Key Infrastructure (PKI) service or obtains certificates from the CA for client certificates. All Citrix products support wildcard and Subject Alternative Name (SAN) certificates. For most deployments, you only need two wildcard or SAN certificates.

Client certificate authentication provides an extra layer of security for mobile apps and lets users seamlessly access HDX Apps. When client certificate authentication is configured, users type their Citrix PIN for single sign-on (SSO) access to Endpoint Management-enabled apps. Citrix PIN also simplifies the user authentication experience. Citrix PIN is used to secure a client certificate or save Active Directory credentials locally on the device.

To enroll and manage iOS devices with Endpoint Management, set up and create an Apple Push Notification Service (APNs) certificate from Apple. For steps, see [APNs certificates](#).

The following table shows the certificate format and type for each Endpoint Management component:

Endpoint Management component	Certificate format	Required certificate type
Citrix Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Root (Citrix Gateway converts PFX to PEM automatically.)
Endpoint Management	.p12 (.pfx on Windows-based computers)	SSL, SAML, APNs (Endpoint Management also generates a full PKI during the installation process.) <b>Important:</b> Endpoint Management doesn't support certificates with a .pem extension. To use a .pem certificate, split the .pem file into a certificate and key and import each into Endpoint Management.
StoreFront	PFX (PKCS #12)	SSL, Root

Endpoint Management supports client certificates with bit lengths of 4096 and 2048.

For Citrix Gateway and Endpoint Management, Citrix recommends obtaining server certificates from

a public CA, such as Verisign, DigiCert, or Thawte. You can create a Certificate Signing Request (CSR) from the Citrix Gateway or the Endpoint Management configuration utility. After you create the CSR, you submit it to the CA for signing. When the CA returns the signed certificate, you can install the certificate on Citrix Gateway or Endpoint Management.

**Important:**

Requirements for trusted certificates in iOS, iPadOS, and macOS

Apple has new requirements for TLS server certificates. Verify that all certificates follow the Apple requirements. See the Apple publication, <https://support.apple.com/en-us/HT210176>.

Apple is reducing the maximum allowed lifetime of TLS server certificates. This change affects only server certificates issued after September 2020. See the Apple publication, <https://support.apple.com/en-us/HT211025>.

## LDAP authentication

Endpoint Management supports domain-based authentication for one or more directories that are compliant with the Lightweight Directory Access Protocol (LDAP). LDAP is a software protocol that provides access to information about groups, user accounts, and related properties. For more information, see [Domain or domain plus security token authentication](#).

## Identity provider authentication

You can configure an identity provider (IdP) through Citrix Cloud to enroll and manage user devices.

Supported use cases for IdPs:

- Azure Active Directory through Citrix Cloud
  - Workspace integration is optional
  - Citrix Gateway configured for certificate-based authentication
  - Android Enterprise (Preview. Supports BYOD, fully managed devices, and enhanced enrollment profiles)
  - iOS for MDM+MAM and MDM enrollments
  - Legacy Android (DA)
  - Auto enrollment features such as the Apple Deployment Program are currently not supported
- Okta through Citrix Cloud
  - Workspace integration is optional
  - Citrix Gateway configured for certificate-based authentication
  - Android Enterprise (Preview. Supports BYOD, fully managed devices, and enhanced enrollment profiles)

- iOS for MDM+MAM and MDM enrollments
- Legacy Android (DA)
- Auto enrollment features such as the Apple Deployment Program are currently not supported
- On-premises Citrix Gateway through Citrix Cloud
  - Citrix Gateway configured for certificate-based authentication
  - Android Enterprise (Preview. Supports BYOD, fully managed devices, and enhanced enrollment profiles)
  - iOS for MDM+MAM and MDM enrollments
  - Legacy Android (DA)
  - Auto enrollment features such as the Apple Deployment Program are currently not supported

### **Identity provider authentication without a Cloud Connector (Preview)**

This feature is available as a public preview. To enable this feature, contact your Citrix representative.

Endpoint Management supports configuring identity providers (IdPs), such as Azure AD and Okta, as authentication methods. This feature, now in preview, lets you configure IdPs without using a Cloud Connector. You can also manage user resource access through those IdPs. By using an IdP to manage access, you can better integrate with cloud services such as Office 365 and reduce the need for on-premises resources.

Endpoint Management still requires a Cloud Connector for the following:

- LDAP
- PKI Server
- Internal DNS queries
- Citrix Virtual Apps

To establish communication between Endpoint Management and a cloud-hosted identity provider without a Cloud Connector, you must configure Citrix identity as the IdP type for Endpoint Management. However, the services that require a Cloud Connector, as mentioned previously, aren't available.

If you have previously configured LDAP, using this feature results in a hybrid environment where LDAP acts as a fallback for group membership and user and group searches. Without LDAP set up, you rely on the IdP fully.

After you finish this configuration, you can't add LDAP settings in Endpoint Management. If you have LDAP set up and you add an IdP, Endpoint Management synchronizes IdP-specific information from your Active Directory groups to the Endpoint Management database. When you deploy policies, apps, and media to users, only the IdP groups receive the resources.

## Prerequisites

There are two sets of prerequisites to must consider depending on your current Endpoint Management configuration:

### With LDAP

- User groups in Active Directory must match the user groups in Azure Active Directory or Okta.
- User names and email addresses in Active Directory must match the information in Azure Active Directory or Okta.
- Citrix Cloud account, with Citrix Cloud Connector installed for directory services synchronization.
- Citrix Gateway. Citrix recommends that you enable certificate-based authentication for a full single sign-on experience. If you use LDAP authentication on the Citrix Gateway for MAM registration, end users experience a dual authentication prompt during enrollment. For more information, see [Client certificate or certificate plus domain authentication](#).
- Synchronize Active Directory SIDs into respective IdPs. Azure AD and Active Directory SIDs or Okta and Active Directory SIDs must match for delivery groups to function properly.
- On Azure AD or Okta, create a group named **Administrators** for Citrix identity to connect to your IdP.
- If you have multiple LDAPs synced to an IdP, set the global context server property `ldap.set.gc.rootcontext` to **True**. This property ensures that the Cloud Connector searches for all parent and child domains.
- If your LDAP and IdP domains don't match, add the appropriate IdP domain alias to the LDAP configuration.

### Without LDAP

- On Azure AD or Okta, create a group named **Administrators** for Citrix identity to connect to your IdP.

## Configuration

To configure Azure AD or Okta as an identity provider through Citrix Cloud and set it up for Endpoint Management, follow one or both of these articles:

- [Authentication with Azure Active Directory through Citrix Cloud](#)
- [Authentication with Okta through Citrix Cloud](#)

## Active Directory synchronization

If you have Active Directory groups set up, Endpoint Management synchronizes IdP-specific information from those groups to the Endpoint Management database after you configure an IdP. To view the status of the synchronization process, go to **Settings > Identity Provider**. One of the following statuses appears under **Directory sync**.

- **Empty:** Endpoint Management isn't configured to manage this identity provider. Check the configuration for your IdP.
- **Done:** The synchronization process successfully completed. Endpoint Management can now manage resources from this identity provider.
- **In progress:** The synchronization process is in progress. If your database contains many user groups, Endpoint Management may take more time to synchronize IdP information for your Active Directory groups.
- **Error:** An error occurred during synchronization. This issue might happen if your IdP is disconnected or a Cloud Connector isn't working properly at the moment. Use debug logs to troubleshoot the issue or try to add the IdP settings again.

After synchronization completes, you can add IdP groups as assignments to your delivery group in **Configure > Delivery groups > Assignments**. When you select a domain for a delivery group assignment, pick the IdP you configured before searching. For information, see [Add a delivery group](#).

You can also apply RBAC permissions to IdP groups. For information, see [Use the RBAC feature](#).

### Expectations for existing configurations

After enabling and configuring this feature, you can expect the following for your existing setup:

- Existing delivery groups and RBAC assignments and permissions are unaffected. Users have the same access and receive the same resources they did before configuring this feature.
- Object identifiers for any Active Directory groups synced with Endpoint Management are automatically populated from the IdPs.
- Existing enrolled devices are unaffected as long as the user information is synced to the IdP. When the user information isn't synced to the IdP:
  - If you have LDAP set up, enrolled devices for users not synced to the IdP can still authenticate through LDAP.
  - If you don't have LDAP set up, enrolled devices for users not synced with the IdP fail to refresh or reconnect.
- For users that are found on the IdP, Endpoint Management determines their group membership based on IdP information.

### Delete an LDAP-compliant directory

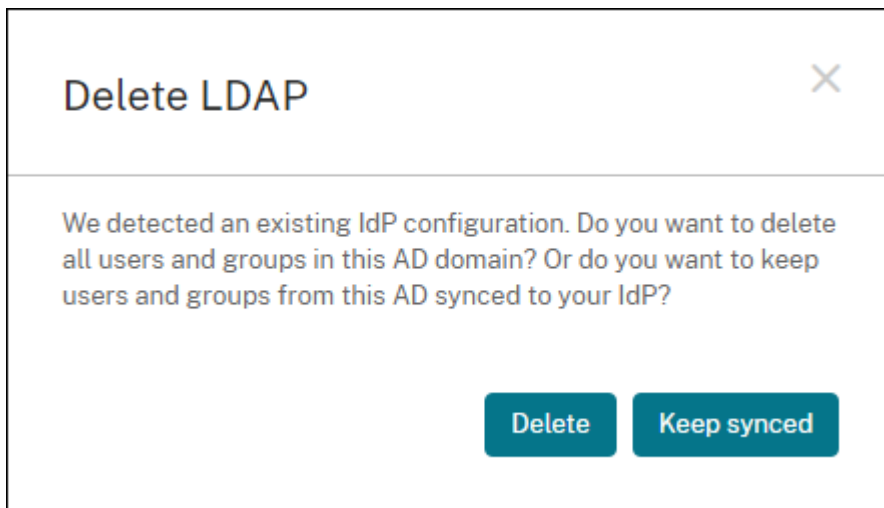
You can delete LDAP profiles that you no longer need. For instance, LDAP profiles with no users or groups being used by Endpoint Management.



1. In the list of LDAP profiles, select the directory you want to delete.

You can delete more than one property by selecting the check box next to each property.

2. Click **Delete**. In the confirmation dialog box, choose one of the following options:



- Click **Delete** to delete all user and group information from the selected LDAP directory. If you configure Azure AD or Okta as an identity provider through Citrix Cloud, this operation lets you delete the default LDAP domain.
- Click **Keep synced** to delete all user and group information that isn't synchronized with an identity provider. Endpoint Management only keeps users and groups synced to an identity provider. Any user devices, delivery groups, and RBAC permissions linked to this LDAP become linked to the identity provider. If your database contains many user groups, Endpoint Management may take more time to map Active Directory objects to the IdP. This operation happens in the background.

### Delete an identity provider

To stop using an identity provider or change the type of your identity provider, you must delete the IdP.

1. In the Endpoint Management console, go to **Settings > Identity Provider**.
2. In the IdP table, select the identity provider.
3. Click **Delete**. In a confirmation dialog box, click **Delete** again.

Endpoint Management removes any user or group information from the database connected to your identity provider. Endpoint Management removes any delivery groups or RBAC assignments for this IdP as well. Any user devices enrolled from this IdP need to re-enroll. After deleting an IdP, you can configure a different type of an identity provider or set up LDAP again.

## Limitations

- This feature doesn't support devices enrolling through Citrix Workspace app.
- If you configure an identity provider, you can't add LDAP settings in Endpoint Management.
- To change the authentication domain, you must delete your identity provider.
- The Self-Help Portal doesn't support authentication with identity providers.
- If you sync your parent and child domains to the IdP and those domains contain identical group names, those groups can't be added to Endpoint Management. Make sure that your group names are unique across domains.

## Upload, update, and renew certificates

October 7, 2021

We recommend that you list the certificates needed for your Endpoint Management deployment. Use the list to track the certificate expiration dates and passwords. This article helps you administer certificates throughout their lifespan.

Your environment might include the following certificates:

- Endpoint Management server
  - SSL Certificate for MDM FQDN (needed if you migrated from XenMobile Server to Endpoint Management; otherwise, Citrix manages this certificate)
  - SAML Certificate (for Citrix Files)
  - Root and Intermediate CA Certificates for the preceding certificates and any other internal resources (StoreFront/Proxy, and so on)
  - APNs Certificate for iOS Device Management
  - PKI User Certificate for connectivity to PKI (required if your environment requires certificate-based authentication)
- MDX Toolkit
  - Apple Developer Certificate
  - Apple Provisioning Profile (per application)
  - Apple APNs Certificate (for use with Citrix Secure Mail)
  - Android Keystore File
  - Windows Phone – DigiCert Certificate

The MAM SDK doesn't wrap apps, so it doesn't require a certificate.

- Citrix Gateway
  - SSL Certificate for MDM FQDN

- SSL Certificate for Gateway FQDN
- SSL Certificate for ShareFile SZC FQDN
- SSL Certificate for Exchange Load Balancing (offload configuration)
- SSL Certificate for StoreFront Load Balancing
- Root and Intermediate CA Certificates for the preceding certificates

## Upload certificates

Each certificate you upload has an entry in the Certificates table, including a summary of its contents. When you configure PKI integration components that require a certificate, choose a server certificate to satisfy the criteria. For example, you might want to configure Endpoint Management to integrate with your Microsoft certificate authority (CA). The connection to the Microsoft CA must be authenticated by using a client certificate.

Endpoint Management might not possess the private key for a given certificate. Likewise, Endpoint Management might not require a private key for uploaded certificates.

This section provides general procedures for uploading certificates. For details about creating, uploading, and configuring client certificates, see [Client certificate or certificate plus domain authentication](#).

You have two options for uploading certificates:

- Upload the certificates to the console individually.
- Perform a bulk upload of certificates using the REST API. This option is available for iOS devices only.

When uploading certificates to the console, you can:

- Import a keystore. Then, you identify the entry in the keystore repository you want to install, unless you are uploading a PKCS #12 format.
- Import a certificate.

You can upload the CA certificate (without the private key) that the CA uses to sign requests. You can also upload an SSL client certificate (with the private key) for client authentication.

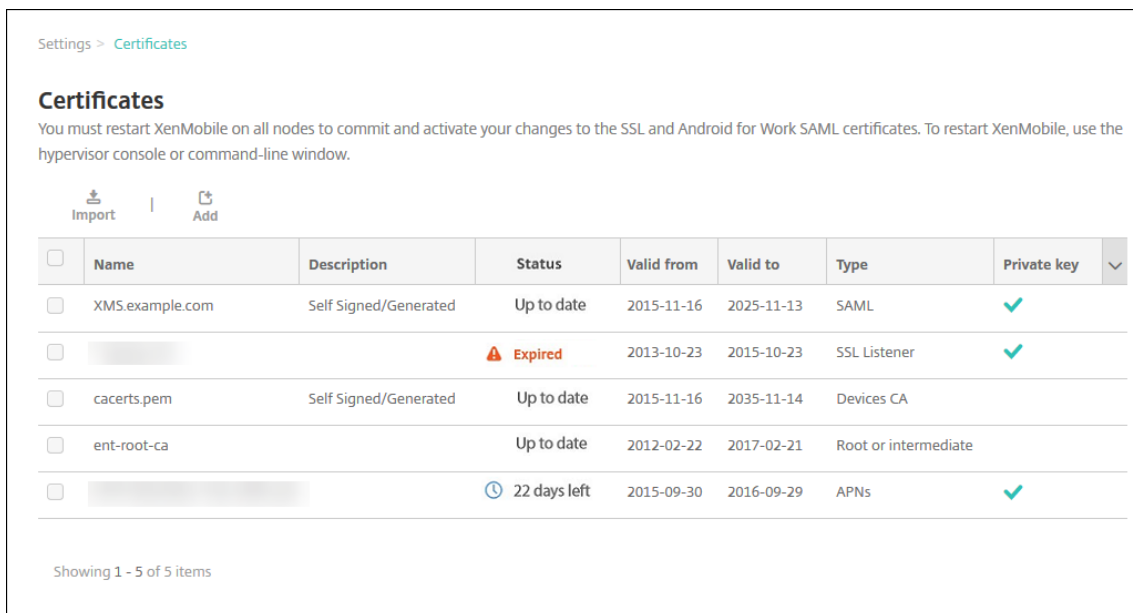
When configuring the Microsoft CA entity, you specify the CA certificate. You select the CA certificate from a list of all server certificates that are CA certificates. Likewise, when configuring client authentication, you can select from a list of all the server certificates for which Endpoint Management has the private key.

## To import a keystore

A keystore is a repository of security certificates. By design, keystores can contain multiple entries. When loading from a keystore, you must specify the entry alias that identifies the entry you want to

load. If you don't specify an alias, the first entry from the store loads. Because PKCS #12 files usually contain only one entry, the alias field doesn't appear when you select PKCS #12 as the keystore type.

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. Use the search bar to find and open the **Certificates** setting.



2. Click **Import**. The **Import** dialog box appears.
3. Configure these settings:
  - **Import:** Select **Keystore**.

## Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

**Import** Keystore

**Keystore type** PKCS#12

**Use as** Server

**Keystore file\***

**Password\***

**Description**

- **Keystore type:** In the list, click **PKCS #12**.
- **Use as:** In the list, click how you plan to use the certificate. The available options are:
  - **Server:** Server certificates are certificates used functionally by Endpoint Management. You upload server certificates to the Endpoint Management web console. Those certificates include CA certificates, RA certificates, and certificates for client authentication with other components of your infrastructure. In addition, you can use server certificates as storage for certificates you want to deploy to devices. This use especially applies to CAs used to establish trust on the device.
  - **SAML:** Security Assertion Markup Language (SAML) certification allows you to provide SSO access to servers, websites, and apps.
  - **APNs:** APNs certificates from Apple enable mobile device management via the Apple Push Network.
  - **SSL Listener:** The Secure Sockets Layer (SSL) Listener notifies Endpoint Management of SSL cryptographic activity.
- **Keystore file:** Browse to find the keystore you want to import. The keystore is a .p12 or .pfx file. Select the file and click **Open**.
- **Password:** Type the password assigned to the certificate.

- **Description:** Optionally, type a description for the keystore to help you distinguish it from your other keystores.
4. Click **Import**. The keystore is added to the Certificates table.

### To import a certificate

When importing a certificate, Endpoint Management attempts to construct a certificate chain from the input. Endpoint Management imports all certificates in a chain to create a server certificate entry for each certificate. This operation only works if the certificates in the file or keystore entry do form a chain. Each subsequent certificate in the chain must be the issuer of the previous certificate.

You can add an optional description for the imported certificate. The description only attaches to the first certificate in the chain. You can update the description of the remaining certificates later.

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. Use the search bar to find and open the **Certificates** setting.
2. On the **Certificates** page, click **Import**. The **Import** dialog box appears. Configure the following:
  - **Import:** click **Certificate**.
  - **Use as:** Select how you plan to use the certificate. The available options are:
    - **Server:** Server certificates are certificates used functionally by Endpoint Management. You upload server certificates to the Endpoint Management web console. Those certificates include CA certificates, RA certificates, and certificates for client authentication with other components of your infrastructure. In addition, you can use server certificates as storage for certificates you want to deploy to devices. This option especially applies to CAs used to establish trust on the device.
    - **SAML:** Security Assertion Markup Language (SAML) certification allows you to provide single sign-on (SSO) access to servers, websites, and apps.
    - **SSL Listener:** The Secure Sockets Layer (SSL) Listener notifies Endpoint Management of SSL cryptographic activity.
  - **Certificate import:** Browse to find the certificate you want to import. Select the file and click **Open**.
  - **Private key file:** Browse to find an optional private key file for the certificate. The private key is used for encryption and decryption along with the certificate. Select the file and click **Open**.
  - **Description:** Type a description for the certificate, optionally, to help you identify it from your other certificates.
3. Click **Import**. The certificate is added to the Certificates table.

## Upload certificates in bulk using the REST API

Sometimes uploading certificates one at a time isn't reasonable. In those cases, perform a bulk upload of certificates using the REST API. This method supports certificates in the .p12 format. For more information about the REST API, see [REST APIs](#).

1. Rename each of the certificate files in the format `device_identity_value.p12`. The `device_identity_value` can be the IMEI, Serial Number, or MEID of each device.

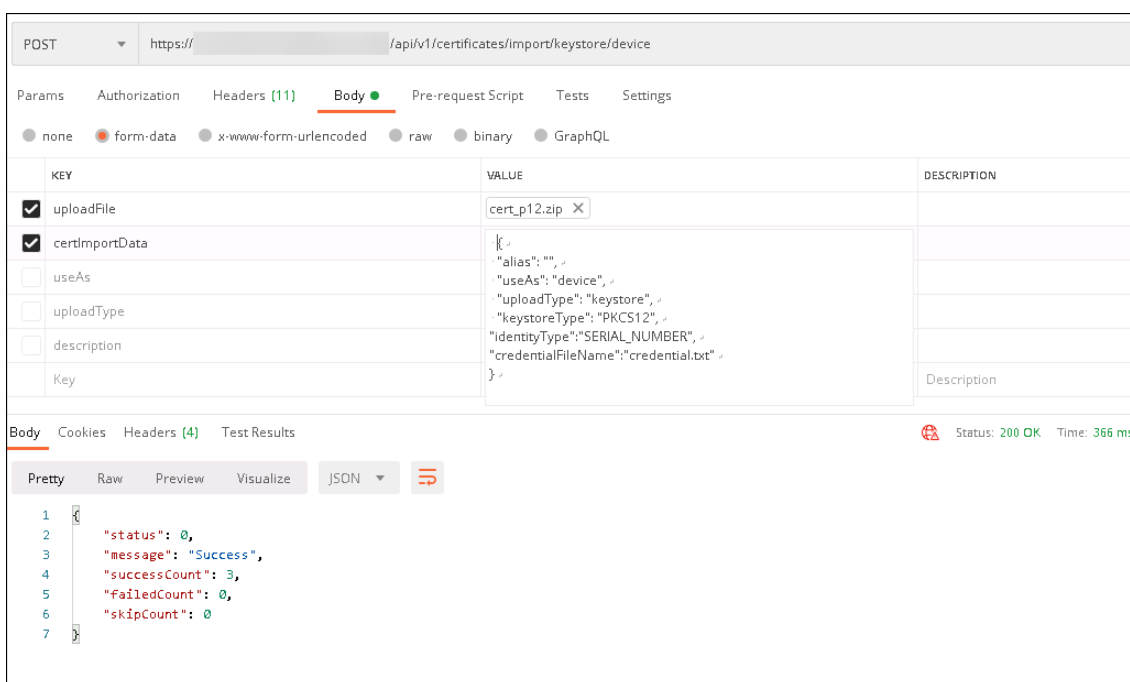
As an example, you choose to use serial numbers as your identification method. One device has a serial number `A12BC3D4EFGH`, so name the certificate file you expect to install on that device `A12BC3D4EFGH.p12`.

2. Create a text file to store the passwords for the .p12 certificates. In that file, type the device identifier and password for each device on a new line. Use the format `device_identity_value=password`. See the following:

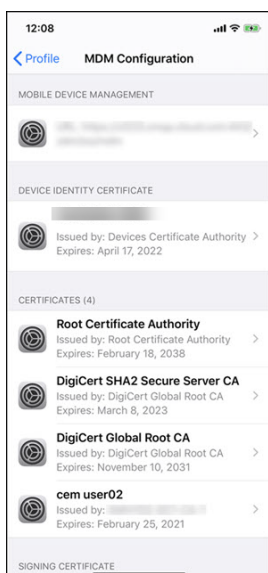
```
1 A12BC3D4EFGH.p12=password1!  
2 A12BC3D4EFIJ.p12=password2@  
3 A12BC3D4EFKL.p12=password3#  
4 <!--NeedCopy-->
```

3. Pack all certificates and the text file you created into a .zip file.
4. Launch your REST API client, log in to Endpoint Management, and get an authentication token.
5. Import your certificates, ensuring you put the following in the message body:

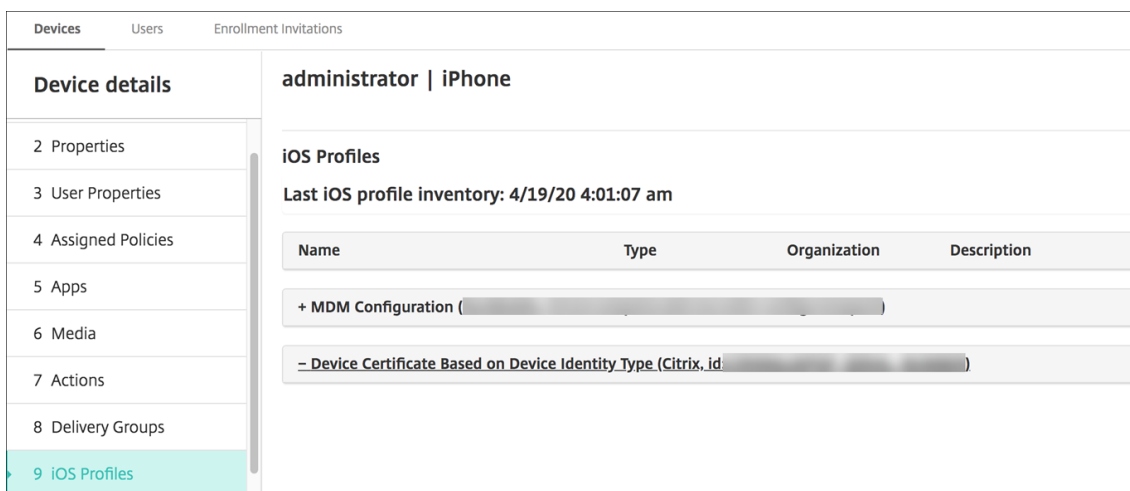
```
1 {  
2  
3     "alias": "",  
4     "useAs": "device",  
5     "uploadType": "keystore",  
6     "keystoreType": "PKCS12",  
7     "identityType": "SERIAL_NUMBER",           # identity type can be  
8     "credentialFileName": "credential.txt"     # The credential file  
9 }                                               name in .zip  
10  
11 <!--NeedCopy-->
```



6. Create a VPN policy with the credential type **Always on IKEv2** and the device authentication method **Device Certificate Based on Device Identity**. Select the **Device identity type** you used in your certificate files names. See [VPN device policy](#).
7. Enroll an iOS device and wait for the VPN policy to deploy. Confirm the certificate installation by checking the MDM configuration on the device. You can also check the device details in the Endpoint Management console.







You can also delete certificates in bulk by creating a text file with the `device_identity_value` listed for each certificate to delete. In the REST API, call the delete API and use the following request, replacing `device_identity_value` with the appropriate identifier:

```

1  ``
2  {
3
4      "identityType"="device_identity_value"
5  }
6
7  <!--NeedCopy--> ``

```

The screenshot shows a REST client interface for a POST request to the endpoint `https://.../api/v1/certificates/remove/keystore/device`. The request body is a JSON object with the following fields:

Key	Value	Description
<input checked="" type="checkbox"/> uploadFile	DEL.txt X	
<input checked="" type="checkbox"/> certRemoveData	{ ...	
<input type="checkbox"/> useAs	none	
<input type="checkbox"/> uploadType	keystore	
<input type="checkbox"/> description	wwwkkk	

The response is a JSON object with the following fields:

```

1 {
2   "status": 0,
3   "message": "Success",
4   "successCount": 2,
5   "failedCount": 0,
6   "skipCount": 0
7 }

```

The status is 200 OK and the time taken is 522 ms.

## Update a certificate

Endpoint Management only allows one certificate per public key to exist in the system at a time. If you attempt to import a certificate for the same key pair as an already imported certificate you can:

- Replace the existing entry.
- Delete the entry.

After you upload a new certificate to replace an old certificate, you can't delete the old certificate. When you configure the PKI Entities setting, both certificates exist in the **SSL client certificate** menu. The newer certificate is lower in the list than the old certificate.

## To update your certificates

1. Create a replacement certificate by following the steps in [Client certificate or certificate plus domain authentication](#).

### Important:

Do not use the option to create a certificate with the existing private key. When you create a certificate to update an expiring certificate, the private key must be new as well.

2. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. Use the search bar to find and open the **Certificates** setting.
3. In the **Import** dialog box, import the new certificate.

When you update a server certificate, components using the previous certificate automatically switch to using the new certificate. Likewise, if you have deployed the server certificate on devices, the certificate automatically updates on the next deployment.

To update an APNs certificate, perform the steps to create a certificate, then go to the Apple Push Certificates Portal. For more information, see [Renew an APNs certificate](#).

If your Citrix Gateway is set up for SSL offload, ensure that you update your load balancer with the new cacert.pem.

### To update a PKI service certificate authority (CA)

You can request that Citrix Cloud Operations refresh or regenerate the internal PKI certificate authorities (CAs) in your Endpoint Management deployment. Open a Technical Support case for these requests.

- 1 When the **new** CAs are available, Cloud Operations lets you know that you can proceed with renewing the device certificates **for** your users.

### Renew device certificates

If a certificate on a device expires, the certificate becomes invalid. You can no longer run secure transactions on your environment and you can't access Endpoint Management resources. The Certification Authority (CA) prompts you to renew your SSL certificate before the expiration date. Perform the steps described previously to update the certificate, and then initiate a certificate renewal on enrolled devices.

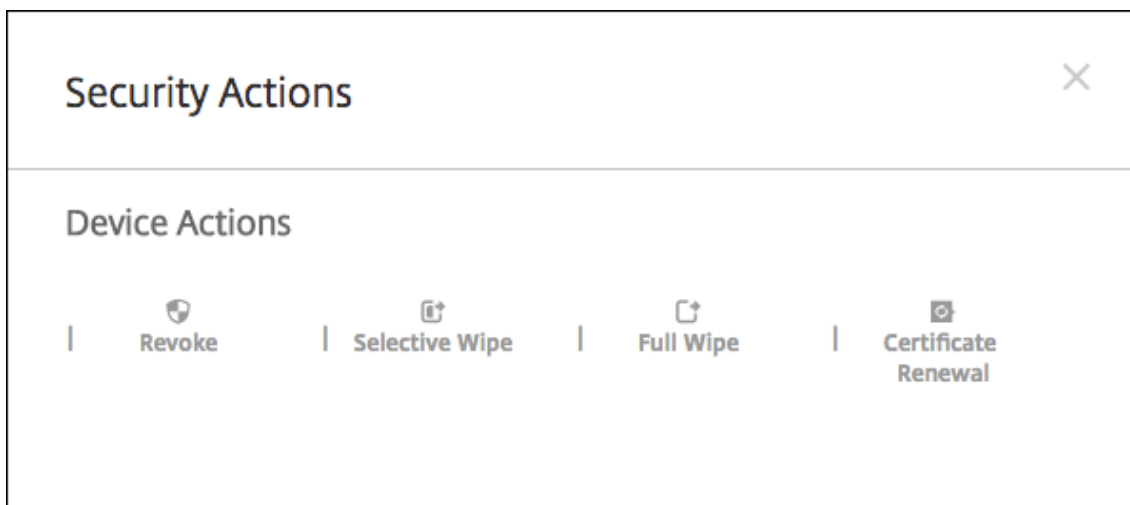
For supported iOS, macOS, and Android devices, you can initiate certificate renewal through the security action, Certificate Renewal. You renew device certificates from the Endpoint Management console or the Public REST API. For enrolled Windows devices, users must re-enroll their devices to receive a new device certificate authority (CA).

The next time that devices connect back to Endpoint Management, the Endpoint Management server issues new device certificates based on the new CA.

### To renew device certificates by using the console

1. Go to **Manage > Devices** and select the devices for which you want to renew device certificates.

2. Click **Secure** and then click **Certificate Renewal**.

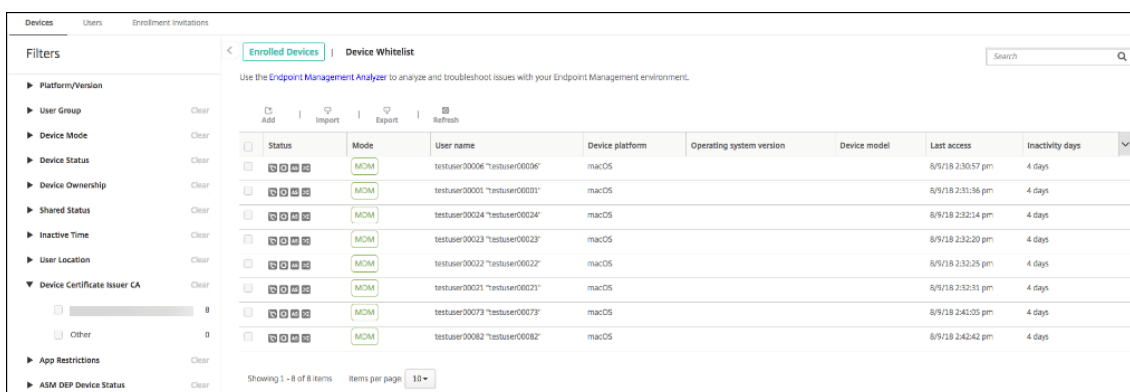


Enrolled devices continue to work without disruption. Endpoint Management issues a device certificate when a device connects back to the server.

To query for the devices that are in a specific device certificate issuer CA group:

1. In **Manage > Devices**, expand the **Filters** pane.
2. In the **Filters** pane, expand **Device Certificate Issuer CA** and then select the issuer CAs that you want to renew.

In the table of devices, the devices for the selected issuer CAs appear.



### To renew device certificates by using the REST API

Endpoint Management uses the following certificate authorities (CAs) internally for PKI: Root CA, device CA, and server CA. Those CAs are a logical group and have a group name. During Endpoint Management provisioning, the server generates three CAs and gives them the group name “default”.

The CA issues the following APIs to manage and renew the device certificates. Already enrolled devices continue to work without disruption. Endpoint Management issues a device certificate when a device

connects back to the server. For more information, download the [Public API for REST Services](#) PDF.

- Return a list of devices still using the old CA (see section 3.16.2 in the Public API for REST Services PDF)
- Renew Device Certificate (see section 3.16.58)
- Get all CA groups (see section 3.23.1)

### **APNs certificate for Citrix Secure Mail**

Apple Push Notification Service (APNs) certificates expire every year. Be sure to create an APNs SSL certificate and update it in the Citrix portal before the certificate expires. If the certificate expires, users face inconsistency with Secure Mail push notifications. Also, you can no longer send push notifications for your apps.

### **APNs certificate for iOS device management**

To enroll and manage iOS devices with Endpoint Management, set up and create an APNs certificate from Apple. If the certificate expires, users cannot enroll in Endpoint Management and you cannot manage their iOS devices. For details, see [APNs certificates](#).

You can view the APNs certificate status and expiration date by logging on to the Apple Push Certificates Portal. Be sure to log on as the same user who created the certificate.

You also receive an email notification from Apple 30 and 10 days before the expiration date. The notification includes the following information:

```
1 The following Apple Push Notification Service certificate, created for
  Apple ID CustomerID will expire on Date. Revoking or allowing this
  certificate to expire will require existing devices to be re-
  enrolled with a new push certificate.
2
3 Please contact your vendor to generate a new request (a signed CSR),
  then visit https://identity.apple.com/pushcert to renew your Apple
  Push Notification Service certificate.
4
5 Thank You,
6
7 Apple Push Notification Service
8 <!--NeedCopy-->
```

### **MDX Toolkit (iOS distribution certificate)**

An app that runs on a physical iOS device (other than apps in the Apple App Store) have these signing requirements:

- Sign the app with a provisioning profile.
- Sign the app with a corresponding distribution certificate.

To verify that you have a valid iOS distribution certificate, do the following:

1. From the Apple Enterprise Developer portal, create an explicit App ID for each app you plan to wrap with MDX. An example of an acceptable App ID is: `com.CompanyName.ProductName`.
2. From the Apple Enterprise Developer portal, go to **Provisioning Profiles > Distribution** and create an in-house provisioning profile. Repeat this step for each App ID created in the previous step.
3. Download all provisioning profiles. For details, see [Wrapping iOS Mobile Apps](#).

To confirm that all Endpoint Management server certificates are valid, do the following:

1. In the Endpoint Management console, click **Settings > Certificates**.
2. Check that all certificates including APNs, SSL Listener, Root, and Intermediate certificate are valid.

### Android keystore

The keystore is a file that contains certificates used to sign your Android app. When your key validity period expires, users can no longer seamlessly upgrade to new versions of your app.

### Enterprise certificate from DigiCert for Windows phones

DigiCert is the exclusive provider of code signing certificates for the Microsoft App Hub service. Developers and software publishers join the App Hub to distribute Windows Phone and Xbox 360 applications for download through the Windows Marketplace. For details, see [DigiCert Code Signing Certificates for Windows Phone](#) in the DigiCert documentation.

If the certificate expires, Windows phone users cannot enroll. The users can't install an app published and signed by the company, or start an installed company app.

### Citrix Gateway

For details on how to handle certificate expiration for Citrix Gateway, see [How to handle certificate expiry on NetScaler](#) in the Citrix Support Knowledge Center.

An expired Citrix Gateway certificate prevents users from enrolling and accessing the Store. The expired certificate also prevents users from connecting to Exchange Server when using Secure Mail. In addition, users cannot enumerate and open HDX apps (depending on which certificate expired).

The Expiry Monitor and Command Center can help you to track your Citrix Gateway certificates. The Center notifies you when the certificate expires. These tools assist to monitor the following Citrix Gateway certificates:

- SSL Certificate for MDM FQDN
- SSL Certificate for Gateway FQDN
- SSL Certificate for ShareFile SZC FQDN
- SSL Certificate for Exchange Load Balancing (offload configuration)
- SSL Certificate for StoreFront Load Balancing
- Root and Intermediate CA Certificates for the preceding certificates

## Citrix Gateway and Endpoint Management

November 17, 2020

When integrated with Endpoint Management, Citrix Gateway provides remote device access to your internal network and resources. Endpoint Management creates a micro VPN from the apps on the device to Citrix Gateway.

You can use the Citrix Gateway service (Preview) or on-premises Citrix Gateway, also known as NetScaler Gateway. For an overview of the two Citrix Gateway solutions, see [Configure Citrix Gateway use with Endpoint Management](#).

### Configure authentication for remote device access to the internal network

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Under **Server**, click **Citrix Gateway**. The **Citrix Gateway** page appears. In the following example, a Citrix Gateway instance exists.

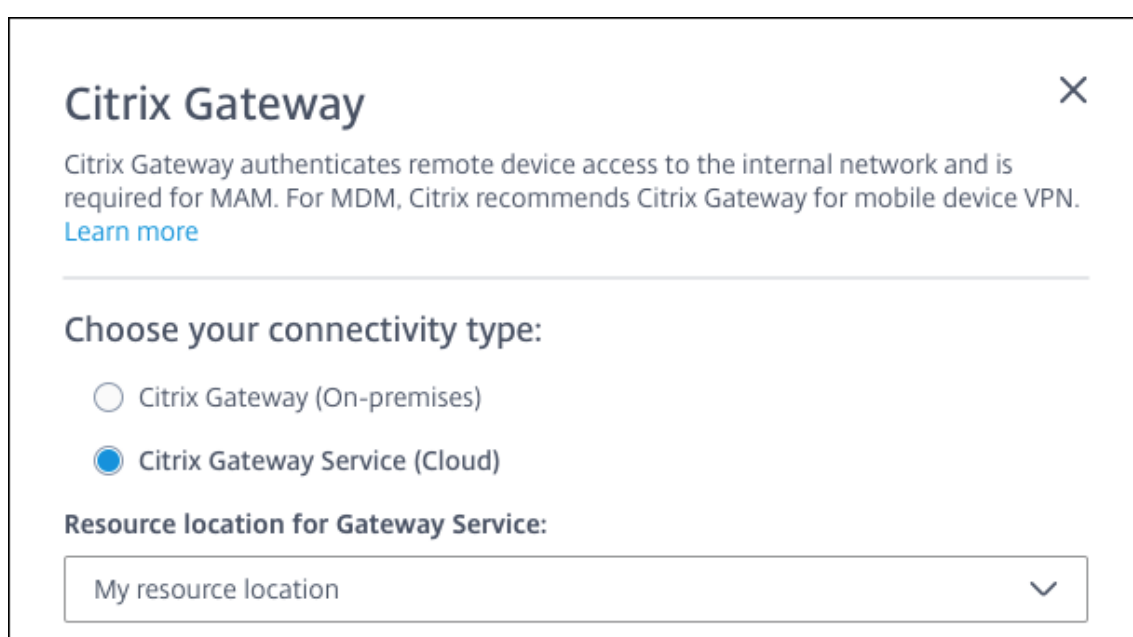
<input type="checkbox"/>	Name	Default	External URL	Logon Type	# of Callback URLs	▼
<input checked="" type="checkbox"/>	testNS	✓	https://testns.domain.com	Domain	0	

3. Configure these settings:
  - **Authentication:** Select whether to enable authentication. The default is **On**.
  - **Deliver user certificate for authentication:** Select whether you want Endpoint Management to share the authentication certificate with Secure Hub. Sharing the certificate enables Citrix Gateway to handle the client certificate authentication. The default is **Off**.
  - **Credential Provider:** In the list, click the credential provider to use. For more information, see [Credential providers](#).
4. Click **Save**.

## Add a Citrix Gateway service instance (Preview)

After you save the authentication settings, you add a Citrix Gateway instance to Endpoint Management.

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page opens.
2. On the **Settings** page, scroll to the Citrix Gateway tile and then click **Start setup**. The **Citrix Gateway** page appears.
3. Select **Citrix Gateway service (cloud)** and specify the resource location for the Gateway service.



- **Resource location for Gateway service:** is required if you use Secure Mail. Specify the resource location for the STA service. The resource location must include a configured Citrix Gateway. If you later want to remove a resource location that's configured for the Gateway service, update this setting.

After you complete those settings, click **Connect** to establish the connection. The new Citrix Gateway is added. The **Citrix Gateway service (cloud)** tile appears on the **Settings** page. To edit an instance, click **See More**. If Gateway Connectors are not available in the selected resource location, click **Add Gateway Connector**. Follow the on-screen guidance to install Gateway Connectors. You can also add Gateway Connectors later.

4. Click **Save and Export Script**.
  - **Save and Export Script.** Click the button to save your settings and export a configuration bundle. You can upload a script from the bundle to Citrix Gateway to configure it with End-



point Management settings. For information, see “Configure an on-premises Citrix Gateway for use with Endpoint Management” after these steps.

You’ve added the new Citrix Gateway. The **Citrix Gateway** tile appears on the **Settings** page. To edit an instance, click **See More**.

## Configure on-premises Citrix Gateway for use with Endpoint Management

To configure an on-premises Citrix Gateway for use with Endpoint Management, you perform the following general steps as detailed in the following sections.

1. Verify that your environment meets the prerequisites.
2. Export the script bundle from the Endpoint Management console.
3. Extract the files from the bundle. If you’re only using classic policies on Citrix Gateway and you’re running Citrix ADC 13.0 or earlier, use the script with “Classic” in the file name. If you’re using any advanced policies or you’re running Citrix ADC 13.1 or later, use the script with “Advanced” in the file name.
4. Run the appropriate script on the Citrix Gateway. See the readme file provided with the scripts for the latest detailed instructions.
5. Test the configuration.

The scripts configure these Citrix Gateway settings required by Endpoint Management:

- Citrix Gateway virtual servers needed for MDM and MAM
- Session policies for the Citrix Gateway virtual servers
- Endpoint Management server details
- Proxy load balancer for certificate validation
- Authentication Policies and Actions for the Citrix Gateway virtual server. The scripts describe the LDAP configuration settings.
- Traffic actions and policies for the proxy server
- Clientless access profile
- Static local DNS record on Citrix Gateway
- Other bindings: Service policy, CA certificate

The scripts don’t handle the following configuration:

- Exchange load balancing
- Citrix Files load balancing
- ICA Proxy configuration
- SSL Offload

## Prerequisites for using the Citrix Gateway configuration scripts

Endpoint Management requirements:

- Complete the LDAP and Citrix Gateway configuration in Endpoint Management before exporting the script bundle. If you change the settings, export the script bundle again.

Citrix Gateway requirements:

- When using certificate-based authentication at the Citrix Gateway, you must create SSL certificates on a Citrix ADC Appliance. See [Create and Use SSL Certificates on a Citrix ADC Appliance](#).
- Citrix Gateway (minimum version 11.0, Build 70.12).
- Citrix Gateway IP address is configured and has connectivity to the LDAP server, unless LDAP is load balanced.
- Citrix Gateway Subnet (SNIP) IP address is configured, has connectivity to the necessary back end servers, and has public network access over port 8443/TCP.
- DNS can resolve public domains.
- Citrix Gateway is licensed with Platform/Universal or Trial licenses. For information, see <https://support.citrix.com/article/CTX126049>.

## Export the script bundle from Endpoint Management

After you save the authentication settings, you add a Citrix Gateway instance to Endpoint Management.

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page opens.
2. On the **Settings** page, scroll to the Citrix Gateway tile and then click **Start setup**. The **Citrix Gateway** page appears.
3. Select **Citrix Gateway (On-premises)** and configure these settings:


## Citrix Gateway ✕

Citrix Gateway authenticates remote device access to the internal network and is required for MAM. For MDM, Citrix recommends Citrix Gateway for mobile device VPN. [Learn more](#)

---

### Choose your connectivity type:

- 1 We recommend that you configure LDAP settings before Citrix Gateway. The script that you export after saving your Gateway configuration must include your LDAP settings.
- 2 Provide the Citrix Gateway details.  
**Name**  
  
**External URL**  
  
**Logon type**  
▼
- 3 Click **Save and Export Script** to save your settings and download a .tar.gz script bundle. The script bundle includes a Readme file with detailed installation instructions.

**Save and Export Script**

- **Name:** Type a name for the Citrix Gateway instance.
- **External URL:** Type the publicly accessible URL for Citrix Gateway. For example, <https://receiver.com>.
- **Logon Type:** Choose a logon type. Types include: **Domain**, **Security token only**, **Domain and security token**, **Certificate**, **Certificate and domain**, and **Certificate and security token**. The default is **Domain**.

If you have multiple domains, use **Certificate and domain**. For more information, see [Configure authentication for multiple domains](#).

Certificate-based authentication at the Citrix Gateway requires extra configuration. For example, you must upload your root CA certificate to your Citrix ADC Appliance. See [Create and Use SSL Certificates on a Citrix ADC Appliance](#).

For more information, see [Authentication](#) in the Deployment Handbook.

4. Click **Save and Export Script**.

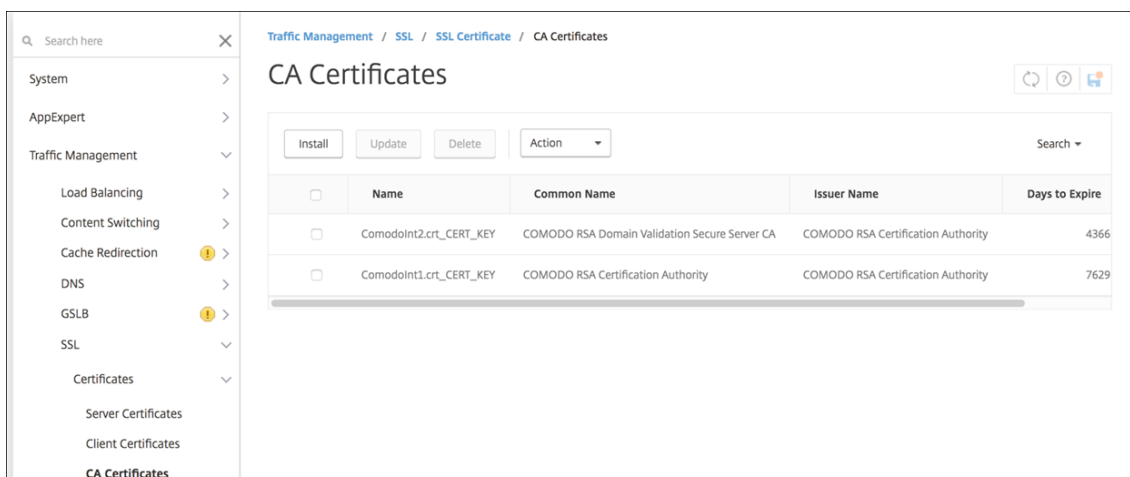
- **Save and Export Script.** Click the button to save your settings and export a configuration bundle. You can upload a script from the bundle to Citrix Gateway to configure it with Endpoint Management settings. For information, see “Configure an on-premises Citrix Gateway for use with Endpoint Management” after these steps.

You’ve added the new Citrix Gateway. The **Citrix Gateway** tile appears on the **Settings** page. To edit an instance, click **See More**.

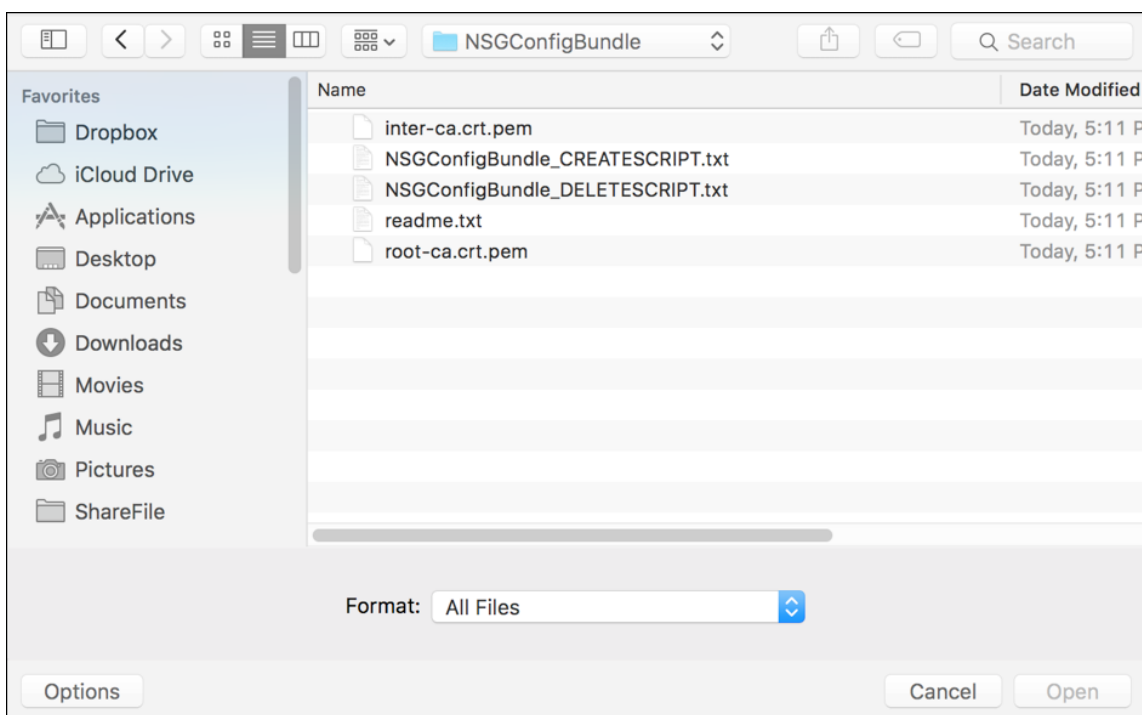
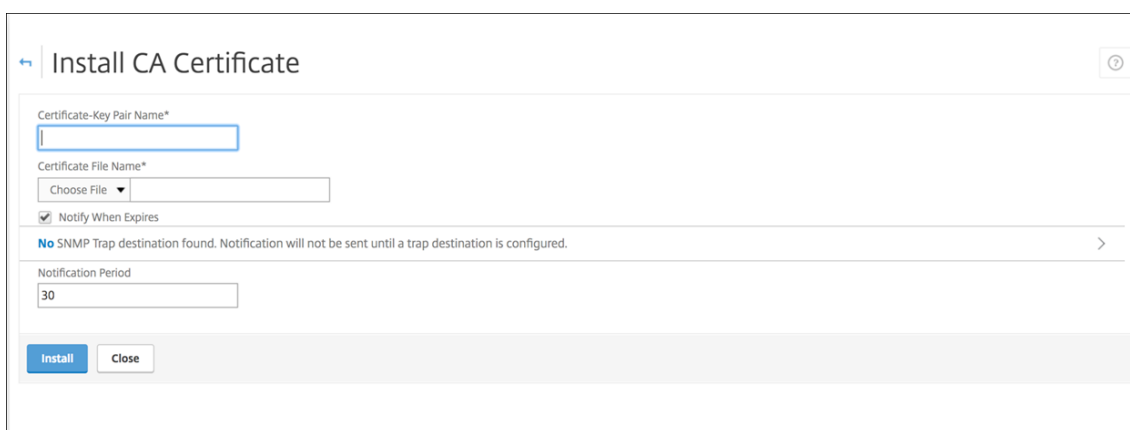
### Install the script in your environment

The script bundle includes the following.

- Readme file with detailed instructions
  - Scripts that contain the NetScaler CLI commands used to configure the required components in NetScaler
  - Public Root CA certificate and the Intermediate CA certificate
  - Scripts that contain the NetScaler CLI commands used to remove the NetScaler configuration
1. Upload and install the certificate files (provided in the script bundle) on the Citrix ADC appliance in the `/nsconfig/ssl/` directory. See [Create and Use SSL Certificates on a Citrix ADC Appliance](#).



The following examples show how to install the root certificate.



	Name	Common Name	Issuer Name	Days to Expire
<input type="checkbox"/>	Comodoint2.crt_CERT_KEY	COMODO RSA Domain Validation Secure Server CA	COMODO RSA Certification Authority	4366
<input type="checkbox"/>	Comodoint1.crt_CERT_KEY	COMODO RSA Certification Authority	COMODO RSA Certification Authority	7629
<input type="checkbox"/>	Citrix Root	Root Certificate Authority	Root Certificate Authority	7659

Ensure that you install both the root and intermediate certificates.

2. Edit the script (ConfigureCitrixGatewayScript\_Classic.txt or ConfigureCitrixGatewayScript\_Advanced.txt) to replace all placeholders with details from your environment.

```
#Important Note: Please update the following placeholders with valid values:
# <NSG_IP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reachable from your devices either directly or via a NAT.
# <PROXY_LB_VIP> -- Virtual IP Address to be assigned to the proxy load-balancer configured on the NetScaler. This IP address must be a private address.
# <LDAP_SVC_USERNAME> -- LDAP Service Account Username.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <SERVER_CERT_NAME> -- Name of the server certificate file on the NetScaler. This certificate is bound to the NetScaler Gateway virtual server.
```

3. Run your edited script in the NetScaler bash shell, as described in the readme file included in the script bundle. For example:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/OfflineNSGConfigtBundle_CREATESCRIPT.txt"
```

```
login as: nsroot
#####
#
#   WARNING: Access to this system is for authorized users only
#   Disconnect IMMEDIATELY if you are not an authorized user!
#
#####

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.

root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

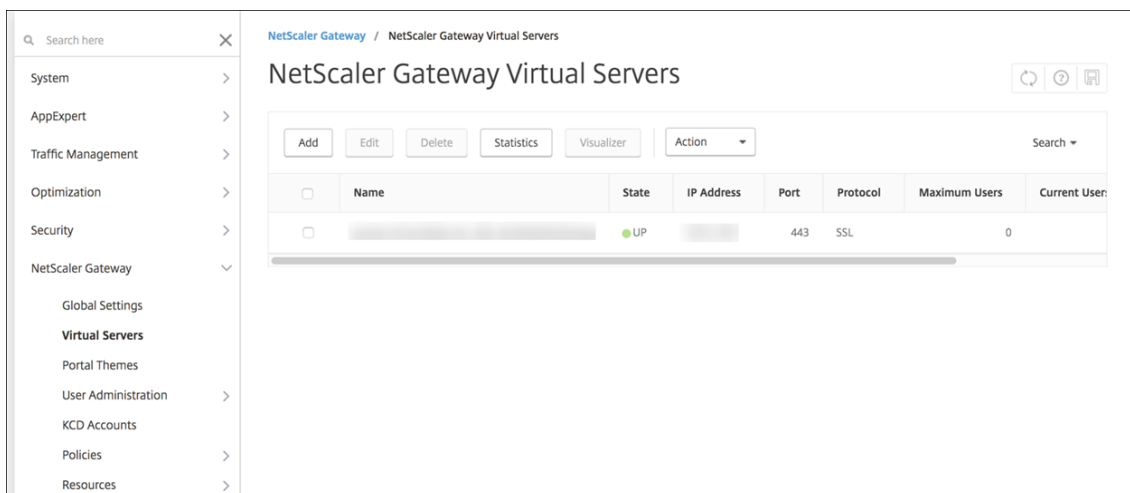
When the script completes, the following lines appear.

```
exec: save ns config
Done
Done
root@ns#
```

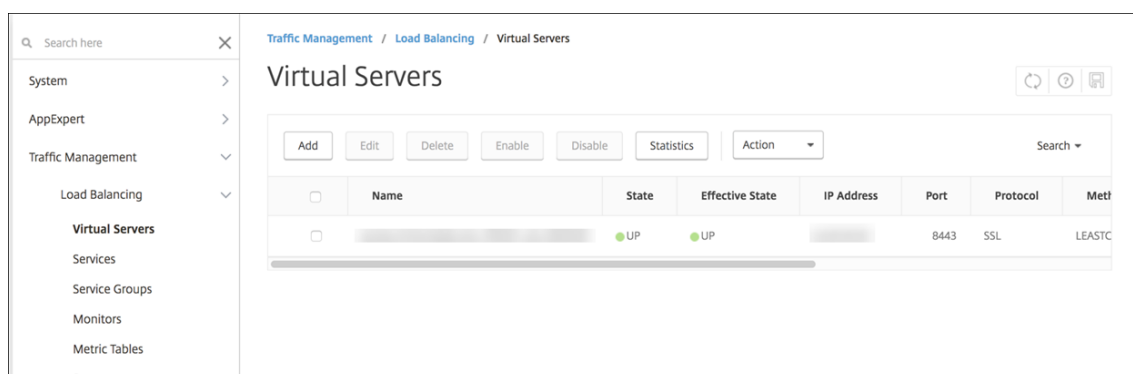
### Test the configuration

To validate the configuration:

1. Validate that Citrix Gateway Virtual Server shows a state of **UP**.



2. Validate that the Proxy Load Balancing Virtual Server shows a state of **UP**.



3. Open a web browser, connect to the Citrix Gateway URL, and attempt to authenticate. If the authentication succeeds, you are redirected to an “HTTP Status 404 - Not Found” message.
4. Enroll a device and ensure it gets both MDM and MAM enrollment.

### Configure authentication for multiple domains

If you have multiple Endpoint Management instances, such as for test, development, and production environments, you configure Citrix Gateway for the additional environments manually. (You can use the NetScaler for XenMobile wizard only one time.)

### Citrix Gateway configuration

To configure Citrix Gateway authentication policies and a session policy for a multi-domain environment:

1. In the Citrix Gateway configuration utility, on the **Configuration** tab, expand **Citrix Gateway > Policies > Authentication**.
2. In the navigation pane, click **LDAP**.
3. Click to edit the LDAP profile. Change the **Server Logon Name Attribute** to **userPrincipalName** or the attribute you want to use for searches. Make a note of the attribute that you specify. You provide it when configuring LDAP settings in the Endpoint Management console.



**Other Settings**

Server Logon Name Attribute

Search Filter

Group Attribute

Sub Attribute Name

4. Repeat those steps for each LDAP policy. A separate LDAP policy is required for each domain.
5. In the session policy bound to the Citrix Gateway virtual server, navigate to **Edit session profile > Published Applications**. Make sure that **Single Sign-On Domain** is blank.

### Endpoint Management configuration

To configure Endpoint Management LDAP for a multi-domain environment:

1. In the Endpoint Management console, go to **Settings > LDAP** and add or edit a directory.

Settings > LDAP

**LDAP**  
 Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Support nested groups  NO

Add

Directory Type	Domain Name	Server:Port	User Base DN	Group Base DN	Default
<input type="checkbox"/> Microsoft Active Directory			dc=,dc=	dc=,dc=	<input checked="" type="checkbox"/>

Showing 1 - 1 of 1 items

2. Provide the information.
  - In **Domain Alias**, specify each domain to use for user authentication. Separate the domains with a comma and don't use spaces between the domains. For example: domain1.com,domain2.com,domain3.com
  - Ensure that the **User search by** field matches the **Server Logon Name Attribute** specified in the Citrix Gateway LDAP policy.

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	Microsoft Active Directory	
Primary server*	10.	
Secondary server	IP Address or FQDN	
Port*	389	
Domain name*	Araujo.local	
User base DN*	dc=,dc=	ⓘ
Group base DN*	dc=,dc=	ⓘ
User ID*	Administrator@	
Password*		
Domain alias*		
XenMobile Lockout Limit	0	ⓘ
XenMobile Lockout Time	1	ⓘ
Global Catalog TCP Port	3268	ⓘ
Global Catalog Root Context	dc=example.dc=com	ⓘ
User search by	userPrincipalName	
Use secure connection	<input type="radio"/> NO	

## Drop inbound connection requests to specific URLs

If the Citrix Gateway in your environment is configured for SSL offload, you might prefer that the gateway drop inbound connection requests for specific URLs. If you prefer that extra security, contact Citrix Cloud Operations and request that they allow your IP to your on-premises data centers.

## Domain or domain plus security token authentication

September 28, 2021

Endpoint Management supports domain-based authentication against one or more directories that are compliant with the Lightweight Directory Access Protocol (LDAP). You configure a connection in Endpoint Management to one or more directories. Endpoint Management uses the LDAP configuration to import groups, user accounts, and related properties.

### Important:

Endpoint Management doesn't support changing the authentication mode from one type of authentication mode to a different authentication mode after users enroll devices in Endpoint Management. For example, you can't change the authentication mode from **Domain authentication** to **Domain + Certificate** after users have enrolled.

## About LDAP

LDAP is an open-source, vendor-neutral application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory information services are used to share information about users, systems, networks, services, and applications available throughout the network.

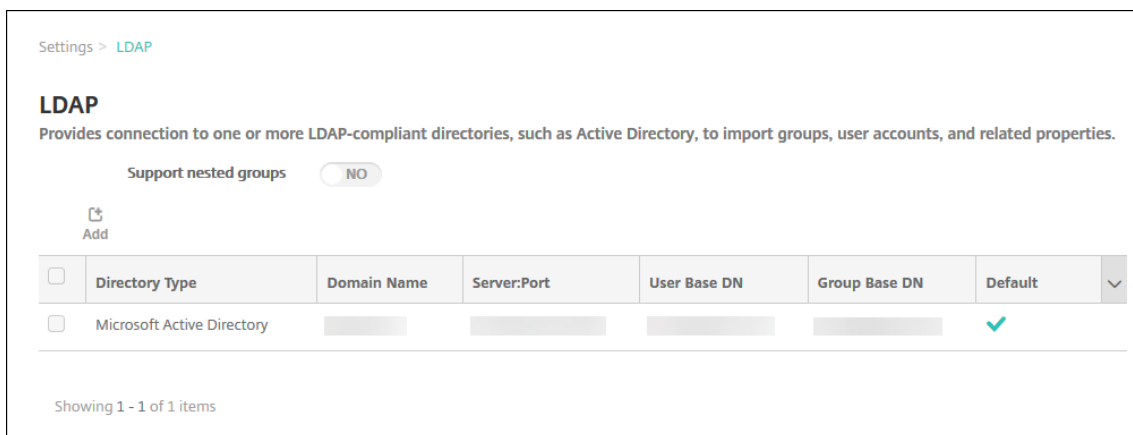
A common usage of LDAP is to provide single sign-on (SSO) for users, where a single password (per user) is shared among multiple services. Single sign-on enables a user to log on one time to a company website, for authenticated access to the corporate intranet.

A client starts an LDAP session by connecting to an LDAP server, known as a Directory System Agent (DSA). The client then sends an operation request to the server, and the server responds with the appropriate authentication.

## To add LDAP connections in Endpoint Management

You typically configure LDAP connections when you onboard to Endpoint Management, as described in [To configure LDAP](#). If you onboarded before the screens shown in that section were available, use the information in this section to add LDAP connections.

1. In the Endpoint Management console, go to **Settings > LDAP**.
2. Under **Server**, click **LDAP**. The **LDAP** page appears.



3. On the **LDAP** page, click **Add**. The **Add LDAP** page appears.

Settings > LDAP > Add LDAP

### Add LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	Microsoft Active Directory	
Primary server*	IP Address or FQDN	
Secondary server	IP Address or FQDN	
Port*	389	
Domain name*		
User base DN*	dc=example,dc=com	?
Group base DN*	dc=example,dc=com	?
User ID*		
Password*		
Domain alias*		
XenMobile Lockout Limit	0	?
XenMobile Lockout Time	1	?
Global Catalog TCP Port	3268	?
Global Catalog Root Context	dc=example,dc=com	?
User search by	userPrincipalName	
Use secure connection	<input type="radio"/> NO	

Cancel Save

#### 4. Configure these settings:

- **Directory type:** In the list, click the appropriate directory type. The default is **Microsoft Active Directory**.
- **Primary server:** Type the primary server used for LDAP; you can enter either the IP address or the fully qualified domain name (FQDN).
- **Secondary server:** Optionally, if a secondary server has been configured, enter the IP address or FQDN for the secondary server. This server is a failover server used if the primary server cannot be reached.
- **Port:** Type the port number used by the LDAP server. By default, the port number is set to **389** for unsecured LDAP connections. Use port number **636** for secure LDAP connections, use **3268** for Microsoft unsecure LDAP connections, or **3269** for Microsoft secure LDAP connections.

- **Domain name:** Type the domain name.
- **User base DN:** Type the location of users in Active Directory through a unique identifier. Syntax examples include: `ou=users`, `dc=example`, or `dc=com`.
- **Group base DN:** Type the location of groups in Active Directory. For example, `cn=users`, `dc=domain`, `dc=net` where `cn=users` represents the container name of the groups and `dc` represents the domain component of Active Directory.
- **User ID:** Type the user ID associated with the Active Directory account.
- **Password:** Type the password associated with the user.
- **Domain alias:** Type an alias for the domain name. If you change the **Domain alias** setting after enrollment, users must re-enroll.
- **Endpoint Management Lockout Limit:** Type a number between **0** and **999** for the number of failed logon attempts. A value of **0** means that Endpoint Management never locks out the user based on failed logon attempts. The default is **0**.

Consider setting this lockout limit to a lower value than your LDAP lockout policy. Doing so helps prevent user lockouts if Endpoint Management is unable to authenticate to the LDAP server. For example, if the LDAP lockout policy is 5 attempts, configure this lockout limit to **4** or lower.

- **Endpoint Management Lockout Time:** Type a number between **0** and **99999** representing the number of minutes a user must wait after exceeding the lockout limit. A value of **0** means that the user isn't forced to wait after a lockout. The default is **1**.
- **Global Catalog TCP Port:** Type the TCP port number for the Global Catalog server. By default, the TCP port number is set to **3268**; for SSL connections, use port number **3269**.
- **Global Catalog Root Context:** Optionally, type the Global Root Context value used to enable a global catalog search in Active Directory. This search is in addition to the standard LDAP search, in any domain without the need to specify the actual domain name.
- **User search by:** Select the format of user name or user ID that Endpoint Management uses to search for users in this directory. Users enter their user name or user ID in this format when enrolling. If you change the **User search by** setting after enrollment, users must re-enroll.

If you choose **userPrincipalName**, users enter a user principal name (UPN) in this format:

– *username@domain*

If you choose **sAMAccountName**, users enter a secure account manager (SAM) name in one of these formats:

– *username@domain*

- *domain\username*

- **Use secure connection:** Select whether to use secure connections. The default is **NO**.

5. Click **Save**.

### To delete an LDAP-compliant directory

1. In the **LDAP** table, select the directory you want to delete.

You can select more than one property to delete by selecting the check box next to each property.

2. Click **Delete**. A confirmation dialog box appears. Click **Delete** again.

### Configure domain plus security token authentication

You can configure Endpoint Management to require users to authenticate with their LDAP credentials plus a one-time password, using the RADIUS protocol.

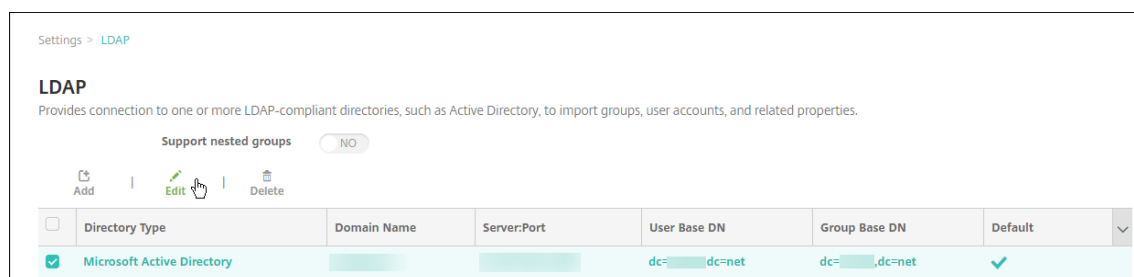
For optimal usability, you can combine this configuration with Citrix PIN and Active Directory password caching. With that configuration, users don't have to enter their LDAP user names and passwords repeatedly. Users enter user names and passwords for enrollment, password expiration, and account lockout.

### Configure LDAP settings

Use of LDAP for authentication requires that you install an SSL certificate from a Certificate Authority on Endpoint Management. For information, see [Upload certificates](#).

1. In **Settings**, click **LDAP**.

2. Select **Microsoft Active Directory** and then click **Edit**.



3. Verify that the Port is **636**, which is for secure LDAP connections, or **3269** for Microsoft secure LDAP connections.

4. Change **Use secure connection** to **Yes**.

Port\* 636

Domain name\*

User base DN\*

Group base DN\*

User ID\*

Password\*

Domain alias\* .net

XenMobile Lockout Limit 0

XenMobile Lockout Time 1

Global Catalog TCP Port 3269

Global Catalog Root Context dc=example.dc=com

User search by userPrincipalName

Use secure connection YES

Cancel Save

### Configure Citrix Gateway settings

The following steps assume that you already have added a Citrix Gateway instance to Endpoint Management. To add a Citrix Gateway instance, see [Citrix Gateway and Endpoint Management](#).

1. In **Settings**, click **Citrix Gateway**.
2. Select the Citrix Gateway and then click **Edit**.
3. From **Logon Type**, select **Domain and security token**.

### Enable Citrix PIN and user password caching

To enable Citrix PIN and user password caching, go to **Settings > Client Properties** and select these check boxes: **Enable Citrix PIN Authentication** and **Enable User Password Caching**. For more information, see [Client properties](#).

### Configure Citrix Gateway for domain and security token authentication

Configure Citrix Gateway session profiles and policies for your virtual servers used with Endpoint Management. For information, see the Citrix Gateway documentation.

## Client certificate or certificate plus domain authentication

May 19, 2021

The default configuration for Endpoint Management is user name and password authentication. To add another layer of security for enrollment and access to Endpoint Management environment, consider using certificate-based authentication. In the Endpoint Management environment, this configuration is the best combination of security and user experience. Certificate plus domain authentication has the best SSO possibilities coupled with security provided by two-factor authentication at Citrix Gateway.

For optimal usability, you can combine certificate plus domain authentication with Citrix PIN and Active Directory password caching. As a result, users don't have to enter their LDAP user names and passwords repeatedly. Users enter user names and passwords for enrollment, password expiration, and account lockout.

### **Important:**

Endpoint Management doesn't support changing the authentication mode from domain authentication to some other authentication mode after users enroll devices in Endpoint Management.

If you don't allow LDAP and use smart cards or similar methods, configuring certificates allows you to represent a smart card to Endpoint Management. Users then enroll using a unique PIN that Endpoint Management generates for them. After a user has access, Endpoint Management then creates and deploys the certificate used to authenticate to the Endpoint Management environment.

You can use the NetScaler for XenMobile wizard to perform the configuration required for Endpoint Management when using Citrix Gateway certificate-only authentication or certificate plus domain authentication. You can run the NetScaler for XenMobile wizard one time only.

In highly secure environments, usage of LDAP credentials outside of an organization in public or insecure networks is considered a prime security threat for the organization. For highly secure environments, two-factor authentication that uses a client certificate and a security token is an option. For information, see [Configuring Endpoint Management for Certificate and Security Token Authentication](#).

Client certificate authentication is available for devices enrolled in MAM and MDM+MAM. To use client certificate authentication for those devices, you must configure the Microsoft server, Endpoint Management, and then Citrix Gateway. Follow these general steps, as described in this article.

On the Microsoft server:

1. Add a certificate snap-in to the Microsoft Management Console.
2. Add the template to Certificate Authority (CA).
3. Create a PFX certificate from the CA server.



On Endpoint Management:

1. Upload the certificate to Endpoint Management.
2. Create the PKI entity for certificate-based authentication.
3. Configure credentials providers.
4. Configure Citrix Gateway to deliver a user certificate for authentication.

For information about Citrix Gateway configuration, see these articles in the Citrix ADC documentation:

- [Client authentication](#)
- [SSL profile infrastructure](#)
- [Configuring and Binding a Client Certificate Authentication Policy](#).

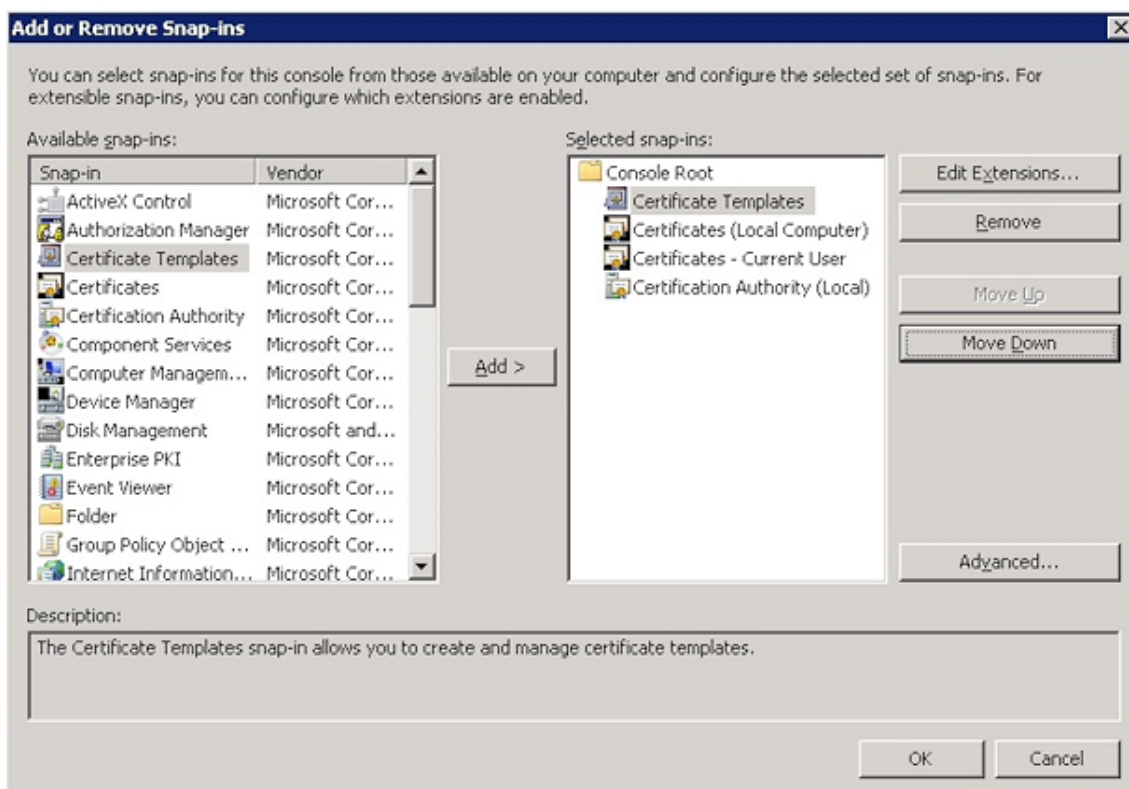
## Prerequisites

- When you create a Microsoft Certificate Services Entity template, avoid possible authentication issues with enrolled devices by excluding special characters. For example, don't use these characters in the template name: : ! \$ ( ) ## % + \* ~ ? | { } []
- To configure Certificate-based Authentication for Exchange ActiveSync, see the [Microsoft documentation on Exchange Server](#). Configure the certificate authority (CA) server site for Exchange ActiceSync to require client certificates.
- If you use private server certificates to secure the ActiveSync traffic to the Exchange Server, ensure that the mobile devices have all of the Root/Intermediate certificates. Otherwise, certificate-based authentication fails during the mailbox setup in Secure Mail. In the Exchange IIS Console, you must:
  - Add a website for Endpoint Management use with Exchange and bind the web server certificate.
  - Use port 9443.
  - For that website, you must add two applications, one for "Microsoft-Server-ActiveSync" and one for "EWS". For both of those applications, under **SSL Settings**, select **Require SSL**.

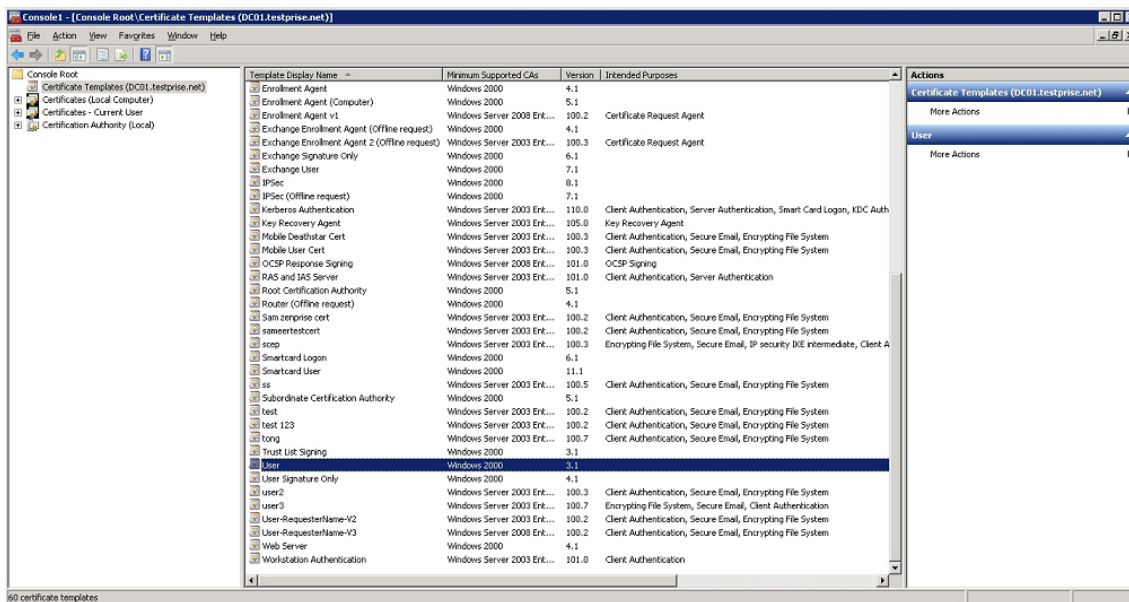
## Add a certificate snap-in to the Microsoft Management Console

1. Open the console and then click **Add/Remove Snap-ins**.
2. Add the following snap-ins:
  - Certificate Templates
  - Certificates (Local Computer)
  - Certificates - Current User

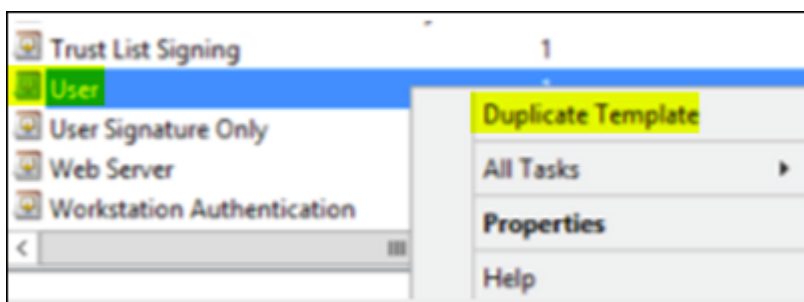
- Certificate Authority (Local)



3. Expand **Certificate Templates**.



4. Select the **User** template and **Duplicate Template**.



5. Provide the Template display name.

**Important:**

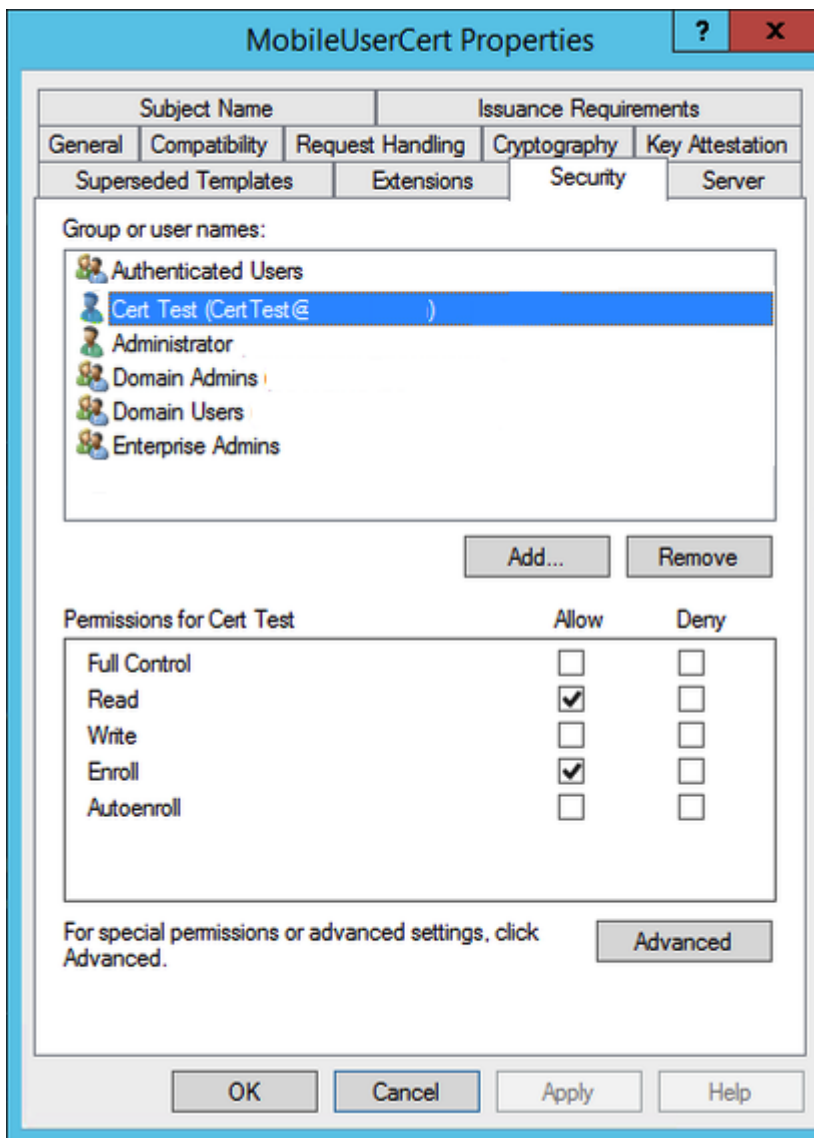
Select the **Publish certificate in Active Directory** check box only if necessary. If this option is selected, all user client certificates are created in Active Directory, which might clutter your Active Directory database.

6. Select **Windows 2003 Server** for the template type. In Windows 2012 R2 server, under **Compatibility**, select **Certificate authority** and set the recipient as **Windows 2003**.
7. Under **Security**, click **Add** and then select the AD user account that Endpoint Management will use to generate certificates.

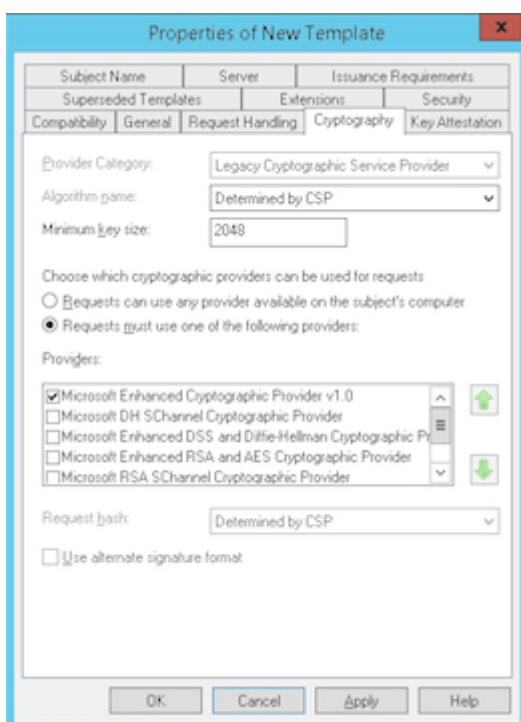
**Important:**

Add only the service account user here. Add the **Enroll** permission only to this AD user account.

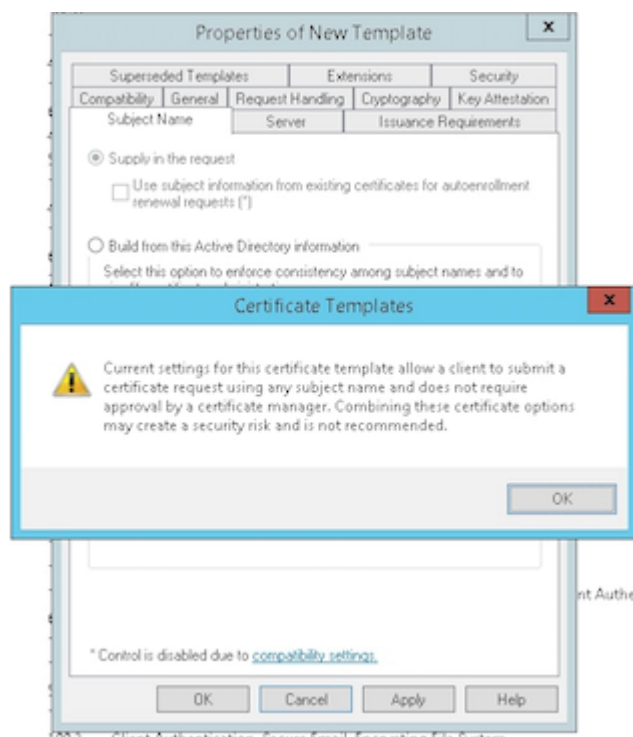
As described later in this article, you will create a user .pfx certificate using the service account. For information, see [Creating a PFX certificate from the CA server](#).



- Under **Cryptography**, ensure that you provide the key size. You later enter the key size during Endpoint Management configuration.



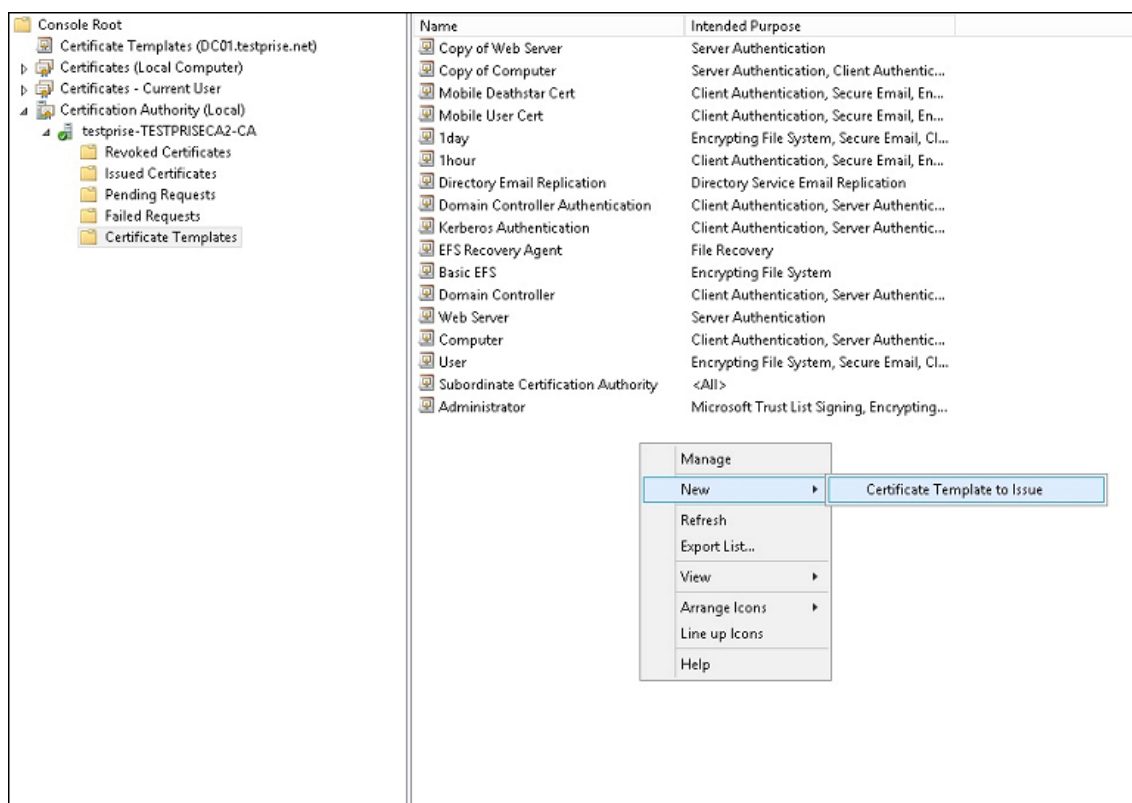
9. Under **Subject Name**, select **Supply in the request**. Apply the changes and then save.



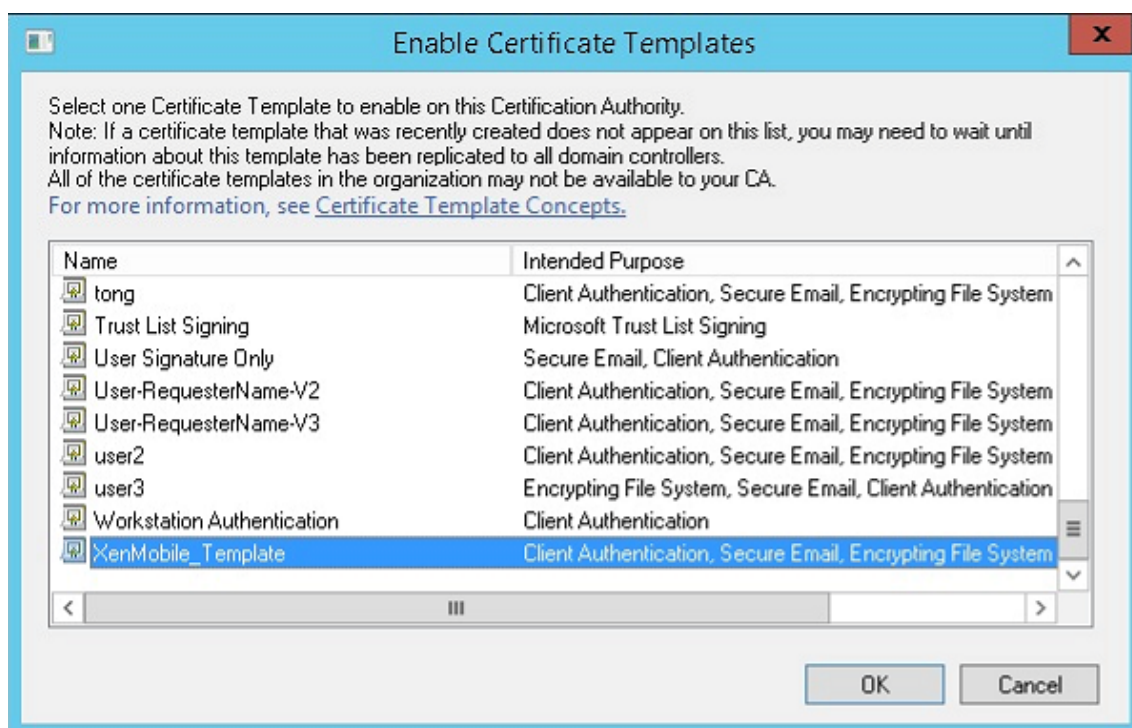
## Adding the template to Certificate Authority

1. Go to **Certificate Authority** and select **Certificate Templates**.

2. Right-click in the right pane and then select **New > Certificate Template to Issue**.

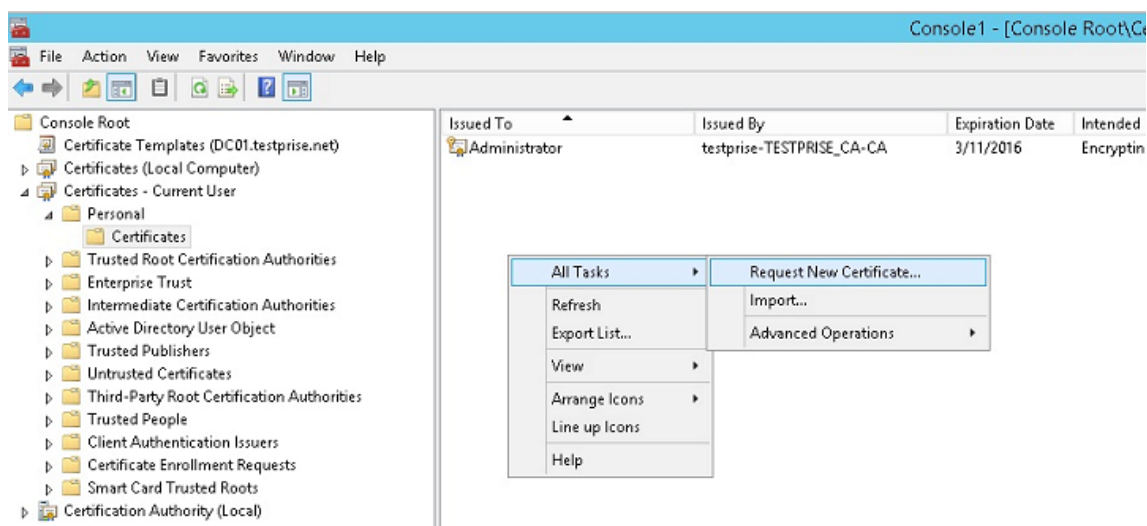


3. Select the template you created in the previous step and then click **OK** to add it into the **Certificate Authority**.

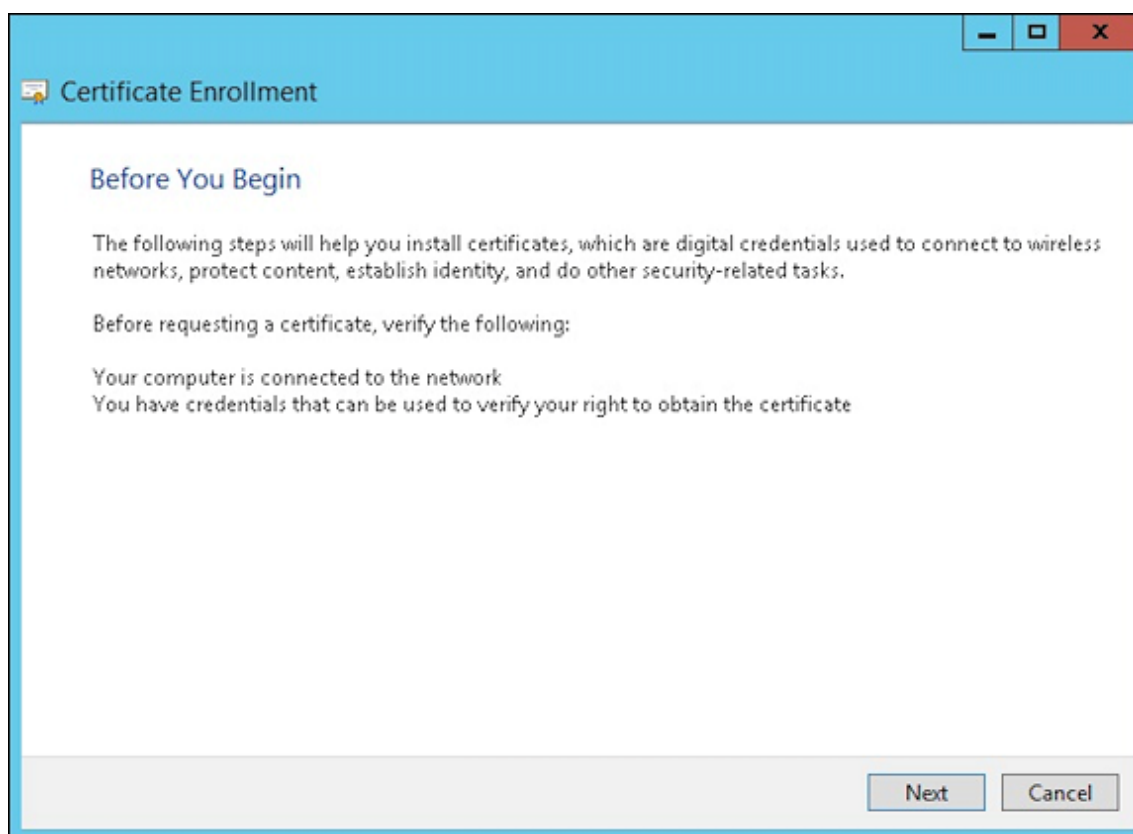


## Creating a PFX certificate from the CA server

1. Create a user .pfx cert using the service account with which you logged in. The .pfx uploads to Endpoint Management, which then requests a user certificate on behalf of the users who enroll their devices.
2. Under **Current User**, expand **Certificates**.
3. Right-click in the right pane and then click **Request New Certificate**.

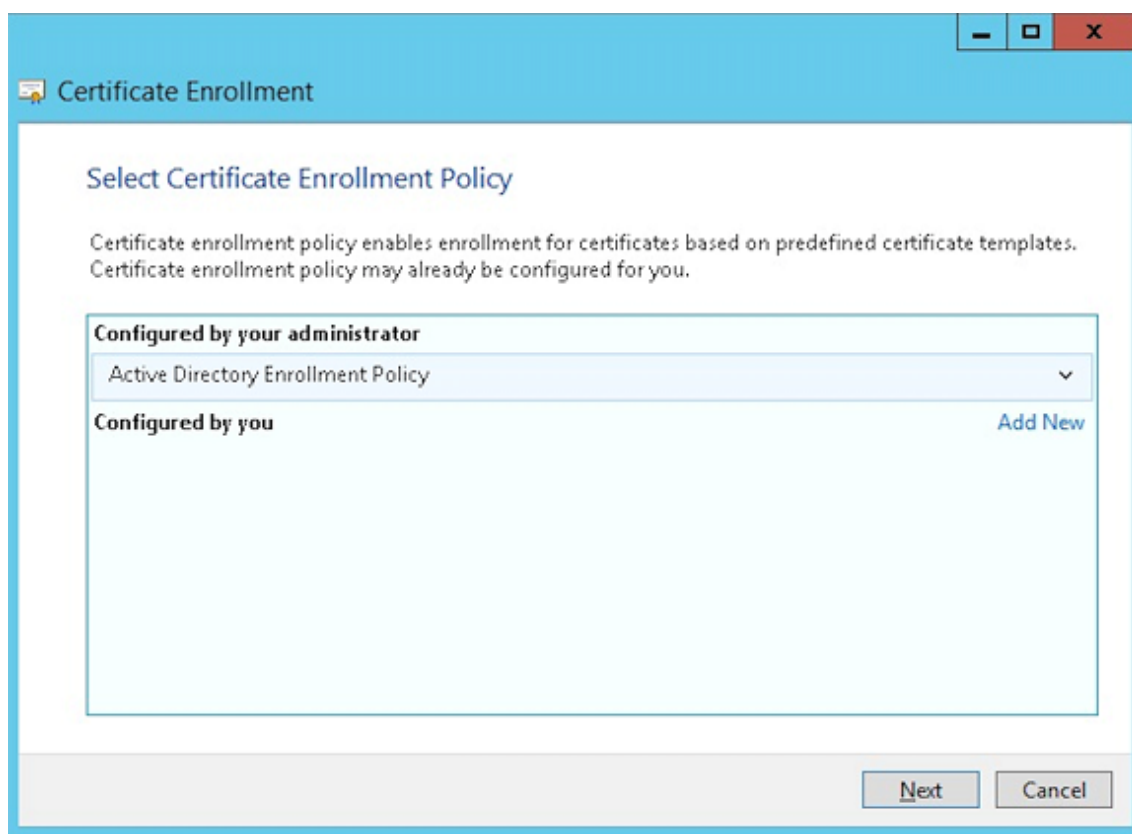


4. The **Certificate Enrollment** screen appears. Click **Next**.

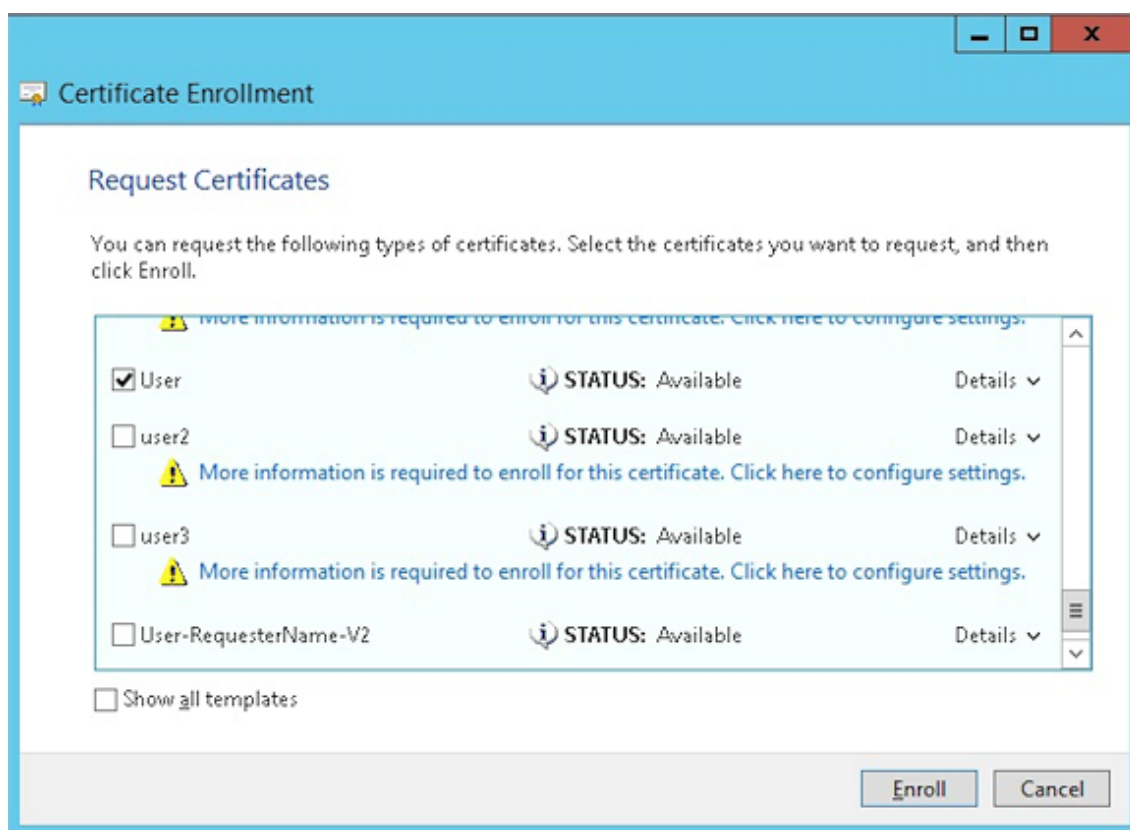


5. Select **Active Directory Enrollment Policy** and then click **Next**.

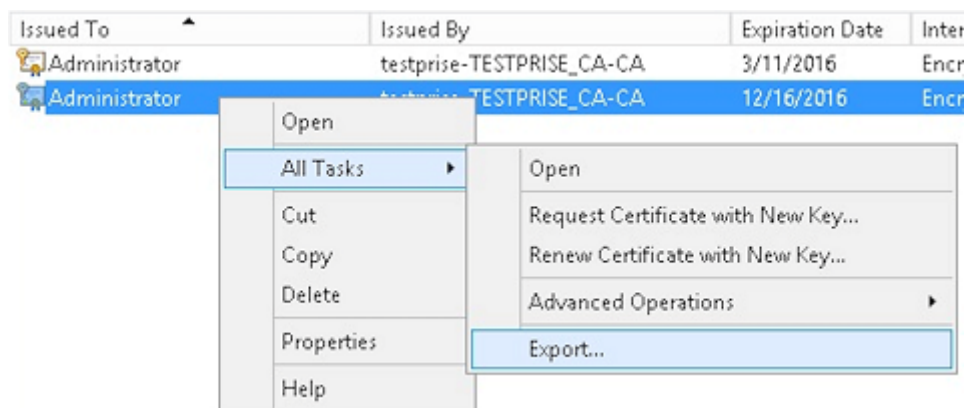




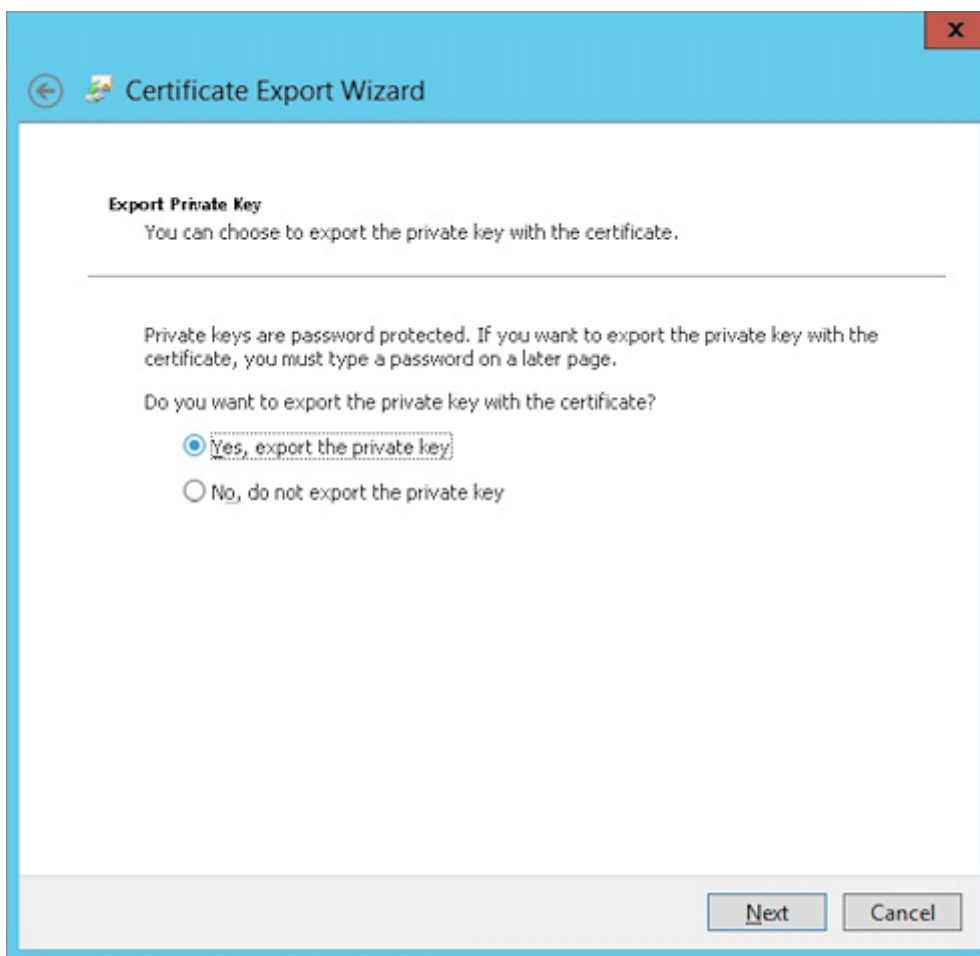
6. Select the **User** template and then click **Enroll**.



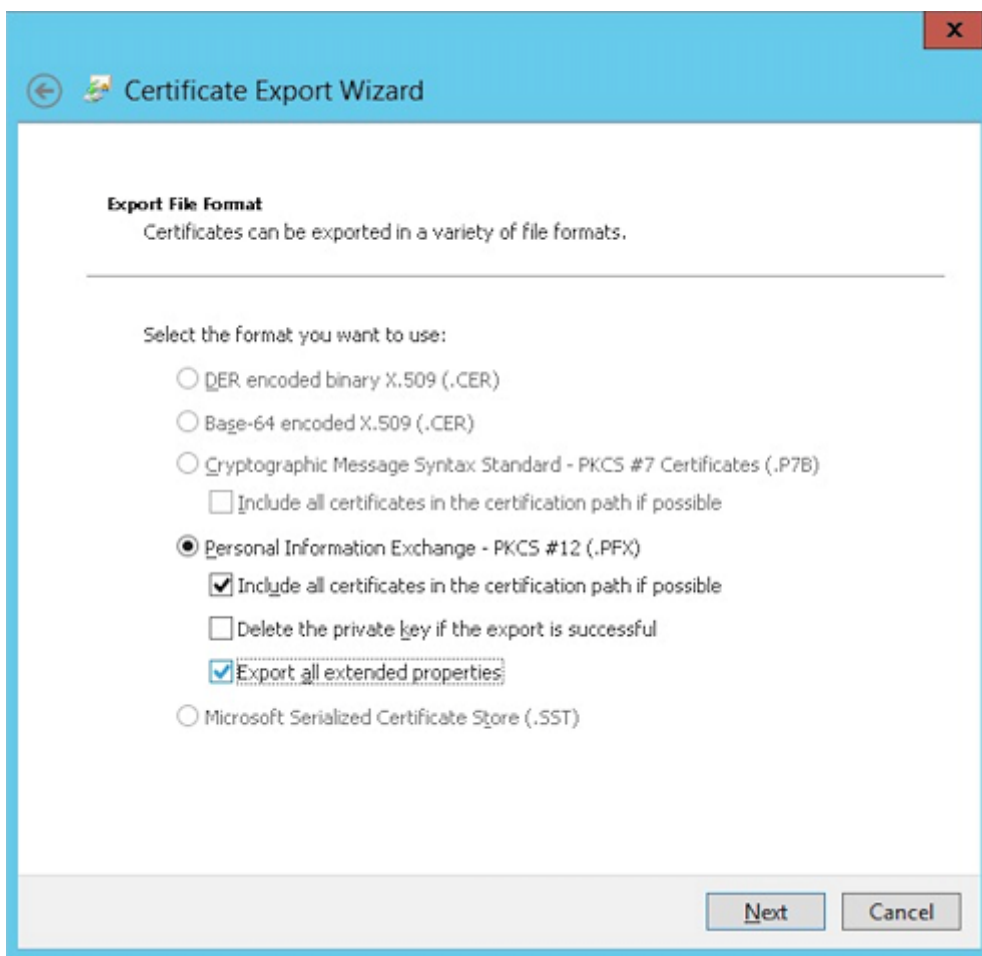
- Export the .pfx file that you created in the previous step.



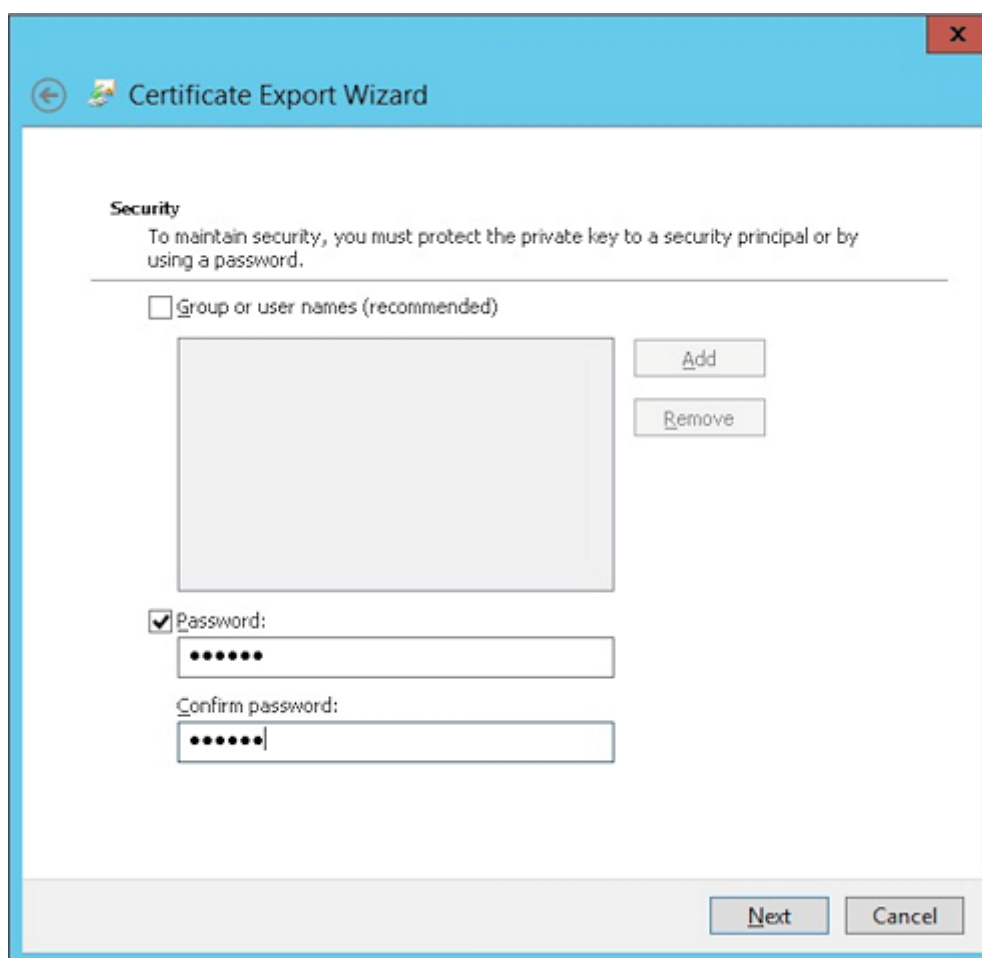
- Click **Yes, export the private key**.



9. Select **Include all certificates in the certification path if possible** and select the **Export all extended properties** check box.



10. Set a password to use when uploading this certificate into Endpoint Management.



11. Save the certificate onto your hard drive.

## Uploading the certificate to Endpoint Management

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** screen appears.
2. Click **Certificates** and then click **Import**.
3. Enter the following parameters:
  - **Import:** Keystore
  - **Keystore type:** PKCS #12
  - **Use as:** Server
  - **Keystore file:** Click Browse to select the .pfx certificate you just created.
  - **Password:** Enter the password you created for this certificate.

### Import ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time. Use the [APNs portal](#) on the Endpoint Management Tools page to create the APNs certificate.

Import Keystore

Keystore type PKCS#12

Use as Server

Keystore file \*  Browse

Password \*

Description

Cancel Import

4. Click **Import**.
5. Verify that the certificate installed correctly. A correctly installed certificate displays as a User certificate.

### Creating the PKI entity for certificate-based authentication

1. In **Settings**, go to **More > Certificate Management > PKI Entities**.
2. Click **Add** and then click **Microsoft Certificate Services Entity**. The **Microsoft Certificate Services Entity: General Information** screen appears.
3. Enter the following parameters:
  - **Name:** Type any name.
  - **Web enrollment service root URL:** `https://RootCA-URL/certsrv/` (Be sure to add the last slash, /, in the URL path.)
  - **certnew.cer page name:** certnew.cer (default value)
  - **certfnsh.asp:** certfnsh.asp (default value)
  - **Authentication type:** Client certificate

- **SSL client certificate:** Select the user certificate to be used to issue the Endpoint Management client certificate. If no certificate exists, follow the procedure in the preceding section to upload certificates.

Settings > PKI Entities > Microsoft Certificate Services Entity

**Microsoft Certificate Services Entity**

1 General  
2 Templates  
3 HTTP Parameters  
4 CA Certificates

**Microsoft Certificate Services Entity: General Information**

Name\* test

Web enrollment service root URL\*

certnew.cer page name\* certnew.cer ⓘ

certfnsh.asp\* certfnsh.asp ⓘ

Authentication type Client certificate ⓘ

SSL client certificate Select an option

Import SSL certificate

4. Under **Templates**, add the template that you created when configuring the Microsoft certificate. Don't add spaces.

**Microsoft Certificate Services Entity**

1 General  
2 Templates  
3 HTTP Parameters  
4 CA Certificates

**Microsoft Certificate Services Entity: Templates**

Specify the internal names of the templates your Microsoft CA supports. Every Credential Provider using this entity uses exactly one such template. When creating the provider, you will be prompted to select from the list defined here.

Templates

Templates*	Add
XVTemplate	

5. Skip HTTP Parameters and then click **CA Certificates**.
6. Select the root CA name that corresponds to your environment. This root CA is part of the chain imported from the Endpoint Management client certificate.

**Microsoft Certificate Services Entity**

1 General  
2 Templates  
3 HTTP Parameters  
4 CA Certificates

**Microsoft Certificate Services Entity: CA Certificates**

Indicate the certificates you want to use for this entity by selecting or clearing the check boxes. An entity is only valid when you select at least one certificate. Add all CA certificates that might be signers of certificates returned by this entity. Although entities may return certificates signed by different CAs, all certificates obtained through a given credential provider must be signed by the same CA. Accordingly, you will have to select one of the certificates configured here in the Distribution page of the Credential Provider setting.

<input type="checkbox"/>	Name	Serial number	Valid from	Valid to
<input checked="" type="checkbox"/>	training-AD-CA		02/22/2013	02/22/2023

7. Click **Save**.

## Configuring credentials providers

1. In **Settings**, go to **More > Certificate Management > Credential Providers**.
2. Click **Add**.
3. Under **General**, enter the following parameters:
  - **Name:** Type any name.

- **Description:** Type any description.
- **Issuing entity:** Select the PKI entity created earlier.
- **Issuing method:** SIGN
- **Templates:** Select the template added under the PKI entity.

Credential Providers	Credential Providers: General Information
1 General	<p>You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for the certificate renewal or revocation, if any.</p> <p><b>Name*</b> XenMobile_PKI</p> <p><b>Description</b> XenMobile PKI Configuration</p> <p><b>Issuing entity</b> MS PKI</p> <p><b>Issuing method</b> SIGN</p> <p><b>Templates</b> XMTemplate</p>
2 Certificate Signing Request	
3 Distribution	
4 Revocation XenMobile	
5 Revocation PKI	
6 Renewal	

4. Click **Certificate Signing Request** and then enter the following parameters:

- **Key algorithm:** RSA
- **Key size:** 2048
- **Signature algorithm:** SHA256withRSA
- **Subject name:** cn=\$user.username

For **Subject Alternative Names**, click **Add** and then enter the following parameters:

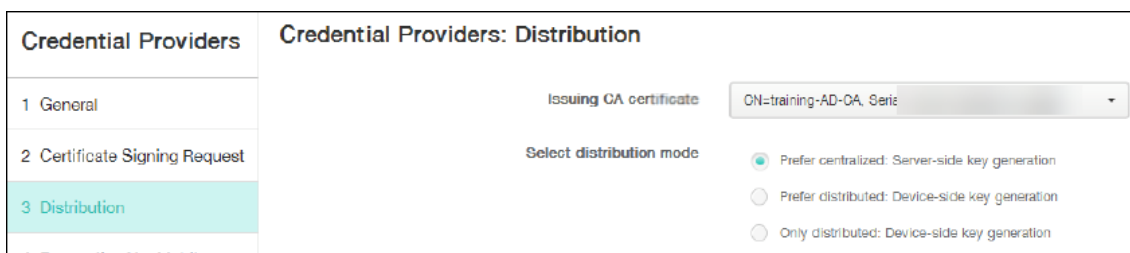
- **Type:** User Principal name
- **Value:** \$user.userprincipalname

Credential Providers	Credential Providers: Certificate Signing Request						
1 General	<p>Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.</p> <p><b>Key algorithm</b> RSA</p> <p><b>Key size*</b> 2048</p> <p><b>Signature algorithm</b> SHA1withRSA</p> <p><b>Subject name*</b> cn=\$user.username</p> <p>Subject alternative names</p> <table border="1"> <thead> <tr> <th>Type</th> <th>Value*</th> <th>Add</th> </tr> </thead> <tbody> <tr> <td>User Principal name</td> <td>\$user.userprincipalname</td> <td></td> </tr> </tbody> </table>	Type	Value*	Add	User Principal name	\$user.userprincipalname	
Type		Value*	Add				
User Principal name		\$user.userprincipalname					
2 Certificate Signing Request							
3 Distribution							
4 Revocation XenMobile							
5 Revocation PKI							
6 Renewal							

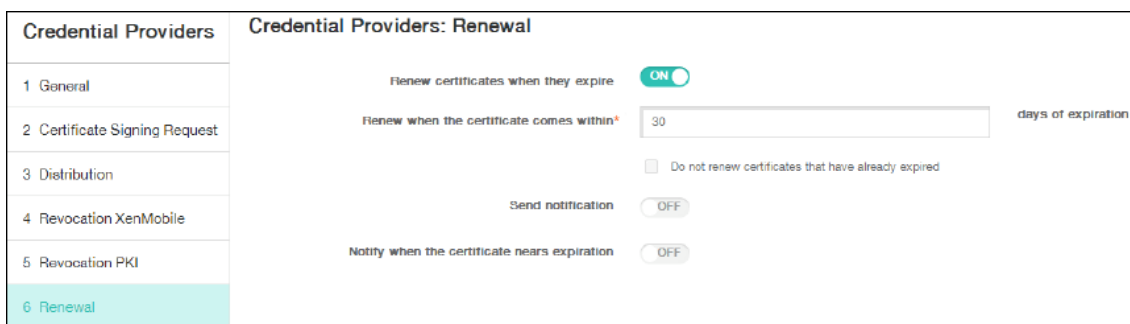
5. Click **Distribution** and enter the following parameters:

- **Issuing CA certificate:** Select the Issuing CA that signed the Endpoint Management Client Certificate.
- **Select distribution mode:** Select **Prefer centralized: Server-side key generation.**





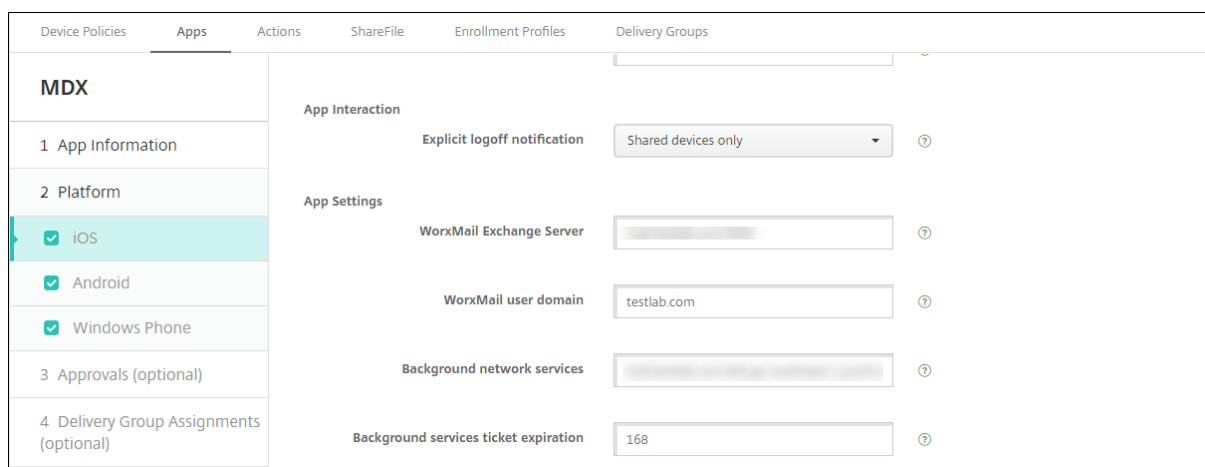
6. For the next two sections, **Revocation Endpoint Management** and **Revocation PKI**, set the parameters as required. In this example, both options are skipped.
7. Click **Renewal**.
8. Enable **Renew certificates when they expire**.
9. Leave all other settings as default or change them as required.



10. Click **Save**.

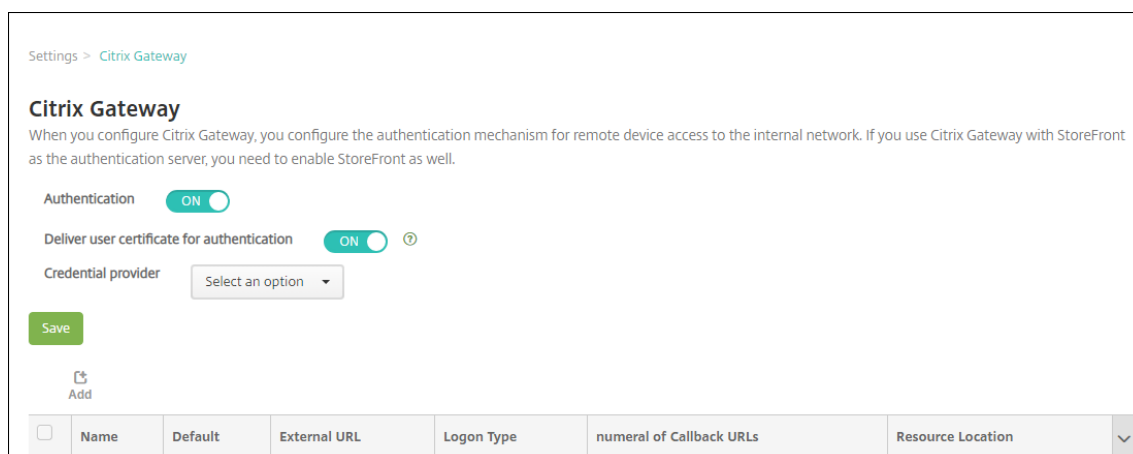
### Configuring Secure Mail to use certificate-based authentication

When you add Secure Mail to Endpoint Management, be sure to configure the Exchange settings under **App Settings**.



## Configuring Citrix Gateway certificate delivery in Endpoint Management

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** screen appears.
2. Under **Server**, click **Citrix Gateway**.
3. If Citrix Gateway isn't already added, click **Add** and specify the settings:
  - **Name:** A descriptive name for the appliance.
  - **Alias:** An optional alias for the appliance.
  - **External URL:** <https://YourCitrixGatewayURL>
  - **Logon Type:** Select **Certificate and domain**
  - **Password Required:** Off
  - **Set as Default:** On
4. For **Authentication** and **Deliver user certificate for authentication**, select **On**.



Settings > Citrix Gateway

### Citrix Gateway

When you configure Citrix Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use Citrix Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

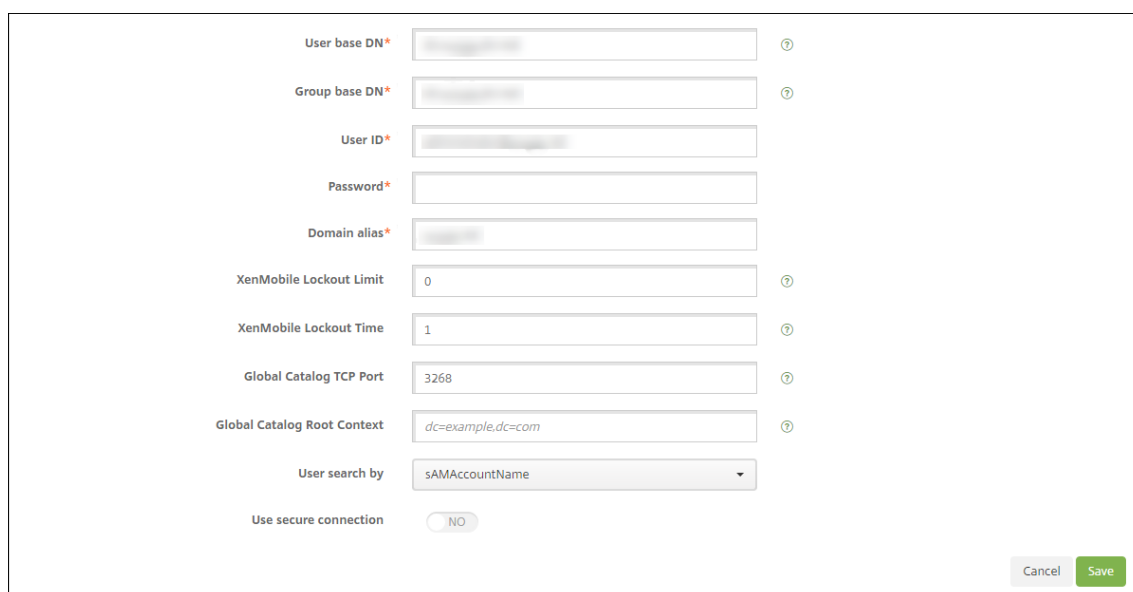
Authentication  ON

Deliver user certificate for authentication  ON ⓘ

Credential provider

<input type="checkbox"/>	Name	Default	External URL	Logon Type	numeral of Callback URLs	Resource Location
--------------------------	------	---------	--------------	------------	--------------------------	-------------------

5. For **Credential Provider**, select a provider and then click **Save**.
6. To use sAMAccount attributes in the user certificates as an alternative to User Principal Name (UPN), configure the LDAP connector in Endpoint Management as follows: Go to **Settings > LDAP**, select the directory and click **Edit**, and select **sAMAccountName** in **User search by**.



The screenshot shows a configuration form with the following fields and values:

- User base DN\*: [Redacted]
- Group base DN\*: [Redacted]
- User ID\*: [Redacted]
- Password\*: [Redacted]
- Domain alias\*: [Redacted]
- XenMobile Lockout Limit: 0
- XenMobile Lockout Time: 1
- Global Catalog TCP Port: 3268
- Global Catalog Root Context: dc=example.dc=com
- User search by: sAMAccountName
- Use secure connection: NO

Buttons: Cancel, Save

### Enable Citrix PIN and user password caching

To enable Citrix PIN and user password caching, go to **Settings > Client Properties** and select these check boxes: **Enable Citrix PIN Authentication** and **Enable User Password Caching**. For more information, see [Client properties](#).

### Creating an Enterprise Hub policy for Windows Phone

For Windows Phone devices, you must create an Enterprise Hub device policy to deliver the AETX file and the Secure Hub client.

#### Note:

Ensure that the AETX and Secure Hub files both use the:

- Same enterprise certificate from the certificate provider.
- Same Publisher ID from the Windows Store developer account.

1. In the Endpoint Management console, click **Configure > Device Policies**.
2. Click **Add** and then, under **More > Endpoint Management Agent**, click **Enterprise Hub**.
3. After naming the policy, be sure to select the correct .AETX file and signed Secure Hub app for the Enterprise Hub.

Device Policies   Apps   Actions   ShareFile   Enrollment Profiles   Delivery Groups

### Enterprise Hub Policy

- 1 Policy Info
- 2 Platforms
- Windows Phone
- 3 Assignment

#### Policy Information

To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe).

Upload .aetx file

Upload signed Enterprise Hub app

4. Assign the policy to delivery groups and save it.

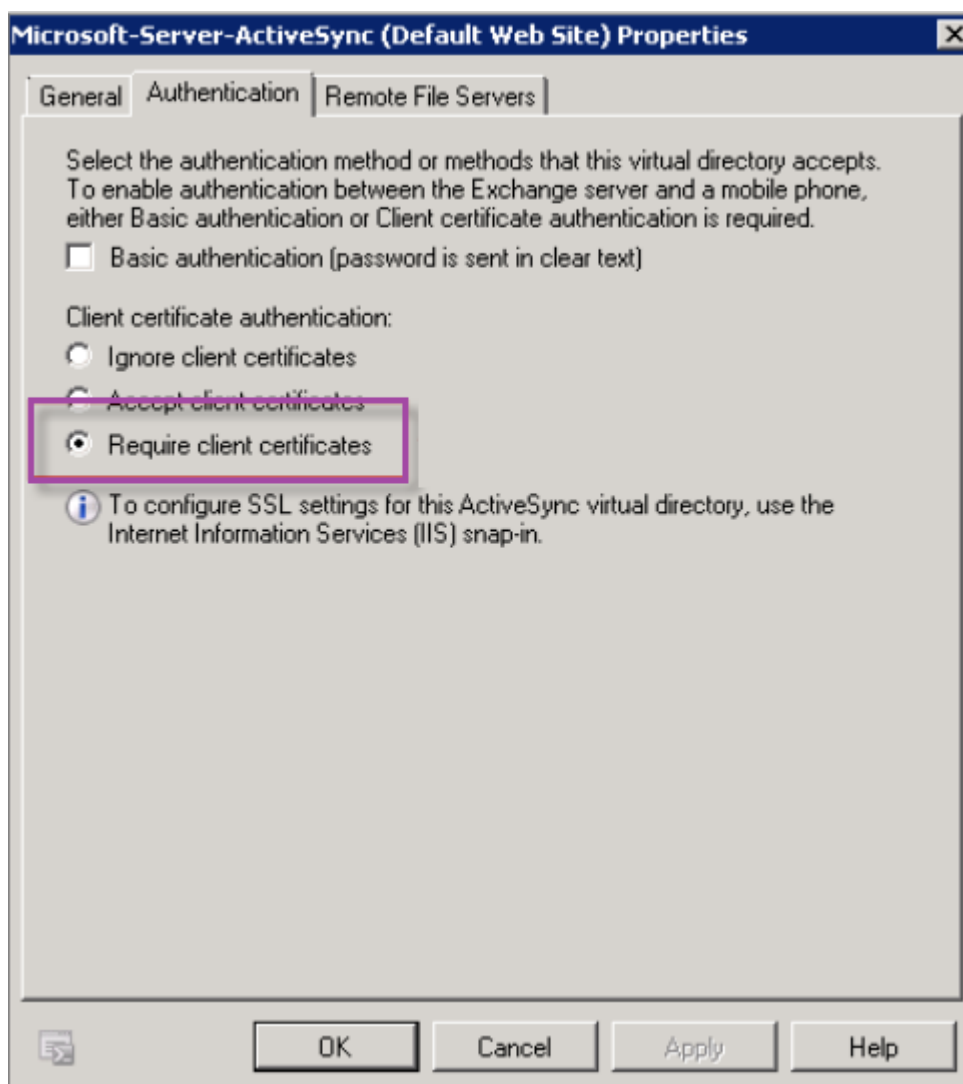
### Troubleshooting your client certificate configuration

After a successful configuration of the preceding configuration plus the Citrix Gateway configuration, the user workflow is as follows:

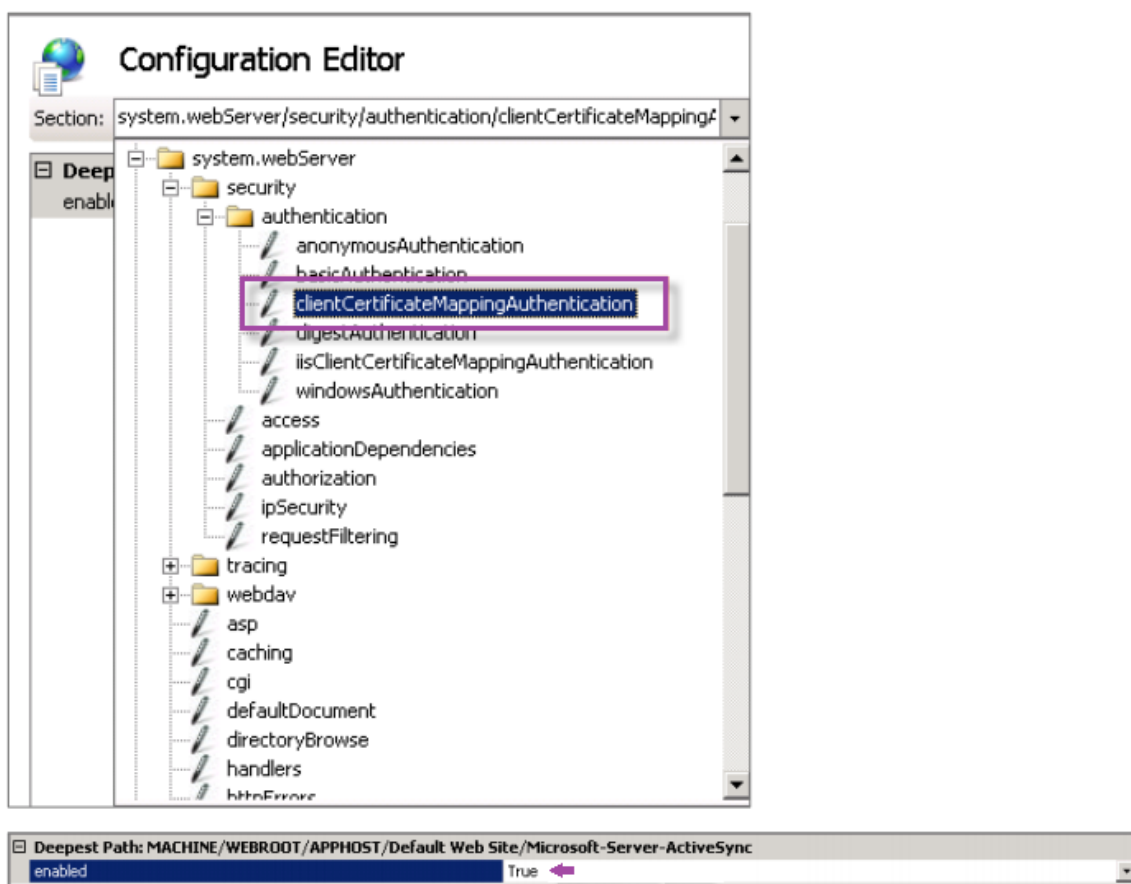
1. Users enroll their mobile device.
2. Endpoint Management prompts users to create a Citrix PIN.
3. Users are then redirected to the app store.
4. When users start Secure Mail, Endpoint Management doesn't prompt them for user credentials for mailbox configuration. Instead, Secure Mail requests the client certificate from Secure Hub and submits it to Microsoft Exchange Server for authentication. If Endpoint Management prompts for credentials when users start Secure Mail, check your configuration.

If users can download and install Secure Mail, but during the mailbox configuration Secure Mail fails to finish the configuration:

1. If Microsoft Exchange Server ActiveSync uses private SSL server certificates to secure the traffic, verify that the Root/Intermediate certificates installed on the mobile device.
2. Verify that the authentication type selected for ActiveSync is **Require client certificates**.



3. On Microsoft Exchange Server, check the **Microsoft-Server-ActiveSync** site to verify that client certificate mapping authentication is enabled. By default client certificate mapping authentication is disabled. The option is under **Configuration Editor > Security > Authentication**.



After selecting **True**, be sure to click **Apply** for the changes take effect.

4. Check the Citrix Gateway settings in the Endpoint Management console: Ensure that **Deliver user certificate for authentication** is **On** and that **Credential provider** has the correct profile selected.

#### To determine if the client certificate was delivered to a mobile device

1. In the Endpoint Management console, go to **Manage > Devices** and select the device.
2. Click **Edit** or **Show More**.
3. Go to the **Delivery Groups** section, and search for this entry:  
**Citrix Gateway Credentials: Requested credential, CertId=**

#### To validate whether client certificate negotiation is enabled

1. Run this `netsh` command to show the SSL Certificate configuration that is bound on the IIS website:

```
netsh http show sslcert
```

2. If the value for **Negotiate Client Certificate** is **Disabled**, run the following command to enable it:

```
netsh http delete sslcert ipport=0.0.0.0:443  
  
netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={  
  app_id } certstorename=store_name verifyclientcertrevocation=Enable  
  VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable  
  clientcertnegotiation=Enable
```

For example:

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=23498dfsdhfahf98rhkjqf9823rkjhd  
  appid={ 123asd456jd-a12b-3c45-d678-123456lkjhgf } certstorename=  
  ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWithCached  
  =Disable UsageCheck=Enable clientcertnegotiation=Enable
```

If you cannot deliver Root/Intermediate certificates to a Windows Phone 8.1 device through Endpoint Management:

- Send Root/Intermediate certificates (.cer) files through email to the Windows Phone 8.1 device and install them directly.

If Secure Mail doesn't install successfully on Windows Phone 8.1, verify the following:

- The Application Enrollment Token (.AETX file) is delivered through Endpoint Management using the Enterprise Hub device policy.
- The Application Enrollment Token was created using the same Enterprise Certificate from the certificate provider used to wrap Secure Mail and sign Secure Hub apps.
- The same Publisher ID is used to sign and wrap Secure Hub, Secure Mail, and the Application Enrollment Token.

## PKI entities

July 29, 2021

An Endpoint Management Public Key Infrastructure (PKI) entity configuration represents a component performing actual PKI operations (issuance, revocation, and status information). These components are either internal or external to Endpoint Management. Internal components are referred to as discretionary. External components are part of your corporate infrastructure.

Endpoint Management supports the following types of PKI entities:

- Generic PKIs (GPKIs)

Endpoint Management GPKI support includes DigiCert Managed PKI.

- Microsoft Certificate Services
- Discretionary Certificate Authorities (CAs)

Endpoint Management supports the following CA servers:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

### Common PKI concepts

Regardless of its type, every PKI entity has a subset of the following capabilities:

- **Sign:** Issuing a new certificate, based on a Certificate Signing Request (CSR).
- **Fetch:** Recovering an existing certificate and key pair.
- **Revoke:** Revoking a client certificate.

### About CA certificates

When you configure a PKI entity, indicate to Endpoint Management which CA certificate is the signer of certificates issued by (or recovered from) that entity. That PKI entity can return (fetched or newly signed) certificates signed by any number of different CAs.

Provide the certificate of each of these authorities as part of the PKI entity configuration. To do so, upload the certificates to Endpoint Management and then reference them in the PKI entity. For discretionary CAs, the certificate is implicitly the signing CA certificate. For external entities, you must specify the certificate manually.

#### Important:

When you create a Microsoft Certificate Services Entity template, avoid possible authentication issues with enrolled devices: Don't use special characters in the template name. For example, don't use: ! : \$ ( ) ## % + \* ~ ? | { } [ ]

### Generic PKI

The Generic PKI (GPKI) protocol is a proprietary Endpoint Management protocol running over a SOAP Web Service layer. The GPKI protocol provides a uniform interface with various PKI solutions. The GPKI protocol defines the following fundamental PKI operations:

- **Sign:** The adapter can take CSRs, transmit them to the PKI, and return newly signed certificates.



- **Fetch:** The adapter can retrieve (recover) existing certificates and key pairs (depending on input parameters) from the PKI.
- **Revoke:** The adapter can cause the PKI to revoke a given certificate.

The receiving end of the GPKI protocol is the GPKI adapter. The adapter translates the fundamental operations to the specific type of PKI for which it was built. For example, there are GPKI adapters for RSA and Entrust.

The GPKI adapter, as a SOAP Web Services endpoint, publishes a self-describing Web Services Description Language (WSDL) definition. Creating a GPKI PKI entity amounts to providing Endpoint Management with that WSDL definition, either through a URL or by uploading the file itself.

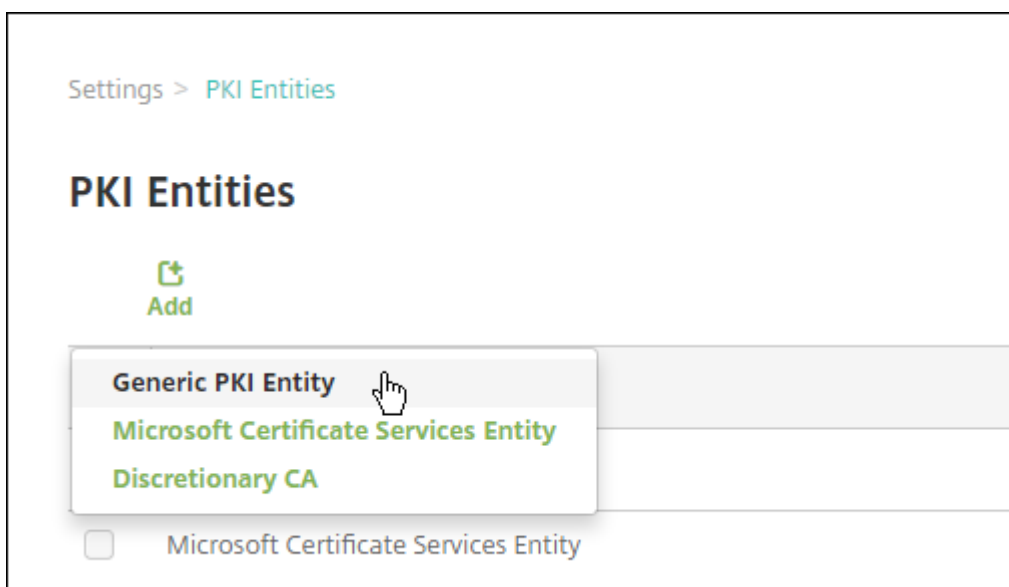
Support for each of the PKI operations in an adapter is optional. If an adapter supports a given operation, the adapter is said to have the corresponding capability (sign, fetch, or revoke). Each of these capabilities might be associated with a set of user parameters.

User parameters are parameters that the GPKI adapter defines for a specific operation. Provide values for user parameters to Endpoint Management. Endpoint Management parses the WSDL file to determine which operations the adapter has and which parameters the adapter requires for each of those operations. If you choose, use SSL client authentication to secure the connection between Endpoint Management and the GPKI adapter.

### To add a generic PKI

1. In the Endpoint Management console, click **Settings > PKI Entities**.
2. On the **PKI Entities** page, click **Add**.

A menu of PKI entity types appears.



### 3. Click **Generic PKI Entity**.

The Generic PKI Entity: General Information page appears.

Settings > PKI Entities > Generic PKI Entity

**Generic PKI Entity**

1 General  
2 Capabilities  
3 CA Certificates

**Generic PKI Entity: General Information**

The Generic PKI (GPKI) protocol is a proprietary XenMobile protocol running over a SOAP Web Service layer to provide uniform interfacing with various PKI solutions. The GPKI adapter, as a SOAP Web Services endpoint, publishes a self-describing Web Services Description Language (WSDL). You can create a GPKI entity to provide XenMobile with the WSDL through a URL.

Name\*

WSDL URL\*  ⓘ

Authentication type  ⓘ

### 4. On the **Generic PKI Entity: General Information** page, do the following:

- **Name:** Type a descriptive name for the PKI entity.
- **WSDL URL:** Type the location of the WSDL describing the adapter.
- **Authentication type:** Click the authentication method you want to use.
  - **None**
  - **HTTP Basic:** Provide the user name and password required to connect to the adapter.
  - **Client certificate:** Select the correct SSL client certificate.

### 5. Click **Next**.

The Generic PKI Entity: Adapter Capabilities page appears.

### 6. On the **Generic PKI Entity: Adapter Capabilities** page, review the capabilities and parameters associated with your adapter and then click **Next**.

The **Generic PKI Entity: Issuing CA Certificates** page appears.

### 7. On the Generic PKI Entity: Issuing CA Certificates page, select the certificates you want to use for the entity.

Although entities can return certificates signed by different CAs, the same CA must sign all certificates obtained through a given certificate provider. Thus, when configuring the **Credential Provider** setting, on the **Distribution** page, select one of the certificates configured here.

### 8. Click **Save**.

The entity appears on the PKI Entities table.

## DigiCert Managed PKI

Endpoint Management GPKI support includes DigiCert Managed PKI, also referred to as MPKI. This section describes how to set up Windows Server and Endpoint Management for DigiCert Managed PKI.

## Prerequisites

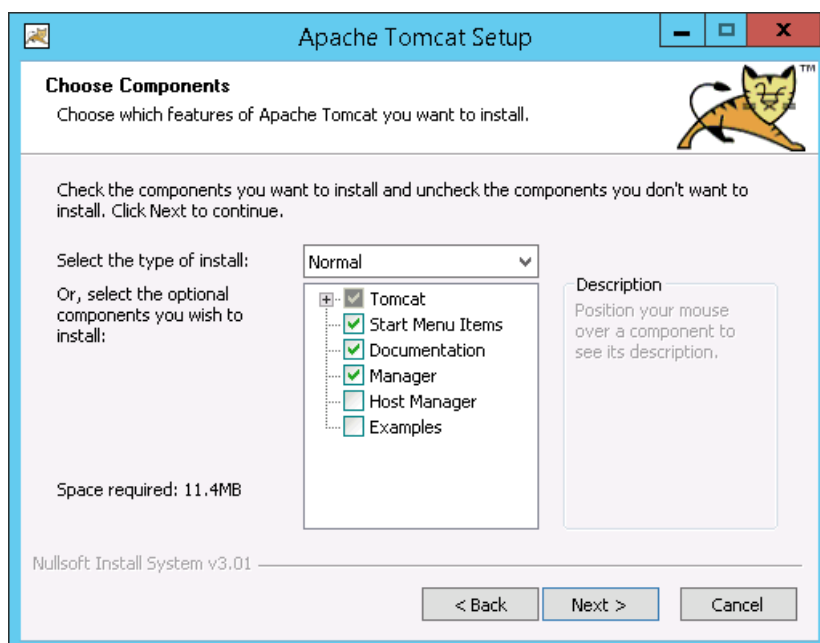
- Access to DigiCert Managed PKI Infrastructure
- Windows Server 2012 R2 server with the following components installed, as described in this article:
  - Java
  - Apache Tomcat
  - Symantec PKI Client
  - Portecle
- Access to the Endpoint Management downloads site

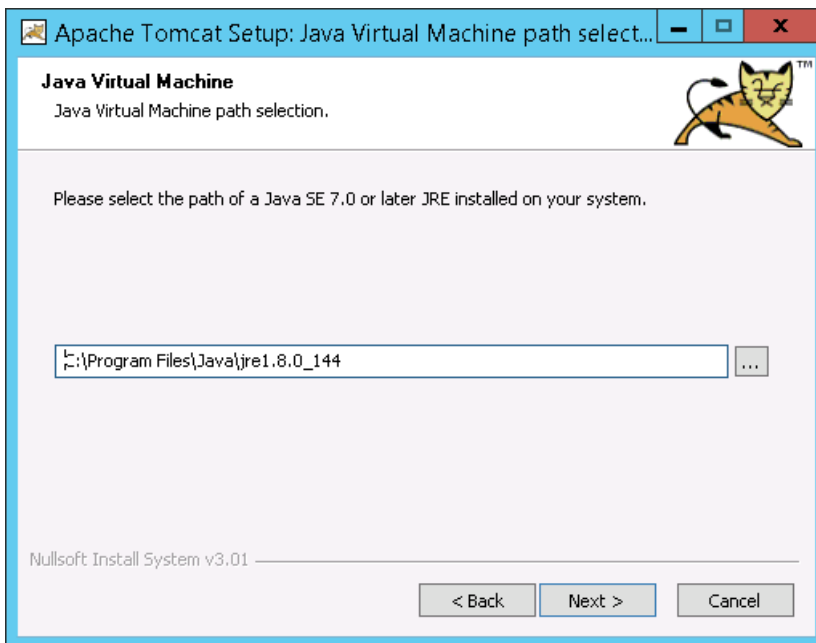
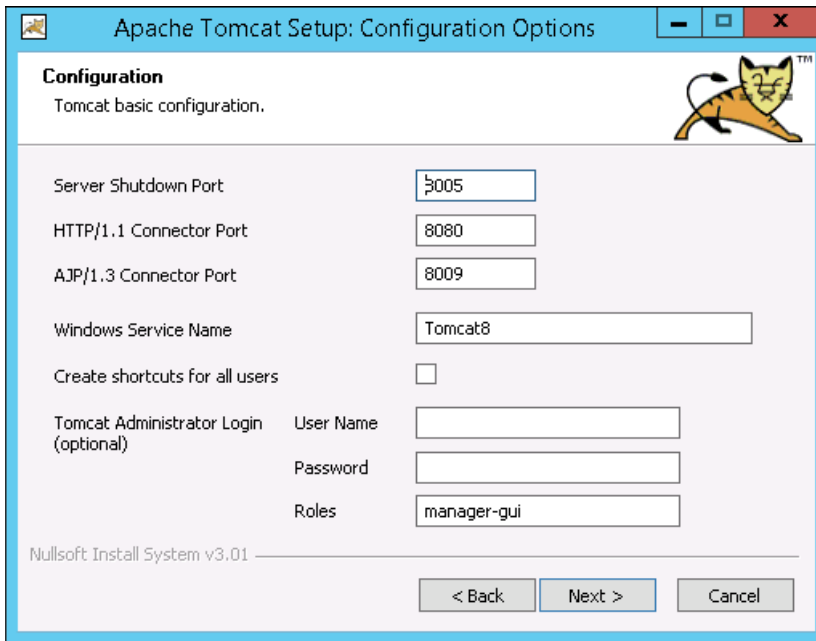
## Install Java on Windows Server

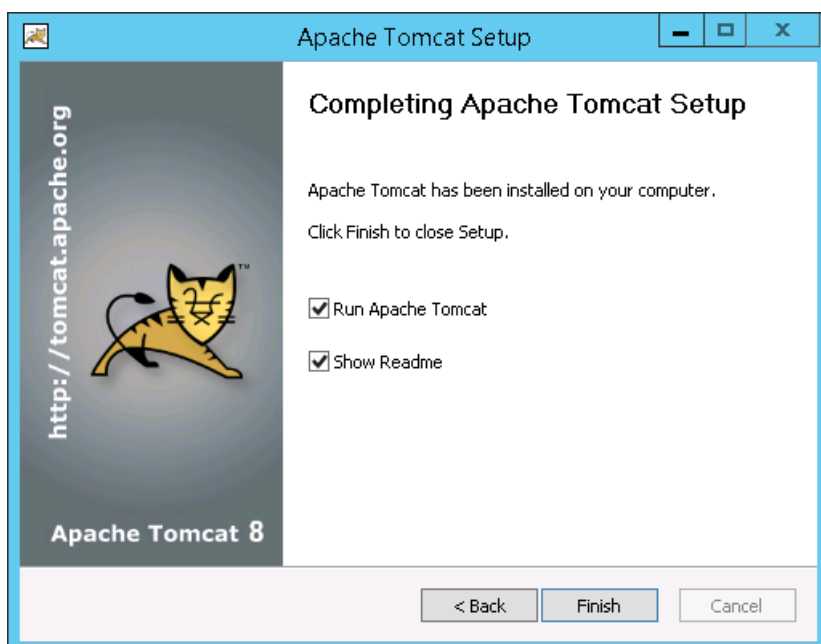
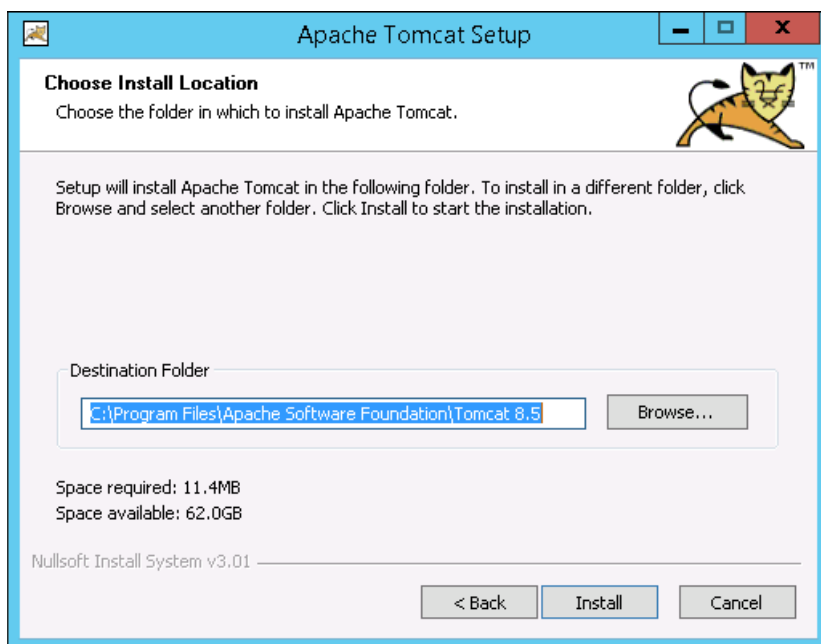
Download Java for 64-bit Windows from the [Java website](#) and then install the application. In the **Security Warning** dialog box, click **Run**.

## Install Apache Tomcat on Windows Server

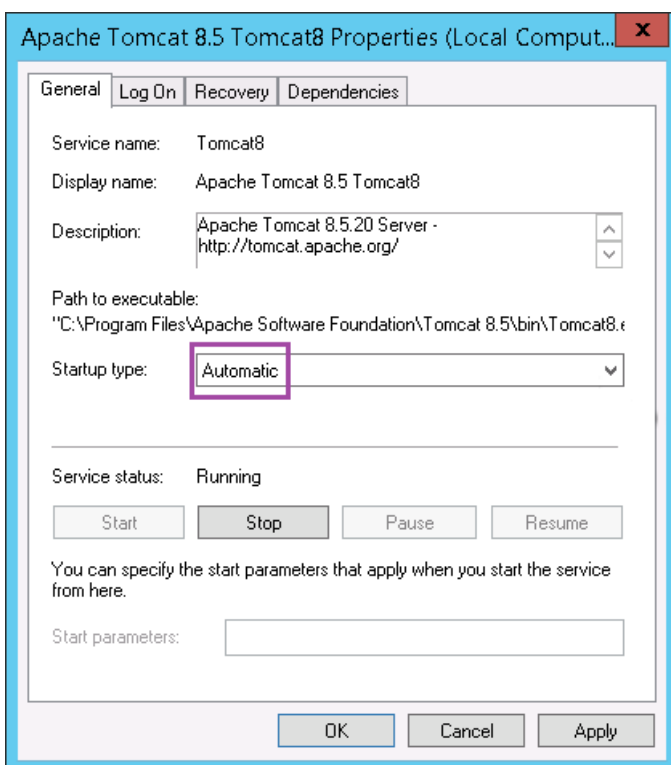
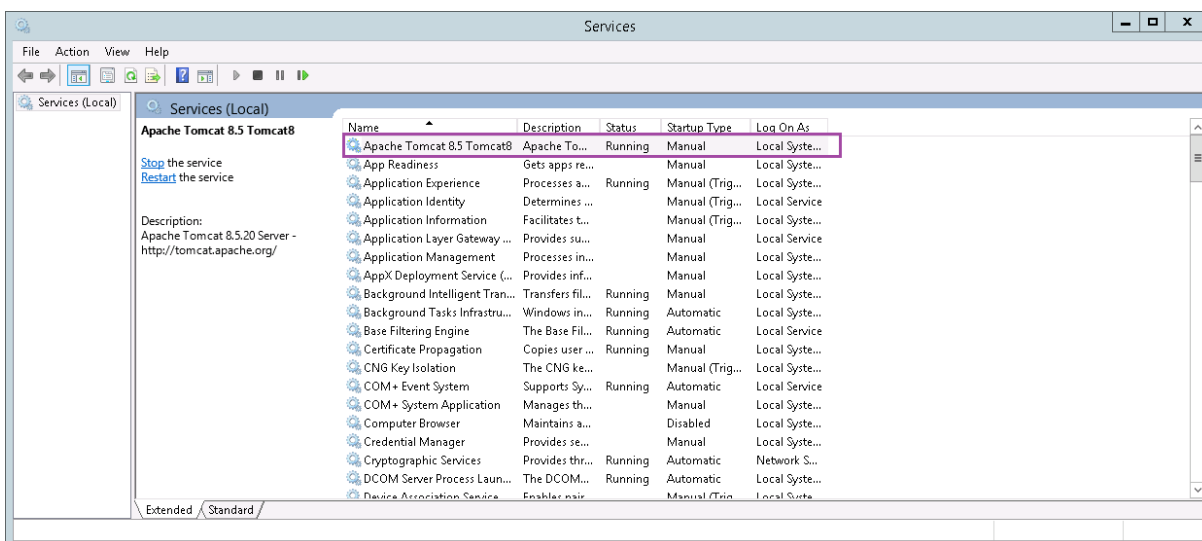
Download the latest Apache Tomcat 32-bit/64-bit Windows Service Installer from <https://tomcat.apache.org/> and then install it. In the **Security Warning** dialog box, click **Run**. Complete the Apache Tomcat setup, using the following examples as a guide.





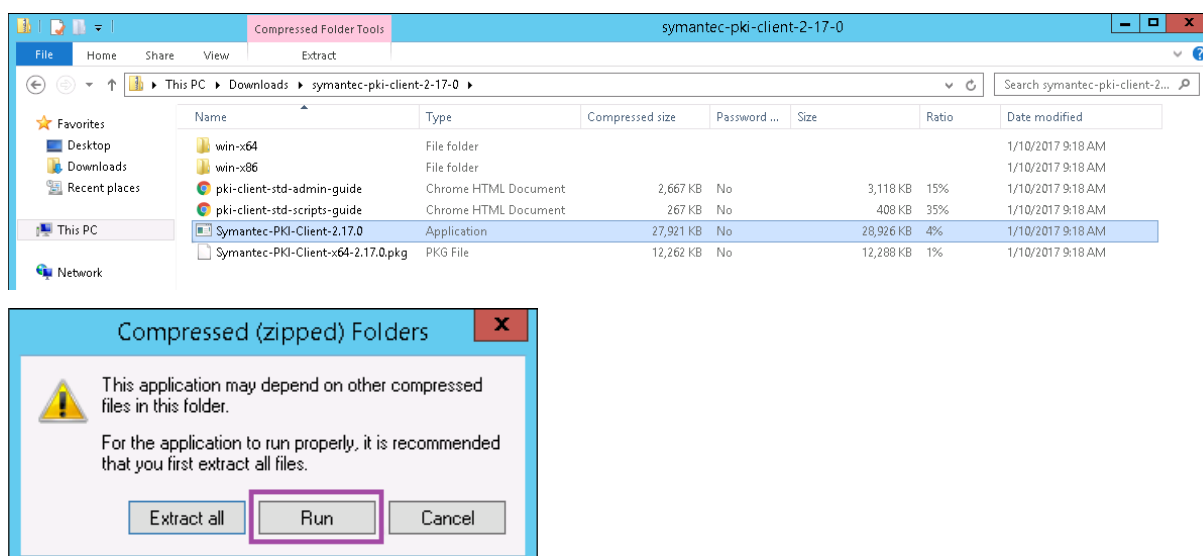


Next, go to Windows Services and change **Startup Type** from **Manual** to **Automatic**.



### Install DigiCert PKI client on Windows Server

Download the installer from the PKI Manager console. If you can't access that console, download the installer from the DigiCert support page, [How to download DigiCert PKI Client](#). Unzip and run the installer.



In the **Security Warning** dialog box, be sure to click **Run**. Follow the instructions in the installer to complete the setup. When the installer completes, it prompts you to restart.

### Install Portecle on Windows Server

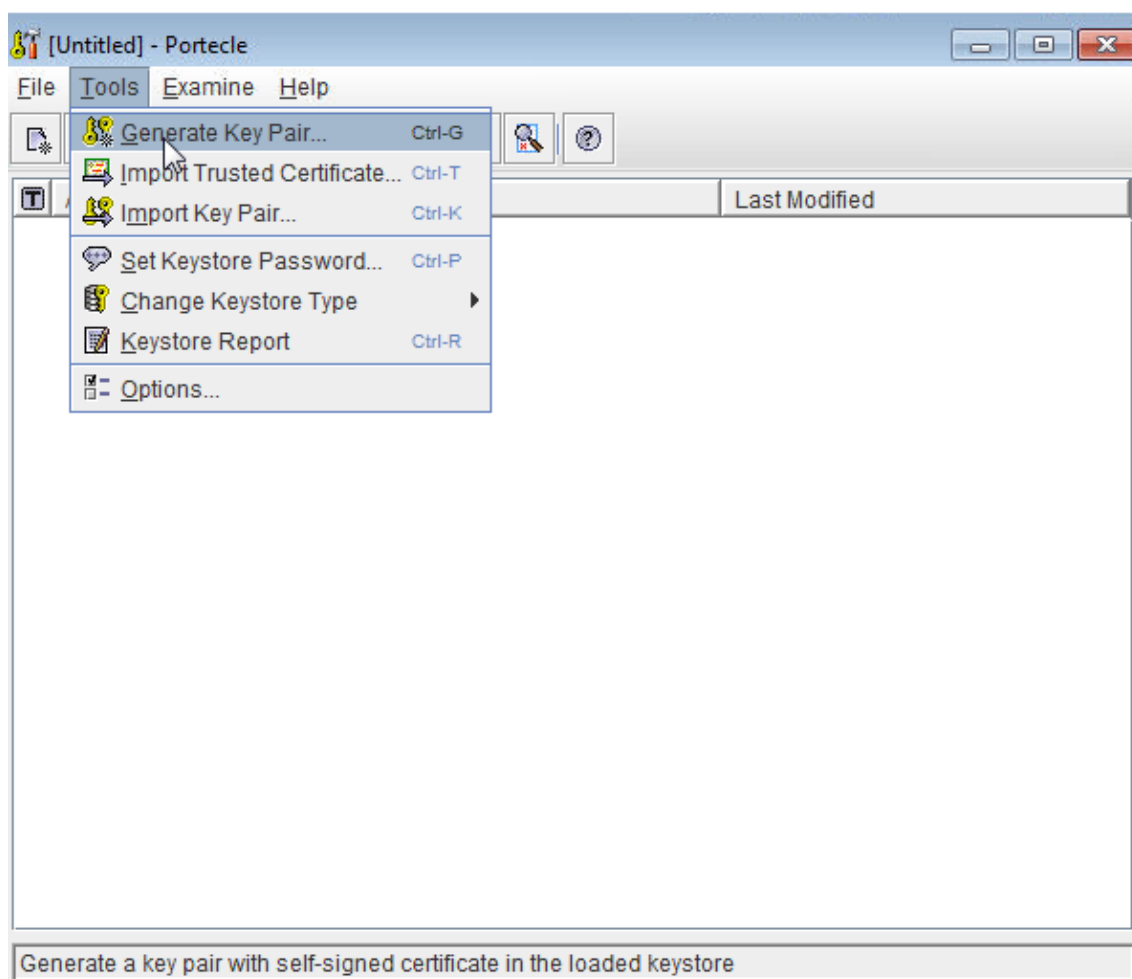
Download the installer from <https://sourceforge.net/projects/portecleinstall/files/> and then unzip and run the installer.

### Generate the registration authority (RA) certificate for DigiCert Managed PKI

The keystore for client certificate authentication is contained in a registration authority (RA) certificate, named RA.jks. The following steps describe how to generate that certificate by using Portecle. You can also generate the RA certificate by using the Java CLI.

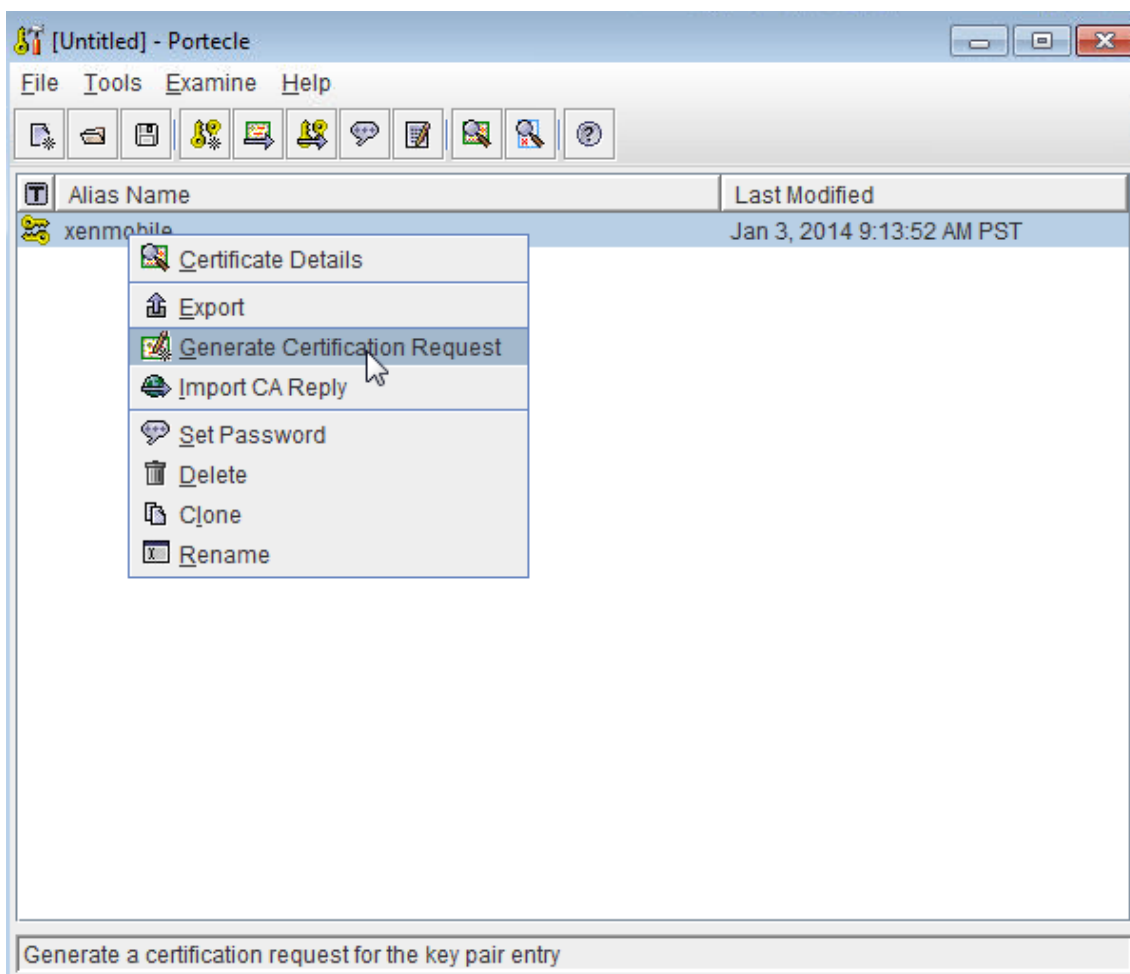
This article also describes how to upload the RA and public certificates.

1. In Portecle, go to **Tools > Generate Key Pair**, provide the required information, and generate the key pair.

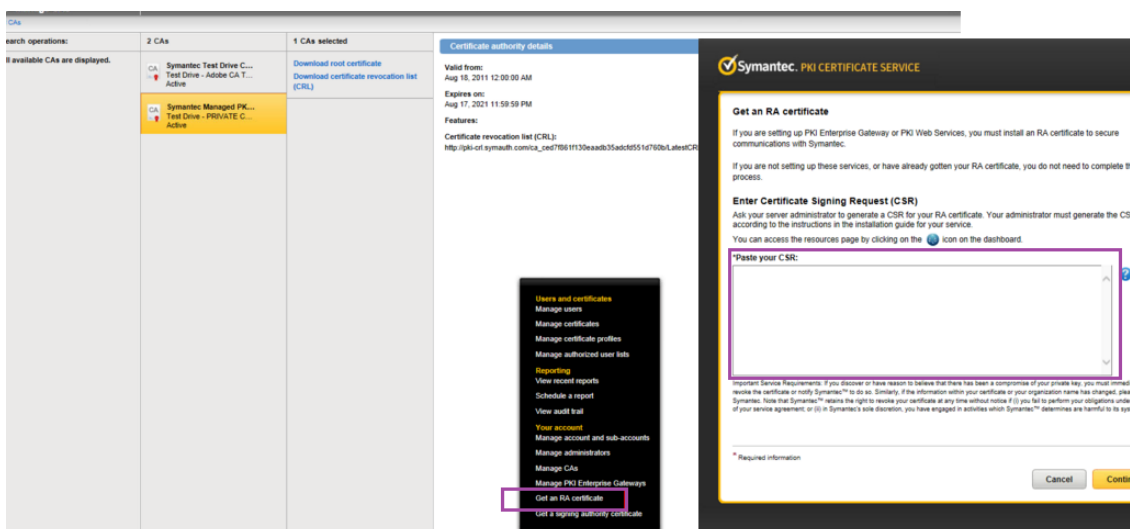


2. Right-click the key pair and then click **Generate Certification Request**.

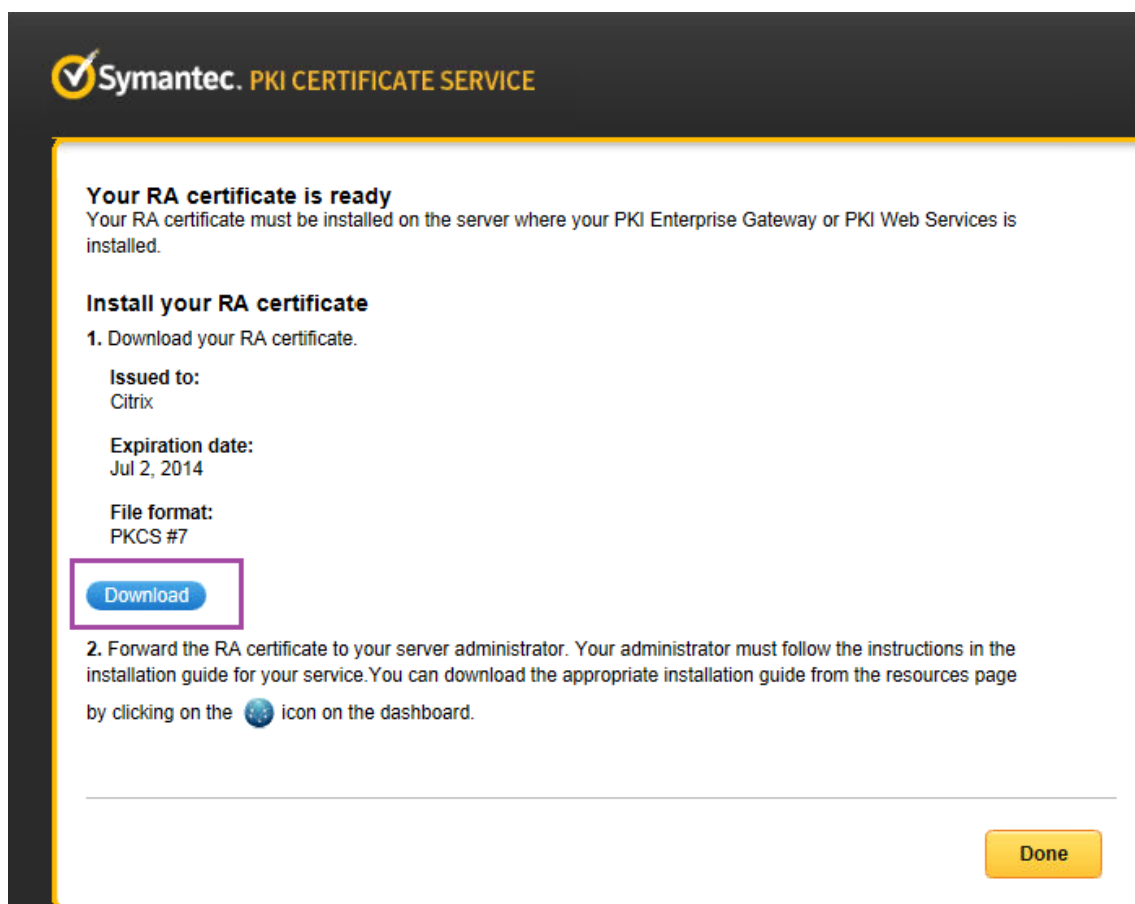




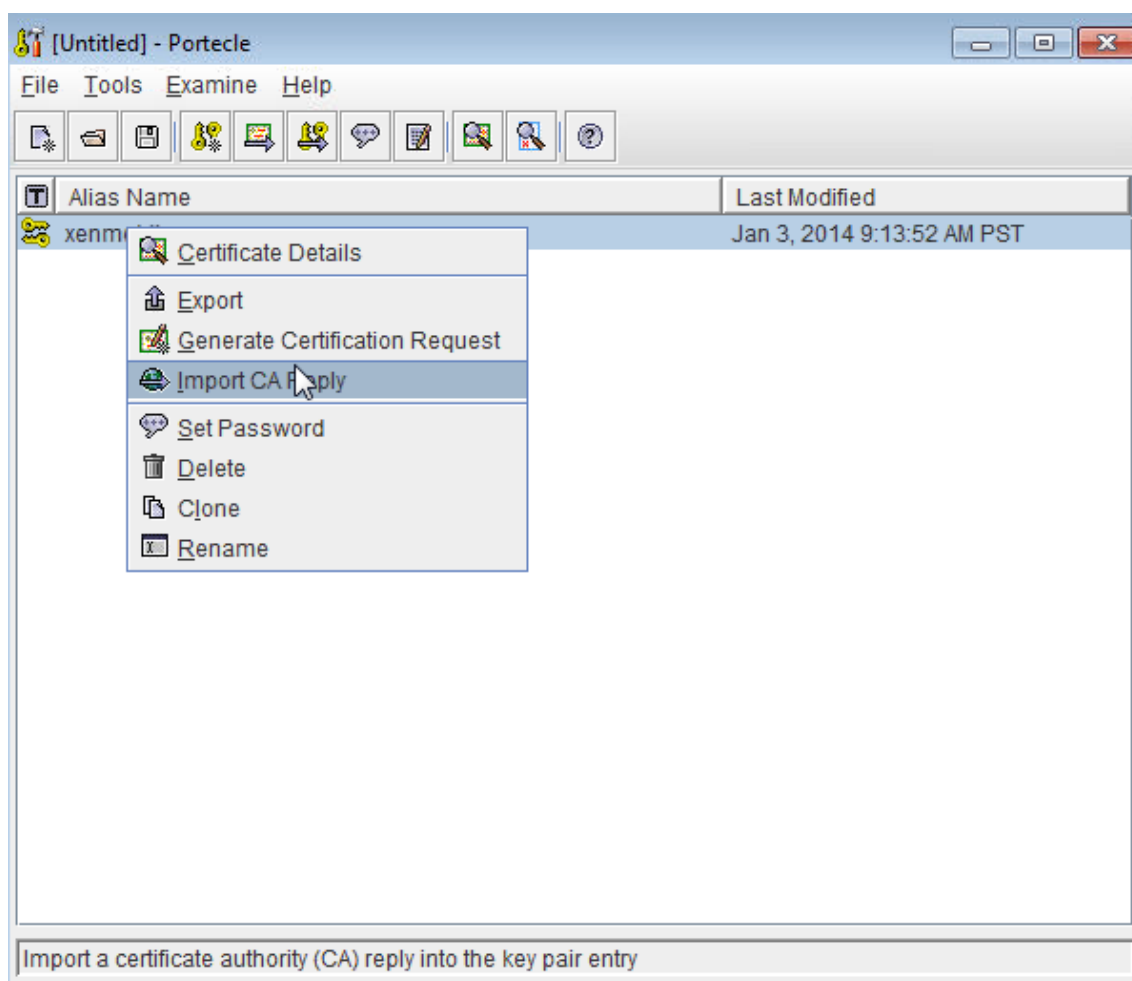
3. Copy the CSR.
4. In Symantec PKI Manager, generate an RA certificate: Click **Settings**, click **Get a RA Certificate**, paste the CSR, and then click **Continue**.



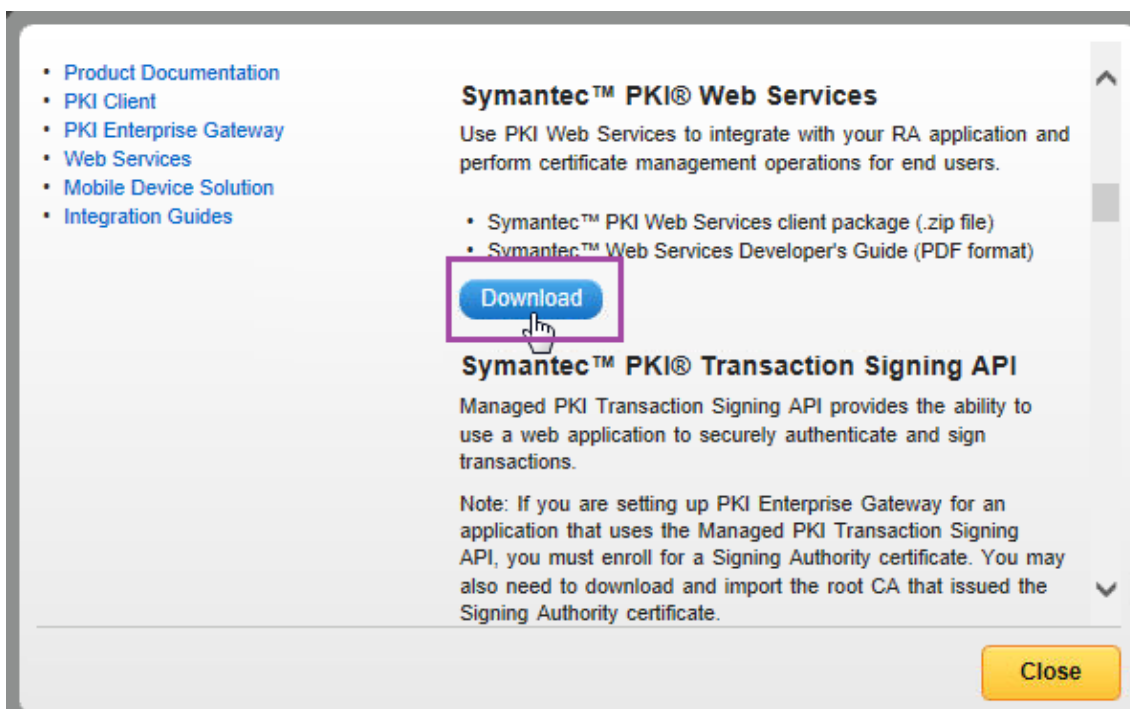
5. Click **Download** to download the generated RA certificate.



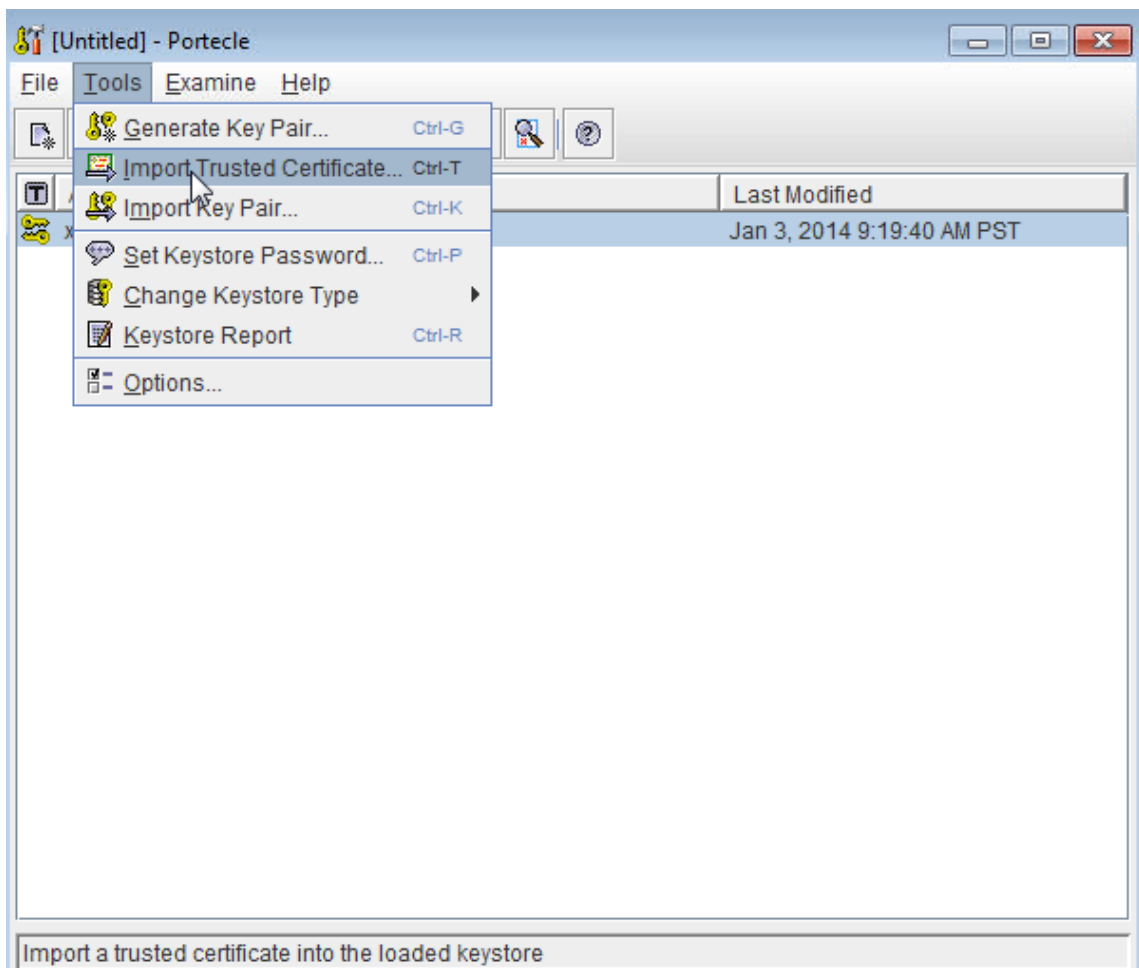
6. In Portecle, import the RA certificate: Right-click the key pair and then click **Import CA Reply**.



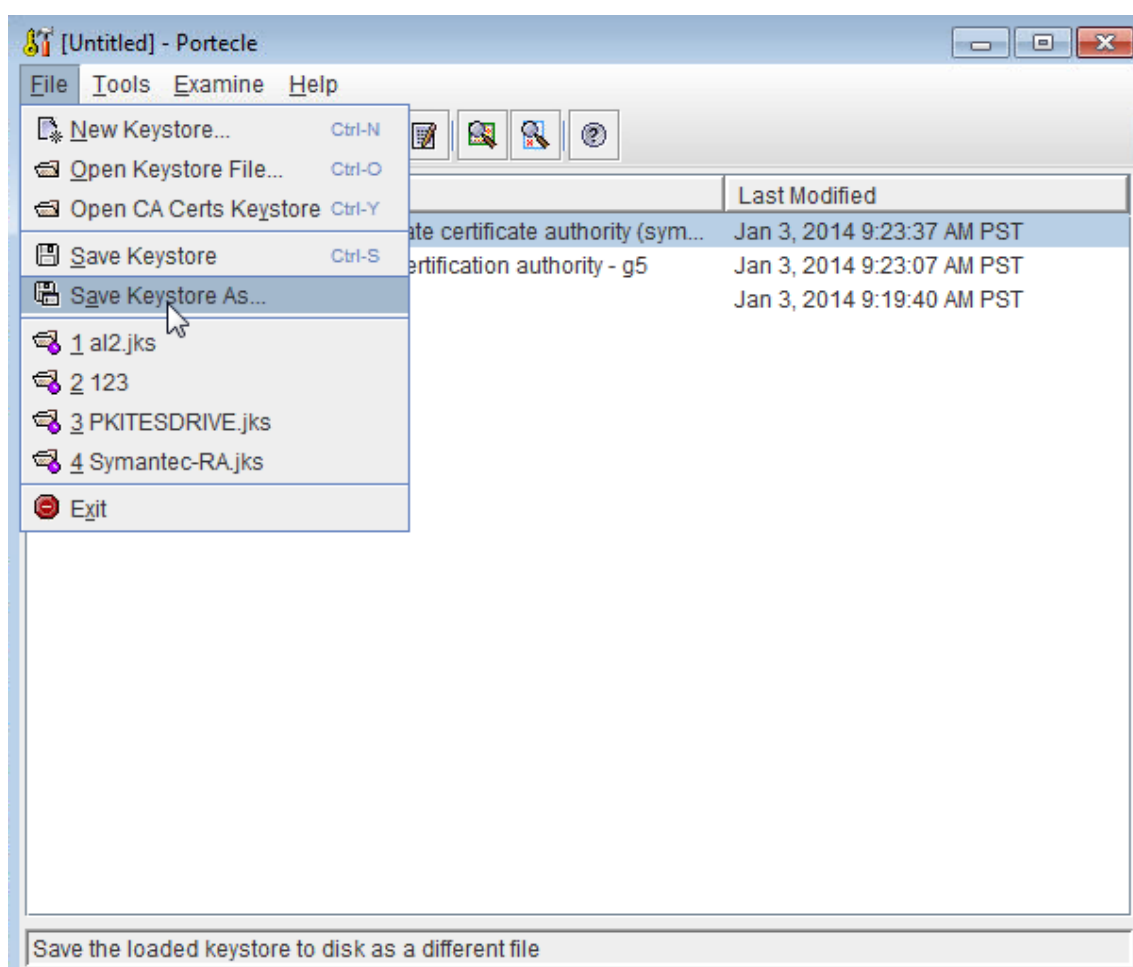
7. In Symantec PKI Manager: Go to **Resources > Web Services** and then download the CA certificates.



8. In Portecle, import the RA intermediate and root certificates into the keystore: Go to **Tools > Import Trusted Certificates**.



9. After importing the CAs, save the keystore as RA.jks under the C:\Symantec folder on the Windows server.



### Configure Symantec PKI adapter on Windows Server

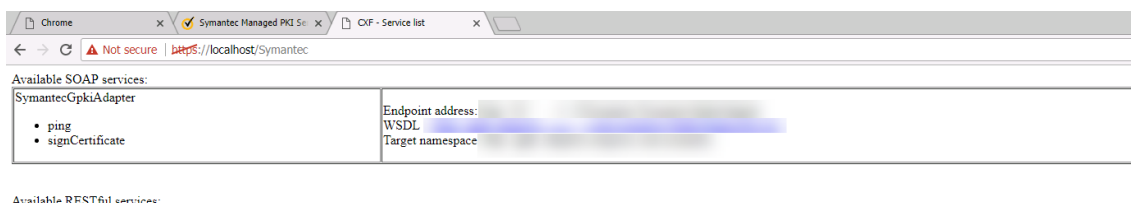
1. Log in to Windows Server as an administrator.
2. Upload the RA.jks file that you generated in the preceding section. Also upload the public certificates (cacerts.jks) for your Symantec MPKI server.
3. Download the Symantec PKI Adapter file:
  - a) Go to <https://www.citrix.com/downloads>.
  - b) Navigate to **Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10 > Tools**.
  - c) On the **Symantec PKI Adapter** tile, click **Download File**.
  - d) Unzip the file and copy these files to the Windows Server C: drive:
    - custom\_gpki\_adapter.properties
    - Symantec.war
4. Open custom\_gpki\_adapter.properties in Notepad and edit the following values:

```
1 Gpki.CaSvc.Url=https://<managed PKI URL>
2
3 # keystore for client-cert auth
4
5 keyStore=C:\\Symantec\\RA.jks
6
7 # truststore for server with self-signed root CA
8
9 trustStore=C:\\Symantec\\cacerts.jks
10 <!--NeedCopy-->
```

5. Copy Symantec.war under the folder <tomcat dir>\webapps and then start Tomcat.
6. Verify that the application deployed: Open a web browser and navigate to <https://localhost/Symantec>. (If you get a certificate error, consider connecting with HTTP instead.)
7. Navigate to the folder <tomcat dir>\webapps\Symantec\WEB-INF\classes and edit gpki\_adapter.properties. Modify the property **CustomProperties** to point it to the custom\_gpki\_adapter file under the C:\Symantec folder:

```
CustomProperties=C:\\Symantec\\custom_gpki_adapter.properties
```

8. Restart Tomcat, navigate to <https://localhost/Symantec>, and then copy the endpoint address. In the next section, you paste that address when configuring the PKI adapter.



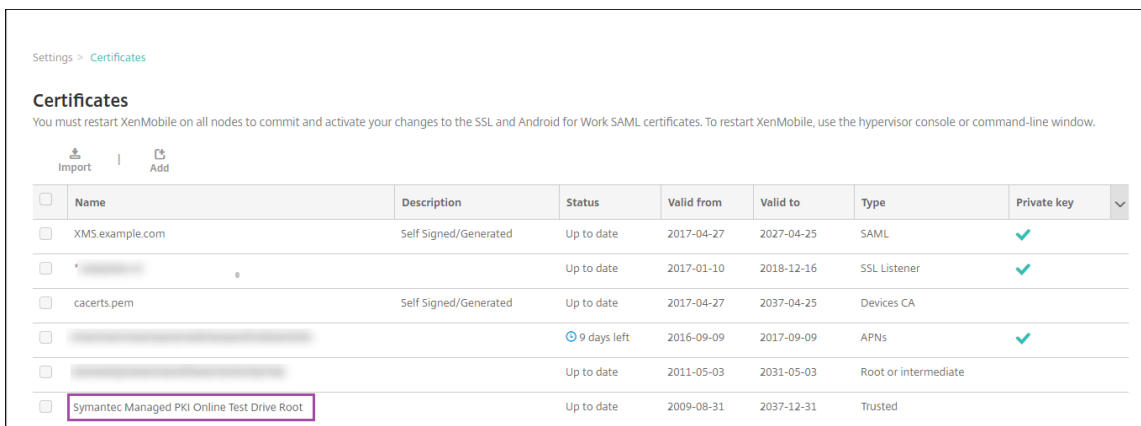
Available RESTful services:

## Configure Endpoint Management for DigiCert Managed PKI

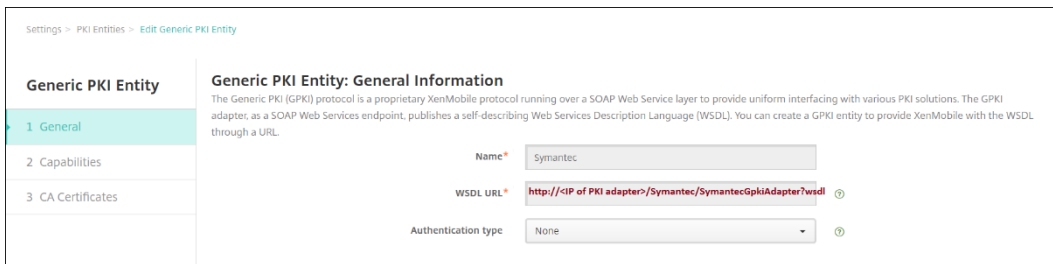
Complete the Windows Server setup before performing the following Endpoint Management configuration.

### To import the Symantec CA certificates and configure the PKI entity

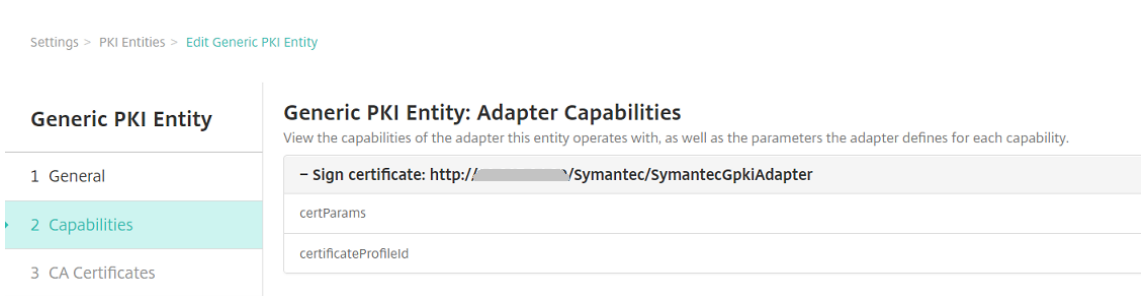
1. Import the Symantec CA certificates that issue the end-user certificate: In the Endpoint Management console, go to **Settings > Certificates** and click **Import**.



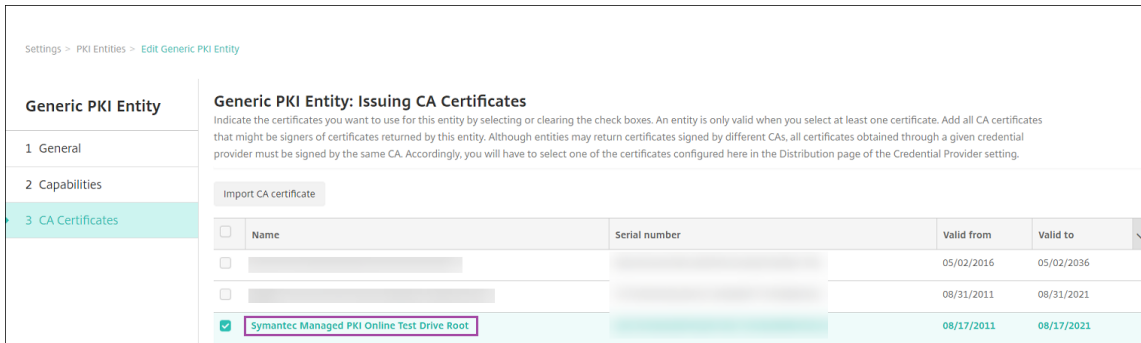
2. Add and configure the PKI Entity: Go to **Settings > PKI Entities**, click **Add**, and then choose **Generic PKI Entity**. In **WSDL URL**, paste the endpoint address that you copied when configuring the PKI adapter in the previous section. Then, append `?wsdl` as shown in the following sample.



3. Click **Next**. Endpoint Management populates the parameter names from the WSDL.



4. Click **Next**, select the correct CA certificate, and then click **Save**.





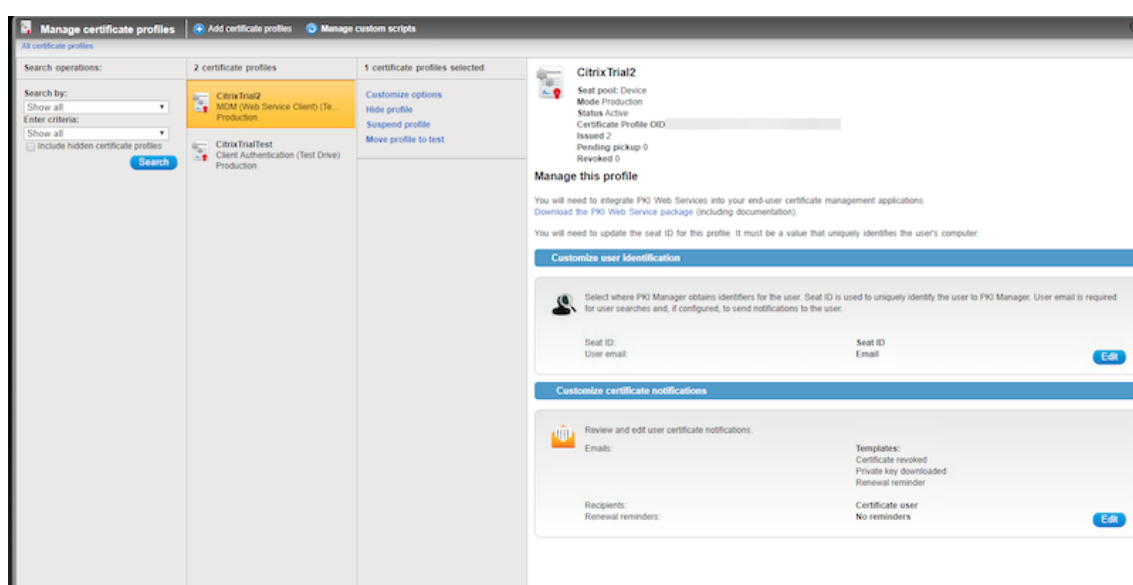
5. On the **Settings > PKI Entities** page, verify that the **State** of the PKI Entity you added is **Valid**.



Name	Type	Capabilities	Description	State
Symantec	GPKI	SIGN	http://[redacted]/Symantec/SymantecGpkiAdapter	Valid

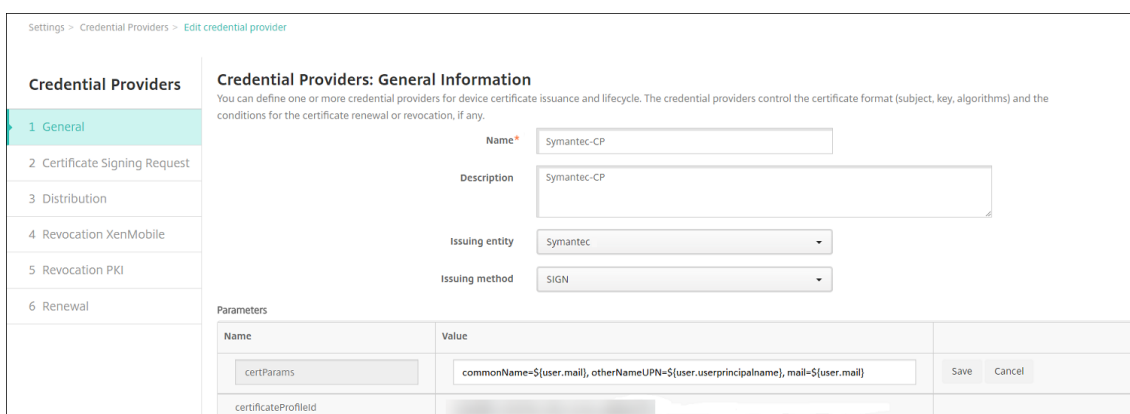
### To create the credential provider for DigiCert Managed PKI

1. In the Symantec PKI Manager console, copy the **Certificate Profile OID** from the Certificate Template.



2. In the Endpoint Management console, go to **Settings > Credential Providers**, click **Add**, and then configure the settings as follows.

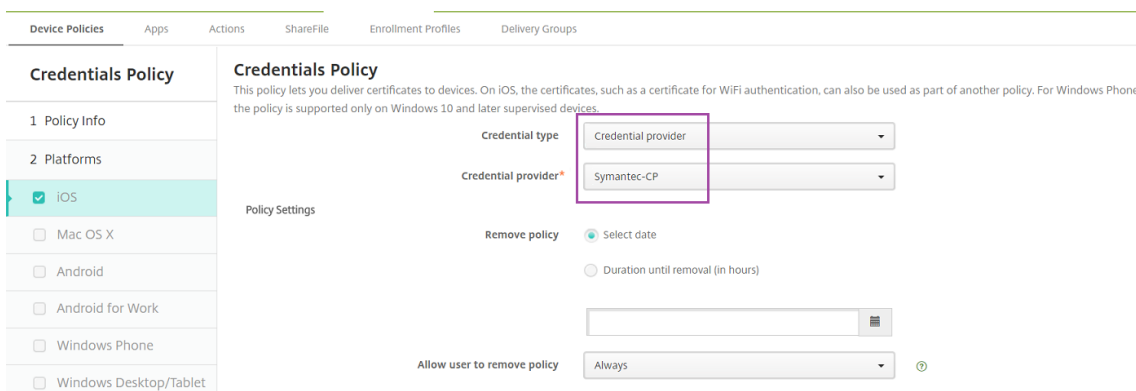
- **Name:** Type a unique name for the new provider configuration. This name is used to refer to the configuration in other parts of the Endpoint Management console.
- **Description:** Describe the credential provider. Although this field is optional, a description can be useful when you need details about the credential provider.
- **Issuing entity:** Choose the certificate issuing entity.
- **Issuing method:** Choose **Sign** as the method that the system uses to obtain client certificates from the configured entity.
- **certParams:** Add the following value: **commonName=\${user.mail},otherNameUPN=\${user.userpr**
- **certificateProfileid:** Paste the Certificate Profile OID that you copied in Step 1.



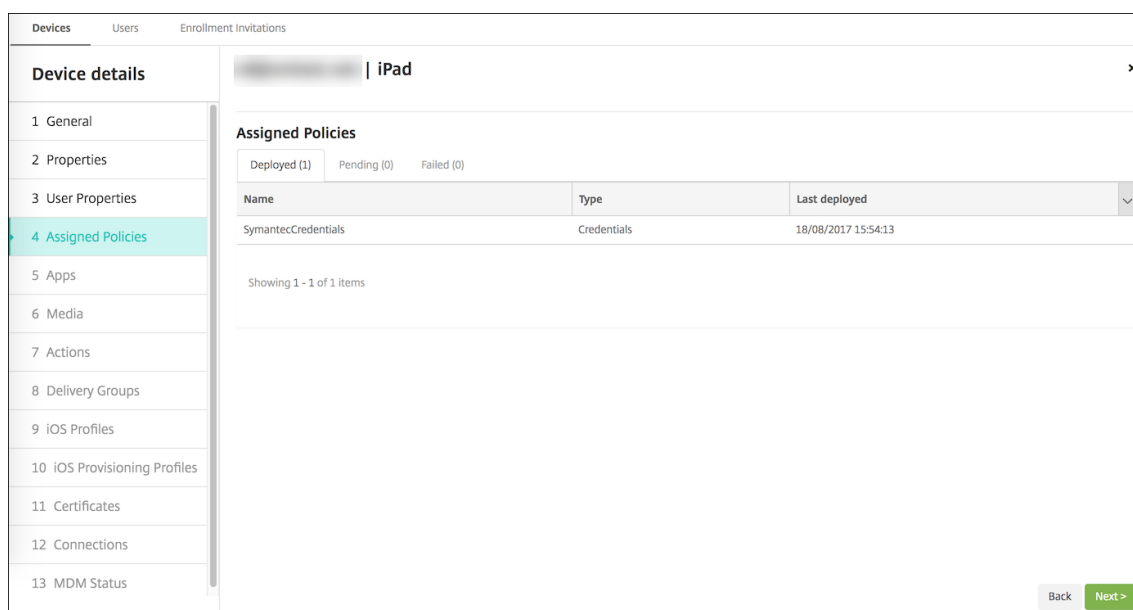
3. Click **Next**. On each of the remaining pages (Certificate Signing Request through Renewal), accept the default settings. When you are finished, click **Save**.

### To test and troubleshoot the configuration

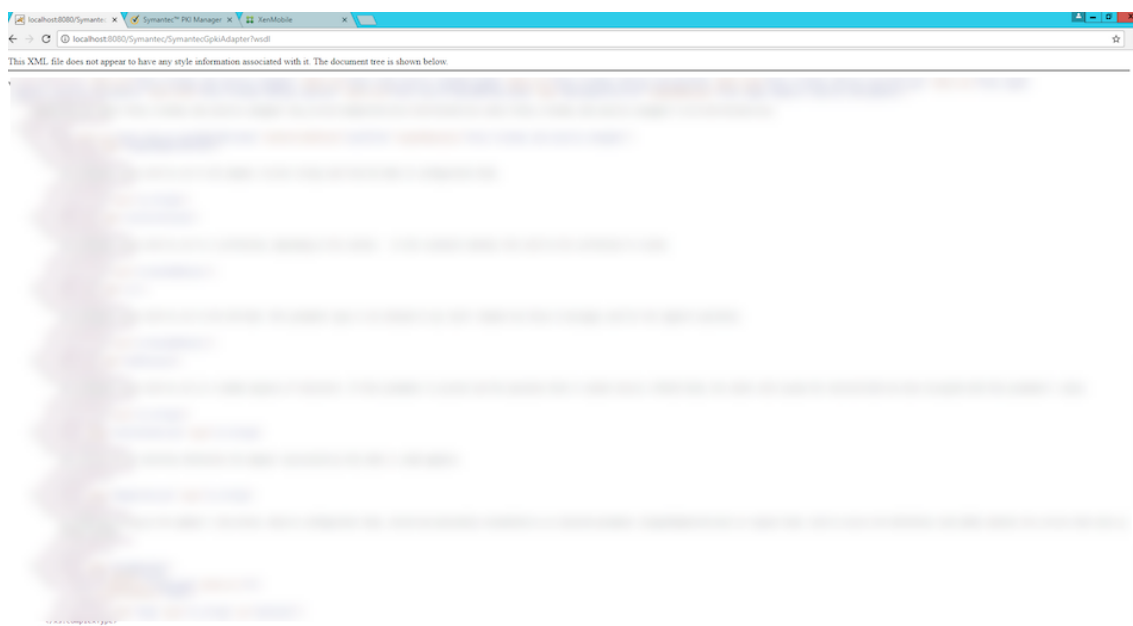
1. Create a Credentials device policy: Go to **Configure > Device Policies**, click **Add**, start typing the word **Credentials**, and then click **Credentials**.
2. Specify a **Policy Name**.
3. Configure the platform settings as follows:
  - **Credential type:** Choose **Credential Provider**.
  - **Credential provider:** Choose the Symantec provider.



4. After you complete the platform settings, continue to the **Assignment** page, assign the policy to delivery groups, and click **Save**.
5. To check whether the policy deployed to the device, go to **Manage > Devices**, select the device, click **Edit**, and click **Assigned Policies**. The following example shows a successful policy deployment.



If the policy didn't deploy, log in to the Windows Server and check if the WSDL is loading properly.



For more troubleshooting information, check the Tomcat logs in `<tomcat dir>\logs\catalina.<current date>`.

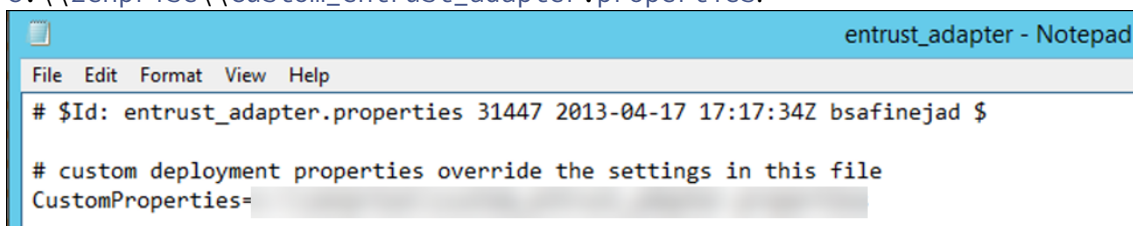
### Entrust PKI adapter

As an alternative to DigiCert Managed PKI, you can install the Entrust PKI adapter. Before installing the adapter, see the steps for installing Java and Apache Tomcat on Windows Server in the DigiCert Managed PKI section of this article.

Ensure that the Citrix Cloud Connector is installed as well. For more information on the Cloud Connector, see [Citrix Cloud Connector](#).

### Install the Entrust PKI adapter

1. Download the Entrust PKI Adapter file:
  - a) Go to <https://www.citrix.com/downloads>.
  - b) Navigate to **Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10 > Tools**.
  - c) On the **Entrust PKI Adapter** tile, click **Download File**.
  - d) Extract the `entrust.war` file from the downloaded `.zip` file and place it in the `C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps` directory.
2. In `C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps\Entrust\WEB-INF\classes`, edit `entrust_adapter.properties` and set `CustomProperties` to `c:\zenprise\custom_entrust_adapter.properties`.



3. In your C: drive, create the following directory and file name: **zenprise/custom\_entrust\_adapter.properties**
4. Edit the file with the following content, taking care to replace the `Entrust.MdmSvc.URL`, `AdminUserId`, and `AdminPassword` appropriately.

```
1 # set the following to the proper URL for AS/IG
2 Entrust.MdmSvc.Url=https://pki.yourcorp.com:19443/mdmws/services/
   AdminServiceV8
3
4 # set to 1 or true to force user creation from passed user and
   group parameters if using IG and user does not exist
5 CreateUser=
6
7 # set the credentials for the endpoint
8 AdminUserId=[User ID]
9 AdminPassword=[password]
10
11
12 # keystore for client-cert auth
13 #keyStore=
14 #keyStorePassword=
```

```

15 #keyStoreType: JKS, JCEKS and PKCS12 -- not needed for .p12 and .
    jks files
16
17 # truststore for server with self-signed root CA
18 #trustStore=
19 #trustStorePassword=
20 #trustStoreType: JKS, JCEKS and PKCS12 -- not needed for .p12 and
    .jks files
21 <!--NeedCopy-->

```

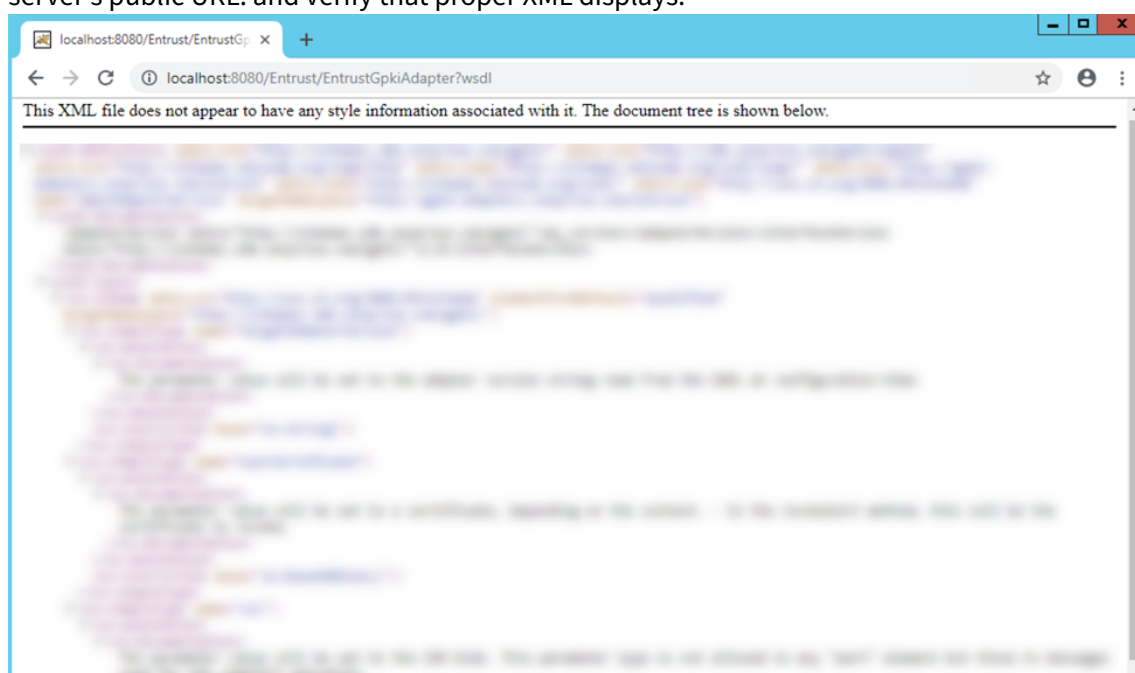
- Restart the Tomcat service. Navigate to C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\logs and open Catalina\_201x-MM-DD.log. Verify there are no errors and that you see the following line:

```

13-Nov-2018 09:02:35.319 INFO [localhost-startStop-1] org.apache.cxf
.endpoint.ServerImpl.initDestination Setting the server's publish
address to be /EntrustGpkiAdapter

```

- Navigate to <http://localhost:8080/Entrust/EntrustGpkiAdapter?wsdl> or your server's public URL. and verify that proper XML displays.



### Configure Endpoint Management for the Entrust PKI adapter

- Log in to your Endpoint Management console and navigate to **Settings > PKI Entities**. Click **Add > Generic PKI Entity**.
- Enter the following information:

- **Name:** - Enter a name for the PKI Entity.
  - **WSDL URL:** If you're using Citrix Cloud Connector, enter <http://localhost:8080/Entrust/EntrustGpkiAdapter?wsdl>. If you aren't using Citrix Cloud Connector, enter your server's public URL.
  - **Authentication type:** Choose the authentication method you want to use.
    - **None**
    - **HTTP Basic:** Type the user name and password required to connect.
    - **Client certificate:** Choose the correct SSL client certificate.
  - **Use Cloud Connector:** **On** or **Off** depending on if you are using the Citrix Cloud Connector or not.
  - **Resource Location:** Select **My Resource Location**.
  - **Allowed Relative Paths:** Enter [/Entrust/\\*](#).
3. Once you've finished configuring the PKI Entity, return to the **Settings** page and add a **Credential Provider**.
  4. On the **General** tab, select your Entrust entity as the **Issuing entity** and **SIGN** as the **Issuing method**.
  5. On the **Certificate Signing Request** tab, configure the settings as follows:
    - **Key algorithm:** **RSA**.
    - **Key size:** **2048**.
    - **Signature algorithm** **SHA256withRSA**.
    - **Subject name:** **cd=\$user.username**
    - **Subject alternative names:** Optional. We recommend the following:
      - **Type:** **User Principal name**.
      - **Value:** **\$user.userprincipalname**.
- Note:**

If you change any settings on the adapter, follow these steps to reconfigure the credential provider.
6. After finishing configuring the credential provider navigate to **Configure > Device Policies** and add a Credentials policy.
  7. Configure the policy for the operating systems you plan to use. On each OS configuration page, for **Credential Type**, select **Credential provider**. For the **Credential provider** menu, select the credential provider you configured earlier.

## Microsoft Certificate Services

Endpoint Management interfaces with Microsoft Certificate Services through its web enrollment interface. Endpoint Management only supports the issuing of new certificates through that interface (the

equivalent of the GPKI sign capability). If the Microsoft CA generates a Citrix Gateway user certificate, Citrix Gateway supports renewal and revocation for those certificates.

To create a Microsoft CA PKI entity in Endpoint Management, you must specify the base URL of the Certificate Services web interface. If you choose, use SSL client authentication to secure the connection between Endpoint Management and the Certificate Services web interface.

### Add a Microsoft Certificate Services entity

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console and then click **PKI Entities**.

2. On the **PKI Entities** page, click **Add**.

A menu of PKI entity types appears.

3. Click **Microsoft Certificate Services Entity**.

The **Microsoft Certificate Services Entity: General Information** page appears.

4. On the **Microsoft Certificate Services Entity: General Information** page, configure these settings:

- **Name:** Type a name for your new entity, which you use later to refer to that entity. Entity names must be unique.
- **Web enrollment service root URL:** Type the base URL of your Microsoft CA web enrollment service. For example: <https://192.0.0.1/certsrv/>. The URL can use plain HTTP or HTTP-over-SSL.
- **certnew.cer page name:** The name of the certnew.cer page. Use the default name unless you have renamed it for some reason.
- **certfnsh.asp:** The name of the certfnsh.asp page. Use the default name unless you have renamed it for some reason.
- **Authentication type:** Choose the authentication method you want to use.
  - **None**
  - **HTTP Basic:** Type the user name and password required to connect.
  - **Client certificate:** Choose the correct SSL client certificate.
- **Use Cloud Connector:** Choose **On** to use Cloud Connector for connections to the PKI server. Then, specify a **Resource Location** and **Allowed Relative Paths** for the connection.
  - **Resource Location:** Choose from the resource locations defined in [Citrix Cloud Connector](#).

- **Allowed Relative Paths:** The relative paths allowed for the specified resource location. Specify one path per line. You can use the asterisk (\*) wildcard.

Suppose that the resource location is <https://www.ServiceRoot/certsrv>. To provide access to all URLs in that path, enter `/*` in **Allowed Relative Paths**.

Settings > PKI Entities > Edit Microsoft Certificate Services Entity

**Microsoft Certificate Services Entity**

- 1 General
- 2 Templates
- 3 HTTP Parameters
- 4 CA Certificates

**Microsoft Certificate Services Entity: General Information**

Name\* AusterCA

Web enrollment service root URL\*

certnew.cer page name\* certnew.cer

certfnsh.asp\* certfnsh.asp

Authentication type Client certificate

SSL client certificate

Import SSL certificate

Use Cloud Connector ON

Resource Location\* My Resource Location

Allowed Relative Paths\* \*

5. Click **Test Connection** to ensure that the server is accessible. If it is not accessible, a message appears, stating that the connection failed. Check your configuration settings.
6. Click **Next**.

The **Microsoft Certificate Services Entity: Templates** page appears. On this page, you specify the internal names of the templates your Microsoft CA supports. When creating credential providers, you select a template from the list defined here. Every credential provider using this entity uses exactly one such template.

For Microsoft Certificate Services templates requirements, see the Microsoft documentation for your Microsoft Server version. Endpoint Management doesn't have requirements for the certificates it distributes other than the certificate formats noted in [Certificates](#).

7. On the **Microsoft Certificate Services Entity: Templates** page, click **Add**, type the name of the template and then click **Save**. Repeat this step for each template you want to add.
8. Click **Next**.

The **Microsoft Certificate Services Entity: HTTP parameters** page appears. On this page, you specify custom parameters for Endpoint Management to add to the HTTP request to the Mi-



Microsoft Web Enrollment interface. Custom parameters are useful only for customized scripts running on the CA.

9. On the **Microsoft Certificate Services Entity: HTTP parameters** page, click **Add**, type the name and value of the HTTP parameters you want to add, and then click **Next**.

The **Microsoft Certificate Services Entity: CA Certificates** page appears. On this page, you must inform Endpoint Management of the signers of the certificates that the system obtains through this entity. When your CA certificate is renewed, update it in Endpoint Management. Endpoint Management applies the change to the entity transparently.

10. On the **Microsoft Certificate Services Entity: CA Certificates** page, select the certificates you want to use for this entity.
11. Click **Save**.

The entity appears on the PKI Entities table.

### **Citrix Gateway Certificate Revocation List (CRL)**

Endpoint Management supports Certificate Revocation List (CRL) only for a third-party Certificate Authority. If you have a Microsoft CA configured, Endpoint Management uses Citrix Gateway to manage revocation.

When you configure client certificate-based authentication, consider whether to configure the Citrix Gateway Certificate Revocation List (CRL) setting, **Enable CRL Auto Refresh**. This step ensures that the user of a device in MAM-only mode can't authenticate using an existing certificate on the device.

Endpoint Management reissues a new certificate, because it doesn't restrict a user from generating a user certificate after one is revoked. This setting increases the security of PKI entities when the CRL checks for expired PKI entities.

### **Discretionary CAs**

A discretionary CA is created when you provide Endpoint Management with a CA certificate and the associated private key. Endpoint Management handles certificate issuance, revocation, and status information internally, according to the parameters you specify.

When configuring a discretionary CA, you can activate Online Certificate Status Protocol (OCSP) support for that CA. If you enable OCSP support, the CA adds the extension `id-pe-authorityInfoAccess` to the certificates that the CA issues. The extension points to the Endpoint Management internal OCSP Responder at the following location:

`https://<server>/<instance>/ocsp`

When configuring the OCSP service, specify an OCSP signing certificate for the discretionary entity in question. You can use the CA certificate itself as the signer. To avoid the unnecessary exposure

of your CA private key (recommended): Create a delegate OCSP signing certificate, signed by the CA certificate, and include this extension: `id-kp-OCSPSigning extendedKeyUsage`.

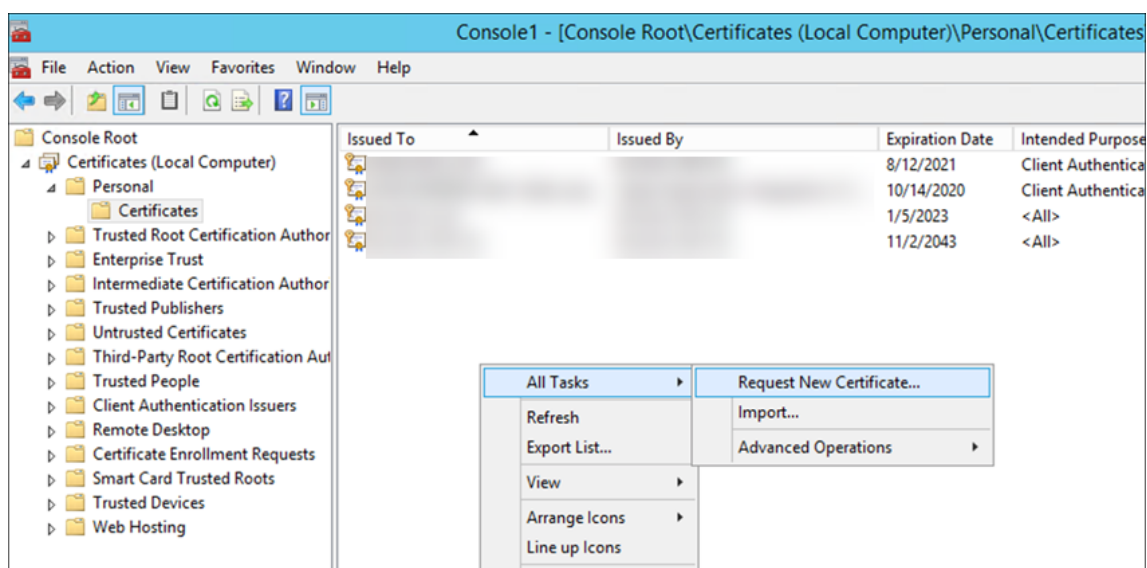
The Endpoint Management OCSP responder service supports basic OCSP responses and the following hashing algorithms in requests:

- SHA-256
- SHA-384
- SHA-512

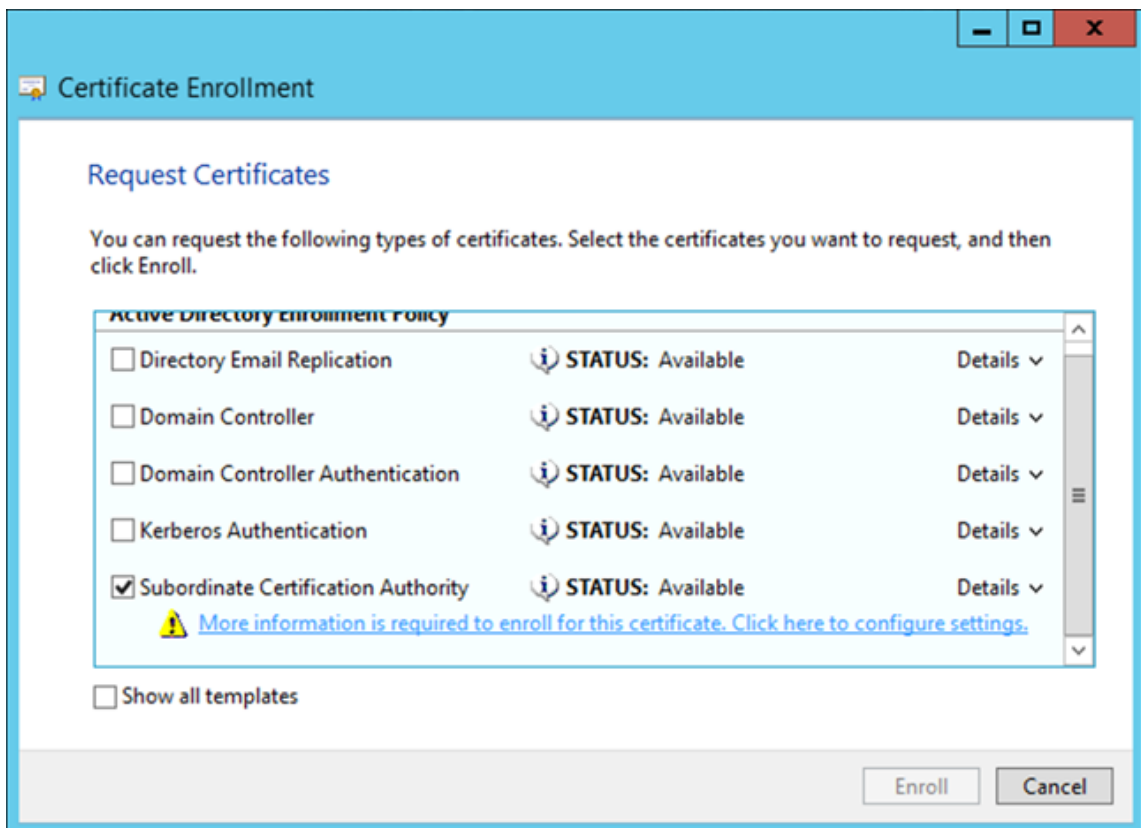
Responses are signed with SHA-256 and the signing certificate key algorithm (DSA, RSA, or ECDSA).

### Generate and import a certificate for your CA

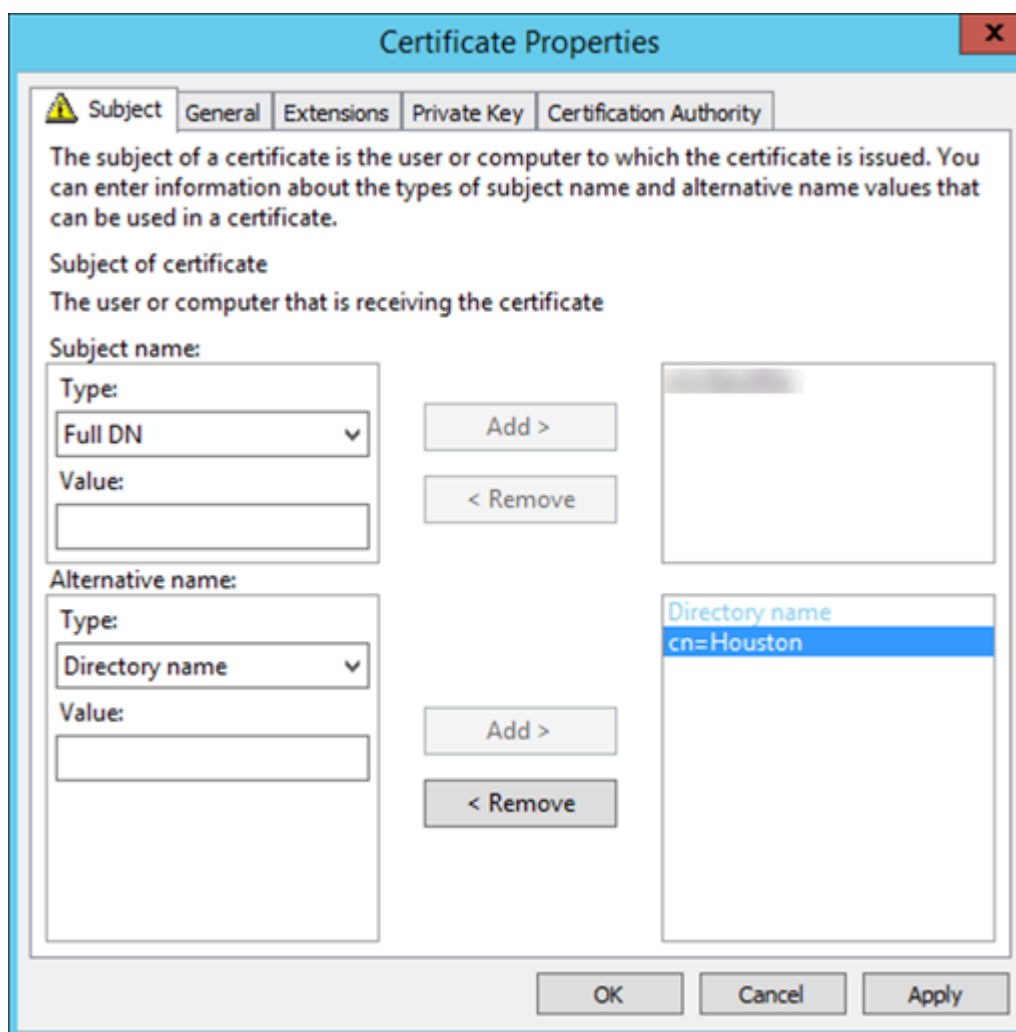
1. On your server, open the Microsoft Management Console (MMC) with your Local System account, and open the certificates snap-in. In the pane on the right, right-click and then click **All Tasks > Request New Certificate**.



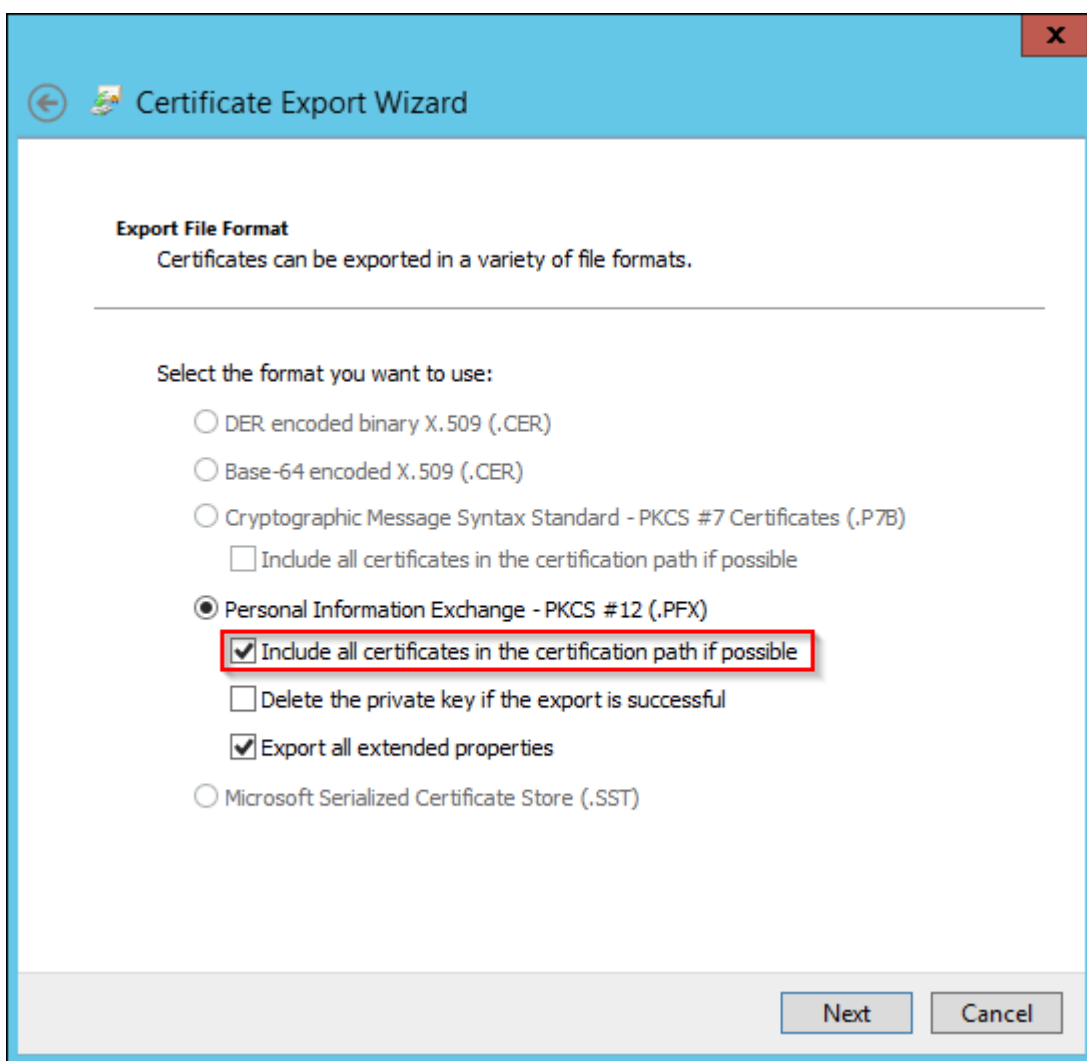
2. In the wizard that opens, click **Next** twice. In the **Request Certificates** list, select **Subordinate Certification Authority** and then click the **More information** link.



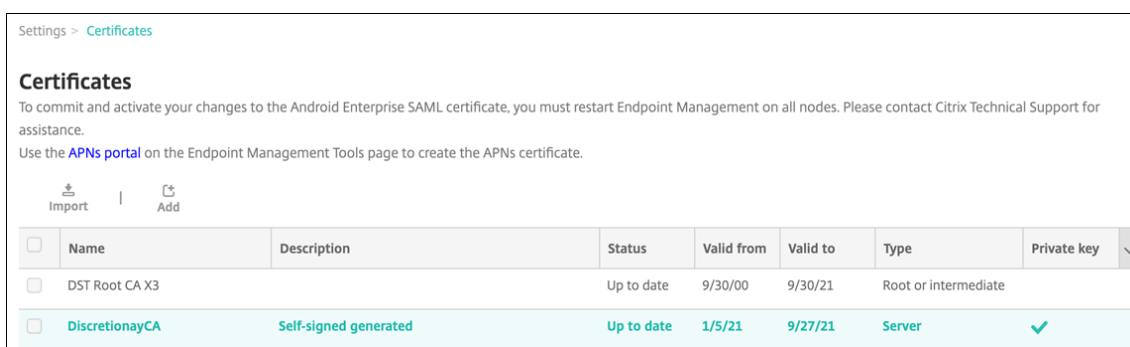
3. In the window, type a **Subject name** and **Alternative name**. Click **OK**.



4. Click **Enroll**, and then click **Finish**.
5. In the MMC, right-click the certificate you created. Click **All Tasks > Export**. Export the certificate as a .pfx file with a private key. Select the option to **Include all certificates in the certification path if possible**.



6. In the Endpoint Management console, navigate to **Settings > Certificates**.



7. Click **Import**. In the window that opens, browse for the certificate and private key files you exported previously.

### Import ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time. Use the [APNs portal](#) on the Endpoint Management Tools page to create the APNs certificate.

**Import** Keystore

**Keystore type** PKCS#12

**Use as** Server

**Keystore file \***  Browse

**Password \***

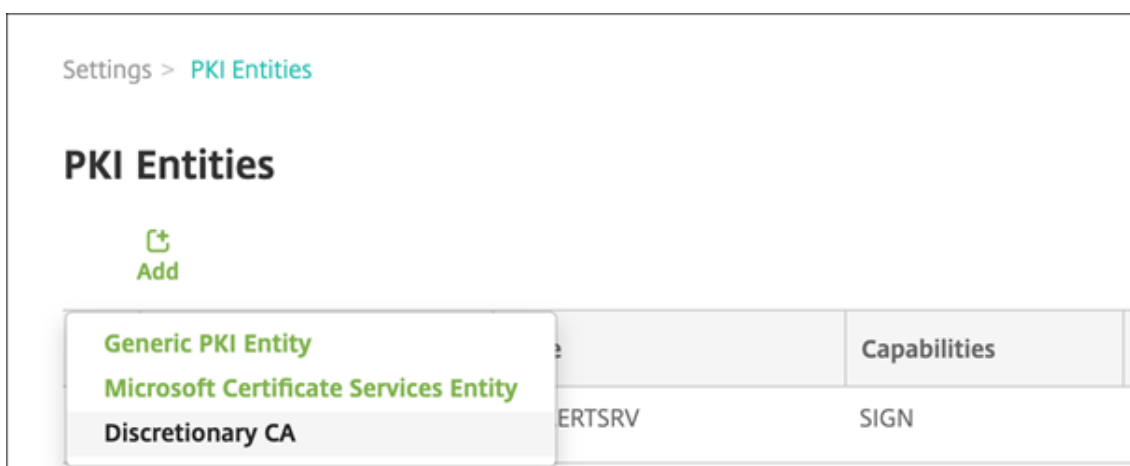
**Description**

Cancel Import

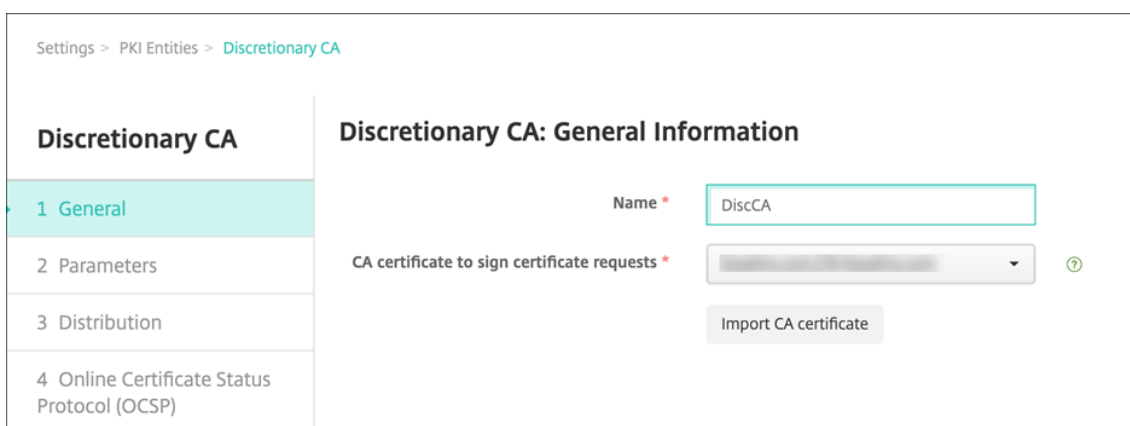
8. Click **Import**. The certificate is added to the table.

### Add discretionary CAs

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console and then click **More > PKI Entities**.
2. On the **PKI Entities** page, click **Add**.



3. Click **Discretionary CA**.



4. On the **Discretionary CA: General Information** page, configure the following:

- **Name:** Type a descriptive name for the discretionary CA.
- **CA certificate to sign certificate requests:** Click a certificate for the discretionary CA to use to sign certificate requests.

This list of certificates is generated from the CA certificates with private keys you uploaded at Endpoint Management at **Configure > Settings > Certificates**.

5. Click **Next**.

Settings > PKI Entities > Edit Discretionary CA

### Discretionary CA

- 1 General
- 2 Parameters
- 3 Distribution
- 4 Online Certificate Status Protocol (OCSP)

### Discretionary CA: Parameters

Serial number generator \*

Next serial number  ⓘ

Certificate valid for  days

Key usage

DigitalSignature  ON

NonRepudiation  OFF

KeyEncipherment  ON

DataEncipherment  OFF

Extended key usage

Name \*  Add

6. On the **Discretionary CA: Parameters** page, configure the following:

- **Serial number generator:** The discretionary CA generates serial numbers for the certificates it issues. From this list, click **Sequential** or **Non-sequential** to determine how the numbers are generated.
- **Next serial number:** Type a value to determine the next number issued.
- **Certificate valid for:** Type the number of days the certificate is valid.
- **Key usage:** Identify the purpose of the certificates issued by the discretionary CA by setting the appropriate keys to **On**. Once set, the CA is limited to issuing certificates for those purposes.
- **Extended key usage:** To add more parameters, click **Add**, type the key name and then click **Save**.

7. Click **Next**.

Settings > PKI Entities > Edit Discretionary CA

### Discretionary CA

- 1 General
- 2 Parameters
- 3 Distribution
- 4 Online Certificate Status Protocol (OCSP)

### Discretionary CA: Distribution

Select distribution mode

Centralized: server-side key generation

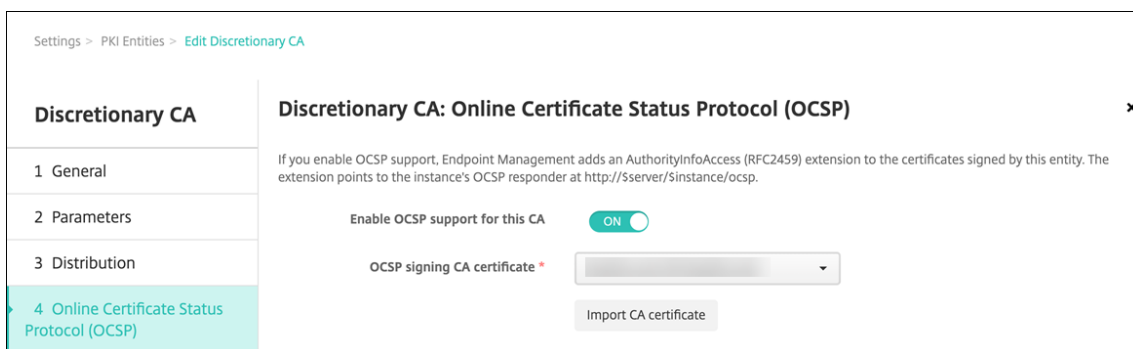
Distributed: device-side key generation



8. On the **Discretionary CA: Distribution** page, select a distribution mode:

- **Centralized: server-side key generation.** Citrix recommends the centralized option. The private keys are generated and stored on the server and distributed to user devices.
- **Distributed: device-side key generation.** The private keys are generated on the user devices. This distributed mode uses SCEP and requires an RA encryption certificate with the **keyUsage keyEncryption** extension and an RA signing certificate with the **keyUsage digitalSignature** extension. The same certificate can be used for both encryption and signing.

9. Click **Next**.



10. On the **Discretionary CA: Online Certificate Status Protocol (OCSP)** page, configure the following:

- If you want to add an [AuthorityInfoAccess](#) (RFC2459) extension to the certificates signed by this CA, set **Enable OCSP support for this CA** to **On**. This extension points to the CA OCSP responder at <https://<server>/<instance>/ocsp>.
- If you enabled OCSP support, select an OCSP signing CA certificate. This list of certificates is generated from the CA certificates you uploaded to Endpoint Management.

Enabling the feature gives the Citrix ADC an opportunity to check the status of certificates. Citrix recommends that you enable this feature.

11. Click **Save**.

The discretionary CA appears on the PKI Entities table.

### Configure a credential provider

1. In the Endpoint Management console, navigate to **Settings > Credential Provider**, and click **Add**.
2. On the **Credential Providers: General Information** page, configure the following:

Settings > Credential Providers > Edit credential provider

**Credential Providers**

- 1 General
- 2 Certificate Signing Request
- 3 Distribution
- 4 Revocation Endpoint Management
- 5 Revocation PKI
- 6 Renewal

**Credential Providers: General Information**

You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for the certificate renewal or revocation, if any.

Name \* Discretionary Provider

Description test

Issuing entity Discretionary CA

Issuing method SIGN

- **Name:** Type a unique name for the new provider configuration. This name is used later to identify the configuration in other parts of the Endpoint Management console.
- **Description:** Describe the credential provider. Although this field is optional, a description can provide useful details about this credential provider.
- **Issuing entity:** Select **Discretionary CA**.
- **Issuing method:** Click **Sign** or **Fetch** to serve as the method that the system uses to obtain certificates from the configured entity. For client certificate authentication, use **Sign**.

3. Click **Next**. On the **Credential Providers: Certificate Signing Request** page, configure the following according to your certificate configuration:

Settings > Credential Providers > Edit credential provider

**Credential Providers**

- 1 General
- 2 Certificate Signing Request
- 3 Distribution
- 4 Revocation Endpoint Management
- 5 Revocation PKI
- 6 Renewal

**Credential Providers: Certificate Signing Request**

Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.

Key algorithm RSA

Key size \* 2048

Signature algorithm SHA256withRSA

Subject name \* cn=Suser.username

Subject alternative names

Type	Value *	Add
User Principal name	Suser.userprincipalname	

- **Key algorithm:** Choose the key algorithm for the new key pair. Available values are **RSA**, **DSA**, and **ECDSA**.
- **Key size:** Type the size, in bits, of the key pair. This field is required. Citrix recommends using **2048** bits.
- **Signature algorithm:** Click a value for the new certificate. Values depend on the key algorithm. Citrix recommends **SHA256withRSA**.

- **Subject name:** Required. Type the Distinguished Name (DN) of the new certificate subject. Use `CN=${ user.username }` for the user name or `CN=${ user.samaccountname }` to use the sAMAccountName.
- To add an entry to the **Subject alternative names** table, click **Add**. Select the type of alternative name and then type a value in the second column.

Add the following:

- **Type:** User Principal name
- **Value:** `$user.userprincipalname`

As with the subject name, you can use Endpoint Management macros in the value field.

4. Click **Next**. On the **Credential Providers: Distribution** page, configure the following:

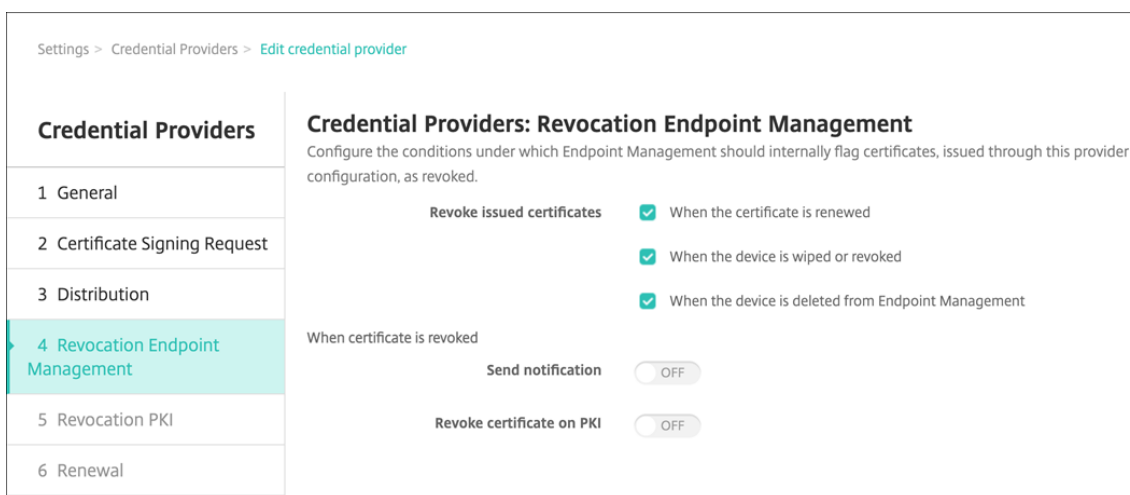
Settings > Credential Providers > Edit credential provider

Credential Providers	Credential Providers: Distribution
1 General	Issuing CA certificate <input type="text"/>
2 Certificate Signing Request	<input type="button" value="Import CA certificate"/>
3 Distribution	Select distribution mode
4 Revocation Endpoint Management	<input checked="" type="radio"/> Prefer centralized: Server-side key generation
5 Revocation PKI	<input type="radio"/> Prefer distributed: Device-side key generation
6 Renewal	<input type="radio"/> Only distributed: Device-side key generation

- **Issuing CA certificate:** Select the discretionary CA certificate you added previously.
- **Select distribution mode:** Select one of the following ways of generating and distributing keys:
  - **Prefer centralized: Server-side key generation:** Citrix recommends this centralized option. It supports all platforms supported by Endpoint Management and is required when using Citrix Gateway authentication. The private keys are generated and stored on the server and distributed to user devices.
  - **Prefer distributed: Device-side key generation:** The private keys are generated and stored on the user devices. This distributed mode uses SCEP and requires an RA encryption certificate with the `keyUsage keyEncryption` and an RA signing certificate with the `KeyUsage digitalSignature`. The same certificate can be used for both encryption and signing.
  - **Only distributed: Device-side key generation:** This option works the same as **Prefer distributed: Device-side key generation**, except that no option is available if device-side key generation fails or is unavailable.

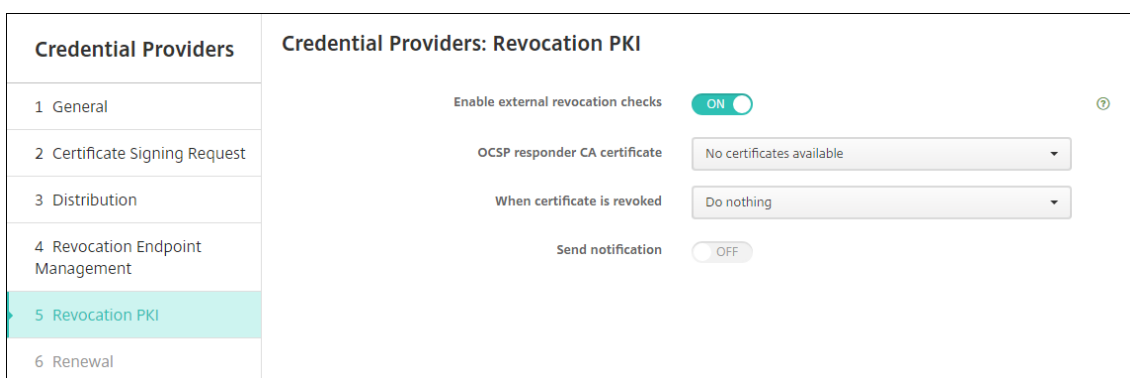
If you selected **Prefer distributed: Device-side key generation** or **Only distributed: Device-side key generation**, click the RA signing certificate and RA encryption certificate. The same certificate can be used for both. New fields appear for these certificates.

5. Click **Next**. On the **Credential Providers: Revocation Endpoint Management** page, configure the conditions under which Endpoint Management internally flags certificates, issued through this provider configuration, as revoked. Configure the following:



- In **Revoke issued certificates**, select one of the options indicating when to revoke certificates.
- To direct Endpoint Management to send a notification when the certificate is revoked: Set the value of **Send notification** to **On** and choose a notification template.
- **Revoke certificate on PKI** doesn't work when using Endpoint Management as your discretionary PKI.

6. Click **Next**. On the **Credential Providers: Revocation PKI** page, identify what actions to take on the PKI if the certificate is revoked. You also have the option of creating a notification message. Configure the following:



- **Enable external revocation checks**: Turn this setting **On**. More fields related to revocation PKI appear.

- In the **OCS responder CA certificate** list, select the distinguished name (DN) of the certificate's subject.

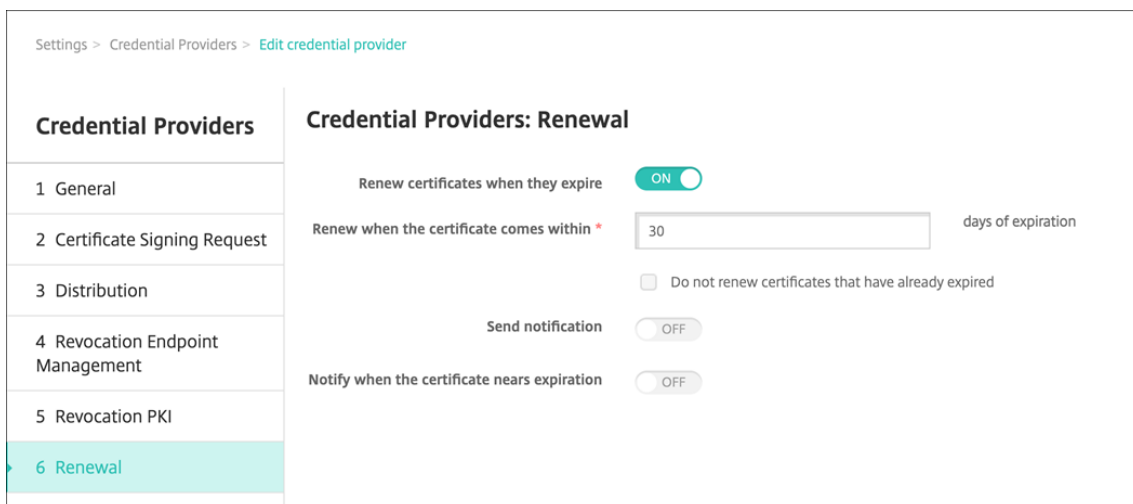
You can use Endpoint Management macros for the DN field values. For example: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`

- In the **When certificate is revoked** list, click one of the following actions to take on the PKI entity when the certificate is revoked:
  - Do nothing.
  - Renew the certificate.
  - Revoke and wipe the device.
- To direct Endpoint Management to send a notification when the certificate is revoked: Set the value of **Send notification** to **On**.

You can choose between two notification options:

- If you select **Select notification template**, you can select a pre-written notification message which you can then customize. These templates are in the Notification template list.
- If you select **Enter notification details**, you can write your own notification message. In addition to providing the recipient's email address and the message, you can set how often the notification is sent.

7. Click **Next**. On the **Credential Providers: Renewal** page, configure the following:



Set **Renew certificates when they expire** to **On**. More fields appear.

- In the **Renew when the certificate comes within** field, type how many days before expiration to renew the certificate.

- Optionally, select **Do not renew certificates that have already expired**. In this case, “already expired” means that the `NotAfter` date is in the past, not that it has been revoked. Endpoint Management doesn’t renew certificates after they are internally revoked.

To direct Endpoint Management to send a notification when the certificate has been renewed: Set **Send notification** to **On**. To direct Endpoint Management to send a notification when the certification nears expiration: Set **Notify when certificate nears expiration** to **On**.

For either of those choices, you can choose between two notification options:

- **Select notification template:** Select a pre-written notification message which you can then customize. These templates are in the Notification template list.
- **Enter notification details:** Write your own notification message. Provide the recipient’s email address, a message, and a frequency for sending the notification.

8. Click **Save**.

## Credential providers

September 8, 2021

Credential providers are the actual certificate configurations you use in the various parts of the Endpoint Management system. Credential providers define the sources, parameters, and life cycles of your certificates. Those operations occur whether the certificates are part of device configurations or are standalone (that is, pushed as is to the device).

Device enrollment constrains the certificate life cycle. That is, Endpoint Management does not issue certificates before enrollment, although Endpoint Management may issue some certificates as part of enrollment. In addition, certificates issued from the internal PKI within the context of one enrollment are revoked when the enrollment is revoked. After the management relationship terminates, no valid certificate remains.

You may use one credential provider configuration in multiple places, to the effect that one configuration may govern any number of certificates at the same time. The unity, then, is on the deployment resource and the deployment. For example, if Credential Provider P is deployed to device D as part of configuration C: The issuance settings for P determine the certificate that is deployed to D. Likewise, the renewal settings for D apply when C is updated. And, the revocation settings for D also apply when C is deleted or when D is revoked.

According to those rules, the credential provider configuration in Endpoint Management determines the following:

- The source of certificates.

- The method in which certificates are obtained: Signing a new certificate or fetching (recovering) an existing certificate and key pair.
- The parameters for issuance or recovery. For example, Certificate Signing Request (CSR) parameters, such as key size, key algorithm, and certificate extensions.
- The manner in which certificates are delivered to the device.
- Revocation conditions. Although all certificates are revoked in Endpoint Management when the management relationship is severed, the configuration may specify an earlier revocation. For instance, the configuration can specify to revoke a certificate when the associated device configuration is deleted. In addition, under some conditions, the revocation of the associated certificate in Endpoint Management may be sent to the back-end public key infrastructure (PKI). That is, certificate revocation in Endpoint Management may cause certificate revocation on the PKI.
- Renewal settings. Certificates obtained through a given credential provider can automatically renew when they near expiration. Or, separately from that situation, notifications can be issued when that expiration approaches.

The availability of configuration options mainly depends on the type of PKI Entity and issuance method that you select for a credential provider.

### Methods of certificate issuance

You can obtain a certificate, which is known as methods of issuance in two ways:

- **Sign:** With this method, the issuance involves creating a new private key, creating a CSR, and submitting the CSR to a Certificate Authority (CA) for signature. Endpoint Management supports the sign method for the three PKI entities (MS Certificate Services Entity, Generic PKI, and Discretionary CA).
- **Fetch:** With this method, the issuance, for the purposes of Endpoint Management, is a recovery of an existing key pair. Endpoint Management supports the fetch method only for Generic PKI.

A credential provider uses the sign or fetch method of issuance. The selected method affects the available configuration options. Notably, CSR configuration and distributed delivery are available only if the issuing method is sign. A fetched certificate is always sent to the device as a PKCS #12, the equivalent of centralized delivery mode for the sign method.

### Certificate Delivery

Two modes of certificate delivery are available in Endpoint Management: centralized and distributed. Distributed mode uses Simple Certificate Enrollment Protocol (SCEP) and is only available in situations in which the client supports the protocol (iOS only). Distributed mode is mandatory in some situations.

For a credential provider to support distributed (SCEP-assisted) delivery, a special configuration step is necessary: Setting up Registration Authority (RA) certificates. The RA certificates are required, because, if you use the SCEP protocol, Endpoint Management acts like a delegate (a registrar) to the actual certificate authority. Endpoint Management must prove to the client that it has the authority to act as such. That authority is established by uploading the previously mentioned certificates to Endpoint Management.

Two distinct certificate roles are required (although a single certificate can fulfill both requirements): RA signature and RA encryption. The constraints for these roles are as follows:

- The RA signing certificate must have the X.509 key usage digital signature.
- The RA encryption certificate must have the X.509 key usage key encipherment.

To configure the credential provider RA certificates, you upload the certificates to Endpoint Management and then link to them in the credential provider.

A credential provider is considered to support distributed delivery only if the provider has a certificate configured for certificate roles. You can configure each credential provider to either prefer centralized mode, to prefer distributed mode, or to require distributed mode. The actual result depends on the context: If the context does not support distributed mode, but the credential provider requires this mode, deployment fails. Likewise, if the context requires distributed mode, but the credential provider does not support distributed mode, deployment fails. In all other cases, the preferred setting is honored.

The following table shows SCEP distribution throughout Endpoint Management:

Context	SCEP supported	SCEP required
iOS Profile Service	Yes	Yes
iOS mobile device management enrollment	Yes	No
iOS configuration profiles	Yes	No
SHTTP enrollment	No	No
SHTTP configuration	No	No
Windows Phone and Tablet enrollment	No	No
Windows Phone and Tablet configuration	No, except for the network device policy, which is supported for Windows Phone 8.1, Windows 10 and Windows 11 releases	No



## Certificate Revocation

There are three types of revocation.

- **Internal revocation:** Internal revocation affects the certificate status as maintained by Endpoint Management. Endpoint Management considers this status when evaluating a presented certificate, or when providing OCSP status information for a certificate. The credential provider configuration determines how this status is affected under various conditions. For instance, the credential provider might specify to flag certificates as revoked when the certificates are deleted from the device.
- **Externally propagated revocation:** Also known as Revocation Endpoint Management, this type of revocation applies to certificates obtained from an external PKI. The certificate is revoked on the PKI when Endpoint Management internally revokes the certificate, under the conditions defined by the credential provider configuration. The call to perform the revocation requires a revoke-capable General PKI (GPKI) entity.
- **Externally induced revocation:** Also known as Revocation PKI, this type of revocation also only applies to certificates obtained from an external PKI. Whenever Endpoint Management evaluates a given certificate status, Endpoint Management queries the PKI as to that status. If the certificate is revoked, Endpoint Management internally revokes the certificate. This mechanism uses the OCSP protocol.

These three types are not exclusive, but rather apply together. An external revocation or independent finding can cause an internal revocation. An internal revocation potentially affects an external revocation.

## Certificate Renewal

A certificate renewal is the combination of a revocation of the existing certificate and an issuance of another certificate.

Endpoint Management first attempts to obtain the new certificate before revoking the previous certificate, to avoid discontinuation of service when issuance fails. For distributed (SCEP-supported) delivery, the revocation also only happens after the certificate has been successfully installed on the device. Otherwise, the revocation occurs before the new certificate is sent to the device. That revocation is independent of the success or failure of certificate installation.

The revocation configuration requires that you specify a certain duration (in days). When the device connects, the server verifies whether the certificate `NotAfter` date is later than the current date, minus the specified duration. If the certificate meets that condition, Endpoint Management attempts to renew the certificate.

## Create a credential provider

Configuring a credential provider varies mostly as a factor of which issuing entity and which issuing method you select for the credential provider. You can distinguish between credential providers that use an internal entity or an external entity:

- A discretionary entity, which is internal to Endpoint Management, is an internal entity. The issuing method for a discretionary entity is always sign. Sign means that with each issuing operation, Endpoint Management signs a new key pair with the CA certificate selected for the entity. Whether the key pair is generated on the device or on the server depends on the distribution method you select.
- An external entity, which is part of your corporate infrastructure, includes Microsoft CA or a GPKI.

For detailed information about setting up DigiCert Managed PKI, including creating the credential provider, see “DigiCert Managed PKI” in [PKI entities](#).

1. In the Endpoint Management console, click the gear icon in the upper-right corner and then click **Settings > Credential Providers**.
2. On the **Credential Providers** page, click **Add**.

The **Credential Providers: General Information** page appears.

3. On the **Credential Providers: General Information** page, do the following:
  - **Name:** Type a unique name for the new provider configuration. This name is used later to identify the configuration in other parts of the Endpoint Management console.
  - **Description:** Describe the credential provider. Although this field is optional, a description can provide useful details about this credential provider.
  - **Issuing entity:** Click the certificate issuing entity.
  - **Issuing method:** Click **Sign** or **Fetch** to serve as the method that the system uses to obtain certificates from the configured entity. For client certificate authentication, use **Sign**.
  - If the **Template** list is available, select the template that you added under the PKI entity for the credential provider.

These templates become available when Microsoft Certificate Services Entities are added at **Settings > PKI Entities**.

4. Click **Next**.

The **Credential Providers: Certificate Signing Request** page appears.

5. On the **Credential Providers: Certificate Signing Request** page, configure the following according to your certificate configuration:

- **Key algorithm:** Choose the key algorithm for the new key pair. Available values are **RSA**, **DSA**, and **ECDSA**.
- **Key size:** Type the size, in bits, of the key pair. This field is required.

The permissible values depend on the key type. For example, the maximum size for DSA keys is 2048 bits. To avoid false negatives, which depends on the underlying hardware and software, Endpoint Management doesn't enforce key sizes. Always test credential provider configurations in a test environment before activating them in production.

- **Signature algorithm:** Click a value for the new certificate. Values depend on the key algorithm.
- **Subject name:** Required. Type the Distinguished Name (DN) of the new certificate subject. For example:  
`CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`

For example, for client certificate authentication, use these settings:

- **Key algorithm:** RSA
  - **Key size:** 2048
  - **Signature algorithm:** SHA256withRSA
  - **Subject name:** `cn=${user.username}`
- To add an entry to the **Subject alternative names** table, click **Add**. Select the type of alternative name and then type a value in the second column.

For client certificate authentication, specify:

- **Type:** User Principal name
- **Value:** `${user.userprincipalname}`

As with Subject name, you can use Endpoint Management macros in the value field.

6. Click **Next**.

The **Credential Providers: Distribution** page appears.

7. On the **Credential Providers: Distribution** page, do the following:

- In the **Issuing CA certificate** list, click the offered CA certificate. Because the credential provider uses a discretionary CA entity, the CA certificate for the credential provider is always the CA certificate configured on the entity itself. The CA certificate is presented here for consistency with configurations that use external entities.
- In **Select distribution mode**, click one of the following ways of generating and distributing keys:

- **Prefer centralized: Server-side key generation:** Citrix recommends this centralized option. It supports all platforms supported by Endpoint Management and is required when using Citrix Gateway authentication. The private keys are generated and stored on the server and distributed to user devices.
- **Prefer distributed: Device-side key generation:** The private keys are generated and stored on the user devices. This distributed mode uses SCEP and requires an RA encryption certificate with the keyUsage keyEncryption and an RA signing certificate with the KeyUsage digitalSignature. The same certificate can be used for both encryption and signing.
- **Only distributed: Device-side key generation:** This option works the same as Prefer distributed: Device-side key generation, except that since it is “Only,” rather than “Prefer,” no option is available if device-side key generation fails or is unavailable.

If you selected **Prefer distributed: Device-side key generation** or **Only distributed: Device-side key generation**, click the RA signing certificate and RA encryption certificate. The same certificate can be used for both. New fields appear for these certificates.

8. Click **Next**.

The **Credential Providers: Revocation Endpoint Management** page appears. On this page, you configure the conditions under which Endpoint Management internally flags certificates, issued through this provider configuration, as revoked.

9. On the **Credential Providers: Revocation Endpoint Management** page, do the following:

- In **Revoke issued certificates**, select one of the options indicating when to revoke certificates.
- To direct Endpoint Management to send a notification when the certificate is revoked: Set the value of **Send notification** to **On** and choose a notification template.
- To revoke the certificate on PKI when the certificate is revoked from Endpoint Management: Set **Revoke certificate on PKI** to **On** and, in the **Entity list**, click a template. The Entity list shows all available GPKI entities with revocation capabilities. When the certificate is revoked from Endpoint Management, a revocation call is sent to the PKI selected from the Entity list.

10. Click **Next**.

The **Credential Providers: Revocation PKI** page appears. On this page, you identify what actions to take on the PKI if the certificate is revoked. You also have the option of creating a notification message.

11. On the **Credential Providers: Revocation PKI** page, do the following if you want to revoke certificates from the PKI:

- Change the setting of **Enable external revocation checks** to **On**. More fields related to revocation PKI appear.
- In the **OCSP responder CA certificate** list, click the distinguished name (DN) of the certificate's subject.

You can use Endpoint Management macros for the DN field values. For example: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`

- In the **When certificate is revoked** list, click one of the following actions to take on the PKI entity when the certificate is revoked:
  - Do nothing.
  - Renew the certificate.
  - Revoke and wipe the device.
- To direct Endpoint Management to send a notification when the certificate is revoked: Set the value of **Send notification** to **On**.

You can choose between two notification options:

- If you select **Select notification template**, you can select a pre-written notification message which you can then customize. These templates are in the Notification template list.
- If you select **Enter notification details**, you can write your own notification message. In addition to providing the recipient's email address and the message, you can set how often the notification is sent.

12. Click **Next**.

The **Credential Providers: Renewal** page appears. On this page, you can configure Endpoint Management to do the following:

- Renew the certificate. You can optionally send a notification on renewal, and optionally exclude already expired certificates from the operation.
- Issue a notification for certificates that near expiration (notification before renewal).

13. On the **Credential Providers: Renewal** page, do the following if you want to renew certificates when they expire:

Set **Renew certificates** when they expire to **On**. More fields appear.

- In the **Renew when the certificate comes within** field, type how many days before expiration to renew the certificate.
- Optionally, select **Do not renew certificates that have already expired**. In this case, "already expired" means that the `NotAfter` date is in the past, not that it has been revoked. Endpoint Management doesn't renew certificates after they are internally revoked.

To direct Endpoint Management to send a notification when the certificate has been renewed: Set **Send notification** to **On**. To direct Endpoint Management to send a notification when the certification nears expiration: Set **Notify when certificate nears expiration** to **On**.

For either of those choices, you can choose between two notification options:

- **Select notification template:** Select a pre-written notification message which you can then customize. These templates are in the Notification template list.
- **Enter notification details:** Write your own notification message. Provide the recipient's email address, a message, and a frequency for sending the notification.

In the **Notify when the certificate comes within** field, type how many days before the certificate's expiration to send the notification.

14. Click **Save**.

The credential provider appears in the Credential Provider table.

## APNs certificates

February 5, 2021

To enroll and manage Apple devices in Endpoint Management, you set up an Apple Push Notification service (APNs) certificate from Apple. The certificate enables mobile device management through the Apple Push Network.

Workflow summary:

**Step 1:** Create a Certificate Signing Request (CSR) through any of these methods:

- Create a CSR by using Keychain Access on macOS (recommended by Citrix)
- Create a CSR by using Microsoft IIS
- Create a CSR by using OpenSSL

**Step 2:** Sign the CSR in Endpoint Management Tools

**Step 3:** Submit the signed CSR to Apple to obtain the APNs certificate

**Step 4:** Using the same computer used for Step 1, Complete the CSR and export a PKCS #12 file:

- Create a PKCS #12 file by using Keychain Access on macOS
- Create a PKCS #12 file by using Microsoft IIS
- Create a PKCS #12 file by using OpenSSL

**Step 5:** Import an APNs certificate into Endpoint Management

**Step 6:** Renew an APNs certificate

## Create a Certificate Signing Request

We recommend that you create a CSR by using Keychain Access on macOS. You can also create a CSR by using Microsoft IIS or OpenSSL.

### Important:

- For the Apple ID used to create the certificate:
  - The Apple ID must be a corporate ID and not a personal ID.
  - Record the Apple ID that you use to create the certificate.
  - To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate require device re-enrollment.
- If you accidentally or intentionally revoke the certificate, you lose the ability to manage your devices.
- If you used the iOS Developer Enterprise Program to create a mobile device manager push certificate: Be sure to handle any actions for the migrated certificates in the Apple Push Certificates Portal.

## Create a CSR by using Keychain Access on macOS

1. On a computer running macOS, under **Applications > Utilities**, start the Keychain Access app.
2. Open the **Keychain Access** menu and then click **Certificate Assistant > Request a Certificate From a Certificate Authority**.
3. The Certificate Assistant prompts you to enter the following information:
  - **Email Address:** Email address of the individual or role account who is responsible for managing the certificate.
  - **Common Name:** Common name of the individual or a role account who is responsible for managing the certificate.
  - **CA Email Address:** Email address of the Certificate Authority.
4. Select the **Saved to disk** and **Let me specify key pair information** options and then click **Continue**.
5. Enter a name for the CSR file, save the file on your computer, and then click **Save**.
6. Specify the key pair information: Select the **Key Size** of 2048 bits and the **RSA algorithm** and then click **Continue**. The CSR file is ready for you to upload as part of the APNs certificate process.
7. Click **Done** when the Certificate Assistant completes the CSR process.
8. To continue, Sign the CSR.

### Create a CSR by using Microsoft IIS

The first step for generating an APNs certificate request is to create a Certificate Signing Request (CSR). For Windows, generate a CSR by using Microsoft IIS.

1. Open Microsoft IIS.
2. Double-click the Server Certificates icon for IIS.
3. In the **Server Certificates** window, click **Create Certificate Request**.
4. Type the appropriate Distinguished Name (DN) information. For example, you can type the fully qualified domain name (FQDN) of your Endpoint Management server, such as `www.domain.com`. Then click **Next**.
5. Select **Microsoft RSA SChannel Cryptographic Provider** for the Cryptographic Service Provider and **2048** for bit length and then click **Next**.
6. Enter a file name and specify a location to save the CSR and then click **Finish**.
7. To continue, Sign the CSR.

### Create a CSR by using OpenSSL

If you can't use a macOS device or Microsoft IIS to generate a CSR, use OpenSSL. You can download and install OpenSSL from the OpenSSL website.

1. On the computer where you install OpenSSL, execute the following command from a command prompt or shell.

```
openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.csr -newkey rsa:2048
```

2. The following message for certificate naming information appears. Enter the information as requested.

```
1 You are about to be asked to enter information that will be
   incorporated into your certificate request.
2 What you are about to enter is what is called a Distinguished Name
   or a DN.
3 There are quite a few fields but you can leave some blank
4 For some fields there will be a default value,
5 If you enter '.', the field will be left blank.
6 -----
7 Country Name (2 letter code) [AU]:US
8 State or Province Name (full name) [Some-State]:CA
9 Locality Name (eg, city) []:RWC
10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
    Customer
11 Organizational Unit Name (eg, section) [:Marketing]
12 Common Name (eg, YOUR name) []:John Doe
```



```
13 Email Address []:john.doe@customer.com
14 <!--NeedCopy-->
```

3. At the next message, enter a password for the CSR private key.

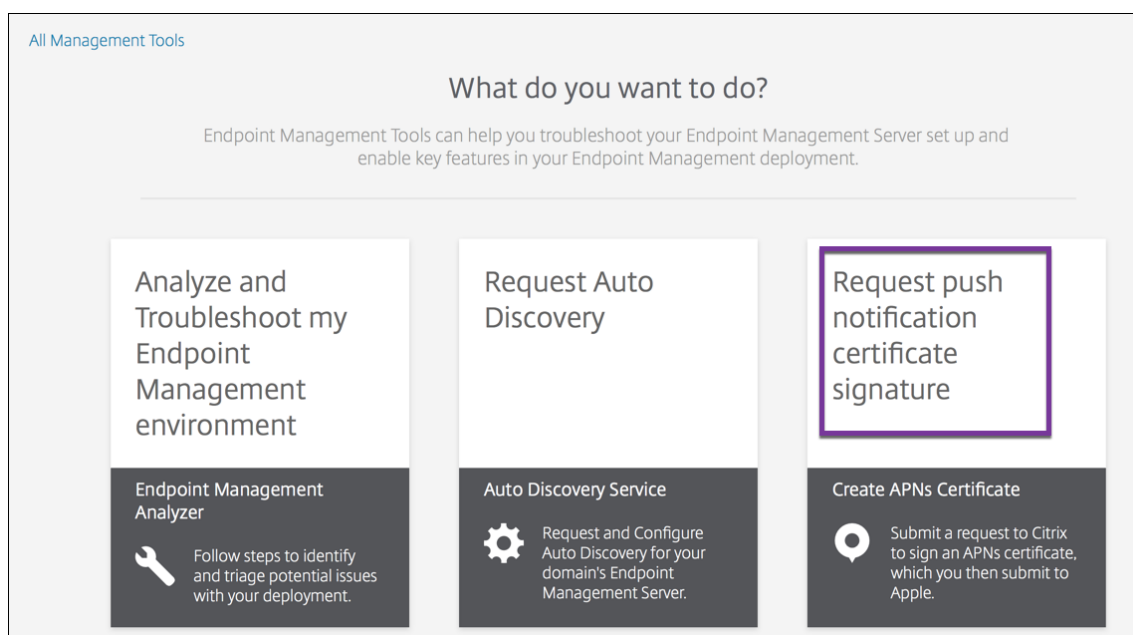
```
1 Please enter the following 'extra' attributes
2 to be sent with your certificate request
3 A challenge password []:
4 An optional company name []:
5 <!--NeedCopy-->
```

4. To continue, sign the CSR as described in the next section.

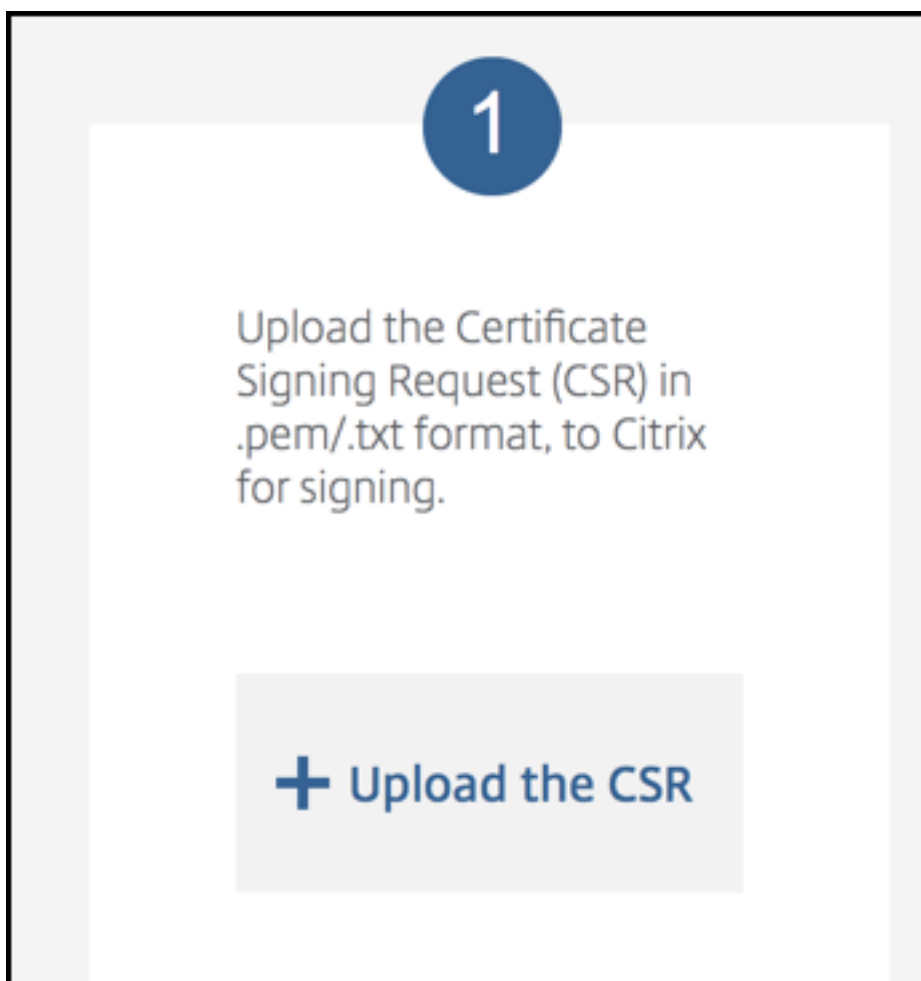
## Sign the CSR

To use a certificate with Endpoint Management, you must submit it to Citrix for signing. Citrix signs the CSR with its mobile device management signing certificate and returns the signed file in a `.plist` format.

1. In your browser, go to the [Endpoint Management Tools](#) website and then click **Request push notification certificate signature**.



2. On the **Creating a new certificate page**, click **Upload the CSR**.



3. Browse to and select the certificate.

The certificate must be in .pem/txt format.

4. On the **Endpoint Management APNs CSR Signing** page, click **Sign**. The CSR is signed and automatically saved to your configured download folder.
5. To continue, submit the signed CSR as described in the next section.

### **Submit the signed CSR to Apple to obtain the APNs certificate**

After receiving your signed Certificate Signing Request (CSR) from Citrix, submit the CSR to Apple to obtain the APNs certificate needed to import into Endpoint Management.

**Note:**

Some users have reported problems logging into the Apple Push Portal. As an alternative, you can log on to the [Apple Developer Portal](#). You can then follow these steps.

1. In a browser, go to the [Apple Push Certificates Portal](#).

2. Click **Create a Certificate**.
3. The first time that you create a certificate with Apple: Select the **I have read and agree to these terms and conditions** check box, and then click **Accept**.
4. Click **Choose File**, browse to the signed CSR on your computer, and then click **Upload**. A confirmation message indicates that the upload succeeds.
5. Click **Download** to retrieve the .pem certificate.
6. To continue, complete the CSR and export a PKCS #12 file as described in the next section.

### Complete the CSR and export a PKCS #12 file

After you receive the APNs certificate from Apple, return to Keychain Access, Microsoft IIS, or OpenSSL to export the certificate into a PKCS #12 file.

A PKCS #12 file contains the APNs certificate file and your private key. PFX files usually have the extension .pfx or .p12. You can use .pfx and .p12 files interchangeably.

#### Important:

Citrix recommends you save or export the personal and public keys from the local system. You need the keys to access the APNs certificates for reuse. Without the same keys, your certificate is invalid and you must repeat the entire CSR and APNs process.

### Create a PKCS #12 file by using Keychain Access on macOS

#### Important:

Use the same macOS device for this task that you used to generate the CSR.

1. On the device, locate the Production identity (.pem) certificate that received from Apple.
2. Start the Keychain Access application and navigate to the **Login > My Certificates** tab. Drag and then drop the Product identity certificate onto the open window.
3. Click the certificate and expand the left arrow to verify that the certificate includes an associated private key.
4. To begin exporting the certificate into a PKCS #12 (.pfx) certificate, choose the certificate and private key, right-click, and select **Export 2 items**.
5. Give the certificate file a unique name for use with Endpoint Management. Don't include space characters in the name. Then, choose a folder location for the saved certificate, select the .pfx file format, and click **Save**.
6. Enter a password for exporting the certificate. Citrix recommends that you use a unique, strong password. Also, be sure to keep the certificate and password safe for later use and reference.

7. The Keychain Access app prompts you for the login password or selected keychain. Type the password, and then click **OK**. The saved certificate is now ready for use with the Endpoint Management server.
8. To continue, see Import an APNs certificate into Endpoint Management.

### Create a PKCS #12 file by using Microsoft IIS

#### Important:

Use the same IIS server for this task that you used to generate the CSR.

1. Open Microsoft IIS.
2. Click the **Server Certificates** icon.
3. In the **Server Certificates** window, click **Complete Certificate Request**.
4. Browse to the Certificate.pem file from Apple. Then, type a friendly name or the certificate name and click **OK**. Don't include space characters in the name.
5. Select the certificate that you identified in Step 4, and then click **Export**.
6. Specify a location and file name for the .pfx certificate and a password, and then click **OK**.  
You need the password for the certificate to import it into Endpoint Management.
7. Copy the .pfx certificate to the server on which you plan to install Endpoint Management.
8. To continue, see Import an APNs certificate into Endpoint Management.

### Create a PKCS #12 file by using OpenSSL

If you use OpenSSL to create a CSR, you can also use OpenSSL to create a .pfx APNs certificate.

1. At a command prompt or shell, execute the following command. `Customer.privatekey.pem` is the private key from your CSR. `APNs_Certificate.pem` is the certificate that you just received from Apple.

```
openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey.pem -out apns_identity.pfx
```

2. Enter a password for the .pfx certificate file. Remember this password because you use the password again when you upload the certificate to Endpoint Management.
3. Note the location for the .pfx certificate file. Then, copy the file to the Endpoint Management server so you can use the console to upload the file.
4. To continue, import an APNs certificate into Endpoint Management as described in the next section.

## Import an APNs certificate into Endpoint Management

After you receive the new APNs certificate: Import the APNs certificate into Endpoint Management to either add the certificate for the first time or to replace a certificate.

1. In the Endpoint Management console, go to **Settings > Certificates**.
2. Click **Import > Keystore**.
3. From **Use as**, choose **APNs**.
4. Browse to the .pfx or .p12 file on your computer.
5. Enter a password, and then click **Import**.

For more information about certificates in Endpoint Management, see [Certificates and authentication](#).

## Renew an APNs certificate

### Important:

If you use a different Apple ID for the renewal process, you must reenroll user devices.

To renew an APNs certificate, perform the steps to create a certificate, then go to the [Apple Push Certificates Portal](#). Use that portal to upload the new certificate. After logging on, your existing certificate or a certificate imported from your previous Apple Developers account appears.

In the Certificates Portal, the only difference when renewing the certificate is that you click **Renew**. You must have a developer account with the Certificates Portal to access the site. To renew your certificate, use the same organization name and Apple ID.

To determine when your APNs certificate expires, in the Endpoint Management console, go to **Settings > Certificates**. If the certificate expires, do not revoke it.

1. Generate a CSR, using Microsoft IIS, Keychain Access (macOS), or OpenSSL. For more information on generating a CSR, see [Create a Certificate Signing Request](#).
2. In your browser, go to [Endpoint Management Tools](#). Then, click **Request push notification certificate signature**.
3. Click **+ Upload the CSR**.
4. In the dialog box, navigate to the CSR, click **Open**, and click **Sign**.
5. When you receive a .plist file, save it.
6. In the step 3 title, click **Apple Push Certificates Portal** and sign on.
7. Select the certificate that you want to renew, and then click **Renew**.
8. Upload the .plist file. You receive a .pem file as the output. Save the .pem file.

- Using that .pem file, complete the CSR (according to the method you used to create the CSR in Step 1).
- Export the certificate as a .pfx file.

In the Endpoint Management console, import the .pfx file and complete the configuration as follows:

- Go to **Settings > Certificates > Import**.
- From the **Import menu**, choose **Keystore**.
- From the **Keystore type** menu, choose **PKCS #12**.
- From **Use as**, choose **APNs**.

**Import** ✕

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time. Use the [APNs portal](#) on the Endpoint Management Tools page to create the APNs certificate.

**Import** Keystore

**Keystore type** PKCS#12

**Use as** APNs

**Keystore file \***

**Password \***

**Description**

- For **Keystore file**, click **Browse** and navigate to the file.
- In **Password**, type the certificate password.
- Type an optional **Description**.
- Click **Import**.

Endpoint Management redirects you back to the **Certificates** page. The **Name**, **Status**, **Valid from**, and **Valid to** fields update.

## SAML for single sign-on with Citrix Files

October 7, 2021

### Important:

This article applies only to Endpoint Management environments that aren't Workspace-enabled. In a Workspace-enabled environment, Content Collaboration is integrated directly with Citrix Workspace.

You can configure Endpoint Management and Content Collaboration to use the Security Assertion Markup Language (SAML) to provide single sign-on (SSO) access to Citrix Files mobile apps. This functionality includes:

- Citrix Files apps that are MAM SDK enabled or wrapped by using the MDX Toolkit
- Non-wrapped Citrix Files clients, such as the website, Outlook plug-in, or sync clients
- **For wrapped Citrix Files apps:** Users who log on to Citrix Files get redirected to Secure Hub for user authentication and to acquire a SAML token. After successful authentication, the Citrix Files mobile app sends the SAML token to Content Collaboration. After the initial logon, users can access the Citrix Files mobile app through SSO. They can also attach documents from Content Collaboration to Secure Mail mails without logging on each time.
- **For non-wrapped Citrix Files clients:** Users who log on to Citrix Files using a web browser or other Citrix Files client are redirected to Endpoint Management. Endpoint Management authenticates the users, who then acquire a SAML token which is sent to Content Collaboration. After the initial logon, users can access Citrix Files clients through SSO without logging on each time.

To use Endpoint Management as a SAML identity provider (IdP) to Content Collaboration, you must configure Endpoint Management for use with Enterprise accounts, as described in this article. Alternatively, you can configure Endpoint Management to work only with storage zone connectors. For more information, see [Content Collaboration use with Endpoint Management](#).

For a detailed reference architecture diagram, see [Architecture](#).

### Prerequisites

Complete the following prerequisites before you can configure SSO with Endpoint Management and Citrix Files apps:

- The MAM SDK or a compatible version of the MDX Toolkit (for Citrix Files mobile apps).  
For more information, see [Endpoint Management compatibility](#).
- A compatible version of Citrix Files mobile apps and Secure Hub.

- Content Collaboration administrator account.
- Connectivity verified between Endpoint Management and Content Collaboration.

## Configure Content Collaboration access

Before setting up SAML for Content Collaboration, provide Content Collaboration access information as follows:

1. In the Endpoint Management web console, click **Configure > Content Collaboration**. The **Content Collaboration** configuration page appears.

The screenshot shows the 'Content Collaboration' configuration page. At the top, there is a title 'Content Collaboration' with a dropdown arrow and a subtitle 'Configure settings to connect to the Content Collaboration and administrator service accounts for user account management.' Below this, there are several sections:

- Domain \***: A text input field containing '.sharefile.com'.
- Assign to delivery groups**: A search input field with the placeholder 'Type to search' and a magnifying glass icon. To the right is a blue 'Search' button. Below the search field is a list of delivery groups with checkboxes: 'AllUsers', 'Local Policy', 'o87', and 'Local'. All checkboxes are currently unchecked.
- Content Collaboration Administrator Account Logon**: This section contains:
  - User name \***: A text input field with a placeholder ending in '.com'.
  - Password \***: A text input field with the placeholder 'Enter new password'.
  - Test Connection**: A green button.
  - User account provisioning**: A toggle switch currently set to 'OFF'.
  - App Internal name**: A text input field containing 'ShareFile\_SAML'.
- SAML certificate**: A section with a **Name** text input field containing '.example.com'.

At the bottom left of the form, it says 'Advanced Content Collaboration Configuration'.

2. Configure these settings:

- **Domain:** Type your Content Collaboration subdomain name. For example: `example.sharefile.com`.
- **Assign to delivery groups:** Select or search for the delivery groups that you want to be able to use SSO with ShareFile.
- **Content Collaboration Administrator Account Logon**
- **User name:** Type the Content Collaboration administrator user name. This user must have administrator privileges.



- **Password:** Type the Content Collaboration administrator password.
  - **User account provisioning:** Leave this setting disabled. Use the Content Collaboration User Management Tool for user provisioning. See [Provision user accounts and distribution groups](#).
3. Click **Test Connection** to verify that the user name and password for the Content Collaboration administrator account authenticate to the specified Content Collaboration account.
  4. Click **Save**.
    - Endpoint Management syncs with Content Collaboration and updates the Content Collaboration settings **ShareFile Issuer/Entity ID** and **Login URL**.
    - The **Configure > Content Collaboration** page shows the **App internal name**. You need that name to complete the steps described later in Modify the Citrix Files.com SSO settings.

### Set up SAML for Wrapped Citrix Files MDX Apps

You don't need to use Citrix Gateway for single sign-on configuration with Citrix Files apps prepared with the MAM SDK. To configure access for non-wrapped Citrix Files clients, such as the website, Outlook plug-in, or the sync clients, see [Configure the Citrix Gateway for Other Citrix Files Clients](#).

To configure SAML for wrapped Citrix Files MDX apps:

1. Download the Citrix Content Collaboration for Endpoint Management clients. See [Citrix.com downloads](#).
2. Prepare the Citrix Files mobile app with the MAM SDK. For details, see [MAM SDK overview](#).
3. In the Endpoint Management console, upload the prepared Citrix Files mobile app. For information about uploading MDX apps, see [To add an MDX app to Endpoint Management](#).
4. Verify the SAML settings: Log on to Content Collaboration with the administrator user name and password you configured earlier.
5. Verify that Content Collaboration and Endpoint Management are configured for the same time zone. Ensure that Endpoint Management shows the correct time for the configured time zone. If not, SSO might fail.

### Validate the Citrix Files mobile app

1. On the user device, install and configure Secure Hub.
2. From the app store, download and install the Citrix Files mobile app.
3. Start the Citrix Files mobile app. Citrix Files starts without prompting for user name or password.

### Validate with Secure Mail

1. On the user device, if it has not already been done, install and configure Secure Hub.
2. From the app store, download, install, and set up Secure Mail.
3. Open a new email form and then tap **Attach from ShareFile**. Files available to attach to the email are shown without asking for user name or password.

### Configure Citrix Gateway for other Citrix Files clients

To configure access for non-wrapped Citrix Files clients, such as the website, Outlook plug-in, or the sync clients: Configure Citrix Gateway to support the use of Endpoint Management as a SAML identity provider as follows.

- Disable home page redirection.
- Create a Citrix Files session policy and profile.
- Configure policies on the Citrix Gateway virtual server.

### Disable home page redirection

Disable the default behavior for requests that come through the /cginfra path. That action enables users to see the original requested internal URL instead of the configured home page.

1. Edit the settings for the Citrix Gateway virtual server that is used for Endpoint Management logons. In Citrix Gateway, go to **Other Settings** and then clear the check box labeled **Redirect to Home Page**.

The screenshot shows the 'Other Settings' configuration page in Citrix Gateway. The 'Redirect to Home page' checkbox is checked. The 'ShareFile' section shows a list of endpoints with 'Citrix Endpoint Management' highlighted in a red box. The 'L2 Connection' checkbox is unchecked. An 'OK' button is visible at the bottom.

2. Under **ShareFile** (now called Content Collaboration), type your Endpoint Management internal server name and port number.

3. Under **Citrix Endpoint Management**, type your Endpoint Management URL.

This configuration authorizes requests to the URL you entered through the /cginfra path.

### Create a Citrix Files session policy and request profile

Configure these settings to create a Citrix Files session policy and request profile:

1. In the Citrix Gateway configuration utility, in the left-hand navigation pane, click **NetScaler Gateway > Policies > Session**.
2. Create a session policy. On the **Policies** tab, click **Add**.
3. In the **Name** field, type **ShareFile\_Policy**.
4. Create an action by clicking the + button. The **Create NetScaler Gateway Session Profile** page appears.

The screenshot shows the 'Configure NetScaler Gateway Session Profile' page. The 'Name' field contains 'Sharefile\_Profile'. Below the name field, there is a note: 'Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.' The 'Client Experience' tab is selected, showing various configuration options:

- Accounting Policy: [Dropdown]
- Override Global: [Checkbox]
- Display Home Page: [Checked]
- Home Page: [none]
- URL for Web-Based Email: [Text Field]
- Split Tunnel\*: [OFF]
- Session Time-out (mins): [1]
- Client Idle Time-out (mins): [Text Field]
- Clientless Access\*: [Allow]
- Clientless Access URL Encoding\*: [Obscure]
- Clientless Access Persistent Cookie\*: [DENY]
- Plug-in Type\*: [Windows/MAC OS X]
- Single Sign-on to Web Applications: [Checked]
- Credential Index\*: [PRIMARY]
- KCD Account: [Text Field]

Configure these settings:

- **Name:** Type **ShareFile\_Profile**.

- Click the **Client Experience** tab and then configure these settings:
  - **Home Page:** Type **none**.
  - **Session Time-out (mins):** Type **1**.
  - **Single Sign-on to Web Applications:** Select this setting.
  - **Credential Index:** Click **PRIMARY**.
- Click the **Published Applications** tab.

The screenshot shows the 'Configure NetScaler Gateway Session Profile' dialog box. The 'Published Applications' tab is active. The 'Override Global' section is expanded, showing the following settings:

- ICA Proxy\*:** ON (checked)
- Web Interface Address:** (empty) (checked)
- Web Interface Address Type\*:** IPV4
- Web Interface Portal Mode\*:** NORMAL (unchecked)
- Single Sign-on Domain:** citrix (checked)
- Citrix Receiver Home Page:** (empty) (unchecked)
- Account Services Address:** (empty) (unchecked)

Buttons for 'OK' and 'Close' are visible at the bottom.

Configure these settings:

- **ICA Proxy:** Click **On**.
- **Web Interface Address:** Type your Endpoint Management server URL.
- **Single Sign-on Domain:** Type your Active Directory domain name.

When configuring the Citrix Gateway Session Profile, the domain suffix for **Single Sign-on Domain** must match the Endpoint Management domain alias defined in LDAP.

5. Click **Create** to define the session profile.
6. Click **Expression Editor**.

Configure these settings:

- **Value:** Type **NSC\_FSRD**.
- **Header Name:** Type **COOKIE**.

7. Click **Create** and then click **Close**.

### Configure policies on the Citrix Gateway virtual server

Configure these settings on the Citrix Gateway virtual server.

1. In the Citrix Gateway configuration utility, in the left navigation pane, click **NetScaler Gateway > Virtual Servers**.
2. In the **Details** pane, click your Citrix Gateway virtual server.
3. Click **Edit**.
4. Click **Configured policies > Session policies** and then click **Add binding**.

5. Select **ShareFile\_Policy**.
6. Edit the auto-generated **Priority** number for the selected policy so that it has the highest priority (the smallest number) in relation to any other policies listed. For example:

Priority	Policy Name	Expression	Action
10	ShareFile_Policy	REQ.HTTP.HEADER Cookie CONTAINS NSC_FSRD	Sharefile_Profile
100	PL_OS_10.217.232.36	REQ.HTTP.HEADER User-Agent CONTAINS CitrixR...	AC_OS_10.217.232.36_A_
100	PL_WB_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_WB_10.217.232.36_A_
100	PL_AG_PLG_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_AG_PLG_10.217.232.36_A_

7. Click **Done** and then save the running Citrix Gateway configuration.

## Modify the Citrix Files.com SSO settings

Make the following changes for both MDX and non-MDX Citrix Files apps.

### Important:

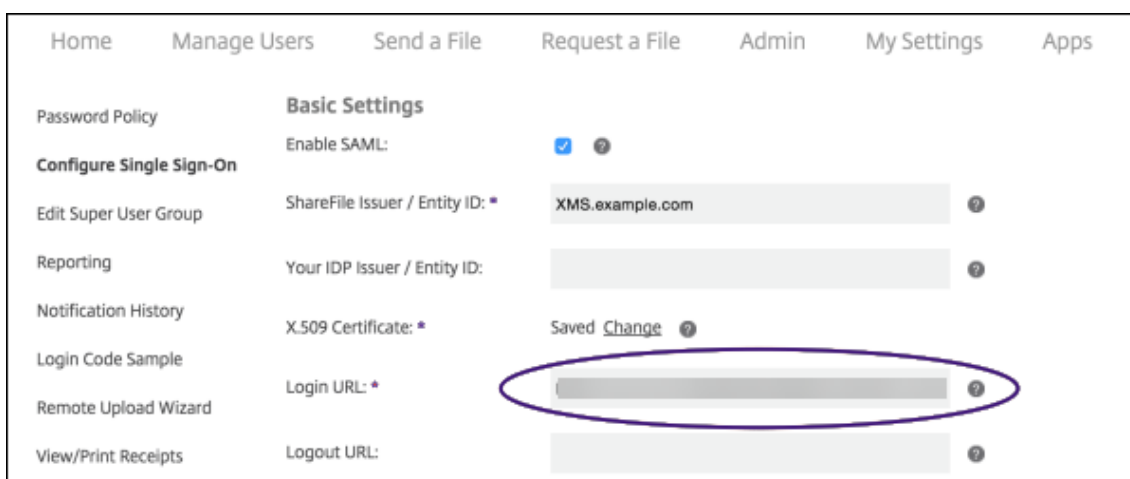
A new number is appended to the internal application name:

- Each time you edit or recreate the Citrix Files app
- Each time you change the Content Collaboration settings in Endpoint Management

As a result, you must also update the Login URL in the Citrix Files website to reflect the updated app name.

1. Log on to your Content Collaboration account (<https://<subdomain>.sharefile.com>) as a Content Collaboration administrator.
2. In the Content Collaboration web interface, click **Admin** and then select **Configure Single Sign-on**.
3. Edit the **Login URL** as follows:

Here's a sample **Login URL** before the edits: [https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile\\_SAML\\_SP&reqtype=1](https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1).



- Insert the Citrix Gateway virtual server external FQDN plus **/cginfra/https/** in front of the Endpoint Management server FQDN and then add **8443** after the Endpoint Management FQDN.

Here's a sample of an edited URL: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`

- Change the parameter `&app=ShareFile_SAML_SP` to the internal Citrix Files application name. The internal name is `ShareFile_SAML` by default. However, every time you change your configuration, a number is appended to the internal name (`ShareFile_SAML_2`, `ShareFile_SAML_3`, and so on). You can look up the **App internal name** on the **Configure > Content Collaboration** page.

Here's a sample of an edited URL: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- Add `&nssso=true` to the end of the URL.

Here's a sample of the final URL: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`.

4. Under **Optional Settings**, select the **Enable Web Authentication** check box.

**Optional Settings**

Require SSO Login:  ?

SSO IP Range:  ?

SP-Initiated SSO certificate: HTTP Redirect with no signature ?

**Enable Web Authentication:  ?**

SP-Initiated Auth Context: User Name and Password Minimum ?

Active Profile Cookies:  ?

Save Cancel

## Validate the configuration

Do the following to validate the configuration.

1. Point your browser to <https://<subdomain>sharefile.com/saml/login>.  
You are redirected to the Citrix Gateway logon form. If you are not redirected, verify the preceding configuration settings.
2. Enter the user name and password for the Citrix Gateway and Endpoint Management environment you configured.

Your Citrix Files folders at [.<subdomain>.sharefile.com](https://<subdomain>.sharefile.com) appear. If you do not see your Citrix Files folders, ensure that you entered the proper logon credentials.

## Authentication with Azure Active Directory through Citrix Cloud

July 30, 2021

Endpoint Management supports authentication with Azure Active Directory (Azure AD) credentials through Citrix Cloud. This authentication method is available only to users enrolling in MDM through the Citrix Workspace app or Citrix Secure Hub. If Endpoint Management is Workspace enabled, users access resources from the Citrix Workspace app. If you don't enable Citrix Workspace integration with Citrix Endpoint Management, users access resources from Secure Hub.

Devices enrolling in MAM can't authenticate using Azure AD credentials through Citrix Cloud. To use Secure Hub with MDM+MAM, configure Endpoint Management to use Citrix Gateway for MAM enrollment. For more information, see [Citrix Gateway and Endpoint Management](#).



Endpoint Management uses the Citrix Cloud service, Citrix identity, to federate with Azure Active Directory. Citrix recommends that you use the Citrix identity provider instead of a direct connection to Azure Active Directory.

Endpoint Management supports authentication with Azure AD for the following platforms:

- iOS devices
- Android Enterprise devices (Preview), for BYOD and fully managed modes
- Android devices that run in the legacy Device Administration mode

Authentication with Azure AD through Citrix Cloud has these limitations:

- Isn't available for Endpoint Management local accounts.
- Doesn't support authentication through Azure AD for enrollment invitations. If you send users an enrollment invitation containing an enrollment URL, users authenticate through LDAP instead of Azure AD.

### Prerequisites

- Azure Active Directory user credentials
- User groups in Active Directory must match the user groups in Azure Active Directory.
- User names and email addresses in Active Directory must match those in Azure Active Directory.
- Citrix Cloud account, with Citrix Cloud Connector installed for directory services synchronization.
- Citrix Gateway. Citrix recommends that you enable certificate-based authentication for a full single sign-on experience. If you use LDAP authentication on the Citrix Gateway for MAM registration, end users experience a dual authentication prompt during enrollment. For more information, see [Client certificate or certificate plus domain authentication](#).
- Secure Hub if Endpoint Management is not Workspace enabled.
- Citrix Workspace app if Endpoint Management is Workspace enabled. For information on enabling Citrix Workspace integration, see [Workspace configuration](#).
- In enrollment profiles for Android Enterprise, set **Allow users to decline device management** to **Off**. If users decline device management, they can't enroll using an identity provider to authenticate. For more information, see [Enrollment security](#).

You can configure this feature with and without Workspace enabled.

### Configuration if Endpoint Management is Workspace enabled

If you integrate Endpoint Management with Citrix Workspace, the general steps to configure authentication with Azure AD through Citrix Cloud are:

1. Configure Citrix Cloud to use Azure AD as your identity provider.
2. Configure Azure AD as the authentication method for Citrix Workspace.

### Configuration if Endpoint Management is not Workspace enabled

If Citrix Workspace isn't enabled for Endpoint Management, the general steps to configure authentication with Azure AD through Citrix Cloud are:

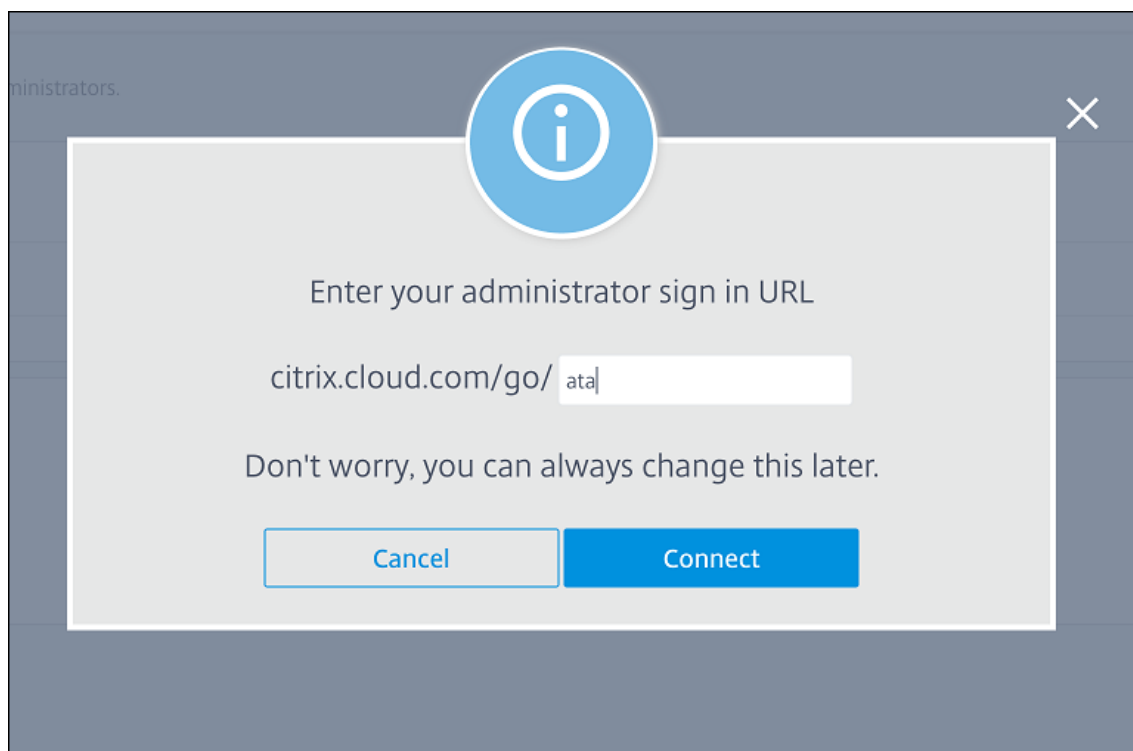
1. Configure Citrix Cloud to use Azure AD as your identity provider.
2. Configure Citrix identity as the IdP type for Endpoint Management.

After that configuration, Secure Hub users who are domain-joined can use Secure Hub to sign on with their Azure AD credentials. Secure Hub uses client certificate authentication for MAM devices.

### Configure Citrix Cloud to use Azure Active Directory as your identity provider

To set up this service for use with the Citrix Workspace app and Secure Hub, configure Azure Active Directory in Citrix Cloud.

1. Go to <https://citrix.cloud.com> and sign in to your Citrix Cloud account.
2. From the Citrix Cloud menu, go to the **Identity and Access Management** page and connect to Azure Active Directory.
3. Type your administrator sign-in URL and then click **Connect**.



4. After you sign in, your Azure Active Directory account connects to Citrix Cloud. The **Identity and Access Management > Authentication** page shows which accounts to use to sign in to your Citrix Cloud and Azure AD accounts.

5. To enable authentication with Azure AD for users enrolling through the Citrix Workspace app and Secure Hub, under **Workspace Configuration > Authentication**, select **Azure Active Directory**. After you complete the configuration, you can enroll user devices through the Citrix Workspace app and Secure Hub.

## Configure Citrix identity as the IdP type for Endpoint Management

This configuration applies only to users enrolling through Secure Hub. After you configure Azure Active Directory in Citrix Cloud, configure Endpoint Management as follows.

1. In the Endpoint Management console, go to **Settings > Identity Provider (IDP)** and then click **Add**.
2. On the **Identity Provider (IDP)** page, configure the following:
  - **IDP Name:** Type a unique name to identify the IdP connection that you're creating.
  - **IDP Type:** Choose **Citrix Identity Platform**.
  - **Authentication Domain:** Choose **Azure Active Directory**. This domain corresponds to the Identity provider domain on the Citrix Cloud **Workspace Configuration > Authentication** page.
3. Click **Next**. On the **IDP Claims Usage** page, configure the following:
  - **User Identifier type:** By default, this field is set to **userPrincipalName**. Ensure that you configure all users with the same identifier in both your on-premises Active Directory and in Azure Active Directory. Endpoint Management uses this identifier to map users on the identity provider with on-premises Active Directory users.
  - **User Identifier string:** This field is automatically filled.
4. Click **Next**, review the **Summary** page, and then click **Save**.

Secure Hub users, Endpoint Management console, and Self-Help Portal users can now sign in with their Azure Active Directory credentials.

## Secure Hub authentication flow

Endpoint Management uses the following flow to authenticate users with Azure AD as an IdP on devices enrolled through Secure Hub:

1. A user starts Secure Hub.
2. Secure Hub passes the authentication request to Citrix identity, which passes the request to Azure Active Directory.
3. The user types their Azure Active Directory user name and password.
4. Azure Active Directory validates the user and sends a code to Citrix identity.

5. Citrix identity sends the code to Secure Hub, which sends the code to the Endpoint Management server.
6. Endpoint Management obtains an ID token by using the code and secret and then validates the user information that's in the ID token. Endpoint Management returns a session ID.

## Authentication with Okta through Citrix Cloud

October 5, 2021

Endpoint Management supports authentication with Okta credentials through Citrix Cloud. This authentication method is available only to users enrolling in MDM through the Citrix Workspace app or Citrix Secure Hub. If Endpoint Management is Workspace enabled, users access resources from the Citrix Workspace app. If you don't enable Citrix Workspace integration with Citrix Endpoint Management, users access resources from Secure Hub.

Devices enrolling in MAM can't authenticate using Okta credentials through Citrix Cloud. To use Secure Hub with MDM+MAM, configure Endpoint Management to use Citrix Gateway for MAM enrollment. For more information, see [Citrix Gateway and Endpoint Management](#).

Endpoint Management uses the Citrix Cloud service, Citrix identity, to federate with Okta. Citrix recommends that you use the Citrix identity provider instead of a direct connection to Okta.

Endpoint Management supports authentication with Okta for the following platforms:

- iOS devices
- Android Enterprise devices (Preview), for BYOD and fully managed modes
- Android devices that run in the legacy Device Administration mode

Authentication with Okta through Citrix Cloud has these limitations:

- Isn't available for Endpoint Management local accounts.
- Doesn't support authentication through Okta for enrollment invitations. If you send users an enrollment invitation containing an enrollment URL, users authenticate through LDAP instead of Okta.

### Prerequisites

- Okta user credentials
- User groups in Active Directory must match the user groups in Okta.
- User names and email addresses in active directory must match those in Okta.
- Citrix Cloud account, with Citrix Cloud Connector installed for directory services synchronization

- Citrix Gateway. Citrix recommends that you enable certificate-based authentication for a full single sign-on experience. If you use LDAP authentication on the Citrix Gateway for MAM registration, end users experience a dual authentication prompt during enrollment. For more information, see [Client certificate or certificate plus domain authentication](#).
- Secure Hub if Endpoint Management is not Workspace enabled.
- Citrix Workspace app if Endpoint Management is Workspace enabled. For information on enabling Citrix Workspace integration, see [Workspace configuration](#).
- In enrollment profiles for Android Enterprise, set **Allow users to decline device management** to **Off**. If users decline device management, they can't enroll using an identity provider to authenticate. For more information, see [Enrollment security](#).

You can configure this feature with and without Workspace enabled.

### **Configuration if Endpoint Management is Workspace enabled**

If you integrate Endpoint Management with Citrix Workspace, the general steps to configure authentication with Okta through Citrix Cloud are:

1. Configure Citrix Cloud to use Okta as your identity provider.
2. Configure Okta as the authentication method for Citrix Workspace.

To configure Citrix Cloud to use Okta as your identity provider and set up Okta as the authentication method for Citrix Workspace, see [Connect Okta as an identity provider to Citrix Cloud](#).

After you complete the configuration, you can enroll user devices through the Citrix Workspace app.

### **Configuration if Endpoint Management is not Workspace enabled**

If Citrix Workspace isn't enabled for Endpoint Management, the general steps to configure authentication with Okta through Citrix Cloud are:

1. Configure Citrix Cloud to use Okta as your identity provider.
2. Configure Citrix identity as the IdP type for Endpoint Management.

### **Configure Citrix Cloud to use Okta as your identity provider**

To configure Okta in Citrix Cloud, see [Connect Okta as an identity provider to Citrix Cloud](#).

### **Configure Citrix identity as the IdP type for Endpoint Management**

This configuration applies only to users enrolling through Secure Hub. After you configure Azure Active Directory in Citrix Cloud, configure Endpoint Management as follows.

1. In the Endpoint Management console, go to **Settings > Identity Provider (IDP)** and then click **Add**.
2. On the **Identity Provider (IDP)** page, configure the following:
  - **IDP Name:** Type a unique name to identify the IdP connection that you are creating.
  - **IDP Type:** Choose **Citrix Identity Platform**.
  - **Authentication Domain:** Choose **Okta**. This domain corresponds to your Identity provider domain on the Citrix Cloud **Workspace Configuration > Authentication** page.
3. Click **Next**. In the **IDP Claims Usage** page, configure the following:
  - **User Identifier type:** By default, this field is set to **userPrincipalName**. Ensure that you configure all users with the same identifier in both your on-premises Active Directory and in Okta. Endpoint Management uses this identifier to map users on the identity provider with on-premises Active Directory users.
  - **User Identifier string:** This field is automatically filled.

After this configuration, Secure Hub users who are domain-joined can use Secure Hub to sign in with their Okta credentials. Secure Hub uses client certificate authentication for MAM devices.

### Secure Hub authentication flow

Endpoint Management uses the following flow to authenticate users with Okta as an IdP on devices enrolled through Secure Hub:

1. A user starts Secure Hub.
2. Secure Hub passes the authentication request to Citrix identity, which passes the request to Okta.
3. The user types their Okta user name and password.
4. Okta validates the user and sends a code to Citrix identity.
5. Citrix identity sends the code to Secure Hub, which sends the code to the Endpoint Management server.
6. Endpoint Management obtains an ID token by using the code and secret and then validates the user information that's in the ID token. Endpoint Management returns a session ID.

## Authentication with an on-premises Citrix Gateway through Citrix Cloud

June 30, 2021

Endpoint Management supports authentication with an on-premises Citrix Gateway through Citrix Cloud. This authentication method is available only to users enrolling in MDM through the Citrix

Workspace app or Citrix Secure Hub. If Endpoint Management is Workspace enabled, users access resources from the Citrix Workspace app. If you don't enable Citrix Workspace integration with Citrix Endpoint Management, users access resources from Secure Hub.

Devices enrolling in MAM can't authenticate using on-premises Citrix Gateway credentials through Citrix Cloud. To use Secure Hub with MDM+MAM, configure Endpoint Management to use Citrix Gateway for MAM enrollment. For more information, see [Citrix Gateway and Endpoint Management](#).

Endpoint Management supports authentication with an on-premises Citrix Gateway through Citrix Cloud for the following platforms:

- iOS devices
- Android Enterprise devices, for BYOD and fully managed modes
- Android devices that run in the legacy Device Administration mode

**Note:**

Endpoint Management doesn't support authentication with an on-premises Citrix Gateway through Citrix Cloud for enrollment invitations. If you send users an enrollment invitation containing an enrollment URL, users authenticate through LDAP instead of an on-premises Citrix Gateway as an identity provider.

Citrix recommends that you enable certificate-based authentication for a full single sign-on experience. If you use LDAP authentication on the Citrix Gateway for MAM registration, end users experience a dual authentication prompt during enrollment. For more information, see [Client certificate or certificate plus domain authentication](#).

### Prerequisites

- Citrix Gateway. Citrix recommends that you enable certificate-based authentication for a full single sign-on experience. If you use LDAP authentication on the Citrix Gateway for MAM registration, end-users experience a dual authentication prompt during enrollment. For more information, see [Client certificate or certificate plus domain authentication](#).
- Citrix Cloud account with Citrix Cloud Connector installed for directory services synchronization.
- Secure Hub 20.5.0 and later if Endpoint Management is not Workspace enabled.
- Citrix Workspace app if Endpoint Management is Workspace enabled. For information on enabling Citrix Workspace integration, see [Workspace configuration](#).

You can configure this feature with and without Workspace enabled.

## Configuration if Endpoint Management is Workspace enabled

If you integrate Endpoint Management with Citrix Workspace, the general steps to configure authentication with an on-premises Citrix Gateway through Citrix Cloud are:

1. Configure Citrix Cloud to use Citrix Gateway as your identity provider.
2. Configure Citrix Gateway as the authentication method for Citrix Workspace.

To configure Citrix Cloud to use Citrix Gateway as your identity provider and set up Citrix Gateway as the authentication method for Citrix Workspace, see [Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud](#).

After you complete the configuration, you can enroll user devices through the Citrix Workspace app.

## Configuration if Endpoint Management is not Workspace enabled

If Citrix Workspace isn't enabled for Endpoint Management, the general steps to configure authentication with an on-premises Citrix Gateway through Citrix Cloud are:

1. Configure Citrix Cloud to use Citrix Gateway as your identity provider.
2. Configure Citrix identity as the IdP type for Endpoint Management.

## Configure Citrix Cloud to use Citrix Gateway as your identity provider

To set up Citrix Gateway authentication in Citrix Cloud, see [Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud](#).

## Configure the Citrix identity provider as the IdP type for Endpoint Management

This configuration applies only to users enrolling through Secure Hub. After you configure Citrix Gateway in Citrix Cloud, configure Endpoint Management as follows.

1. In the Endpoint Management console, go to **Settings > Identity Provider (IDP)** and then click **Add**.
2. On the **Identity Provider (IDP)** page, configure the following:
  - **IDP Name:** Type a unique name to identify the IdP connection that you're creating.
  - **IDP Type:** Choose **Citrix Identity Provider**.
  - **Authentication Domain:** Choose **Citrix Gateway**. This domain corresponds to your Identity provider domain on the Citrix Cloud **Workspace Configuration > Authentication** page.
3. Click **Next**. On the **IDP Claims Usage** page, configure the following:
  - **User Identifier type:** By default, this field is set to **userPrincipalName**.



- **User Identifier string:** This field is automatically filled.
4. Click **Next**, review the **Summary** page, and then click **Save**.

You can now enroll user devices through Secure Hub using an on-premises Citrix Gateway as an identity provider.

### Secure Hub authentication flow

Endpoint Management uses the following flow to authenticate users with an on-premises Citrix Gateway as an IdP on devices enrolled through Secure Hub:

1. A user starts Secure Hub.
2. Secure Hub passes the authentication request to Citrix identity, which passes the request to an on-premises Citrix Gateway.
3. The user types their user name and password.
4. An on-premises Citrix Gateway validates the user and sends a code to Citrix identity.
5. Citrix identity sends the code to Secure Hub, which sends the code to the Endpoint Management server.
6. Endpoint Management obtains an ID token by using the code and secret and then validates the user information that's in the ID token. Endpoint Management returns a session ID.

## Derived credentials

August 31, 2021

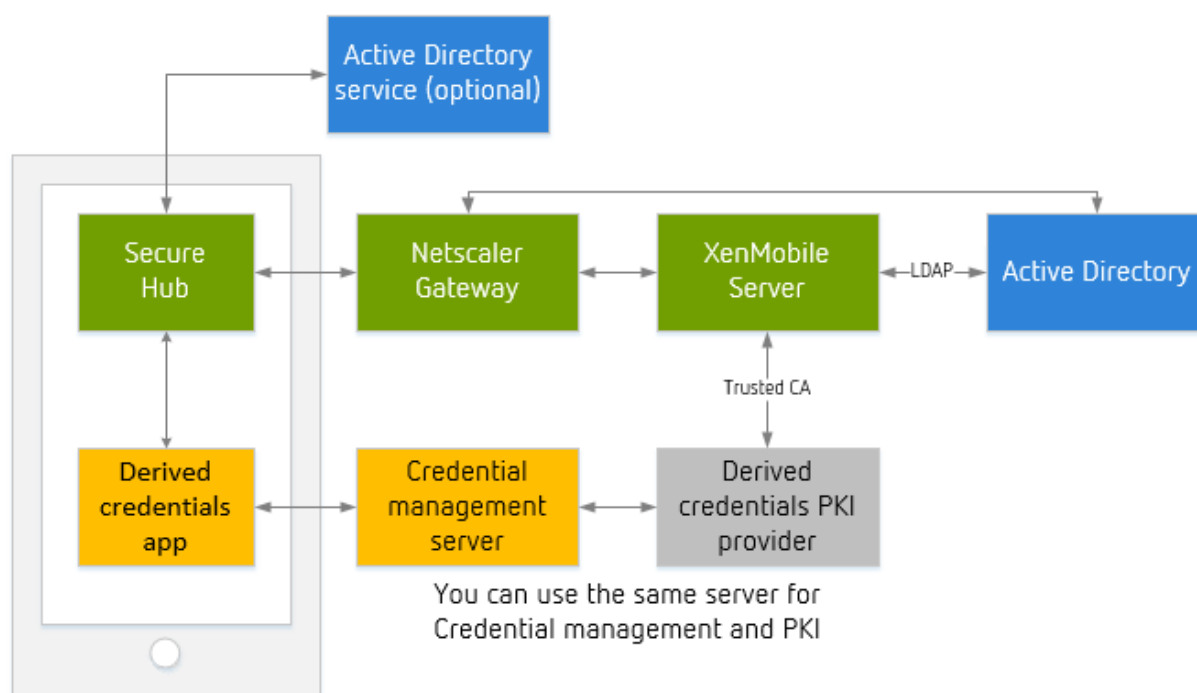
Derived credentials provide strong authentication for mobile devices. The credentials, derived from a smart card, reside in a mobile device instead of the card. The smart card is a Personal Identity Verification (PIV) card.

The derived credentials are an enrollment certificate that contains the user identifier, such as UPN. Endpoint Management saves the credentials obtained from the credential provider in a secure vault on the device.

Endpoint Management can use derived credentials for device enrollment and authentication. If configured for derived credentials, Endpoint Management doesn't support enrollment invitations or other enrollment security modes. Citrix supports use of a derived credentials app during enrollment of iOS.

### Architecture

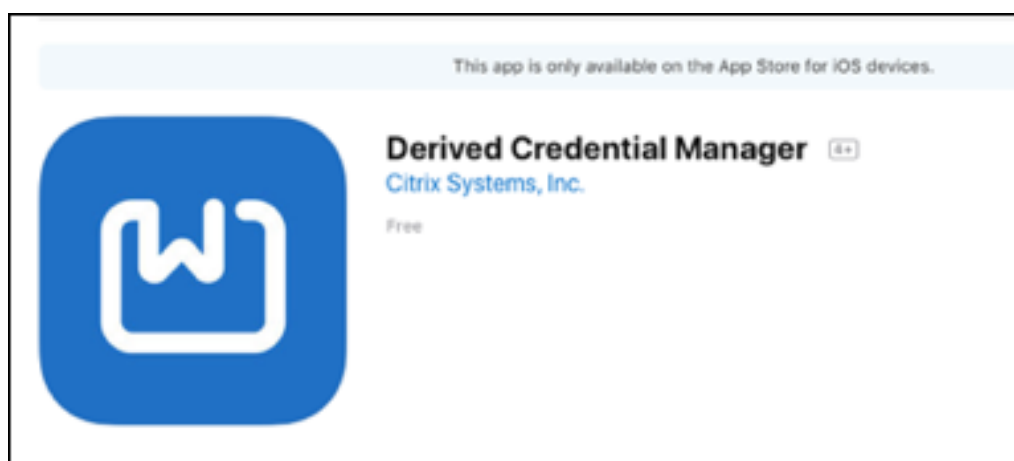
For enrollment, Endpoint Management connects to the components, as shown in the following diagram.



- During device enrollment, Secure Hub obtains certificates from the derived credentials app.
- The derived credentials app communicates with the credential management server during enrollment.
- You can use the same or different server for the credential management server and a third-party PKI provider.
- Endpoint Management connects to your third-party PKI server to obtain certificates.

## Requirements

- Download and install Citrix Secure Hub.
- Based on your derived credential solution, download and configure the app:
  - **For Entrust Datacard:**
    - \* Download and install the Citrix Derived Credential Manager app on your devices *before* enrolling in Endpoint Management. The Derived Credentials Manager app is the identity provider app for Citrix. The logo for that app follows.



**Note:**

Citrix Derived Credential Manager app supports new enrollments only. Device users must re-enroll.

\* Requires device enrollment in MDM+MAM.

- **For other derived credentials providers:** While it's likely that most other credential solutions are compatible with XenMobile, test the integration before deploying it to production.
- Must have the root certificate of the authority that issues certificates to the Credentials Provider server. That setup enables Endpoint Management to accept the digitally signed certificates during enrollment. For information about adding the certificates, see [Certificates and authentication](#).
  - If the user email domain differs from the LDAP domain, include the email domain in the **Domain alias** setting in **Settings > LDAP**. For example, if the domain for email addresses is `citrix.com` and the LDAP domain name is `sample.com`, set **Domain alias** to **sample.com, citrix.com**.
  - Endpoint Management doesn't support the use of derived credentials with shared devices.
- User identity certificates:
  - The user name in the Subject alternative name field must be formatted as the otherName, rfc822Name, or dNSName field of the SubjectAltName extension. Other fields are not supported. For more information about Subject alternative name, see the RFC, <https://www.ietf.org/rfc/rfc5280.txt>.
  - User identity in the Subject field in either Email or CN isn't supported.
- Citrix Gateway configured for certificate authentication or certificate plus security token authentication

## Enable derived credentials

By default, the Endpoint Management console doesn't include the **Settings > Derived Credentials** page.

To enable the interface for derived credentials:

- Go to **Settings > Server Properties**, add **derived.credentials.enable** as the server property, and set the property value to **true**.

Settings > Server Properties > Edit New Server Property

### Edit New Server Property

Key	<input type="text" value="derived.credentials.enable"/>
Value*	<input type="text" value="true"/>
Display name*	<input type="text" value="derived.credentials.enable"/>
Description	<input type="text"/>

## Configure derived credentials

The assumption is that you have a working configuration for the derived credentials provider that you plan to integrate with Endpoint Management. You can configure Endpoint Management to communicate with that server. You can also choose a derived credentials CA certificate already added to Endpoint Management or import the certificate.

You can activate Online Certificate Status Protocol (OCSP) support for that CA certificate. For more information about OCSP, see “Discretionary CAs” in [PKI entities](#).

1. In the Endpoint Management console, go to **Settings > Derived Credentials for iOS**.
2. For **Choose derived credentials provider**, choose **Other** for Entrust Datacard. Type `dcapp://mode=SecureHub` in the **App URL (iOS)**.

Settings > Derived Credentials for iOS

### Derived Credentials for iOS

Configure a derived credentials provider to enable iOS users to enroll with a smart card.

**Provider**

Choose derived credentials provider \*

Intercede

Other (tech preview)

App URL (iOS) \*

Optional parameters ⓘ

Name *	Value *	Add
--------	---------	-----

**Details**

Issuer CA \*

C=US,O=Entrust,OU=Demonstration and Evaluation,OU=Cert...  ⓘ

CA Info  
Name: C=US,O=Entrust,OU=Demonstration and Evaluation,OU=Certificate Authorities,OU=Entrust Demonstration and Evaluation Issuing CA  
Expire: 2024-08-14

User Identifier field \*

Subject name ⓘ

Subject alternative name

User identifier type \*

UPN ⓘ

**OCSF**

OCSF Check  OFF ⓘ

3. **Optional parameters:** Some derived credential providers might require that you provide parameters for the connection. For example, a vendor might require that you specify the URLs of a back-end server. Click **Add** to provide parameters.
4. Specify a certificate for derived credentials: If the certificate is already uploaded to Endpoint Management, choose that certificate from **Issuer CA**. Otherwise, click **Import** to add a certificate. The **Import Certificate** dialog box appears.
5. In the **Import Certificate** dialog box, click **Browse** to navigate to the certificate. Then click **Browse** to navigate to the private key file.

**Import** ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

**Import** Certificate ▾

**Use as** Server ▾

**Certificate import\***  **Browse**

**Private key file**  **Browse**

**Description**

**Cancel** **Import**

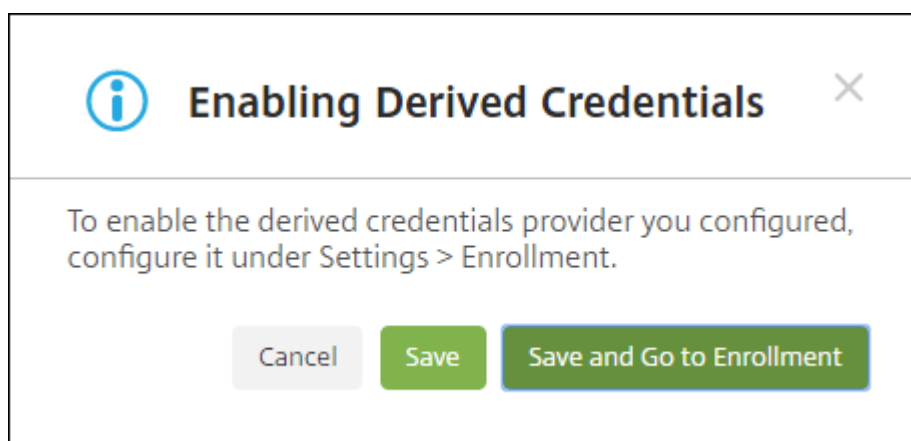
6. Configure the settings.

- For Citrix Derived Credential Manager app: The **User Identifier field** is **Subject alternative name**, and the **User Identifier type** is **userPrincipalName**.
- Contact other derived credential providers for their information.

7. You can optionally use an OCSP responder for certificate revocation checking. Citrix recommends using an OCSP responder for security purposes. By default, OSP checking is **Off**.

- If you activate OCSP support for the CA certificate, choose an option for **Use custom OCSP URL**. By default, Endpoint Management extracts the OCSP URL from the certificate (the **Use certificate definition for revocation** option). To specify a responder URL, click **Use custom** and then type the URL.
- **Responder CA:** From **Responder CA**, choose a certificate. Or, click **Import** and then use the **Import Certificate** dialog box to locate the certificate.

8. Click **Save**. The **Enabling Derived Credentials** dialog box appears.



- To enable the derived credentials configuration, click **Save**. To use derived credentials, you must also configure enrollment settings.
  - To enable the derived credentials configuration and then go immediately to **Settings > Enrollment**, click **Save and Go to Enrollment**.
9. To enable derived credentials for enrollment: On the **Settings > Enrollment** page, under **Advanced Enrollment**, select **Derived Credentials (iOS only)** and then click **Enable**.

Settings > Enrollment

### Enrollment

Enable and disable enrollment modes for users. You can also enable the Self Help Portal to allow users to generate enrollment links that let them download Secure Hub and enroll their devices, or to send themselves an enrollment invitation.

**Enrollment for other platforms** ⚠ Enrollment for other platforms will be available here. X

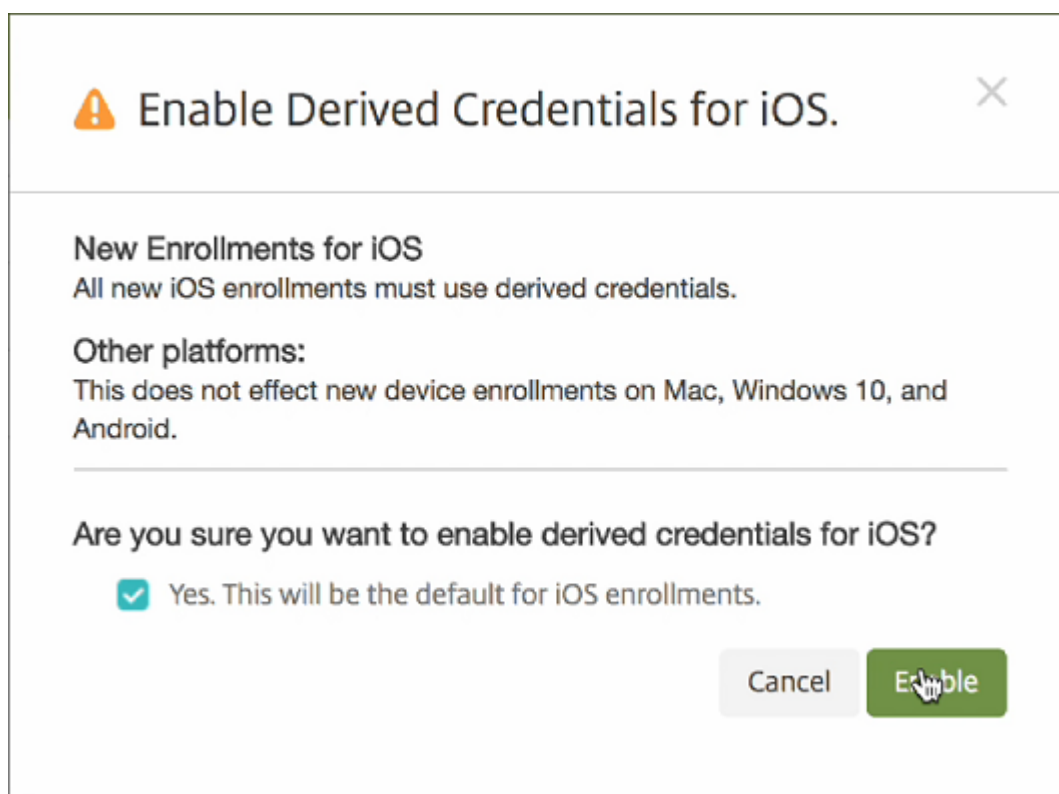
<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire after	Attempts	PIN length	PIN type	Templates
<input type="checkbox"/>	User name + Password	✓	✓						
<input type="checkbox"/>	High Security	✓			1 day(s)	3	8	numeric	
<input type="checkbox"/>	Invitation URL	✓			1 day(s)				
<input type="checkbox"/>	Invitation URL + PIN	✓			1 day(s)	3	8	numeric	
<input type="checkbox"/>	Invitation URL + Password	✓			1 day(s)	3			
<input type="checkbox"/>	Two Factor	✓			1 day(s)	3	8	numeric	
<input type="checkbox"/>	User name + PIN	✓			1 day(s)	3	8	numeric	

Showing 1 - 7 of 7 items

#### Advanced Enrollment

<input type="checkbox"/>	Name	Enabled	Default
<input type="checkbox"/>	Derived Credentials (iOS only)	✓	✓

10. A confirmation dialog box appears. To enable derived credentials, select the check box, and click **Enable**.



11. To edit options for derived credentials enrollment, go to **Settings > Enrollment**, select **Derived Credentials (iOS only)** and then click **Edit**.

After you enable derived credentials: In the **Devices Enrollment** report, the column **Enrollment mode** shows **derived\_credentials**.

### Configure Endpoint Management for Secure Mail

To enable Secure Mail to work with derived credentials, add the **LDAP Attributes** client property. For information about adding a client property, see [Client properties](#).

Use the following information for the client property:

- **Key:** SEND\_LDAP\_ATTRIBUTES
- **Value:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountName=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`



Settings > Client Properties > Edit Client Property

### Edit Client Property

Key	SEND_LDAP_ATTRIBUTES
Value *	userPrincipalName=\${user.userprincipalname},sAM
Name *	SEND_LDAP_ATTRIBUTES
Description *	SEND_LDAP_ATTRIBUTES

## Activating Entrust Datacard derived credentials on iOS devices

### Note:

While using Entrust website:

- Clear the browser cache when changing the PIV card.

1. To request new smart credentials, use a desktop or any device to log in to the Entrust site. Log in using the **Smart Credential Log In** button at the bottom of the page. Users insert their smart card into a reader attached to their desktop.

The screenshot displays two login sections. The top section, titled "Log In", includes a "Sign In Using:" dropdown menu currently set to "Corporate Domain Password". Below this are two required fields, marked with a red asterisk: "User Name:" and "Password:". A "Log In" button is positioned below the password field. Underneath the button are four blue links with arrow icons: "Forgot your password?", "Perform SAML login", "Forgot your smart credential PIN?", and "Let me use an OTP to log in.". The bottom section, titled "Smart Credential Log In", contains the instruction: "Ensure your smart credential can be read by your computer, then click this button to log in." A blue "Log In" button is highlighted with a red rectangular box. Below this button, the text reads: "Close your web browser when you are done."

2. From the **Self-Administration Actions**, select the **I'd like to enroll for a derived mobile smart credential** and click **Done**.

**Self-Administration Actions**

Please select one of the actions below or click Done if you're finished:

- [I'd like to update my personal information.](#)
- [I'd like to change my question and answer pairings.](#)
- [I'd like to request a grid.](#)
- [I'd like to change my Entrust IdentityGuard password.](#)
- [I've forgotten my Entrust IdentityGuard password.](#)
- [I'd like to request a soft token.](#)
- [I'd like to unblock my smart credential.](#)
- [I'd like to activate or update my smart credential.](#)
- [I've permanently lost my smart credential or it has been compromised.](#)
- [I've temporarily forgotten or misplaced my smart credential.](#)
- [I'd like to enroll for a derived mobile smart credential.](#)

Done

3. In the **Derived Mobile Smart Credential** screen, provide the **Identity Name**. The user can choose a unique name such as a user name or ID numbers.
4. Select the **Citrix DCAPP** from the Derived credential app menu, and click **Ok**.

**Derived Mobile Smart Credential**

Enter any name you would like to use to identify your new derived mobile smart credential identity.

\* Identity Name:

Choose which app you want to associate with your new derived mobile smart credential.

\* Derived Mobile Smart Credential App:

Citrix DCAPP

You will receive an email message, to be opened on your mobile device, that contains a link that will launch the derived mobile smart credential app with the appropriate activation data.

To unlock the activation data, you will be required to enter a password that will be provided on the next page.

The activation email message will be delivered to the account associated with citrix.com.

You will have approximately 60 minutes to complete the activation of your derived mobile smart credential.

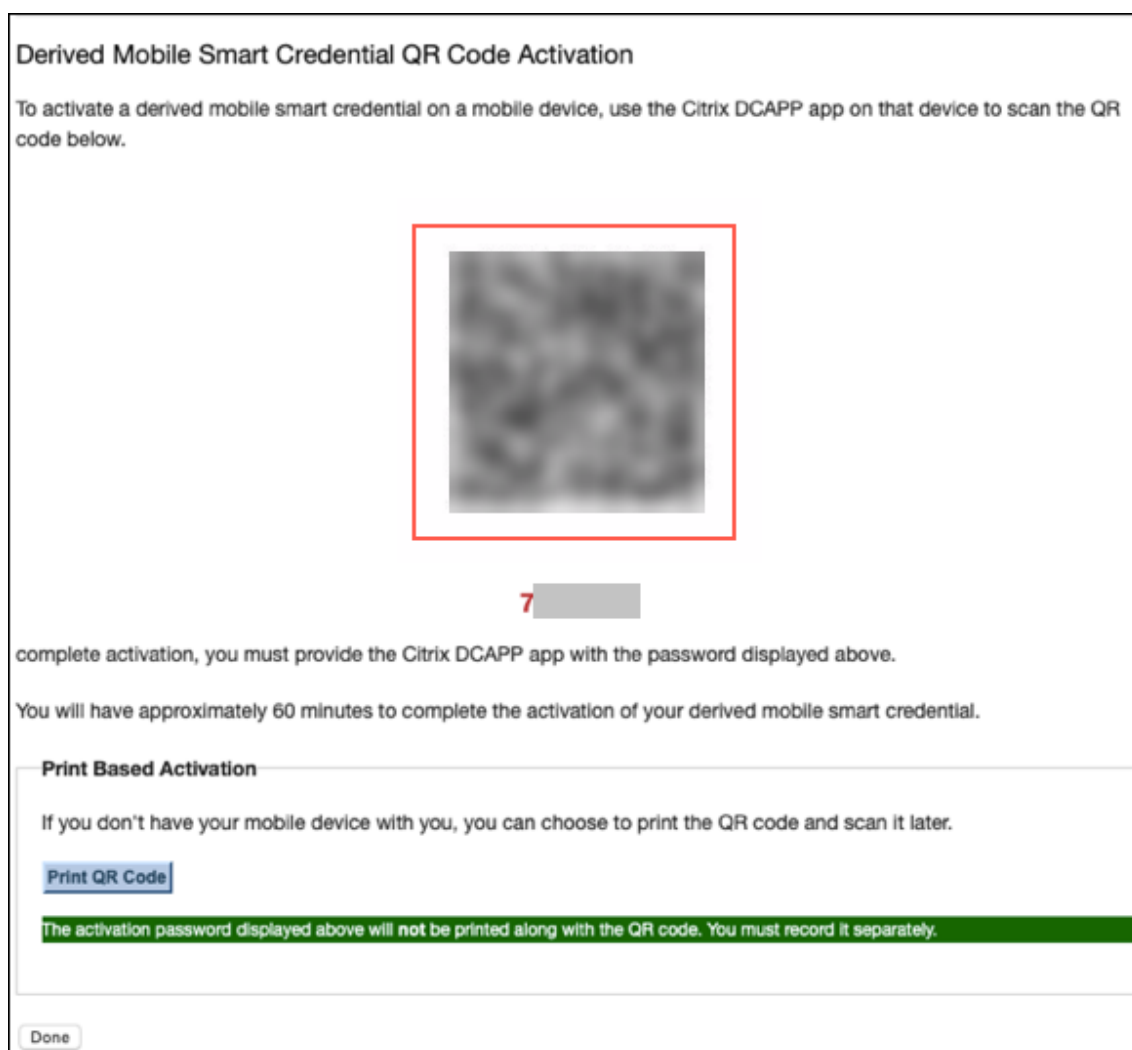
OK Cancel

A QR code Activation screen appears and prompts the user to scan the code with their mobile device.

**Note:**

By default, the derived credentials QR code expires in 3 minutes.

5. Scan the QR code using the **Derived Credential Manager** app on the device to complete the activation.



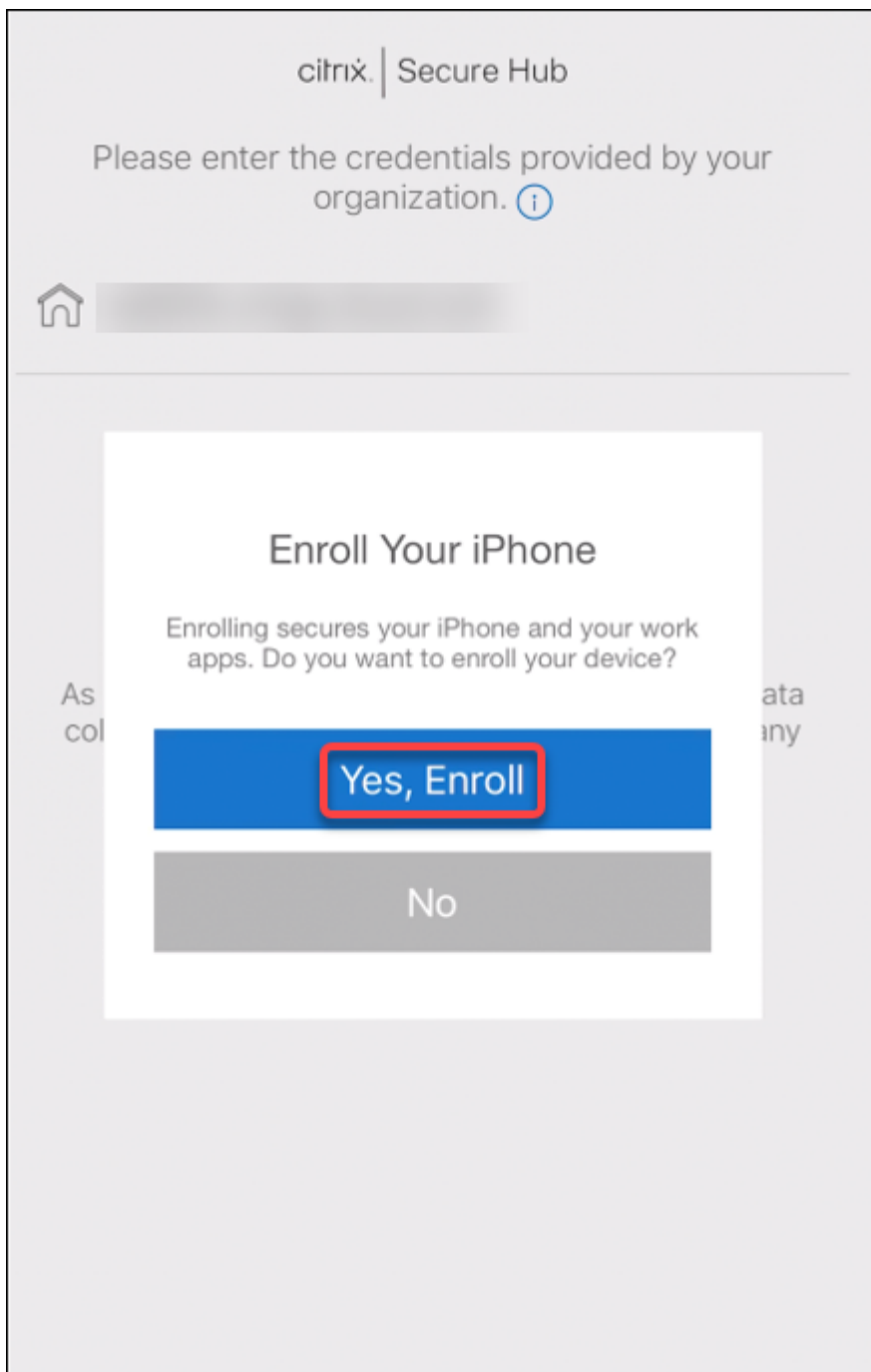
## Device enrollment

After you complete the setup described earlier in this article, users can enroll their devices by using derived credentials.

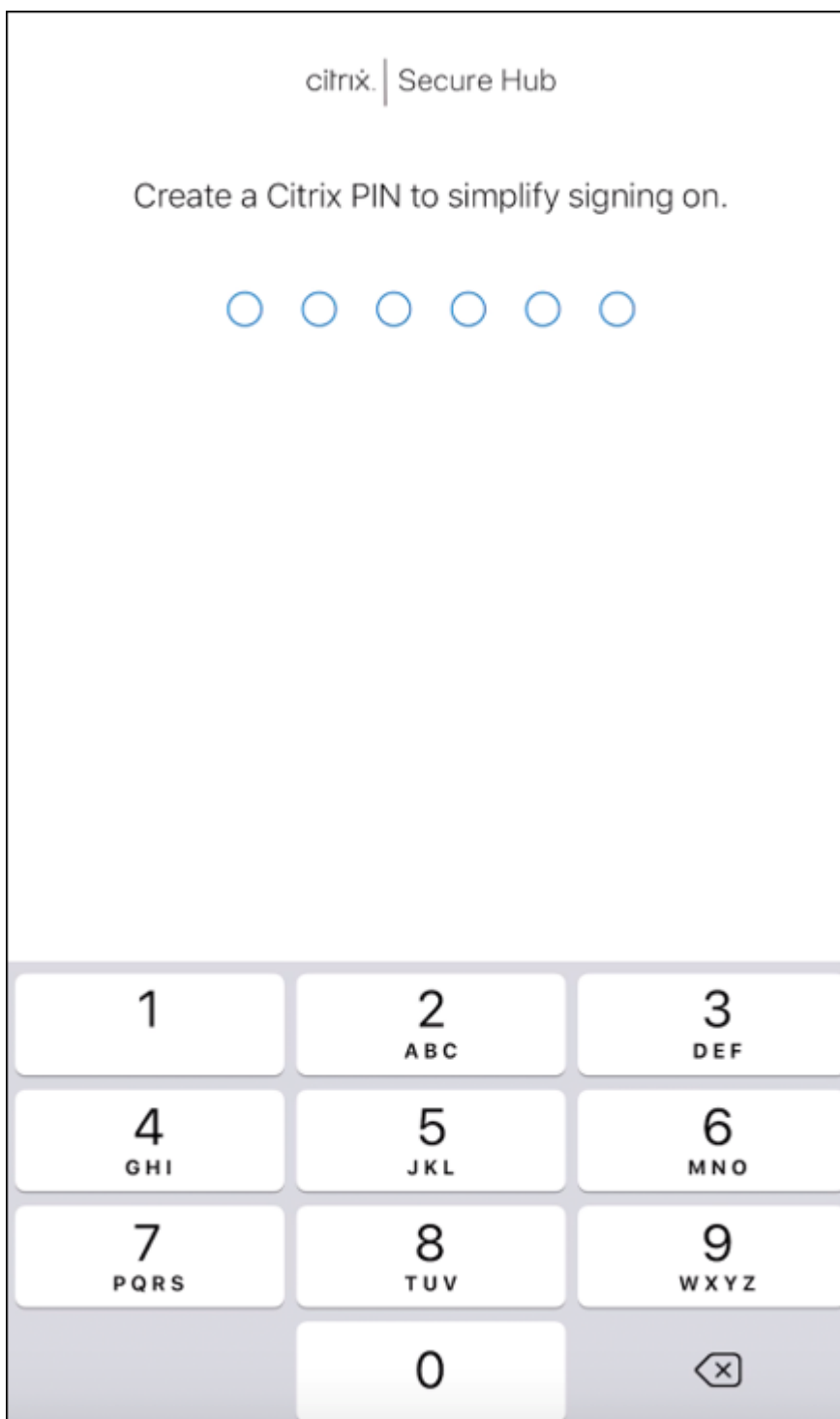
**Note:**

Screenshots in this section use Entrust Datacard as an example.

1. Tap to open **Secure Hub**. When prompted, type the Endpoint Management server fully qualified domain name and then click **Next**.
2. Click **Yes, Enroll**. Device enrollment in Secure Hub starts.

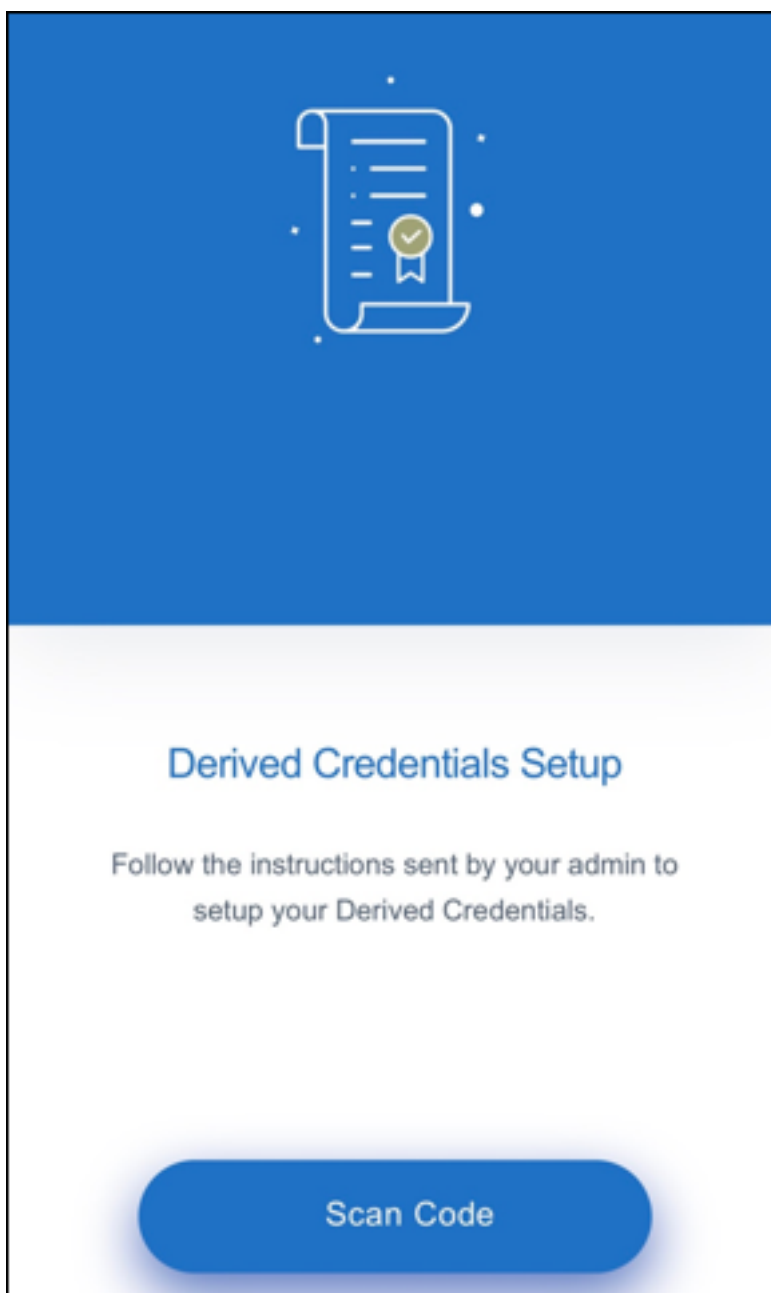


If Endpoint Management is configured for derived credentials, Secure Hub prompts the user to create and confirm the Citrix PIN.



After confirming the Citrix PIN the Derived Credentials setup splash screen appears. Follow the instructions to activate smart credentials.

3. Tap **Scan code**. The mobile phone camera activates.



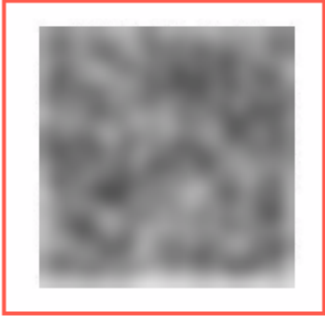
**Note:**

To scan the QR code, ensure your camera and microphone is enabled and has required access permissions.

4. In the derived credentials app, scan the QR code that was created in earlier steps.

**Derived Mobile Smart Credential QR Code Activation**

To activate a derived mobile smart credential on a mobile device, use the Citrix DCAPP app on that device to scan the QR code below.



7

complete activation, you must provide the Citrix DCAPP app with the password displayed above.

You will have approximately 60 minutes to complete the activation of your derived mobile smart credential.

**Print Based Activation**

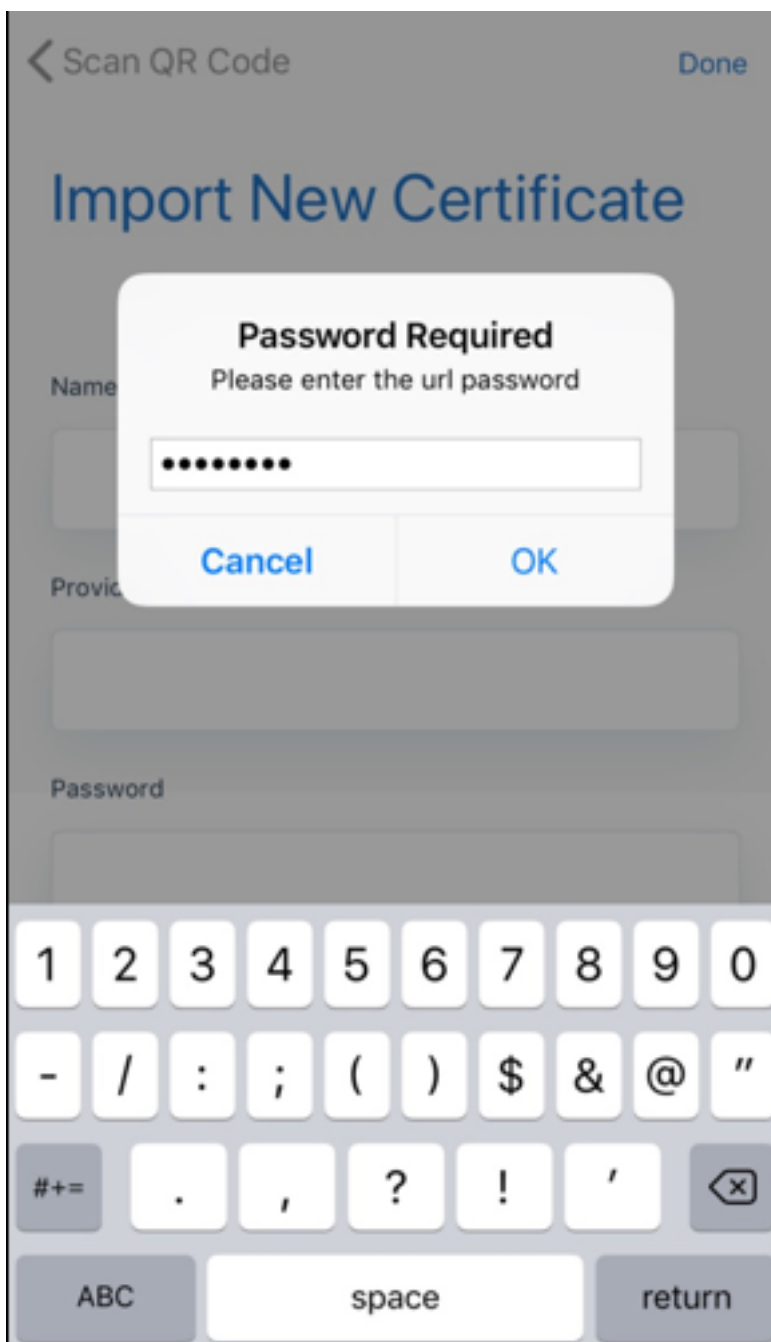
If you don't have your mobile device with you, you can choose to print the QR code and scan it later.

[Print QR Code](#)

The activation password displayed above will not be printed along with the QR code. You must record it separately.

5. After scanning the QR code, on the **Import New Certificate** screen a password dialog box appears, enter the password and click **OK**.





**Import New Certificate** screen appears with fields auto-populated.

Scan QR Code Done

## Import New Certificate

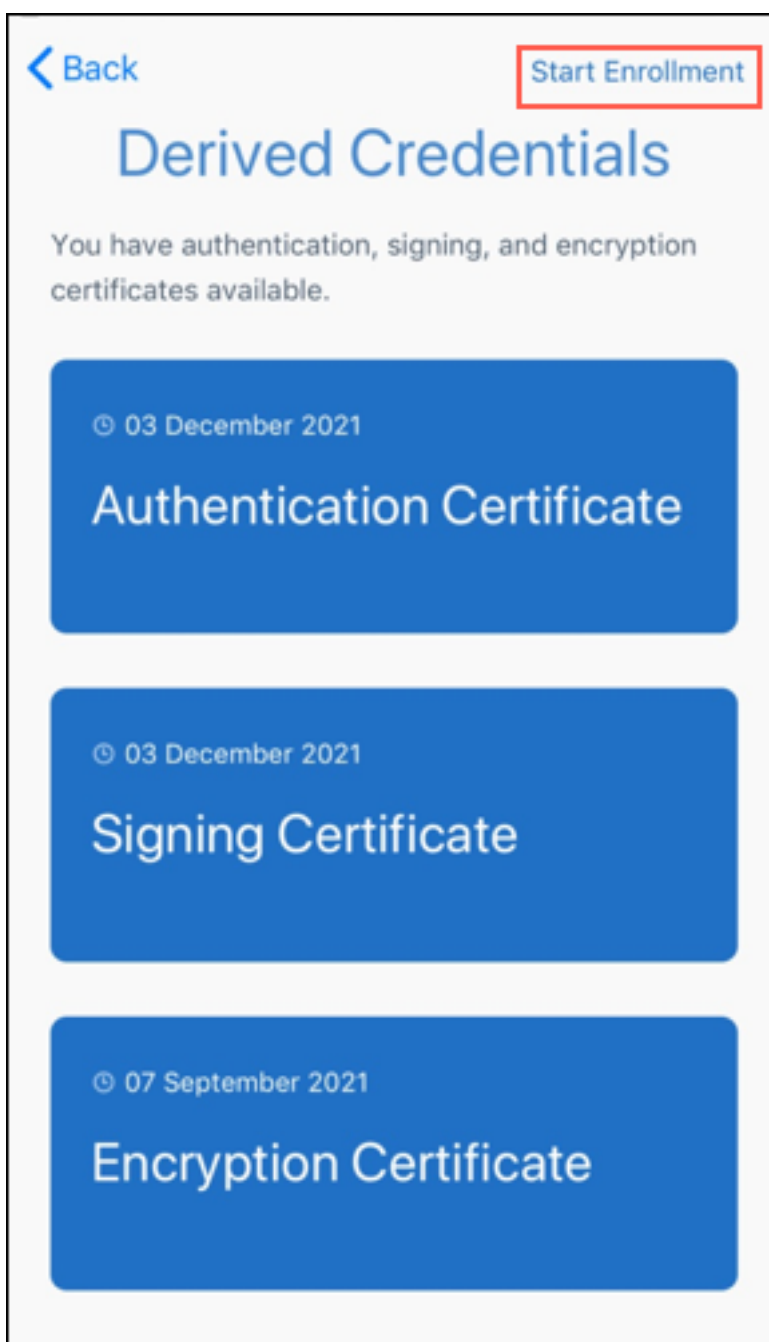
Name

Provider

Password

Credential ID

6. After the certificates are added successfully, in the **Derived Credentials** screen, click **Start Enrollment**.



7. In Secure Hub, enter a new PIN when prompted.

After authenticating the PIN, Secure Hub downloads the certificates. Follow the prompts to complete the enrollment.

To view device information in the Endpoint Management console:

- Go to **Manage > Devices** and then select a device to display a command box. Click **Show more**.
- Go to **Analyze > Dashboard**.

## User accounts, roles, and enrollment

July 9, 2021

You perform user configuration tasks in the Endpoint Management console on the **Manage** tab and the **Settings** page. Unless otherwise indicated, the steps for the following tasks are provided in this article.

- Enrollment security mode and invitations
  - From **Settings > Enrollment**, configure up to seven enrollment security modes and send enrollment invitations. Each enrollment security mode has its own level of security and number of steps users must take to enroll their devices.
- Roles for user accounts and groups
  - From **Settings > Role-Based Access Control**, assign predefined roles, or sets of permissions, to users and groups. These permissions control the level of access users have to system functions. For more information, see [Configure roles with RBAC](#).
  - From **Settings > Notification Templates**, to create or update the notification templates to use in automated actions, enrollment, and standard notification messages sent to users. You configure the notification templates to send messages over three different channels: Secure Hub, SMTP, or SMS. For more information, see: [Creating and updating Notification Templates](#).
- User accounts and groups:
  - From **Manage > Users**, you can add local user accounts manually or use a .csv provisioning file to import the accounts and to manage local groups. However, most Endpoint Management deployments connect to LDAP for user and group information. You might prefer to create user accounts locally in use cases such as the following:
    - \* In environments, such as retail, where devices are shared rather than dedicated to individual users.
    - \* If you use an unsupported directory, such as Novell eDirectory.
  - From **Settings > Workflows**, use workflows to manage the creation and removal of user accounts.

### About user accounts

An Endpoint Management user account is either for a local, Active Directory, or cloud user.

- **Cloud users:** A cloud user is a special user account that Citrix Cloud creates when an administrator is added to your Citrix Cloud customer account. A cloud user account uses the same user name as the administrator account on Citrix Cloud and defaults to the Admin role. The cloud user account provides single sign-on and performs other administrative functions.

To add administrators to a Citrix Cloud account, see [Invite new administrators](#).

For cloud users:

- You can change the roles and user properties of cloud users through the Citrix Cloud console. See [Manage Citrix Cloud administrators](#).
- To change the password, see [Administrators](#).
- To delete a cloud user, in Citrix Cloud, go to **Identity and access management > Administrators**. Click the ellipsis at the end of the user's row, and then select **Delete Administrator**.
- You cannot add cloud users to a local group.

## Configure enrollment security modes

You configure a device enrollment security mode to specify a security level and notification template for device enrollment in Endpoint Management.

Endpoint Management offers six enrollment security modes, each with its own level of security and steps users must take to enroll their devices. You configure enrollment security modes in the Endpoint Management console from the **Manage > Enrollment Invitations** page. For information, see [Enrollment invitations](#).

### Note:

If you plan to use custom notification templates, you must set up the templates before you configure enrollment security modes. For more information about notification templates, see [Creating or Updating Notification Templates](#).

1. On the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Click **Enrollment**. The **Enrollment** page appears, containing a table of all available enrollment security modes. By default, all enrollment security modes are enabled.
3. Select any enrollment security mode in the list to edit it. Then, set the mode as the default or disable the mode.

Select the check box next to an enrollment security mode to view the options menu. Or, click anywhere else in the list to view the options menu on the right side of the listing.

### Tip:

When you edit the enrollment security mode, you can specify an expiration deadline after which users cannot enroll their devices. For information, see [To edit an enrollment security mode](#) in this article. The value appears in the user and group enrollment invitation configuration pages.

Settings > Enrollment

### Enrollment

Enable and disable enrollment modes for users. You can also enable the Self Help Portal to allow users to generate enrollment links that let them download Secure Hub and enroll their devices, or to send themselves an enrollment invitation.

<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire after	Attempts	PIN length	PIN type	Templates	▼
<input type="checkbox"/>	User name + Password	✓	✓							
<input type="checkbox"/>	High Security	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL	✓			1 day(s)					
<input type="checkbox"/>	Invitation URL + PIN	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL + Password	✓			1 day(s)	3				
<input type="checkbox"/>	Two Factor	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	User name + PIN	✓			1 day(s)	3	8	numeric		

Showing 1 - 7 of 7 items

You have the following enrollment security mode choices depending on your platform:

- User name + Password
- Invitation URL
- Invitation URL + PIN
- Invitation URL + Password
- Two Factor
- User name + PIN

For information about platform-specific enrollment security modes, see [Enrollment security modes by platform](#).

You can use enrollment invitations as an effective way to restrict the ability to enroll to specific users or groups. To send enrollment invitations, you can use only **Invitation URL**, **Invitation URL + PIN**, or **Invitation URL + Password** enrollment security modes. For devices enrolling with **User name + Password**, **Two-factor authentication**, or **User name + PIN**, users must manually enter their credentials in Secure Hub.

You can use one-time PIN (sometimes also called OTP) enrollment invitations as a two-factor authentication solution. One-time PIN enrollment invitations control the number of devices a user can enroll. OTP invitations aren't available for Windows devices.

## To edit an enrollment security mode

1. In the **Enrollment** list, select an enrollment security mode and then click **Edit**. The **Edit Enrollment Mode** page appears. Depending on the mode you select, you might see different options.

Settings > Enrollment > Edit Enrollment Mode

### Edit Enrollment Mode

Name High Security

Expire after\* 1 Days ?

Maximum attempts\* 3 ?

PIN Length\* 8 Numeric

Notification templates

Template for enrollment URL -- SELECT ONE --

Template for Enrollment PIN -- SELECT ONE --

Template for enrollment confirmation -- SELECT ONE --

Cancel Save

2. Change the following information as appropriate:
  - **Expire after:** Type an expiration deadline after which users cannot enroll their devices. This value appears in the user and group enrollment invitation configuration pages.  
Type **0** to prevent the invitation from expiring.
  - **Days:** In the list, click **Days** or **Hours** to correspond to the expiration deadline you entered in **Expire after**.
  - **Maximum attempts:** Type the number of attempts to enroll that a user can make before being locked out of the enrollment process. This value appears in the user and group enrollment invitation configuration pages.  
Type **0** to allow unlimited attempts.
  - **PIN length:** Type a numeral to set the length of the generated PIN.
  - **Numeric:** In the list, click **Numeric** or **Alphanumeric** for the PIN type.
  - **Notification templates:**
    - **Template for enrollment URL:** In the list, click a template to use for the enrollment URL. For example, the Enrollment invitation template sends users an email or SMS.

The method depends on how you configured the template that lets them enroll their devices in Endpoint Management. For more information on notification templates, see [Create or update notification templates](#).

- **Template for enrollment PIN:** In the list, click a template to use for the enrollment PIN.
- **Template for enrollment confirmation:** In the list, click a template to use to inform a user that they enrolled successfully.

3. Click **Save**.

### To set an enrollment security mode as default

The default enrollment security mode is used for all device enrollment requests unless you select a different enrollment security mode. If no enrollment security mode is set as the default, you must create an enrollment request for each device enrollment.

1. If the enrollment security mode that you want to use as a default isn't enabled, select it and click **Enable**. The only enrollment security modes that you can use as a default are **User name + Password**, **Two Factor**, or **User name + PIN**.
2. Select the enrollment security mode and click **Default**. The selected mode is now the default. If any other enrollment security mode was set as the default, the mode is no longer the default.

### To disable an enrollment security mode

Disabling an enrollment security mode makes it unavailable for use, both for group enrollment invitations and on the Self-Help Portal. You might change how you allow users to enroll their devices by disabling one enrollment security mode and enabling another.

1. Select an enrollment security mode.  

You cannot disable the default enrollment security mode. If you want to disable the default enrollment security mode, you must first remove its default status.
2. Click **Disable**. The enrollment security mode is no longer enabled.

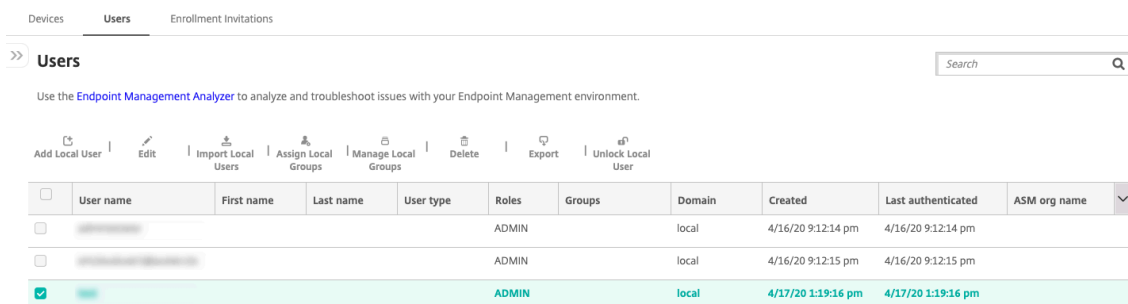
### Add, edit, unlock, or delete local user accounts

You can add local user accounts to Endpoint Management manually or you can use a provisioning file to import the accounts. For the steps to import user accounts from a provisioning file, see [Import user accounts](#).

All Citrix Cloud administrators get created as Endpoint Management administrators. If you create a Citrix Cloud administrator with custom access, make sure that access includes Endpoint Management. For information on adding Citrix Cloud administrators, see [Add administrators](#).



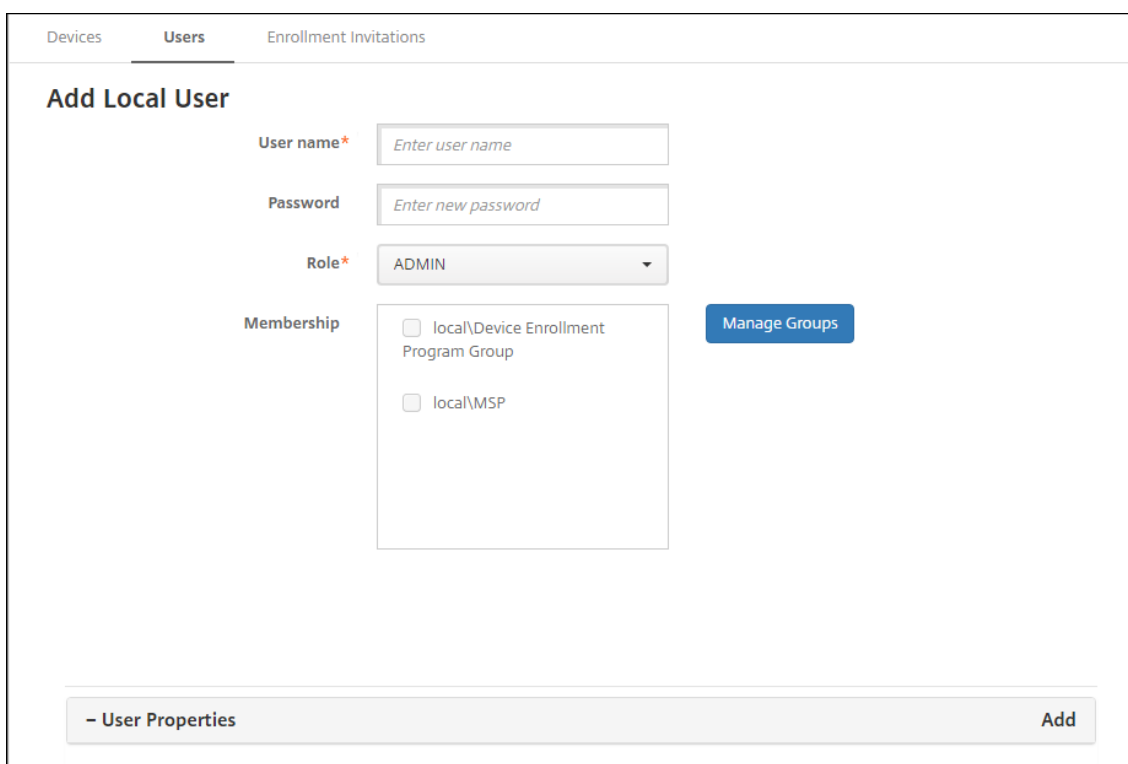
1. In the Endpoint Management console, click **Manage > Users**. The **Users** page appears.



2. Click **Show filter** to filter the list.

### To add a local user account

1. On the **Users** page, click **Add Local User**. The **Add Local User** page appears.



2. Configure these settings:

- **User name:** Type the name, a required field. You can include the following in names: spaces, uppercase letters, and lowercase letters.
- **Password:** Type an optional user password. The password must be at least 14 characters long and meet all of the following criteria:
  - Include at least two numbers
  - Include at least one uppercase and one lowercase letter

- Include at least one special character
- Don't include dictionary words or restricted words, such as your Citrix user name or email address
- Don't include more than three sequential and repeating characters or keyboard patterns, such as 1111, 1234, or asdf
- **Role:** In the list, click the user role. For more information about roles, see [Configure roles with RBAC](#). Possible options are:
  - ADMIN
  - DEVICE\_PROVISIONING
  - SUPPORT
  - USER
- **Membership:** In the list, click the group or groups to which to add the user.
- **User Properties:** Add optional user properties. For each user property you want to add, click **Add** and do the following:
  - **User Properties:** In the list, click a property and then type the user property attribute in the field next to the property.
  - Click **Done** to save the user property or click **Cancel**.

To delete an existing user property, hover over the line containing the property and then click the **X** on the right side. The property is deleted immediately.

To edit an existing user property, click the property and make changes. Click **Done** to save the changed listing or **Cancel** to leave the listing unchanged.

3. Click **Save**. After you create a user, the **User type** field for a local user account remains empty.

### To edit a local user account

1. On the **Users** page, in the list of users, click to select a user and then click **Edit**. The **Edit Local User** page appears.

The screenshot displays the 'Edit Local User' configuration page. At the top, there are tabs for 'Devices', 'Users', and 'Enrollment Invitations'. The 'Users' tab is active. The main content area is titled 'Edit Local User' and contains the following fields:

- User name\***: A text input field containing 'administrator'.
- Password**: A text input field with the placeholder text 'Enter new password'.
- Role\***: A dropdown menu currently set to 'ADMIN'.
- Membership**: A list of groups with checkboxes. The groups listed are 'local\Device Enrollment Program Group' and 'local\MSP'. A blue 'Manage Groups' button is positioned to the right of this list.

At the bottom of the page, there is a section titled '- User Properties' with an 'Add' button on the right side.

2. Change the following information as appropriate:

- **User name:** You cannot change the user name.
- **Password:** Change or add a user password.
- **Role:** In the list, click the user role.
- **Membership:** In the list, click the group or groups to which to add or edit the user account. To remove the user account from a group, clear the check box next to the group name.
- **User properties:** Do one of the following:
  - For each user property you want to change, click the property and make changes. Click **Done** to save the changed listing or **Cancel** to leave the listing unchanged.
  - For each user property you want to add, click **Add** and do the following:
    - \* **User Properties:** In the list, click a property and then type the user property attribute in the field next to the property.
    - \* Click **Done** to save the user property or click **Cancel**.
  - For each existing user property you want to delete, hover over the line containing the property and then click the **X** on the right side. The property is deleted immediately.

3. Click **Save** to save your changes or click **Cancel** to leave the user unchanged.

### To unlock a local user account

A local user account gets locked according to these server properties:

- `local.user.account.lockout.time`

- `local.user.account.lockout.limit`

For more information, see [Server Property Definitions](#).

When a local user account gets locked, you can unlock the account from the Endpoint Management console.

1. On the **Users** page, in the list of user accounts, click to select a user account.
2. Click **Unlock User**. A confirmation dialog box appears.
3. Click **Unlock** to unlock the user account or click **Cancel** to leave the user unchanged.

You can't unlock an Active Directory user from the Endpoint Management console. A locked Active Directory user must contact their Active Directory help desk for a password reset.

### To delete a local user account

1. On the **Users** page, in the list of user accounts, click to select a user account.  
You can select more than one user account to delete by selecting the check box next to each user account.
2. Click **Delete**. A confirmation dialog box appears.
3. Click **Delete** to delete the user account or click **Cancel**.

### To delete Active Directory users

To delete one or more Active Directory users at a time, select the users and click **Delete**.

If a user that you delete has enrolled devices and you want to re-enroll those devices, delete the devices before re-enrolling them. To delete a device, go to **Manage > Devices**, select the device, and then click **Delete**.

### Import user accounts

You can import local user accounts and properties from a .csv file called a provisioning file, which you can create manually. For more information about formatting provisioning files, see Provisioning file formats.

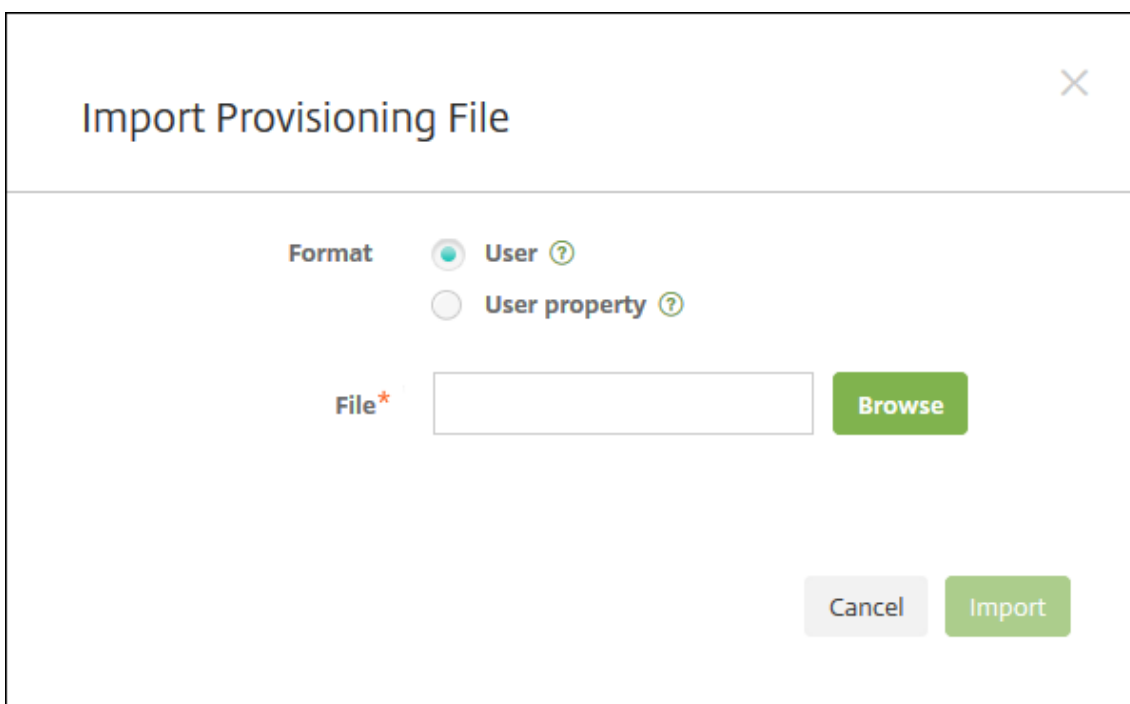
#### Note:

- For local users, use the domain name along with the user name in the import file. For example, specify `username@domain`. If the local user that you create or import is for a managed domain in Endpoint Management, the user cannot enroll by using the corresponding LDAP credentials.

- If importing user accounts to the Endpoint Management internal user directory, disable the default domain to speed up the import process. Keep in mind that disabling the domain affects enrollments. Reenable the default domain after the import of internal users is complete.
- Local users can be in User Principal Name (UPN) format. However, Citrix recommends that you do not use the managed domain. For example, if example.com is managed, do not create a local user with this UPN format: user@example.com.

After you prepare a provisioning file, follow these steps to import the file to Endpoint Management.

1. In the Endpoint Management console, click **Manage > Users**. The **Users** page appears.
2. Click **Import Local Users**. The **Import Provisioning File** dialog box appears.



The screenshot shows a dialog box titled "Import Provisioning File". It contains a "Format" section with two radio buttons: "User" (selected) and "User property". Below this is a "File\*" input field with a "Browse" button. At the bottom right, there are "Cancel" and "Import" buttons.

3. Select either **User** or **Property** for the format of the provisioning file you are importing.
4. Select the provisioning file to use by clicking **Browse** and then navigating to the file location.
5. Click **Import**.

### Provisioning file formats

You can create a provisioning file and use it to import user accounts and properties to Endpoint Management. Use one of the following formats for a provisioning file:

- **User provisioning file fields:** `user;password;role;group1;group2`
- **User attribute provisioning file fields:** `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

**Note:**

- Separate the fields within the provisioning file with a semi-colon (;). If part of a field contains a semi-colon, escape it with a backslash character (\). For example, type the property **propertyV; test;1;2** as **propertyV\;test\;1\;2** in the provisioning file.
- Valid values for **Role** are the predefined roles USER, ADMIN, SUPPORT, and DEVICE\_PROVISIONING, plus any other roles that you defined.
- Use the period character (.) as a separator to create a group hierarchy. Don't use a period in group names.
- Use lowercase for property attributes in attribute provisioning files. The database is case sensitive.

### Example of user provisioning content

The entry `user01;pwd\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` means:

- **User:** user01
- **Password:** pwd; 01
- **Role:** USER
- **Groups:**
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users01

As another example, `AUser0;1.password;USER;ActiveDirectory.test.net` means:

- **User:** AUser0
- **Password:** 1.password
- **Role:** USER
- **Group:** ActiveDirectory.test.net

### Example of user attribute provisioning content

The entry `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` means:

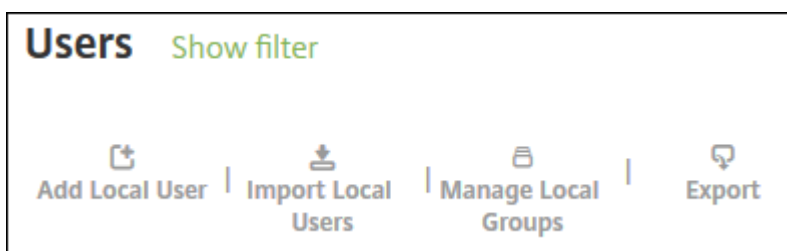
- **User:** user01
- **Property 1**
  - **name:** propertyN
  - **value:** propertyV;test;1;2
- **Property 2:**
  - **name:** prop 2
  - **value:** prop2 value

## Add or remove groups

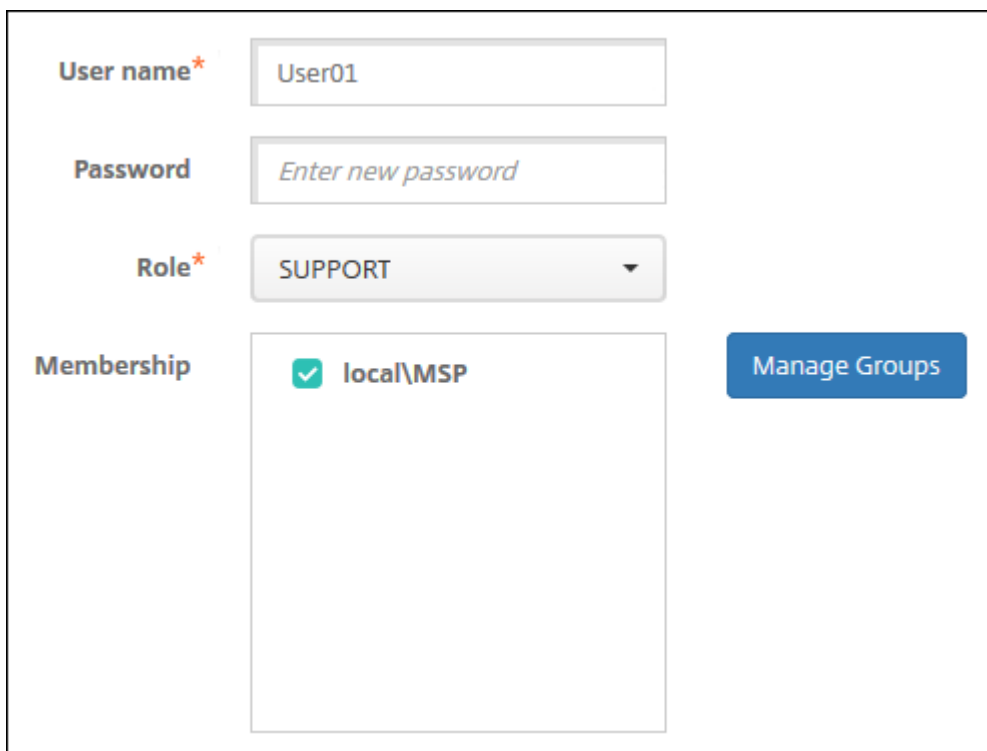
You manage groups in the **Manage Groups** dialog box in the Endpoint Management console on these pages: **Users**, **Add Local User**, or **Edit Local User**. There is no group edit command.

### To add a local group

1. Do one of the following:
  - On the **Users** page, click **Manage Local Groups**.



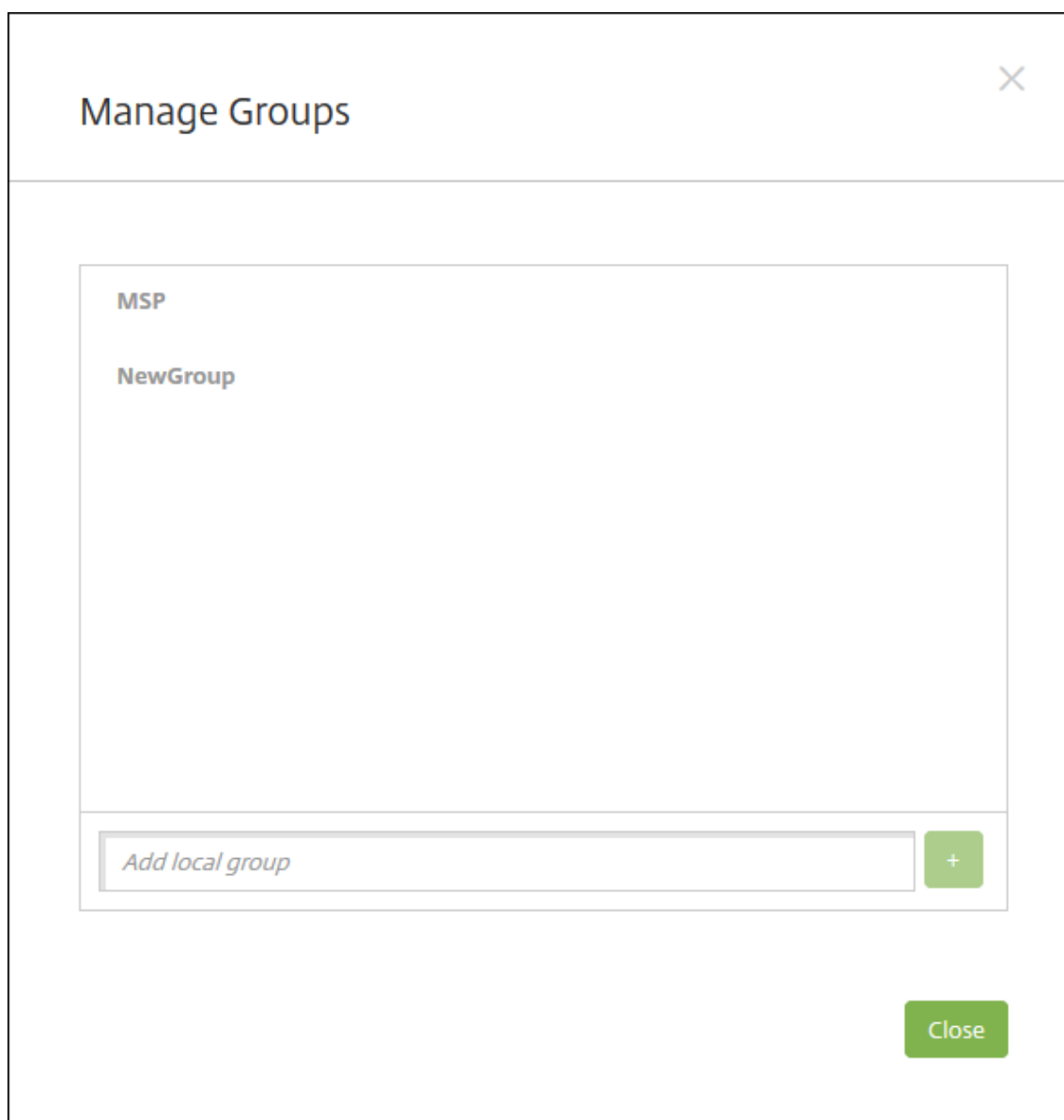
- On either the **Add Local User** page or the **Edit Local User** page, click **Manage Groups**.



The screenshot shows the 'Manage Groups' dialog box. It contains the following fields and controls:

- User name\***: Text input field containing 'User01'.
- Password**: Text input field containing the placeholder text 'Enter new password'.
- Role\***: Dropdown menu with 'SUPPORT' selected.
- Membership**: A list box containing one entry: 'local\MSP' with a checked checkbox.
- Manage Groups**: A blue button located to the right of the membership list.

The **Manage Group** dialog box appears.



2. Below the group list, type a new group name and then click the plus sign (+). The user group is added to the list.
3. Click **Close**.

### **To remove a group**

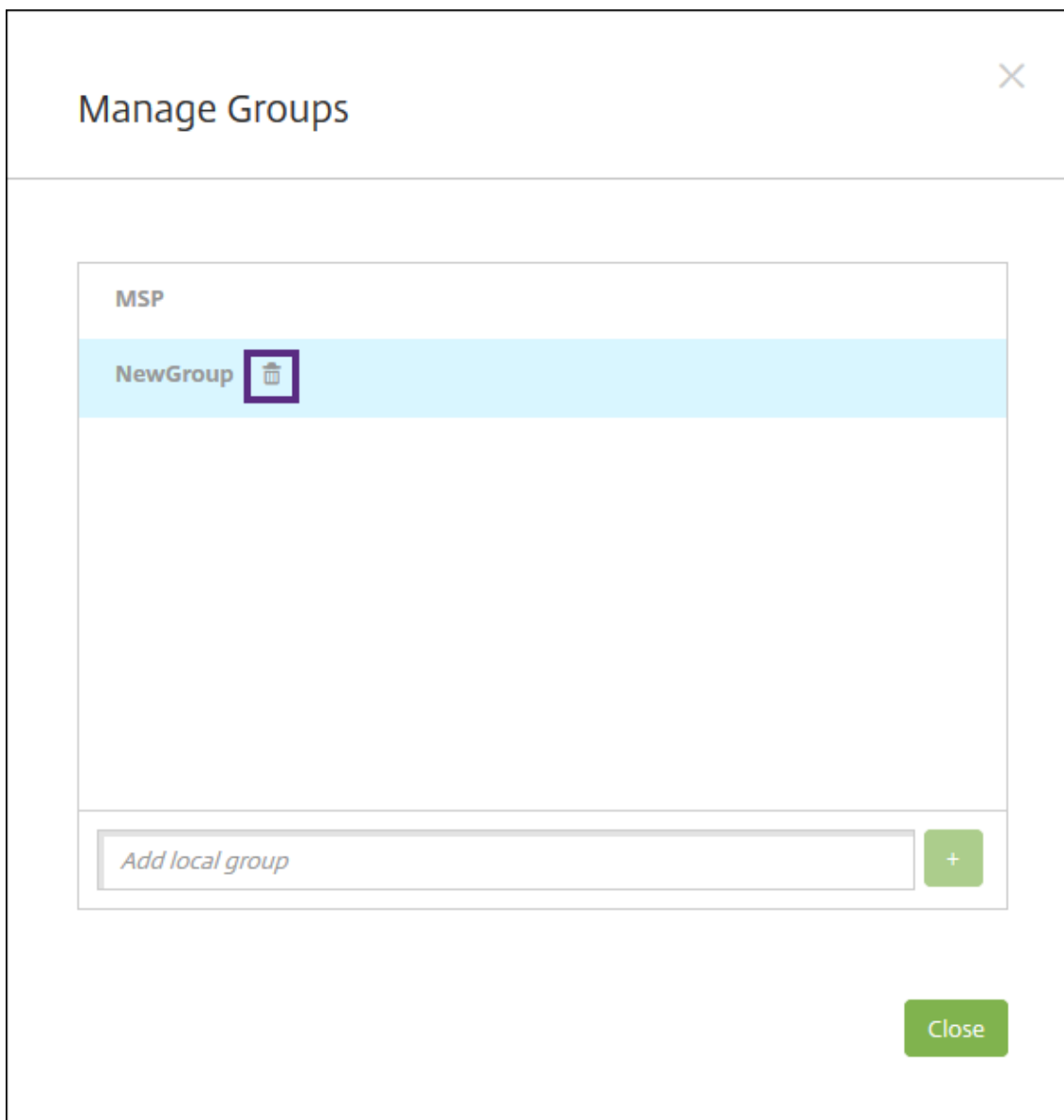
Removing a group has no effect on user accounts. Instead, removing a group only removes the user association with that group. Users also lose access to apps or profiles provided by the Delivery Groups that are associated with that group. However, any other group associations remain intact. If users aren't associated with any other local groups, they are associated at the top level.

1. Do one of the following:



- On the **Users** page, click **Manage Local Groups**.
- On either the **Add Local User** page or the **Edit Local User** page, click **Manage Groups**.

The **Manage Groups** dialog box appears.



2. On the **Manage Groups** dialog box, click the group you want to delete.
3. Click the trash can icon to the right of the group name. A confirmation dialog box appears.
4. Click **Delete** to confirm the operation and remove the group.

**Important:**

You cannot undo this operation.

5. On the **Manage Groups** dialog box, click **Close**.

## Create and manage workflows

You can use workflows to manage the creation and removal of user accounts. Before you create a workflow, identify individuals in your organization who have the authority to approve user account requests. Then, use the workflow template to create and approve user account requests.

When you set up Endpoint Management for the first time, you configure workflow email settings, which must be set before you can use workflows. You can change workflow email settings at any time. These settings include the email server, port, email address, and whether the request to create the user account requires approval.

You can configure workflows in two places in Endpoint Management:

- In the **Settings > Workflows** page in the Endpoint Management console. On the **Workflows** page, you can configure multiple workflows for use with app configurations. When you configure workflows on the Workflows page, you can select the workflow when you configure the app.
- When you configure an application connector in the app, provide a workflow name and then configure the individuals to approve the user account request. See [Add apps](#).

You can assign up to three levels for manager approval of user accounts. If you need other persons to approve the user account, you can search for and select them by using their name or email address. When Endpoint Management finds the person, you then add them to the workflow. All individuals in the workflow receive emails to approve or deny the new user account.

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Click **Workflows**. The **Workflows** page appears.
3. Click **Add**. The **Add Workflow** page appears.

Settings > Workflows > Add Workflow

### Add Workflow

Name\*

Description

Email Approval Templates Workflow Approval Request

Levels of manager approval 1 level

Select Active Directory domain agsag.com

Find additional required approvers

Selected additional required approvers

4. Configure these settings:

- **Name:** Type a unique name for the workflow.
- **Description:** Optionally, type a description for the workflow.
- **Email Approval Templates:** In the list, select the email approval template to be assigned. You create email templates in the **Notification Templates** section under **Settings** in the Endpoint Management console. When you click the eye icon to the right of this field, you see a preview of the template you are configuring.
- **Levels of manager approval:** In the list, select the number of levels of manager approval required for this workflow. The default is **1 level**. Possible options are:
  - Not Needed
  - 1 level
  - 2 levels
  - 3 levels
- **Select Active Directory domain:** In the list, select the appropriate Active Directory domain to be used for the workflow.
- **Find additional required approvers:** Type a name in the search field and then click **Search**. Names originate in Active Directory.

- When the name appears in the field, select the check box next to the name. The name and email address appear in the **Selected additional required approvers** list.
    - To remove a name from the list, do one of the following:
      - \* Click **Search** to see a list of everyone in the selected domain.
      - \* Type a full or partial name in the search box, and then click **Search** to limit the search results.
      - \* Persons in the **Selected additional required approvers** list have check marks next to their name in the search results list. Scroll through the list and clear the check box next to each name that you want to remove.
5. Click **Save**. The created workflow appears on the **Workflows** page.

After you create the workflow, you can view the workflow details, view the apps associated with the workflow, or delete the workflow. You cannot edit a workflow after you create the workflow. If you need a workflow with different approval levels or approvers, create another workflow.

#### To view details and delete a workflow

1. On the **Workflows** page, in the list of existing workflows, select a specific workflow. To do that, click the row in the table or select the check box next to the workflow.
2. To delete a workflow, click **Delete**. A confirmation dialog box appears. Click **Delete** again.

**Important:**

You cannot undo this operation.

## Enrollment profiles

September 17, 2021

An enrollment profile specifies the following:

- Device management enrollment options for Android, iOS, and Windows devices.
- App management enrollment options for Android and iOS devices.
- Other enrollment options:
  - Whether to limit the number of devices a user can enroll.  
If the device limit is reached, an error message lets the user know that they exceeded the device registration limit.
  - Whether to allow a user to decline device management.

You can use enrollment profiles to combine multiple use cases and device migration paths within a single Endpoint Management console. Some use cases include:

- Mobile Device Management (MDM only)
- MDM+Mobile Application Management (MAM)
- MAM only
- Corporate-owned enrollments
- BYOD enrollments (the ability to opt out of MDM enrollment)
- Migration of Android Device Administrator enrollments to Android Enterprise enrollments (fully managed, work profile, dedicated device)
- Automatic enrollment of Windows 10 and Windows 11 devices through Workspace app for Windows (preview)

If your current site is MDM only and you want to add MAM, you must configure a Citrix Gateway. For more information, see [Citrix Gateway requirements](#).

When you create a delivery group, you can use the default enrollment profile named Global or specify a different enrollment profile.

Enrollment profile features by platform include the following.

- **For Android devices:** You specify the management and device owner mode. For example: Company-owned device, fully managed with work profile, and BYOD work profile.

New devices enroll in Android Enterprise by default. You can opt to manage the devices using legacy Android device administrator (DA) mode. New devices also enroll in app management by default.

For information about specifying the level of security and required enrollment steps, see [User accounts, roles, and enrollment](#).

- **For iOS devices:** You specify the device management type: **Apple User Enrollment**, **Apple Device enrollment**, or **Do not manage devices**. This **Apple User Enrollment** mode is available as a public preview. To enable this feature, contact your support team.

If you select Apple User Enrollment, you can choose to use a custom domain for Managed Apple IDs and configure that domain.

New devices enroll in Apple device management by default. New devices also enroll in app management by default.

- **For Windows 10 and Windows 11 devices:** You specify whether to use Citrix device management for Windows. New devices enroll in device management by default.

**Preview:** If Endpoint Management is Workspace-enabled, you can also choose to allow devices to enroll through the Workspace app. For more information, see [Enroll Windows 10 and Windows 11 devices through Citrix Workspace app](#).

## Global enrollment profile

The default enrollment profile is named Global. The Global profile is useful for testing until you have a chance to create enrollment profiles.

If you onboard to Endpoint Management 20.2.1 or later, the Global enrollment profile has predefined settings. The following screenshots show the default settings for the Global enrollment profile. MAM only deployments display a subset of these options.

Enrollment Profile	Enrollment Info
1 Enrollment Info	<p>Set the number of devices a user can enroll. The default is unlimited, which lets users enroll an unlimited number of devices.</p> <p>Enrollment profile name * <input type="text"/></p> <p>Total number of devices a user can enroll <input type="text" value="unlimited"/></p>
2 Platforms	
Android	
iOS	
Windows	
3 Assignment (optional)	

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	<p>Specify device management settings for this enrollment profile.</p> <p><b>Device management</b> ?</p> <p><b>Management</b></p> <ul style="list-style-type: none"> <li><input checked="" type="radio"/> Android Enterprise ?</li> <li><input type="radio"/> Legacy device administration (not recommended) ?</li> <li><input type="radio"/> Do not manage devices ?</li> </ul> <p><b>Device owner mode</b></p> <ul style="list-style-type: none"> <li><input checked="" type="radio"/> Company Owned device ?</li> <li><input type="radio"/> Fully managed with work profile ?</li> <li><input type="radio"/> Dedicated device ?</li> <li><input type="radio"/> None ?</li> </ul> <p><b>BYOD work profile</b> <input checked="" type="checkbox"/> ?</p> <p><b>Application management</b> ?</p> <p>Citrix MAM <input checked="" type="checkbox"/> ?</p> <p><b>User consent</b></p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ?</p>
2 Platforms	
Android	
iOS	
Windows	
3 Assignment (optional)	

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	<p>Specify device management settings for this enrollment profile.</p> <p><b>Device management</b> <a href="#">?</a></p> <p><b>Management</b></p> <p><input checked="" type="radio"/> Apple User Enrollment <a href="#">?</a></p> <p><input type="radio"/> Apple Device enrollment <a href="#">?</a></p> <p><input type="radio"/> Do not manage devices <a href="#">?</a></p> <p><b>Use custom domain for Managed Apple ID</b> <input checked="" type="checkbox"/> <a href="#">?</a></p> <p><b>Managed Apple ID custom domain</b> <input type="text" value="example.appleid.com"/> <a href="#">?</a></p> <p><b>Application management</b> <a href="#">?</a></p> <p><b>Citrix MAM</b> <input checked="" type="checkbox"/> <a href="#">?</a></p> <p><b>User consent</b></p> <p><b>Allow users to decline device management</b> <input checked="" type="checkbox"/> <a href="#">?</a></p>
2 Platforms	
Android	
<b>iOS</b>	
Windows	
3 Assignment (optional)	

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	<p>Specify device management settings for this enrollment profile.</p> <p><b>Device management</b> <a href="#">?</a></p> <p><b>Management</b></p> <p><input checked="" type="radio"/> Fully managed <a href="#">?</a></p> <p><input type="radio"/> Do not manage devices <a href="#">?</a></p> <p><b>User consent</b></p> <p><b>Allow users to decline device management</b> <input checked="" type="checkbox"/> <a href="#">?</a></p> <p><b>Workspace integration</b> <a href="#">?</a></p> <p><b>Enrollment through Workspace app</b> <input type="checkbox"/> <a href="#">?</a></p>
2 Platforms	
Android	
iOS	
<b>Windows</b>	
3 Assignment (optional)	

### Enrollment profiles, delivery groups, and enrollment

Enrollment profiles and delivery groups interact as follows:

- You can attach an enrollment profile to one or more delivery groups.
- If a user belongs to multiple delivery groups that have different enrollment profiles, the name of the delivery group determines the enrollment profile used. Endpoint Management selects

the delivery group that appears last in an alphabetized list of delivery groups. For example, suppose that you have the following:

- Two enrollment profiles, named “EP1” and “EP2”.
- Two delivery groups, named “DG1” and “DG2”.
- “DG1” is associated with “EP1”.
- “DG2” is associated with “EP2”.

If the enrolling user is in both the “DG1” and “DG2” delivery groups, Endpoint Management uses the “EP2” enrollment profile to determine the enrollment type for the user.

- Deployment order applies only to devices in a delivery group that has an enrollment profile configured for MDM (device management).
- After a device enrolls, some changes to an enrollment profile require re-enrollment:
  - Changing the configuration to downgrade a device from MDM+MAM to MAM or MDM enrollment. A downgrade might occur when you update an enrollment profile or move a device to a different delivery group.
  - Adding MAM to an enrollment profile that’s configured for MDM.
  - Adding MDM to an enrollment profile that’s configured for MAM.
- Switching to a different enrollment profile does not affect existing enrolled devices. However, users must unenroll and then reenroll those devices for the changes to take effect.

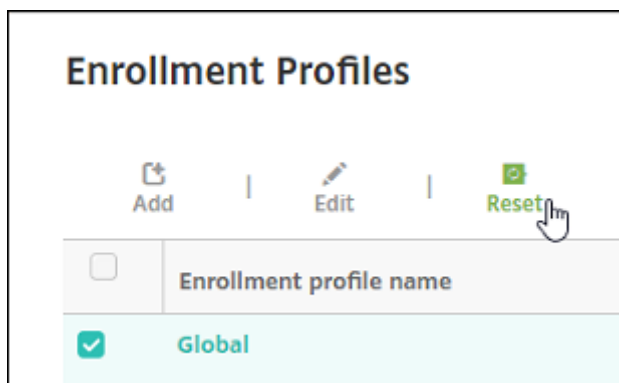
### To create an enrollment profile

1. In the Endpoint Management console, go to **Configure > Enrollment Profiles**.
2. On the **Enrollment Info** page, type a descriptive name for the profile. By default, a user can enroll unlimited devices. Select a value to limit the number of devices per user. The limit applies to the sum of MAM or MDM managed Android, iOS, and Windows devices that a user enrolls.
3. Complete the platform pages. For information about enrollment settings specific to the platforms, see:
  - Android Enterprise: [Creating enrollment profiles](#)
  - iOS: [Supported enrollment methods](#)
  - Windows Desktop and Tablet: [Supported enrollment methods](#)
4. On the **Assignments** page, attach one or more delivery groups to the enrollment profile.

A user might belong to multiple delivery groups that have different enrollment profiles. In that case, the name of the delivery group determines the enrollment profile used. Endpoint Management selects the delivery group that appears last in an alphabetized list of delivery groups. To create delivery groups, go to **Configure > Delivery Groups**.



A list of your enrollment profiles appears on the **Configure > Enrollment Profiles** page. To edit the Global profile or reset it to the original defaults, select the row for the Global profile and click **Reset**. You can't delete the Global profile.



## Notifications

August 31, 2021

You can use notifications in Endpoint Management for the following purposes:

- To communicate with select groups of users for several system-related functions. You can also target these notifications for certain users. For example, all users with iOS devices, users whose devices are out of compliance, users with employee-owned devices, and so on.
- To enroll users and their devices
- To automatically notify users (using automated actions) when certain conditions are met. For example:
  - When a user device is about to be blocked from the corporate domain because of a compliance issue
  - When a device has been jailbroken or rooted

For details about automated actions, see [Automated Actions](#).

To send notifications with Endpoint Management, you must configure a gateway and a notification server. You can set up a notification server in Endpoint Management to configure SMTP and SMS gateway servers. Those servers send email and text (SMS) notifications to users. You can use notifications to send messages over two different channels: SMTP or SMS.

- SMTP is a connection-oriented, text-based protocol in which a mail sender communicates with a mail receiver. The mail sender issues command strings and supplies necessary data, typically over a TCP connection. SMTP sessions consist of commands originated by an SMTP client (the person sending the message) and corresponding responses from the SMTP server.

- SMS is a text messaging service component of phone, Web, or mobile communication systems. SMS uses standardized communications protocols to enable fixed line or mobile phone devices to exchange short text messages.

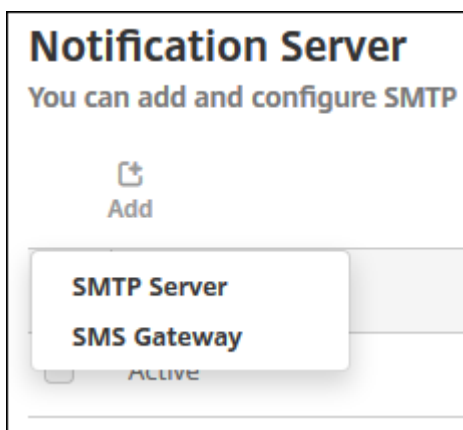
You can also set up a Carrier SMS Gateway in Endpoint Management to configure notifications that are sent through an SMS gateway of a carrier. Carriers use SMS gateways to send or receive SMS transmissions to or from a telecommunications network. These text-based messages use standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages.

### Prerequisites

- Before configuring the SMS gateway, consult your system administrator to determine the server information. Learn whether the SMS server is hosted on an internal corporate server or is part of a hosted email service. If the SMS server is part of a hosted email service, you need information from the website of the service provider.
- Configure the SMTP notifications server to send messages to users. If the server is hosted on an internal server, contact your system administrator for configuration information. If the server is a hosted email service, locate the appropriate configuration information on the website of the service provider.
- You can use one active SMTP server and one active SMS server simultaneously. Both of those communication channels allow one active configuration.
- Open port 25 from Endpoint Management located in your network DMZ to point back to the SMTP server on your internal network. That enables Endpoint Management to send notifications successfully.

### Configure an SMTP server and SMS gateway

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Under **Notifications**, click **Notification Server**. The **Notification Server** page appears.
3. Click **Add**. A menu appears with options to configure an SMTP server or an SMS gateway.



- To add an SMTP server, click **SMTP Server** and then see Add an SMTP server for the steps to configure this setting.
- To an SMS gateway, click **SMS Gateway** and then see Add an SMS gateway for the steps to configure this setting.

## Add an SMTP server

Settings > Notification Server > Add SMTP Server

### Add SMTP Server

You need to configure the SMTP notifications server to send messages to users. If the SMTP server is hosted on an internal server, you get the server information from your IT department. If the server is a hosted email service, you can find information from the service provider's website. Only one SMTP server is activated at one time.

Name*	<input type="text"/>
Description	<input type="text"/>
SMTP Server*	<input type="text"/>
Secure channel protocol	None ▾
SMTP server port*	25
Authentication	<input type="radio"/> OFF
Microsoft Secure Password Authentication (SPA)	<input type="radio"/> OFF
From name*	<input type="text"/>
From email*	<input type="text"/>

▶ Advanced Settings

#### 1. Configure these settings:

- **Name:** Type the name associated with this SMTP server account.
- **Description:** Optionally, enter a description of the server.
- **SMTP Server:** Type the host name for the server. Specify either a fully qualified domain name (FQDN) or an IP address.
- **Secure channel protocol:** In the list, click **SSL**, **TLS**, or **None** for the secure channel protocol used by the server (if the server is configured to use secure authentication). The default is **None**.
- **SMTP server port:** Type the port used by the SMTP server. By default, the port is set to 25. If SMTP connections use the SSL secure channel protocol, set the port to 465.
- **Authentication:** Select **On** or **Off**. The default is **Off**.

- If you enable **Authentication**, configure these settings:
    - **User name:** Type the user name for authentication
    - **Password:** Type the authentication user's password.
  - **Microsoft Secure Password Authentication (SPA):** If the SMTP server is using the SPA, click **On**. The default is **Off**.
  - **From Name:** Type the name displayed in the **From** box when a client receives a notification email from this server. For example, Corporate IT.
  - **From email:** Type the email address used if an email recipient replies to the notification sent by the SMTP server.
2. Click **Test Configuration** to send a test email notification.
  3. Expand **Advanced Settings** and then configure these settings:
    - **Number of SMTP retries:** Type the number of times to retry a failed message sent from the SMTP server. The default is 5.
    - **SMTP Timeout:** Type the duration to wait (in seconds) when sending an SMTP request. Increase this value if message sending continuously fails because of timeouts. Use caution when decreasing this value, to avoid increasing the number of timed out and undelivered messages. The default is 30 seconds.
    - **Maximum number of SMTP recipients:** Type the maximum number of recipients per email message sent by the SMTP server. The default is 100.
  4. Click **Add**.

## Add an SMS gateway

Settings > Notification Server > Add SMS Gateway

### Add SMS Gateway

Please consult with your IT department about the server info if the SMS server is hosted on internal corporate server; if this is a hosted email service, the info is available from the service provider's website. Only one SMS server is activated at one time.

**Name\***

**Description**

**Key\***

**Secret\***

**Virtual phone number\***

**HTTPS**  OFF

**Country code**

**Use Carrier Gateway**  ON

#### Note:

Endpoint Management only supports Nexmo SMS messaging. If you do not already have an account to use Nexmo messaging, visit their [website](#) to create one.

#### 1. Configure the following settings:

- **Name:** Type a name for the SMS Gateway configuration. This field is required.
- **Description:** Optionally, type a description of the configuration.
- **Key:** Type the numerical identifier provided by the system administrator when activating the account. This field is required.
- **Secret:** Type a secret provided by the system administrator that is used to access your account. If the password is lost or stolen, the secret enables you to recover. This field is required.
- **Virtual Phone Number:** This field is used when sending to North American phone numbers (with the +1 prefix). Type a Nexmo virtual phone number, using digits only. You can purchase virtual phone numbers on the Nexmo website.

- **HTTPS:** Select whether to use HTTPS to transmit SMS requests to Nexmo. The default is **Off**.

**Important:**

Leave HTTPS set to **On** unless you have guidance from Citrix Support to turn it to **Off**.

- **Country Code:** In the list, click the default SMS country code prefix for recipients in your organization. This field always starts with a + symbol. The default is **Afghanistan +93**.
2. Click **Test Configuration** to send a test message using the current configuration. Connection errors, such as authentication or virtual phone number errors, are detected and appear immediately. Messages are received in the same time frame as messages sent between mobile phones.
  3. Click **Add**.



### Add a carrier SMS gateway

You can set up a Carrier SMS Gateway in Endpoint Management to configure notifications that are sent through a carrier's SMS gateway. Carriers use Short Message Service (SMS) gateways to send or receive SMS transmissions to or from a telecommunications network. These text-based messages use standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages.



1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Under **Notifications**, click **Carrier SMS Gateway**. The **Carrier SMS Gateway** page opens.

Settings > Carrier SMS Gateway

### Carrier SMS Gateway

 Add |  Detect

<input type="checkbox"/>	Carrier	SMTP domain	Country code	Sending prefix	▼
<input type="checkbox"/>	Alltel	message.alltel.com	+1		
<input type="checkbox"/>	AT&T	txt.att.net	+1		
<input type="checkbox"/>	Boost Mobile	myboostmobile.com	+1		
<input type="checkbox"/>	Bouygues Telecom	mms.bouyguestelecom.fr	+33		
<input type="checkbox"/>	Cingular	cingularme.com	+1		
<input type="checkbox"/>	Metro PCS	mymetropcs.com	+1		
<input type="checkbox"/>	Nextel	messaging.nextel.com	+1		
<input type="checkbox"/>	Orange	websmsmms.orange.fr	+33		
<input type="checkbox"/>	Powertel	ptel.net	+1		
<input type="checkbox"/>	SFR	sfr.fr	+33		

Showing 1 - 10 of 16 items Showing 1 of 2  

3. Do one of the following:

- Click **Detect** to automatically discover a gateway. A dialog box appears indicating that there are no new carriers detected or listing the new carriers detected among enrolled devices.
- Click **Add**. The **Add a Carrier SMS Gateway** dialog box appears.



### Add a Carrier SMS Gateway ✕

Converts email messages passing through the gateway to a pre-defined format, such as an instant message.

**Carrier\***

**Gateway SMTP domain\***

**Country code\***

**Email sending prefix**

**Note:**

Endpoint Management only supports Nexmo SMS messaging. If you do not already have an account to use Nexmo messaging, visit their [website](#) to create one.

4. Configure these settings:
  - **Carrier:** Type the name of the carrier.
  - **Gateway SMTP domain:** Type the domain associated with the SMTP gateway.
  - **Country code:** In the list, click the country code for the carrier.
  - **Email sending prefix:** Optionally, specify an email sending prefix.
5. Click **Add** to add the new carrier or click **Cancel** to not add the new carrier.

### Create and update notification templates

You can create or update notification templates in Endpoint Management to be used in automated actions, enrollment, and standard notification messages sent to users. You configure the notification

templates to send messages over three different channels: Secure Hub, SMTP, or SMS.

Endpoint Management includes many predefined notification templates. The templates reflect the distinct types of events that Endpoint Management automatically responds to for every device in the system.

**Note:**

If you plan to use SMTP or SMS channels to send notifications to users, you must set up the channels before you can activate them. Endpoint Management prompts you to set up the channels when you add notification templates if they are not already set up.

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Click **Notification Templates**. The **Notification Templates** page appears.

Settings > Notification Templates

### Notification Templates

Create notification templates to use in automated actions, enrollment, and standard notification message delivery to users.

Add

<input type="checkbox"/>	Name	Channels	Type	Deletable	Manual sending supported	
<input type="checkbox"/>	ActiveSync Gateway Blocked	Worx Home	ActiveSync Gateway blocked device			
<input type="checkbox"/>	Android Download Link	SMTP, SMS	Android Download Link			
<input type="checkbox"/>	APNS cert expiration	SMTP	APNS Cert Expiration			
<input type="checkbox"/>	Certificate renewal	Worx Home	Certificate is renewed			
<input type="checkbox"/>	Enrollment	SMTP, SMS	Enrollment Notification			
<input type="checkbox"/>	Enrollment Confirmation	SMTP, SMS	Enrollment Confirmation			
<input type="checkbox"/>	Enrollment Invitation	SMTP, SMS	Enrollment Invitation			
<input type="checkbox"/>	Enrollment PIN	SMTP, SMS	Enrollment PIN			
<input type="checkbox"/>	Failed Samsung KNOX attestation	Worx Home	Failed Samsung KNOX attestation			
<input type="checkbox"/>	iOS Download Link	SMTP, SMS	iOS Download Link			

Showing 1 - 10 of 25 items Showing  of 3

### Add a notification template

1. Click **Add**. If no SMS gateway or SMTP server is set up, a message about the use of SMS and SMTP notifications appears. You can choose to set up the SMTP server or SMS gateway now or set them up later.

If you choose to set up SMS or SMTP server settings now, you are redirected to the **Notification Server** page on the **Settings** page. After setting up the channels you want to use, you can return

to the **Notification Template** page to continue adding or modifying notification templates.

**Important:**

If you choose to set up SMS or SMTP server settings later, you can't activate those channels when you add or edit a notification template. As a result, those channels aren't available for sending user notifications.

## 2. Configure these settings:

- **Name:** Type a descriptive name for the template.
- **Description:** Type a description for the template.
- **Type:** In the list, click the notification type. Only supported channels for the selected type appear. Only one APNS Cert Expiration template is allowed, which is a predefined template. You can't add a template of this type.

**Note:**

For some template types, the phrase "Manual sending supported" appears below the type. Those template types are available in the **Notifications** list on the **Dashboard** and on the **Devices** page. From those locations you can manually send the notification to users. Manual sending is not available in any template that uses the following macros in the Subject or Message field on any channel:

- `${outofcompliance.reason(whitelist_blacklist_apps_name)}`
- `${outofcompliance.reason(smg_block)}`

**Note:**

The Endpoint Management console includes the terms "blacklist" and "whitelist". We are changing those terms in an upcoming release to "block list" and "allow list".

3. Under **Channels**, configure the information for each channel to be used with this notification. You can choose any or all channels. The channels you choose depends on how you want to send notifications:

- If you choose **Secure Hub**, only iOS and Android devices receive the notifications, which appear in the device notification tray.
- If you choose **SMTP**, users who enrolled with their email address receive the message.
- If you choose **SMS**, only users using devices with a SIM card receive the notification.

**Secure Hub:**

- **Activate:** Click to enable the notification channel.
- **Message:** Type the message to be sent to the user. This field is required if you are using Secure Hub. For information about using macros in a message, see [Macros](#).
- **Sound File:** In the list, click the notification sound the user hears when the notification is received.

**SMTP:**

- **Activate:** Click to enable the notification channel.

You can activate the SMTP notification only after you set up the SMTP server.

- **Sender:** Type an optional sender for the notification, which can be a name, an email address, or both.
- **Recipient:** This field contains a pre-built macro for all but Ad Hoc notifications to ensure that notifications are sent to the correct SMTP recipient address. Citrix recommends that you do not modify macros in templates. You can add more recipients (such as a corporate administrator), by adding their addresses in this field. Use a semi-colon (;) to separate the macros and other addresses. To send Ad Hoc notifications, you can enter specific recipients, or you can select devices from the **Manage > Devices** page and send notifications from there. For details, see [Devices](#).
- **Subject:** Type a descriptive subject for the notification. This field is required.
- **Message:** Type the message to be sent to the user. For information about using macros in a message, see [Macros](#).

**SMS:**

- **Activate:** Click to enable the notification channel.

You can activate the SMTP notification only after you set up the SMTP server.

- **Recipient:** This field contains a pre-built macro for all but Ad Hoc notifications to ensure that notifications are sent to the correct SMS recipient address. Citrix recommends that you do not modify macros in templates. To send Ad Hoc notifications, you can enter specific recipients, or you can select devices from the **Manage > Devices** page.
- **Message:** Type the message to be sent to the user. This field is required. You can use HTML and macros to draft the message. For information about using macros in a message, see [Macros](#). See the following for an example of using HTML. The `<!DOCTYPE html>` tag is case sensitive.

```
1 <!DOCTYPE html>
2 <TITLE>Your Title Here</TITLE>
3
4 <BODY>
5
6 <HR>
7
8 <a href="http://somegreatsite.com">Link Name</a> is a link to
   another site.
9
```

```
10 <H1>This is a Header</H1>
11
12 <H2>This is a Medium Header</H2>
13
14 Send me mail at <a href="mailto:support@yourcompany.com">
    support@yourcompany.com</a>.
15
16 <P> This is a new paragraph.
17
18 <P> <B>This is a new paragraph, in bold.</B>
19
20 <BR> <B><I>This is a new sentence without a paragraph break,
    in bold italics.</I></B>
21
22 <HR>
23 
24
25 </BODY>
26
27 </html>
28 <!--NeedCopy-->
```

4. Click **Add**. When all channels are correctly configured, they appear in this order on the **Notification Templates** page: SMTP, SMS, and Secure Hub. Any channels not correctly configured appear after the correctly configured channels.

### Edit a notification template

1. Select a notification template. The edit page specific to that template appears. You can edit the template, except for the **Type** field, and activate or deactivate channels.
2. Click **Save**.

### Delete a notification template

You can delete only notification templates that you have added. You cannot delete predefined notification templates.

1. Select an existing notification template.
2. Click **Delete**. A confirmation dialog box appears.
3. Click **Delete** to delete the notification template or click **Cancel** to cancel deleting the notification template.

## Configure roles with RBAC

September 30, 2021

The role-based access control (RBAC) feature in Endpoint Management lets you assign roles to users and groups. Roles are sets of permissions that control the level of access users have to system functions.

Endpoint Management comes with the following default user roles. You can use the default roles as templates that you customize to create your own user roles.

- **Administrator:** Grants full system access.
- **User:** Allows users to enroll devices and access the Self-Help Portal.

You can use the RBAC feature in Endpoint Management to:

- Create and edit user roles.
- Assign local user groups and Active Directory groups to a role.
- Assign local users to roles. Use **Manage > Users** in Endpoint Management to make this assignment.

For cloud administrators, you assign roles in Citrix Cloud. See [Manage Citrix Cloud administrators](#).

### Important:

Only new Endpoint Management customers onboarded after October 4, 2021 can assign RBAC roles to cloud administrators.

For details on the predefined Admin and User role permissions, see [Predefined roles](#).

## Use the RBAC feature

You can assign roles to local users, to cloud administrators (in Citrix Cloud), and to local user groups and Active Directory groups.

- **Local users:** Assign roles to local users using **Manage > Users**. You can assign only one role to local users. To change the roles, you can manually edit the user account. Or, you can create a group for local users and assign a role to that group.
- **Cloud administrators:** A cloud administrator is a special user account that Citrix Cloud creates when an administrator is added to your Citrix Cloud customer account. A cloud administrator account uses the same user name as the administrator account on Citrix Cloud.

You can assign only one role to cloud administrators. You can't add these users to a group. Change the roles and permissions of cloud administrators through the Citrix Cloud console. However, these users are listed in the **Manage > Users** tab in Endpoint Management.

- **Active Directory groups:** All users in an Active Directory group have the same permissions. If a user belongs to several Active Directory groups, all the permissions merge to define the permissions for that user. For example, suppose ADGroupA users can locate manager devices and ADGroupB users can wipe employee devices. A user who belongs to both groups can locate and wipe the devices of managers and employees. If a user belongs to groups with conflicting permissions, the allowed permissions prevail.

**Note:**

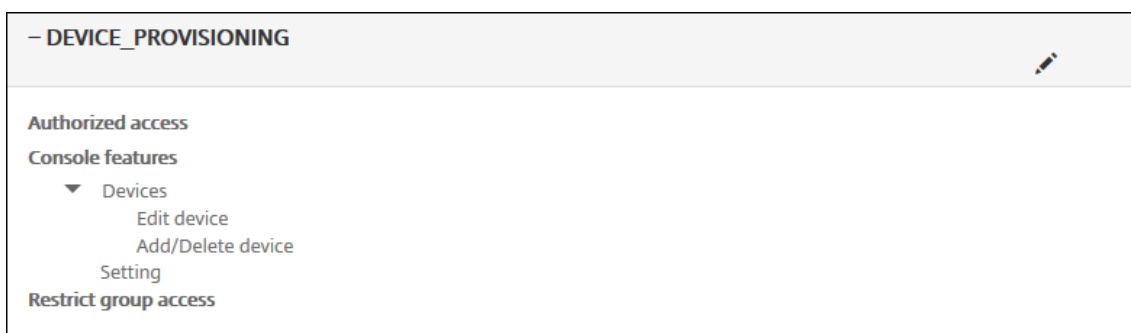
You can modify the permissions of an Endpoint Management administrator only after the administrator has accepted an administrator invitation and clicked **Manage** on the Endpoint Management tile.

For more information, see [About user accounts](#).

To add roles and assign them to user groups:

1. In the Endpoint Management console, to access the **Settings** page, click the gear icon in the upper-right corner.
2. Click **Role-Based Access Control**. The **Role-Based Access Control** page shows the default user roles and any roles that you added.

Click the plus sign (+) next to a role to see all the permissions for that role.



3. To add a role, click **Add**. Or, to edit a role, click the pen to the right of an existing role.

**Note:**

You can delete a role by clicking the trash can to the right of a role that you defined. You can't delete the default user roles.

4. On the **Add Role** page, enter the following information:
  - **RBAC name:** Enter a descriptive name for the new user role. You can't change the name of an existing role.
  - **RBAC template:** Optionally, select a template as the starting point for the new role. (When editing a role, you can't select or change templates.) RBAC templates are the default user roles that define the access to system functions.

5. Click **Apply** to the right of the **RBAC template** field to populate the **Authorized access** and **Console features** check boxes. Endpoint Management fills those fields with the predefined access and feature permissions for the selected template.

Settings > Role-Based Access Control > Add Role

**Add Role**

1 Role Info

2 Assignment

**Role Info**

RBAC name \*

RBAC template Select a template Apply

Authorized access

- Admin console access
- Self Help Portal access
- Shared devices enroller
- Remote Support access
- Public API access
- COSU devices enroller

Console features

- Dashboard
- Reporting
- ▶  Devices
- ▶  Local Users and Groups
- ▶  Enrollment
- ▶  Policies
- ▶  App
- ▶  Media
- ▶  Emulation

Apply permissions

To all user groups

To specific user groups

Next >

6. To customize the role, select or clear the check boxes in **Authorized access** and **Console features**.

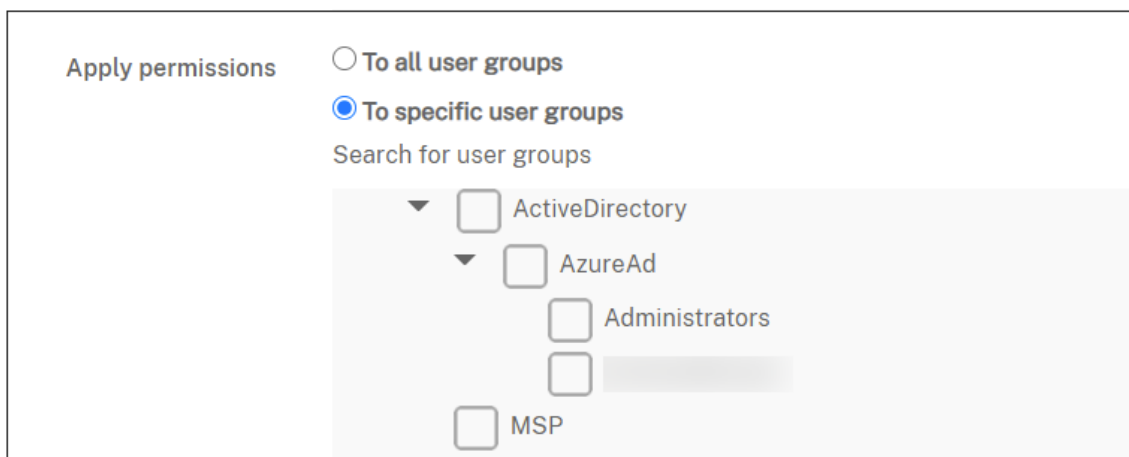
Click the triangle next to a console feature to select permissions specific to that feature. Clicking the top-level check box does not select the individual permissions. Select individual options after expanding the top-level permission.

7. **Apply permissions:** Click **To specific user groups** to apply permissions to the groups you select.

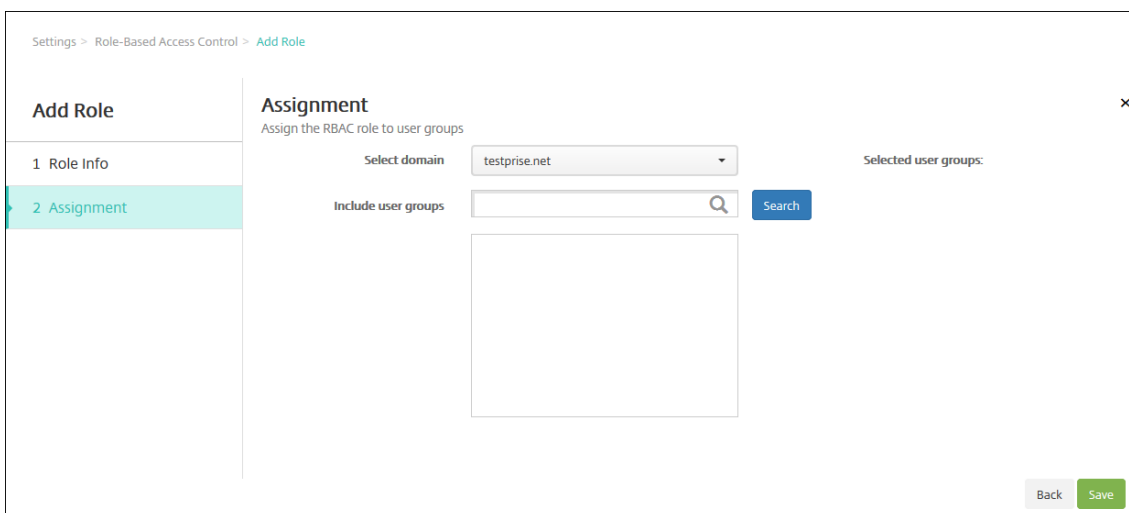
For example, if an RBAC administrator has permissions to the ActiveDirectory and MSP user groups:

- The administrator can access information only for users who are in the ActiveDirectory group, the MSP group, or both of those groups.
- The administrator can't view any other local or AD users. The administrator can view users who are members of child groups of either of those groups.
- The administrator can send invitations to:
  - The permission groups and their child groups
  - The users who are members of permission groups and their child groups



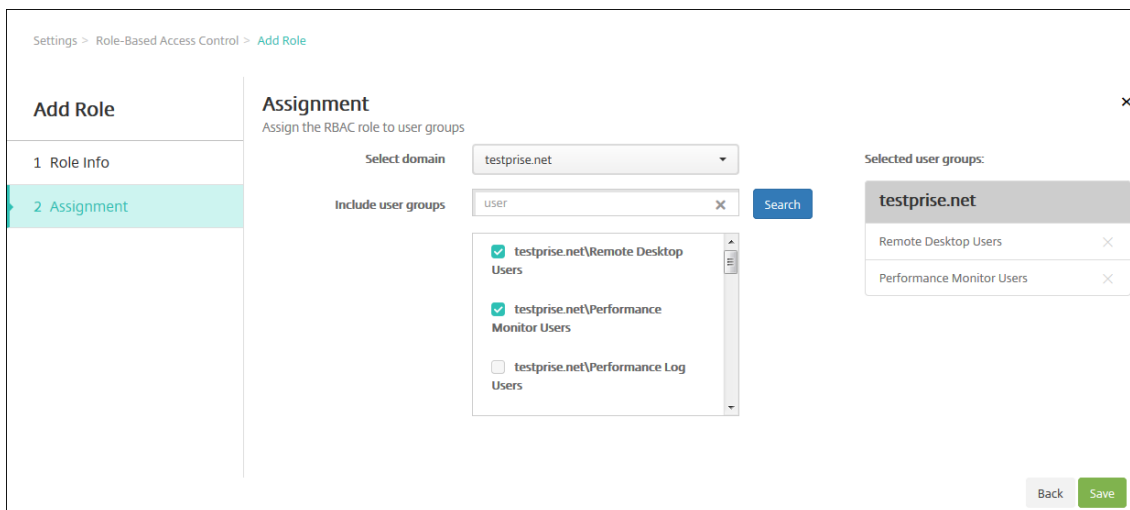


8. To continue to the **Assignment** page, click **Next**.



9. Enter the following information to assign the role to user groups.

- **Select domain:** From the list, select a domain.
- **Include user groups:** Click **Search** to see a list of all available groups. Type a full or partial group name to narrow the search.
- In the list that appears, select the user groups you want to assign the role to. When you select a user group, the group appears in the **Selected user groups** list.



**Tip:**

To remove a user group from the **Selected user groups** list, click the X next to the user group name.

10. Click **Save**.

**Predefined roles**

Each predefined RBAC role has certain associated access and feature permissions. The tables that follow describe each of the permissions for the Admin role and for the User role. You can't delete or edit the predefined roles.

- For a full list of default permissions for each built-in role, download [Role-Based Access Control Defaults](#)
- For information about the Endpoint Management user accounts, see [About user accounts](#).

**Important:**

Under the Settings permission, the RBAC permission gives Admin users full access, including the ability to assign their own permissions. Give this access only to users who you intend to give the ability to manipulate everything in the Endpoint Management system.

**Admin role**

The predefined Admin role provides specific access in Endpoint Management. By default, **Authorized access** (except Self-Help Portal), **Console features**, and **Apply permissions** are enabled.

You can change the role for local users who are assigned the Admin role by using **Manage > Users**. For cloud users who have the Admin role, use the Citrix Cloud console to change the role. By default, cloud and local users with the Admin role have Full access.

## Authorized access for administrators

---

Admin console access	Administrators can access all features on the Endpoint Management console.
Self-Help Portal access	By default, administrators can't access the Self-Help Portal. (Users with the <a href="#">User role</a> can access only the Self-Help portal.)
Remote Support access	Administrators can access the Remote Support feature.
Public API access	Administrators can access the public API to perform actions programmatically that are available on the Endpoint Management console. The actions include administering certificates, apps, devices, delivery groups, and local users.

---

## Console features for administrators

Administrators have unrestricted access to the Endpoint Management console.

---

Dashboard	The <b>Dashboard</b> is the first page that administrators see after logging on to the Endpoint Management console. The <b>Dashboard</b> shows basic information about notifications and devices.
Reporting	The <b>Analyze &gt; Reporting</b> page provides pre-defined reports that let you analyze your app and device deployments.
Devices	The <b>Manage &gt; Devices</b> page is where you manage user devices. You can add individual devices on the page or import a device provisioning file to add multiple devices at one time.

Local Users and Groups	The <b>Manage &gt; Users</b> page is where you can add, edit, or delete local users and local user groups.
Enrollment	The <b>Manage &gt; Enrollment Invitations</b> page is where you manage how users are invited to enroll their devices in Endpoint Management.
Policies	The <b>Configure &gt; Device Policies</b> page is where you manage device policies, such as VPN and network.
App	The <b>Configure &gt; Apps</b> page is where you manage the various apps that users can install on their devices.
Media	The <b>Configure &gt; Media</b> page is where you manage the various media that users can install on their devices.
Action	The <b>Configure &gt; Actions</b> page is where you manage responses to trigger events.
Delivery Group	The <b>Configure &gt; Delivery Groups</b> page is where you manage delivery groups and the resources associated with them.
Enrollment Profile	The <b>Configure &gt; Enrollment Profiles</b> page is where you specify how users can enroll their devices.
Alexa for Business	The <b>Settings</b> page is where you manage your Alexa for Business profiles.
Settings	The <b>Settings</b> page is where you manage system settings, such as client and server properties, certificates, and credential providers. <b>Important:</b> These settings include the RBAC permission. The RBAC permission gives admins full access, including the ability to assign their own permissions. Give this access only to users who you intend to give the ability to manipulate everything in the Endpoint Management system.

---

---

Support	The <b>Troubleshooting and Support</b> page is where you perform troubleshooting activities such as running diagnostics and generating logs.
---------	--

---

### Device restrictions for administrators

Administrators access device features throughout the console by setting device restrictions, setting up and sending notifications to devices, administering apps on the devices, and so on.

---

---

Full Wipe device	Erase all data and apps from a device, including memory cards if the device has one.
Clear Restriction	Remove one or more device restrictions.
Selective Wipe device	Erase all corporate data and apps from a device, leaving personal data and apps in place.
View locations	See the location of and set geographic restrictions on a device. Includes: Locate device, Track device.
Lock device	Remotely lock a device so that users can't use the device.
Unlock device	Remotely unlock a device so that users can use the device.
Lock container	Remotely lock the corporate container on a device.
Unlock container	Remotely unlock the corporate container on a device.
Reset container password	Reset the corporate container password.
Enable ASM/Bypass activation lock	Store a bypass code on a supervised iOS device when Activation Lock is enabled. To erase the device, use this code to clear the Activation Lock automatically.

Get Resident Users	List the users that have active accounts on the current device. This action forces a sync between the device and the Endpoint Management console.
Logout Resident User	Force a log out of the current user.
Delete Resident User	Delete the current session for a specific user. The user can sign in again.
Rings the device	Remotely ring a Windows device at full volume for 5 minutes.
Reboot the device	Restart Windows devices from the Endpoint Management console.
Deploy to device	Send apps, notifications, restrictions, and other resources to a device.
Edit device	Change settings on the device.
Notification to device	Send a notification to a device.
Add/Delete device	Add or remove devices from Endpoint Management.
Devices import	Import a group of devices from a file into Endpoint Management.
Export device table	Collect device information from the Device page and export it to a .csv file.
Revoke device	Prohibit a device from connecting to Endpoint Management.
App lock	Deny access to all apps on a device. On Android, this restriction prevents users from signing in to Endpoint Management. On iOS, users can sign in, but they can't access apps.
App wipe	On Android, this restriction deletes the user's Endpoint Management account. On iOS, this restriction deletes the encryption key required for users to access Endpoint Management features.
View software inventory	See what software is installed on a device.
Request AirPlay mirroring	Request to start AirPlay streaming.

Stop AirPlay mirroring	Stop AirPlay streaming.
Enable lost mode	On the <b>Manage &gt; Devices</b> page, you can put a supervised device in lost mode to block a supervised device on the lock screen. You can then locate the device when the device is lost or stolen.
Disable lost mode	On the <b>Manage &gt; Devices</b> page, you can disable lost mode for a device that is set to lost mode.
OS Update device	You can deploy an OS Update device policy to devices.
Shut down device	Shut down iOS devices from the Endpoint Management console.
Restart device	Restart iOS devices from the Endpoint Management console.
Renew Device Enrollment Certificate	Renew a device CA certificate.

### Local Users and Groups

Administrators manage local users and local user groups on the **Manage > Users** page in Endpoint Management.

Add Local Users
Delete Local Users
Edit Local Users
Import Local Users
Export Local Users
Local User Groups
Get Local User Lock ID
Delete Local User Lock

## Enrollment

Administrators can add and delete enrollment invitations, send notifications to users, and export the enrollment table to a .csv file.

---

Add/Delete enrollment	Add or remove an enrollment invitation to a user or a group of users.
Notify user	Send and enrollment invitation to a user or group of users.
Export enrollment invitation table	Collect enrollment information from the Enrollment page and export it to a .csv file.

---

## Policies

---

Add/Delete policy	Add or remove a device or app policy.
Edit policy	Change a device or app policy.
Upload Policy	Upload a device or app policy.
Clone Policy	Copy a device or app policy.
Disable Policy	Disable an existing app policy.
Export Policy	Collect device policy information from the Device Policies page and export it to a .csv file.
Assign Policy	Assign a device policy to one or more delivery groups.

---

## App

Administrators manage apps on the **Configure > Apps** page in Endpoint Management.

---

Add/Delete app store or enterprise app	Add or remove a public app store app or an enterprise app (not MDX-enabled).
Edit app store or enterprise app	Change a public app store app or an enterprise app (not MDX-enabled).

---



---

Add/Delete MDX, Web, and SaaS app	Add or remove an MDX-enabled app, an app from your internal network (Web app), or an app from a public network (SaaS) to Endpoint Management.
Edit MDX, Web, and SaaS app	Change an MDX-enabled app, an app from your internal network (Web app), or an app from a public network (SaaS) to Endpoint Management.
Add/Delete category	Add or delete a category in which apps can appear in the app store.
Assign public/enterprise app to delivery group	Assign a public app store app or an MDX-enabled app to a delivery group for deployment.
Assign MDX/WebLink/SaaS app to delivery group	Assign to a delivery group an app that is MDX-enabled, doesn't require single sign-on (WebLink), or that's from a public network (SaaS).
Export app table	Collect app information from the App page and export it to a .csv file.

---

## Media

Manage media from a public app store or a volume purchase license.

---

---

Add/Delete app store or enterprise books
Assign public/enterprise books to delivery group
Edit app store or enterprise books

---

## Action

Add/delete action	Add or remove an action defined by a trigger and associated response. A trigger is an event, device or user property, or installed app name.
Edit action	Change an action defined by a trigger and associated response. A trigger is an event, device or user property, or installed app name.
Assign action to delivery group	Assign an action to a delivery group for deployment to user devices.
Export action	Collect action information from the Actions page and export it to a .csv file.

### Delivery group

Administrators manage delivery groups from the **Configure > Delivery Groups** page.

Add/delete delivery group	Create or remove a delivery group, which adds specified users and optional policies, apps, and actions.
Edit delivery group	Change an existing delivery group, which modifies users and optional policies, apps, and actions.
Deploy delivery group	Make the delivery group available for use.
Export delivery group	Collect delivery group information from the Delivery group page and export it to a .csv file.

### Enrollment profile

Manage enrollment profiles.

Add/delete enrollment profile
Edit enrollment profile

---

Assign enrollment profile to delivery group

---

### Alexa for Business

Manage Alexa for Business profiles.

---

---

Add/delete/edit Rooms

Add/delete/edit Room profiles

Add/delete/edit Skill groups

---

### Settings for administrators

Administrators configure various settings on the **Settings** pages.

---

RBAC	RBAC Assignment. <b>Important:</b> This permission gives admins full access, including the ability to assign their own permissions. Give this access only to users who you intend to give the ability to manipulate everything in the Endpoint Management system.
LDAP	Administer one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.
Enrollment	Enable enrollment security modes for users and the Self-Help Portal.
Release Management	View the current installed release. Includes: Release Management Update
Certificates	Edit APNS certificate
Notification Templates	Create notification templates to use in automated actions, enrollment, and standard notification message delivery to users.

Workflows	Manage the creation, approval, and removal of user accounts for use with app configurations.
Credential Providers	Add one or more credential providers authorized to issue device certificates. The credential providers control the certificate format and the conditions for renewing or revoking the certificate.
PKI Entities	Manage public key infrastructure entities (generic, Microsoft Certificate Services, or discretionary CA).
Test PKI Connection	Use the <b>Test Connection</b> button on the <b>Settings &gt; PKI Entities</b> page to make sure that the server is accessible.
Client Properties	Manage various properties on user devices, such as passcode type, strength, and expiration.
Client Support	Set the ways in which users can contact your support services (email, phone, or support ticket email).
Client Branding	Create a custom store name and default store views for the app store. Add a custom logo that appears in the app store or Secure Hub.
Carrier SMS Gateway	Set up carrier SMS gateways to configure notifications that Endpoint Management sends through carrier SMS gateways.
Notification Server	Set up an SMTP gateway server to send email to users.
ActiveSync Gateway	Manage user access to users and devices through rules and properties.
Google Chrome	Configure Endpoint Management to communicate with your Google Workspace account.
Apple Deployment Program	Add an Apple Deployment Program account to Endpoint Management.

Apple Configurator Device Enrollment	Configure Apple Configurator settings in Endpoint Management.
iOS/volume purchase Settings	Add Apple volume purchase accounts.
Mobile Service Provider	Use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and to issue operations.
NetScaler Gateway	Configure NetScaler Gateway (now renamed Citrix Gateway) settings in Endpoint Management.
Network Access Control	Set the conditions that determine a device is noncompliant so that it can't access the network.
Samsung Knox	Enable or disable Endpoint Management to query Samsung Knox attestation server REST APIs.
Server Properties	Add or modify server properties. Requires restarting Endpoint Management on all nodes.
Virtual Apps and Desktops	Allow users to add Citrix Virtual Apps and Desktops through Citrix Workspace.
Citrix Files	When using Endpoint Management with Enterprise accounts: Configure settings to connect to the Content Collaboration and administrator service accounts for user account management. Requires existing Citrix Files domain and administrator credentials. When using Endpoint Management with storage zone connectors: Configure Endpoint Management to point to network shares and SharePoint locations defined in storage zone connectors.
Android Enterprise	Configure Android Enterprise server settings.
Identity Provider (IdP)	Configure an identity provider.
Microsoft Store for Business	Configure Microsoft Store for Business settings in Endpoint Management.

---

Endpoint Management Tools	Access the Endpoint Management Tools page.
Windows Bulk Enrollment	Configure Windows bulk enrollment settings.

---

## Support

Administrators can do various support tasks.

---

---

NetScaler Gateway Connectivity Checks	Perform various connectivity checks for NetScaler Gateway by IP address. Requires a user name and password.
Endpoint Management Connectivity Checks	Do connectivity checks for selected Endpoint Management features, such as database, DNS, and Google Plan.
Citrix Product Documentation	Access the public Citrix Endpoint Management documentation site.
Citrix Knowledge Center	Access the Citrix Support site to search for knowledge base articles.
Logs	View and download log files.
Macros	Populate user or device property data in the text field of a profile, policy, notification, or enrollment template. Configure a single policy, deploy the policy to a large user base, and have user-specific values appear for each targeted user.
PKI Configuration	Import and export PKI configuration information.
APNS Signing Utility	Submit a request for Apple Push Network signing (APNs) certificates, or upload a Secure Mail APNs certificate for iOS.
Citrix Insight Services	Upload logs to Citrix Insight Services (CIS) for assistance with various issues.

---

Device Citrix Gateway connector for Exchange ActiveSync Status	Query Endpoint Management for the status of a device sent to the connector for Exchange ActiveSync. The query is based on the device ActiveSync ID.
--	---

---

### Restrict Group Access

Admin users can apply permissions to all user groups.

### Console features for device provisioning

Device provisioning users have the following restricted access to the Endpoint Management console. By default, each of the following features is enabled.

### Device restrictions

---

---

Edit device	Change settings on the device.
Add/Delete device	Add or remove devices from Endpoint Management.

---

### Settings for device provisioning

Device provisioning users can access the **Settings** page, but do not have the rights to configure the features.

### User role

Users with the User role have the following limited access to Endpoint Management.

### Authorized access for users

Self-Help Portal	Provide users access only to the Self-Help Portal in Endpoint Management.
------------------	---

### Console features for users

Users have the following restricted access to the Endpoint Management console.

### Device restricted access for users

Full Wipe device	Erase all data and apps from a device, including memory cards if the device has one.
Selective Wipe device	Erase all corporate data and apps from a device, leaving personal data and apps in place.
View locations	See the location of and set geographic restrictions on a device. Included: Locate device, See the location of a device, Track device, Track device location over time
Lock device	Remotely lock a device so that it cannot be used.
Unlock device	Remotely unlock a device so that It can be used.
Lock container	Remotely lock the corporate container on a device.
Unlock container	Remotely unlock the corporate container on a device.
Reset container password	Reset the corporate container password.
Enable ASM/Bypass activation lock	Store a bypass code on a supervised iOS device when Activation Lock is enabled. To erase the device, use this code to clear the Activation Lock automatically.



Get Resident Users	List the users that have active accounts on the current device. This action forces a sync between the device and the Endpoint Management console.
Logout Resident User	Force a log out of the current user.
Delete Resident User	Delete the current session for a specific user. The user can sign in again.
Rings the device	Remotely ring a Windows device at full volume for 5 minutes.
Reboot the device	Restart a Windows device.
App lock	Deny access to all apps on a device. On Android, users can't sign in to Endpoint Management. On iOS, users can sign in, but they can't access apps.
App wipe	On Android, this restriction deletes the user's Endpoint Management account. On iOS, this restriction deletes the encryption key required for users to access Endpoint Management features.
View software inventory	See what software is installed on a device.

### Enrollment restrictions for users

---

Add/Delete enrollment	Add or remove an enrollment invitation to a user or a group of users.
Notify user	Send an enrollment invitation to a user or group of users.

### Restrict Group Access for all roles

For the default roles, this permission is set by default and can be applied to all user groups. You can't edit the role.

## Licenses

April 3, 2020

For information about Citrix license usage, see:

- [Monitor license and active usage for cloud services](#)
- [Monitor license and active usage for Endpoint Management](#)

## Device management

October 7, 2021

Citrix Endpoint Management can provision, manage, secure, and inventory a broad range of device types within a single management console.

- Use a common set of device policies to manage supported devices. For a quick look at the device policies available by platform:
  1. Go to the Endpoint Management console and navigate to **Configure > Device Policies**.
  2. Click **Add** and then select the platforms you want to view.

For more information, see [Filter the list of added device policies](#).

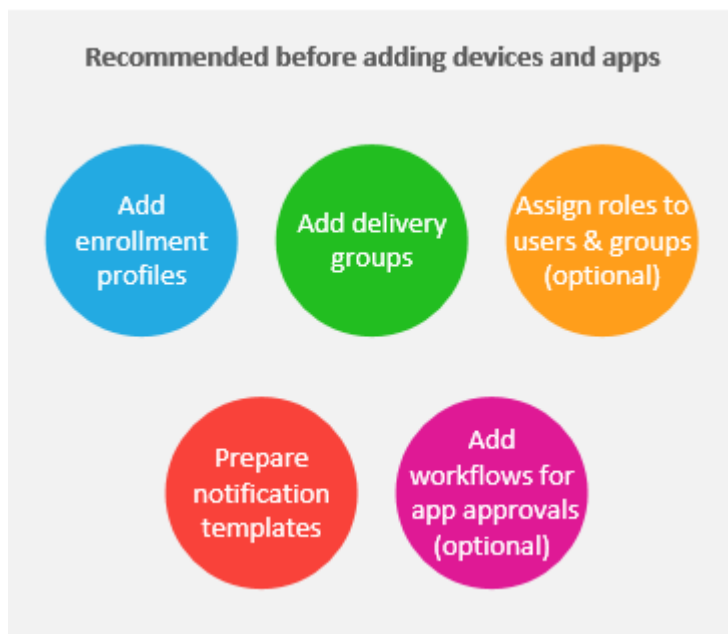
- Protect business information with strict security for identity, corporate-owned and BYO devices, apps, data, and network. Specify the user identities to use to authenticate to devices. Configure how to keep enterprise and personal data separate on devices.
- Deliver any app to end users, regardless of device or operating system. Protect your information at the app level and ensure enterprise-grade mobile application management.
- Use provisioning and configuration controls to set up devices. Those controls include device enrollment, policy application, and access privileges.
- Use security and compliance controls to create a customized security baseline with actionable triggers. For example, lock, wipe, or notify a device in violation of defined compliance standards.
- Use OS update controls to prevent or enforce operating system updates. This feature is critical for data loss prevention against targeted operating system vulnerabilities.

To access articles about each supported platform, expand the “Device management” section in the contents list. Those articles provide details specific to each device platform. The rest of this article describes how to perform general device management tasks.

## Device management workflows

The workflow diagrams in this section provide a suggested sequence for performing device management tasks.

1. **Recommended prerequisites for adding devices and apps:** Performing the following setup in advance lets you configure devices and apps without interruption.



See:

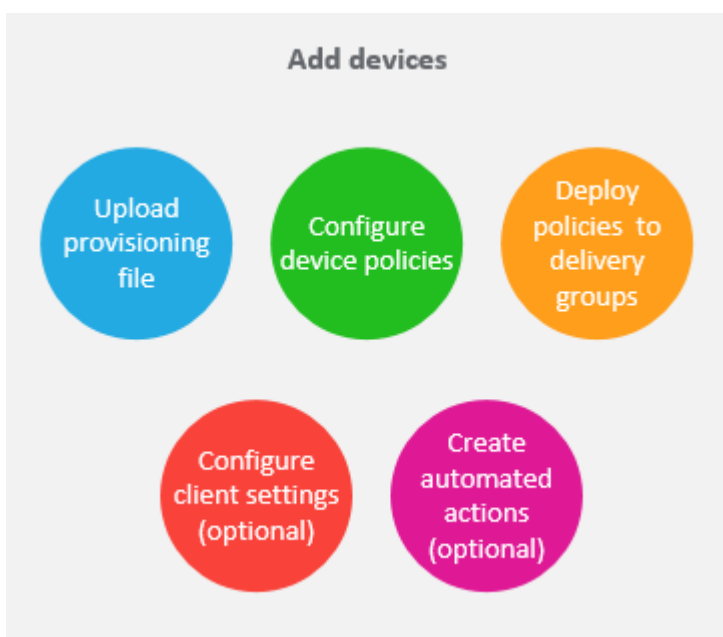
[Deploy resources](#)

[Configure roles with RBAC](#)

[Create and update notification templates](#)

[Create and manage workflows](#)

2. **Add devices:**



See:

[Prepare to enroll devices and deliver resources](#)

[Device policies](#)

[Deploy to delivery groups](#)

[Automated actions](#)

3. **Prepare enrollment invitations:** You can send enrollment invitations to users with iOS, iPadOS, macOS, Android Enterprise, and legacy Android devices. Perform these tasks if you plan to use enrollment invitations.



See:

[Configure enrollment security modes](#)

[Send a notification to devices](#)

4. **Add apps:**



See:

[MAM SDK](#)

[Add apps](#)

[About app categories](#)

[Apply workflows](#)

[Deploy to delivery groups](#)

5. **Perform ongoing device and app management:** In addition to using the Endpoint Management dashboard, we encourage you to review the [What's new](#) content for each release. What's new provides information about any needed actions, such as configuring new device policies.



See:

[Monitor and support](#)

[Reports](#)

[Security actions](#)

[What's new](#)

[Device policies](#)

## Enrollment invitations

To manage user devices remotely and securely, you enroll user devices in Endpoint Management. The Endpoint Management client software is installed on the user device and the user identity is authenticated. Then, Endpoint Management and the user profile are installed. For enrollment details for supported device platforms, see the device articles under this section.

In the Endpoint Management console:

- You can send an enrollment invitation to users with iOS, iPadOS, macOS, Android Enterprise, and legacy Android devices. Enrollment invitations are not available Windows devices.
- You can send an invitation URL to users with iOS, iPadOS, Android Enterprise, or legacy Android devices. If you plan to enroll iPadOS devices by sending an invitation URL to users, see the Citrix support article [CTX261981](#). Invitation URLs are not available for Windows devices.

Enrollment invitations are sent as follows:

- If the enrollment invitation is for one local or Active Directory user: The user receives the invitation from SMS at the phone number and carrier name you specify.
- If the enrollment invitation is for a group: The users receive invitations from SMS. If Active Directory users have an email address and mobile phone number in Active Directory, they receive the invitation. Local users receive the invitation at the email and phone number specified in user properties.

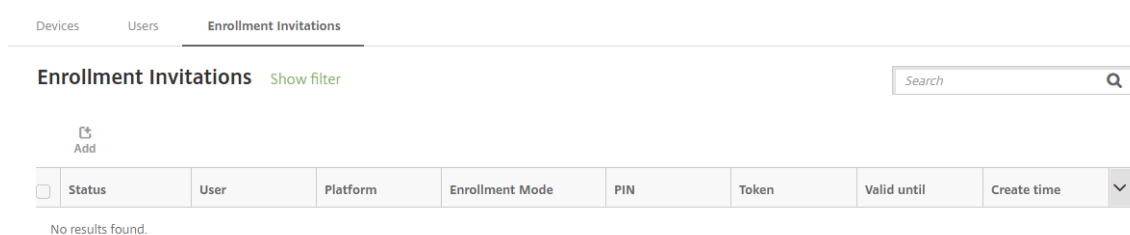
After users enroll, their devices appear as managed on **Manage > Devices**. The status of the invitation URL is shown as **Redeemed**.

### Prerequisites

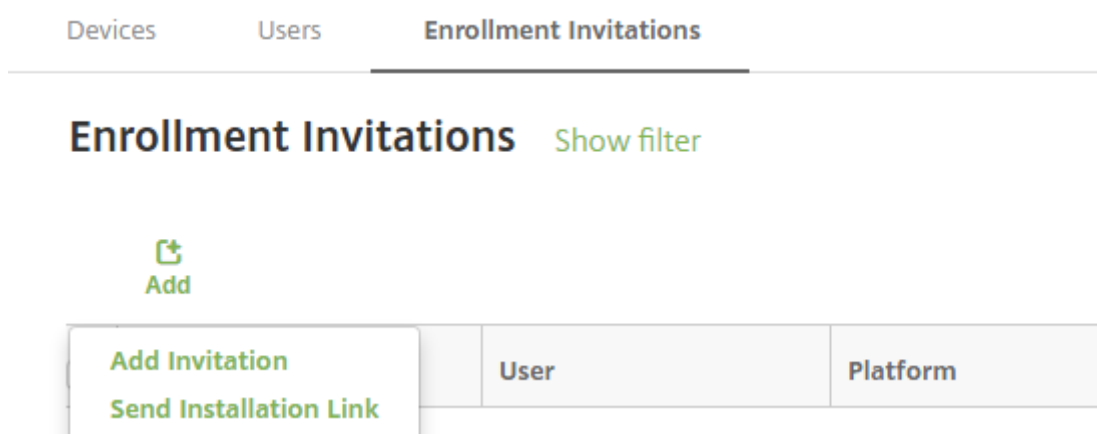
- LDAP configured
- If using local groups and local users:
  - One or more local groups.
  - Local users assigned to local groups.
  - Delivery groups are associated with local groups.
- If using Active Directory:
  - Delivery groups are associated with Active Directory groups.

### Create an enrollment invitation

1. In the Endpoint Management console, click **Manage > Enrollment Invitations**. The **Enrollment Invitations** page appears.



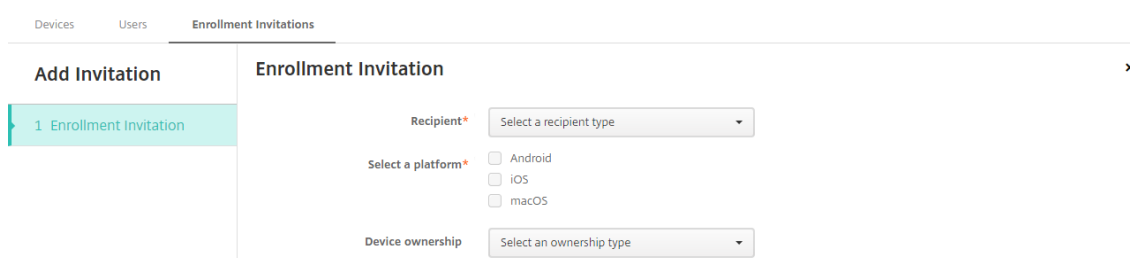
2. Click **Add**. A menu of enrollment options appears.



- To send an enrollment invitation to a user or group, click **Add Invitation**.
- To send an enrollment installation link to a list of recipients over SMTP or SMS, click **Send Installation Link**.

Sending enrollment invitations and installation links are described after these steps.

3. Click **Add Invitation**. The **Enrollment Invitation** screen appears.



4. Configure these settings:

- **Recipient:** Choose **Group** or **User**.
- **Select a platform:** If **Recipient** is **Group**, all platforms are selected. You can change the platform selection. If **Recipient** is **User**, no platforms are selected. Select a platform.  
To create an enrollment invitation for Android Enterprise devices, select **Android**.
- **Device ownership:** Select **Corporate** or **Employee**.

Settings for users or groups appear, as described in the following sections.



## To send an enrollment invitation to a user

The screenshot shows the 'Add Invitation' form in the Citrix Endpoint Management console. The form is titled 'Enrollment Invitation' and is located under the 'Enrollment Invitations' tab. The form includes the following fields and options:

- Recipient\***: A dropdown menu set to 'User'.
- Select a platform\***: Three radio buttons for 'Android', 'iOS', and 'macOS'.
- Device ownership**: A dropdown menu set to 'Select an ownership type'.
- User name\***: A text input field with a help icon (i) to its right.
- Enrollment mode\***: A dropdown menu set to 'User name + Password'.
- Template for agent download**: A dropdown menu set to 'Select a template'.
- Template for enrollment URL**: A dropdown menu set to 'Select a template'.
- Template for enrollment confirmation**: A dropdown menu set to 'Select a template'.
- Expire after**: A text input field set to 'Never'.
- Maximum Attempts**: A text input field set to '0'.
- Send invitation**: A toggle switch set to 'OFF'.

### 1. Configure these **User** settings:

- **User name:** Type a user name. The user must exist in Endpoint Management as a local or Active Directory user. If the user is local, set the email property of the user so you can send that user notifications. If the user is in Active Directory, ensure that LDAP is configured.
- **Phone number:** This setting doesn't appear if you select multiple platforms or if you select only macOS. Optionally, type the phone number of the user.
- **Carrier:** This setting doesn't appear if you select multiple platforms or if you select only macOS. Choose a carrier to associate to the phone number of the user.
- **Enrollment mode:** Choose the enrollment security mode for users. The default is **User name + Password**. Some of the following options aren't available for all platforms:
  - **User name + Password**
  - **High Security**
  - **Invitation URL**
  - **Invitation URL + PIN**
  - **Invitation URL + Password**
  - **Two Factor**
  - **User name + PIN**

We deprecated support for **High Security** enrollment mode. To send enrollment invitations, you can use only **Invitation URL**, **Invitation URL + PIN**, or **Invitation URL + Password** enrollment security modes. For devices enrolling with **User name + Password**, **Two Factor**, or **User name + PIN**, users must download Secure Hub and manually enter their credentials.

For more information, see [Enrollment security modes by platform](#). A PIN for enrollment is also

called a one-time PIN. Such PINs are valid only when the user enrolls.

**Note:**

When you select any enrollment security mode that includes a PIN, the **Template for enrollment PIN** field appears. Click **Enrollment PIN**.

- **Template for agent download:** Choose the download link template named **Download link**. That template is for all supported platforms.
  - **Template for enrollment URL:** Choose **Enrollment Invitation**.
  - **Template for enrollment confirmation:** Choose **Enrollment Confirmation**.
  - **Expire after:** This field is set when you configure the enrollment security mode and indicates when the enrollment expires. For more information about configuring enrollment security modes, see [Configure enrollment security modes](#).
  - **Maximum Attempts:** This field is set when you configure the enrollment security mode and indicates the maximum number of times the enrollment process occurs.
  - **Send invitation:** Select **On** to send the invitation immediately. Select **Off** to add the invitation to the table on the **Enrollment Invitations** page, but not send it.
2. Click **Save and Send** if you enabled **Send invitation**. Otherwise, click **Save**. The invitation appears in the table on the **Enrollment Invitations** page.

<input type="checkbox"/>	Status	User	Platform	Enrollment Mode	PIN	Token	Valid until	Create time
<input type="checkbox"/>	PENDING	[Redacted]	Android	User name + Password		[Redacted]		05/03/2017 10:32:24 am
<input type="checkbox"/>	PENDING	[Redacted]	macOS	User name + Password		[Redacted]		05/01/2017 07:33:38 pm
<input type="checkbox"/>	PENDING	[Redacted]	iOS	User name + Password		[Redacted]		05/01/2017 07:29:02 pm

### To send an enrollment invitation to a group

The following figure shows the settings for configuring an enrollment invitation to a group.

The screenshot shows the 'Add Invitation' form in Citrix Endpoint Management. The form is titled 'Enrollment Invitation' and contains the following fields:

- Recipient\***: Group
- Select a platform\***:  Android,  iOS,  macOS
- Device ownership**: Select an ownership type
- Domain\***: Select a domain
- Group\***: Select a group
- Enrollment mode\***: User name + Password
- Template for agent download**: Select a template
- Template for enrollment URL**: Select a template
- Template for enrollment confirmation**: Select a template
- Expire after**: Never
- Maximum Attempts**: 0
- Send invitation**: OFF

### 1. Configure these settings:

- **Domain:** Choose the domain of the group to receive the invitation.
- **Group:** Choose the group to receive the invitation. Endpoint Management gets the user list from Active Directory. The list includes users whose names contain special characters.
- **Enrollment mode:** Choose how you want users in the group to enroll. The default is **User name + Password**. Some of the following options aren't available for all platforms:
  - **User name + Password**
  - **High Security**
  - **Invitation URL**
  - **Invitation URL + PIN**
  - **Invitation URL + Password**
  - **Two Factor**
  - **User name + PIN**

We deprecated support for **High Security** enrollment mode. To send enrollment invitations, you can use only **Invitation URL**, **Invitation URL + PIN**, or **Invitation URL + Password** enrollment security modes. For devices enrolling with **User name + Password**, **Two Factor**, or **User name + PIN**, users must download Secure Hub and manually enter their credentials.

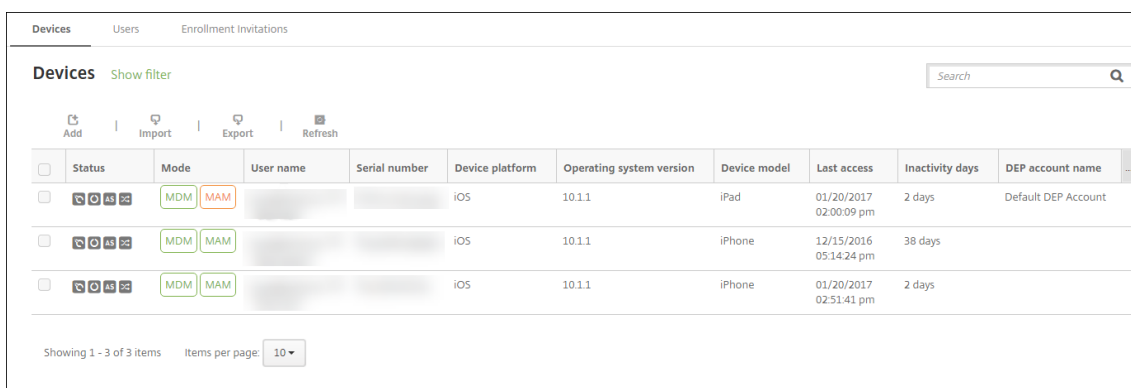
Only the enrollment security modes that are valid for each of the selected platforms appear. For more information, see [Enrollment security modes by platform](#).

#### Note:

When you select any enrollment security mode that includes a PIN, the **Template for en-**

**rollment PIN** field appears. Click **Enrollment PIN**.

- **Template for agent download:** Choose the download link template named **Download link**. That template is for all supported platforms.
  - **Template for enrollment URL:** Choose **Enrollment Invitation**.
  - **Template for enrollment confirmation:** Choose **Enrollment Confirmation**.
  - **Expire after:** This field is set when you configure the enrollment security mode and indicates when the enrollment expires. For more information about configuring enrollment security modes, see [Configure enrollment security modes](#).
  - **Maximum Attempts:** This field is set when you configure the enrollment security mode and indicates the maximum number of times the enrollment process occurs.
  - **Send invitation:** Select **On** to send the invitation immediately. Select **Off** to add the invitation to the table on the **Enrollment Invitations** page, but not send it.
2. Click **Save and Send** if you enabled **Send invitation**. Otherwise, click **Save**. The invitation appears in the table on the **Enrollment Invitation** page.



The screenshot shows the 'Devices' page in Citrix Endpoint Management. It features a search bar, a 'Show filter' link, and a table of devices. The table has columns for Status, Mode, User name, Serial number, Device platform, Operating system version, Device model, Last access, Inactivity days, and DEP account name. There are three rows of device data.

Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP account name
	MDM MAM	[Redacted]	[Redacted]	iOS	10.1.1	iPad	01/20/2017 02:00:09 pm	2 days	Default DEP Account
	MDM MAM	[Redacted]	[Redacted]	iOS	10.1.1	iPhone	12/15/2016 05:14:24 pm	38 days	
	MDM MAM	[Redacted]	[Redacted]	iOS	10.1.1	iPhone	01/20/2017 02:51:41 pm	2 days	

Showing 1 - 3 of 3 items    Items per page: 10

### To send an installation link

Before you can send an enrollment installation link, you must configure channels (SMTP or SMS) on the notification server from the **Settings** page. For details, see [Notifications](#)

Devices Users **Enrollment Invitations**

**Send Link**

1 Details

**Send Installation Link**

Recipients\*

Email*	Phone number*	Add
		+

Channels ⓘ

**SMTP** ⚠ Channel cannot be activated until you define the SMTP server in the [Notification Server](#) section in Settings.

Sender

Subject

Message

**SMS** ⚠ Channel cannot be activated until you define the SMS server in the [Notification Server](#) section in Settings.

Message

1. Configure these settings and then click **Save**.

- **Recipient:** For each recipient that you want to add, click **Add** and then do the following:
  - **Email:** Type the email address of the recipient. This field is required.
  - **Phone number:** Type the phone number of the recipient. This field is required.

**Note:**

To delete a recipient, hover over the line containing the listing and then click the trash icon on the right side. A confirmation dialog box appears. Click **Delete** to delete the listing or click **Cancel** to keep the listing.

To edit a recipient, hover over the line containing the listing. Then, click the pen icon on the right side. Update the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

- **Channels:** Select a channel to use for sending the enrollment installation link. You can send notifications over **SMTP** or **SMS**. These channels cannot be activated until you configure the server settings on the **Settings** page in **Notification Server**. For details, see [Notifications](#).
- **SMTP:** Configure these optional settings. If you do not type anything in these fields, the default values specified in the notification template configured for the platform you selected are used:
  - **Sender:** Type an optional sender.
  - **Subject:** Type an optional subject for the message. For example, “Enroll your device.”
  - **Message:** Type an optional message to be sent to the recipient. For example, “Enroll your device to gain access to organizational apps and email.”

- **SMS:** Configure this setting. If you do not type anything in this field, the default value specified in the notification template configured for the platform you selected is used:

- **Message:** Type a message to be sent to the recipients. This field is required for SMS-based notification.

In North America, SMS messages that exceed 160 characters are delivered in multiple messages.

2. Click **Send**.

**Note:**

If your environment uses sAMAccountName: After users receive the invitation and click the link, they must edit the user name to complete the authentication. The user name appears in the form of sAMAccountName@domainname.com. Users must remove the @domainname.com portion.

### **Enrollment security modes by platform**

The following table displays security modes that you can use to enroll user devices. In the table, **Yes** indicates which device platforms support specific enrollment and management modes with different enrollment profiles.

	MDM enrollment security mode	MAM enrollment security mode	Citrix Gateway Management modes	Support different enrollment profiles	Android (legacy)	Android Enterprise	iOS (user enrollment mode)	iOS	macOS	Windows
Azure AD and Okta as identity provider through Citrix Cloud	Client certificate	MDM+MAM or MDM	Yes	Yes	Yes	Yes	Yes	Yes	No	No
User name + Password	LDAP, LDAP + client certificate, and client certificate only	MDM+MAM or MDM, (MAM-only mode doesn't support client certificates on Citrix Gateway)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

	MAM enrollment security mode	Citrix Gateway	Management modes	Support different enrollment profiles	Android (legacy)	Android Enterprise	iOS (user enrollment mode)	iOS	macOS	Windows
MDM enrollment security mode	Client certificate	MDM+MAM or MDM	Yes	Yes	Yes	No	Yes	No	No	
Invitation URL	Client certificate	MDM+MAM or MDM	Yes	Yes	Yes	No	Yes	No	No	
Invitation URL + PIN	Client certificate	MDM+MAM or MDM	Yes	Yes	Yes	No	Yes	No	No	
Invitation URL + Password	LDAP, LDAP + client certificate, and client certificate only	MDM+MAM or MDM	Yes	Yes	Yes	No	Yes	No	No	
Two-factor authentication (user name + password + PIN)	LDAP, LDAP + client certificate, and client certificate only	MDM+MAM or MDM	Yes	Yes	Yes	No	Yes	Yes	No	



	MAM								
	enroll- ment								
	secu- rity		Support						
MDM	mode		differ- ent				iOS		
enroll- ment	on		enroll- ment				(user enroll- ment		
secu- rity	Citrix		Android		Android		Android		
mode	Gate- way	Managem- ent	pro- files	Android	Enter- prise		mode)	iOS	macOS Windows
User name + PIN	Client certifi- cate	MDM+M, or MDM	Yes	Yes	Yes	No	Yes	Yes	No

The following describes how the enrollment security modes behave on iOS, Android, and Android Enterprise devices:

- **User name + Password** (default)
  - Sends a user a single notification that contains an enrollment URL. When the user clicks the URL, Secure Hub opens. The user then types a user name and password to enroll the device in Endpoint Management.
- **Invitation URL**
  - Sends a user a single notification that contains an enrollment URL. When the user clicks the URL, Secure Hub opens. The Endpoint Management server name and the **Yes, Enroll** button appear. The user taps **Yes, Enroll** to enroll the device in Endpoint Management.
- **Invitation URL + PIN**
  - Sends a user the following emails:
    - \* An email with an enrollment URL, which lets the user enroll the device in Endpoint Management through Secure Hub.
    - \* An email with a one-time PIN that the user must type when enrolling the device, along with the user’s Active Directory (or local) password.
  - With this mode, the user enrolls only by using the enrollment URL in the notification. If the user loses the notification invitation, the user cannot enroll. However, you can send another invitation.
- **Invitation URL + Password**
  - Sends a user a single notification that contains an enrollment URL. When the user clicks the URL, Secure Hub opens. The Endpoint Management server name appears, along with a field that lets the user type a password.
- **Two Factor**

- Sends a user a single notification that contains an enrollment URL and a one-time PIN. When the user clicks the URL, Secure Hub opens. The Endpoint Management server name appears, along with two fields that let the user type a password and the PIN number.
- **User name + PIN**
  - Sends a user the following emails:
    - \* An email with an enrollment URL, which lets the user download and install Secure Hub. After Secure Hub opens, the user is prompted to type a user name and password to enroll the device in Endpoint Management.
    - \* An email with a one-time PIN that the user must type when enrolling the device, along with the user's Active Directory (or local) password.
  - If the user loses the notification invitation, the user cannot enroll. However, you can send another invitation.

The following describes how the enrollment security modes behave on macOS devices:

- **User name + Password**
  - Sends a user a single notification that contains an enrollment URL. When the user clicks the URL, the Safari browser opens. A sign-in page appears, prompting the user to type a user name and password to enroll the device in Endpoint Management.
- **Two Factor**
  - Sends a user a single notification that contains an enrollment URL and a one-time PIN. When the user clicks the URL, the Safari browser opens. A sign-in page appears, displaying two fields that let the user type a password and the PIN number.
- **User name + PIN**
  - Sends a user the following emails:
    - \* An email with an enrollment URL. When the user clicks the URL, the Safari browser opens. A sign-in page appears, prompting the user to type a user name and password to enroll the device in Endpoint Management.
    - \* An email with a one-time PIN that the user must type when enrolling the device, along with the user's Active Directory (or local) password.
  - If the user loses the notification invitation, the user cannot enroll. However, you can send another invitation.

You cannot send enrollment invitations to Windows devices. Windows users enroll directly through their devices. For information about enrolling Windows devices, see [Windows devices](#).

## Security actions

You perform device and app security actions from the **Manage > Devices** page. Device actions include revoke, lock, unlock, and wipe. App security actions include app lock and app wipe.

- **Activation Lock Bypass:** Removes the Activation Lock from supervised iOS devices before de-

vice activation. This command doesn't require the personal Apple ID or password for a user.

- **App lock:** Denies access to all apps on a device. On Android, after an app lock, users can't sign in to Endpoint Management. On iOS, users can sign in, but they can't access any apps.
- **App wipe:** Removes the user account from Secure Hub and unenrolls the device. Users can't reenroll until you perform the **App unwipe** action.
- **ASM Deployment Program Activation Lock:** Creates an Activation Lock bypass code for iOS devices enrolled in Apple School Manager.
- **Certificate renewal:** For supported iOS, macOS, and Android devices, the Certificate Renewal security action initiates certificate renewal. The next time that devices connect back to Endpoint Management, the Endpoint Management server issues new device certificates based on the new certificate authority.
- **Clear restrictions:** On supervised iOS devices, this command allows Endpoint Management to clear the restrictions password and restrictions settings configured by the user.
- **Enable/disable Lost Mode:** Puts a supervised iOS device in Lost Mode and sends the device a message, phone number, and footnote to display. The second time that you send this command takes the device out of Lost Mode.
- **Enable tracking:** On Android or iOS devices, this command allows Endpoint Management to poll the location of specific devices at a frequency you define. To view device coordinates and location on a map, go to **Manage > Devices**, select a device, and then click **Edit**. The device info is on the **General** tab under **Security**. Use **Enable tracking** to track the device continuously. Secure Hub reports the location periodically when the device is running.
- **Full wipe:** Immediately erases all data and apps from a device, including from any memory cards. Wiped devices remain in the device list on the **Manage > Devices** page for auditing purposes. You can remove a wiped device from the device list.
  - For Android devices, this request can also include the option to wipe memory cards.
  - For Android Enterprise fully managed devices with a work profile (COPE devices), you can perform a full wipe after a selective wipe removes the work profile.
  - For iOS, macOS, and tvOS devices, the wipe occurs immediately, even if the device is locked.

For iOS 11 devices and iPadOS 12 devices (minimum version): When you confirm the full wipe, you can choose to preserve the cellular data plan on the device.

For iOS 11.3 devices (minimum version): When you confirm the full wipe, you can prevent iOS devices from performing proximity setup. When setting up a new iOS device, users can normally use an already configured iOS device to set up their own. You can block proximity setup on devices that are Endpoint Management managed and have been wiped.

- For Windows Phone devices, a full wipe removes all Endpoint Management information and all user data. The user data removed includes personal content such as apps, emails, contacts, and media.
- If the device user turns off the device before the memory card content is deleted, the user might still have access to device data.
- You can cancel the wipe request until the request is sent to the device.
- **Locate:** Locates a device and reports the device location, including a map, on the **Manage > Devices** page, under **Device details > General**. Locate is a one-time action. Use **Locate** to display the current device location at the time you perform the action. To continuously track the device over a period, use **Enable tracking**.
  - When applying this action to Android (except for Android Enterprise) devices or to Android Enterprise (corporate-owned or BYOD) devices, be aware of the following behavior:
    - \* **Locate** requires the user to grant location permission during enrollment. The user can choose not to grant location permission. If the user doesn't grant the permission during enrollment, Endpoint Management again requests location permission when sending the **Locate** command.
  - When applying this feature to iOS or Android Enterprise devices, be aware of the following limitations:
    - \* For Android Enterprise devices, this request fails unless the [Location device policy](#) has set the location mode for the device to **High Accuracy** or **Battery Saving**.
    - \* For iOS devices, the command succeeds only if the devices are in MDM Lost Mode.
- **Lock:** Remotely locks a device. The lock is useful when a user loses a device and you want to lock it in case it's stolen. Endpoint Management then generates a PIN code and sets it in the device. To access the device, the user types the PIN code. Use **Cancel Lock** to remove the lock from the Endpoint Management console.
- **Lock and Reset Password:** Remotely locks a device and resets the passcode.
  - Not supported for devices that are:
    - \* enrolled in Android Enterprise in work profile mode and
    - \* running Android versions earlier than Android 7.0
  - On devices enrolled in Android Enterprise in work profile mode and that are running Android 7.0 or greater:
    - \* The passcode sent locks the work profile. The device is not locked.
    - \* If a passcode isn't sent, or the passcode sent doesn't meet requirements and the work profile doesn't have a passcode: The device is locked.
    - \* If a passcode isn't sent, or the passcode sent doesn't meet requirements, but the work profile has a passcode: The work profile is locked but the device isn't locked.
- **Notify (Ring):** Plays a sound on Android devices.

- **Reboot:** Restarts Windows 10 and Windows 11 devices. For Windows Tablet and PCs, a message about the pending reboot appears. The reboot occurs in five minutes. For Windows Phone, the reboot occurs after a few minutes, with no warning message to users.
- **Request/Stop AirPlay Mirroring:** Starts and stops AirPlay mirroring on supervised iOS devices.
- **Restart/Shut Down:** Immediately restarts or shuts down supervised devices. tvOS supports Restart but not Shut Down.
- **Revoke:** Prohibits a device from connecting to Endpoint Management.
- **Revoke/Authorize:** Performs the same actions as a Selective Wipe. After revocation, you can reauthorize the device to reenroll it.
- **Ring:** If the device is in Lost Mode, Ring plays a sound on a supervised iOS device. The sound plays until you removed the device from Lost Mode or the user disables the sound.
- **Rotate personal recovery key:** If you have enabled the FileVault device policy, this action generates a new personal recovery key and replaces the old key with this new key. You can cancel this request while the request is still pending. To do so, click **Cancel Rotate personal recovery key**.
- **Selective wipe:** Erases all corporate data and apps from a device, leaving personal data and apps in place. After a selective wipe, use the **Authorize** action to reauthorize the device so a user can reenroll it. Wiped devices remain in the device list on the **Manage > Devices** page for auditing purposes. You can remove a wiped device from the device list.
  - Selectively wiping an Android device does not disconnect the device from Device Manager and the corporate network. To prevent the device from accessing Device Manager, you must also revoke the device certificates.
  - Selectively wiping an Android device also revokes the device. You can reenroll the device only after reauthorizing it or deleting it from the console.
  - For Android Enterprise fully managed devices with a work profile (COPE devices), you can perform a full wipe after a selective wipe removes the work profile. Or, you can re-enroll the device with the same user name. Re-enrolling the device recreates the work profile.
  - If the Samsung Knox API is enabled, selectively wiping the device also removes the Samsung Knox container.
  - For iOS and macOS devices, this command removes any profile installed through MDM.
  - A selective wipe on a Windows device also removes the contents of the profile folder for any currently signed on user. A selective wipe doesn't remove any web clips that you deliver to users through a configuration. To remove web clips, users manually unenroll their devices. You can't reenroll a selectively wiped device.
  - Selectively wiping a Windows Phone device removes the enterprise token that allows Endpoint Management to install apps on the device. The wipe also removes all Endpoint Man-

agement certificates and configurations deployed to the device. You can't reenroll a selectively wiped Windows Phone device.

- **Unlock:** Clears the passcode sent to the device when it was locked. This command doesn't unlock the device.

In **Manage > Devices**, the **Device details** page also lists device Security properties. Those properties include Strong ID, Lock Device, Activation Lock Bypass, and other information for the platform type. The **Full Wipe of Device** field includes the user PIN code. The user must enter that code after the device is wiped. If the user forgets the code, you can look it up here.

You can automate some actions. For more information, see [Automated actions](#).

## Remove a device from the Endpoint Management console

### Important:

When you remove a device from the Endpoint Management console, managed apps and data remain on the device. To remove managed apps and data from the device, see "Delete a device" later in this article.

To remove a device from the Endpoint Management console, go to **Manage > Devices**, select a managed device, and then click **Delete**.

Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version
	MDM   MAM			Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0

## Selectively wipe a device

1. Go to **Manage > Devices**, select a managed device, and then click **Secure**.
2. In **Security Actions**, click **Selective wipe**.
3. For Android devices only, disconnect the device from the corporate network: After the device is wiped, in **Security Actions**, click **Revoke**.

To withdraw a selective wipe request before the wipe occurs, in **Security Actions**, click **Cancel selective wipe**.

## Delete a device

This procedure removes managed apps and data from the device and deletes the device from the Devices list in the Endpoint Management console. You can use the Endpoint Management Public REST API to delete devices in bulk.

1. Go to **Manage > Devices**, select a managed device, and then click **Secure**.
2. Click **Selective Wipe**. When prompted, click **Perform Selective Wipe**.
3. To verify that the wipe command succeeded, refresh **Manage > Devices**. In the **Mode** column, the amber color for MDM and MAM indicates that the wipe command succeeded.

Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version
	MDM MAM			Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0

4. On **Manage > Devices**, select the device, and then click **Delete**. When prompted, click **Delete** again.

### Lock, unlock, wipe, or unwipe apps

1. Go to **Manage > Devices**, select a managed device, and then click **Secure**.
2. In **Security Actions**, click the app action.

You can also use the **Security Actions** box to check the device status for a user whose account is disabled or deleted from Active Directory. The presence of the App Unlock or App Unwipe actions indicate apps that are locked or wiped.

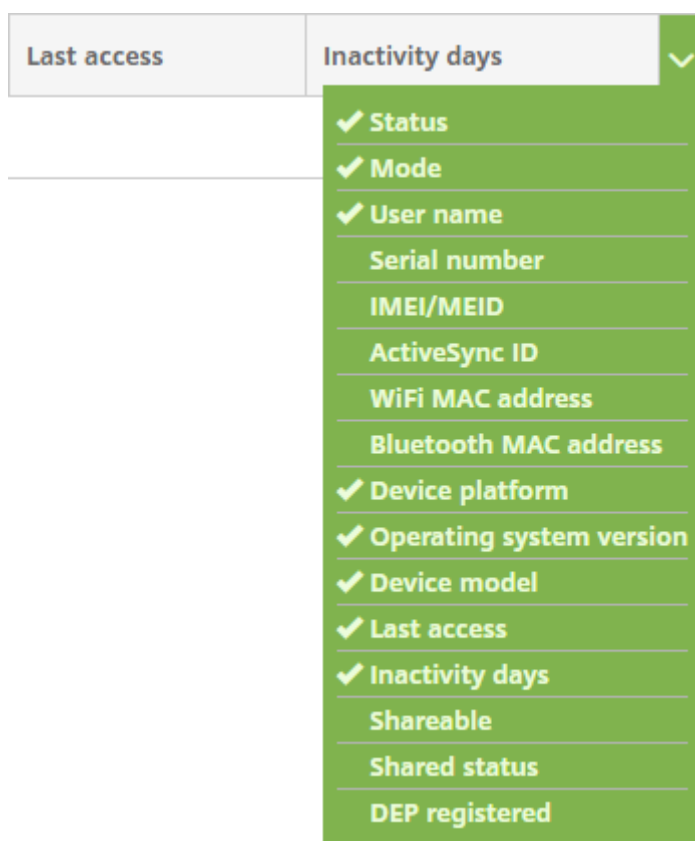
### Get information about devices

The Endpoint Management database stores a list of mobile devices. To populate the Endpoint Management console with your devices, you can add the devices manually or you can import a list of devices from a file. For more information about device provisioning file formats, see Device provisioning file formats later in this article.

The **Manage > Devices** page in the Endpoint Management console lists each device and the following information:

- **Status:** Icons indicate whether the device is jailbroken, is managed, whether ActiveSync Gateway is available, and the deployment state.
- **Mode:** Indicates the device mode, such as MDM or MDM+MAM.
- Other information about the device, such as **User name**, **Device platform**, **Last access**, and **Inactivity days**. Those headings are the defaults shown.

To customize the **Devices** table, click the down arrow on the last heading. Then, select the additional headings you want to see in the table or clear any headings to remove them.



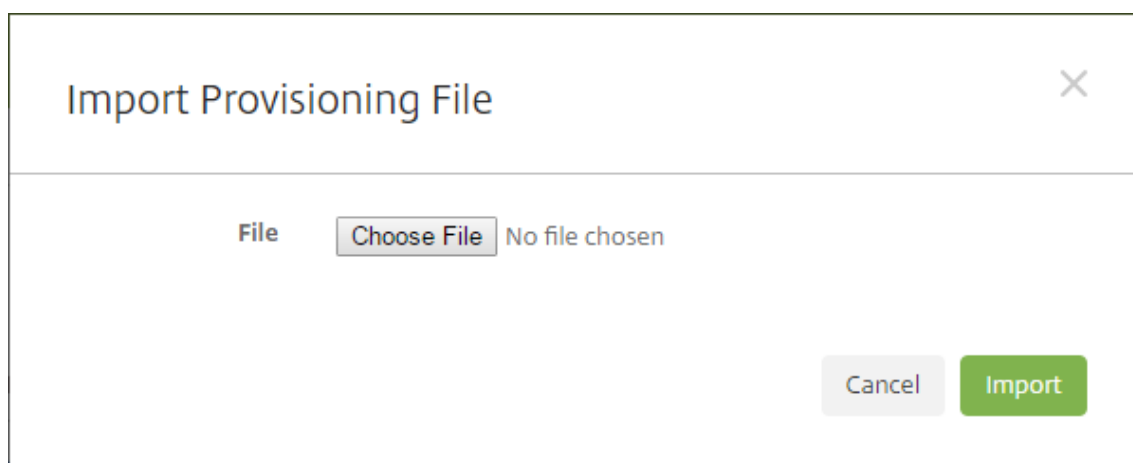
You can add devices manually, import devices from a device provisioning file, edit device details, customize the Active Directory user properties, perform security actions, and send notifications to devices. You can also export all device table data to a .csv file to create a custom report. The server exports all device attributes. If you apply filters, Endpoint Management uses the filters when creating the .csv file.

### Import devices from a provisioning file

You can import a file supplied by mobile operators or device manufacturers, or you can create your own device provisioning file. For details, see Device provisioning file formats later in this article.

1. Go to **Manage > Devices** and then click **Import**. The **Import Provisioning File** dialog box appears.

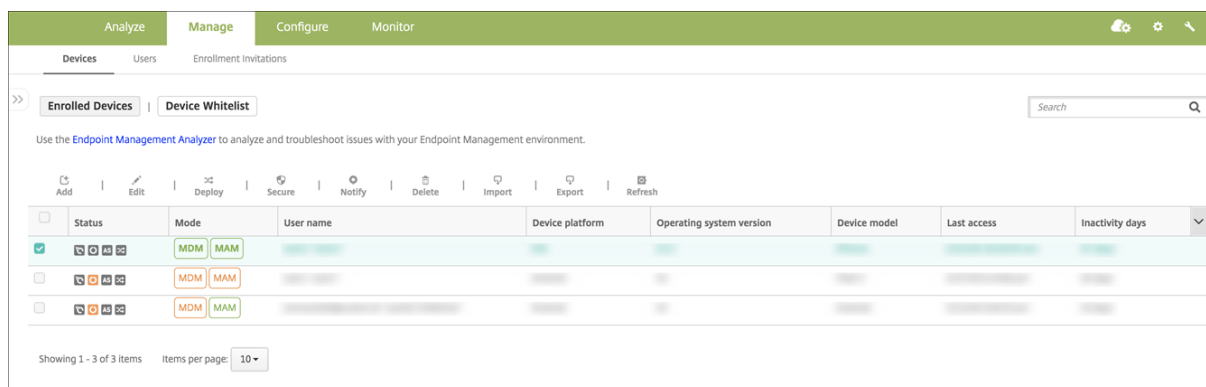




2. Click **Choose File** and then navigate to the file you want to import.
3. Click **Import**. The **Devices** table lists the imported file.
4. To edit the device information, select it and then click **Edit**. For information about the **Device details** pages, see Get information about devices.

## Deploy to a device

You can force one or several devices to connect with Endpoint Management. The selected devices immediately receive resources without waiting for the next scheduled check-in.



1. Go to **Manage > Devices**, select an MDM or MDM+MAM managed device, and then click **Deploy**.
2. In the dialog box, click **Deploy** to confirm your action.

## Send a notification to devices

You can send notifications to devices from the Devices page. For more information about notifications, see [Notifications](#).

1. On the **Manage > Devices** page, elect the device or devices to which you want to send a notification.

2. Click **Notify**. The **Notification** dialog box appears. The **Recipients** field lists all devices to receive the notification.

The screenshot shows a 'Notification' dialog box with the following fields and options:

- Recipients:** CMVVXKX06J6A
- Templates:** Ad Hoc
- Channels:**  SMTP  SMS
- SMTP Tab:**
  - Sender:** [Empty text box]
  - Subject:** [Empty text box]
  - Message:** [Empty text area]
- Buttons:** Cancel, Notify

3. Configure these settings:

- **Templates:** In the list, click the type of notification you want to send. For each template except for **Ad Hoc**, the **Subject** and **Message** fields show the text configured for the template that you choose.
- **Channels:** Select how to send the message. The default is **SMTP** and **SMS**. Click the tabs to see the message format for each channel.
- **Sender:** Enter an optional sender.
- **Subject:** Enter a subject for an **Ad Hoc** message.
- **Message:** Enter the message for an **Ad Hoc** message.

4. Click **Notify**.

## Export the Devices table

1. Filter the **Devices** table according to what you want to appear in the export file.
2. Click the **Export** button above the **Devices** table. Endpoint Management extracts the information in the filtered **Devices** table and converts it to a .csv file.
3. When prompted, open or save the .csv file.

## Tag user devices manually

You can manually tag a device in Endpoint Management in the following ways:

- During the invitation-based enrollment process.
- During the Self-Help Portal enrollment process.
- By adding device ownership as a device property

You have the option of tagging the device as either corporate- or employee-owned. When using the Self-Help Portal to self-enroll a device, you can tag the device as corporate- or employee-owned. You can also tag a device manually, as follows.

1. Add a property to the device from the **Devices** tab in the Endpoint Management console.
2. Add the property named **Owned by** and choose either **Corporate** or **BYOD** (employee-owned).

The screenshot shows the 'Device details' page for an iPhone. The 'Properties' section is active, showing several expandable categories: Battery, Location information, Network information, Security information, Storage space, and System information. The 'System information' section is expanded, showing the 'Owned by' property set to 'Corporate' (selected with a radio button). Other properties include Active iTunes account (Yes), Baseband firmware version (2.16.00), Cloud backup enabled (No), Color (BLACK), DEP account name (DEP), and DEP profile assigned (01/08/2017 06:47:15).

## Customize Active Directory user attributes

You can customize certain Active Directory user attributes to define which attributes Endpoint Management can access to create a user account.

To view the list of attributes, add the `optional.user.identity.attributes` server property as a custom key in **Settings > Server Properties**. In the **Values** field, you can remove and later restore the optional Active Directory user attributes that Endpoint Management provides by default. For more information, see [Server properties](#).

After you edit the list of default values and save the changes, you can view the updated Active Directory user attributes in **Manage > Devices > User properties**. Endpoint Management updates the console after the user signs in to the device or during the next scheduled device check-in. If you make a spelling error or add a value that's not supported, Endpoint Management ignores your changes.

Removing the optional Active Directory user attributes can affect the following functionality:

- **Provisioning of the user account:** If you remove the first and last name values, Endpoint Management can't provision the user account for Citrix Content Collaboration and Salesforce.
- **Enrollment invitations:** If you remove the user's email or mobile phone details, the user can't receive an enrollment invitation.
- **Device notification actions:** If you remove the user's email details, the user can't receive the notifications through SMTP.
- **Single sign-on to Secure Mail:** If you remove the display name value, the user can't sign in to Secure Mail using single sign-on.
- **User property and deployment rules:** If you remove any of the optional attributes that you use to configure the user property and deployment rules, you can affect existing configurations.
- **Actions:** If you remove any of the optional attributes that you use to set an automated action in **Configure > Actions**, you can affect existing configurations.
- **Custom reports:** If you remove any of the optional attributes that you use in custom reports, you can affect existing configurations.

## Search for devices

For fast searching, the default search scope includes the following device properties:

- Serial Number
- IMEI
- Wi-Fi MAC address
- Bluetooth MAC address
- Active Sync ID
- User Name

You can configure the search scope through a server property, **include.device.properties.during.search**, which defaults to **false**. To include all device properties in a device search, go to **Settings > Server Properties** and change the setting to **true**.

## Device provisioning file formats

Many mobile operators or device manufacturers provide lists of authorized mobile devices. You can use these lists to avoid having to enter a long list of mobile devices manually. Endpoint Management supports an import file format that is common to these supported device types: Android, iOS, and Windows.

A provisioning file that you create manually must be in the following format:

```
SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;
propertyName2;propertyValue2; ... propertyNameN;propertyValueN
```

Keep in mind the following:

- For valid values for each property, see the PDF [Device property names and values](#).
- Use the UTF-8 character set.
- Use a semi-colon (;) to separate the fields within the provisioning file. If part of a field contains a semi-colon, escape it with a backslash character (\).

For example, for this property:

```
propertyV;test;1;2
```

Escape it as follows:

```
propertyV\;test\;1\;2
```

- The serial number is required for iOS devices because the serial number is the iOS device identifier.
- For other device platforms, you must include either the serial number or the IMEI.
- Valid values for **OperatingSystemFamily** are **WINDOWS**, **ANDROID**, or **iOS**.

Example of a device provisioning file:

```
1 `1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyName;
   propertyV\;test\;1\;2;prop 2
2 2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyName;
   propertyV$*&&ééétest
3 3050BF3F517301081610065510590393;35244201625379903;iOS;test;
4 4050BF3F517301081610065510590393;;iOS;test;
5 ;55244201625379903;ANDROID;test.testé;value;`
```

Each line in the file describes a device. The first entry in that sample means the following:

- SerialNumber: 1050BF3F517301081610065510590391
- IMEI: 15244201625379901
- OperatingSystemFamily: WINDOWS

- PropertyName: `propertyN`
- PropertyValue: `propertyV\;test\;1\;2;prop 2`

## Shared devices

Endpoint Management lets you configure devices that multiple users can share. The shared devices feature lets, for example, clinicians in hospitals use any nearby device to access apps and data rather than having to carry around a specific device. You might also want shift workers in fields like law enforcement, retail, and manufacturing to share devices to reduce equipment costs.

### Key points about shared devices

You can use any of the supported iOS and Android devices as shared devices. For a list of supported devices, see [Supported device operating systems](#).

### MDM enrollment

- Available on both iOS and Android tablets and phones. Basic Apple Deployment Program enrollment is not supported for an Endpoint Management Enterprise shared device. Use an authorized Apple Deployment Program to enroll a shared device in this mode.
- Authentication types not supported: Client certificate authentication, Citrix PIN, Touch ID, User Entropy, and two-factor authentication.

### MDM+MAM enrollment

- Available only on iOS and Android tablets.
- Only Active Directory user name and password authentication is supported.
- Doesn't support client certificate authentication, passcode for Secure Hub, Touch ID, User Entropy, and two-factor authentication.
- MAM-only enrollment is not supported. The devices must enroll in MDM.
- Only Secure Mail, Secure Web, and the Citrix Files mobile app are supported. HDX apps are not supported.
- Active Directory users are the only supported users. Local users and groups are not supported.
- Re-enrollment is required for existing MDM-only shared devices to update to MDM+MAM.
- Users cannot share native apps on the devices.
- Once downloaded during first-time enrollment, Citrix mobile productivity apps are not downloaded again each time a new user signs in to the device. The new user can pick up the device, sign on, and get going.
- On Android, to isolate each user's data for security purposes, enable the **Disallow rooted devices** policy in the Endpoint Management console.

### Prerequisites for enrolling shared devices

Before you can enroll shared devices, you must do the following:

- Create a shared device enrollment user role. See [Configure roles with RBAC](#).
- Create a shared device user. See [Add, edit, unlock, or delete local user accounts](#).
- Create a delivery group that contains the base policies, apps, and actions that you want applied to the shared device enrollment user. See [Deploy resources](#).

### Prerequisites for MDM+MAM

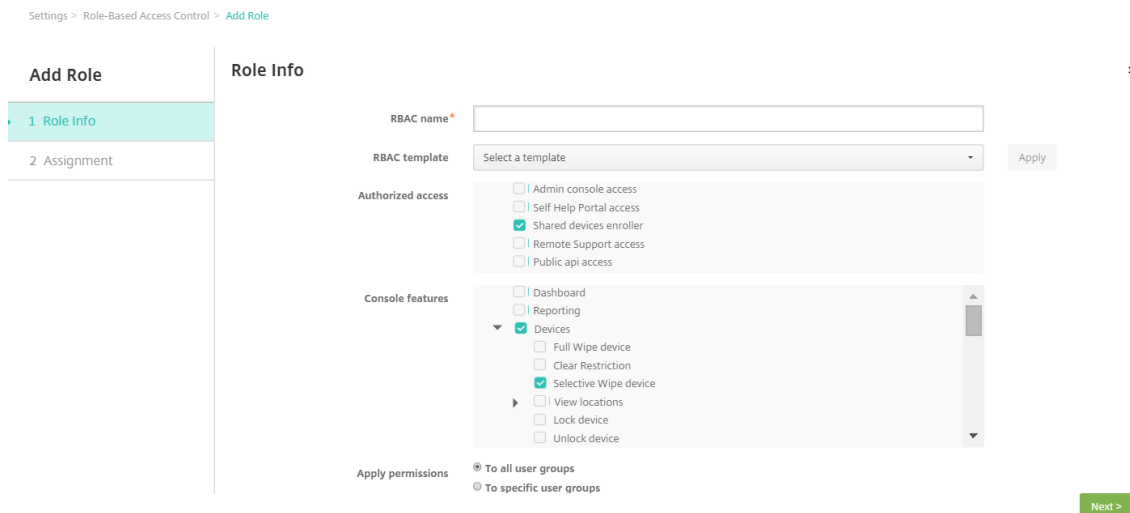
1. Create an Active Directory group named something like **Shared Device Enrollers**.
2. Add to this group the Active Directory users who you want to enroll shared devices. If you want a new account for this purpose, create a new Active Directory user (for example, `sdenroll`) and add that user to the Active Directory group.

### Configuring a shared device

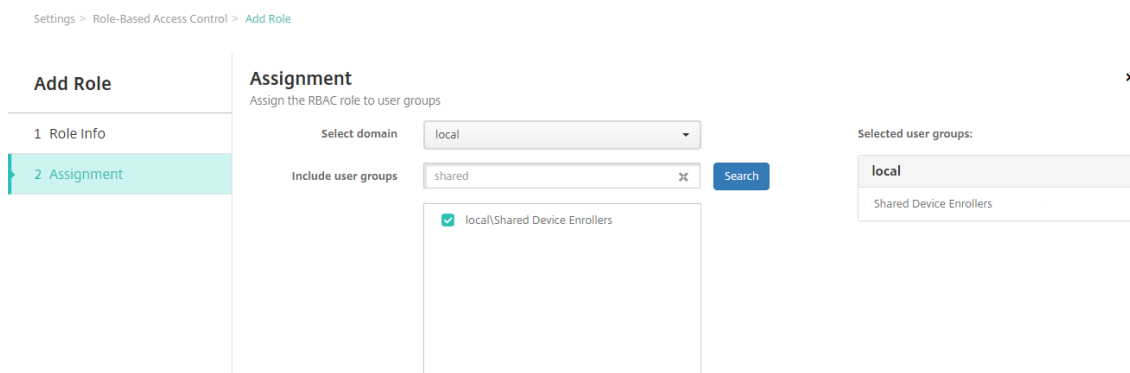
Follow these steps to configure a shared device.

1. From the Endpoint Management console, click the gear in the upper-right corner. The **Settings** page appears.
2. Click **Role-Based Access Control**, then click **Add**. The **Add Role** screen appears.
3. Create a shared-device enrollment user role named **Shared Device Enrollment User** with **Shared devices enroller** permissions under **Authorized Access**. Be sure to expand **Devices** in **Console features** and then select **Selective Wipe device**. This setting ensures that the apps and policies provisioned through the shared devices enroller account are deleted through Secure Hub, when the device is unenrolled.

For **Apply Permissions**, keep the default setting, **To all user groups**. Or, assign permissions to Active Directory user groups with the **To specific user groups**.

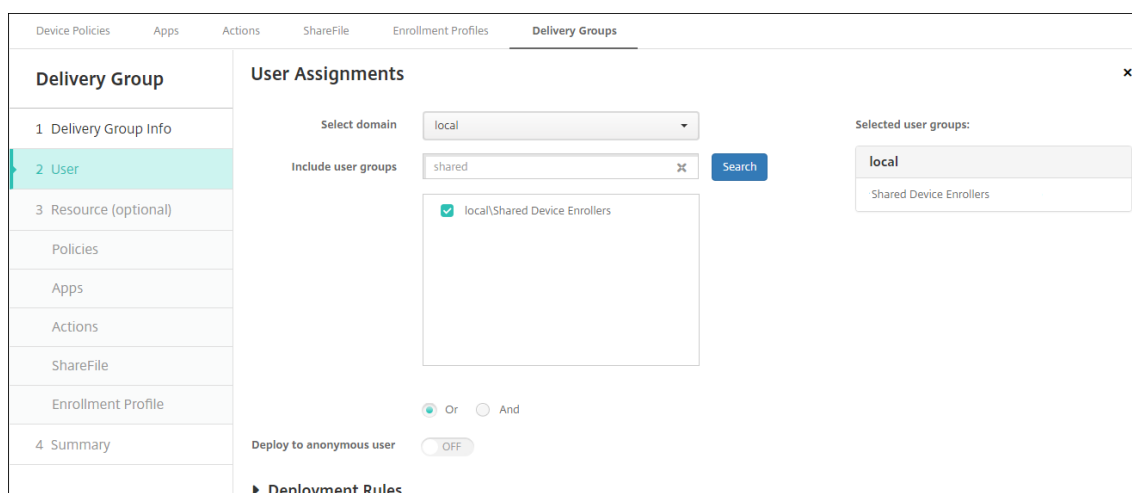


Click **Next** to move to the **Assignment** screen. Assign the shared-device enrollment role you created to the Active Directory group for shared device enrollment users. In the following image, **citrix.lab** is the Active Directory domain and **Shared Device Enrollers** is the Active Directory group.



4. Create a delivery group that contains the base policies, apps, and actions to apply to the device when a user is not signed on. Then, associate that delivery group with the shared device enrollment user Active Directory group.





5. Install Secure Hub on the shared device and enroll it in Endpoint Management using the shared device enrollment user account. You can now view and manage the device through the Endpoint Management console.
6. To apply different policies or to provide more apps for authenticated users, create a delivery group associated with those users and deploy the group to shared devices only. When creating the groups, configure deployment rules to ensure that the packages are deployed to shared devices. For more information, see [Deploy Resources](#).
7. To stop sharing the device, perform a selective wipe to remove the shared device enrollment user account from the device. The selective wipe also removes any apps and policies deployed to the device.

## Shared device user experience

### MDM enrollment

Users see only the resources available to them, and they have the same experience on every shared device. The shared device enrollment policies and apps always remain on the device. When a user who isn't enrolled in shared devices signs on to Secure Hub, their policies and apps deploy to the device. When that user signs off, any policies and apps that differ from the shared device enrollment get removed. The shared-device enrollment resources remain intact.

### MDM+MAM enrollment

Secure Mail and Secure Web are deployed to the device when enrolled by the shared device enrollment user. User data is maintained securely on the device. The data is not exposed to other users when they sign on to Secure Mail or Secure Web.

Only one user at a time can sign on to Secure Hub. The previous user must sign off before the next user can sign on. For security reasons, Secure Hub does not store user credentials on shared devices,

so users must enter their credentials each time they sign on. To ensure that a new user cannot access resources intended for the previous user: Secure Hub does not allow new users to sign on while the policies, apps, and data associated with the previous user are being removed.

Shared device enrollment doesn't change the process for upgrading apps. You can push upgrades to shared-device users as always, and shared-device users can upgrade apps right on their devices.

### Recommended Secure Mail policies

- For the best Secure Mail performance, set **Max sync period** based on the number of users to share the device. Allowing unlimited sync is not recommended.

---

Number of users sharing device	Recommended max sync period
21–25	1 week or less
6–20	2 weeks or less
5 or fewer	1 month or less

---

- Block **Enable contact export** to avoid exposing a user's contacts to other users who share the device.
- On iOS, only the following settings can be set per user. All other settings are common across users who share the device:
  - Notifications
  - Signature
  - Out of Office
  - Sync Mail Period
  - S/MIME
  - Check Spelling

## Alexa for Business

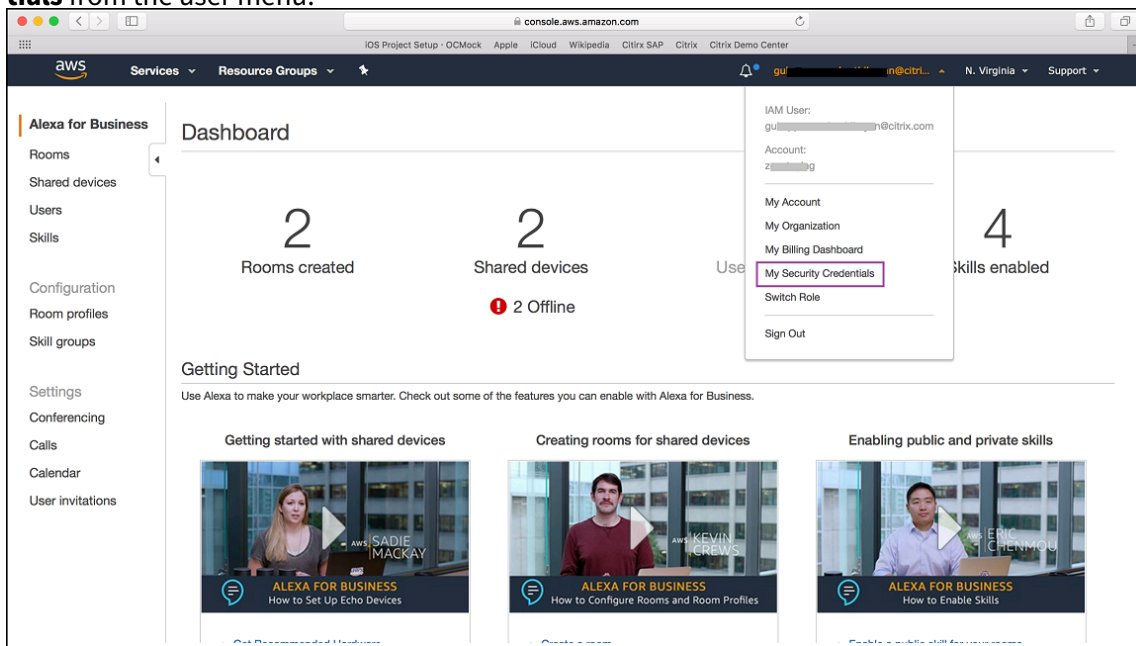
August 31, 2021

The Alexa for Business service of Amazon Web Services (AWS) lets you manage large numbers of Alexa-enabled devices for business uses, such as conference room assistance. Endpoint Management lets you configure and manage these devices in the Endpoint Management console. Endpoint Management doesn't deploy policies directly to Alexa devices. Instead, Endpoint Management updates AWS services and AWS delivers the configurations to Alexa devices.

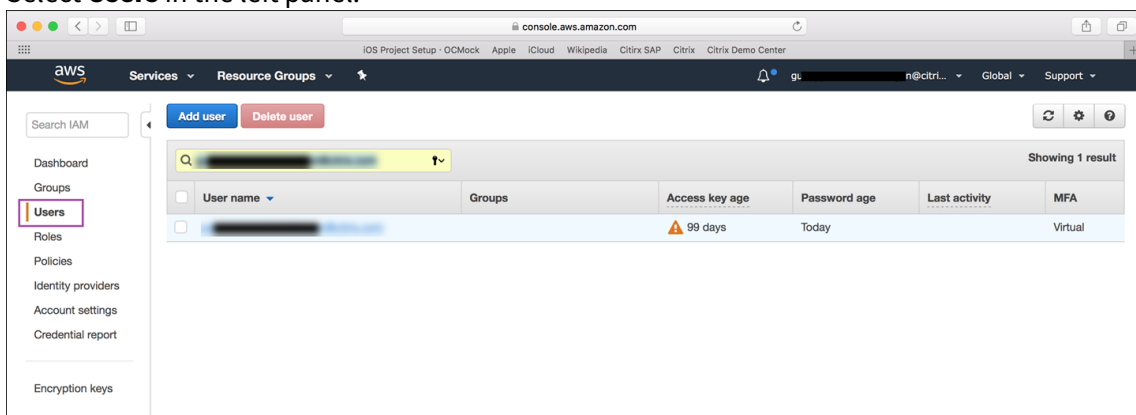
For information about using Alexa for Business, see the [Alexa for Business Administration Guide](#).

### Authenticate your AWS account to Endpoint Management

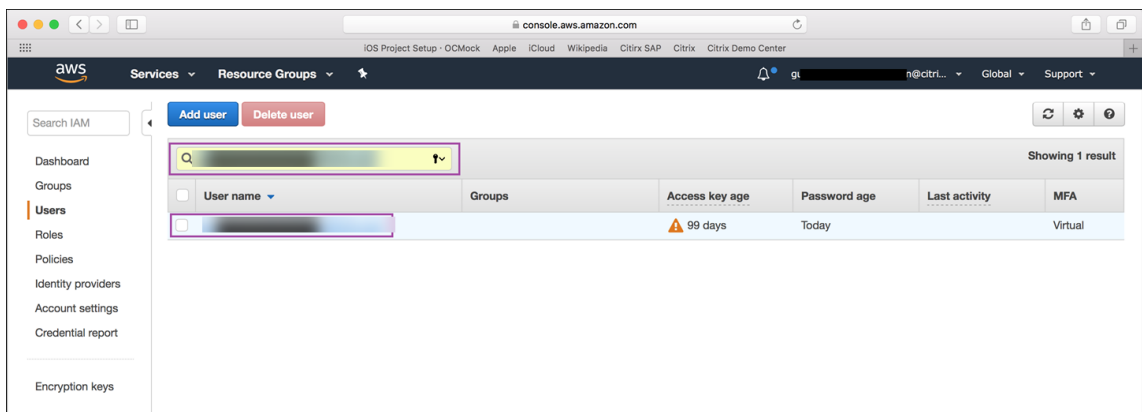
1. To get your AWS account credentials, log in to the AWS console and select **My Security Credentials** from the user menu.



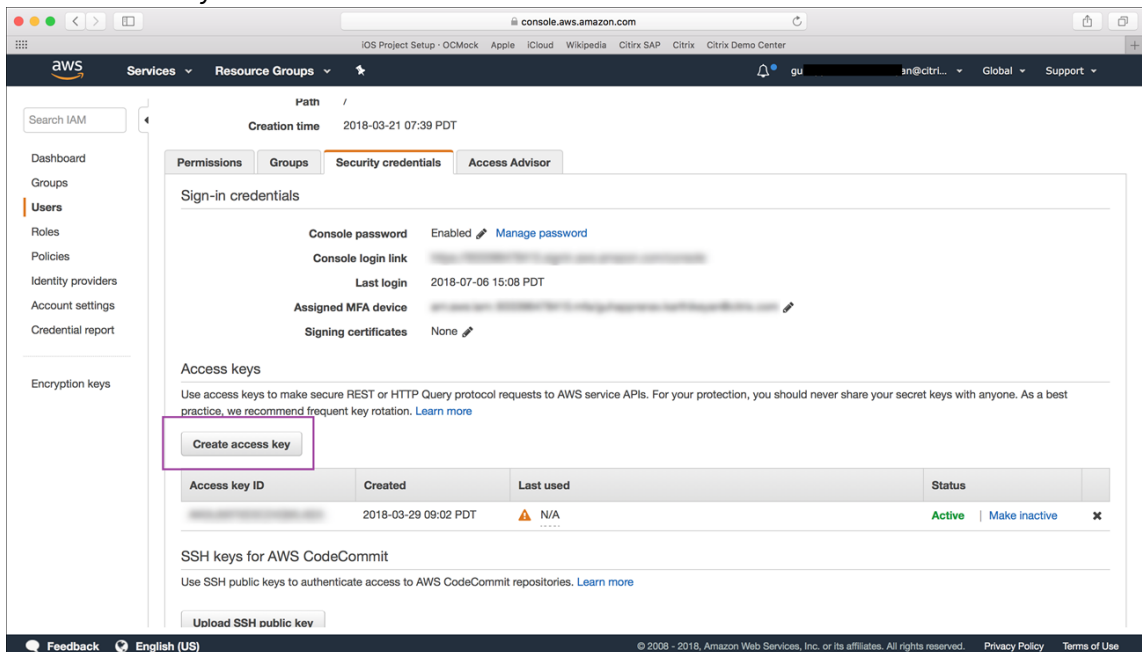
2. Select **Users** in the left panel.



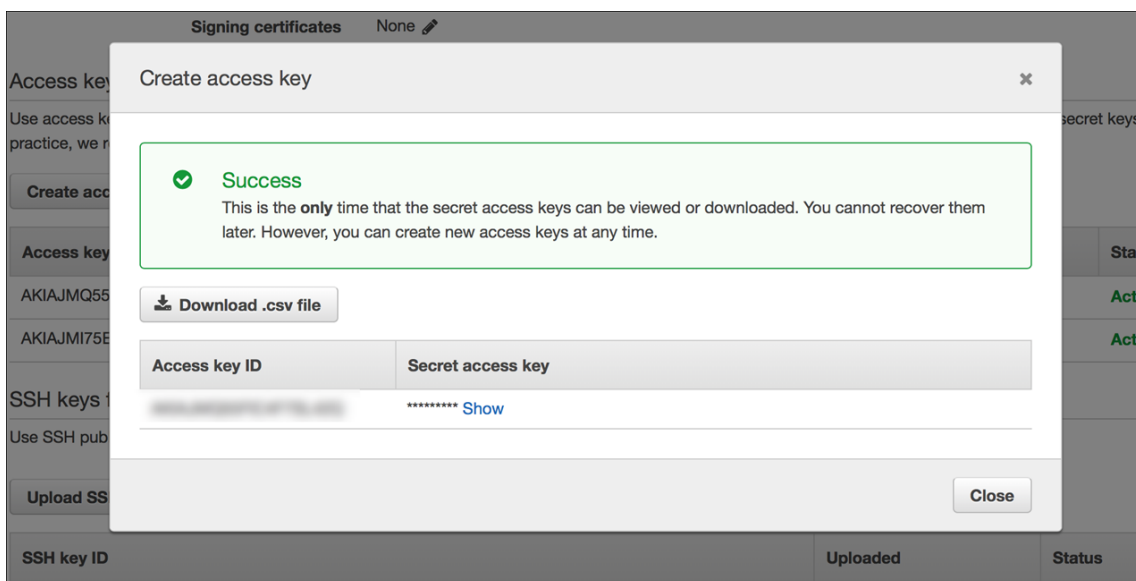
3. Search for your user name and then select it.



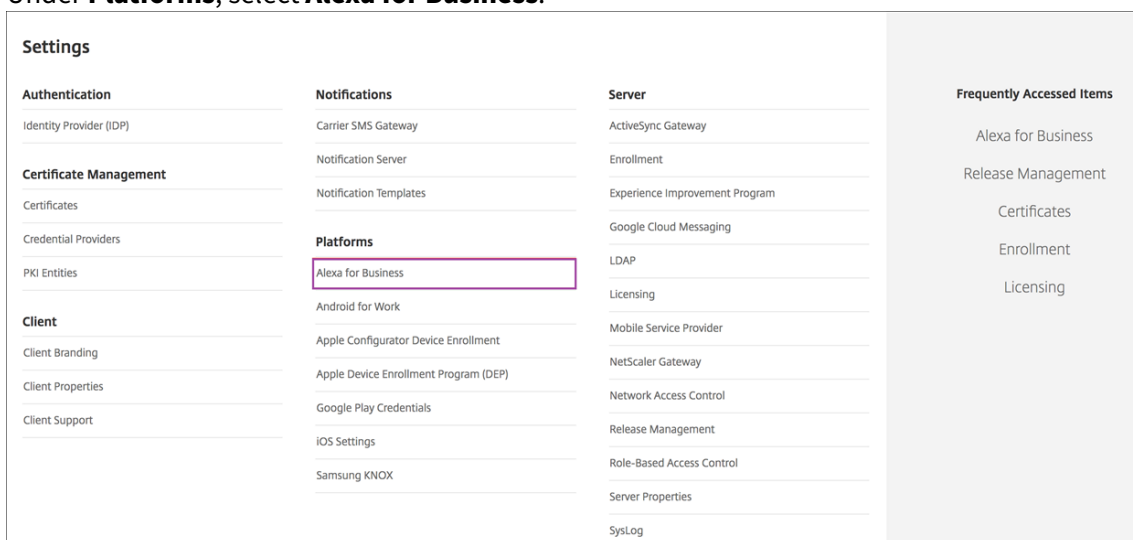
4. In the **Security Credentials** tab, click **Create access key** to generate your access key ID and secret access key.



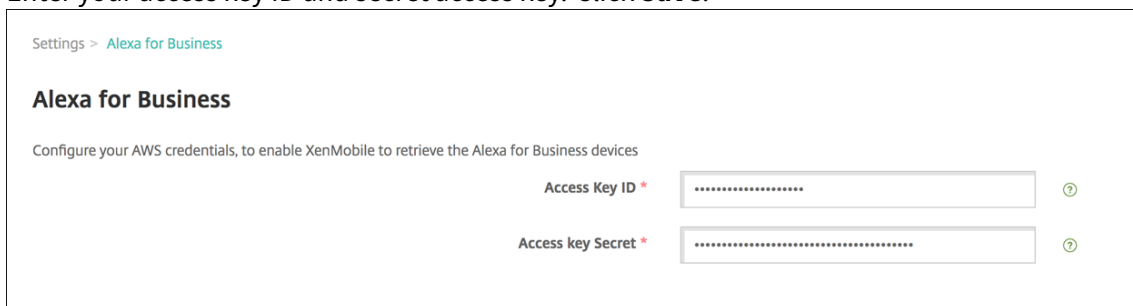
5. Download the access key ID and secret access key. Save or make a note of them.



6. In the Endpoint Management console, click the gear icon to go to **Settings**.
7. Under **Platforms**, select **Alexa for Business**.



8. Enter your access key ID and secret access key. Click **Save**.



## Configure Alexa for Business on Endpoint Management

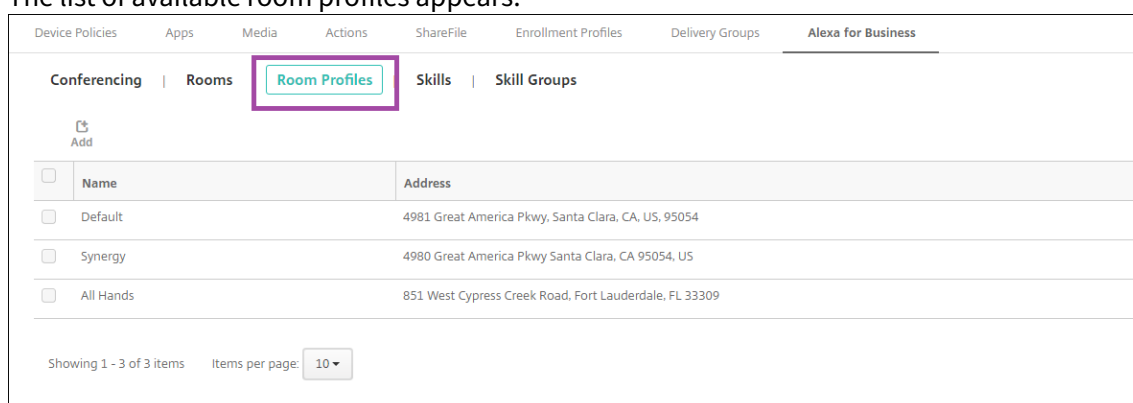
Endpoint Management lets you configure:

- Room profiles of settings that you apply to rooms containing Alexa devices
- Rooms that represent the physical rooms that contain the devices
- Skill groups that you assign to rooms or devices
- Alexa skills from the Alexa skill store that can be added to skill groups
- Conferencing features that let you choose a conferencing provider and control how people schedule and join meetings in your rooms

### Configure room profiles

A room profile is a set of common configurations that can be applied to a collection of rooms that contain Alexa devices. You can add, edit, and delete room profiles.

1. In the Endpoint Management console, select **Configure > Alexa for Business > Room Profiles**. The list of available room profiles appears.



2. To add a room profile, click **Add**. To edit a room profile, select the room profile you want to edit and click **Edit**.
3. Enter the room profile settings:

The screenshot displays the 'Add room profile' configuration interface. At the top, there is a navigation bar with tabs for 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', 'Delivery Groups', and 'Alexa for Business'. The main content area is titled 'Add room profile' and contains the following fields:

- Profile name \***: Text input field containing 'Synergy'.
- Address \***: Text input field containing '4980 Great America Parkway'.
- Time zone \***: Dropdown menu showing 'America/Los\_Angeles'.
- Device settings** (expanded):
  - Wake word**: Dropdown menu showing 'Alexa'.
  - Temperature units**: Radio buttons for 'US (Fahrenheit)' (selected) and 'Metric (Celsius)'.
  - Distance units**: Radio buttons for 'US (Feet, inches)' (selected) and 'Metric (Meters)'.
  - Maximum volume**: Dropdown menu showing '10'.
  - Device setup mode**: Radio buttons for 'On' (selected) and 'Off'.
- Outbound calling** (expanded):
  - Outbound calling**: Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Address book**: Text input field at the bottom.

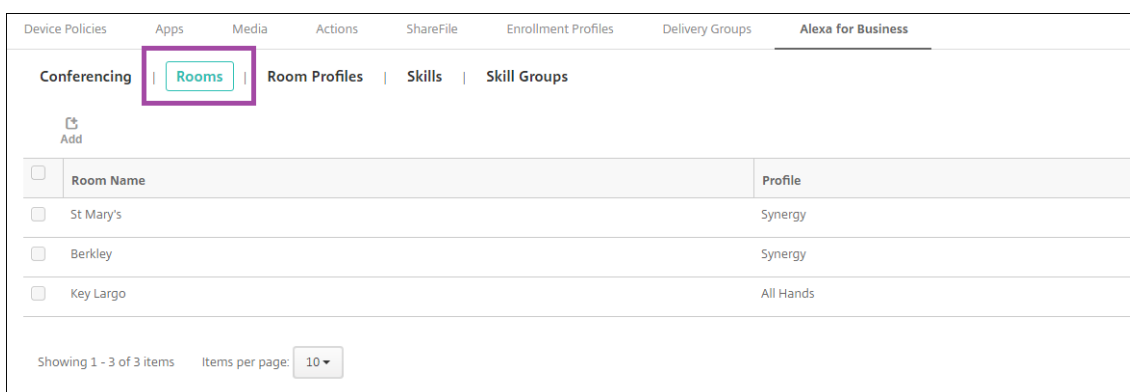
- **Profile Name:** Type the name of the profile.
- **Address:** Type the physical (street) address of the building where the rooms containing Alexa devices are.
- **Time zone:** Choose the time zone of the place.
- **Wake word:** Choose the wake word that Alexa devices respond to.
- **Temperature units:** Select the units in which Alexa devices report the temperature.
- **Distance units:** Select the units in which Alexa devices report the distance.
- **Maximum volume:** Choose the maximum volume setting for Alexa.
- **Device setup mode:** Select whether the Alexa devices can be reconfigured by forcing them to the device setup mode.
- **Outbound calling:** Enable or disable the outbound calling capability of Alexa devices.
- **Address book:** Set up the address book configuration for Alexa devices.

4. Click **Save**.

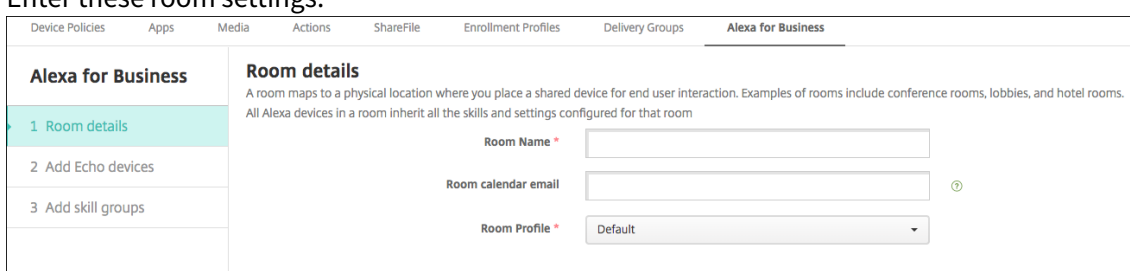
## Configure rooms

The rooms you configure in the Endpoint Management console represent the physical conference rooms, meeting rooms, and other rooms in the building. While configuring a room, you associate an Alexa device for the room and add a skills group to the device. You can add, edit, and delete rooms.

1. In the Endpoint Management console, select **Configure > Alexa for Business > Rooms**. The list of available rooms appears.

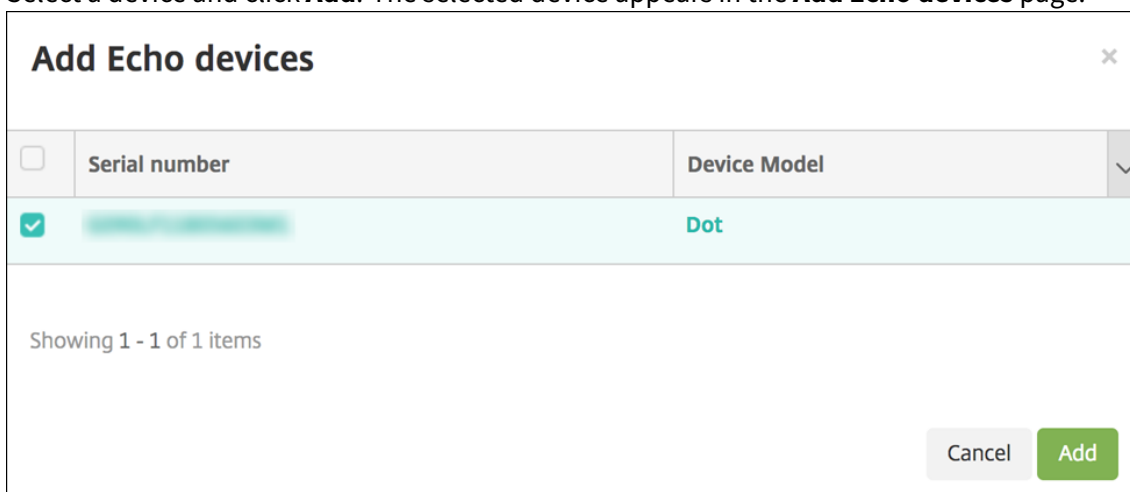


- To add a room, click **Add**. To edit a room, select the room you want to edit and click **Edit**.
- Enter these room settings:



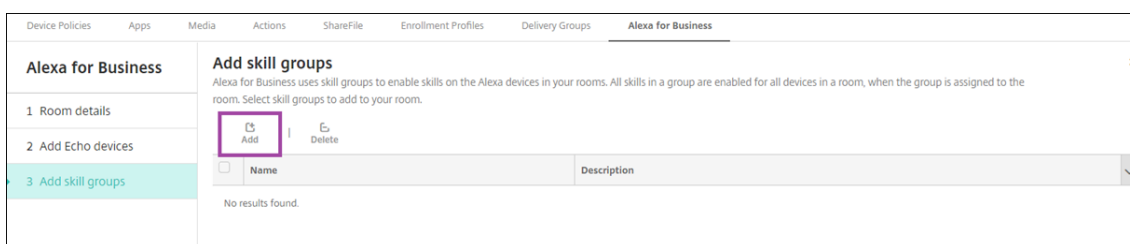
- **Room Name:** Type the name of the conference room, meeting room, or other room.
- **Room calendar email:** Type the calendar email address of the room.
- **Room Profile:** Choose the name of the room profile configuration for the room.

- Click **Next**.
- To associate an Alexa device with the room, click **Add**.
- Select a device and click **Add**. The selected device appears in the **Add Echo devices** page.

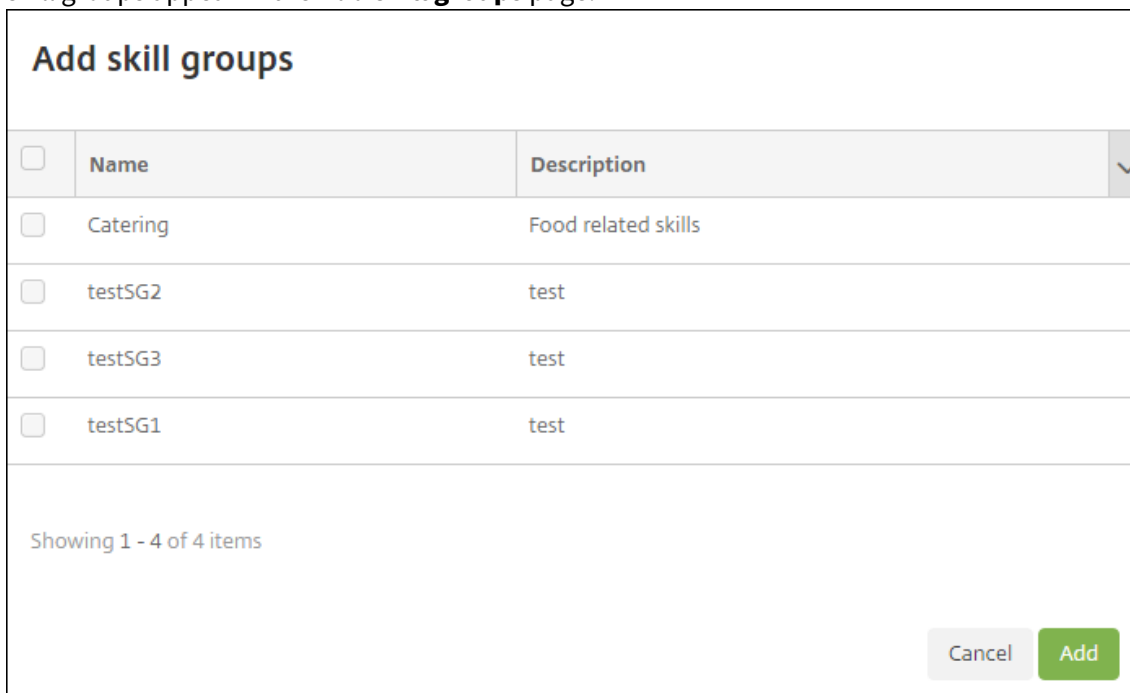


- Click **Next**.
- To add skill groups to the Alexa devices in the room, click **Add**.





9. Select the skill groups you want to add to the Alexa devices in the room. Click **Add**. The selected skill groups appear in the **Add skill groups** page.

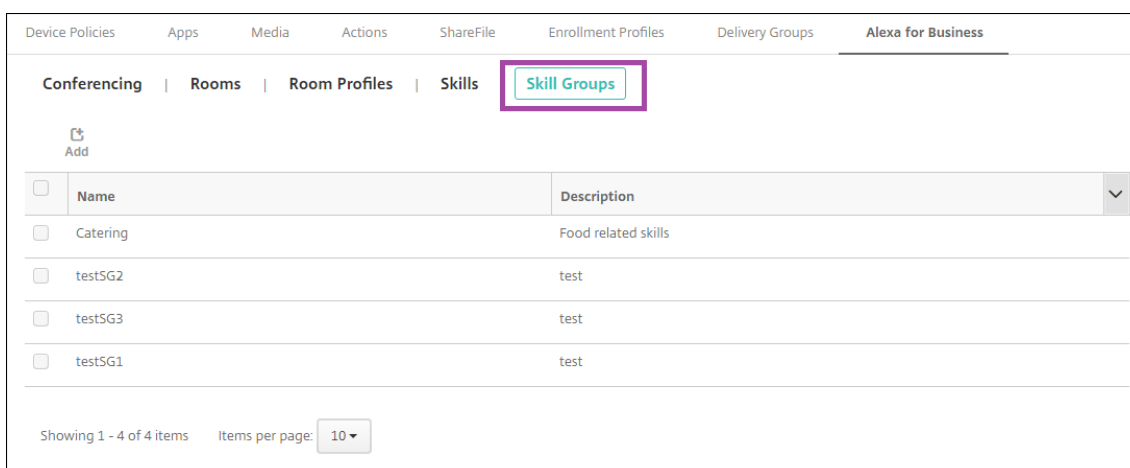


10. Click **Save**.

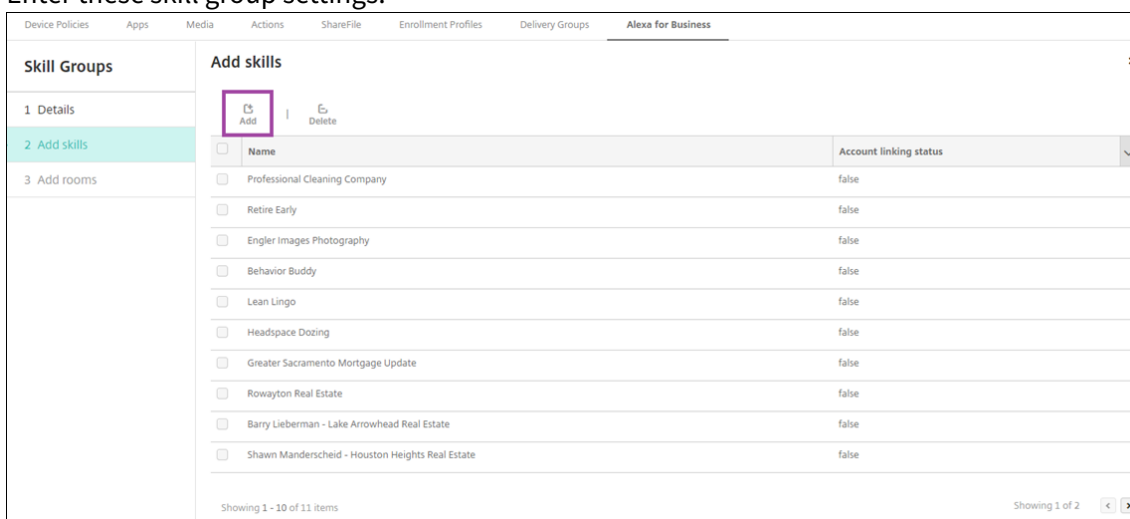
### Configure skill groups

Skill groups are collections of skills that can be applied to a room. You can create a skill group and then assign it to a room. Skills let you use an Alexa device to do things like start and end an online meeting or review a list of agenda items. You can add, edit, and delete skill groups.

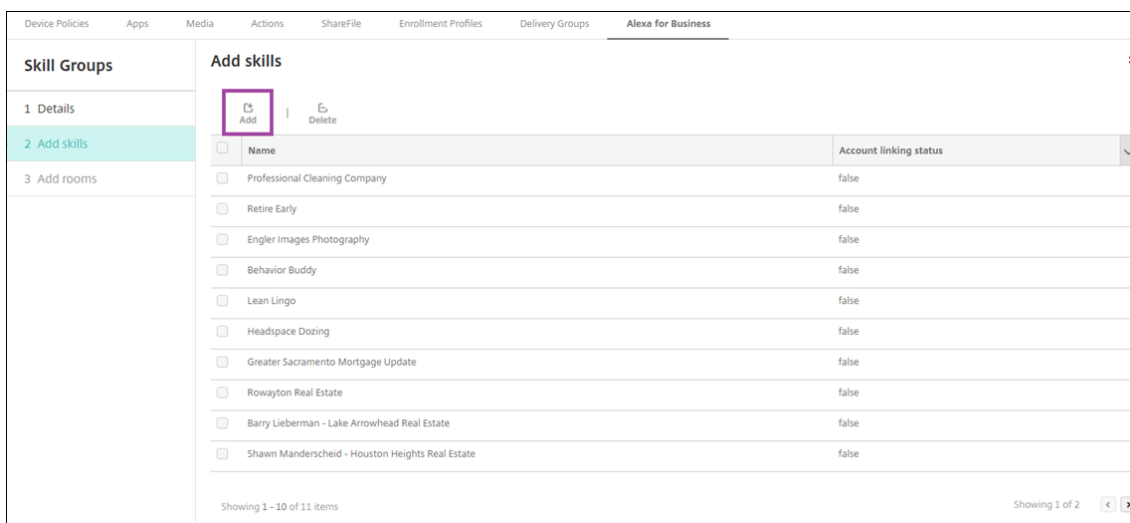
1. In the Endpoint Management console, select **Configure > Alexa for Business > Skill Groups**. The list of available skill groups appears.



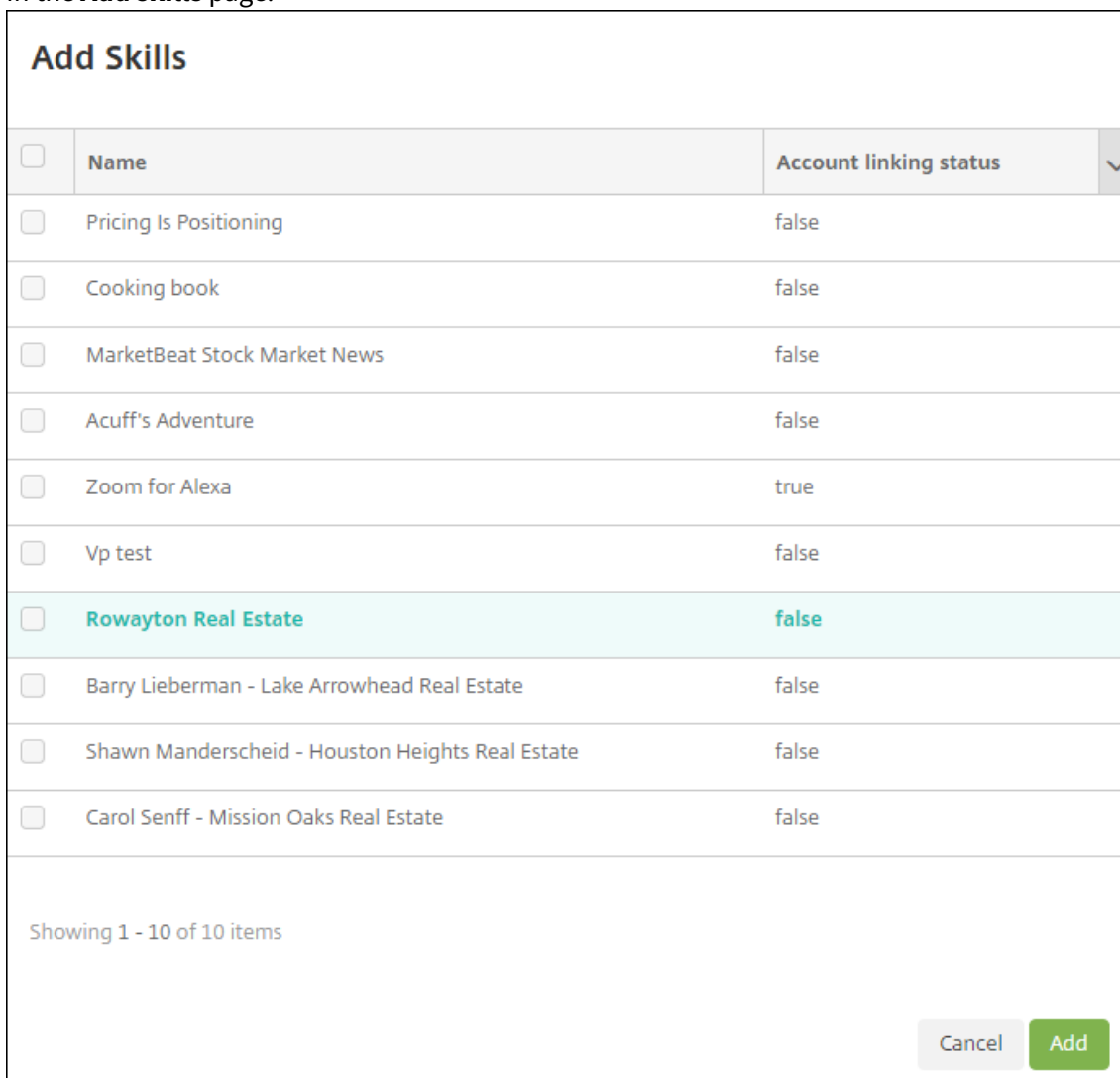
2. To add a skill group, click **Add**. To edit a skill group, select the skill group you want to edit and click **Edit**.
3. Enter these skill group settings:



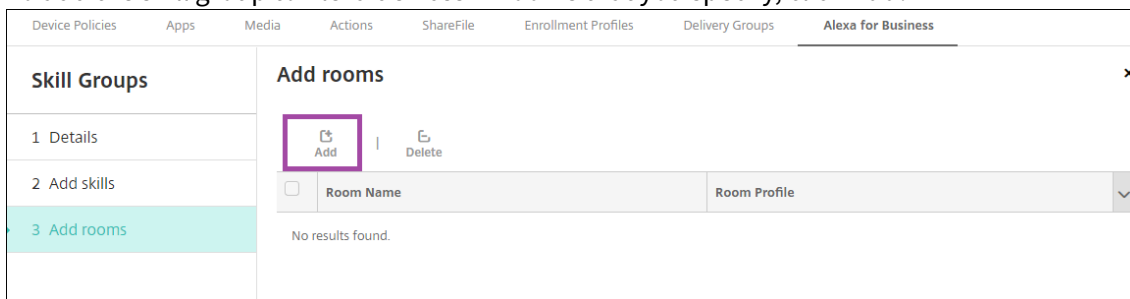
- **Name:** Type the name of the skill group.
  - **Description:** Type a brief description of the skill group.
4. Click **Next**.
  5. To add skills to the skill group, click **Add**.



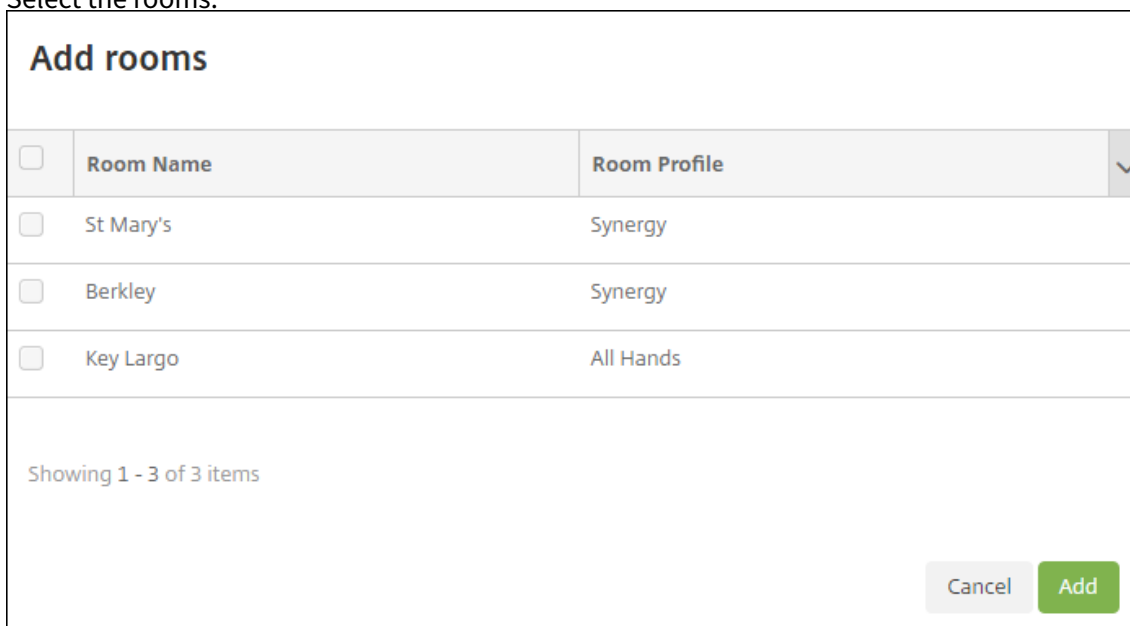
6. Select the skills you want to include in the skill group and click **Add**. The selected skills appear in the **Add skills** page.



7. To add the skill group to Alexa devices in rooms that you specify, click **Add**.



8. Select the rooms.



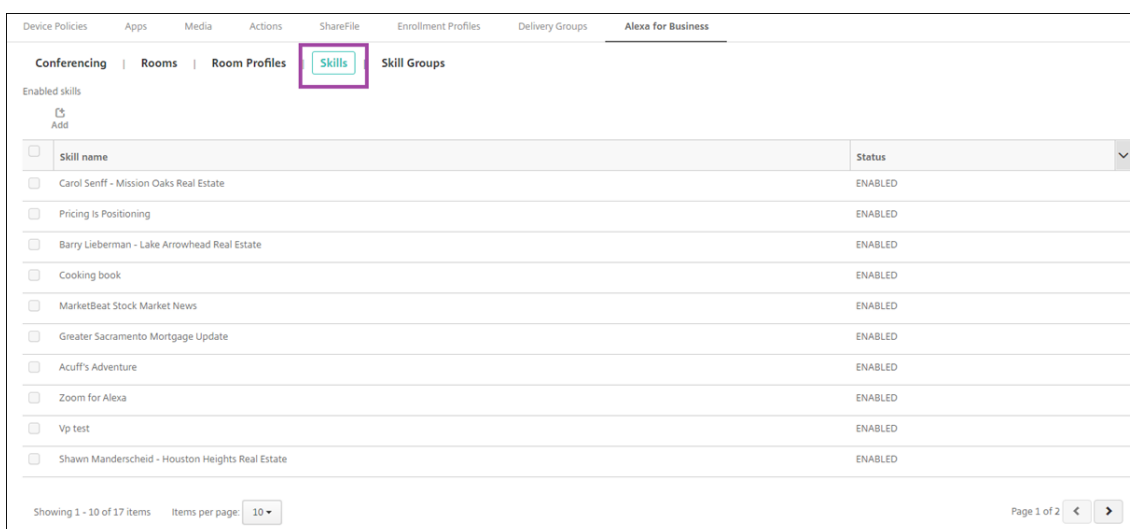
9. Click **Save**.

### Make skills available for skill groups

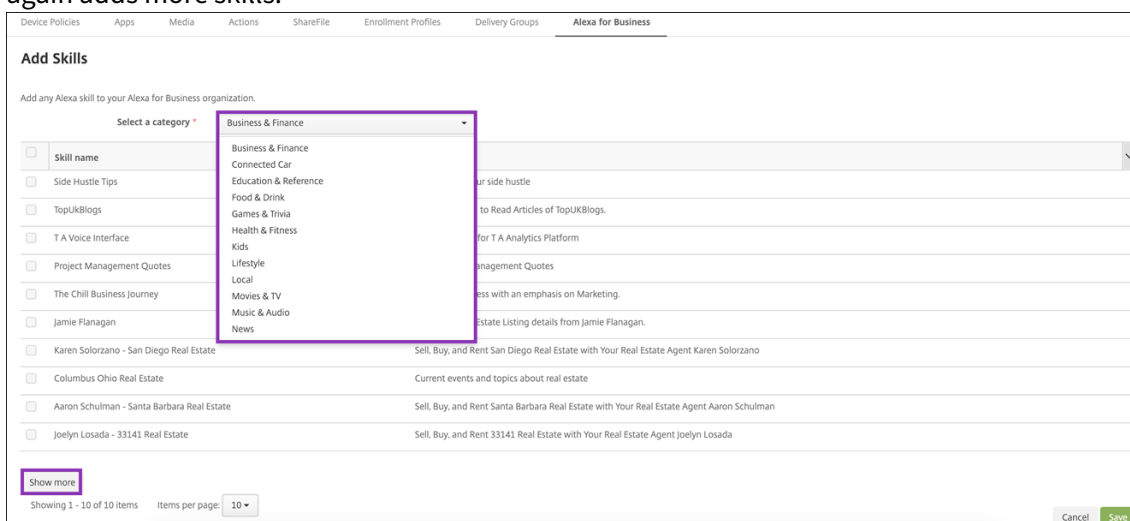
You configure the list of Alexa skills available to be included in skill groups in your Alexa for Business organization. These skills are from the public Alexa skills store or private skills published to your organization.

### Add skills to your organization

1. In the Endpoint Management console, select **Configure > Alexa for Business > Skills**. The list of enabled skills appears.



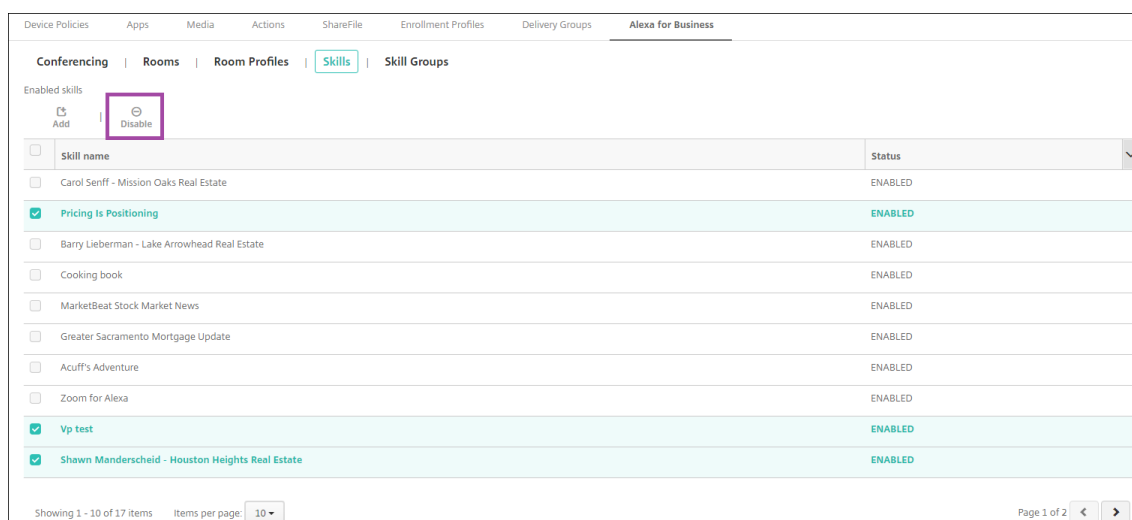
2. To add a skill, click **Add**.
3. To see more Alexa skills, select a category and click **Show more**. Clicking **Show more** adds up to 10 more skills to the list of skills available to add to your organization. Click **Show more** again adds more skills.



4. Select the skills you want to add to your organization.
5. Click **Save**.

### Remove skills from your organization

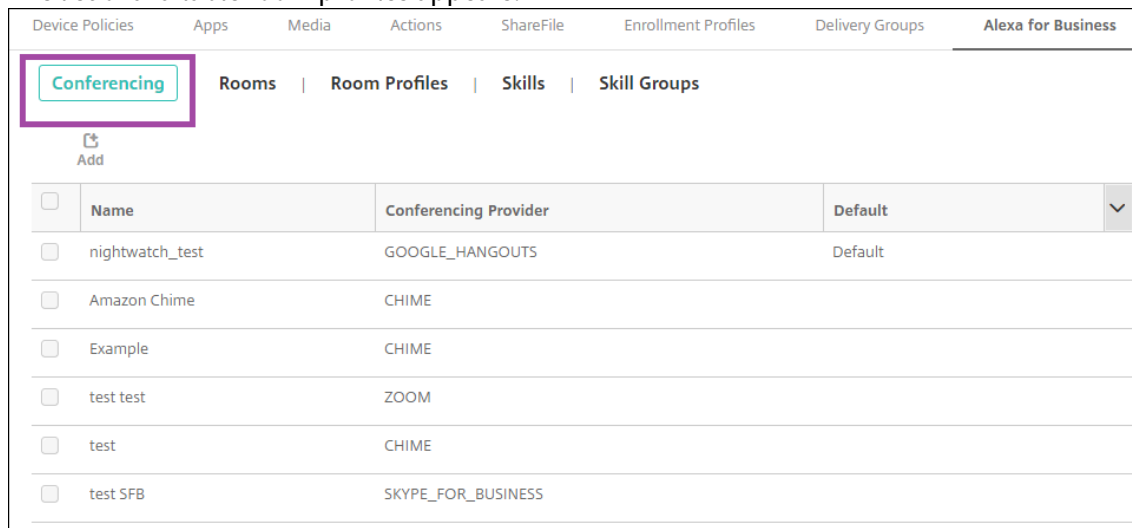
1. In the Endpoint Management console, select **Configure > Alexa for Business > Skills**. The list of enabled skills appears.
2. Select the skills you want to remove from your organization.
3. Click **Disable**.



## Configure conferencing

Conferencing features let you configure conferencing providers, like Google Hangout or Amazon Chime, that control how people join conferences in rooms that contain Alexa devices. You can add, edit, and delete conferencing providers. You can also set a default conferencing provider.

1. In the Endpoint Management console, select **Configure > Alexa for Business > Conferencing**. The list of available room profiles appears.



2. To add a conferencing provider, click **Add**. To edit a conferencing provider, select the room profile you want to edit and click **Edit**.
3. Enter the room profile settings:

- **Conferencing provider:** Select a conferencing provider from the list.
- **Name:** Type the name you want to give the conferencing provider.
- **Meeting PIN:** Specify whether to require a PIN to join the meeting.
- **PSTN dial-in settings**
  - **Country code:** Type the country code.
  - **Phone number:** Type the phone number.
  - **Meeting ID delay:** Specify the number of seconds before the meeting ID is sent.
  - **Meeting PIN delay:** Specify the number of seconds before the PIN is sent.
- **SIP/H323 dial-in settings** The SIP/H323 dial-in settings are used to join meetings using your existing video conferencing equipment.
  - **Protocol:** Select a protocol.
  - **IP address:** Type the IP address.

4. Click **Save**.

If you configure more than one conferencing provider, set the default provider.

1. In the Endpoint Management console, select **Configure > Alexa for Business > Conferencing**. The list of available room profiles appears.
2. Select the conferencing provider you want to set as the default.
3. Click **Set Default**.

## Migrate from device administration to Android Enterprise

July 7, 2021

This article discusses considerations and recommendations for migrating from legacy Android device administration to Android Enterprise. Google is deprecating the Android Device Administration API. That API supported enterprise apps on Android devices. Android Enterprise is the modern management solution recommended by Google and Citrix.

Endpoint Management is changing to Android Enterprise as the default enrollment method for Android devices. After Google deprecates the APIs, enrollment will fail for Android Q devices in device administration mode.

Android Enterprise includes support for fully managed and work profile device modes. The Google publication, [Android Enterprise Migration Bluebook](#), explains in detail about how legacy device administration and Android Enterprise differ. We recommend that you read the migration information from Google.

We recommend that you also refer to the Citrix Tech Zone article, [Migration from Android Device Administrator to Android Enterprise with Citrix Endpoint Management](#).

### Impact of device administration deprecation

Google has deprecated the Device Administrator APIs and won't support them as of November 2, 2020. These APIs won't work on devices running Android 10+ after we upgrade Citrix Secure Hub to target Android API level 29:

- **Disable camera:** Controls access to device cameras.
- **Keyguard features:** Controls features that are related to device locking, such as biometrics and patterns.
- **Expire password:** Forces users to change their password after a configurable time period.
- **Limit password:** Sets restrictive password requirements.

### Requirements and recommendations

- If you can upgrade a device to Android 10+, you must enroll that device in Android Enterprise.
  - You must enroll Android 11 devices into Android Enterprise.
  - As of September 2020, for Android 10 devices: Citrix doesn't support new enrollments or device re-enrollments into device administration mode. Devices already enrolled continue to work until November 2, 2020, as noted in the preceding section.
- For devices running Android 9 and lower, we support the legacy device administration mode. However, we recommend moving those devices to Android Enterprise as soon as possible.



- For new or existing devices enrolled in Citrix MAM-only mode, no action is needed. The deprecated Google APIs have no impact on devices in MAM-only mode. However, with the move to platform encryption, we highly recommend moving from MAM-only mode to Android Enterprise work profile mode (BYOD). Work profile mode provides MAM functionality, but in a container on the device.

### **Analysis**

The analysis phase of migration consists of:

- Understanding your legacy Android setup
- Documenting your legacy setup so you can map legacy features to Android Enterprise features

### **Recommended analysis**

1. Evaluate Android Enterprise on Endpoint Management: Fully managed, fully managed with work profile, dedicated device, work profile (BYOD).
2. Analyze your current device administration features against Android Enterprise.
3. Document your device administration use cases.

To document your device administration use cases:

1. Create a spreadsheet and list the current policy groups in your Endpoint Management console.
2. Create separate use cases based on the existing policy groups.
3. For each use case, document the following:
  - Name
  - Business owner
  - User identity model
  - Device Requirements
    - Security
    - Management
    - Usability
  - Device inventory
    - Make and model
    - OS Version
  - Apps
4. For each app, list:
  - App name
  - Package name

- Hosting method
- Whether the app is public or private
- Whether the app is mandatory (true/false)

## Requirements mapping

Based on the completed analysis, determine your Android Enterprise feature requirements.

### Recommended requirements mapping

1. Determine the management mode and enrollment method:
  - Work profile (BYOD): Requires re-enrollment. No factory reset needed.
  - Fully managed: Requires factory reset. Enroll devices by using QR code, Near field communication (NFC) bump, device policy controller (DPC) identifier, zero touch.
2. Create an app migration strategy.
3. Map use case requirements to Android Enterprise features. Document the feature for each device requirement that most closely matches the requirement and its corresponding Android version.
4. Determine the minimum Android OS based on feature requirements (7.0, 8.0, 9.0).
5. Choose an identity model:
  - Recommended: Managed Google Play Account
  - Use Google Workspace accounts only if you're a Google Cloud Identity Customer
6. Create a device strategy:
  - No action: If devices meet the minimum OS level
  - Upgrade: If devices support and can be updated to the supported OS
  - Replace: If devices can't be updated to the supported OS level

### Recommended app migration strategy

After you complete the requirements mapping, move the apps from the Android platform to the Android Enterprise platform. For details about publishing apps, see [Add apps](#).

- Public store apps
  1. Select the apps to migrate and then edit the apps to clear the Google Play setting and select **Android Enterprise** as the platform.

2. Select the delivery group. If an app is mandatory, move the app to the **Required Apps** list in the delivery group.

After you save an app, it appears in the Google Play Store. If you have a work profile, apps appear in the Google Play Store in the work profile.

- Private (enterprise) apps

Private apps are developed in-house or by a third-party developer. We recommend that you publish private apps by using Google Play.

1. Select the apps to migrate and then edit the apps to select **Android Enterprise** as the platform.
2. Upload the APK file and then configure the app settings.
3. Publish the app to the required delivery group.

- MDX apps

1. Select the apps to migrate and then edit the apps to select **Android Enterprise** as the platform.
2. Upload the MDX File. Go through the app approval process.
3. Select the MDX policies.

For Enterprise MDX apps, we recommend changing them to MDX SDK mode wrapped apps:

- Option 1: Host the APK in Google Play with a developer account assigned privately to your organization. Publish the MDX file in Endpoint Management.
- Option 2: Publish the app from Endpoint Management as an enterprise app. Publish the APK in Endpoint Management and select the platform **Android Enterprise** for the MDX file.

### Citrix device policy migration

For policies that are available for both the **Android (legacy DA)** and **Android Enterprise** platforms: Edit the policy and select the platform **Android Enterprise**.

- For Android Enterprise, consider the device enrollment method. Some policy options are available only for devices in work profile mode or fully managed mode. See [Configure Android Enterprise device and app policies](#).
- If you use the Exchange device policy for legacy DA devices, create a Managed configurations policy device policy instead to configure email settings.
- To ensure that you target a policy to the intended devices (Android Enterprise versus legacy DA), add a deployment rule to the policy. For example, for the legacy DA platform, use this deployment rule:

```
1 Limit by known device property name Android Enterprise
2 Enabled Device? Isn' t equal to true
3 <!--NeedCopy-->
```

That deployment rule checks if the device is NOT enabled for Android Enterprise and delivers the policy along with the apps to devices enabled for legacy DA.

## Proof of concept

After you migrate apps to Android Enterprise, you can set up a migration test to verify that the features are working as intended.

### Recommended proof-of-concept setup

1. Set up the deployment infrastructure:
  - Create a Delivery Group for your Android Enterprise testing.
  - Configure Android Enterprise in Endpoint Management.
2. Set up user apps.
3. Configure Android Enterprise features.
4. Assign policies to the Android Enterprise delivery group.
5. Test and confirm features.
6. Complete a device setup walkthrough for each use case.
7. Document user setup steps.

## Deployment

You can now deploy your Android Enterprise setup and prepare your users for migration.

### Recommended deployment strategy

The Citrix recommended deployment strategy is to test all of your production systems for Android Enterprise, then complete device migration later.

- In this scenario, users continue to use legacy devices with their current configuration. You set up new devices for Android Enterprise management.
- Migrate existing devices only when an upgrade or replacement is necessary.

- Migrate existing devices to Android Enterprise management at the end of their usual lifecycle. Or, migrate those devices when they need replacement due to loss or breakage.

## Android Enterprise

October 21, 2021

Android Enterprise is a set of tools and services provided by Google as an enterprise management solution for Android devices. With Android Enterprise:

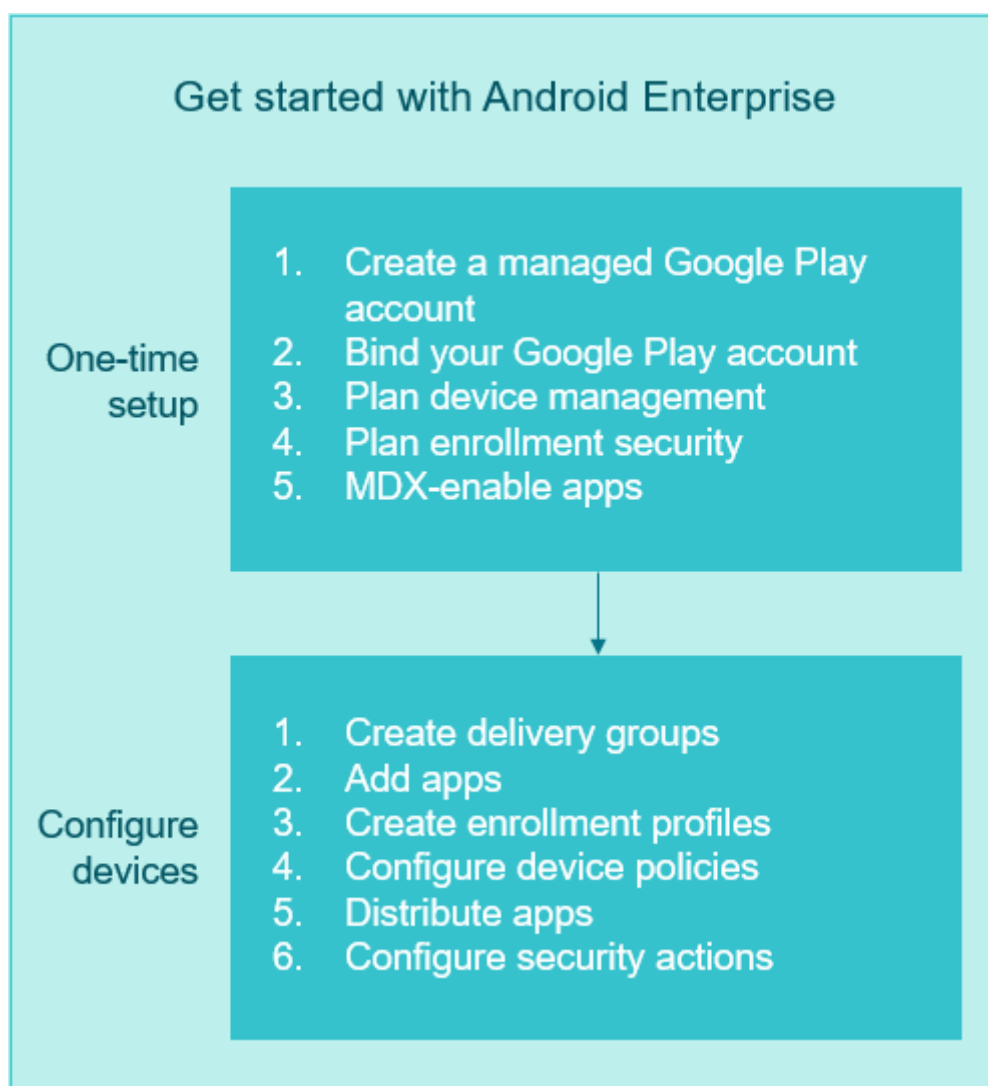
- You use Endpoint Management to manage company-owned and bring your own device (BYOD) Android devices.
- You can manage the entire device or a separate profile on the device. The separate profile isolates business accounts, apps, and data from personal accounts, apps, and data.
- You can also manage devices dedicated to a single use, such as inventory management. For an overview of Android Enterprise capabilities from Google, see [Android Enterprise Management](#).

Resources:

- For a list of terms and definitions related to Android Enterprise, see the Google Android Enterprise developers guide article, [Android Enterprise terminology](#). Google updates these terms frequently.
- For a list of Android operating systems supported for Endpoint Management, see [Supported device operating systems](#).
- For information about the outbound connections to consider when setting up network environments for Android Enterprise, see the Google support article, [Android Enterprise Network Requirements](#).
- For information about deploying Android Enterprise, see [Deploy resources](#)).

### Getting started with Android Enterprise

If your users have devices in device administration mode, see [Migrate from device administration to Android Enterprise](#). After your devices are migrated to Android Enterprise, use the following steps to set up Android Enterprise devices.



### **One-time setup**

1. Create a managed Google Play account.  
See Using managed Google Play with Endpoint Management and Requirements.
2. Bind your Google Play account to Endpoint Management.  
See Connecting Endpoint Management to Google Play.
3. Plan how you want to manage devices.  
See Device deployment scenarios and profiles.
4. Plan enrollment security for user devices.  
See Enrollment security.
5. Prepare to deliver MDX-enabled apps.

Use the MAM SDK to develop apps. Or, if you aren't ready to transition to the new SDK, use the command-line based MDX Toolkit to wrap the apps.

See [MAM SDK overview](#).

At this point, you're prepared to configure your Android Enterprise devices with app and devices policies, enrollment profiles, and apps. See the following section for guidance.

## Configure devices

1. Create delivery groups.

Control who gets what resources and when they get them. See [Deploy resources](#).

We will stop delivering apps published for the legacy DA platform to devices enrolled in Android Enterprise. For Android Enterprise devices, publish apps for the Android Enterprise platform. To continue to publish legacy DA apps to devices in DA mode, create a separate delivery group for those apps. See [Deprecation](#).

2. Add apps. You can approve the apps in Google Play directly from the Endpoint Management console.

See the Google support article, [Manage apps in your organization](#).

3. Create enrollment profiles.

Specify device and app management enrollment options. See [Device deployment scenarios and profiles](#) and [Creating enrollment profiles](#).

- When you deploy an Android Enterprise public app store app to an Android device user, that user is automatically enrolled in Android Enterprise.
- Zero-touch enrollment allows you to configure devices to enroll automatically when they are first powered on. See [Zero-touch enrollment](#).
- Knox Mobile Enrollment (KME) lets you enroll multiple Samsung Knox devices into Endpoint Management. See [Samsung Knox bulk enrollment](#) and [Samsung](#).

4. Configure device and app policies.

Balance enterprise security with user privacy and user experience. See [Configure Android Enterprise device and app policies](#).

5. Distribute apps.

You use managed Google Play to add, buy, and approve apps for deployment to the Android Enterprise workspace on a device. Users can only install apps from managed Google Play that you make available for them.

See:

- [Distribute Android Enterprise and Android for Workspace apps](#)
  - [Managed configurations policy](#)
  - [App permissions policy](#)
6. Configure security actions to monitor and ensure compliance.

See Security actions.

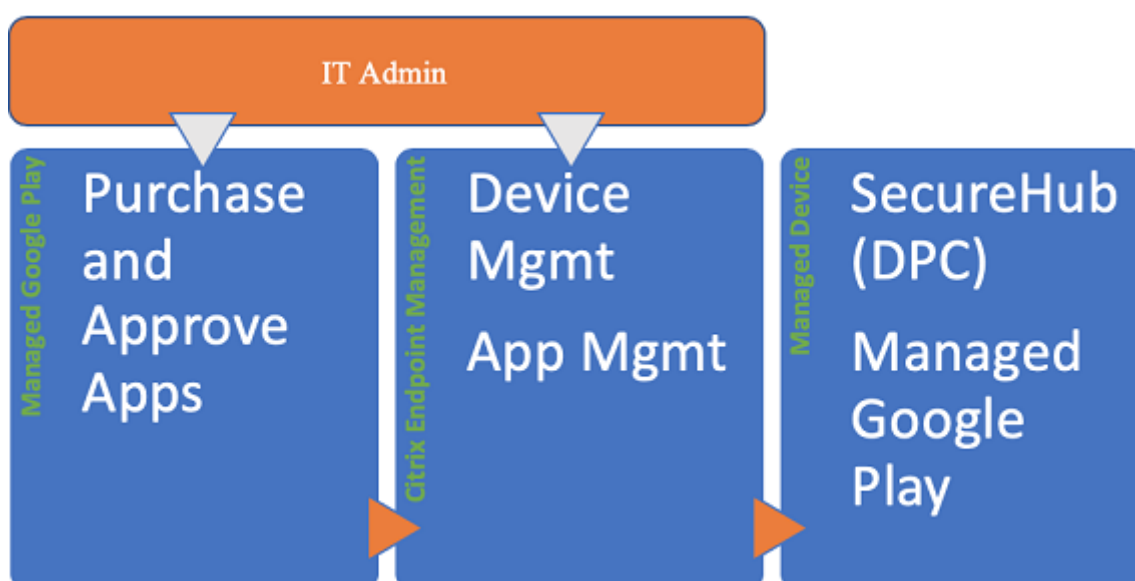
## Using managed Google Play with Endpoint Management

When you integrate Endpoint Management with managed Google Play to use Android Enterprise, you create an enterprise. Google defines an enterprise as binding between the organization and your enterprise mobile management (EMM) solution. All the users and devices that the organization manages through your solution belong to its enterprise.

An enterprise for Android Enterprise has three components: an EMM solution, a device policy controller (DPC) app, and a Google enterprise app platform. When you integrate Endpoint Management with Android Enterprise, the complete solution has these components:

- **Citrix Endpoint Management:** The Citrix EMM. Endpoint Management is the unified endpoint management for a secure digital workspace. Endpoint Management provides the means for IT administrators to manage devices and apps for their organizations.
- **Citrix Secure Hub:** The Citrix DPC app. Secure Hub is the launchpad for Endpoint Management. Secure Hub enforces policies on the device.
- **Managed Google Play:** A Google enterprise app platform that integrates with Endpoint Management. The Google Play EMM API sets app policies and distributes apps.

This illustration shows how administrators interact with these components and how the components interact with each other:





**Note:**

You can use either managed Google Play or Google Workspace (formerly G Suite) to register Citrix as your EMM provider. This article discusses using Android Enterprise with managed Google Play. If your organization uses Google Workspace to provide access to apps, you can use it with Android Enterprise. See [Legacy Android Enterprise for Google Workspace customers](#).

When you use managed Google Play, provision managed Google Play Accounts for devices and end users. Managed Google Play Accounts provide access to managed Google Play, allowing users to install and use the apps you make available. If your organization uses a third-party identity service, you can link managed Google Play Accounts with your existing identity accounts.

Because this type of enterprise is not tied to a domain, you can create more than one enterprise for a single organization. For example, each department or region within an organization can enroll as a different enterprise. Using different enterprises lets you manage separate sets of devices and apps.

For Endpoint Management administrators, managed Google Play combines the user experience and app store features of Google Play with a set of management capabilities designed for enterprises. You use managed Google Play to add, buy, and approve apps for deployment to the Android Enterprise workspace on a device. You can use Google Play to deploy public apps, private apps, and third-party apps.

For users of managed devices, managed Google Play is the enterprise app store. Users can browse apps, view app details, and install them. Unlike the public version of Google Play, users can only install apps from managed Google Play that you make available for them.

### Device deployment scenarios and profiles

Device deployment scenarios refer to who owns the devices you deploy and how you manage them. Device profiles refer to how the DPC manages and enforces policies on devices.

A work profile isolates business accounts, apps, and data from personal accounts, apps, and data. Work profiles and personal profiles are separated at an OS level. For more details about work profiles, see the Google Android Enterprise help topic, [What is a work profile](#).

**Important:**

When Android Enterprise devices update to Android 11, Google migrates devices managed as “fully managed with a work profile” to a new security-enhanced work profile experience. The new enrollment mode is called “work profile on corporate-owned devices.” For more information, see [Changes ahead for Android Enterprise’s Fully Managed with Work Profile](#). For Android 12 devices, see [Security and privacy enhancements for work profile](#).

Device management	Use cases	Work profile	Personal profile	Notes
Company-owned devices (fully managed)	Company-owned devices intended only for work use	No	No	For new or factory reset devices only. See Provisioning Android Enterprise fully managed devices.
Fully managed with a work profile / Work profile on corporate-owned devices	Company-owned devices intended for work and personal use	Yes	Yes. Two copies of the DPC run on these devices: One manages the device in device owner mode and the other manages the work profile in profile owner mode. You can apply separate policies to the device and the work profile.	See Provisioning Android Enterprise fully managed devices with a work profile or work profile on corporate-owned devices.
Dedicated devices*	Company-owned devices configured for a single use case, such as digital signage or ticket printing	No	No	See Provisioning dedicated Android Enterprise devices.

Device management	Use cases	Work profile	Personal profile	Notes
BYOD work profile**	Personal devices enrolled with work profile management (also known as profile owner mode)	Yes	Yes. The DPC manages only the work profile, not the whole device.	These devices don't need to be new or factory reset. See Provisioning Android Enterprise work profile devices.

\* Users can share a dedicated device. When a user signs on to an app on a dedicated device, the state of their work is with the app, not the device.

\*\* Endpoint Management does not support Zebra devices as in BYOD work profile mode. Endpoint Management supports Zebra devices as fully managed devices and in device legacy mode (also called device admin mode).

## Enrollment security

Enrollment profiles determine whether Android devices enroll in MAM, MDM, or MDM+MAM, with the option for users to opt out of MDM.

For information about specifying the level of security and required enrollment steps, see [User accounts, roles, and enrollment](#).

Endpoint Management supports the following authentication methods for Android devices enrolled in MDM or MDM+MAM. For information, see the following articles:

- [Domain or domain plus security token authentication](#)
- [Client certificate or certificate plus domain authentication](#)
- Identity providers:
  - [Authentication with Azure Active Directory through Citrix Cloud](#) (Preview)
  - [Authentication with Okta through Citrix Cloud](#) (Preview)

A rarely used authentication method is client certificate plus security token. For information, see <https://support.citrix.com/article/CTX215200>.

## Requirements

Before you start using Android Enterprise, you need:

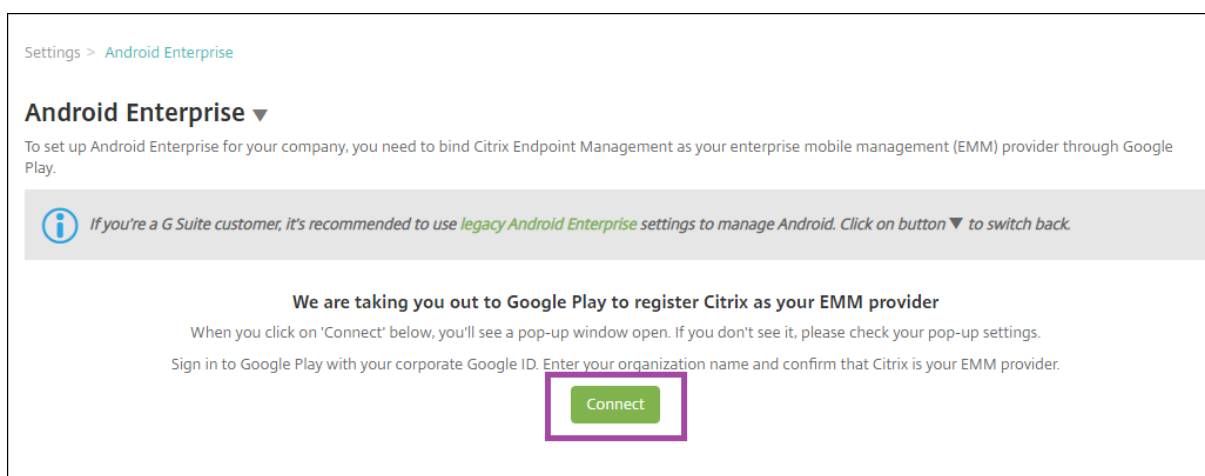
- Accounts and credentials:
  - To set up Android Enterprise with managed Google Play, a corporate Google account
  - To download the latest MDX files, a Citrix customer account
- Firebase Cloud Messaging (FCM) and a Connection scheduling device policy configured for Endpoint Management. See [Firebase Cloud Messaging](#) and [Connection scheduling device policy](#).
- For Samsung Knox Mobile Enrollment (optional), Knox premium licenses.

### Connecting Endpoint Management to Google Play

To set up Android Enterprise for your organization, register Citrix as your EMM provider through managed Google Play. That setup connects managed Google Play to Endpoint Management and creates an enterprise for Android Enterprise in Endpoint Management.

You need a corporate Google account to sign in to Google Play.

1. In the Endpoint Management console, go to **Settings > Android Enterprise**.
2. Click **Connect**. Google Play opens.



1. Sign in to Google Play with your corporate Google account credentials. Enter your organization name and confirm that Citrix is your EMM provider.
2. An enterprise ID is added for Android Enterprise. To enable Android Enterprise, slide **Enable Android Enterprise** to **Yes**.

Settings > Android Enterprise

### Android Enterprise

To set up Android Enterprise for your company, you need to bind Citrix Endpoint Management as your enterprise mobile management (EMM) provider through Google Play.

Enterprise ID	Name	Created Time
[Redacted]	xm tools test enterprise	9/26/18 5:06:04 pm

Showing 1 - 1 of 1 items    Items per page: 10

Enable Android Enterprise  YES

Unenroll

Your Enterprise ID appears in the Endpoint Management console.

### Android Enterprise

To set up Android Enterprise for your company, you need to bind Citrix Endpoint Management as your enterprise mobile management (EMM) provider through Google Play.

Enterprise ID	Name	Created Time
[Redacted]	[Redacted]	5/13/19 11:46:24 am

Showing 1 - 1 of 1 items    Items per page: 10

Enable Android Enterprise  YES

Your environment is connected to Google and is ready to manage devices. You can now provide apps for users.

Endpoint Management can provide users with Citrix mobile productivity apps, MDX apps, public app store apps, web and SaaS apps, enterprise apps, and web links. For more information on providing these types of apps to users, see [Distribute Android Enterprise and Android for Workspace apps](#).

The following section shows how to provide mobile productivity apps.

### Providing Citrix mobile productivity apps to Android Enterprise users

Providing Citrix mobile productivity apps for Android Enterprise users requires these steps.

1. Publish the apps as MDX apps. See [Configure apps as MDX apps](#).
2. Configure the rules for the security challenge your users use to access the work profiles on their devices. See [Configure security challenge policy](#).

The apps you publish are available to devices enrolled in your Android Enterprise enterprise.

**Note:**

When you deploy an Android Enterprise public app store app to an Android user, that user is automatically enrolled in Android Enterprise.

**Configure apps as MDX apps**

To configure a Citrix productivity app as an MDX app for Android Enterprise:

1. In the Endpoint Management console, click **Configure > Apps**. The **Apps** page appears.

Icon	App Name	Type	Category	Created On	Last Updated	Disable
	Classroom - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>

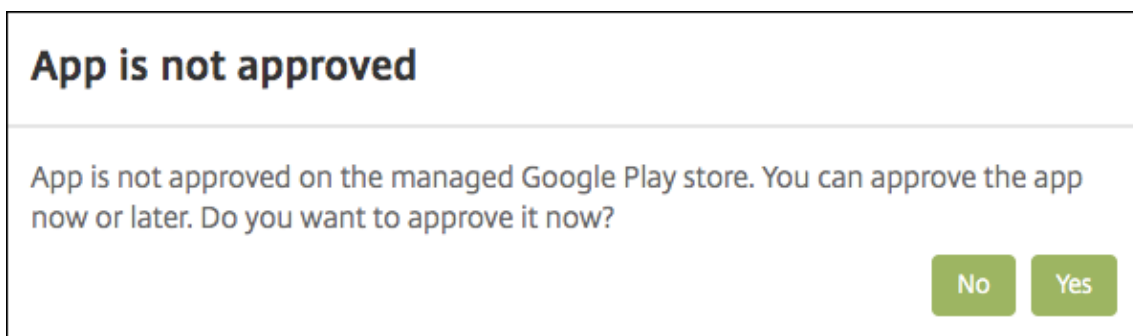
2. Click **Add**. The **Add App** dialog box appears.

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

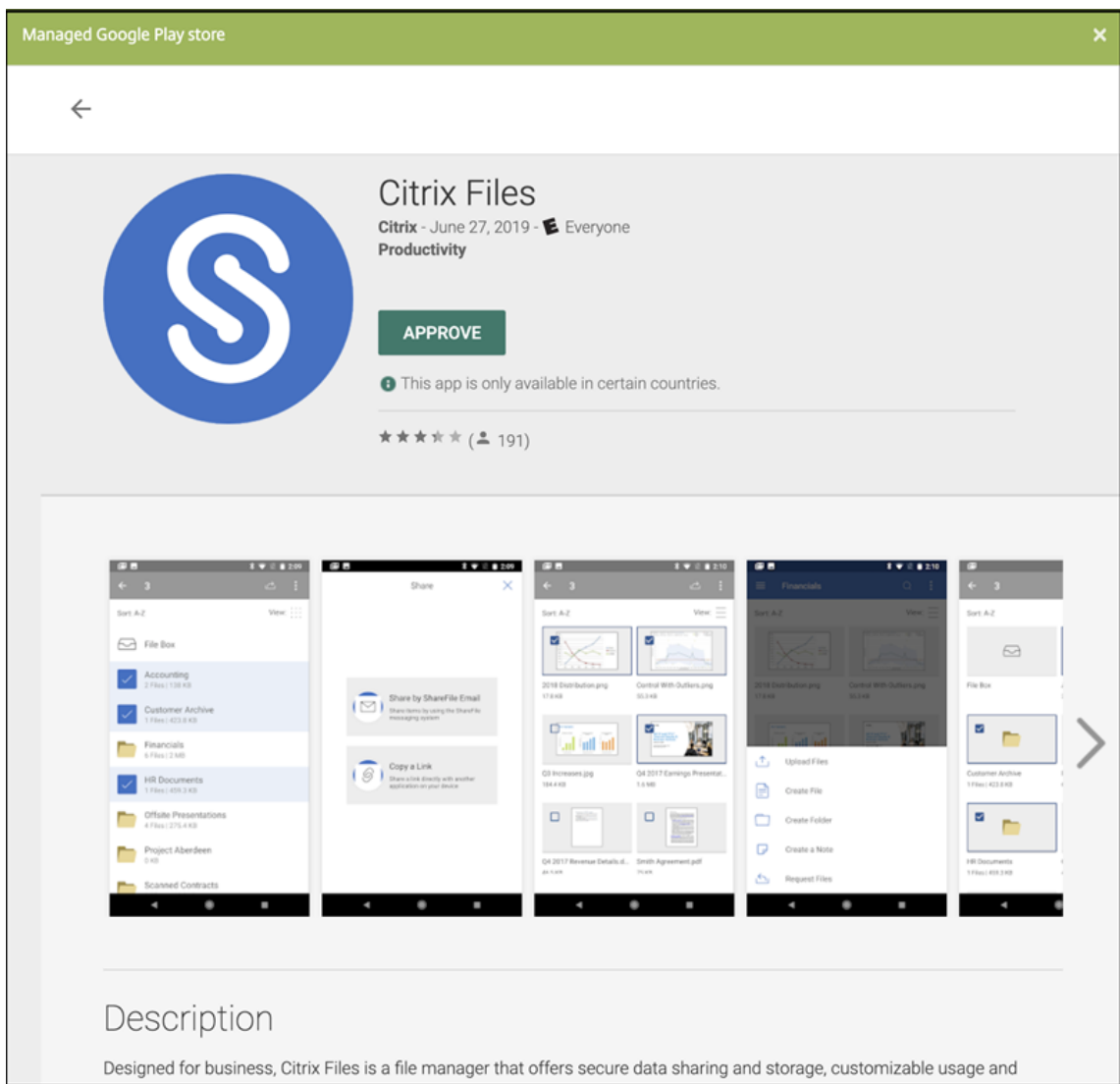
- MDX**  
Apps wrapped with the [MDX Service](#) to include app policies. You can deploy MDX apps obtained from internal and public stores.  
Example: Secure Mail
- Public App Store**  
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.  
Example: GoToMeeting
- Web & SaaS**  
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.  
Example: GoogleApps\_SAML
- Enterprise**  
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.  
Example: Quick-iLaunch
- Web Link**  
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Click **MDX**. The **App Information** page appears.
4. On the left side of the page, select **Android Enterprise** as the platform.
5. On the **App Information** page, type the following information:
  - **Name:** Type a descriptive name for the app. This name appears under **App Name** on the **Apps** table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see [About app categories](#).

6. Click **Next**. The **Android Enterprise MDX App** page appears.
7. Click **Upload** and navigate to the file location of the .mdx files for the app. Select the file and click **Open**.
8. The UI notifies you if the attached application requires approval from the managed Google Play store. To approve the application without leaving the Citrix Endpoint Management console, click **Yes**.



9. When the managed Google Play store page opens, click **Approve**.



10. Click **Approve** again.
11. Select **Keep approved when app requests new permissions**. Click **Save**.



The screenshot shows the 'Approval Settings' for the Podio app. At the top, there are two tabs: 'Approval Settings' (active) and 'Notifications'. Below the tabs, the Podio logo is displayed next to the text 'Podio' and 'Podio ApS'. The main heading asks, 'How would you like to handle new app permission requests?'. There are two radio button options: the first is selected and reads 'Keep approved when app requests new permissions. Users will be able to install the updated app.'; the second is unselected and reads 'Revoke app approval when this app requests new permissions. App will be removed from the store until it is reapproved.' A green 'Done' button is located in the bottom right corner.

12. When the app is approved and saved, more settings appear on the page. Configure these settings:
  - **File name:** Type the file name associated with the app.
  - **App Description:** Type a description for the app.
  - **Product track:** Specify which product track you want to push to user devices. If you have a track designed for testing, you can select and assign it to your users. The default is Production.
  - **App version:** Optionally, type the app version number.
  - **Package ID:** The URL of the app in the Google Play store.
  - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
  - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
  - **Excluded devices:** Optionally, type the manufacturer or models of devices that cannot run the app.
13. Configure the **MDX Policies**. For more information about app policies for MDX apps, see [MDX Policies at a Glance](#) and [MAM SDK overview](#).
14. Configure the deployment rules. For information, see [Deploy resources](#).
15. Expand **Store Configuration**. This setting doesn't apply to Android Enterprise apps, which appear only in managed Google Play.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

Allow app comments

Optionally, you can add an FAQ for the app or screen captures that appear in the app store. You can also set whether users can rate or comment on the app.

- Configure these settings:
  - **App FAQ:** Add FAQ questions and answers for the app.
  - **App screenshots:** Add screen captures to help classify the app in the app store. The graphic you upload must be a PNG. You cannot upload a GIF or JPEG image.
  - **Allow app ratings:** Select whether to permit a user to rate the app. The default is **On**.
  - **Allow app comments:** Select whether to permit users to comment about the selected app. The default is **On**.

16. Click **Next**. The **Approvals** page appears.

The screenshot displays the Citrix Endpoint Management console interface. At the top, there are navigation tabs: Device Policies, Apps, Media, Actions, ShareFile, Enrollment Profiles, and Delivery Groups. The 'Apps' tab is active, showing a configuration page for an MDX app. The left sidebar contains a navigation menu with the following items: 1 App Information, 2 Platform, 3 Approvals (optional) (highlighted), and 4 Delivery Group Assignments (optional). The main content area is titled 'Approvals (optional)' and includes the instruction: 'Apply an existing workflow or create a new workflow to require approval before allowing users to access the app.' Below this instruction is a 'Workflow to Use' dropdown menu currently set to 'None'.

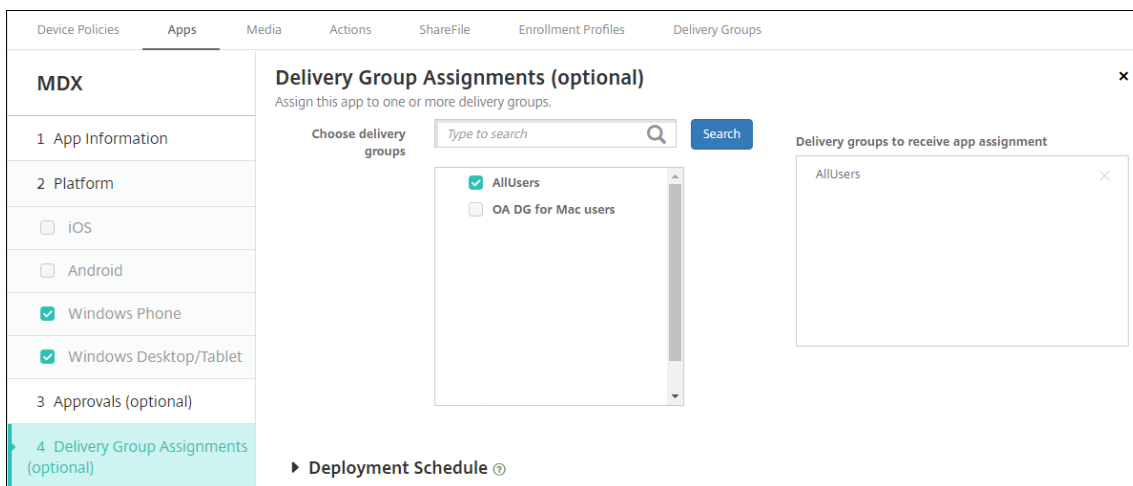
You use workflows when you need approval when creating user accounts. If you don't want to set up approval workflows, you can skip to Step 15.

Configure these settings to assign or create a workflow:

- **Workflow to Use:** In the list, click an existing workflow or click **Create a new workflow**. The default is **None**.
- If you select **Create a new workflow**, configure these settings. For more information, see [Create and manage workflows](#).
- **Name:** Type a unique name for the workflow.
- **Description:** Optionally, type a description for the workflow.
- **Email Approval Templates:** In the list, select the email approval template to be assigned. When you click the eye icon to the right of this field, a dialog box appears where you can preview the template.
- **Levels of manager approval:** In the list, select the number of levels of manager approval required for this workflow. The default is 1 level. Possible options are:
  - Not Needed
  - 1 level
  - 2 levels
  - 3 levels
- **Select Active Directory domain:** In the list, select the appropriate Active Directory domain to be used for the workflow.
- **Find additional required approvers:** Type the name of the additional required person in the search field and then click **Search**. Names originate in Active Directory.
- When the name appears in the field, select the check box next to the name. The name and email address appear in the **Selected additional required approvers** list.
  - To remove a person from the **Selected additional required approvers** list, do one of the following:
    - \* Click **Search** to see a list of all the persons in the selected domain.

- \* Type a full or partial name in the search box, and then click **Search** to limit the search results.
- \* Persons in the **Selected additional required approvers** list have check marks next to their name in the search results list. Scroll through the list and clear the check box next to each name you want to remove.

17. Click **Next**. The **Delivery Group Assignment** page appears.



18. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.

19. Expand **Deployment Schedule** and then configure the following settings:

- Next to **Deploy**, click **On** to schedule deployment or click **Off** to prevent deployment. The default option is **On**.
- Next to Deployment schedule, click **Now** or **Later**. The default option is **Now**.
- If you click **Later**, click the calendar icon and then select the date and time for deployment.
- Next to **Deployment condition**, click **On every connection** or click **Only when previous deployment has failed**. The default option is **On every connection**.
- Next to **Deploy for always-on connection**, ensure that **Off** is selected. The default option is **Off**. The always-on connections are not available for Android Enterprise to customers who began using Endpoint Management with version 10.18.19 or later. We don't recommend the connections for customers who began using Endpoint Management before version 10.18.19.

This option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.

The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

20. Click **Save**.

Repeat the steps for each mobile productivity app.

### Configure security challenge policy

The Endpoint Management Passcode device policy configures security challenge rules. The challenges appear when users access their devices or the Android Enterprise work profiles on their devices. A security challenge can be a passcode or biometric recognition. For more information about the Passcode policy, see [Passcode device policy](#).

- If your Android Enterprise deployment includes BYOD devices, configure the passcode policy for the work profile.
- If your deployment includes, company-owned, fully managed devices, configure the passcode policy for the device itself.
- If your deployment includes both types of devices, configure both types of passcode policy.

To configure the passcode policy:

1. In the Endpoint Management console, go to **Configure > Device Policies**.
2. Click **Add**.
3. Click **Show filter** to show the **Policy Platform** pane. In the **Policy Platform** pane, select **Android Enterprise**.
4. Click **Passcode** on the right pane.

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles
<b>Policy Platform</b> <span>Clear All</span>		<b>Add a New Policy</b> <span>Hide filter</span>			
<input type="checkbox"/>	iOS	10			
<input type="checkbox"/>	Windows Desktop/Tablet	11			
<input type="checkbox"/>	Android	11			
<input type="checkbox"/>	macOS	8			
<input type="checkbox"/>	Windows Mobile/CE	8			
<input type="checkbox"/>	Windows Phone	9			
<input checked="" type="checkbox"/>	Android Enterprise	17			
			<b>Policies most often used</b>		
			Exchange		
			Location		
			Passcode		
			Restrictions		
			Scheduling		

1. Enter a **Policy Name**. Click **Next**.

The screenshot shows the Citrix Endpoint Management console interface for configuring a Passcode Policy. The top navigation bar includes tabs for Device Policies, Apps, Media, Actions, ShareFile, Enrollment Profiles, and Delivery Groups. The left sidebar is titled 'Passcode Policy' and contains a list of configuration steps: '1 Policy Info' (highlighted), '2 Platforms' (with a 'Clear All' link), and a list of operating systems: iOS, macOS, Android, Samsung KNOX, and Android Enterprise (checked). The main content area is titled 'Policy Information' and contains a description: 'This policy creates a passcode policy based on the standards of your organization rules, such as the grace period before device lock.' Below the description, there is a 'Policy Name \*' field with the value 'Passcode - AE' and a 'Description' field which is currently empty.

2. Configure the Passcode policy settings.
  - Set **Device passcode required** to **On** to see the settings available for security challenges for the device itself.
  - Set **Work profile security challenge** to **On** to see the settings available for work profile security challenges.
3. Click **Next**.
4. Assign the policy to one or more delivery groups.
5. Click **Save**.

## Creating enrollment profiles

Enrollment profiles control how Android devices are enrolled if Android Enterprise is enabled for your Endpoint Management deployment. When you create an enrollment profile to enroll Android Enterprise devices, you can configure the enrollment profile to enroll new and factory reset devices as:

- Fully managed devices
- Dedicated devices
- Fully managed devices with a work profile/Work profile on corporate-owned devices

You can also configure each of these Android Enterprise enrollment profiles to enroll BYOD Android devices as work profile devices.

If Android Enterprise is enabled for your Endpoint Management deployment, all newly enrolled or reenrolled Android devices are enrolled as Android Enterprise devices. By default, the Global enrollment profile enrolls new and factory reset Android devices as fully managed devices and enrolls BYOD Android devices as work profile on corporate-owned devices.

When you create enrollment profiles, you assign delivery groups to them. If a user belongs to multiple delivery groups that have different enrollment profiles, the name of the delivery group determines the enrollment profile used. Endpoint Management selects the delivery group that appears last in an alphabetized list of delivery groups. For more information, see [Enrollment profiles](#).

### Add an enrollment profile for fully managed devices

The Global enrollment profile enrolls fully managed devices by default, but you can create more enrollment profiles to enroll fully managed devices.

1. In the Endpoint Management console, go to **Configure > Enrollment Profiles**.
2. To add an enrollment profile, click **Add**. In the Enrollment Info page, type a name for the enrollment profile.
3. Set the number of devices that members with this profile can enroll.
4. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
5. Set **Management** to **Android Enterprise**.
6. Set **Device owner mode** to **Company-owned device**.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<p><b>Workspace integration</b> ⓘ</p> <p>Enrollment through Workspace app <input type="checkbox"/> ⓘ</p>
Android	<p><b>Device management</b> ⓘ</p> <p>Management <input checked="" type="radio"/> Android Enterprise ⓘ  <input type="radio"/> Legacy device administration (not recommended) ⓘ  <input type="radio"/> Do not manage devices ⓘ</p> <p>Device owner mode <input checked="" type="radio"/> Company-owned device ⓘ  <input type="radio"/> Fully managed with work profile / Work profile on corporate-owned devices ⓘ  <input type="radio"/> Dedicated device ⓘ  <input type="radio"/> None ⓘ</p> <p>BYOD work profile <input checked="" type="checkbox"/> ⓘ</p>
iOS	<p><b>Application management</b> ⓘ</p> <p>Citrix MAM <input checked="" type="checkbox"/> ⓘ</p>
Windows	<p><b>User consent</b></p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ⓘ</p>
3 Assignment (optional)	

7. **BYOD work profile** allows you to configure the enrollment profile to enroll BYOD devices as work profile devices. New and factory reset devices are enrolled as fully managed devices. Set **BYOD work profile** to **On** to allow enrollment of BYOD devices as work profile devices. Set **BYOD work profile** to **Off** to restrict enrollment to fully managed devices. Default is **On**.
8. Choose whether to enroll devices in Citrix MAM.
9. If you set **BYOD work profile** to **On**, configure user consent. To allow users of BYOD work profile devices to decline device management when they enroll their devices, set **Allow users to decline device management** to **On**.  
  
If **BYOD work profile** is set to **On**, the default value of **Allow users to decline device management** is **On**. If **BYOD work profile** is set to **Off**, then **Allow users to decline device management** is disabled.
10. Select **Assignment (options)**. The Delivery Group Assignment screen appears.
11. Choose the delivery group or delivery groups containing the administrators who enroll fully managed devices. Then click **Save**.

The Enrollment Profile page appears with the profile you added.

### **Add a dedicated device enrollment profile**

When your Endpoint Management deployment includes dedicated devices, a single Endpoint Management administrator or small group of administrators enroll many dedicated devices. To ensure that these administrators can enroll all the devices required, create an enrollment profile for them with unlimited devices allowed per user.

1. In the Endpoint Management console, go to **Configure > Enrollment Profiles**.
2. To add an enrollment profile, click **Add**. In the Enrollment Info page, type a name for the enrollment profile. Set to **Unlimited** the number of devices members with this profile can enroll.
3. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
4. Set **Management** to **Android Enterprise**.
5. Set **Device owner mode** to **Dedicated device**.



Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<p><b>Workspace integration</b> ⓘ</p> <p>Enrollment through Workspace app <input type="checkbox"/> ⓘ</p> <p><b>Device management</b> ⓘ</p> <p>Management <input checked="" type="radio"/> Android Enterprise ⓘ  <input type="radio"/> Legacy device administration (not recommended) ⓘ  <input type="radio"/> Do not manage devices ⓘ</p> <p>Device owner mode <input type="radio"/> Company-owned device ⓘ  <input type="radio"/> Fully managed with work profile / Work profile on corporate-owned devices ⓘ  <input checked="" type="radio"/> Dedicated device ⓘ  <input type="radio"/> None ⓘ</p> <p>BYOD work profile <input checked="" type="checkbox"/> ⓘ</p> <p><b>Application management</b> ⓘ</p> <p>Citrix MAM <input checked="" type="checkbox"/> ⓘ</p> <p><b>User consent</b></p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ⓘ</p>
Android	
iOS	
Windows	
3 Assignment (optional)	

6. **BYOD work profile** allows you to configure the enrollment profile to enroll BYOD devices as work profile devices. New and factory reset devices are enrolled as dedicated devices. Set **BYOD work profile** to **On** to allow enrollment of BYOD devices as work profile devices. Set **BYOD work profile** to **Off** to restrict enrollment to company-owned devices. Default is **On**.

7. Choose whether to enroll devices in Citrix MAM.

8. If you set **BYOD work profile** to **On**, configure user consent. To allow users of BYOD work profile devices to decline device management when they enroll their devices, set **Allow users to decline device management** to **On**.

If **BYOD work profile** is set to **On**, the default value of **Allow users to decline device management** is **On**. If **BYOD work profile** is set to **Off**, then **Allow users to decline device management** is disabled.

9. Select **Assignment (options)**. The Delivery Group Assignment screen appears.

10. Choose the delivery group or delivery groups containing the administrators who enroll dedicated devices. Then click **Save**.

The Enrollment Profile page appears with the profile you added.

### Add an enrollment profile for fully managed devices with a work profile / work profile on corporate-owned devices

1. In the Endpoint Management console, go to **Configure > Enrollment Profiles**.

2. To add an enrollment profile, click **Add**. In the Enrollment Info page, type a name for the enrollment profile.
3. Set the number of devices that members with this profile can enroll.
4. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
5. Set **Management** to **Android Enterprise**. Set **Device owner mode** to **Fully managed with work profile / Work profile on corporate-owned devices**.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<b>Workspace integration</b> ⓘ Enrollment through Workspace app <input type="checkbox"/> ⓘ
Android	<b>Device management</b> ⓘ Management <input checked="" type="radio"/> Android Enterprise ⓘ <input type="radio"/> Legacy device administration (not recommended) ⓘ <input type="radio"/> Do not manage devices ⓘ
iOS	Device owner mode <input type="radio"/> Company-owned device ⓘ <input checked="" type="radio"/> Fully managed with work profile / Work profile on corporate-owned devices ⓘ <input type="radio"/> Dedicated device ⓘ <input type="radio"/> None ⓘ
Windows	BYOD work profile <input checked="" type="checkbox"/> ⓘ
3 Assignment (optional)	<b>Application management</b> ⓘ Citrix MAM <input checked="" type="checkbox"/> ⓘ
	<b>User consent</b> Allow users to decline device management <input checked="" type="checkbox"/> ⓘ

6. **BYOD work profile** allows you to configure the enrollment profile to enroll BYOD devices as work profile devices. New and factory reset devices are enrolled as fully managed devices with a work profile. Set **BYOD work profile** to **On** to allow enrollment of BYOD devices as work profile devices. Set **BYOD work profile** to **Off** to restrict enrollment to dedicated devices. Default is **Off**.
7. Choose whether to enroll devices in Citrix MAM.
8. If you set **BYOD work profile** to **On**, configure user consent. To allow users of BYOD work profile devices to decline device management when they enroll their devices, set **Allow users to decline device management** to **On**.  
  
 If **BYOD work profile** is set to **On**, the default value of **Allow users to decline device management** is **On**. If **BYOD work profile** is set to **Off**, then **Allow users to decline device management** is disabled.
9. Select **Assignment (options)**. The Delivery Group Assignment screen appears.

10. Choose the delivery group or delivery groups containing the administrators who enroll fully managed devices with a work profile. Then click **Save**.

The Enrollment Profile page appears with the profile you added.

### **Adding an enrollment profile for legacy devices**

Google deprecated the device administrator mode of device management. Google encourages customers to manage all Android devices in device owner mode or profile owner mode. (See [Device admin deprecation](#) in the Google Android Enterprise developer guides.)

To support this change:

- Citrix made Android Enterprise the default enrollment option for Android devices.
- If Android Enterprise is enabled for your Endpoint Management deployment, all newly enrolled or re-enrolled Android devices are enrolled as Android Enterprise devices.

Your organization might not be ready to begin managing legacy Android devices using Android Enterprise. In that case, you can continue to manage them in device administrator mode. For devices already enrolled in device administrator mode, Endpoint Management continues to manage them in device administrator mode.

Create an enrollment profile for legacy devices to allow new Android device enrollments to use device administrator mode.

To create an enrollment profile for legacy devices:

1. In the Endpoint Management console, go to **Configure > Enrollment Profiles**.
2. To add an enrollment profile, click **Add**. In the Enrollment Info page, type a name for the enrollment profile.
3. Set the number of devices that members with this profile can enroll.
4. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
5. Set **Management** to **Legacy device administration (not recommended)**. Click **Next**.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<p><b>Workspace integration</b> ?</p> <p>Enrollment through Workspace app <input type="checkbox"/> x ?</p> <p><b>Device management</b> ?</p> <p>Management <input type="radio"/> Android Enterprise ?</p> <p><input checked="" type="radio"/> Legacy device administration (not recommended) ?</p> <p><input type="radio"/> Do not manage devices ?</p> <p><b>Application management</b> ?</p> <p>Citrix MAM <input checked="" type="checkbox"/> ?</p> <p><b>User consent</b></p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ?</p>
<b>Android</b>	
iOS	
Windows	
3 Assignment (optional)	

- Choose whether to enroll devices in Citrix MAM.
- To allow users to decline device management when they enroll their devices, set **Allow users to decline device management** to **On**. Default is **On**.
- Select **Assignment (options)**. The Delivery Group Assignment screen appears.
- Choose the delivery group or delivery groups containing the administrators who enroll dedicated devices. Then click **Save**.

The Enrollment Profile page appears with the profile you added.

To continue managing legacy devices in device administrator mode, enroll or re-enroll them using this profile. You enroll device administrator devices similar to work profile devices, by having users download Secure Hub and providing an enrollment server URL.

### Provisioning Android Enterprise work profile devices

Android Enterprise work profile devices are enrolled in profile owner mode. These devices do not need to be new or factory reset. BYOD devices are enrolled as work profile devices. The enrollment experience is similar to Android enrollment in Endpoint Management. Users download Secure Hub from Google Play and enroll their devices.

By default, the **USB Debugging and Unknown Sources** settings get disabled on a device when you enroll the device in Android Enterprise as a work profile device.

When enrolling devices in Android Enterprise as work profile devices, always go to Google Play. From there, enable Secure Hub to appear in the user's personal profile.

## Provisioning Android Enterprise fully managed devices

You can enroll fully managed devices in the deployment you set up in the previous sections. Fully managed devices are company-owned devices and are enrolled in device owner mode. Only new or factory reset devices can be enrolled in device owner mode.

You can enroll devices in device owner mode using any of these enrollment methods:

- **DPC identifier token:** With this enrollment method, users enter the characters `afw##xenmobile` when setting up the device. `afw##xenmobile` is the Citrix DPC identifier token. This token identifies the device as managed by Endpoint Management and downloads Secure Hub from the Google Play store. See Enrolling devices using the Citrix DPC identifier token.
- **Near field communication (NFC) bump:** The NFC bump enrollment method transfers data through between two devices using near-field communication. Bluetooth, Wi-Fi, and other communication modes are disabled on a new or factory-reset device. NFC is the only communication protocol that the device can use in this state. See Enrolling devices with NFC bump.
- **QR code:** QR code enrollment can be used to enroll a distributed fleet of devices that do not support NFC, such as tablets. The QR code enrollment method sets up and configures device profile mode by scanning a QR code from the setup wizard. See Enrolling devices using a QR code.
- **Zero-touch:** Zero-touch enrollment allows you to configure devices to enroll automatically when they are first powered on. Zero-touch enrollment is supported on some Android devices running Android 8.0 or later. See Zero-touch enrollment.
- **Google Accounts:** Users enter their Google Account credentials to initiate the provisioning process. This option is for enterprises using Google Workspace.

### Enrolling devices using the Citrix DPC identifier token

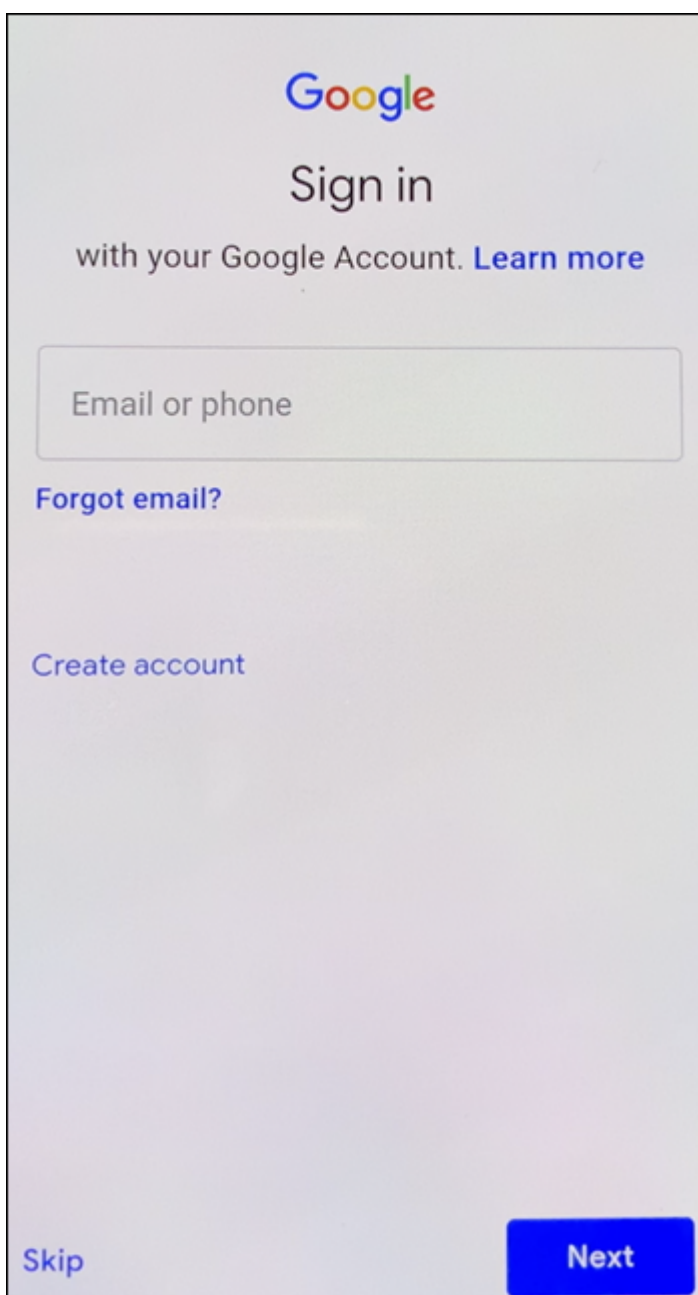
Users enter `afw##xenmobile` when prompted to enter a Google account after powering on new or factory reset devices for initial setup. This action downloads and installs Secure Hub. Users then follow the Secure Hub set-up prompts to complete the enrollment.

### System requirements

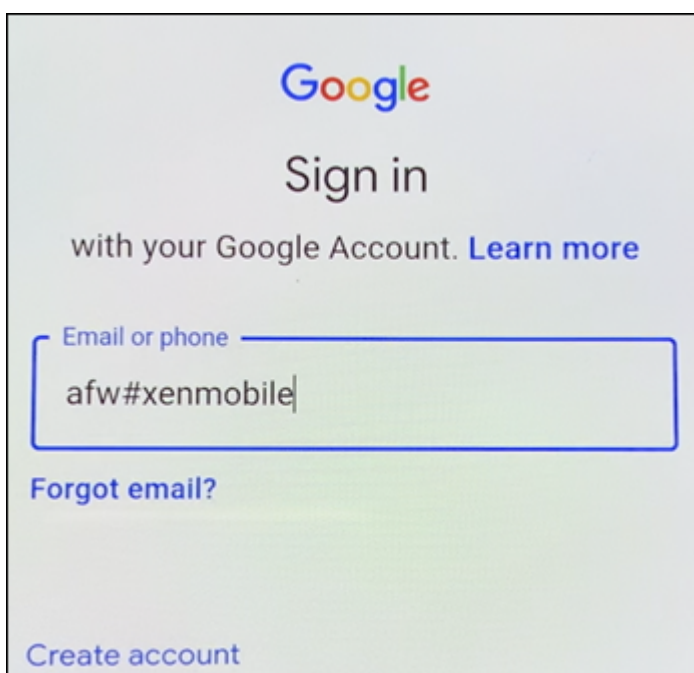
- Supported on all Android devices running the Android OS.

### To enroll the device

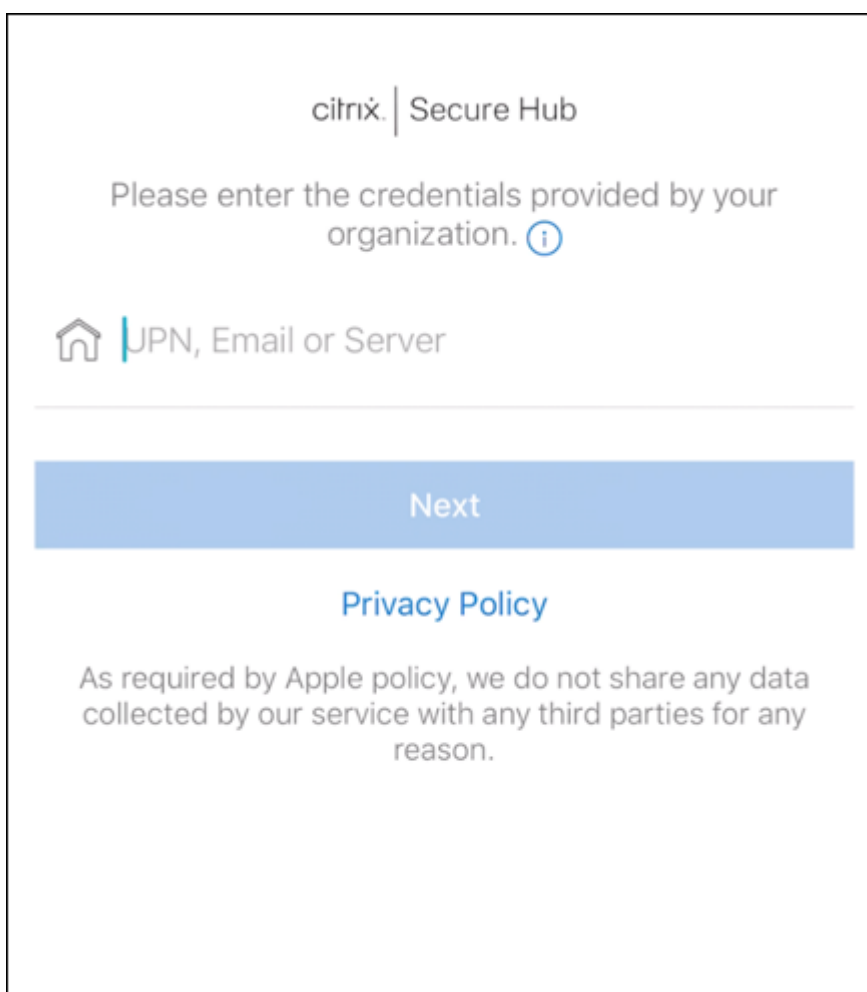
1. Power on a new or factory reset device.
2. The initial device setup loads and prompts for a Google account. If the device loads the home screen of the device, check the notification bar for a **Finish Setup** notification.



3. Enter `afw##xenmobile` in the **Email or phone** field.

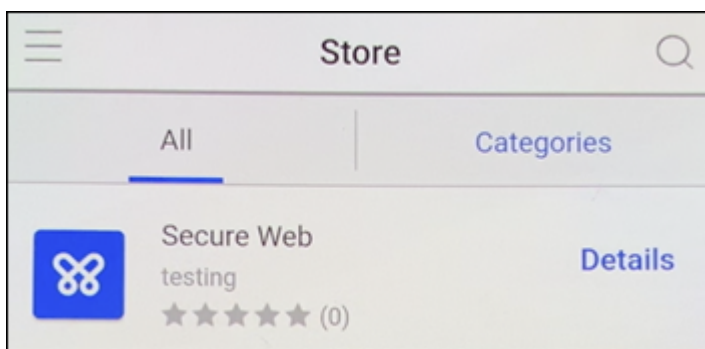


4. Tap **Install** on the Android Enterprise screen prompting to install Secure Hub.
5. Tap **Install** on the Secure Hub installer screen.
6. Tap **Allow** for all app permission requests.
7. Tap **Accept & Continue** to install Secure Hub and allow it to manage the device.
8. Secure Hub is now installed and on the default enrollment screen. In this example, AutoDiscovery is not set up. If it was, the user can enter their username/email and a server would be found for them. Instead, enter the enrollment URL for the environment and tap **Next**.

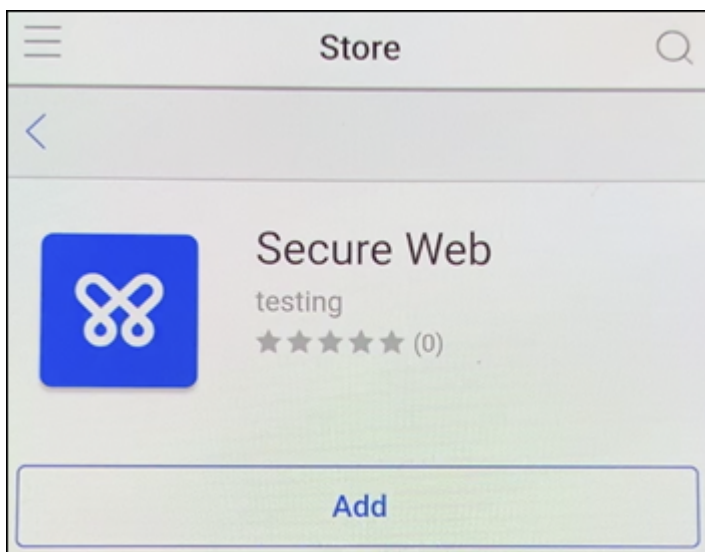


9. The default configuration for Endpoint Management allows users to choose if they use MAM or MDM+MAM. If prompted in this way, tap **Yes, Enroll** to choose MDM+MAM.
10. Enter the user email address and password, then tap **Next**.
11. The user is prompted to configure a device passcode. Tap **Set** and enter a passcode.
12. The user is prompted to configure a work profile unlock method. For this example, tap **Password**, tap **PIN**, and enter a PIN.
13. The device is now on the Secure Hub **My Apps** landing screen. Tap **Add apps from Store**.
14. To add Secure Web, tap **Secure Web**.

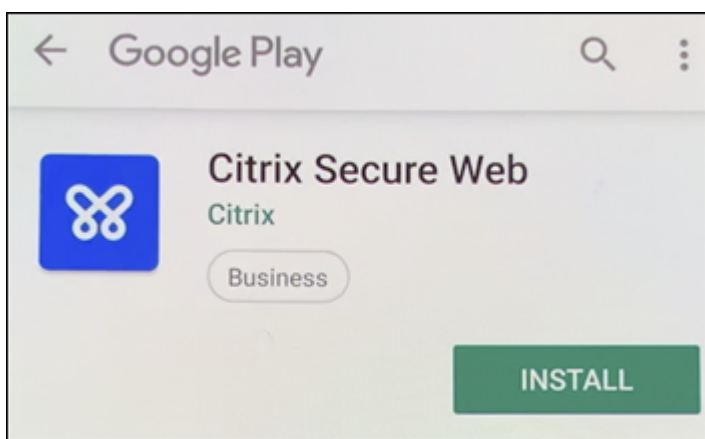




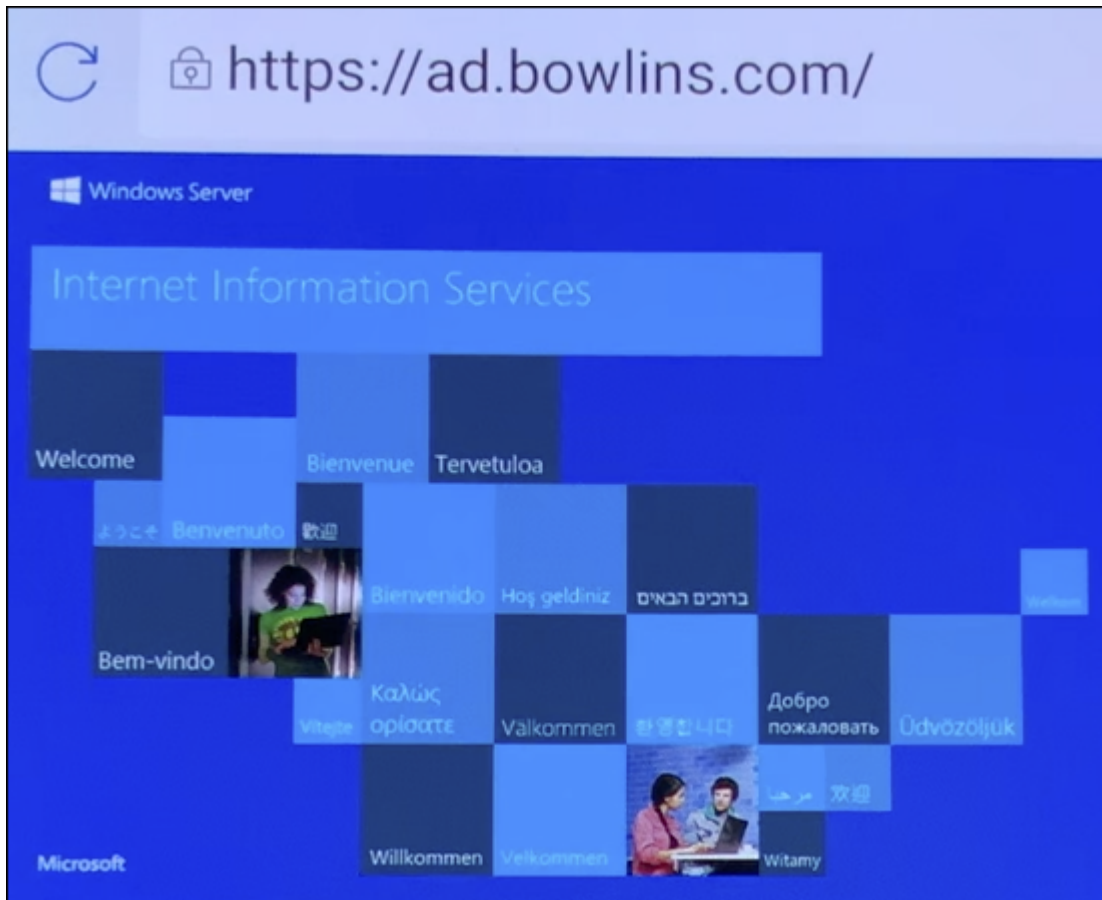
15. Tap **Add**.



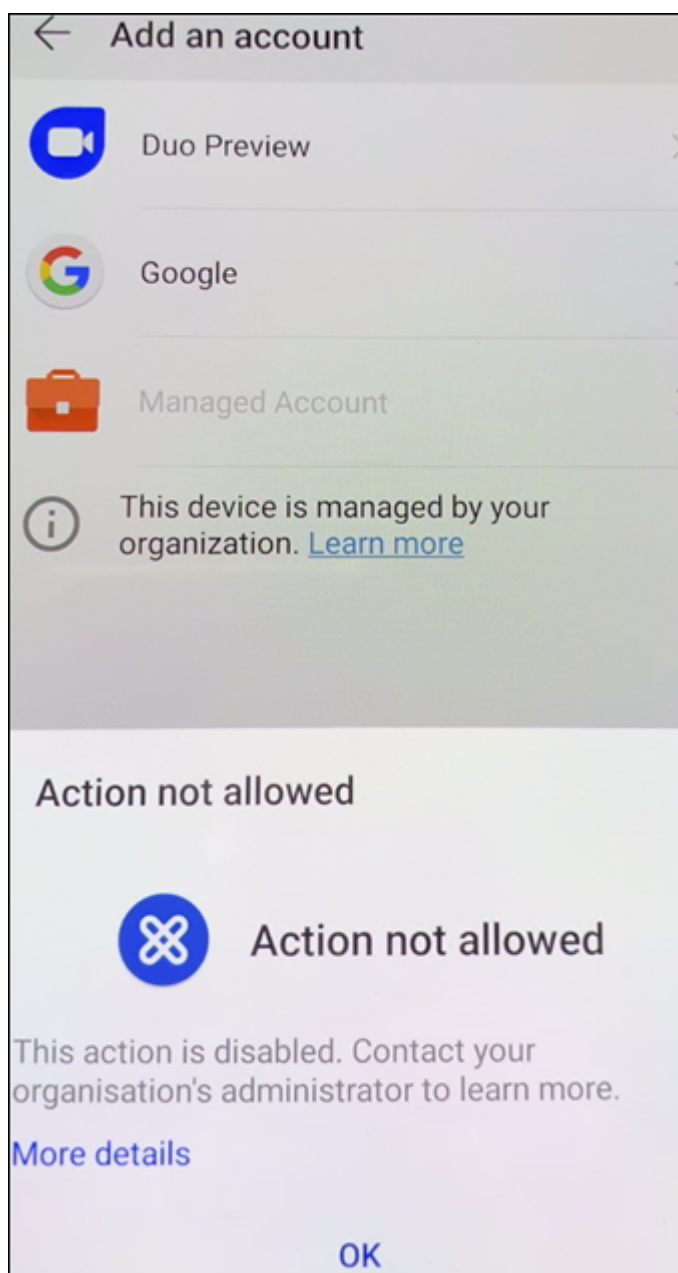
16. Secure Hub directs the user to the Google Play store to install Secure Web. Tap **Install**.



17. After Secure Web is installed, tap **Open**. Enter a URL from an internal site in the address bar and verify that the page loads.



18. Go to **Settings > Accounts** on the device. Observe that the **Managed Account** can't be modified. The developer options for sharing screen or remote debugging are also blocked.



### Enrolling devices with NFC bump

To enroll a device as a fully managed device using NFC bumps requires two devices: One that is reset to its factory settings and one running the Endpoint Management Provisioning Tool.

### System requirements and prerequisites

- Supported Android devices.
- A new or factory-reset device with NFC capability, provisioned for Android Enterprise as a fully managed device. See the section on [Provisioning Android Enterprise fully managed devices](#).

- Another device with NFC capability, running the configured Provisioning Tool. The Provisioning Tool is available in Secure Hub or on the [Citrix downloads page](#).

Each device can have only one Android Enterprise profile. In this case, the profile is for managed Secure Hub. Attempting to add a second DPC app removes the installed Secure Hub.

### **Data transferred through the NFC bump**

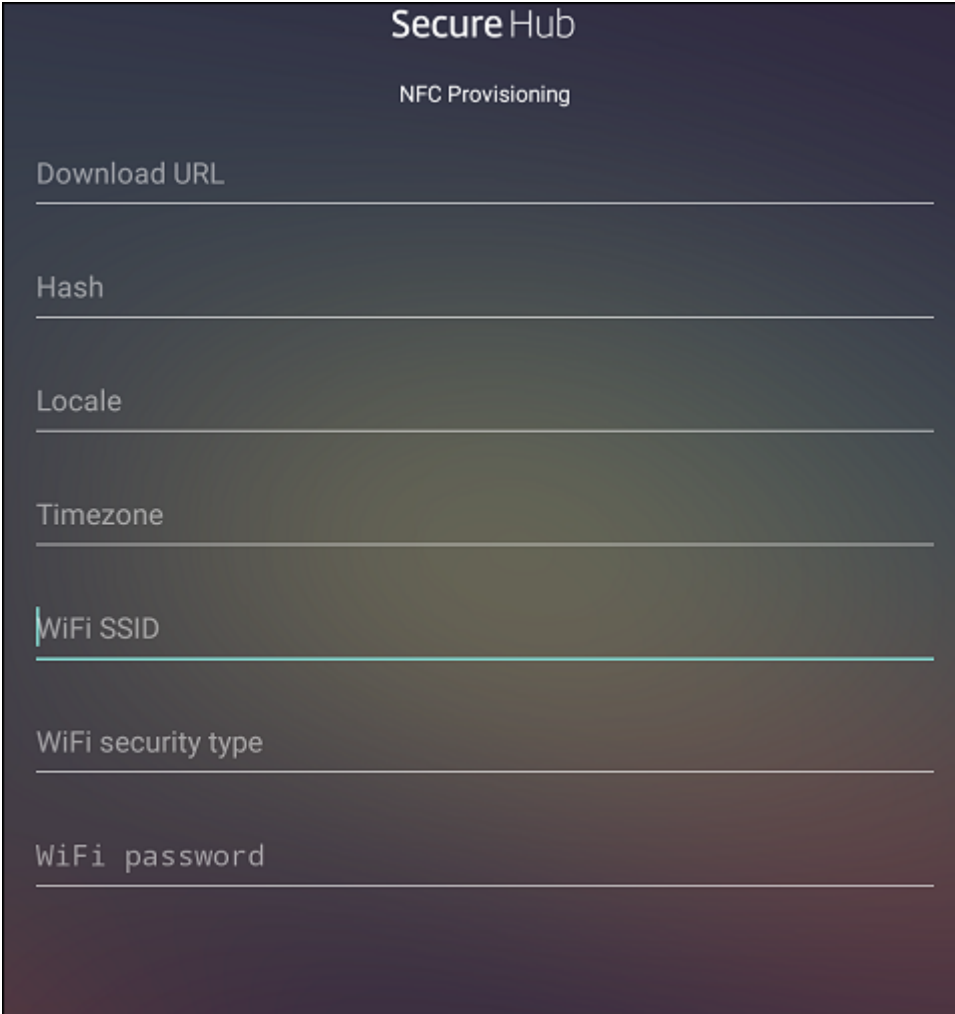
Provisioning a factory-reset device requires you to send the following data through an NFC bump to initialize Android Enterprise:

- Package name of the DPC app that acts as device owner (in this case, Secure Hub).
- Intranet/Internet location from which the device can download the DPC app.
- SHA-256 hash of the DPC app to verify if the download is successful.
- Wi-Fi connection details so that a factory-reset device can connect and download the DPC app.  
Note: Android now does not support 802.1x Wi-Fi for this step.
- Time zone for the device (optional).
- Geographic location for the device (optional).

When the two devices are bumped, the data from the Provisioning Tool is sent to the factory-reset device. That data is then used to download Secure Hub with administrator settings. If you don't enter time zone and location values, Android automatically configures the values on the new device.

### **Configuring the Endpoint Management Provisioning Tool**

Before doing an NFC bump, you must configure the Provisioning Tool. This configuration is then transferred to the factory-reset device during the NFC bump.



The image shows a dark-themed mobile application interface titled "Secure Hub" with a subtitle "NFC Provisioning". Below the title are seven input fields, each with a label and a horizontal line for text entry. The labels are: "Download URL", "Hash", "Locale", "Timezone", "WiFi SSID", "WiFi security type", and "WiFi password". The "WiFi SSID" field has a blue vertical bar on its left side.

You can type data into the required fields or populate them by using a text file. The steps in the next procedure describe how to configure the text file with descriptions for each field. The app doesn't save information after you type it, so you might want to create a text file to keep the information for future use.

### **To configure the Provisioning Tool by using a text file**

Name the file `nfcprovisioning.txt` and place the file in the `/sdcard/` folder on the SD card of the device. The app can then read the text file and populate the values.

The text file must contain the following data:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<
download_location>
```

This line is the intranet/internet location of the EMM provider app. After the factory-reset device connects to Wi-Fi following the NFC bump, the device must have access to this location for downloading. The URL is a regular URL, with no special formatting required.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>
```

This line is the checksum of the EMM provider app. This checksum is used to verify that the download is successful. Steps to obtain the checksum are discussed later in this article.

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

This line is the connected Wi-Fi SSID of the device on which the Provisioning Tool is running.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

Supported values are WEP and WPA2. If the Wi-Fi is unprotected, this field must be empty.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

If the Wi-Fi is unprotected, this field must be empty.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

Enter language and country codes. The language codes are two-letter lowercase ISO language codes (such as en) as defined by [ISO 639-1](#). The country codes are two-letter uppercase ISO country codes (such as US) as defined by [ISO 3166-1](#). For example, type en\_US for English as spoken in the United States. If you don't type any codes, the country and language are automatically populated.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

The time zone in which the device is running. Type the [database name of the area/location](#). For example, type **America/Los\_Angeles** for Pacific time. If you don't type a name, the time zone automatically populates.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

This data isn't required, because the value is hardcoded into the app as Secure Hub. It's mentioned here only for the sake of completion.

If there is a Wi-Fi protected by using WPA2, a completed nfcprovisioning.txt file might look like the following:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crh\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
```

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
```

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

If there is an unprotected Wi-Fi, a completed `nfcprovisioning.txt` file might look like the following:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crh
\u003d
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
android.app.extra.PROVISIONING_LOCALE=en_US
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

### To get the checksum of Citrix Secure Hub

The checksum of Secure Hub is a constant value: `qn7oZUtheu3JBAinzZRrjCQv6L006Ll10jcxT3-yKM`. To download an APK file for Secure Hub, use the following Google Play store link: <https://play.google.com/managed/downloadManagingApp?identifier=xenmobile>.

### To get an app checksum

Prerequisites:

- The **apksigner** tool from the Android SDK Build Tools
- OpenSSL command line

To get the checksum of any app, follow these steps:

1. Download the app's APK file from the Google Play store.
2. In the OpenSSL command line, navigate to the **apksigner** tool: `android-sdk/build-tools/<version>/apksigner` and type the following:

```
1 apksigner verify -print-certs <apk_path> | perl -nle 'print $& if
   m{
2   (?<=SHA-256 digest:) .* }
3   ' | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
4 <!--NeedCopy-->
```

The command returns a valid checksum.

3. To generate the QR code, enter the checksum in the `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM` field. For example:

```
1 {
2
3   "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.
   zenprise/com.zenprise.configuration.AdminFunction",
```

```
4  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "
    qn7oZUtheu3JBainzZRrrjCQv6L006Ll10jcxT3-yKM",
5  "android.app.extra.
    PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
    play.google.com/managed/downloadManagingApp?identifier=xenmobile",
6  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
7
8      "serverURL": "https://supportability.xm.cloud.com"
9  }
10
11 }
12
13 <!--NeedCopy-->
```

### Libraries used

The Provisioning Tool uses the following libraries in its source code:

- v7 `appcompat` library, Design Support library, and v7 palette support library by Google under Apache license 2.0  
For information, see [Support Library Features Guide](#).
- `Butter Knife` by Jake Wharton under Apache license 2.0

### Enrolling devices using a QR code

Users can enroll a fully managed device by using the QR code you generate for them.

### System requirements

Android devices that run Android 7.0 or later.

### Create a QR code

You generate a QR code by specifying enrollment information as needed. After you generate a QR code, save the QR code locally. Endpoint Management doesn't store it.



Settings > Android Enterprise QR Code

### Android Enterprise QR Code

Input the required information and click the button below to generate QR code for Android Enterprise enrollment.

Server FQDN:

User name:

Password:

Skip encryption:

Enable all system apps:

Skip user consent:

JSON output:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "qn7oZUtheu3JBainzZRrjCQv6LO06L10jcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
  "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
  "android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": false,
  "android.app.extra.PROVISIONING_SKIP_USER_CONSENT": true
}
```

1. Navigate to **Settings > Android Enterprise QR Code**.
2. If needed, specify the following enrollment information:
  - **Server FQDN:** Type the FQDN of the Endpoint Management server (for example, `example.cem.cloud.com`). This field is optional. If you leave it empty, users must populate this information when they enroll.
  - **User name:** Type the user name used to enroll. If you plan on distributing the QR code to multiple users, we recommend leaving this field empty. Configuring a QR code with a user name and password is useful for enrolling kiosk devices. If you leave the field empty, users must populate this information when they enroll.
  - **Password:** Type the password associated with the user name you typed. If you leave the field empty, users must populate this information when they enroll.
  - **Skip encryption:** If **On**, the device isn't encrypted during enrollment. The default is **Off**.
  - **Enable all system apps:** If **On**, allows access to all the system apps on the device. The default is **Off**.
  - **Skip user consent:** If **Off**, users can opt out of device management. The default is **Off**.

The **JSON output** box displays the JSON content that corresponds to the information you spec-

ified.

3. To add more enrollment information, edit the JSON content in the **JSON output** box.
4. Click **Generate QR Code**. The QR code appears to the right of the JSON output.
5. Right-click the QR code image and save it.
6. Send the image to the users for device enrollment.

A factory-reset device scans this QR code to enroll as a fully managed device.

### **To enroll the device**

After powering up a new or factory reset device:

1. Tap the screen six times on the welcome screen to launch the QR code enrollment flow.
2. When prompted, connect to Wi-Fi. The download location for Secure Hub in the QR code is accessible over this Wi-Fi network.

Once the device successfully connects to Wi-Fi, it downloads a QR code reader from Google and launches the camera.

3. Point the camera to the QR code to scan the code.

Android downloads Secure Hub from the download location in the QR code, validates the signing certificate signature, installs Secure Hub, and sets it as the device owner.

For more information, see this Google guide for Android EMM developers: [https://developers.google.com/android/work/prov-devices#qr\\_code\\_method](https://developers.google.com/android/work/prov-devices#qr_code_method).

### **Zero-touch enrollment**

Zero-touch enrollment lets you set up devices to provision themselves as fully managed devices when they are powered on for the first time.

Your device reseller creates an account for you on the Android zero-touch portal, an online tool that lets you apply configurations to devices. Using the Android zero-touch portal, you create one or more zero-touch enrollment configurations and apply the configurations to the devices assigned to your account. When your users power up these devices, the devices are automatically enrolled in Endpoint Management. The configuration assigned to the device defines its automatic enrollment process.

### **System requirements**

- Supported for zero-touch enrollment begins with Android 8.0.

### Devices and account information from your reseller

- Devices eligible for zero-touch enrollment are purchased from an enterprise reseller or Google partner. For a list of Android Enterprise zero-touch partners, see the [Android website](#).
- An Android Enterprise zero-touch portal account, created by your reseller.
- Android Enterprise zero-touch portal account login information, provided by your reseller.

### Create a zero-touch configuration

When you create a zero-touch configuration, include a custom JSON to specify details of the configuration.

Use this JSON to configure the device to enroll on the Endpoint Management server you specify. Substitute the URL of your server for 'URL' in this example.

```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4      {
5
6          "serverURL": "URL"
7      }
8
9      }
10
11 <!--NeedCopy-->
```

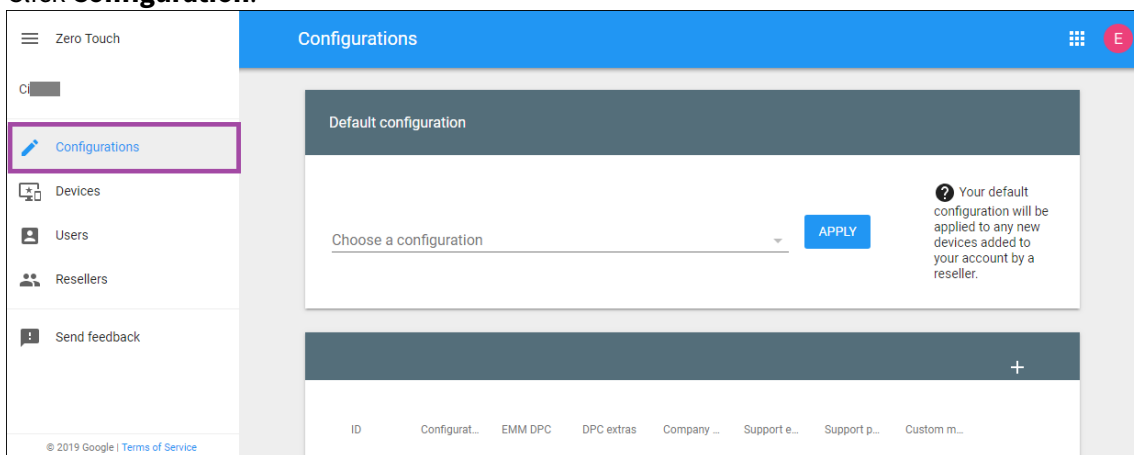
You can use an optional JSON with more parameters to further customize your configuration. This example specifies the Endpoint Management server and the user name and password that devices using this configuration use to log on to the server.

```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4      {
5
6          "serverURL": "URL",
7          "xm_username": "username",
8          "xm_password": "password"
9      }
10
11      }
12
13 <!--NeedCopy-->
```

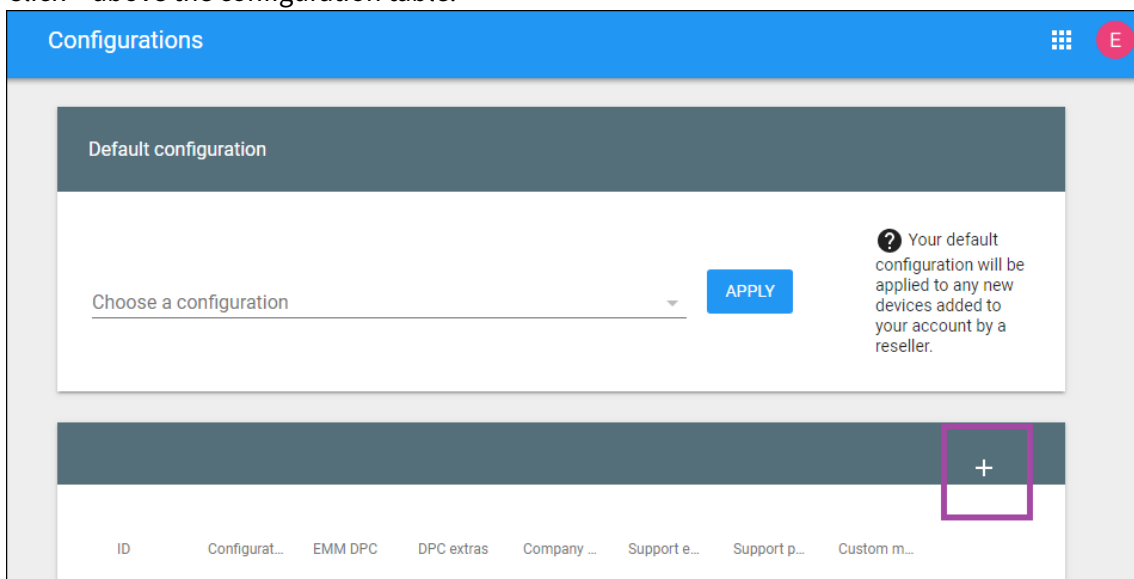
**Important:**

To enroll devices in the work profile on corporate-owned devices mode, add { "desiredProvisioningMode": "managedProfile" } to the custom JSON under PROVISIONING\_ADMIN\_EXTRAS\_BUNDLE

1. Go to the Android zero-touch portal at <https://partner.android.com/zerotouch>. Log in with the account information from your zero-touch device reseller.
2. Click **Configuration**.



3. Click + above the configuration table.



4. Enter your configuration information in the configuration window that appears.

**Add a new configuration**

Configuration name

EMM DPC

Select

DPC extras

Company name

Support email address

Support phone number

CANCEL ADD

- **Configuration name:** Type the name you choose for this configuration.
- **EMM DPC:** Choose **Citrix Secure Hub**.
- **DPC extras:** Paste your custom JSON text in this field.
- **Company name:** Type the name you want to appear on your Android Enterprise zero-touch devices during device provisioning.
- **Support email address:** Type an email address that your users can contact for help. This

address appears on your Android Enterprise zero-touch devices before device provisioning.

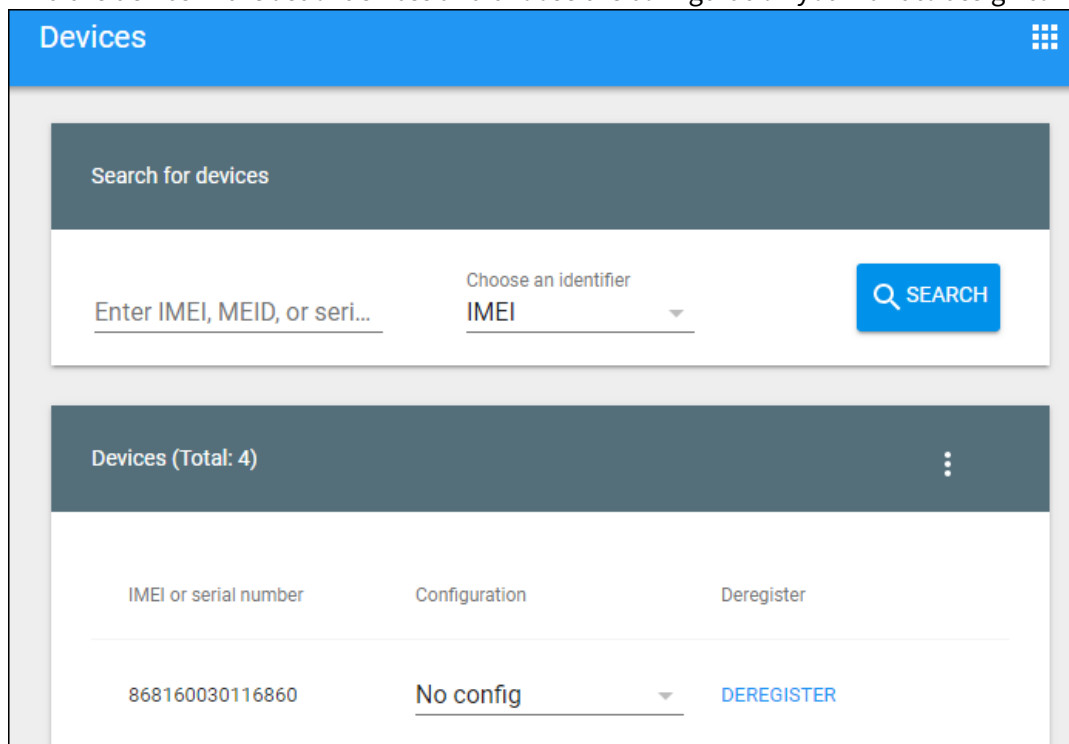
- **Support phone number:** Type a phone number that your users can contact for help. This phone number appears on your Android Enterprise zero-touch devices before device provisioning.
- **Custom Message:** Optionally, add one or two sentences to help your users contact you or give them more details about what’s happening to their device. This custom message appears on your Android Enterprise zero-touch devices before device provisioning.

5. Click **Add**.

6. To create more configurations, repeat steps 2 through 4.

7. To apply a configuration to a device:

- In the Android zero-touch portal, click **Devices**.
- Find the device in the list of devices and choose the configuration you want to assign to it.



c) Click **Update**.

You can apply a configuration to many devices using a CSV file.

For information on how to apply a configuration to many devices, see the Android Enterprise help topic [Zero-touch enrollment for IT admins](#). This Android Enterprise help topic contains more information on how to manage configurations and apply them to devices.

## Provisioning dedicated Android Enterprise devices

Dedicated Android Enterprise devices are fully managed devices that are dedicated to fulfill a single use case. You restrict these devices to one app or a small set of apps required to perform the tasks needed for this use case. You also prevent users from enabling other apps or performing other actions on the device.

Enroll dedicated devices using any of the enrollment methods used for other fully managed devices, as described in Provisioning Android Enterprise fully managed devices. Provisioning dedicated devices require more setup before enrollment.

To provision dedicated devices:

- Add an enrollment profile for Endpoint Management administrators that you allow to enroll dedicated devices to your Endpoint Management deployment. See [Creating enrollment profiles](#).
- To enable a dedicated device to access apps, add them to the allow list.
- Optionally, set the allowed app to allow lock task mode. When an app is in lock task mode, the app is pinned to the device screen when the user opens it. No Home button appears and the Back button is disabled. The user exits the app using an action programmed into the app, such as signing out.
- Enroll each device in the enrollment profile you added.

## System requirements

- Support for enrolling dedicated devices begins with Android 6.0.

## Allow apps and set lock task mode

The Kiosk device policy lets you allow apps and set lock task mode. By default, Secure Hub and Google Play services are on the allow list.

To add the Kiosk policy:

1. In the Endpoint Management console, click **Configure > Device Policies**. The **Device Policies** page appears.
2. Click **Add**. The **Add a New Policy** dialog box appears.
3. Expand **More** and then, under Security, click **Kiosk**. The **Kiosk Policy** page appears.
4. Under Platforms, select **Android Enterprise**. Clear other platforms.
5. In the Policy Information pane, type the **Policy Name** and an optional **Description**.
6. Click **Next** and then click **Add**.
7. To allow an app and allow or deny lock task mode for that app:

Select the app you want to allow from the list.

Choose **Allow** to set the app to be pinned to the device screen when the user starts the app. Choose **Deny** to set the app not to be pinned. Default is **Allow**.

The screenshot shows the 'Kiosk Policy' configuration interface. The sidebar on the left has three main sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Android Enterprise' is checked. The main area displays the policy details, including a description: 'This policy lets you whitelist apps onto a Kiosk for Corporate Owned Single Use devices. If an app supports lock task mode and when lock task status of that app is set to allow, it will get pinned to the screen on the device.' Below this is a table for 'Allowed apps' with the following structure:

Apps to whitelist *	Lock task status	
Cosu App	<input checked="" type="radio"/> Allow <input type="radio"/> Deny	Save Cancel

Below the table is a section for 'Deployment Rules'. At the bottom right of the main area are 'Back' and 'Next >' buttons.

8. Click **Save**.

9. To allow another app and allow or deny lock task mode for that app, click **Add**.

10. Configure deployment rules and choose delivery groups. For more information, see [Device policies](#).

### Provisioning Android Enterprise fully managed devices with a work profile or work profile on corporate-owned devices

Devices running Android 8.0-10.x enroll as “fully managed with a work profile.” Starting with Android 11+, devices enroll as “work profile on corporate-owned devices.” All of these devices are company-owned devices that are used for both work and personal purposes. Your organization manages the entire device. You can apply one set of policies to the device and a separate set of policies to the work profile.

In the Endpoint Management console, fully managed devices with a work profile appear with these terms:

- The device ownership is “Corporate”.
- The device Android Enterprise install type is “Corporate Owner Personally Enabled”.



## System requirements

- Support for enrolling fully managed devices with work profiles begins with Android 8.0.

## To enroll the device

New and factory reset devices enroll as fully managed devices with a work profile. Those devices use any of the enrollment methods used for other fully-managed devices, as described in Provisioning Android Enterprise fully managed devices. Devices running Android 11 can enroll in the work profile on corporate-owned devices mode using the QR code or zero-touch enrollment methods described in that section.

### Important:

When enrolling devices in the work profile on corporate-owned devices mode using the QR code method, add the following to the JSON output, above the `serverURL` field:

```
"desiredProvisioningMode": "managedProfile",
```

```
JSON output

{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
  "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
  "qn7oZUtheu3JBAinzZRrjCQv6L006LL10jcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
  "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
  "android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": false,
  "android.app.extra.PROVISIONING_SKIP_USER_CONSENT": true,
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
    "desiredProvisioningMode": "managedProfile",
    "serverURL": "https://testServer.xmqa.cloud.com",
    "username": "username",
    "password": "password"
  }
}
```

Devices that are not new or factor reset are enrolled as work profile devices as described in Provisioning Android Enterprise work profile devices.

## Viewing Android Enterprise devices in the Endpoint Management console

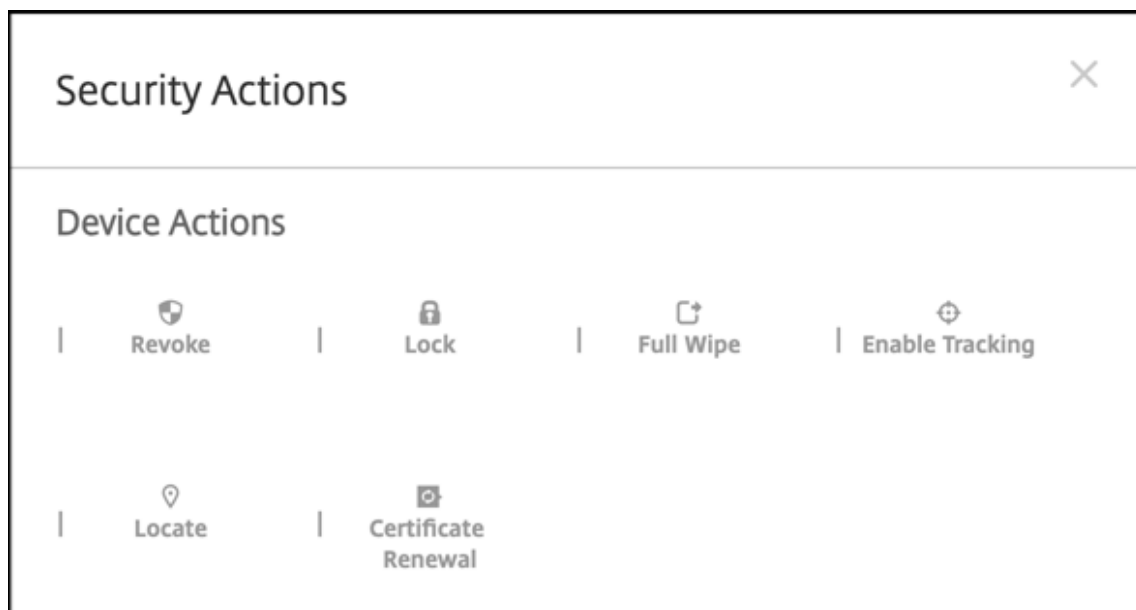
To view Android Enterprise fully managed devices, dedicated devices, and fully managed devices with a work profile:

1. In the Endpoint Management console, go to **Manage > Devices**.

2. Add the **Android Enterprise Enabled Device?** column by clicking the menu on the right edge of the table on this screen.



3. To view available security actions, select a fully managed device and click **Secure**. When the device is fully managed, the **Full Wipe** action is available but **Selective Wipe** is not. That difference is because the device only allows apps from the managed Google Play store. There is not an option for the user to install applications from the public store. Your organization manages all the content on the device.



## Configure Android Enterprise device and app policies

For an overview of the policies controlled at both the device and app levels, see [Supported device policies and MDX policies for Android Enterprise](#).

What to know about policies:

- **Device restrictions:** Dozens of device restrictions let you control features such as:
  - Use of the device camera
  - Use of copy and paste between work and personal profiles
- **Per-app VPN:** Use the Managed configurations device policy to configure VPN profiles for Android Enterprise.
- **Email policy:** We recommend using the Managed configurations device policy to configure apps.

## Device policies

This table lists all device policies available for Android Enterprise devices.

### Important:

For devices that enroll in Android Enterprise and use MDX apps: You can control some settings through MDX and Android Enterprise. Use the least restrictive policy settings for MDX and control the policy through Android Enterprise.

App permissions	App inventory	App uninstall
Automatically update managed apps	Connection scheduling	Credentials
Custom XML	Endpoint Management options	Exchange
Files	Keyguard management	Kiosk
Knox Platform for Enterprise	Launcher configuration	Location
Managed configurations	Network	OS update
Passcode	Restrictions	Samsung MDM license key

## Device policies for fully managed devices with work profile (COPE devices)

For fully managed devices with work profiles, you can use some device policies to apply separate settings to the entire device and the work profile. You can use other device policies to apply settings only to the entire device or only to the work profile of fully managed devices with work profiles. For devices enrolled in the work profile on corporate-owned devices mode, policies apply only to the work profile and not the entire device.

Policy	Applies to
<a href="#">App permissions</a>	Work profile
<a href="#">App inventory</a>	Work profile
<a href="#">App uninstall</a>	Work profile
<a href="#">Automatically update managed apps</a>	Work profile
<a href="#">Connection scheduling</a>	Work profile
<a href="#">Credentials</a>	Work profile
<a href="#">Custom XML</a>	N/A
<a href="#">Endpoint Management options</a>	Work profile
<a href="#">Exchange</a>	N/A
<a href="#">Files</a>	Work profile
<a href="#">Keyguard management</a>	Device and work profile
<a href="#">Kiosk</a>	N/A
<a href="#">Knox Platform for Enterprise</a>	Work profile
<a href="#">Launcher configuration</a>	Device and work profile
<a href="#">Location</a>	Device (location mode only)
<a href="#">Managed configurations</a>	Work profile
<a href="#">Network</a>	Device
<a href="#">OS update</a>	N/A
<a href="#">Passcode</a>	Device and work profile
<a href="#">Restrictions</a>	Device and work profile (create separate policies for the device and the work profile)
<a href="#">Samsung MDM license key</a>	N/A
<a href="#">VPN</a>	

See also, [Supported device policies and MDX policies for Android Enterprise](#) and [MAM SDK overview](#).

## Security actions

Android Enterprise supports the following security actions. For a description of each security action, see [Security actions](#).

Security action	Work profile	Fully managed
Certificate Renewal	Yes	Yes
Full Wipe	Yes (after a selective wipe)	Yes
Locate	Yes	Yes
Lock	Yes	Yes
Lock and Reset Password	No	Yes
Notify (Ring)	Yes	Yes
Revoke	Yes	Yes
Selective Wipe	Yes	Yes

### Security action notes

- The locate security action fails unless the Location device policy sets the location mode for the device to **High Accuracy** or **Battery Saving**. See [Location device policy](#).
- On work profile devices that are running versions of Android earlier than Android 8.0:
  - The lock and reset password action isn't supported.
- On work profile devices with Android 8.0 or greater:
  - The passcode sent locks the work profile. The device itself isn't locked.
  - If no passcode is set on the work profile:
    - \* If no passcode is sent, or the passcode sent doesn't meet passcode requirements: The device is locked.
  - If a passcode is set on the work profile:
    - \* If no passcode is sent, or the passcode sent doesn't meet passcode requirements: The work profile is locked but the device itself isn't locked.

## Unenroll an Android Enterprise enterprise

If you no longer want to use your Android Enterprise enterprise, you can unenroll the enterprise.

**Warning:**

After you unenroll an enterprise, Android Enterprise apps on devices already enrolled through it reset to their default states. Google no longer manages the devices. If you enroll into a new Android Enterprise enterprise, you must approve apps for the new organization from managed Google Play. You can then update the apps from the Endpoint Management console.

After the Android Enterprise enterprise is unenrolled:

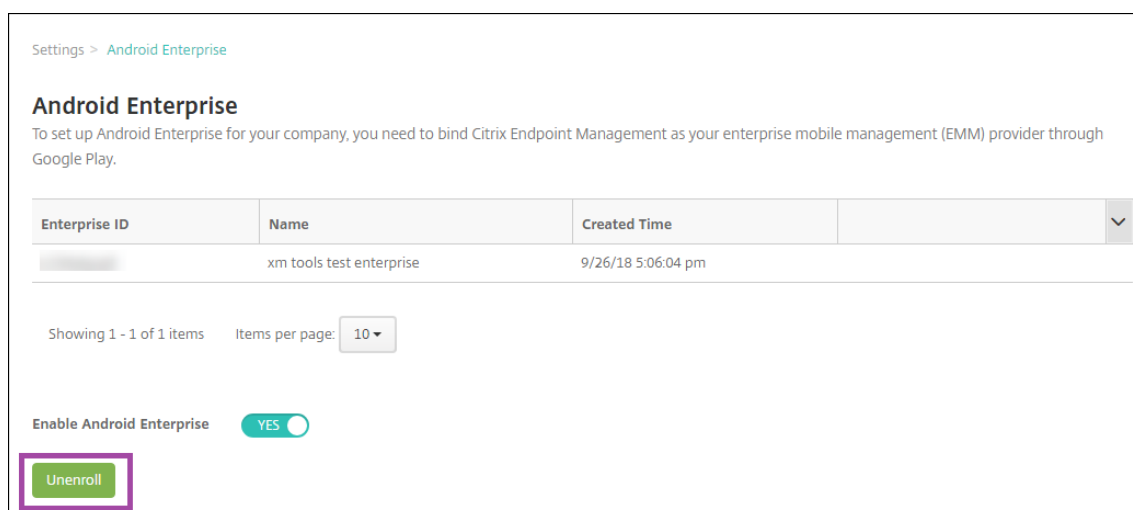
- Devices and users enrolled through the enterprise have the Android Enterprise apps reset to their default state. Managed configurations policies previously applied no longer affect operations.
- Endpoint Management manages devices enrolled through the enterprise. From the perspective of Google, those devices are unmanaged. You can't add new Android Enterprise apps. You can't apply Managed configurations policies. You can apply other policies, such as Scheduling, Password, and Restrictions, to these devices.
- If you attempt to enroll devices in Android Enterprise, they are enrolled as Android devices, not Android Enterprise devices.

Unenroll an Android Enterprise enterprise using the Endpoint Management server console and Endpoint Management Tools.

When you perform this task, Endpoint Management opens a Tools popup window. Before you begin, ensure that your browser has permission to open popup windows. Some browsers, such as Google Chrome, require you to disable popup blocking and add the address of the Endpoint Management site to the popup allow list.

To unenroll an Android Enterprise enterprise:

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The Settings page appears.
2. On the Settings page, click **Android Enterprise**.
3. Click **Unenroll**.



## Android for Workspace

October 7, 2021

Android for Workspace uses the Android Management API (AMAPI) provided by Google to manage Android devices. With Android for Workspace, users no longer need to enroll their devices through Secure Hub. Users enroll through the Citrix Workspace app, and they access all apps and content through Workspace.

Android for Workspace is available for Citrix Workspace enabled cloud deployments only. The initial release of Android for Workspace supports the work profile enrollment method only. With this enrollment method, devices have a work profile and a personal profile to separate corporate data from personal data. Work profiles and personal profiles are separated at an OS level. For more details about work profiles, see the Google help topic, [What is a work profile](#).

This platform is separate from the Android Enterprise platform. Existing configurations for Android Enterprise aren't compatible with Android for Workspace. If you already have Android Enterprise configured, you must create new versions of the following:

- Google account
- Delivery groups
- Enrollment profiles
- Device and app policies

Also, Android Enterprise users enrolled in Endpoint Management must re-enroll using the Citrix Workspace app.

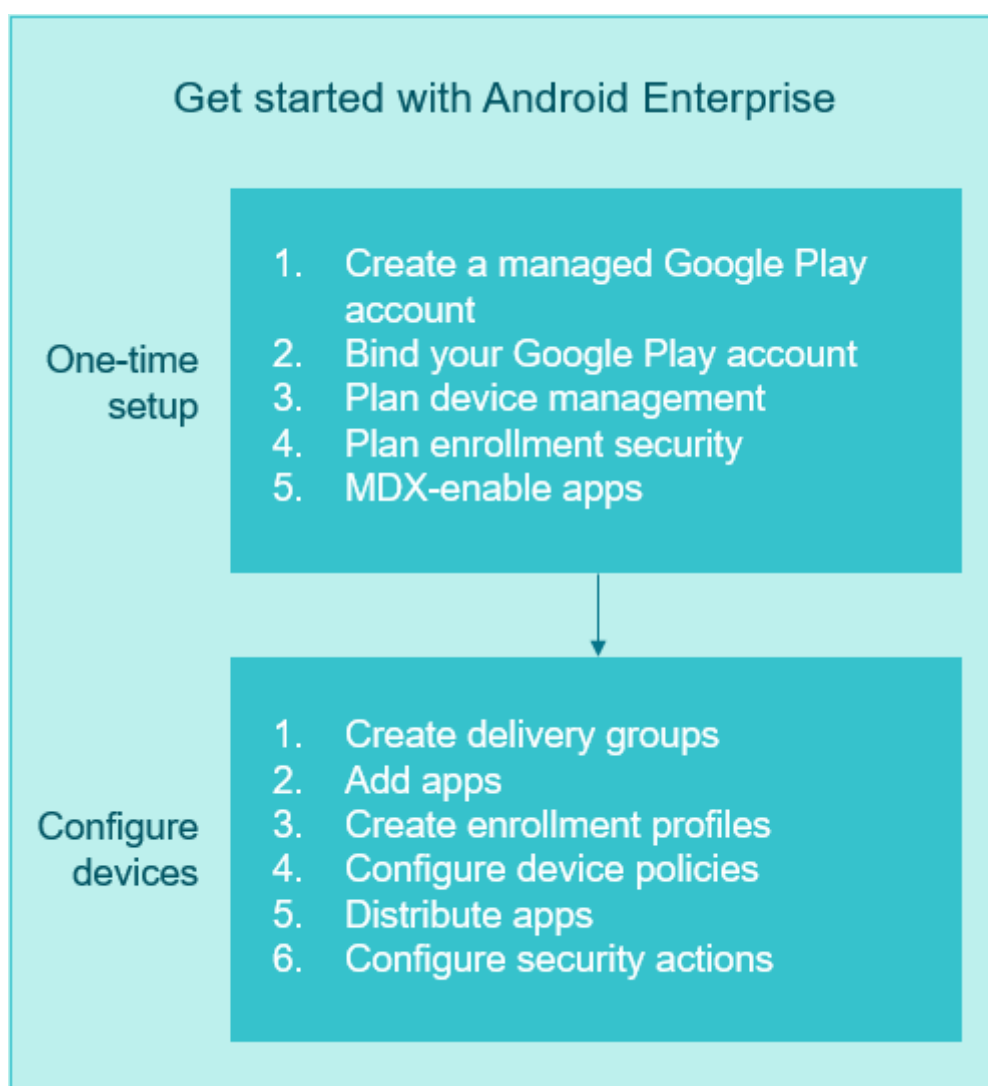
If you want to use Android Enterprise without the AMAPI features, see [Android Enterprise](#).

## Requirements

Before you start using Android for Workspace, you need:

- Citrix Gateway Service
- Accounts and credentials:
  - To set up Android for Workspace with managed Google Play, a corporate Google account
  - To download the latest MDX files, a Citrix customer account
- To use Android for Workspace, devices must have the following:
  - Android 7 or later
  - Citrix Workspace app version

## Getting started with Android for Workspace





## One-time setup

Follow these steps to perform the initial setup of the Android for Workspace platform.

1. Create a Google account. If you already have Android Enterprise set up, you must use a Google account with a different email address.  
See [Using managed Google Play with Endpoint Management and Requirements](#).
2. Bind your Google account to Endpoint Management.  
See [Connecting Endpoint Management to Google Play](#).
3. Create and configure enrollment profiles.  
See [Creating enrollment profiles](#).
4. Prepare to deliver MDX-enabled apps.  
Use the MAM SDK to develop apps.  
See [MAM SDK overview](#).

## Configure devices

1. Create delivery groups. Existing delivery groups for Android Enterprise don't deliver resources to Android for Workspace devices.  
Control who gets what resources and when they get them. See [Deploy resources](#).
2. Add apps. You can approve the apps in Google Play directly from the Endpoint Management console.
3. Create enrollment profiles.  
Specify device and app management enrollment options. See [Creating enrollment profiles](#).
4. Configure device and app policies.  
Balance enterprise security with user privacy and user experience. See [Configure Android for Workspace device and app policies](#).
5. Distribute apps.  
See:
  - [Add apps](#)
  - [Distribute Android Enterprise and Android for Workspace apps](#)
  - [Managed configurations policy](#)
  - [App permissions device policy](#)

Apps published for Android for Workspace have no deployment rules. Endpoint Management pushes new apps and policies to Android for Workspace devices every 30 minutes.

6. Configure security actions to monitor and ensure compliance.

See Security actions.

## Using managed Google Play with Endpoint Management

When you integrate Endpoint Management with managed Google Play to use Android for Workspace, you create an enterprise. Google defines an enterprise as a binding between the organization and your enterprise mobile management (EMM) solution. All the users and devices that the organization manages through your solution belong to its enterprise.

An enterprise for Android for Workspace has two components: an EMM solution and a Google enterprise app platform. When you integrate Endpoint Management with Android for Workspace, the complete solution has these components:

- **Citrix Endpoint Management:** The Citrix EMM. Endpoint Management is the unified endpoint management for a secure digital workspace. Endpoint Management provides the means for IT administrators to manage devices and apps for their organizations.
- **Managed Google Play:** A Google enterprise app platform that integrates with Endpoint Management. The Google Play EMM API sets app policies and distributes app.

When you use managed Google Play, you provision managed Google Play Accounts for devices and end users. Managed Google Play Accounts provide access to managed Google Play, allowing users to install and use the apps you make available. If your organization uses a third-party identity service, you can link managed Google Play Accounts with your existing identity accounts.

Because this type of enterprise is not tied to a domain, you can create more than one enterprise for a single organization. For example, each department or region within an organization can enroll as a different enterprise. Using different enterprises lets you manage separate sets of devices and apps.

For Endpoint Management administrators, managed Google Play combines the user experience and app store features of Google Play with a set of management capabilities designed for enterprises. You use managed Google Play to add, buy, and approve apps for deployment to the Android for Workspace workspace on a device. You can use Google Play to deploy public apps, private apps, and third-party apps.

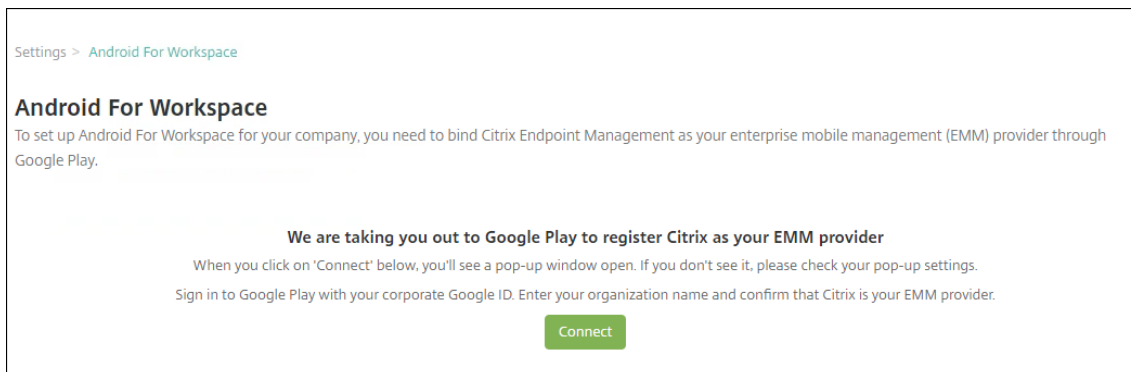
For users of managed devices, managed Google Play is the enterprise app store. Users can browse apps, view app details, and install them. Unlike the public version of Google Play, users can only install apps from managed Google Play that you make available for them.

## Connecting Endpoint Management to Google Play

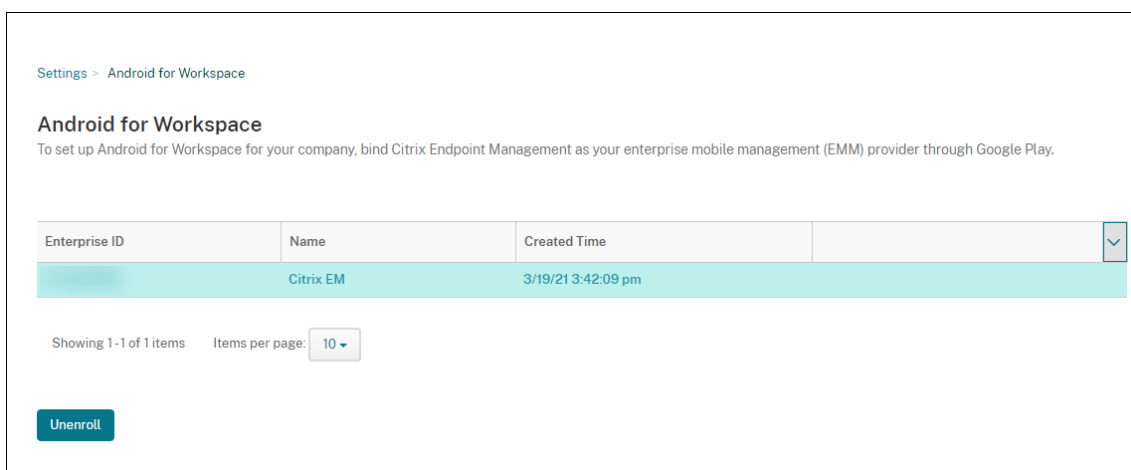
To set up Android for Workspace for your organization, register Citrix as your EMM provider through managed Google Play. That setup connects managed Google Play to Endpoint Management and creates an enterprise for Android for Workspace in Endpoint Management.

You need a corporate Google account to sign in to Google Play.

1. In the Endpoint Management console, go to **Settings > Android for Workspace**.
2. Click **Connect**. Google Play opens.



3. Sign in to Google Play with your corporate Google account credentials. Enter your organization name and confirm Citrix is your EMM provider.
4. An enterprise ID is added for Android for Workspace. Your Enterprise ID appears in the Endpoint Management console.



Your environment is connected to Google and is ready to manage devices. You can now provide apps for users.

Endpoint Management can provide users with Citrix mobile productivity apps, MDX apps, public app store apps, web and SaaS apps, enterprise apps, and web links. For more information on these types of apps and providing them to users, see [Add apps](#).

### Creating enrollment profiles

Enrollment profiles control how Android devices enroll if Android for Workspace is enabled for your Endpoint Management deployment. Configure the enrollment profile to enroll new and factory reset

devices as Android for Workspace work profile devices. You can also configure each of these enrollment profiles to enroll BYOD Android devices as work profile devices.

Citrix Workspace is an MDM+MAM solution only. When a user enrolls in Endpoint Management through the Workspace app, they must agree to device management and app management.

The authentication method for Android for Workspace devices defaults to the authentication method set up for the Citrix Workspace app. Configuring an authentication method in the Endpoint Management console has no effect on these devices. See [Change authentication methods](#).

When you create enrollment profiles, you assign delivery groups to them. If a user belongs to multiple delivery groups that have different enrollment profiles, the name of the delivery group determines the enrollment profile used. Endpoint Management selects the delivery group that appears last in an alphabetized list of delivery groups. For more information, see [Enrollment profiles](#).

### Add an enrollment profile for work profile devices

1. In the Endpoint Management console, go to **Configure > Enrollment Profiles**.
2. To add an enrollment profile, click **Add**. In the Enrollment Info page, type a name for the enrollment profile.
3. Set the number of devices that members with this profile can enroll.
4. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
5. Enable **Enrollment through Workspace app**. Endpoint Management enables **BYOD work profile** and **Citrix MAM** automatically.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<b>Workspace integration</b> ⓘ Enrollment through Workspace app <input checked="" type="checkbox"/> ⓘ
Android	<b>Device management</b> ⓘ BYOD work profile <input checked="" type="checkbox"/> ⓘ
iOS	<b>Application management</b> ⓘ Citrix MAM <input checked="" type="checkbox"/> ⓘ
Windows	<b>Gateway configuration</b>
3 Assignment (optional)	Gateway server <input type="text" value="Citrix Gateway service"/> ⓘ

6. Select **Assignment (optional)**. The Delivery Group Assignment screen appears.
7. Choose the delivery group or delivery groups containing the administrators who enroll fully managed devices with a work profile. Then click **Save**.

The Enrollment Profile page appears with the profile you added.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<p><b>Workspace integration</b> ⓘ</p> <p>Enrollment through Workspace app <input type="checkbox"/> ⓘ</p> <p><b>Device management</b> ⓘ</p> <p>Management <input checked="" type="radio"/> Android Enterprise ⓘ  <input type="radio"/> Legacy device administration (not recommended) ⓘ  <input type="radio"/> Do not manage devices ⓘ</p> <p>Device owner mode <input type="radio"/> Company-owned device ⓘ  <input checked="" type="radio"/> Fully managed with work profile / Work profile on corporate-owned devices ⓘ  <input type="radio"/> Dedicated device ⓘ  <input type="radio"/> None ⓘ</p> <p>BYOD work profile <input checked="" type="checkbox"/> ⓘ</p> <p><b>Application management</b> ⓘ</p> <p>Citrix MAM <input checked="" type="checkbox"/> ⓘ</p> <p><b>User consent</b></p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ⓘ</p>
Android	
iOS	
Windows	
3 Assignment (optional)	

### Provisioning Android for Workspace BYOD work profile devices

Android for Workspace BYOD work profile devices are enrolled in profile owner mode. These devices do not need to be new or factory reset. Users download Citrix Workspace from Google Play and enroll their devices.

By default, Endpoint Management disables the **USB Debugging** and **Unknown Sources** settings on a device when you enroll the device in Android for Workspace as a work profile device.

When enrolling devices in Android for Workspace as work profile devices, always go to Google Play. From there, enable Citrix Workspace to appear in the user's personal profile.

### Configure Android for Workspace device and app policies

For an overview of the policies controlled at both the device and app levels, see [Supported device policies and MDX policies for Android Enterprise](#).

What to know about policies:

- **Device restrictions:** Dozens of device restrictions let you control features such as:
  - Use of the device camera
  - Use of copy and paste between work and personal profiles
- **Per-app VPN:** Use the Managed configurations device policy to configure VPN profiles for Android for Workspace.

## Device policies

The following is a list of device policies available for Android for Workspace.

- [Automatically update managed apps](#)
- [App permissions](#)
- [Keyguard Management](#)
- [Managed configurations](#)
- [Endpoint Management options](#)
- [Passcode](#)
- [Restrictions](#)

## Security actions

Android for Workspace supports the following security actions. For a description of each security action, see [Security actions](#).

- Full Wipe
- Locate
- Lock
- Notify (Ring)
- Selective Wipe

The locate security action fails unless the Location device policy sets the location mode for the device to **High Accuracy** or **Battery Saving**. See [Location device policy](#).

## Unenroll an Android for Workspace enterprise

If you no longer want to use your Android for Workspace enterprise, you can unenroll the enterprise.

### Warning:

After you unenroll an enterprise, apps on devices already enrolled through the enterprise reset to their default states. Google no longer manages the devices. If you enroll into a new Android for Workspace enterprise, you must approve apps for the new organization from managed Google Play. You can then update the apps from the Endpoint Management console.

After you unenroll the Android for Workspace enterprise:

- Devices and users enrolled through the enterprise have the apps reset to their default state. Managed Configurations policies previously applied no longer affect operations.
- Endpoint Management manages devices enrolled through the enterprise. From the perspective of Google, those devices are unmanaged. You can't add new apps. You can't apply Managed configurations policies. You can apply other policies, such as Scheduling, Password, and Restrictions, to these devices.

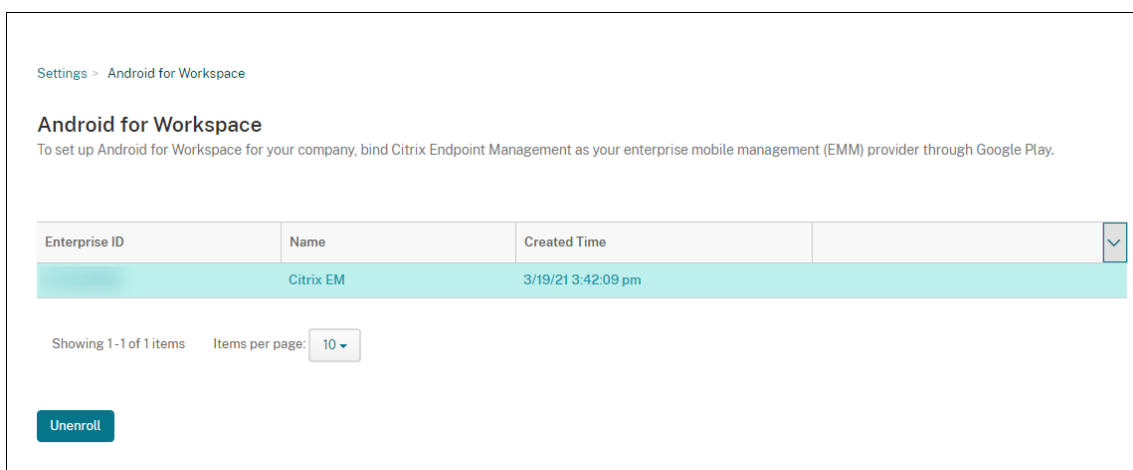
- If you attempt to enroll devices in Android for Workspace, they are enrolled as Android devices, not Android for Workspace devices.

Unenroll an Android for Workspace enterprise using the Endpoint Management server console and Endpoint Management Tools.

When you perform this task, Endpoint Management opens a Tools popup window. Before you begin, ensure that your browser has permission to open popup windows. Some browsers, such as Google Chrome, require you to disable popup blocking and add the address of the Endpoint Management site to the popup allow list.

To unenroll an Android for Workspace enterprise:

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. On the **Settings** page, click **Android for Workspace**.
3. Click **Unenroll**.



## User experience

Users on the Android for Workspace platform enroll their devices through the Citrix Workspace app. Once users enroll, they access apps and corporate data through the Workspace app.

For information about setting up the Citrix Workspace app, see [Citrix Workspace app for Android](#).

For information about enrollment and setting up the app on user devices, see [About Citrix Workspace app for Android](#) in the user help documentation.

## Known limitations

- Google doesn't support the following features with Android for Workspace. Any policy that affects these features doesn't apply to these devices and mobile productivity apps won't allow

users to access the functionality.

- Calendar widget
- Calendar synchronization with personal profile
- Cross profile contacts
- End users need to import certificate authority (CA) certificates manually. Endpoint Management doesn't push the CA certificates to the device.
- URLs inside Secure Mail don't automatically open in Secure Web. Users need to choose **Open-In App** and select Secure Web.
- All DNS servers configured in your Citrix Gateway connector must be able to resolve all fully qualified domain names (FQDN). If the DNS servers can't resolve all FQDNs, URLs may fail to load in Secure Web.
- Secure Web may show a blank screen when launched. If this happens, open the Citrix Workspace app, authenticate, and launch Secure Web again.
- Intranet websites may fail to load in Secure Web. If this occurs, configure a Web SaaS app in the Citrix Cloud app library for that URL.
- Apps prepared using the MAM SDK may not show as managed. If this occurs, launch the Citrix Workspace App and open the apps from there.

## Distribute Android Enterprise and Android for Workspace (Preview) apps

October 7, 2021

Endpoint Management manages apps deployed to devices. You can organize and deploy the following types of Android Enterprise and Android for Workspace apps.

- **Managed app store apps:** These apps include free or paid apps available in the managed Google Play Store. For example, GoToMeeting.
- **MDX:** Apps prepared with the MAM SDK or wrapped with the MDX Toolkit. These apps include MDX policies. You get MDX apps from internal sources and public stores. Deploy Citrix mobile productivity apps as MDX apps.
- **Enterprise:** Private apps you develop or obtain from another source. You provide these apps to your users through the managed Google Play Store. The managed Google Play Store is the Google enterprise app store.
- **MDX-enabled private apps:** Enterprise apps prepared with the MAM SDK or wrapped with the MDX Toolkit.

You can add enterprise apps and MDX-enabled private apps two different ways.

- Add the apps to the Endpoint Management console as enterprise apps, as described in the En-



enterprise apps and MDX-enabled private apps sections in this article.

- Publish the apps directly to the managed Google Play Store using your Google developer account. Then add the apps to the Endpoint Management console as managed app store apps. See [Managed app store apps](#).

If you publish apps using your Google developer account and then switch to using the Endpoint Management console, the ownership of the apps differs. You need to manage your apps in both locations, in this case. Citrix recommends adding your apps using one method or the other.

If you need to remove self-managed apps from the managed Google Play Store, open a ticket with Google. Developers can disable, but not delete, apps from the managed Google Play Store.

The following sections provide more in depth information for Android Enterprise and Android for Workspace app configuration. For information about distributing apps, see [Add Apps](#). That article includes:

- The general workflows for adding web and SaaS apps or web links
- The required app workflow for enterprise and public store apps
- How to deliver enterprise apps from the Citrix Content Delivery Network (CDN) for Enterprise Apps

### Managed app store apps

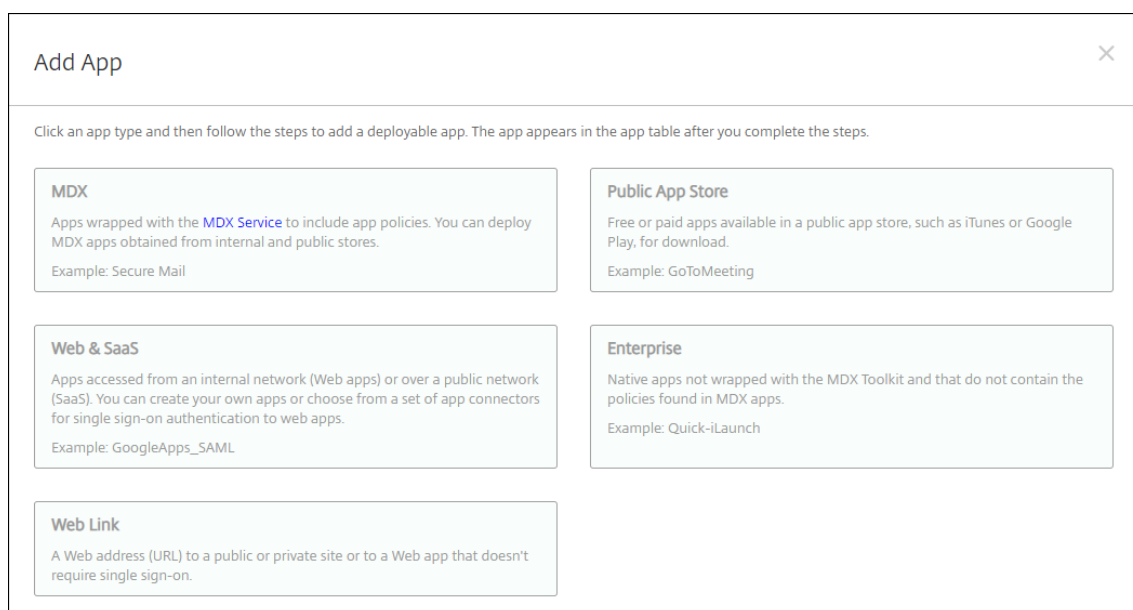
You can add free and paid apps available on the managed Google Play Store to Citrix Endpoint Management.

#### Note:

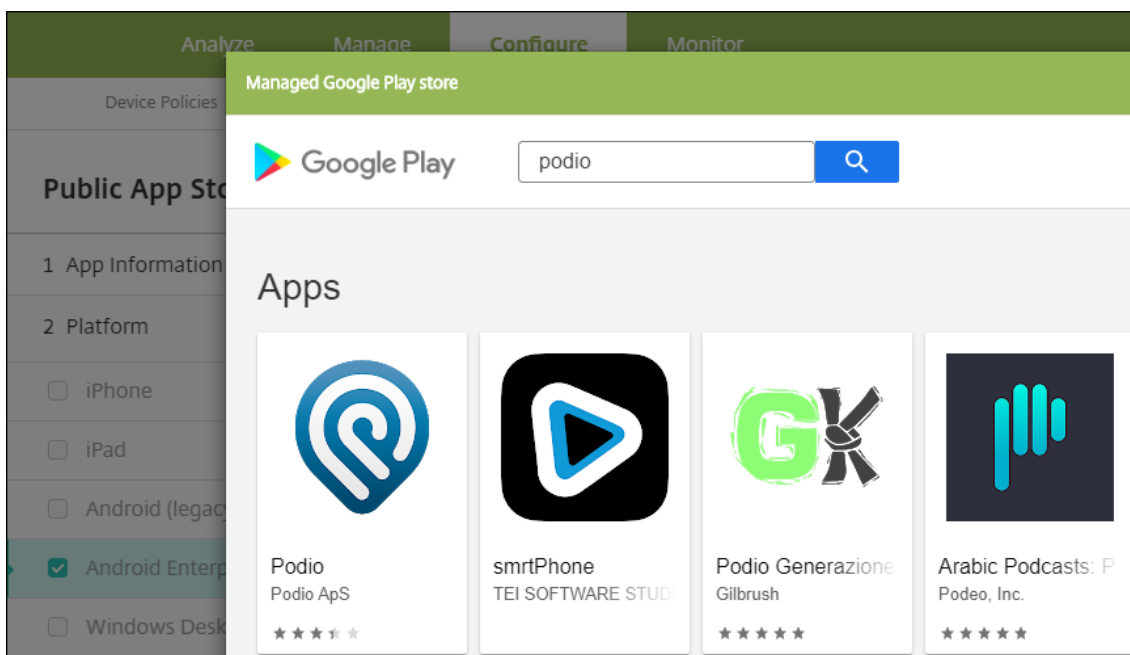
To make all apps in the Google Play store accessible from managed Google Play, use the **Access all apps in the managed Google Play store** server property. See [Server properties](#). Setting this property to **true** allows all Android Enterprise and Android for Workspace users to access public Google Play store apps. You can then use the [Restrictions device policy](#) to control access to these apps.

### Step 1: Add and configure apps

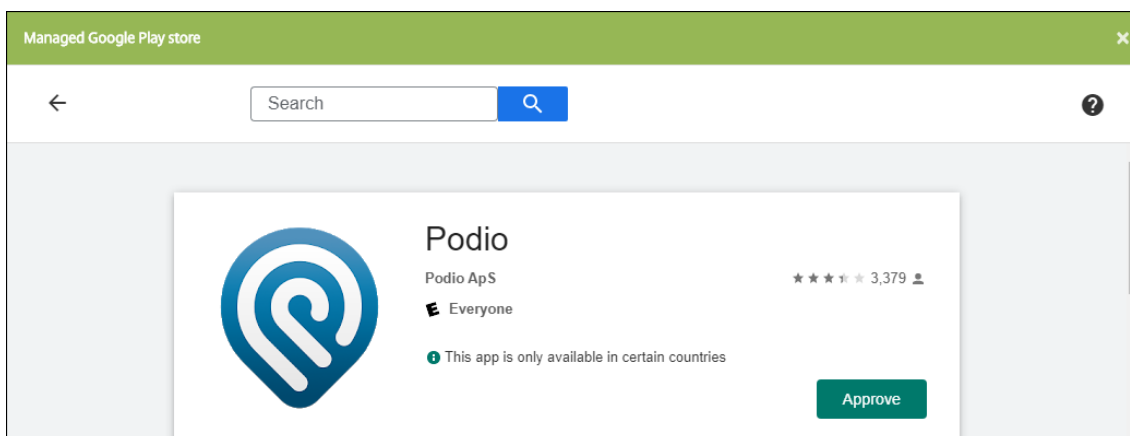
1. In the Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.
2. Click **Public App Store**.



3. In the **App Information** pane, type the following information:
  - **Name:** Type a descriptive name for the app. The name appears under **App Name** on the **Apps** table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see [About app categories](#).
4. Select **Android Enterprise** or **Android for Workspace** as the platform.
5. Type the app name or package ID in the search box and click **Search**. You can locate the package ID in the Google Play store. The ID is in the URL of the app. For example, `com.Slack` is the package ID in `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`.

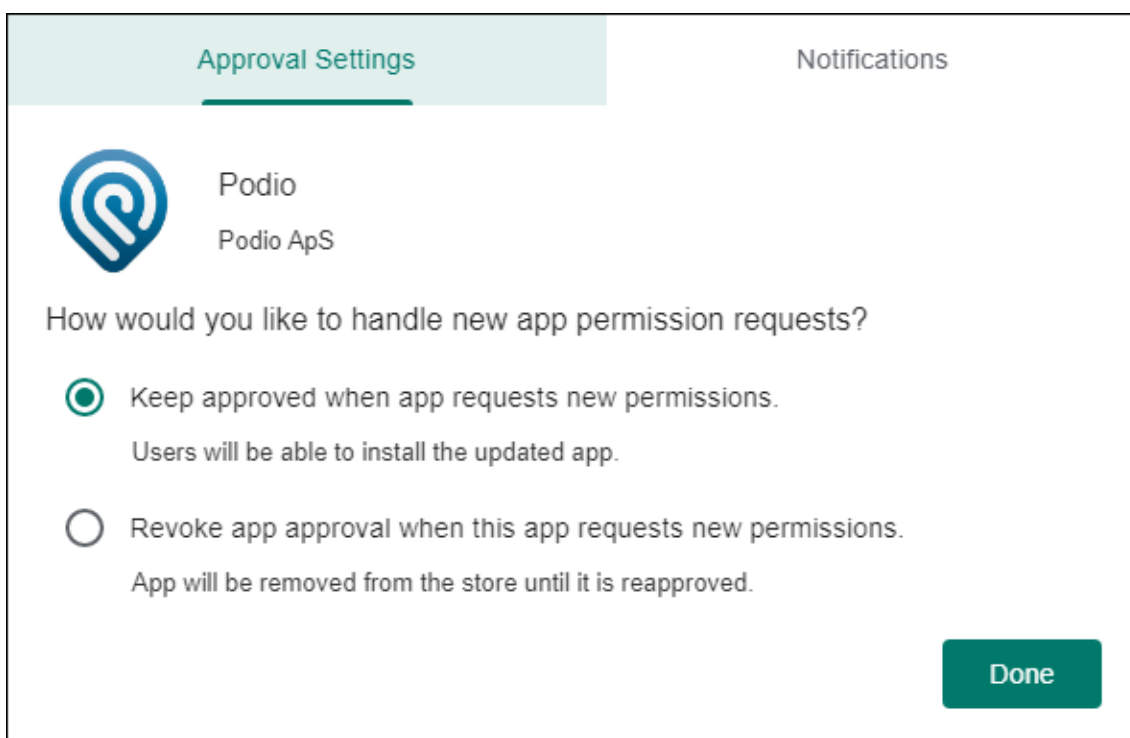


6. Apps matching the search criteria appear. Click the desired app then click **Approve**.

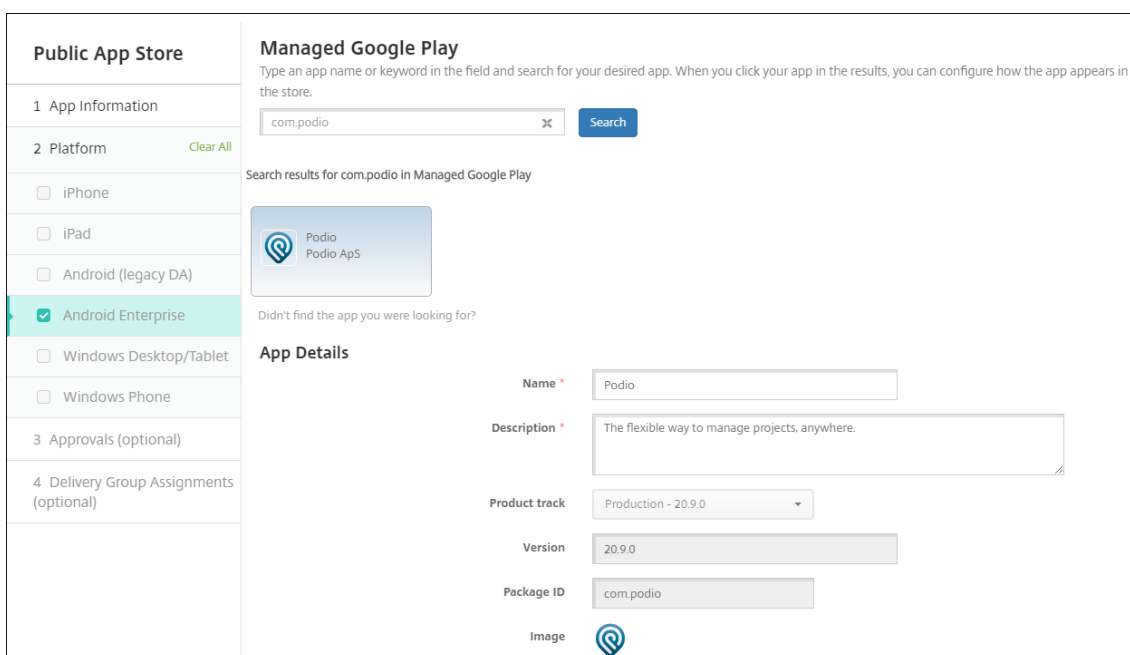


7. Click **Approve** again.

8. Select **Keep approved when app requests new permissions**. Click **Save**.



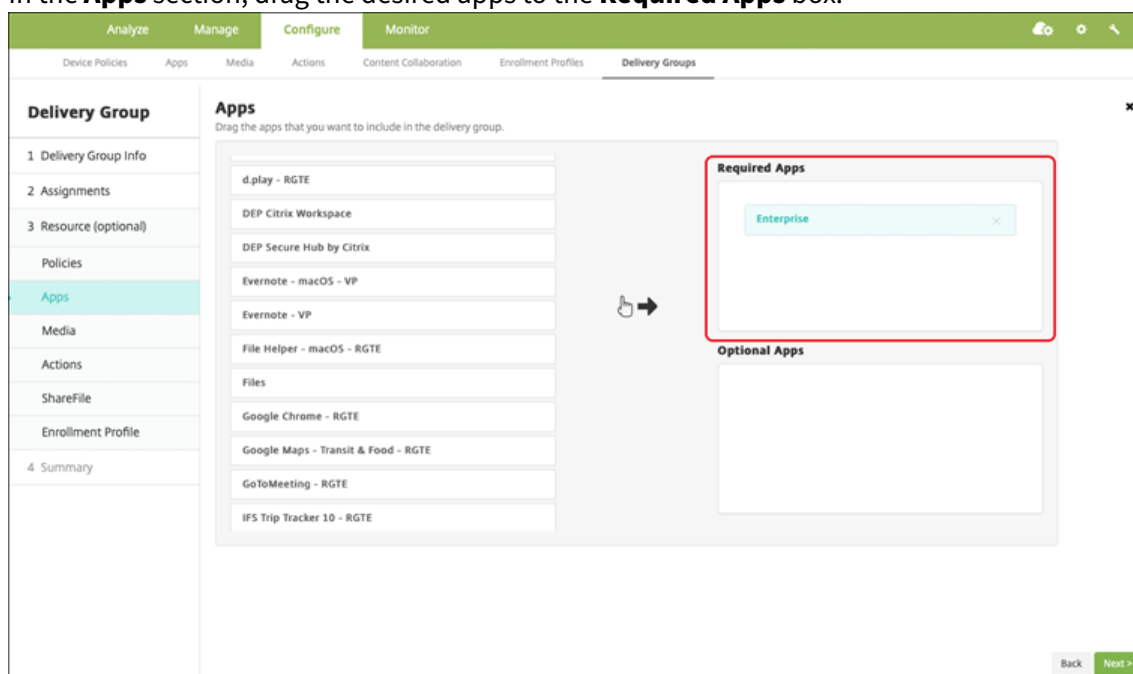
9. Click the app icon and configure the app **Name** and **Description**.



10. Assign any delivery groups to the app and click **Save**. For information, see [Deploy resources](#).

## Step 2: Configure app deployment

1. Navigate to **Configure > Delivery Groups** and select the delivery group you configured. Click **Edit**.
2. In the **Apps** section, drag the desired apps to the **Required Apps** box.



3. On the **Summary** page, click **Save**.
4. On the **Delivery Groups** page, select the delivery group and click **Deploy**.

## MDX apps

Add MDX files to Endpoint Management and configure app details and policy settings. To configure Citrix mobile productivity apps for Android Enterprise, add them as MDX apps. For information about the app policies that are available for each device platform type, see:

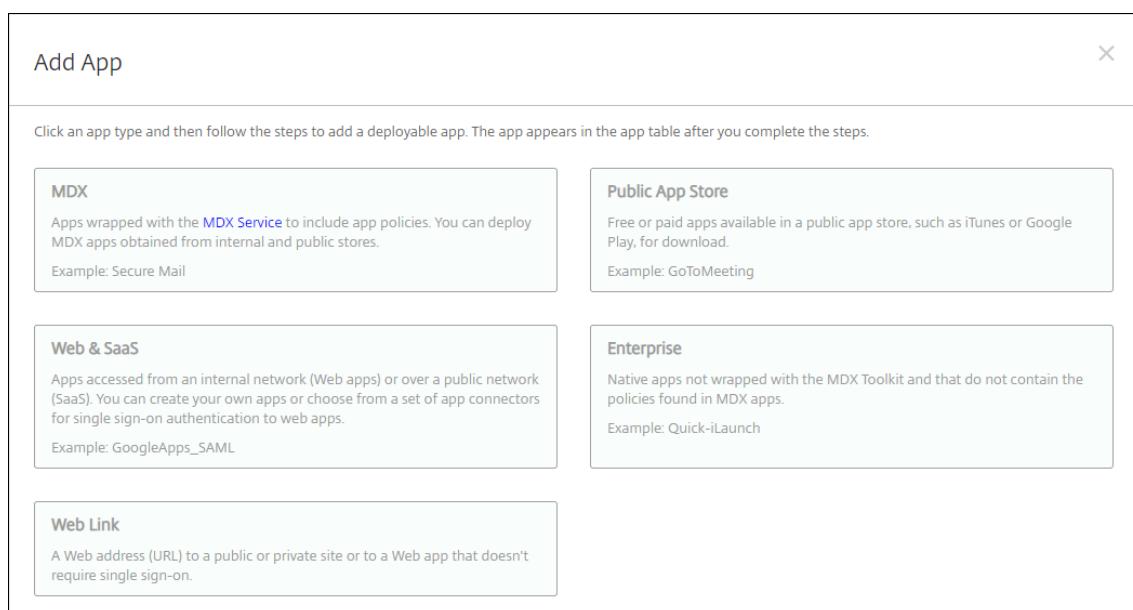
- [MAM SDK overview](#)
- [MDX Policies at a Glance](#)

## Step 1: Add and configure apps

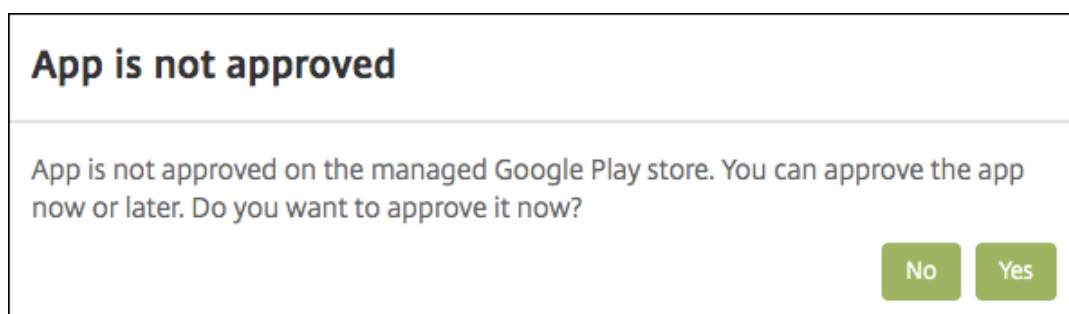
1. For Citrix mobile productivity apps, download the public-store MDX files: Go to <https://www.citrix.com/downloads>. Navigate to **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.

For other types of MDX apps, obtain the MDX file.

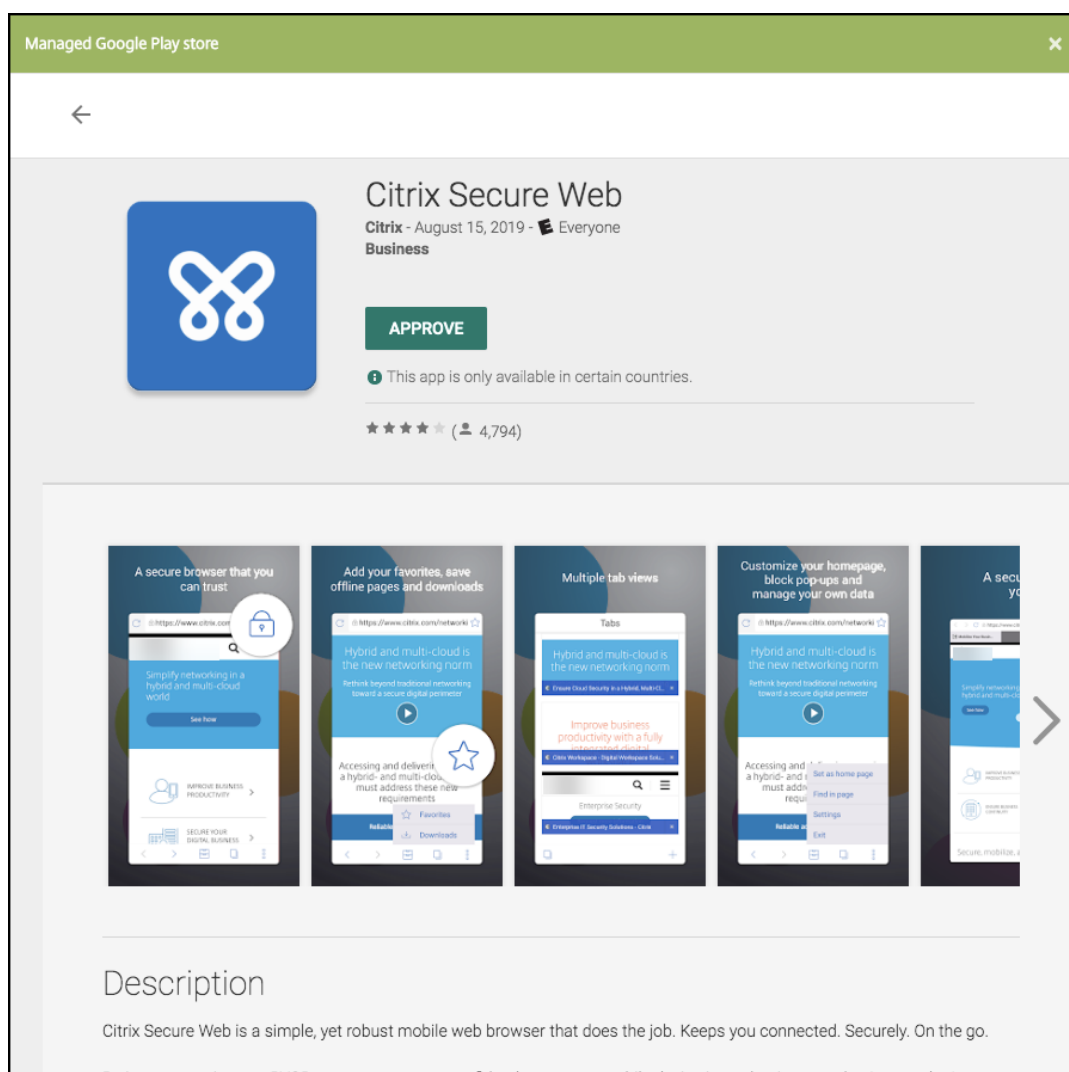
2. In the Endpoint Management console, click **Configure > Apps**. Click **Add**. The **Add App** dialog box appears.



3. Click **MDX**. The **MDX App Information** page appears. In the **App Information** pane, type the following information:
  - **Name:** Type a descriptive name for the app. The name appears under **App Name** on the **Apps** table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see [About app categories](#).
4. Select **Android Enterprise** or **Android for Workspace** as the platform.
5. Click **Upload** and navigate to the MDX file. Android Enterprise and Android for Workspace only support apps prepared with the MAM SDK or MDX Toolkit.
  - The UI notifies you if the attached application requires approval from the managed Google Play Store. To approve the application without leaving the Citrix Endpoint Management console, click **Yes**.



After the managed Google Play Store opens, follow the instructions to approve and save the app.



When you successfully add the app, the **App details** page appears.

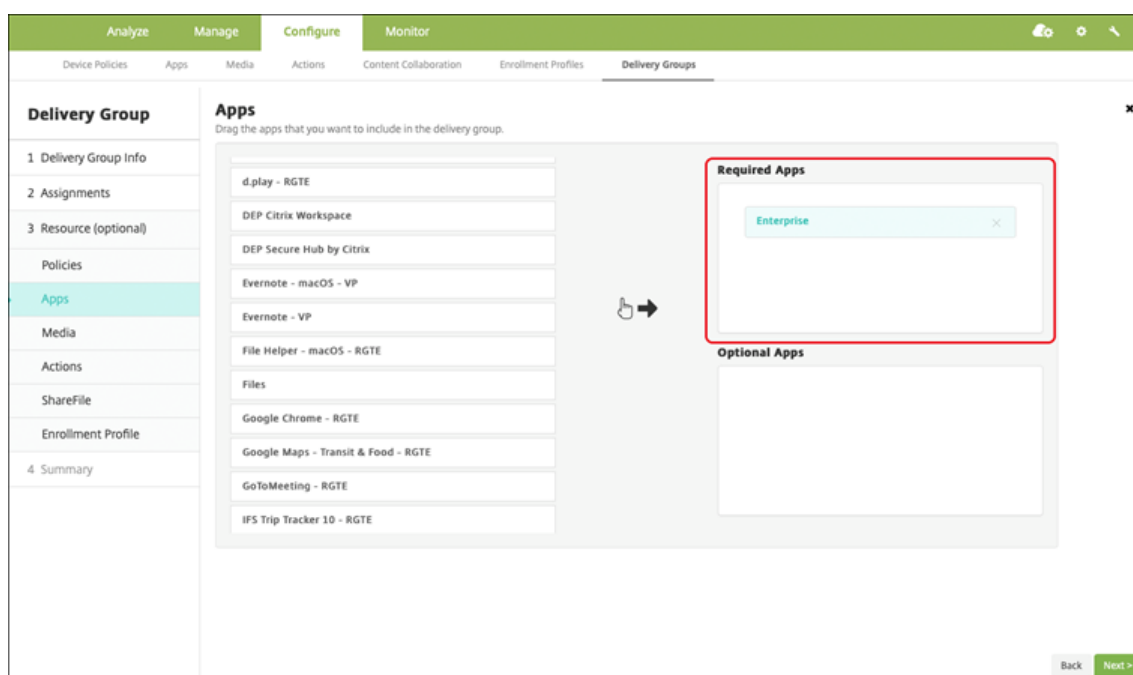
6. Configure these settings:

- **File name:** Type the file name associated with the app.
- **App Description:** Type a description for the app.
- **App version:** Optionally, type the app version number.
- **Package ID:** Type the package ID for the app, obtained from the managed Google Play Store.
- **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
- **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
- **Excluded devices:** Optionally, type the manufacturer or models of devices that cannot run the app.

7. Configure the **MDX Policies**. MDX policies vary by platform and include options for policy areas, including authentication, device security, and app restrictions. In the console, each of the policies has a tooltip that describes the policy. For information about the app policies that are available for each device platform type, see:
  - [MAM SDK overview](#)
  - [MDX Policies at a Glance](#)
8. Configure the deployment rules and store configuration.
9. Assign any delivery groups to the app and click **Save**. For information, see [Deploy resources](#).

## Step 2: Configure app deployment

1. Navigate to **Configure > Delivery Groups** and select the delivery group you configured. Click **Edit**.
2. In the **Apps** section, drag the desired apps to the **Required Apps** box.



3. On the **Summary** page, click **Save**.
4. On the **Delivery Groups** page, select the delivery group and click **Deploy**.

## Enterprise apps

Enterprise apps represent private apps that are not prepared with the MAM SDK or MDX Toolkit. You develop these apps yourself or obtain them directly from other sources. To add an enterprise app, you



need the APK file associated with the app. Ensure that you follow Google [Best practices for private apps](#).

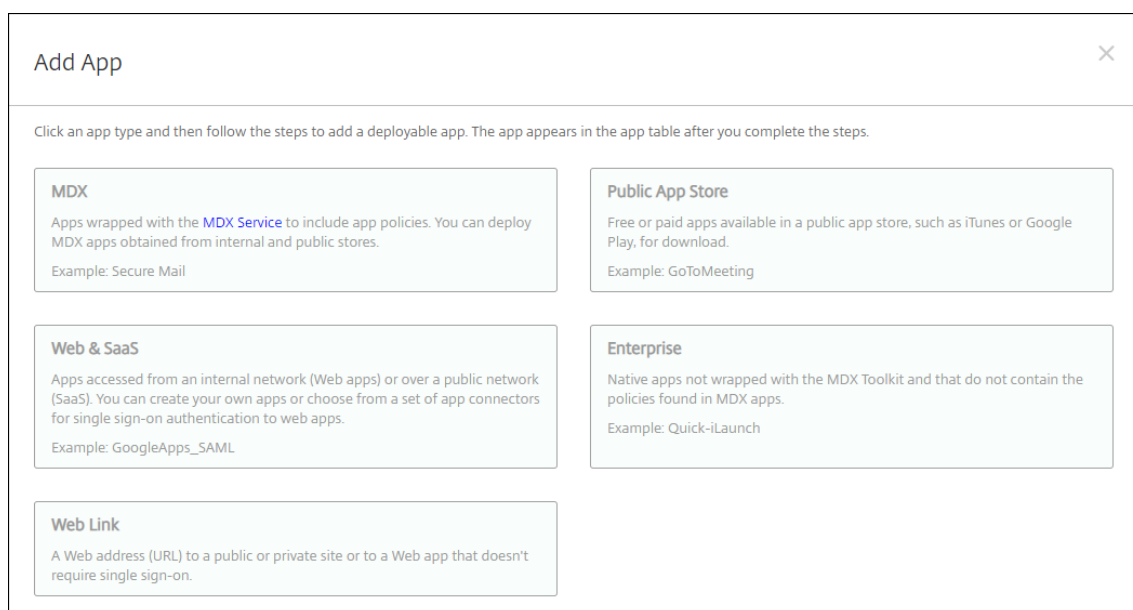
Watch this video to learn more:



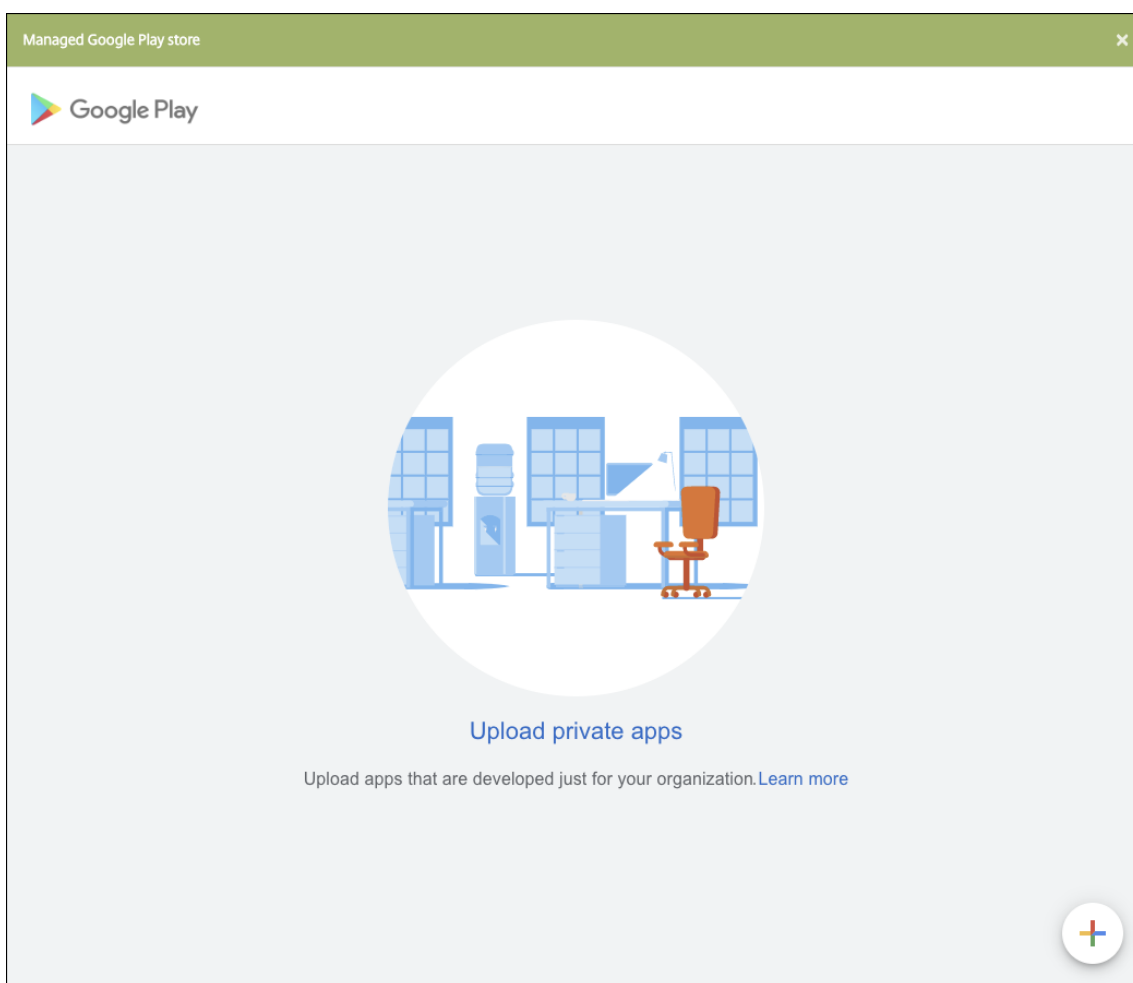
### **Step 1: Add and configure apps**

Add the app one of two ways:

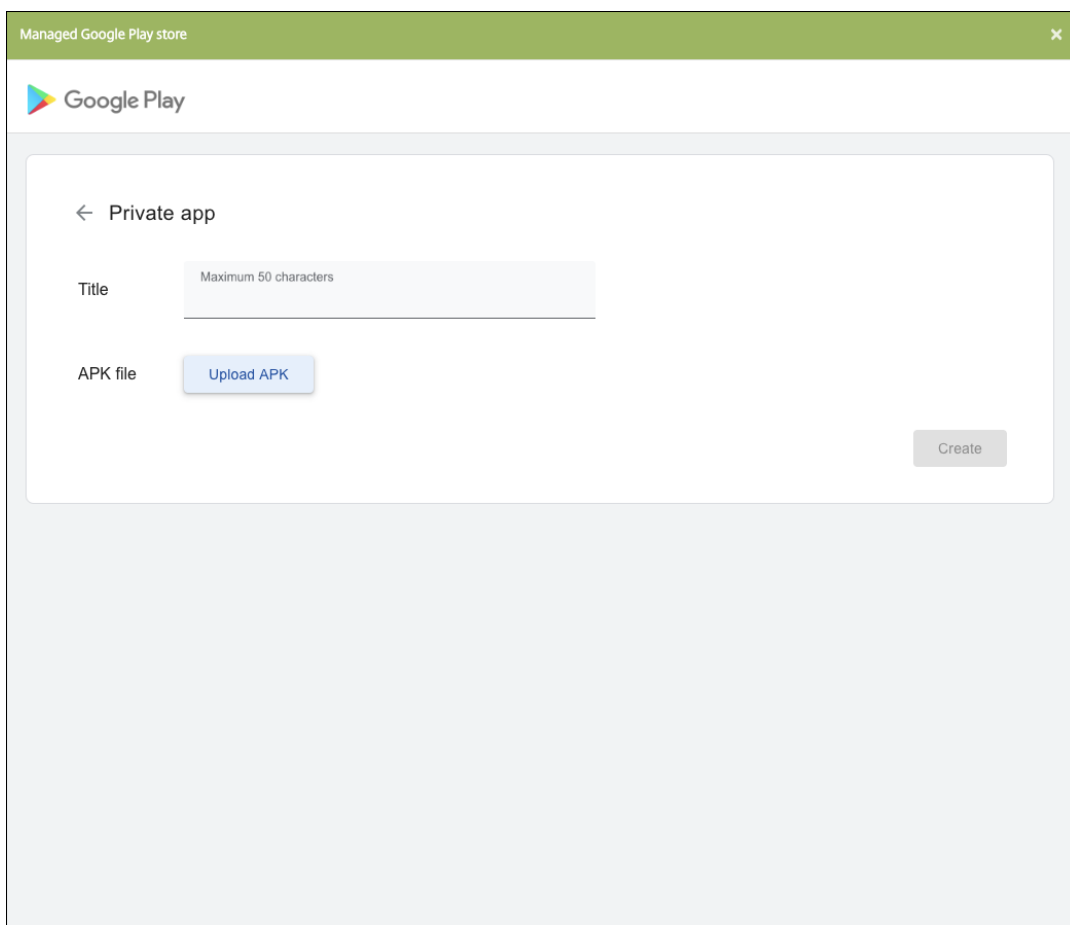
- Publish the app directly to the managed Google Play Store and add it to the Endpoint Management console as a Managed play store app. Follow the Google documentation on how to [Publish private apps](#), and then follow the steps in the Managed app store apps section.
- Add the app to the Endpoint Management console as an enterprise app. Perform the following steps:
  1. In the Endpoint Management console, click **Configure > Apps**. Click **Add**. The **Add App** dialog box appears.



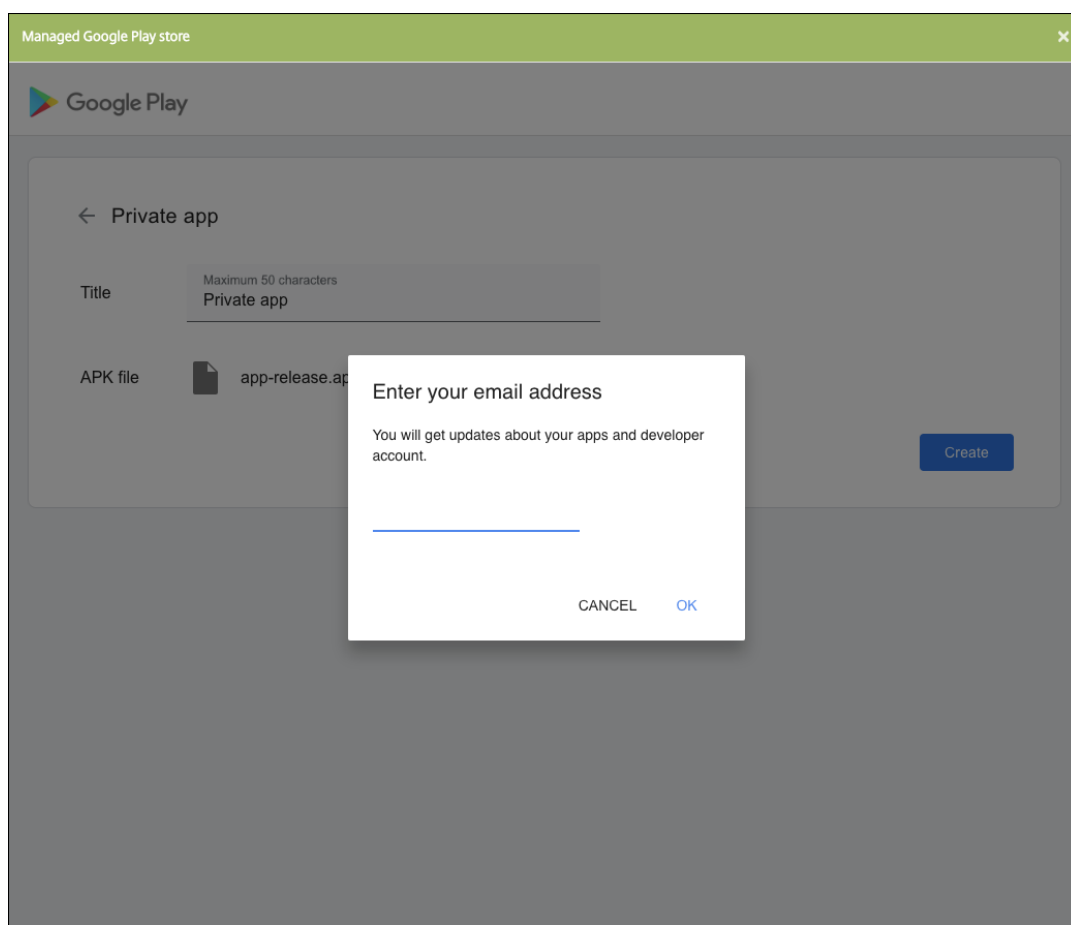
2. Click **Enterprise**. In the **App Information** pane, type the following information:
  - **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see [About app categories](#).
3. Select **Android Enterprise** or **Android for Workspace** as the platform.
4. The **Upload** button opens the managed Google Play Store. You do not need to register for a developer account to publish a private app. Click the **Plus** icon in the lower right corner to continue.



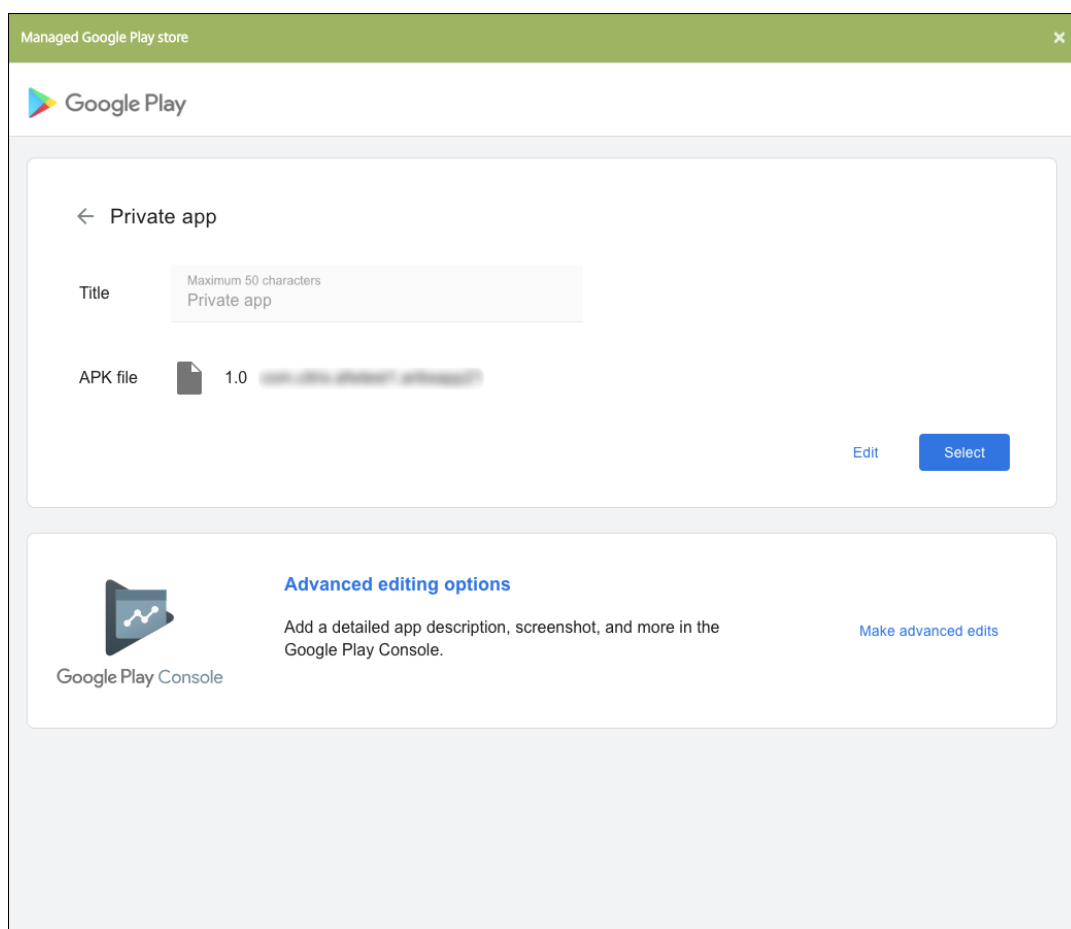
- a) Type the name for your app and upload the .apk file. When finished, click **Create**. It might take up to 10 minutes for your private app to publish.



b) Enter an email address to get updates about your apps.



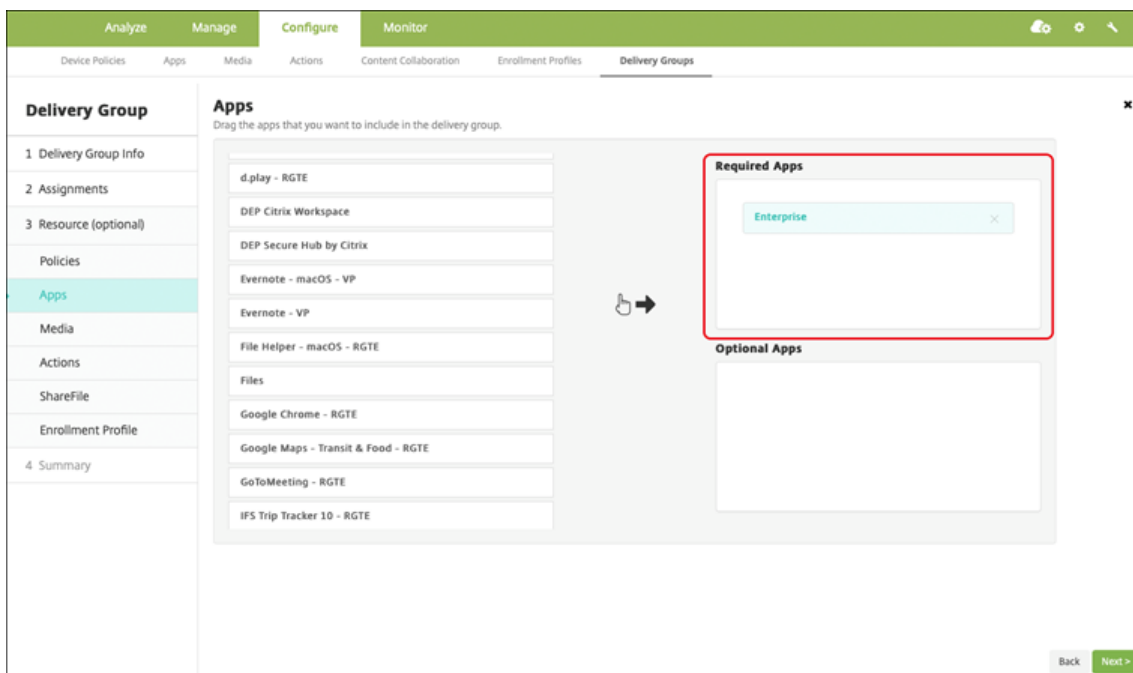
- c) After your application is published, click the icon for the private app. If you want to add an app description, change the app icon, and other actions, click **Make advanced edits**. Otherwise, click **Select** to open the app information page.



5. Click **Next**. The app information page for the platform appears.
6. Configure the settings for the platform type, such as:
  - **File name:** Optionally, type a new name for the app.
  - **App description:** Optionally, type a new description for the app.
  - **App version:** You can't change this field.
  - **Package ID:** Unique identifier of your app.
  - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
  - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
  - **Excluded devices:** Optionally, type the manufacturer or models of devices that cannot run the app.
7. Configure the deployment rules and store configuration.
8. Assign any delivery groups to the app and click **Save**. For information, see [Deploy resources](#).

## Step 2: Configure app deployment

1. Navigate to **Configure > Delivery Groups** and select the delivery group you configured. Click **Edit**.
2. In the **Apps** section, drag the desired apps to the **Required Apps** box.



3. On the **Summary** page, click **Save**.
4. On the **Delivery Groups** page, select the delivery group and click **Deploy**.

## MDX-enabled private apps

To add Android Enterprise and Android for Workspace apps as MDX-enabled enterprise apps:

1. Create a private Android Enterprise or Android for Workspace app and MDX-enable the app.
2. Add the app to the Endpoint Management console.
  - Host and publish the app on the managed Google Play Store.
  - Add the app to the Endpoint Management console as an Enterprise app.
3. Add the MDX file to Endpoint Management.

If you decide to host and publish apps through the Google Play Store, don't opt in for Google certificate signing. Sign the app with the same certificate used to MDX-enable the app. For more information on publishing apps, see Google documentation on [Publishing your app](#) and [Signing your app](#). The MAM SDK doesn't wrap apps, so it doesn't require a certificate other than the one used to develop the app.

For more information about publishing private apps through the Google Play Console, see the Google documentation on how to [Publish private apps from the Play Console](#).

To publish an app through Endpoint Management, see the following sections.

### Prepare an Android Enterprise or an Android for Workspace app

When you create an Android Enterprise app or an Android for Workspace app, ensure that you follow Google [Best practices for private apps](#).

After you create an Android Enterprise app or an Android for Workspace app, integrate the MAM SDK with the app or wrap the app by using the MDX Toolkit. Then, add the resulting files to XenMobile.

You can update the app by uploading an updated.apk file. The following steps cover app wrapping with the MDX Toolkit.

1. Create your Android Enterprise app or Android for Workspace app and generate a signed .apk file.
2. The following sample file contains all known policies, some of which may not be applicable for your environment. Any unusable settings are ignored. Create an XML file with the following parameters:

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <MobileAppPolicies>
3   <PolicySchemaVersion>
4     1.0
5   </PolicySchemaVersion>
6   <Policies>
7     <DevicePasscode>false</DevicePasscode>
8     <AppPasscode>false</AppPasscode>
9     <MaxOfflinePeriod>72</MaxOfflinePeriod>
10    <StepupAuthAddress/>
11    <RequireUserEntropy>false</RequireUserEntropy>
12    <BlockRootedDevices>true</BlockRootedDevices>
13    <BlockDebuggerAccess>false</BlockDebuggerAccess>
14    <RequireDeviceLock>false</RequireDeviceLock>
15    <NonCompliantDeviceBehavior>AllowAppAfterWarning</
16      NonCompliantDeviceBehavior>
17    <WifiOnly>false</WifiOnly>
18    <RequireInternalNetwork>false</RequireInternalNetwork>
19    <InternalWifiNetworks/>
20    <AllowedWifiNetworks/>
21    <UpgradeGracePeriod>168</UpgradeGracePeriod>
22    <WipeDataOnAppLock>false</WipeDataOnAppLock>
23    <ActivePollPeriod>60</ActivePollPeriod>
24    <PublicFileAccessLimitsList/>
25    <CutAndCopy>Unrestricted</CutAndCopy>
    <Paste>Unrestricted</Paste>
```



```
26     <DocumentExchange>Unrestricted</DocumentExchange>
27     <OpenInExclusionList/>
28     <InboundDocumentExchange>Unrestricted</
      InboundDocumentExchange>
29     <InboundDocumentExchangeWhitelist/>
30     <connectionSecurityLevel>TLS</connectionSecurityLevel>
31     <DisableCamera>false</DisableCamera>
32     <DisableGallery>false</DisableGallery>
33     <DisableMicrophone>false</DisableMicrophone>
34     <DisableLocation>false</DisableLocation>
35     <DisableSms>false</DisableSms>
36     <DisableScreenCapture>false</DisableScreenCapture>
37     <DisableSensor>false</DisableSensor>
38     <DisableNFC>false</DisableNFC>
39     <BlockLogs>false</BlockLogs>
40     <DisablePrinting>false</DisablePrinting>
41     <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
      MvpnNetworkAccess>
42     <MvpnSessionRequired>False</MvpnSessionRequired>
43     <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
44     <DisableLocalhostConnections>false</
      DisableLocalhostConnections>
45     <CertificateLabel/>
46     <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
47     <DefaultLoggerLevel>15</DefaultLoggerLevel>
48     <MaxLogFiles>2</MaxLogFiles>
49     <MaxLogFileSize>2</MaxLogFileSize>
50     <RedirectSystemLogs>false</RedirectSystemLogs>
51     <EncryptLogs>false</EncryptLogs>
52     <GeofenceLongitude>0</GeofenceLongitude>
53     <GeofenceLatitude>0</GeofenceLatitude>
54     <GeofenceRadius>0</GeofenceRadius>
55     <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
56     <Authentication>OfflineAccessOnly</Authentication>
57     <ReauthenticationPeriod>480</ReauthenticationPeriod>
58     <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
59     </Policies>
60 </MobileAppPolicies>
61 <!--NeedCopy-->
```

3. Wrap the app using the MDX Toolkit. For information about using the MDX Toolkit, see [Wrapping Android mobile apps](#).

Set the **apptype** parameter to **Premium**. Use the XML file from the previous step in the command described next.

If you know the store URL for the app, set the **storeURL** parameter to the store URL. Users download the app from the store URL after you publish the app.

Here is an example of an MDX Toolkit command used to wrap an app called SampleAEApp:

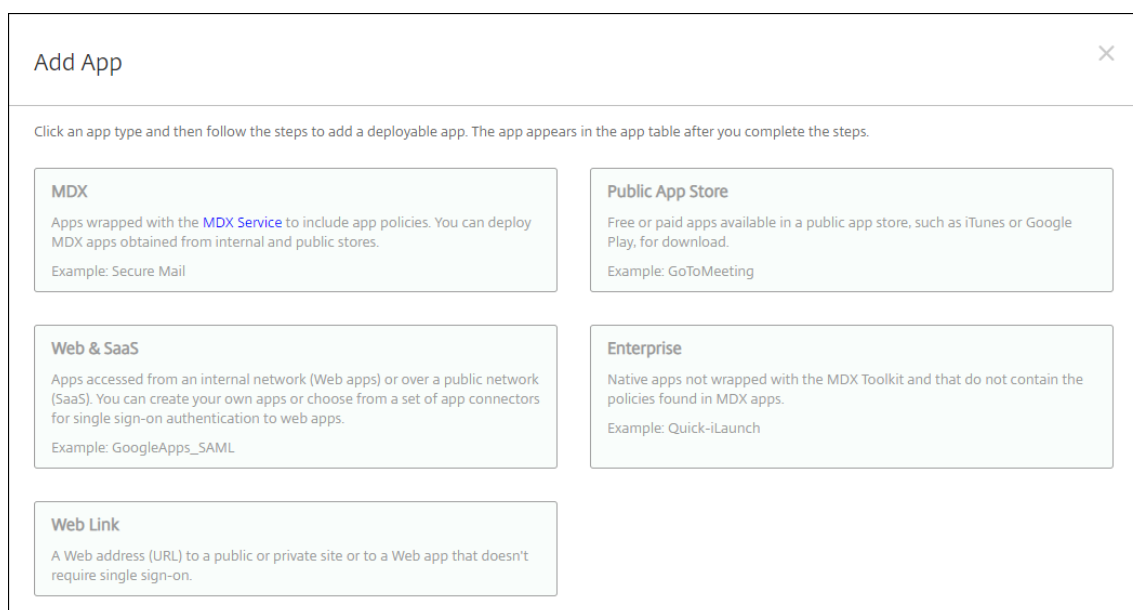
```
1  ```
2  java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -
   Duser.variant
3  -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
4  -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
5  -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
6  -MinPlatform 5.0
7  -keystore /MyKeystore
8  -storepass mystorepwd123
9  -keyalias key0
10 -keypass mykeypwd123
11 -storeURL "https://play.google.com/store/apps/details?id=
   SampleAEAppPackage"
12 -appType Premium
13 -premiumMdxPolicies <Path to Premium policy XML>
14 <!--NeedCopy--> ```
```

Wrapping the app generates a wrapped .apk file and a .mdx file.

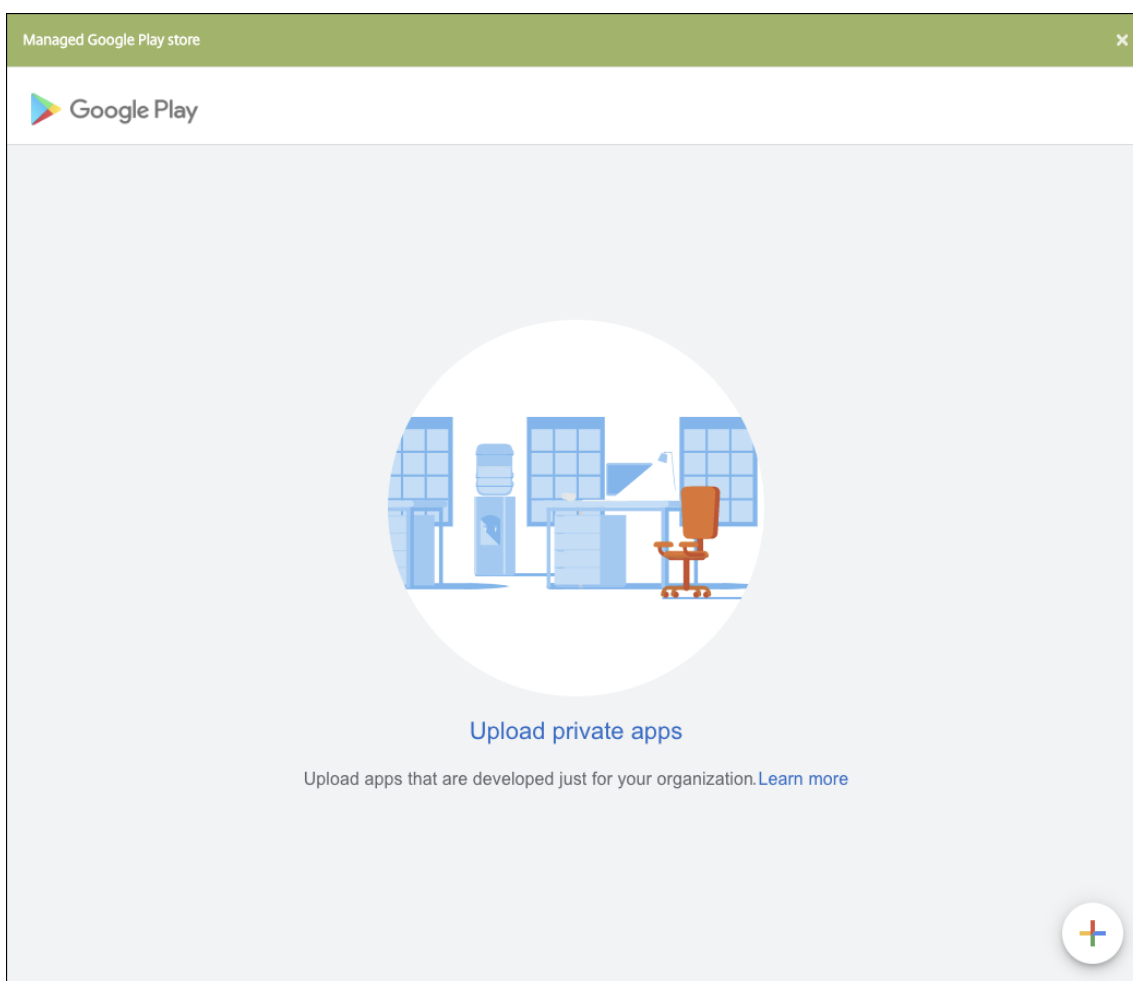
### Add the wrapped .apk file

Add the app one of two ways:

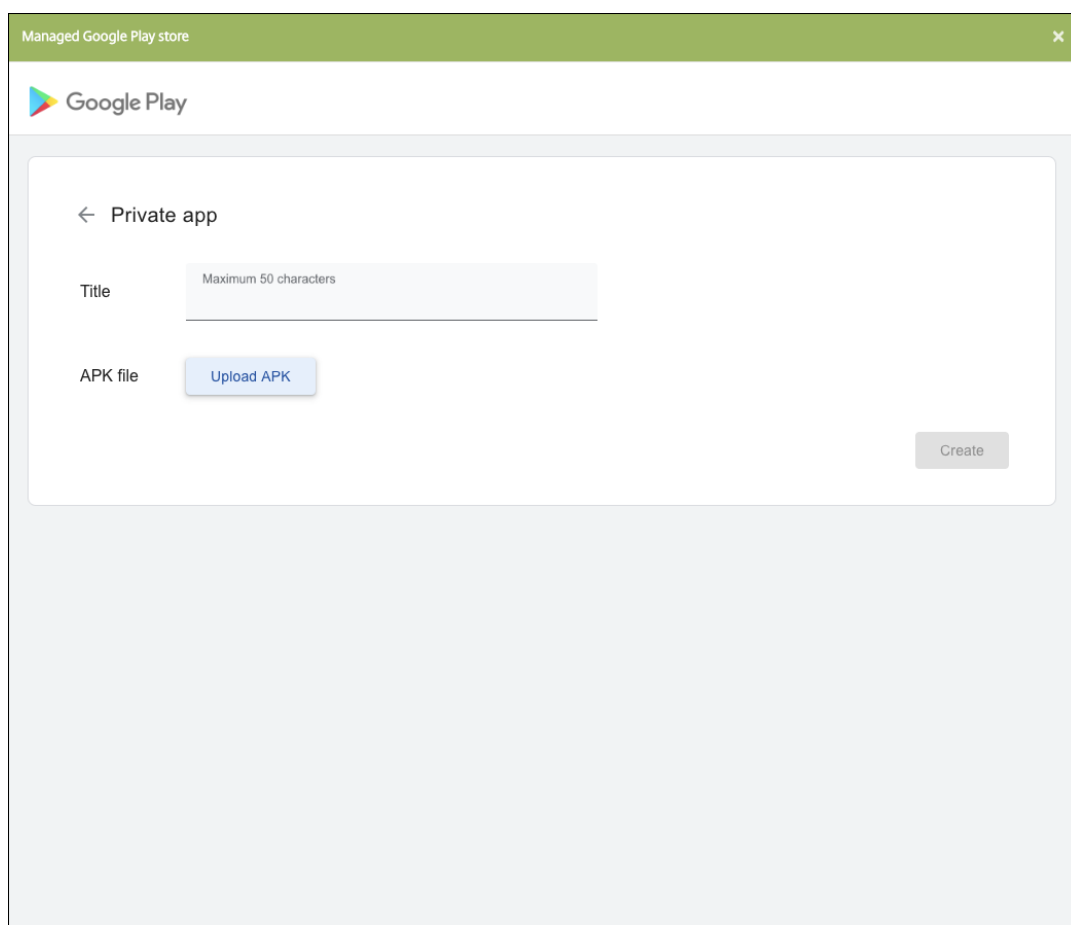
- Publish the app directly to the managed Google Play Store and add it to the Endpoint Management console as a Managed play store app. Follow the Google documentation on how to [Publish private apps](#), and then follow the steps in the Managed app store apps section.
- Add the app to the Endpoint Management console as an enterprise app. Perform the following steps:
  1. In the Endpoint Management console, click **Configure > Apps**. The **Apps** page opens.
  2. Click **Add**. The **Add App** dialog box appears.



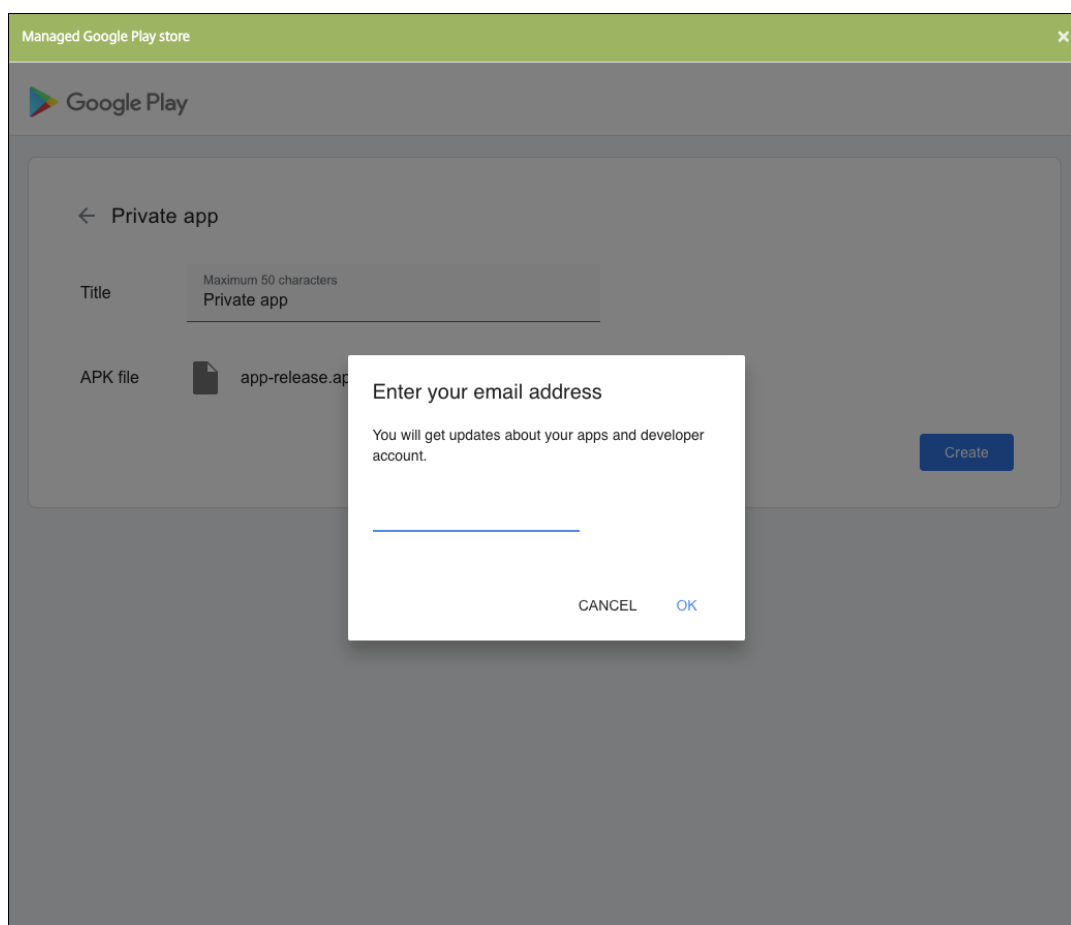
3. Click **Enterprise**. In the **App Information** pane, type the following information:
  - **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see [About app categories](#).
4. Select **Android Enterprise** or **Android for Workspace** as the platform.
5. The **Upload** button opens the managed Google Play Store. You do not need to register for a developer account to publish a private app. Click the **Plus** icon in the lower right corner to continue.



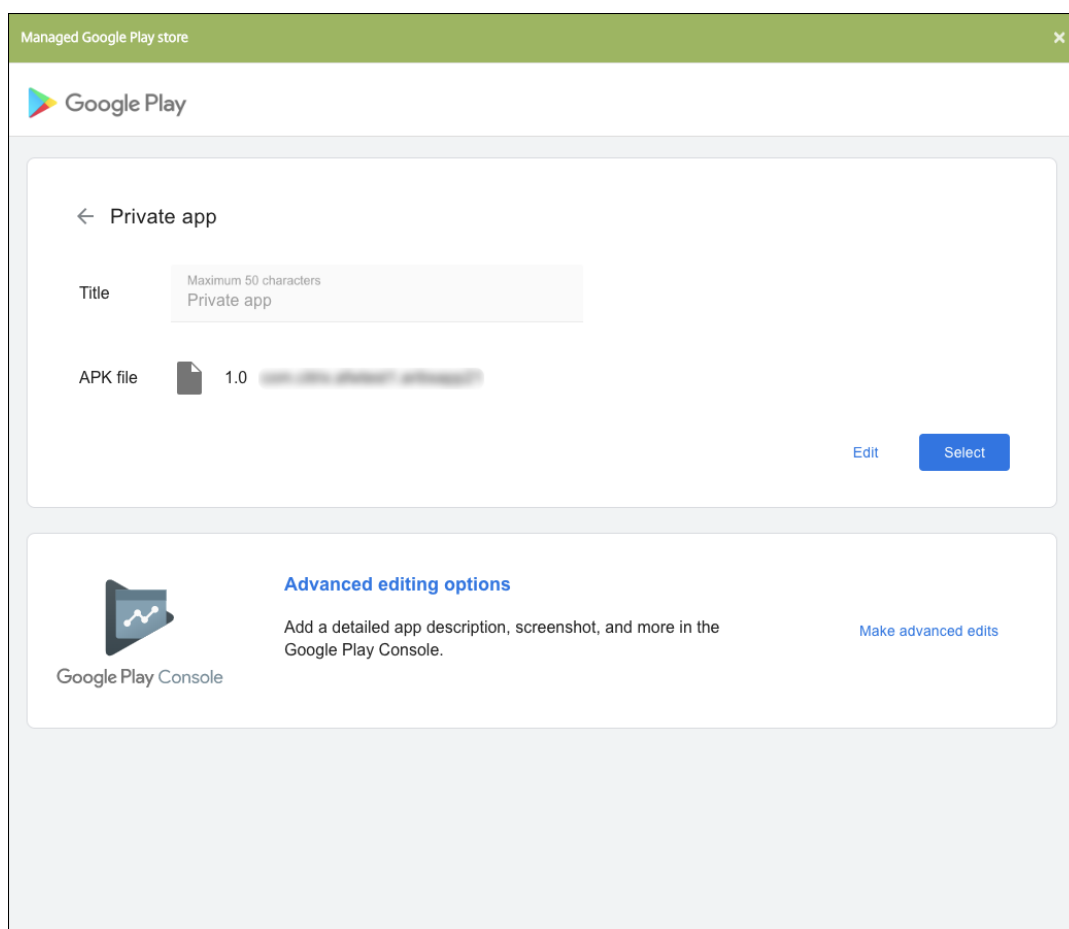
- a) Type the name for your app and upload the .apk file. When finished, click **Create**. It might take up to 10 minutes for your private app to publish.



b) Enter an email address to get updates about your apps.



- c) After your application is published, click the icon for the private app and click **Select** to open the app information page.



6. Click **Next**. The app information page for the platform appears.
7. Configure the settings for the platform type, such as:
  - **File name:** Optionally, type a new name for the app.
  - **App description:** Optionally, type a new description for the app.
  - **App version:** You can't change this field.
  - **Package ID:** Unique identifier of your app.
  - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
  - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
  - **Excluded devices:** Optionally, type the manufacturer or models of devices that cannot run the app.
8. Configure the deployment rules and store configuration.
9. In the **Enterprise App** page, click **Next**. The **Approvals** page appears.

To use workflows to require approval before allowing users to access the app, see [Apply workflows](#). If you don't need an approval workflow, you can skip to Step 13.

10. Click **Next**.
11. The **Delivery Group Assignment** page appears. No action is needed on this page. You configure the delivery groups and deployment schedule for this app when you add the .mdx file. Click **Save**.

### Optional: Add or change the store URL

If you didn't know the store URL when you wrapped the app, add the store URL now.

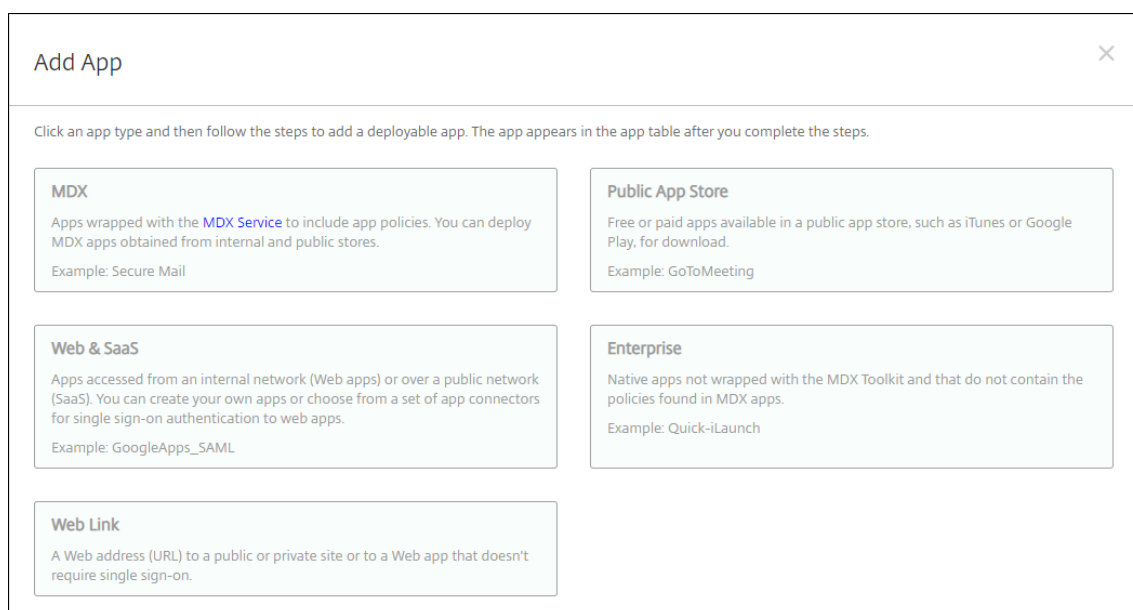
1. View the app in the managed Google Play Store. When you select the app, the store URL appears in the address bar of your browser. Copy the package name of the app from the URL form. For example: <https://play.google.com/store/apps/details?id=SampleAEappPackage>. The URL you copy may begin with <https://play.google.com/work/>. Ensure that you change *work* to *store*.
2. Use the MDX Toolkit to add the store URL to the .mdx file:

```
1 java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \  
2 setinfo \  
3 -in ~/Desktop/SampleApps/Sample.mdx \  
4 -out ~/Desktop/SampleApps/wrapped/Sample.mdx \  
5 -storeURL "https://play.google.com/store/apps/details?id=  
SampleAEappPackage"  
6 <!--NeedCopy-->
```

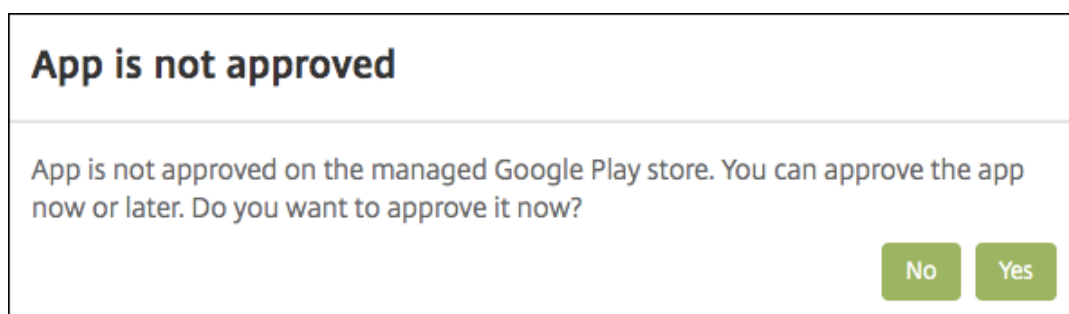
### Add the .mdx file

1. In the Endpoint Management console, click **Configure > Apps**. Click **Add**. The **Add App** dialog box appears.

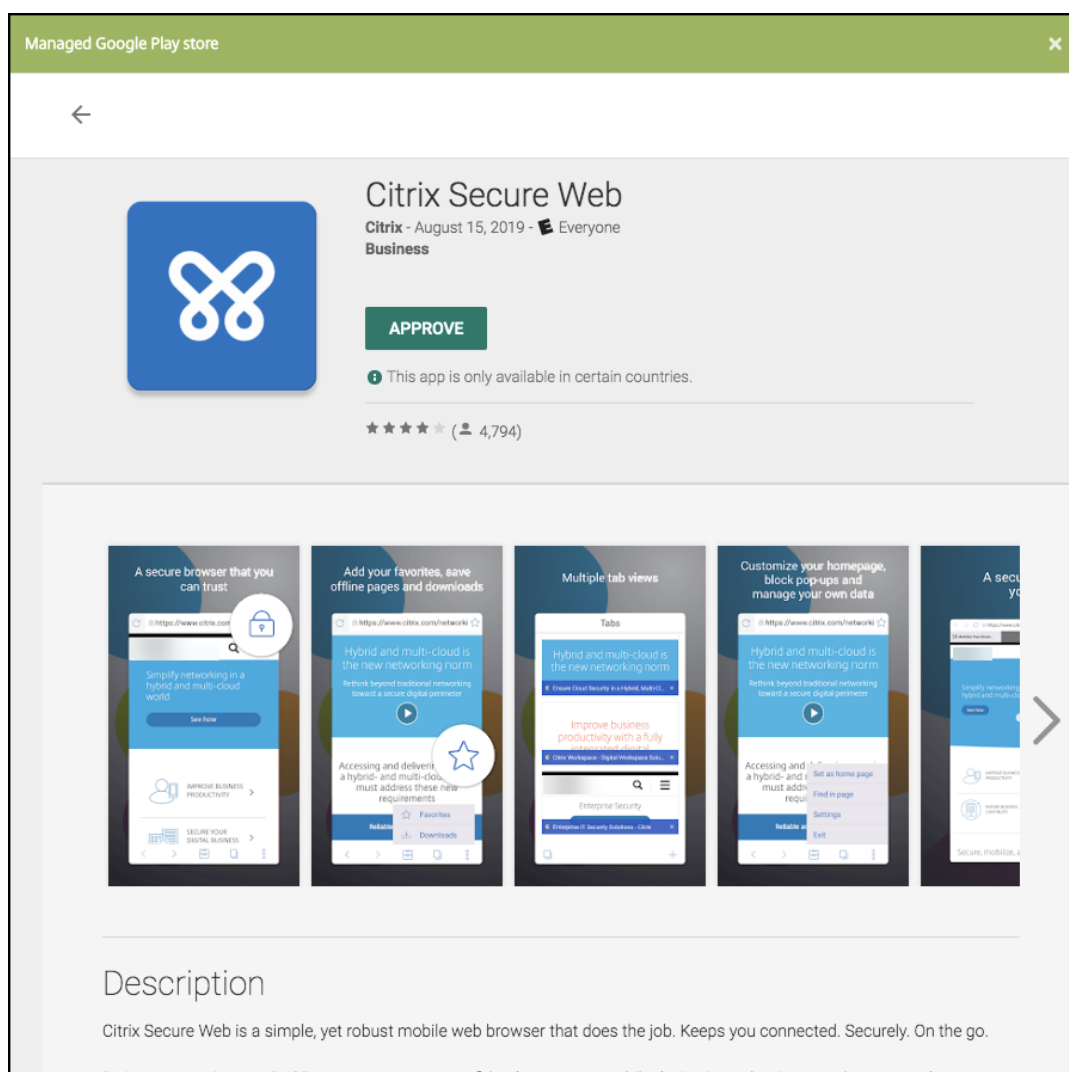




2. Click **MDX**. The **MDX App Information** page appears. In the **App Information** pane, type the following information:
  - **Name:** Type a descriptive name for the app. The name appears under **App Name** on the **Apps** table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see [About app categories](#).
3. Select **Android Enterprise** or **Android for Workspace** as the platform.
4. Click **Upload** and navigate to the MDX file. Android Enterprise and Android for Workspace only support apps wrapped with the MDX Toolkit.
  - The UI notifies you if the attached application requires approval from the managed Google Play Store. To approve the application without leaving the Citrix Endpoint Management console, click **Yes**.



After the managed Google Play Store opens, follow the instructions to approve and save the app.



When you successfully add the app, the **App details** page appears.

5. Configure these settings:

- **File name:** Type the file name associated with the app.
- **App Description:** Type a description for the app.
- **App version:** Optionally, type the app version number.
- **Package ID:** Type the package ID for the app, obtained from the managed Google Play Store.
- **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
- **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
- **Excluded devices:** Optionally, type the manufacturer or models of devices that cannot run the app.

6. Configure the **MDX Policies**. MDX policies vary by platform and include options for policy areas, including Authentication, Device Security, and App Restrictions. In the console, each of the policies has a tooltip that describes the policy. For information about the app policies that are available for each device platform type, see:

- [MAM SDK overview](#)
- [MDX third-party app policies at a glance](#)

7. Configure the deployment rules and store configuration.

The **Deploy for always-on connection** applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.

The always-on option:

- Is not available for iOS devices
- Is not available for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management with version 10.18.19 or later
- Is not recommended for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management before version 10.18.19

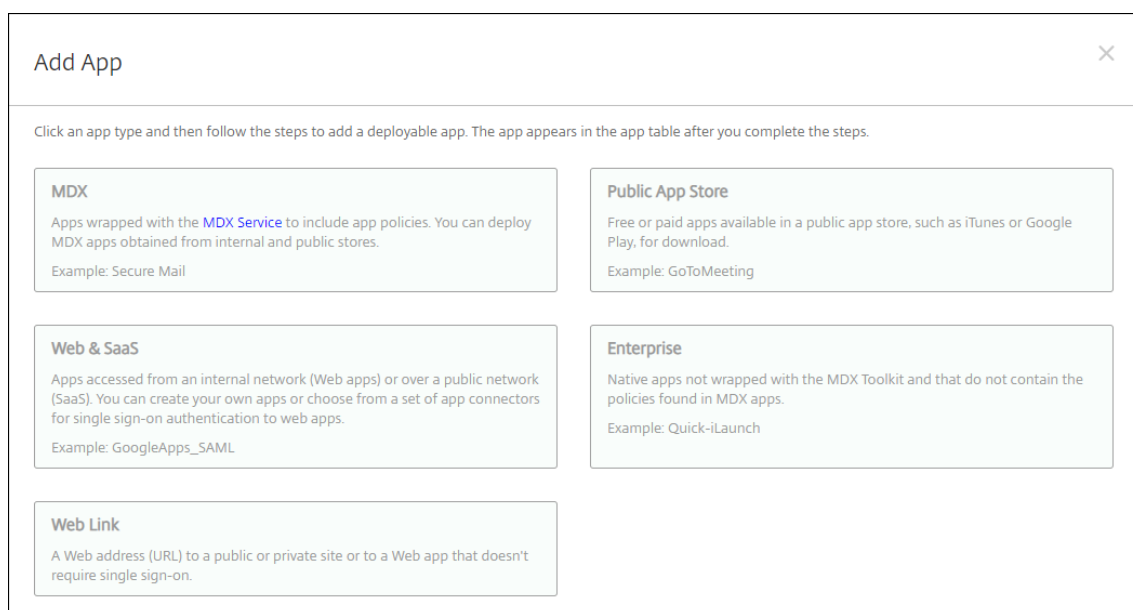
The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

8. Assign any delivery groups to the app and click **Save**. For information, see [Deploy resources](#).

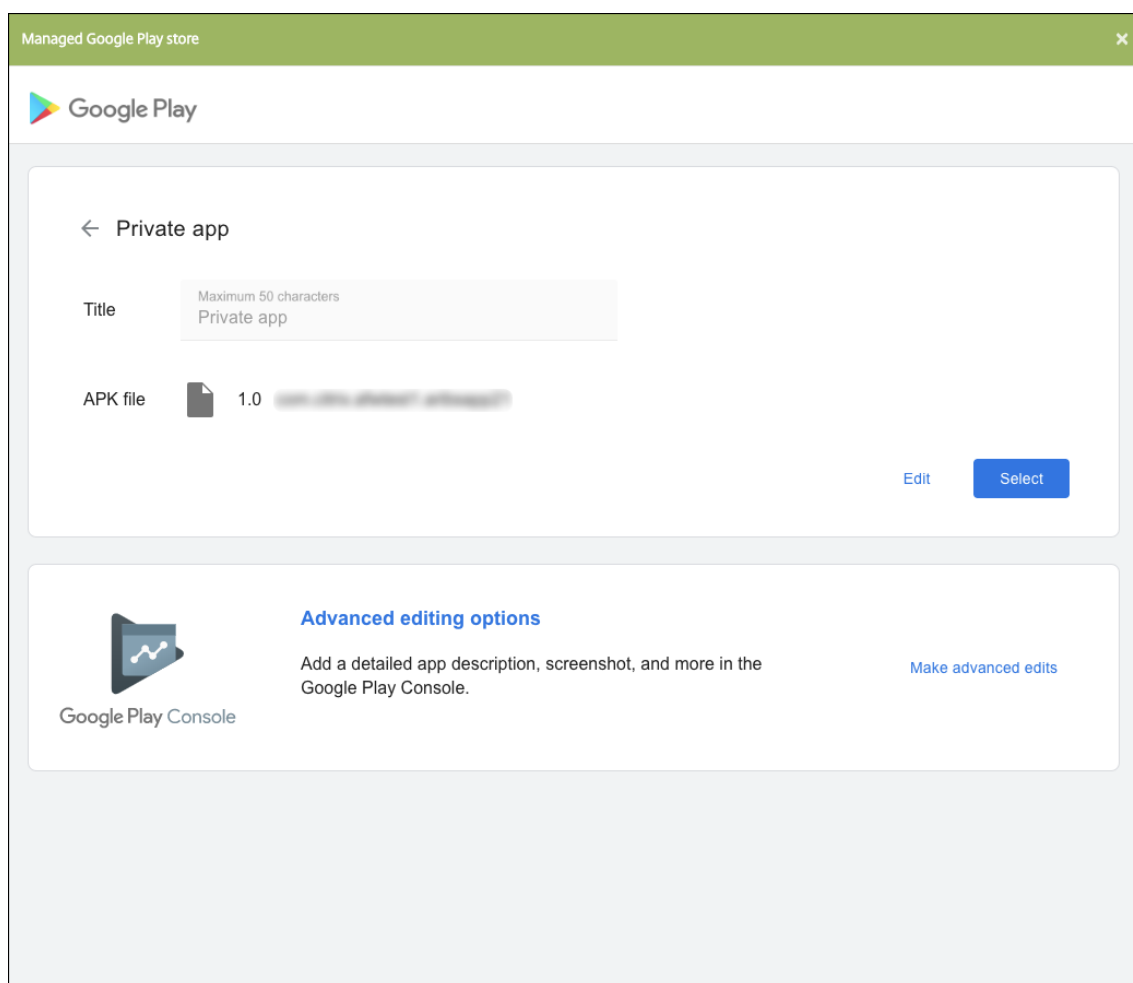
### Update the app

To update the Android Enterprise or Android for Workspace app, wrap and upload an updated .apk file:

1. Wrap the .apk file for the updated app using the MAM SDK or MDX Toolkit.
2. In the Endpoint Management console, click **Configure > Apps**. The **Apps** page opens.



3. Click **Add**. The **Add App** dialog box appears.
4. Click **Enterprise**. In the **App Information** pane, type the following information:
  - **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see [About app categories](#).
5. Select **Android Enterprise** or **Android for Workspace** as the platform.
6. Click **Next**. The **Enterprise App** page appears.
7. Click **Upload**.
8. In the managed Google Play Store page, select the app you want to update.
9. In the app information page, click **edit** next to the .apk file name.



10. Navigate to the new .apk file and upload it.
11. In the managed Google Play Store page, click **Save**.

## Legacy Android Enterprise for Google Workspace (formerly G Suite) customers

July 20, 2021

Google Workspace customers must use the legacy Android Enterprise settings to configure legacy Android Enterprise. Google recently renamed G Suite to Google Workspace.

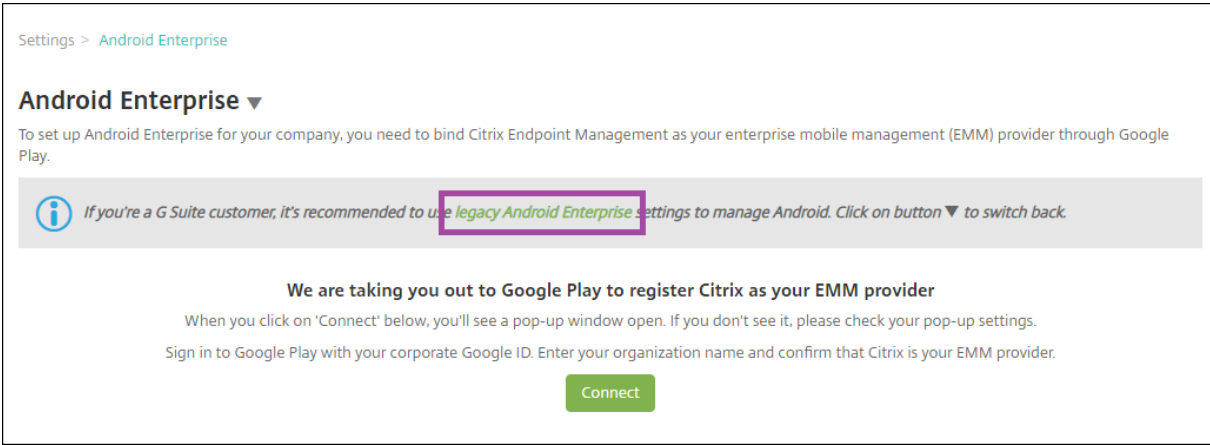
If your organization already uses Google Workspace to provide users access to Google apps, you can use Google Workspace to register Citrix as your EMM. If your organization uses Google Workspace, it has an existing enterprise ID and existing Google Accounts for users. To use Endpoint Management with Google Workspace, you sync with your LDAP directory and retrieve Google Account information

from Google using the Google Directory API. Because this type of enterprise is tied to an existing domain, each domain can only create one enterprise. To enroll a device in Endpoint Management, each user must manually sign in with their existing Google Account. The account gives them access to managed Google Play in addition to any other Google services provided by your Google Workspace plan.

Requirements for legacy Android Enterprise:

- A publicly accessible domain
- A Google administrator account
- Android devices that have managed profile support
- A Google account that has Google Play installed
- A Work profile set up on the device

To start configuring legacy Android Enterprise, click **legacy Android Enterprise** in the **Android Enterprise** page in Endpoint Management Settings.



Settings > Android Enterprise

### Android Enterprise ▼

To set up Android Enterprise for your company, you need to bind Citrix Endpoint Management as your enterprise mobile management (EMM) provider through Google Play.

*If you're a G Suite customer, it's recommended to use **legacy Android Enterprise** settings to manage Android. Click on button ▼ to switch back.*

**We are taking you out to Google Play to register Citrix as your EMM provider**

When you click on 'Connect' below, you'll see a pop-up window open. If you don't see it, please check your pop-up settings.

Sign in to Google Play with your corporate Google ID. Enter your organization name and confirm that Citrix is your EMM provider.

[Connect](#)

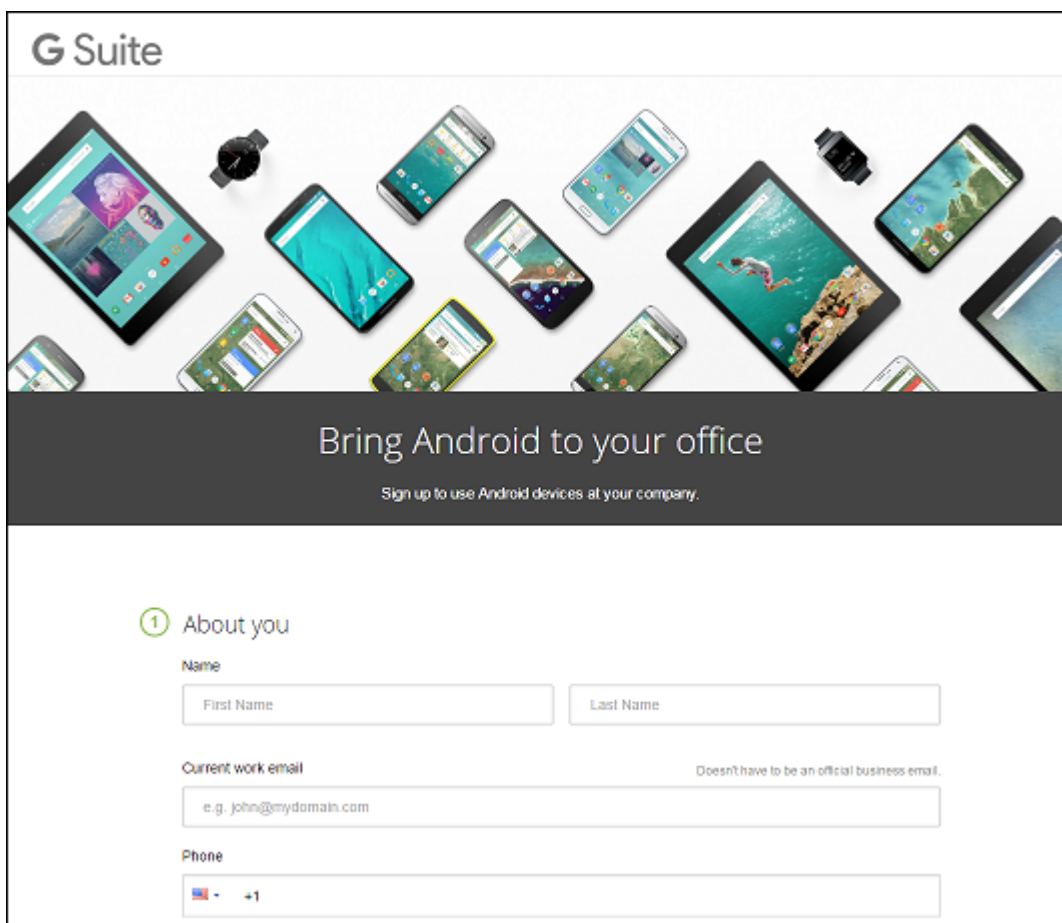
## Create an Android Enterprise Account

Before you can set up an Android Enterprise account, you must verify your domain name with Google.

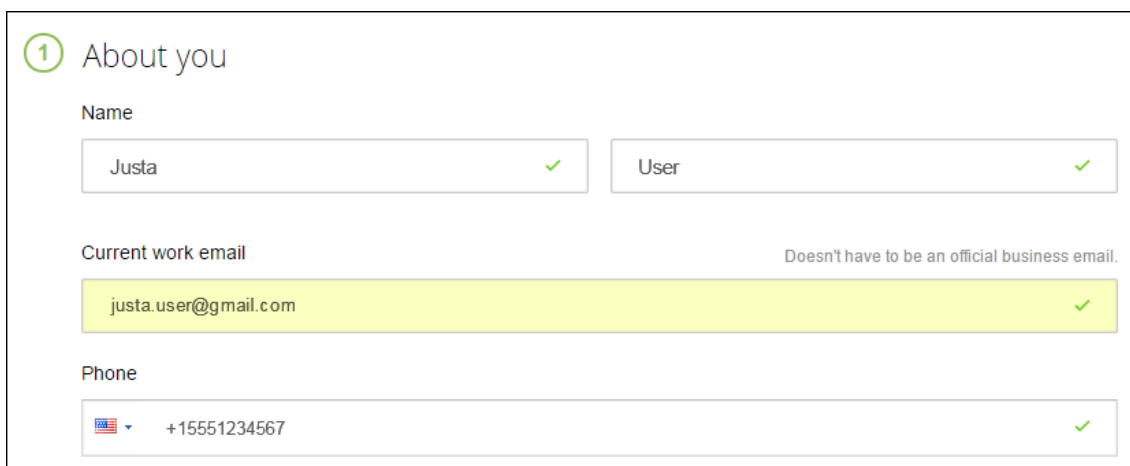
If you have already verified your domain name with Google, you can skip to this step: Set up an Android Enterprise service account and download an Android Enterprise certificate.

1. Navigate to <https://gsuite.google.com/signup/basic/welcome>.

The following page displays where you type your administrator and company information.



2. Type your administrator user information.



3. Type your company information, in addition to your administrator account information.

2 About your business

Business name  
EXAMPLE CORP ✓

Business domain address You'll need to verify that you own this domain.  
example.com ✓

Number of employees Country/Region  
1 employee United States

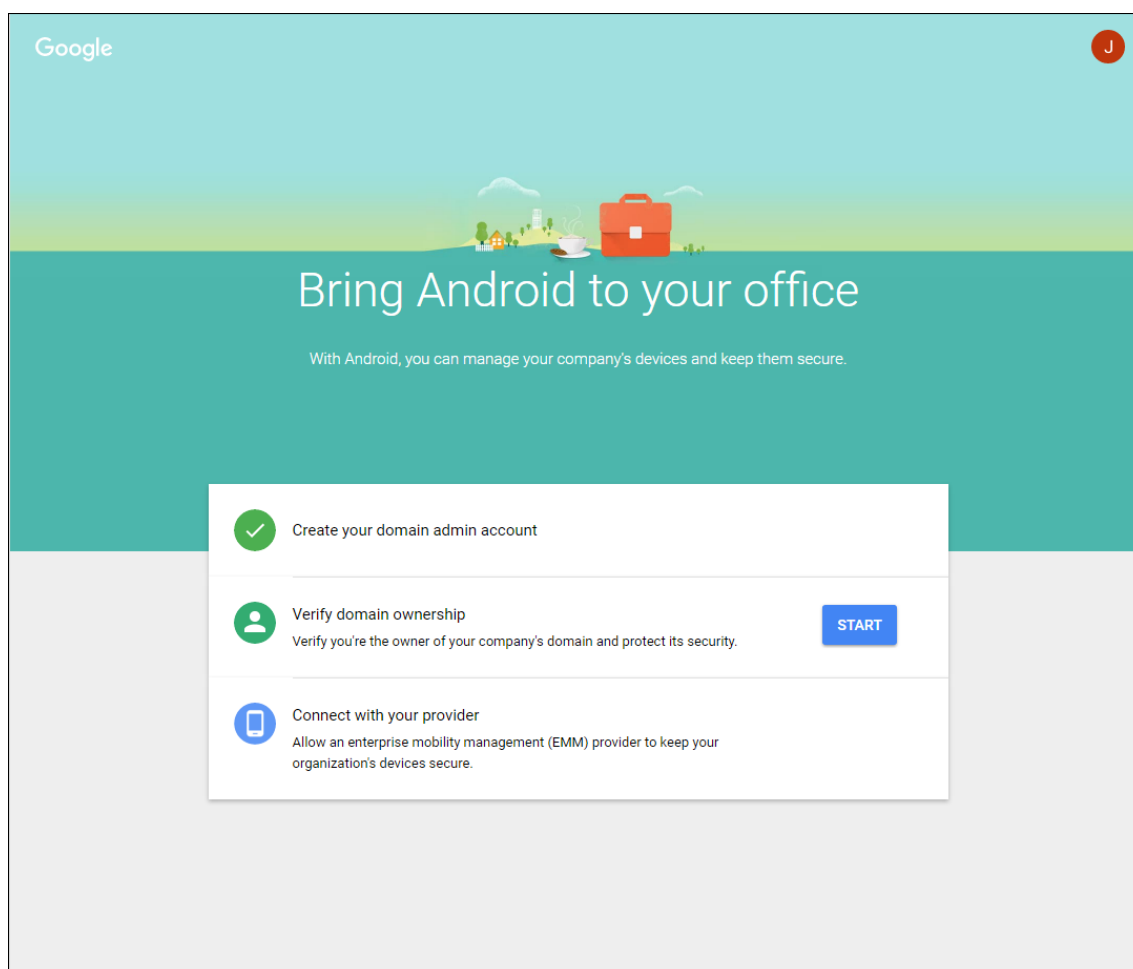
3 Your Google admin account Why do I need this?

Username Create an account to manage Android for Work  
justa.user ✓ @ example.com

Create a password 8-character minimum; case sensitive  
..... ✓  
..... ✓

The first step in the process is complete and you see the following page.





## Verify domain ownership


Allow Google to verify your domain in one of the following ways:

- Add a TXT or CNAME record to the website of your domain host.
- Upload an HTML file to the web server of your domain.
- Add a `<meta>` tag to your home page. Google recommends the first method. This article does not cover the steps to verify your domain ownership, but you can find the information you need here: <https://support.google.com/a/answer/6248925>.

1. Click **Start** to begin the verification of your domain.

The **Verify domain ownership** page appears. Follow the instructions on the page to verify your domain.

2. Click **Verify**.

 **Verify domain ownership**


Before you can use Google Apps with domain **example.com**, we need to contact your domain host to verify that you own it. Doing this helps ensure that no one can pose as you on Google Apps and send email from your domain. [Learn more](#)


After your domain is verified, we will set up Google Apps email for your users on **example.com**. This will automatically re-route your emails to Google Apps. [Learn more](#)

We have detected that **example.com** is hosted at **GoDaddy.com**. If you're having trouble, try to [verify your domain here](#).

**Note:** Before you route email to Google Apps, make sure that you create a user on Google Apps for each person receiving mail at **example.com**.

[VERIFY](#)

 Need help? Search the [Help Center](#) or call **844-390-7627** and provide your unique PIN **12345678**

 **Verify domain ownership**

**Verification checklist**

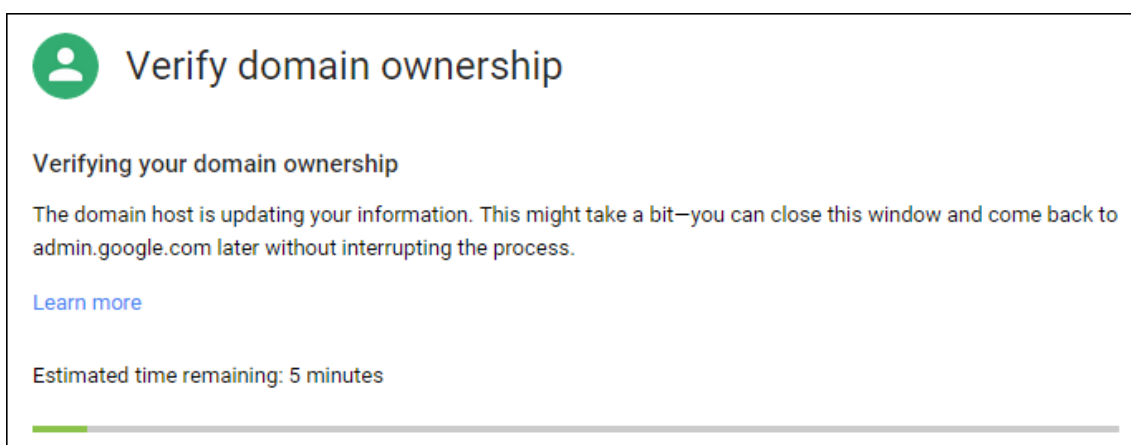
Follow these steps to help Google verify that you own the domain **example.com**.

[Learn more](#)

- I have successfully logged in.
- I have opened the control panel for my domain.
- I have created the CNAME record.
- I have saved the CNAME record.

[VERIFY](#)

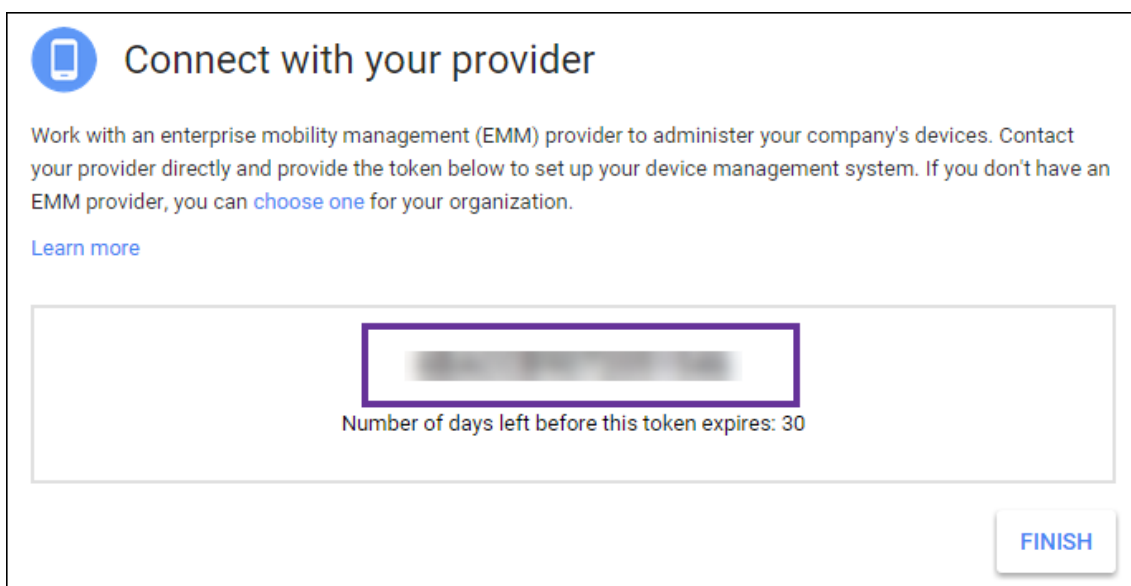
3. Google verifies your domain ownership.



4. After successful verification, the following page appears. Click **Continue**.



5. Google creates an EMM binding token that you provide to Citrix and use when you configure Android Enterprise settings. Copy and save the token; you need it later in the setup procedure.



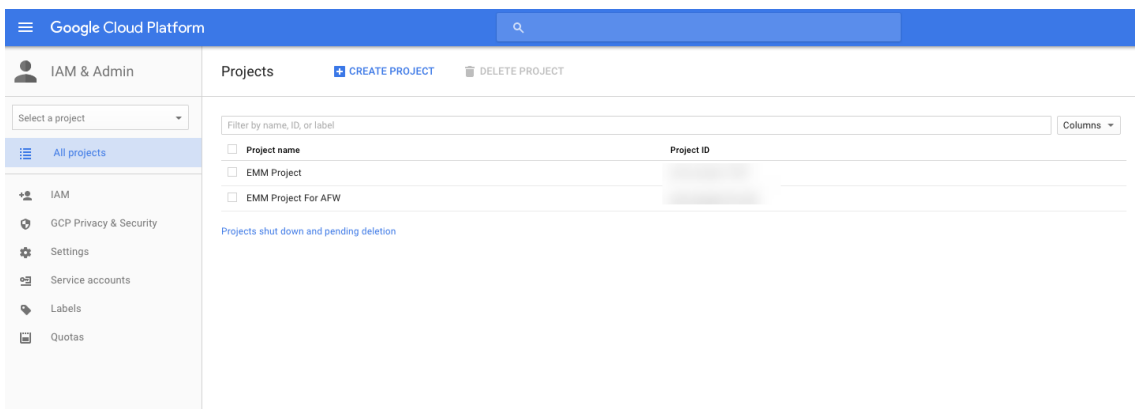
6. Click **Finish** to complete setting up Android Enterprise. A page appears, indicating that you've successfully verified your domain.

After you create an Android Enterprise service account, you can sign in to the Google Admin console to manage your mobility management settings.

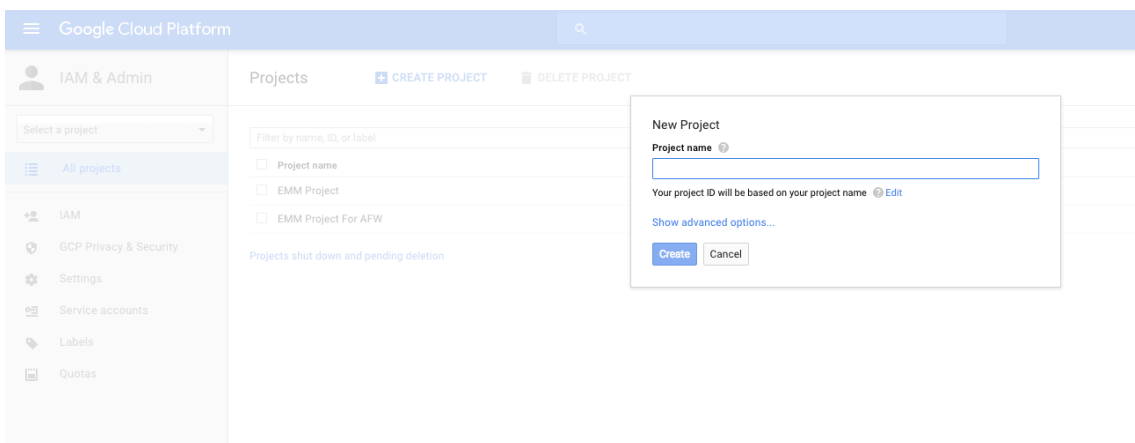
### Set up an Android Enterprise service account and download an Android Enterprise certificate

To allow Endpoint Management to contact Google Play and Directory services, you must create a service account using the Google Project portal for developers. This service account is used for server-to-server communication between Endpoint Management and Google services for Android. For more information about the authentication protocol being used, go to <https://developers.google.com/identity/protocols/OAuth2ServiceAccount>.

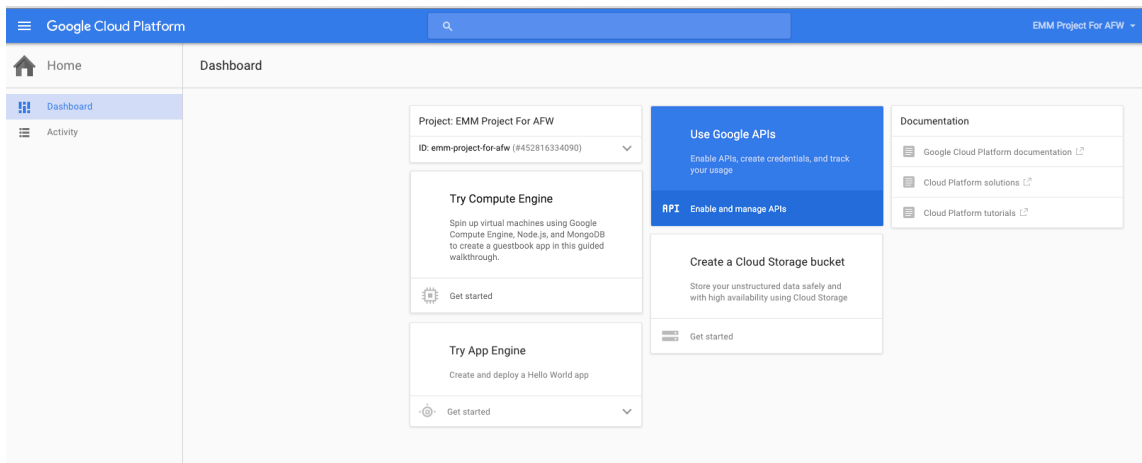
1. In a web browser, go to <https://console.cloud.google.com/project> and sign in with your Google administrator credentials
2. In the **Projects** list, click **Create Project**.



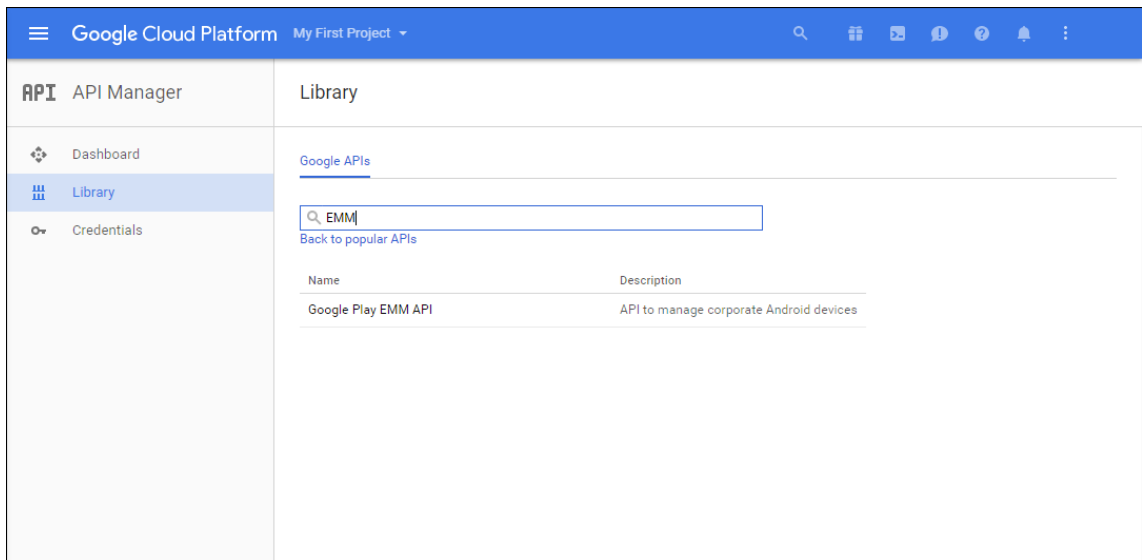
3. In **Project name**, type a name for the project.



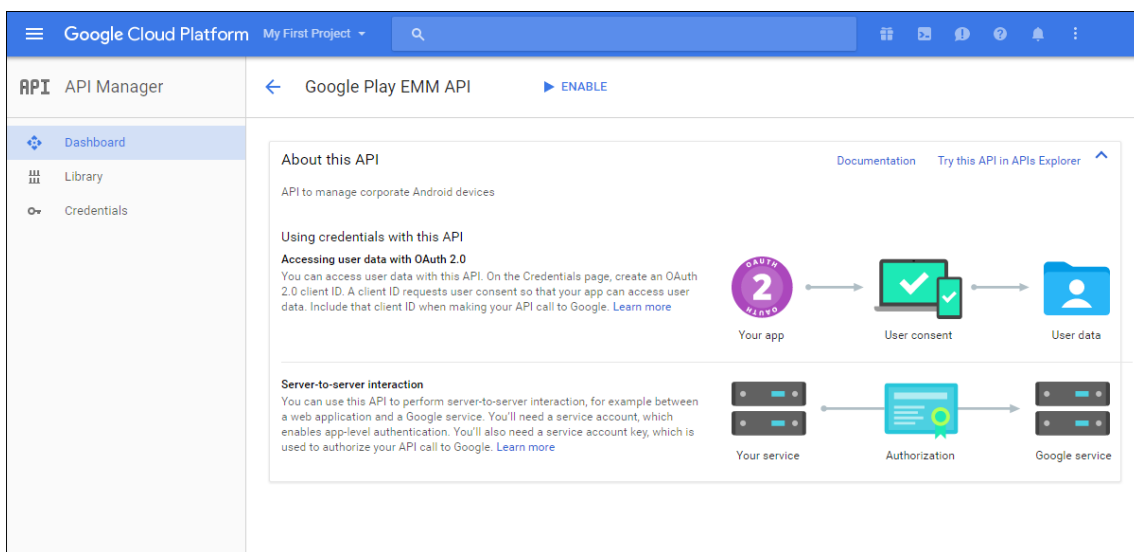
4. On the Dashboard, click **Use Google APIs**.



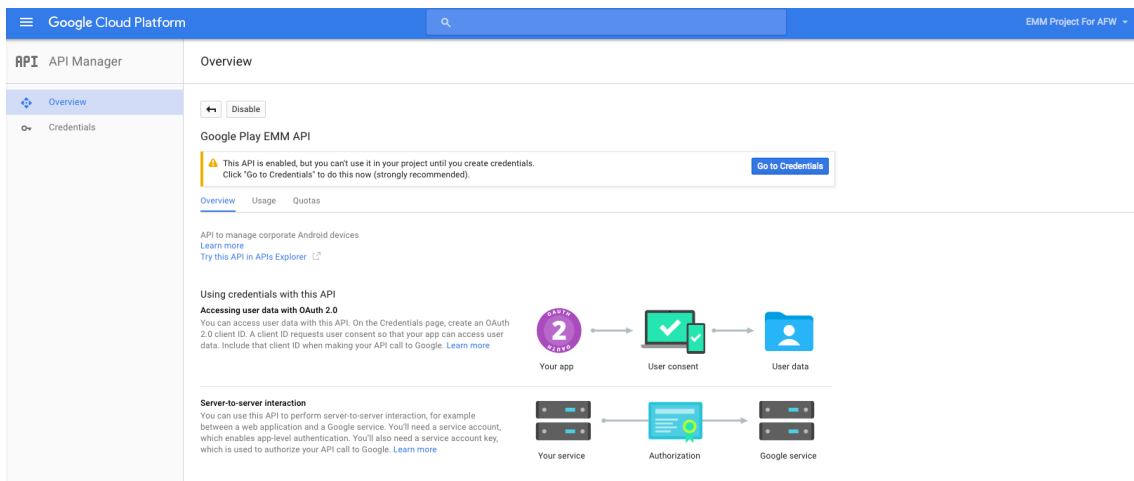
5. Click **Library**, in **Search**, type **EMM** and then click the search result.



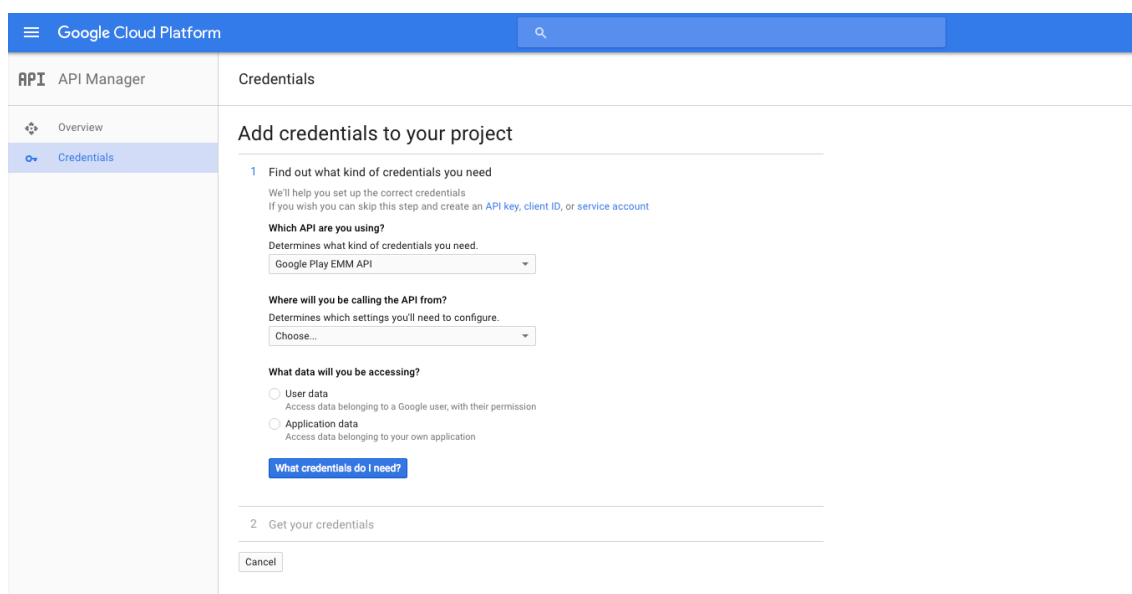
6. On the **Overview** page, click **Enable**.



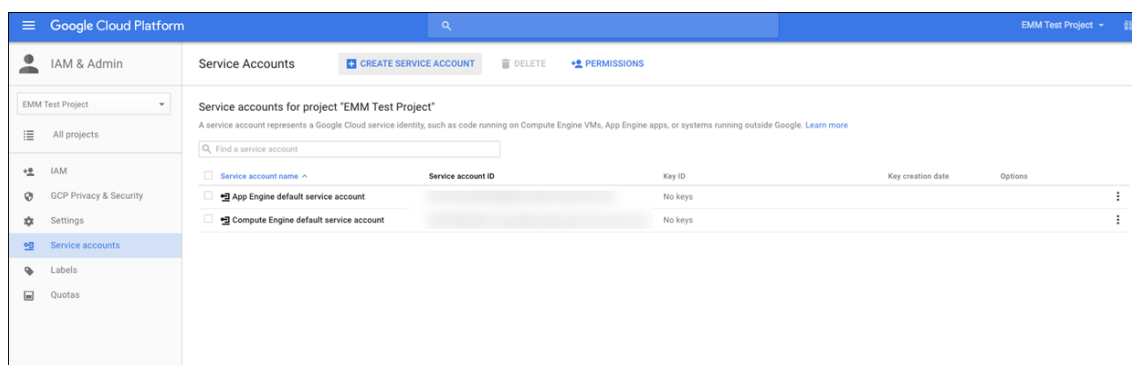
7. Next to **Google Play EMM API**, click **Go to Credentials**.



8. In the **Add credentials to our project** list, in step 1, click **service account**.



9. On the **Service Accounts** page, click **Create Service Account**.



10. In **Create service account**, name the account, and select the **Furnish a new private key** check box. Click **P12**, select the **Enable Google Apps Domain-wide Delegation** check box and then click **Create**.

**Create service account**

Service account name <sup>?</sup>  
testemmsvcacct

Service account ID  
testemmsvcacct

**Furnish a new private key**  
Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

**Key type**

JSON  
Recommended

P12  
For backward compatibility with code using the P12 format

**Enable Google Apps Domain-wide Delegation**  
Grants a client access to all users' data on a Google Apps domain without manual authorization on their part. [Learn more](#)

**To change settings for Google Apps domain, product name for the OAuth consent screen must be configured. Assign the product name below or configure the OAuth consent screen.**

Product name for the consent screen  
anynamewilldo

**Create** Configure consent screen Cancel

The certificate (P12 file) is downloaded to your computer. Be sure to save the certificate in a secure location.

11. On the **Service account created** confirmation page, click **Close**.

**Service account created**

The service account "testemmsvcacct" was given editor permission for the project.

The account's private key [redacted] has been saved on your computer. This is the only copy of the key, so store it securely.

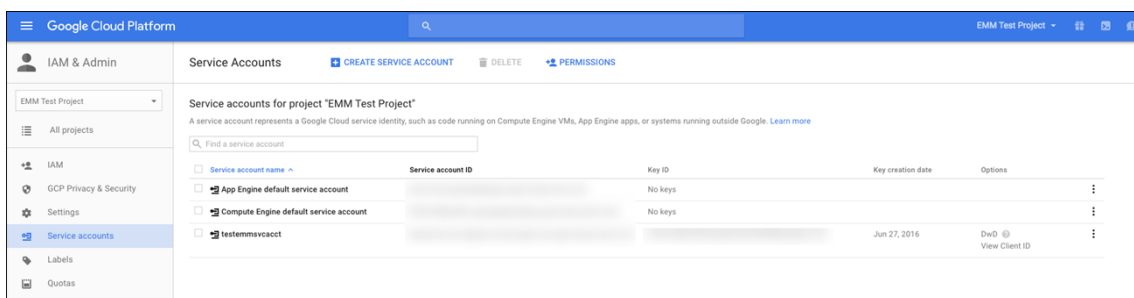
This is the private key's password. It will not be shown again. You must present this password to use the private key. [Learn more](#)

notasecret

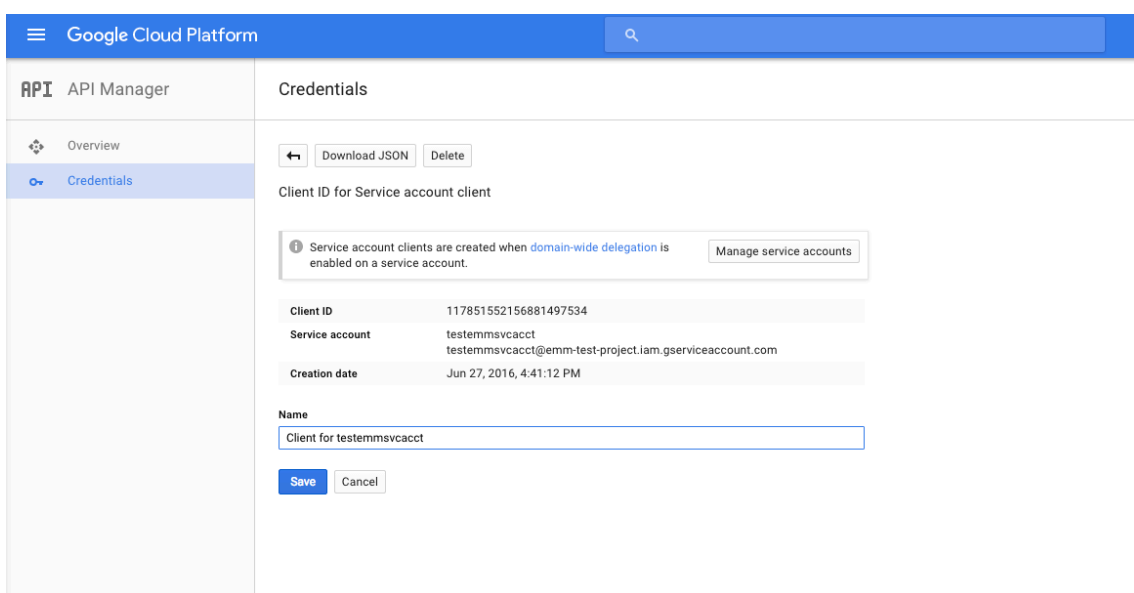
**Close**

12. In **Permissions**, click **Service accounts** and then under **Options** for your service account, click **View Client ID**.

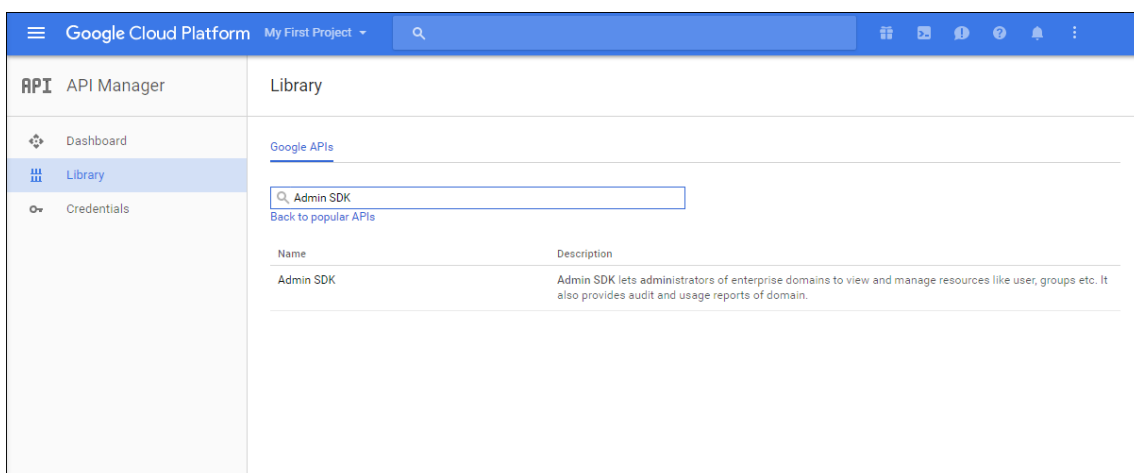




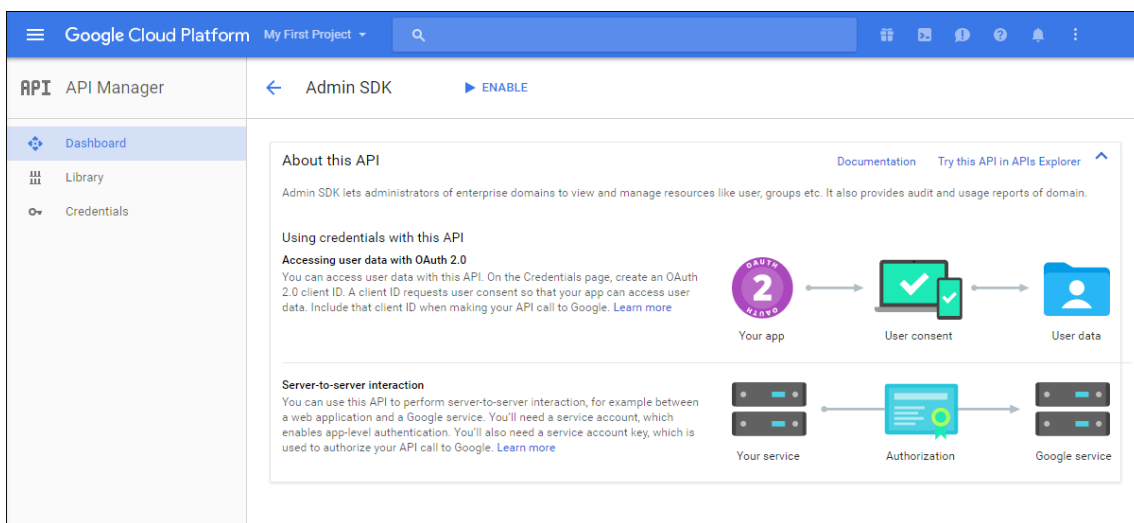
- The details required for account authorization on the Google admin console display. Copy the **Client ID** and **Service account ID** to a location where you can retrieve the information later. You need this information, along with the domain name to send to Citrix support to add to an allow list.



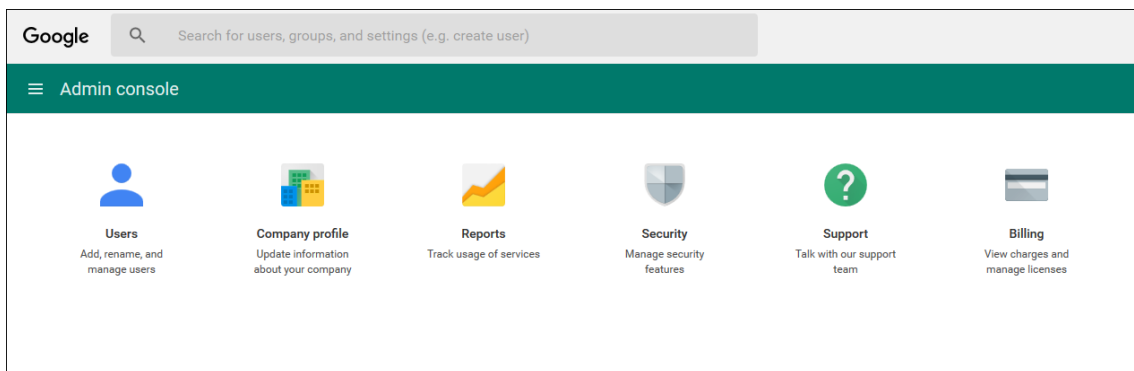
- On the **Library** page, search for **Admin SDK** and then click the search result.



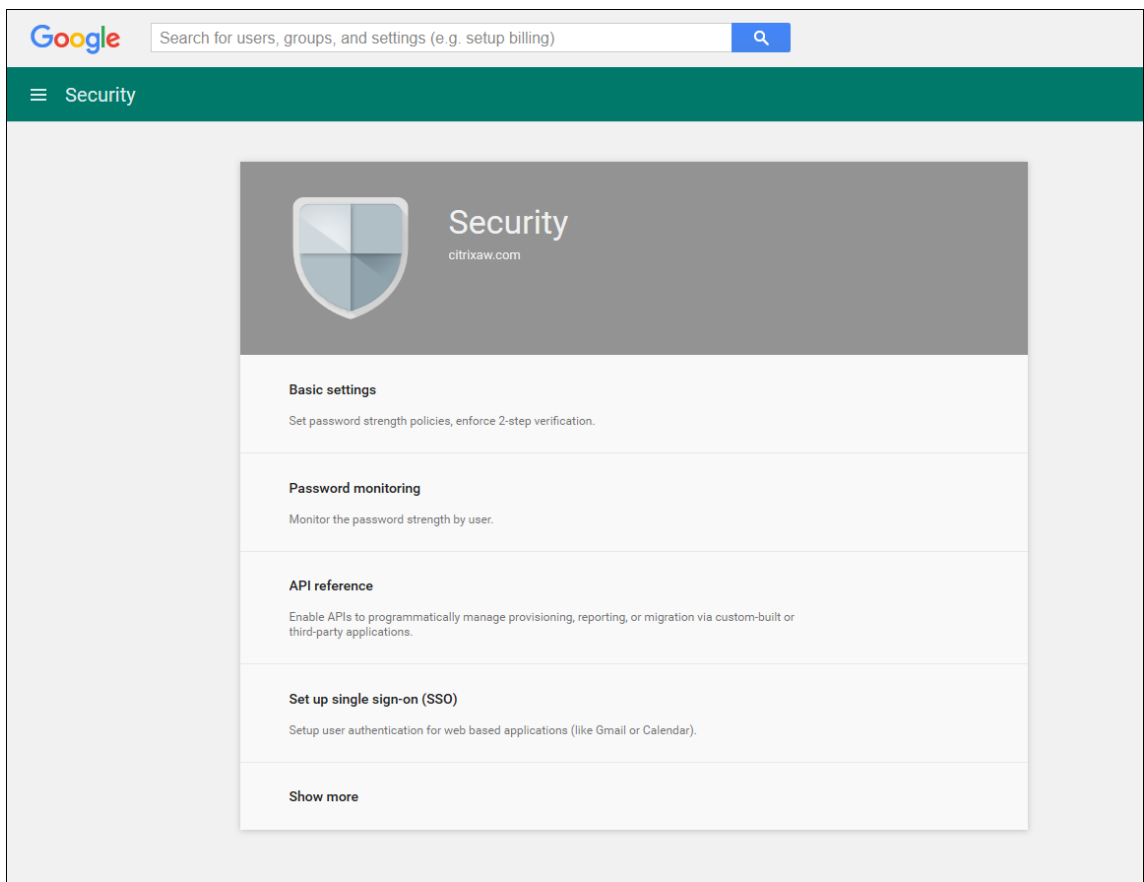
- On the **Overview** page, click **Enable**.

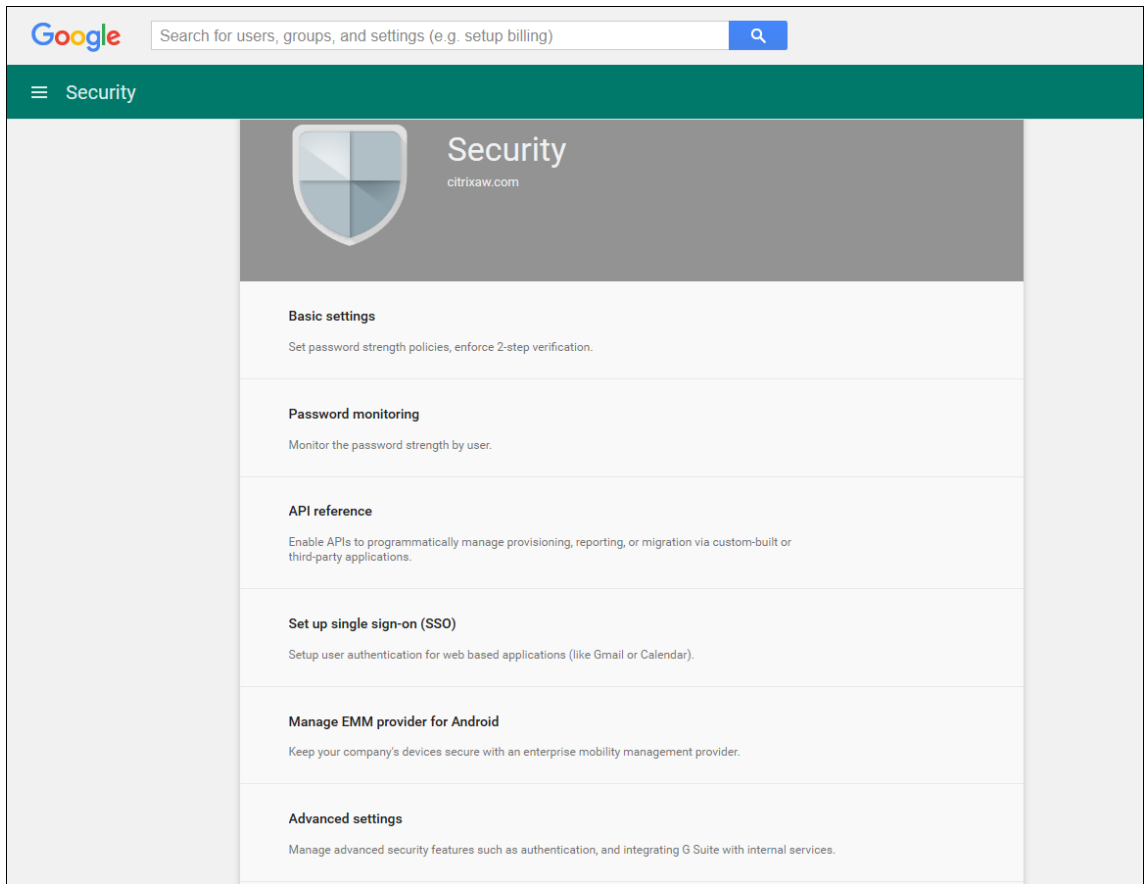


16. Open the Google admin console for your domain and then click **Security**.

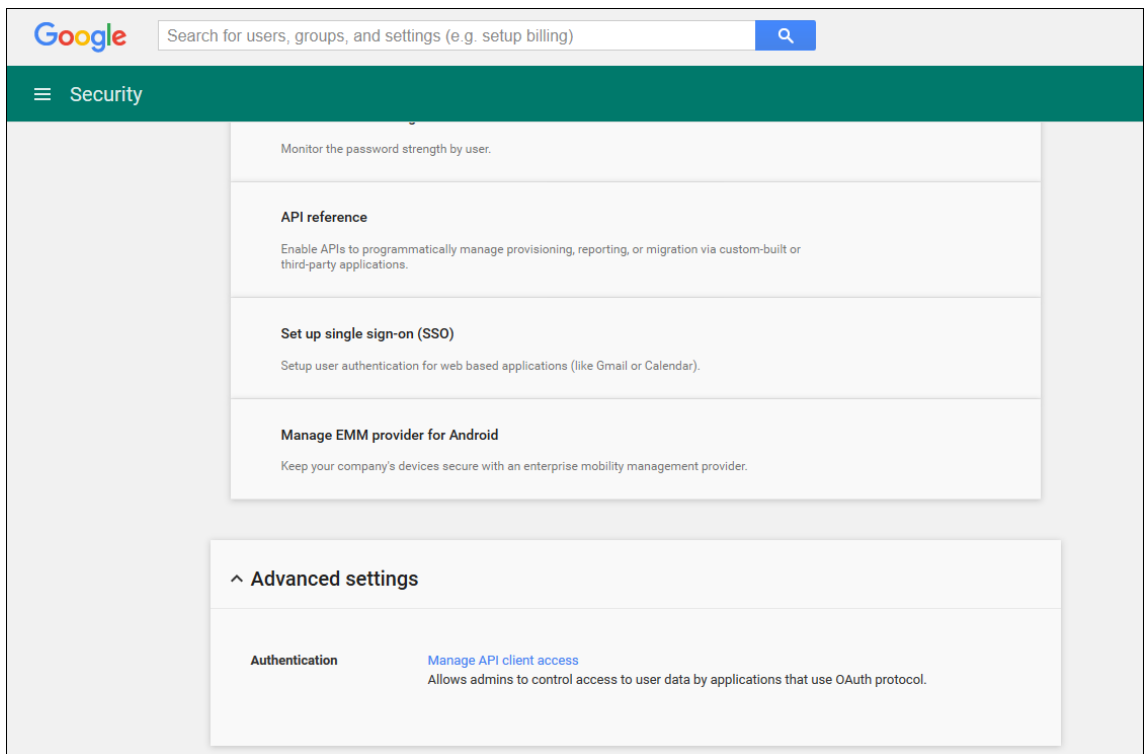


17. On the **Settings** page, click **Show more** and then click **Advanced settings**.

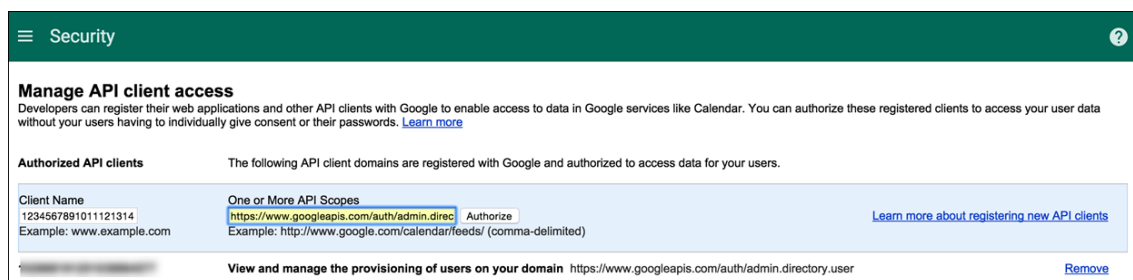




18. Click **Manage API client access**.



19. In **Client Name**, type the client ID that you saved earlier, in **One or More API Scopes**, type `https://www.googleapis.com/auth/admin.directory.user` and then click **Authorize**.



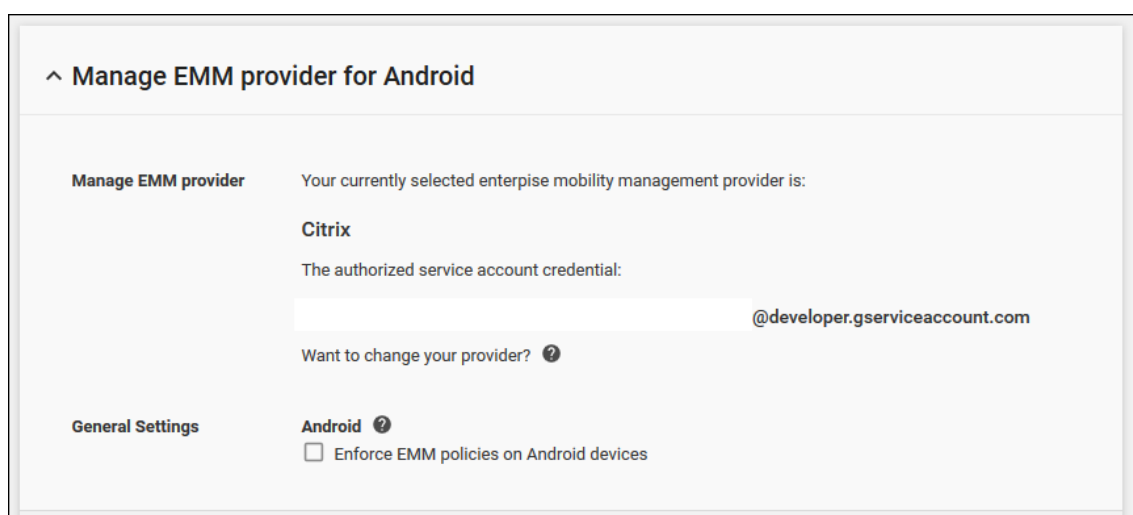
## Binding to EMM

Before you can use Endpoint Management to manage your Android devices, you must contact Citrix Technical Support and provide your domain name, service account, and binding token. Citrix binds the token to Endpoint Management as your enterprise mobility management (EMM) provider. For contact information for Citrix Technical Support, see [Citrix Technical Support](#).

1. To confirm the binding, sign in to the Google Admin portal and then click **Security**.
2. Click **Manage EMM provider for Android**.

You see that your Google Android Enterprise account is bound to Citrix as your EMM provider.

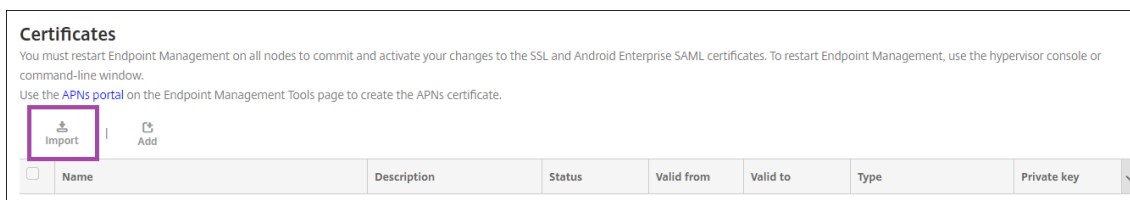
After you confirm the token binding, you can start using the Endpoint Management console to manage your Android devices. Import the P12 certificate you generated in step 14. Set up Android Enterprise server settings, enable SAML-based single-sign-on (SSO), and define at least one Android Enterprise device policy.



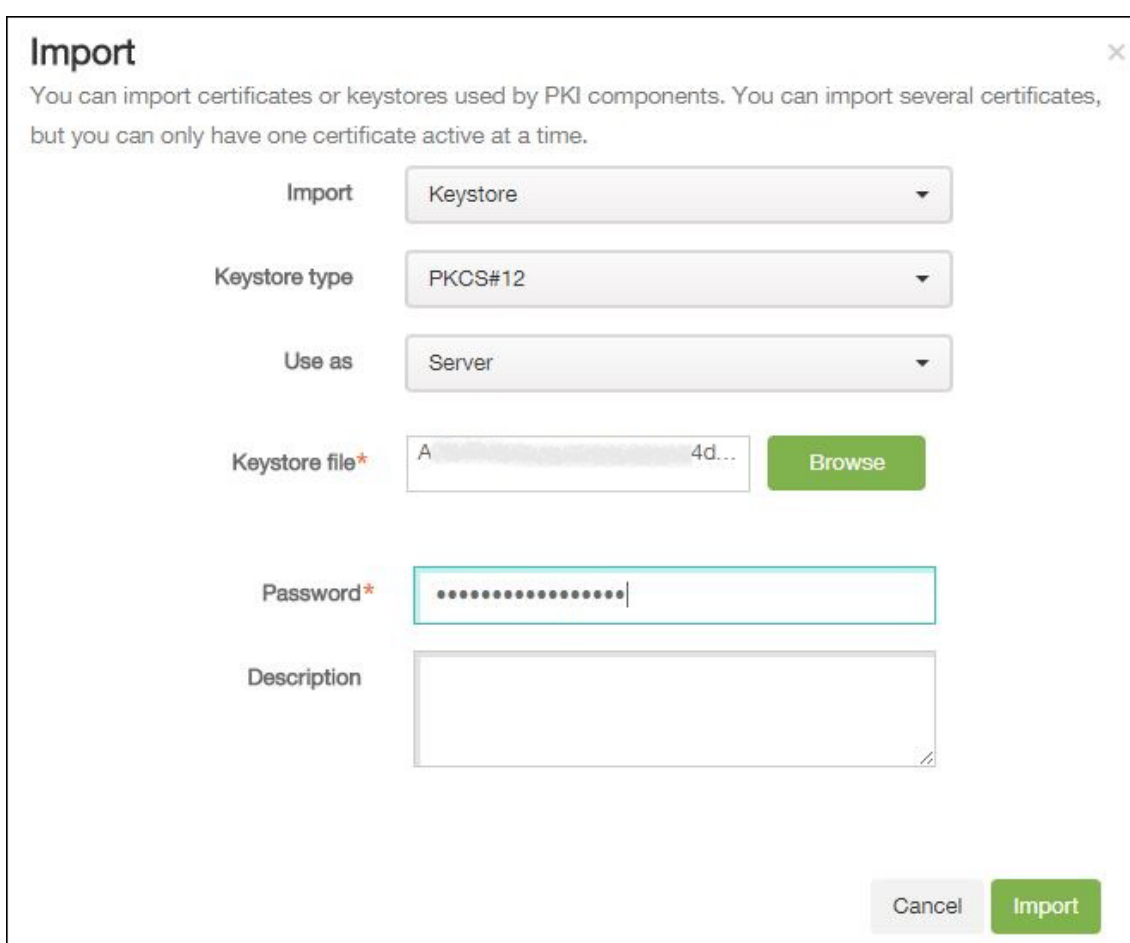
## Import the P12 certificate

Follow these steps to import your Android Enterprise P12 certificate:

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console to open the **Settings** page and then click **Certificates**. The **Certificates** page appears.



2. Click **Import**. The **Import** dialog box appears.



Configure the following settings:

- **Import:** In the list, click **Keystore**.
- **Keystore type:** In the list, click **PKCS#12**.
- **Use as:** In the list, click **Server**.
- **Keystore file:** Click **Browse** and navigate to the P12 certificate.

- **Password:** Type the certificate password. This is the private key password you created when setting up your Android Enterprise account.
  - **Description:** Optionally, type a description of the certificate.
3. Click **Import**.

## Set up Android Enterprise server settings

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Under **Platforms**, click **Android Enterprise**. The **Android Enterprise** page appears.

Settings > Android Enterprise

### Legacy Android Enterprise ▼

Provide Android Enterprise configuration parameters.

Domain Name \*  ?

Domain Admin Account \*  ?

Service Account ID \*  ?

Client ID \*  ?

Enable Android Enterprise  NO

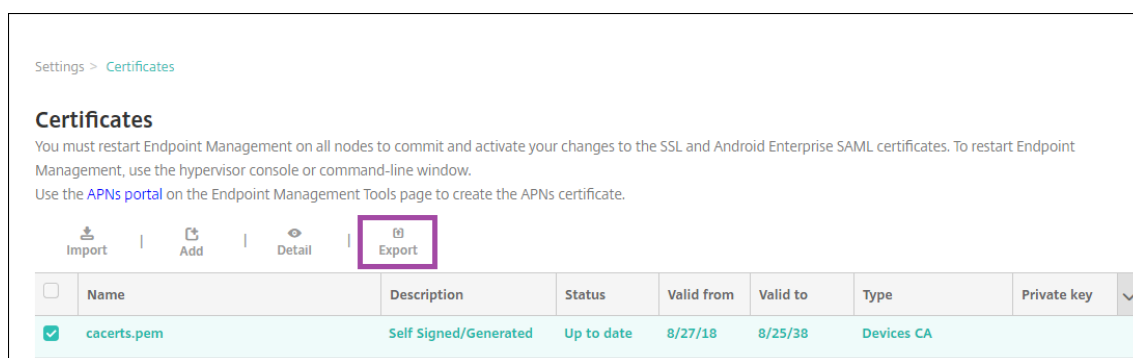
Cancel Save

Configure the following settings and then click **Save**.

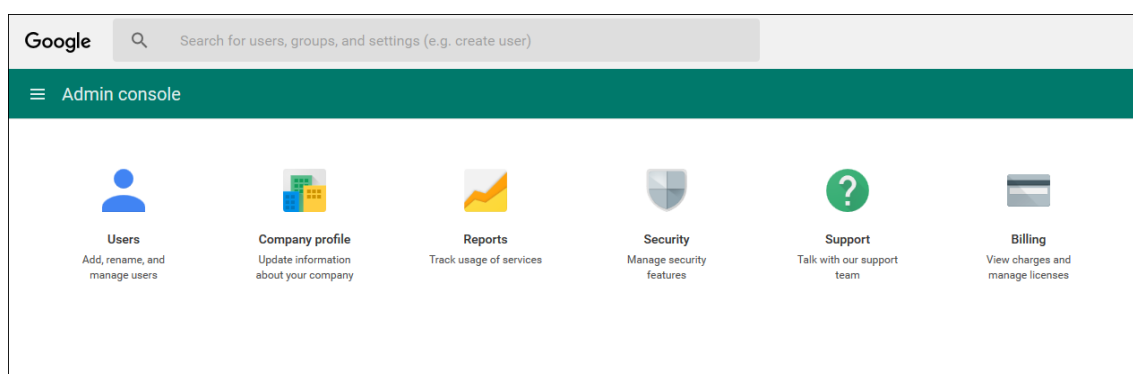
- **Domain name:** Type your Android Enterprise domain name; for example, domain.com.
- **Domain Admin Account:** Type your domain administrator user name; for example, the email account used for Google Developer Portal.
- **Service Account ID:** Type your service account ID; for example, the email associated in the Google Service Account ([serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com](#)).
- **Client ID:** Type the numerical client ID of your Google service account.
- **Enable Android Enterprise:** Select to enable or disable Android Enterprise.

## Enable SAML-based single-sign-on

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **Certificates**. The **Certificates** page appears.



3. In the list of certificates, click the SAML certificate.
4. Click **Export** and save the certificate to your computer.
5. Sign in to the Google Admin portal by using your Android Enterprise administrator credentials. For access to the portal, see [Google Admin portal](#).
6. Click **Security**.



7. Under **Security**, click **Set up single sign-on (SSO)** and then configure the following settings.



### ^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console. ?

Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL   
URL for signing in to your system and Google Apps

Sign-out page URL   
URL for redirecting users to when they sign out

Change password URL   
URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

Verification certificate    
The certificate file must contain the public key for Google to verify sign-in requests. ?

Use a domain specific issuer ?

Network masks   
Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

[DISCARD CHANGES](#) [SAVE CHANGES](#)

- **Sign-in page URL:** Type the URL for users signing in to your system and Google Apps. For example: <https://<Xenmobile-FQDN>/aw/saml/signin>.
- **Sign out page URL:** Type the URL to which users are redirected when they sign out. For example: <https://<Xenmobile-FQDN>/aw/saml/signout>.
- **Change password URL:** Type the URL to let users change their password in your system. For example: <https://<Xenmobile-FQDN>/aw/saml/changepassword>. If this field is defined, users see this prompt even when SSO is not available.
- **Verification certificate:** Click **CHOOSE FILE** and then navigate to the SAML certificate exported from Endpoint Management.

8. Click **SAVE CHANGES**.

## Set up an Android Enterprise device policy

Set up a Passcode policy so that users must establish a passcode on their devices when they first enroll.

The basic steps to setting up any device policy are as follows.

1. In the Endpoint Management console, click **Configure**, and then click **Device Policies**.
2. Click **Add** and then on the **Add a New Policy** dialog box, select the policy you want to add. In this example, you click **Passcode**.
3. Complete the **Policy Information** page.
4. Click **Android Enterprise** and then configure the settings for the policy.
5. Assign the policy to a Delivery Group.

### Configure Android Enterprise account settings

Before you can start managing Android apps and policies on devices, you must set up an Android Enterprise domain and account information in Endpoint Management. First, complete Android Enterprise setup tasks on Google to set up a domain administrator and to obtain a service account ID and a binding token.

1. In the Endpoint Management web console, click the gear icon in the upper-right corner. The **Settings** page displays.

2. Under **Platforms**, click **Android Enterprise**. The **Android Enterprise** configuration page appears.

Settings > Android Enterprise

### Legacy Android Enterprise ▾

Provide Android Enterprise configuration parameters.

Domain Name *	<input type="text"/>	?
Domain Admin Account *	<input type="text"/>	?
Service Account ID *	<input type="text"/>	?
Client ID *	<input type="text"/>	?

Enable Android Enterprise  NO

Cancel Save

1. On the **Android Enterprise** page, configure the following settings:
  - **Domain Name:** Type your domain name.
  - **Domain Admin Account:** Type your domain administrator user name.
  - **Service Account ID:** Type your Google Service Account ID.
  - **Client ID:** Type the client ID of your Google service account.
  - **Enable Android Enterprise:** Select whether to enable Android Enterprise or not.
2. Click **Save**.

## Set up Google Workspace partner access for Endpoint Management

Some Endpoint Management features for Chrome use Google partner APIs to communicate between Endpoint Management and your Google Workspace domain. For example, Endpoint Management requires the APIs for device policies that manage Chrome features such as Incognito mode and Guest mode.

To enable the partner APIs, you set up your Google Workspace domain in the Endpoint Management console and then configure your Google Workspace account.

## Set up your Google Workspace domain in Endpoint Management

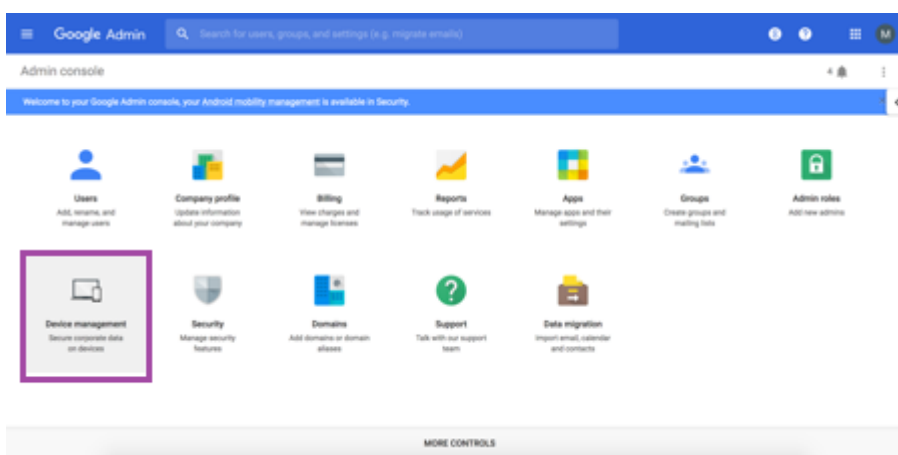
To enable Endpoint Management to communicate with the APIs in your Google Workspace domain, go to **Settings > Google Chrome Configuration** and configure the settings.

- **Google Workspace domain:** The Google Workspace domain that hosts the APIs needed by Endpoint Management.
- **Google Workspace admin account:** The administrator account for your Google Workspace domain.

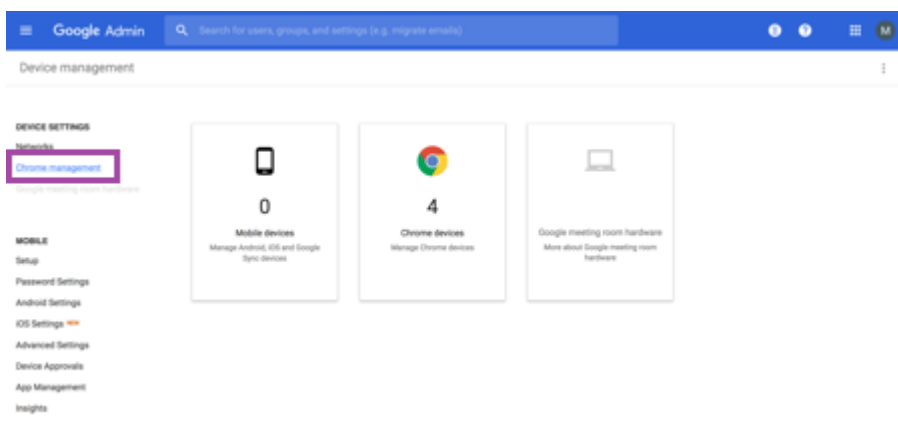
- **Google Workspace client ID:** The client ID for Citrix. Use this value to configure partner access for your Google Workspace domain.
- **Google Workspace enterprise ID:** The enterprise ID for your account, filled in from your Google enterprise account.

### Enable partner access for devices and users in your Google Workspace domain

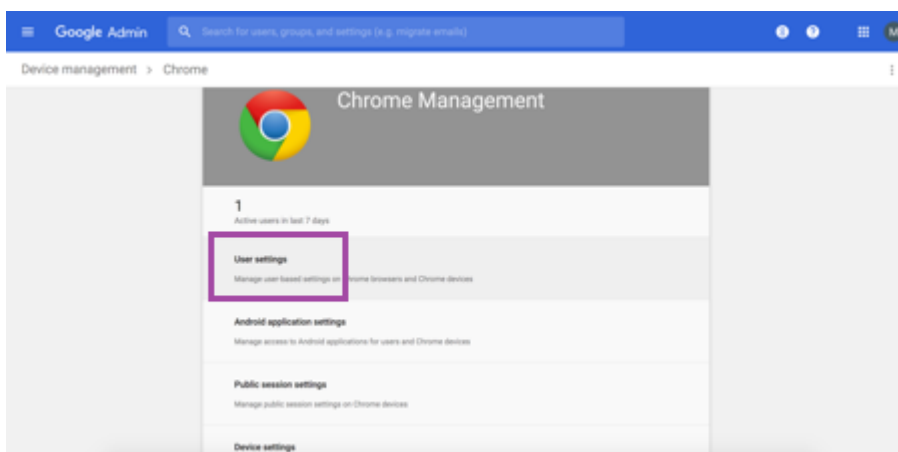
1. Log in into the Google admin console: <https://admin.google.com>
2. Click **Device Management**.



3. Click **Chrome management**.



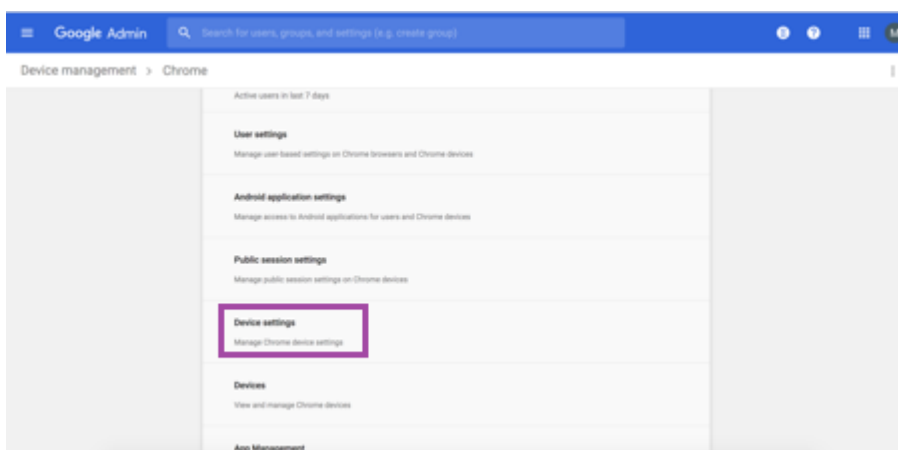
4. Click **User settings**.



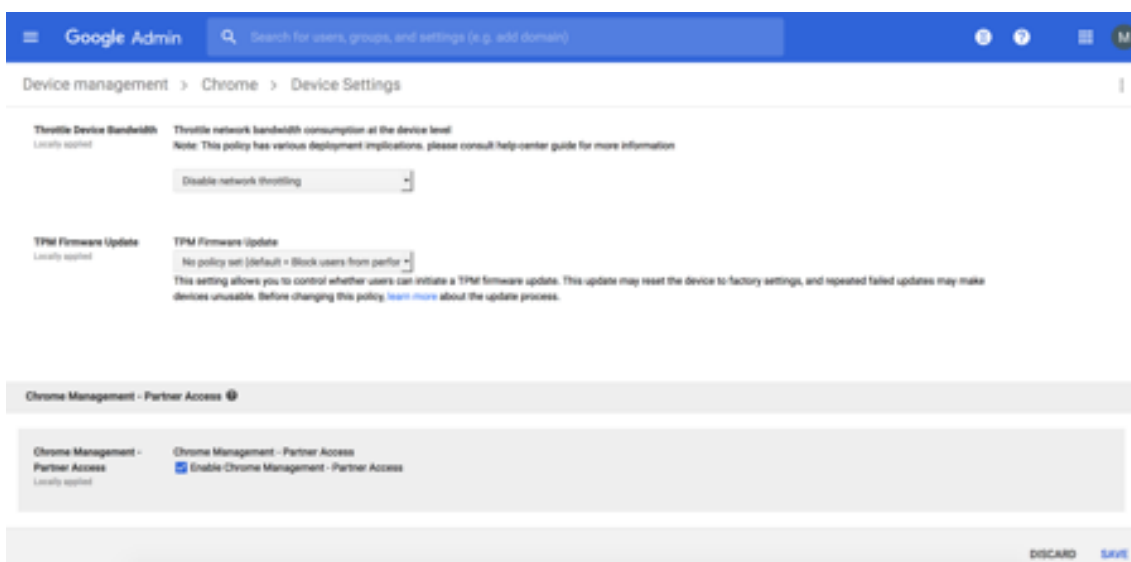
5. Search for **Chrome Management - Partner Access**.



- 6. Select the **Enable Chrome Management - Partner Access** check box.
- 7. Agree that you understand and want to enable partner access. Click **Save**.
- 8. In the Chrome management page, click **Device Settings**.



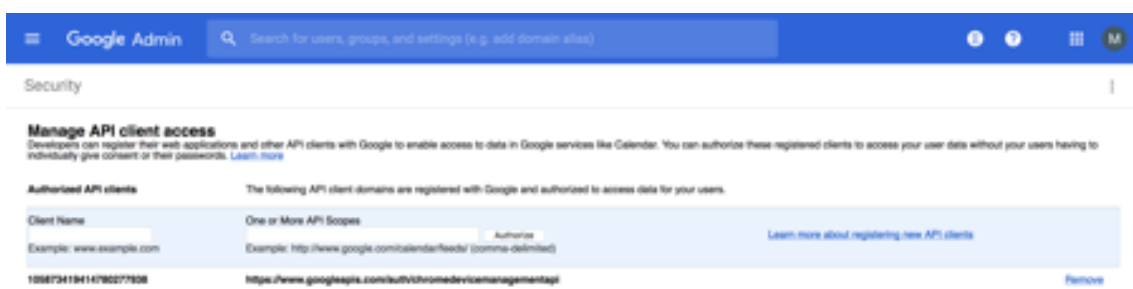
9. Search for **Chrome Management - Partner Access**.



10. Select the **Enable Chrome Management - Partner Access** check box.
11. Agree that you understand and want to enable partner access. Click **Save**.
12. Go to the **Security** page and then click **Advanced Settings**.



13. Click **Manage API client Access**.
14. In the Endpoint Management console, go to **Settings > Google Chrome Configuration** and copy the value of G Suite Client ID. Then, return to the **Manage API client Access** page and paste the copied value to the **Client Name** field.
15. In **One or More API Scopes**, add the URL: <https://www.googleapis.com/auth/chromedevicemanagementapi>



16. Click **Authorize**.  
The message “Your settings have been saved” appears.

## Enrolling Android Enterprise devices

If your device enrollment process requires users to enter a user name or user ID, the format accepted depends on how the Endpoint Management server is configured to search for users by User Principal Name (UPN) or SAM account name.

If the Endpoint Management server is configured to search for users by UPN, users must enter a UPN in the format:

- *username@domain*

If the Endpoint Management server is configured to search for users by SAM users must enter a SAM in one of these formats:

- *username@domain*
- *domain\username*

To determine which type of user name your Endpoint Management server is configured for:

1. In the Endpoint Management server console click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **LDAP** to view the configuration of the LDAP connection.
3. Near the bottom of the page, view the **User search by** field:
  - If it is set to **userPrincipalName**, Endpoint Management server is set for UPN.
  - If it is set to **sAMAccountName**, Endpoint Management server is set for SAM.

## Unenrolling an Android Enterprise enterprise

You can unenroll an Android Enterprise enterprise using the Endpoint Management server console and Endpoint Management Tools.

When you perform this task, the Endpoint Management server opens a popup window for Endpoint Management Tools. Before you begin, ensure that the Endpoint Management server has permission to open popup windows in the browser you are using. Some browsers, such as Google Chrome, require you to disable popup blocking and add the address of the Endpoint Management site to the popup allow list.

### Warning:

After an enterprise is unenrolled, Android Enterprise apps on devices already enrolled through it are reset to their default states. The devices will no longer be managed by Google. Re-enrolling them in an Android Enterprise enterprise may not restore previous functionality without further configuration.

After the Android Enterprise enterprise is unenrolled:

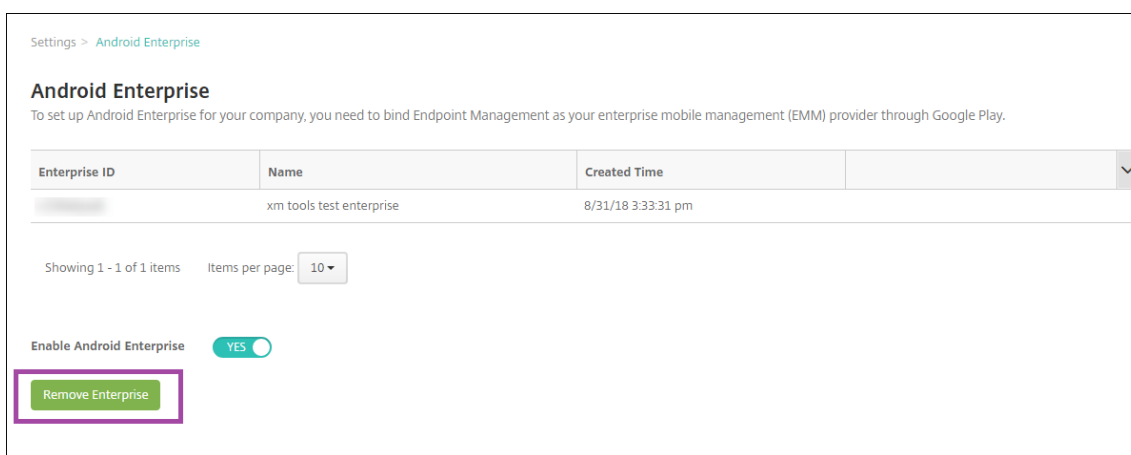
- Devices and users enrolled through the enterprise have the Android Enterprise apps reset to their default state. App permissions and Managed configurations policies previously applied no longer have an effect.
- Devices enrolled through the enterprise are managed by Endpoint Management, but are unmanaged from Google perspective. No new Android Enterprise apps can be added. No App permissions or Managed configurations policies can be applied. Other policies, such as Scheduling, Password, and Restrictions can still be applied to these devices.



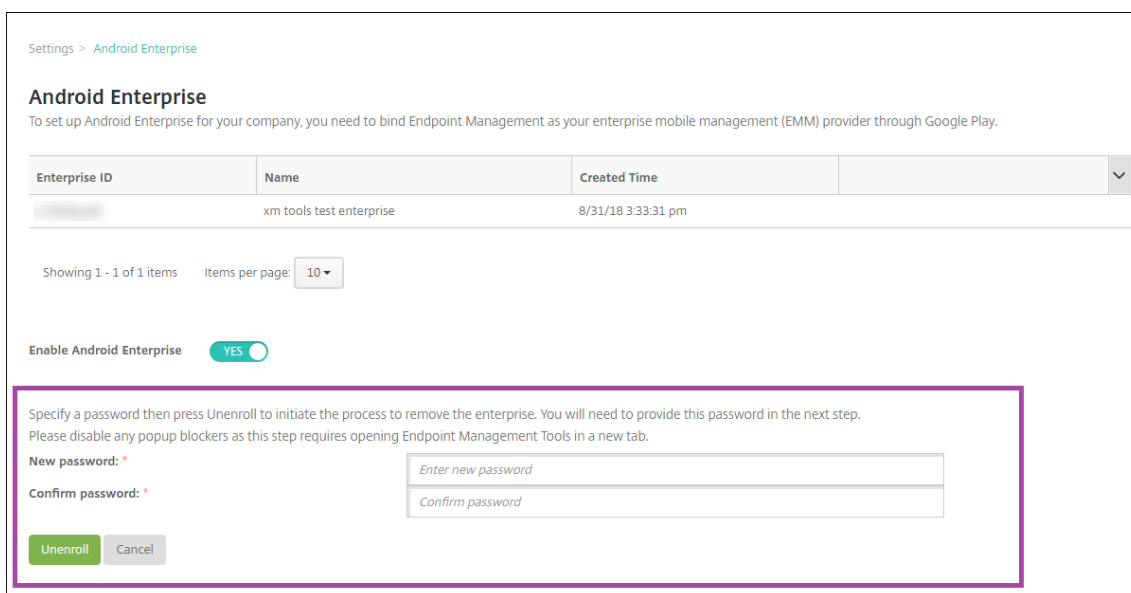
- If you attempt to enroll devices in Android Enterprise, they are enrolled as Android devices, not Android Enterprise devices.

To unenroll an Android Enterprise enterprise:

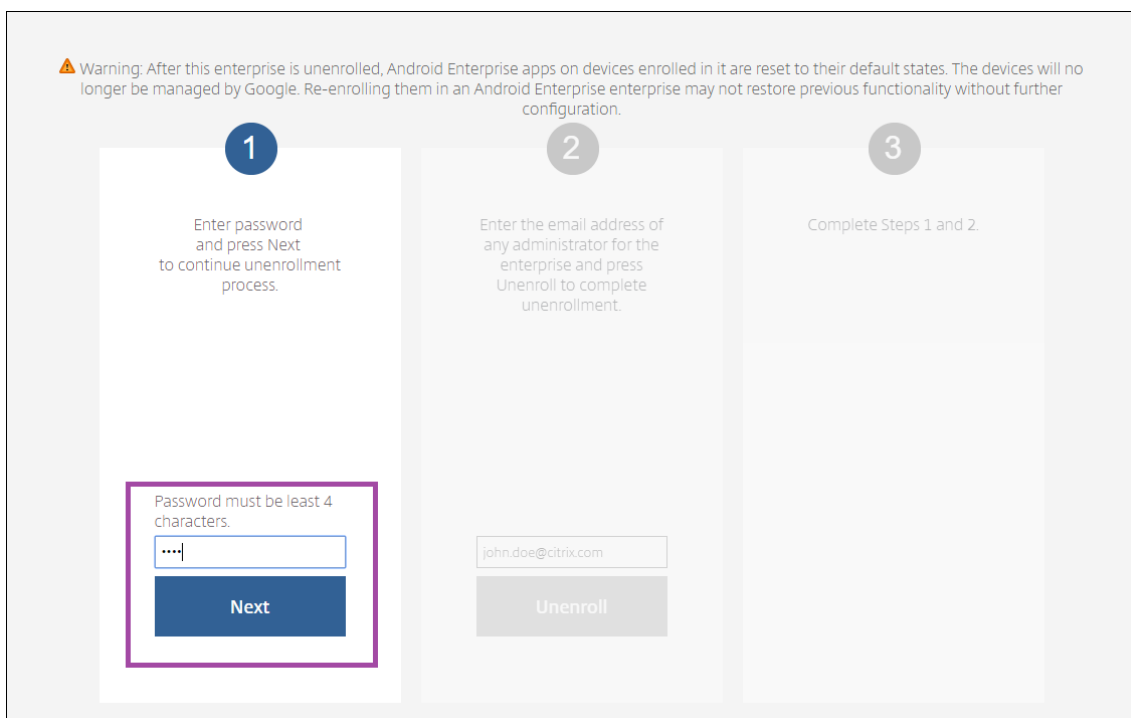
1. In the Endpoint Management console, click the gear icon in the upper-right corner. The Settings page appears.
2. On the Settings page, click **Android Enterprise**.
3. Click **Remove Enterprise**.



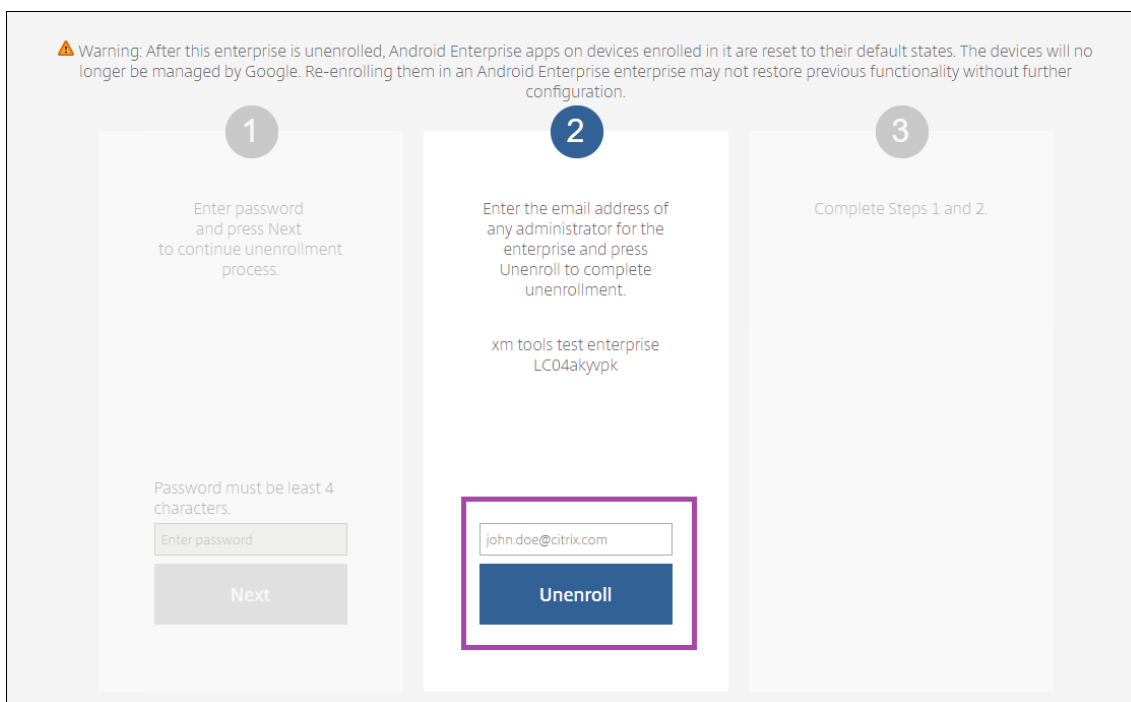
4. Specify a password. You'll need this for the next step to complete the unenrollment. Then click **Unenroll**.



5. When the Endpoint Management Tools page opens, enter the password you created in the previous step.



6. Click **Unenroll**.



**Provisioning fully managed devices in Android Enterprise**

Only company-owned devices can be fully managed devices in Android Enterprise. On fully managed devices the entire device, not just the work profile, is controlled by the company or organization. Fully

managed devices are also known as work-managed devices.

Endpoint Management supports these methods of enrollment for fully managed devices:

- **afw#xenmobile:** With this enrollment method, the user enters the characters `afw##xenmobile` when setting up the device. This token identifies the device as managed by Endpoint Management and downloads Secure Hub.
- **QR code:** QR code provisioning is an easy way to provision a distributed fleet of devices that do not support NFC, such as tablets. The QR code enrollment method can be used on fleet devices that have been reset to their factory settings. The QR code enrollment method sets up and configures fully managed devices by scanning a QR code from the setup wizard.
- **Near field communication (NFC) bump:** The NFC bump enrollment method can be used on fleet devices that have been reset to their factory settings. An NFC bump transfers data through between two devices using near-field communication. Bluetooth, Wi-Fi, and other communication modes are disabled on a factory-reset device. NFC is the only communication protocol that the device can use in this state.

### **afw#xenmobile**

The enrollment method is used after powering on a new or factory reset devices for initial setup. Users enter `afw##xenmobile` when prompted to enter a Google account. This action downloads and installs Secure Hub. Users then follow the Secure Hub set-up prompts to complete the enrollment.

This enrollment method is recommended for most customers because the latest version of Secure Hub is downloaded from the Google Play store. Unlike with other enrollment methods, you do not provide Secure Hub for download from the Endpoint Management server.

Prerequisites:

- Supported on all Android devices running Android OS.

### **QR code**

To enroll a device in device mode using a QR code, you generate a QR code by creating a JSON and converting the JSON to a QR code. Device cameras scan the QR code to enroll the device.

Prerequisites:

- Supported on all Android devices running Android 7.0 and above.

### **Create a QR code from a JSON**

Create a JSON with the following fields.

These fields are required:

Key: android.app.extra.PROVISIONING\_DEVICE\_ADMIN\_COMPONENT\_NAME

Value: com.zenprise/com.zenprise.configuration.AdminFunction

Key: android.app.extra.PROVISIONING\_DEVICE\_ADMIN\_SIGNATURE\_CHECKSUM

Value: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Key: android.app.extra.PROVISIONING\_DEVICE\_ADMIN\_PACKAGE\_DOWNLOAD\_LOCATION

Value: <https://play.google.com/managed/downloadManagingApp?identifier=xenmobile>

These fields are optional:

- **android.app.extra.PROVISIONING\_LOCALE:** Enter language and country codes.  
The language codes are two-letter lowercase ISO language codes (such as en) as defined by [ISO 639-1](#). The country codes are two-letter uppercase ISO country codes (such as US) as defined by [ISO 3166-1](#). For example, enter en\_US for English as spoken in the United States.
- **android.app.extra.PROVISIONING\_TIME\_ZONE:** The time zone in which the device is running.  
Type the [database name of the area/location](#). For example, type **America/Los\_Angeles** for Pacific time. If you don't type a name, the time zone automatically populates.
- **android.app.extra.PROVISIONING\_LOCAL\_TIME:** Time in milliseconds since the Epoch.  
The Unix epoch (or Unix time, POSIX time, or Unix timestamp) is the number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT). The time doesn't include leap seconds (in ISO 8601: 1970-01-01T00:00:00Z).
- **android.app.extra.PROVISIONING\_SKIP\_ENCRYPTION:** Set to **true** to skip encryption during profile creation. Set to **false** to force encryption during profile creation.

A typical JSON looks like the following:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

Validate the JSON that is created using any JSON validation tool, such as <https://jsonlint.com>. Convert that JSON string to a QR code using any online QR code generator.

This QR code gets scanned by a factory-reset device to enroll the device as fully managed devices.

### To enroll the device

To enroll a device as a fully managed device, the device must be in factory reset state.

1. Tap the screen six times on the welcome screen to launch the QR code enrollment flow.
2. When prompted, connect to Wi-Fi. The download location for Secure Hub in the QR code (encoded in the JSON) is accessible over this Wi-Fi network.

Once the device successfully connects to Wi-Fi, it downloads a QR code reader from Google and launches the camera.

3. Point the camera to the QR code to scan the code.

Android downloads Secure Hub from the download location in the QR code, validate the signing certificate signature, install Secure Hub and sets it as device owner.

For more information about provisioning devices using the QR code method, see the [Google API documentation for Android EMM developers](#).

### **NFC bump**

To enroll a device as a fully managed device using NFC bumps requires two devices: One that is reset to its factory settings and one running the Endpoint Management Provisioning Tool.

Prerequisites:

- Supported Android devices
- Endpoint Management enabled for Android Enterprise
- A new or factory-reset device, provisioned for Android Enterprise as a fully managed device. You can find steps to complete this prerequisite later in this article.
- Another device with NFC capability, running the configured Provisioning Tool. The Provisioning Tool is available in Secure Hub or on the [Citrix downloads page](#).

Each device can have only one Android Enterprise profile, managed by an enterprise mobility management (EMM) app. In Endpoint Management, Secure Hub is the EMM app. Only one profile is allowed on each device. Attempting to add a second EMM app removes the first EMM app.

### **Data transferred through the NFC bump**

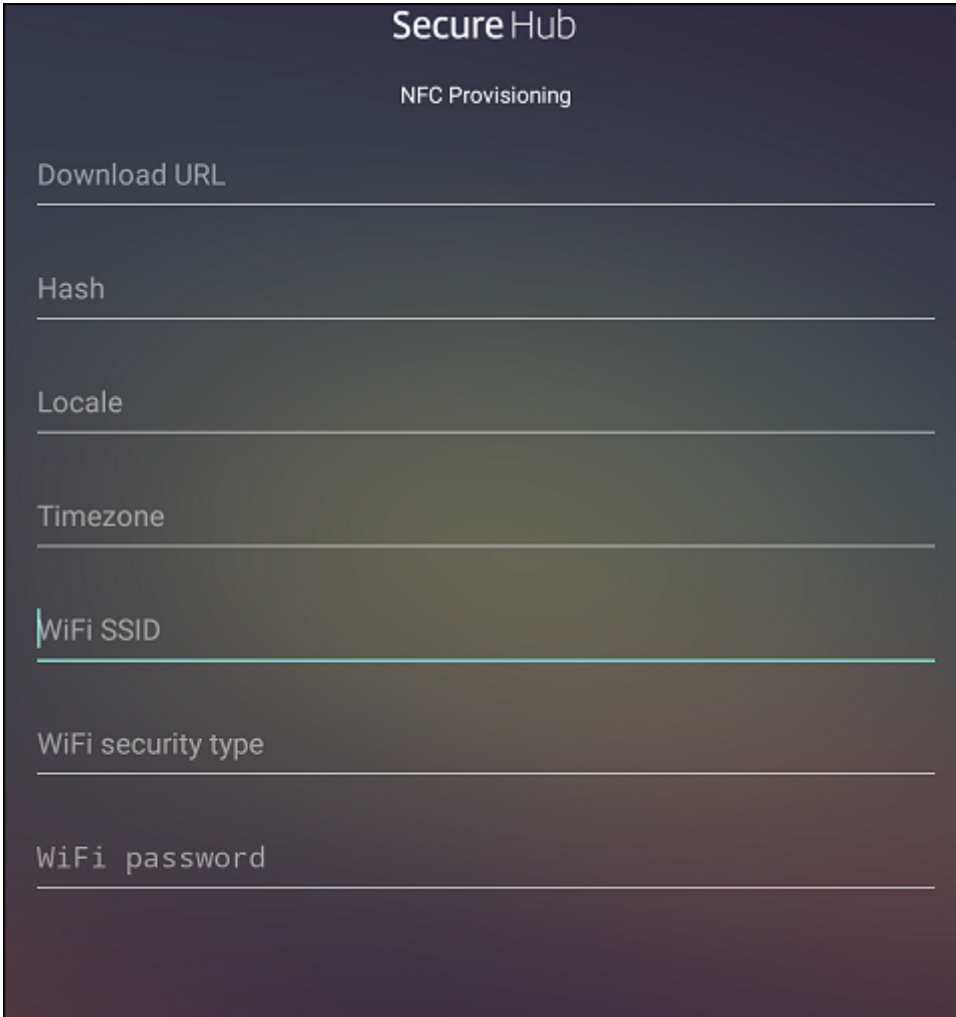
Provisioning a factory-reset device requires you to send the following data through an NFC bump to initialize Android Enterprise:

- Package name of the EMM provider app that acts as device owner (in this case, Secure Hub).
- Intranet/Internet location from which the device can download the EMM provider app.
- SHA-256 hash of EMM provider app to verify if the download is successful.
- Wi-Fi connection details so that a factory-reset device can connect and download the EMM provider app. Note: Android now does not support 802.1x Wi-Fi for this step.
- Time zone for the device (optional).
- Geographic location for the device (optional).

When the two devices are bumped, the data from the Provisioning Tool is sent to the factory-reset device. That data is then used to download Secure Hub with administrator settings. If you don't enter time zone and location values, Android automatically configures the values on the new device.

### **Configuring the Endpoint Management Provisioning Tool**

Before doing an NFC bump, you must configure the Provisioning Tool. This configuration is then transferred to the factory-reset device during the NFC bump.



The image shows a screenshot of the 'SecureHub' application interface for 'NFC Provisioning'. The screen has a dark background with white text. At the top, it says 'SecureHub' and 'NFC Provisioning'. Below this, there are seven input fields, each with a label and a horizontal line for text entry. The labels are: 'Download URL', 'Hash', 'Locale', 'Timezone', 'WiFi SSID', 'WiFi security type', and 'WiFi password'. The 'WiFi SSID' field has a small blue vertical bar on its left side.

You can type data into the required fields or populate them via text file. The steps in the next procedure describe how to configure the text file and contain descriptions for each field. The app doesn't save information after you type it, so you might want to create a text file to keep the information for future use.

### **To configure the Provisioning Tool by using a text file**

Name the file `nfcprovisioning.txt` and place the file in the `/sdcard/` folder on the SD card of the device. The app can then read the text file and populate the values.

The text file must contain the following data:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>
```

This line is the intranet/internet location of the EMM provider app. After the factory-reset device connects to Wi-Fi following the NFC bump, the device must have access to this location for downloading. The URL is a regular URL, with no special formatting required.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>
```

This line is the checksum of the EMM provider app. This checksum is used to verify that the download is successful. Steps to obtain the checksum are discussed later in this article.

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

This line is the connected Wi-Fi SSID of the device on which the Provisioning Tool is running.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

Supported values are WEP and WPA2. If the Wi-Fi is unprotected, this field must be empty.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

If the Wi-Fi is unprotected, this field must be empty.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

Enter language and country codes. The language codes are two-letter lowercase ISO language codes (such as `en`) as defined by [ISO 639-1](#). The country codes are two-letter uppercase ISO country codes (such as `US`) as defined by [ISO 3166-1](#). For example, type `en_US` for English as spoken in the United States. If you don't type any codes, the country and language are automatically populated.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

The time zone in which the device is running. Type the [database name of the area/location](#). For example, type **America/Los\_Angeles** for Pacific time. If you don't type a name, the time zone automatically populates.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

This data isn't required, because the value is hardcoded into the app as Secure Hub. It's mentioned here only for the sake of completion.

If there is a Wi-Fi protected by using WPA2, a completed `nfcprovisioning.txt` file might look like the following:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicur\here.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crh  
\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
```

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
```

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

If there is an unprotected Wi-Fi, a completed nfcprovisioning.txt file might look like the following:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https  
://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crh  
\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

### To get the checksum of Citrix Secure Hub

The checksum of Secure Hub is a constant value: qn7oZUtheu3JBAinzZRrrjCQv6L006Ll10jcxT3-yKM. To download an APK file for Secure Hub, use the following Google Play store link: <https://play.google.com/managed/downloadManagingApp?identifier=xenmobile>.

### To get an app checksum

Prerequisites:

- The **apksigner** tool from the Android SDK Build Tools
- OpenSSL command line

To get the checksum of any app, follow these steps:

1. Download the app's APK file from the Google Play store.
2. In the OpenSSL command line, navigate to the **apksigner** tool: `android-sdk/build-tools/<version>/apksigner` and type the following:

```
1 apksigner verify -print-certs <apk_path> | perl -nle 'print $& if  
   m{  
2   (?<=SHA-256 digest:) .* }  
3   ' | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
```



```
4 <!--NeedCopy-->
```

The command returns a valid checksum.

3. To generate the QR code, enter the checksum in the `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM` field. For example:

```
1 {
2
3   "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.
4     zenprise/com.zenprise.configuration.AdminFunction",
5   "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "
6     qn7oZUtheu3JBAinzZRrjCQv6L006Ll10jcxT3-yKM",
7   "android.app.extra.
8     PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
9     play.google.com/managed/downloadManagingApp?identifier=xenmobile",
10  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
11    "serverURL": "https://supportability.xm.cloud.com"
12  }
13 }
14 <!--NeedCopy-->
```

### Libraries used

The Provisioning Tool uses the following libraries in its source code:

- v7 `appcompat` library, Design Support library, and v7 palette support library

For information, look for the Support Library Features Guide in the [Android developers documentation](#).

- [Butter Knife](#) by Jake Wharton under Apache license 2.0

### Provision work profile devices in Android Enterprise

On work profile devices in Android Enterprises, you securely separate the corporate and personal areas on a device. For example, BYOD devices can be work profile devices. The enrollment experience for work profile devices is similar to Android enrollment in Endpoint Management. Users download Secure Hub from Google Play and enroll their devices.

By default, the USB Debugging and Unknown Sources settings are disabled on a device when it is enrolled in Android Enterprise as a work profile device.

**Tip:**

When enrolling devices in Android Enterprise as work profile devices, always go to Google Play. From there, enable Secure Hub to appear in the user's personal profile.

## Android OS

October 13, 2021

**Note:**

This article doesn't apply to devices that are managed with Android Enterprise, Samsung Knox, or Samsung SAFE. For information about those devices, see other articles in this section.

Endpoint Management also supports Android OS devices that aren't managed through an Android or Samsung enterprise program. To control how and when Android devices connect to the Endpoint Management service, use Firebase Cloud Messaging (FCM). For information, see [Firebase Cloud Messaging](#).

Enrollment profiles determine whether Android devices enroll in MAM, MDM, or MDM+MAM, with the option for users to opt out of MDM. Endpoint Management supports the following authentication types for Android devices in MDM+MAM. For information, see the following articles:

- [Domain or domain plus security token authentication](#)
- [Client certificate or certificate plus domain authentication](#)
- Identity providers:
  - [Authentication with Azure Active Directory through Citrix Cloud](#)
  - [Authentication with Okta through Citrix Cloud](#)

Another rarely used authentication method is client certificate plus security token. For information, see <https://support.citrix.com/article/CTX215200>.

A general workflow for starting Android device management is as follows:

1. Complete the onboarding process. See [Onboarding and resource setup](#) and [Prepare to enroll devices and deliver resources](#).
2. Choose and configure an enrollment method. See [Supported enrollment methods](#).
3. Configure Android device policies.
4. Enroll Android devices.
5. Set up device and app security actions. See [Security actions](#).

For supported operating systems, see [Supported device operating systems](#).

### Supported enrollment methods

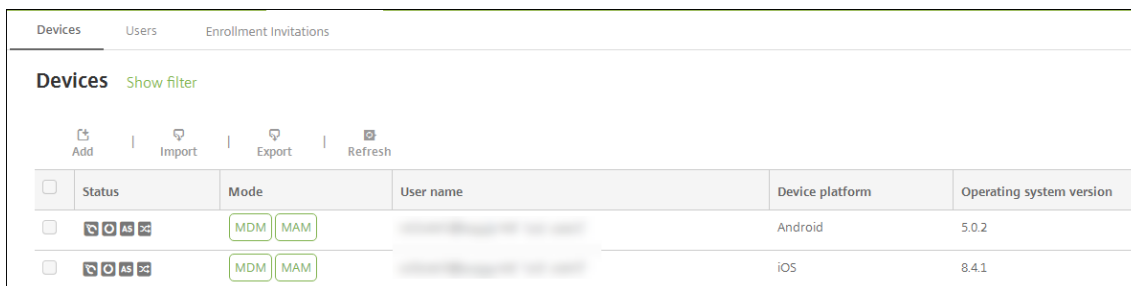
The following table lists the enrollment methods that Endpoint Management supports for Android devices:

Method	Supported
Bulk enrollment	No
Manual enrollment	Yes
Enrollment invitations	Yes

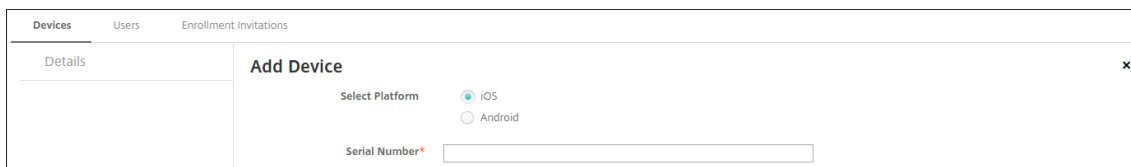
### Add an Android device manually

If you want to add an Android or iOS device manually, such as for testing purposes, follow these steps.

1. In the Endpoint Management console, click **Manage > Devices**. The **Devices** page appears.



2. Click **Add**. The **Add Device** page appears.



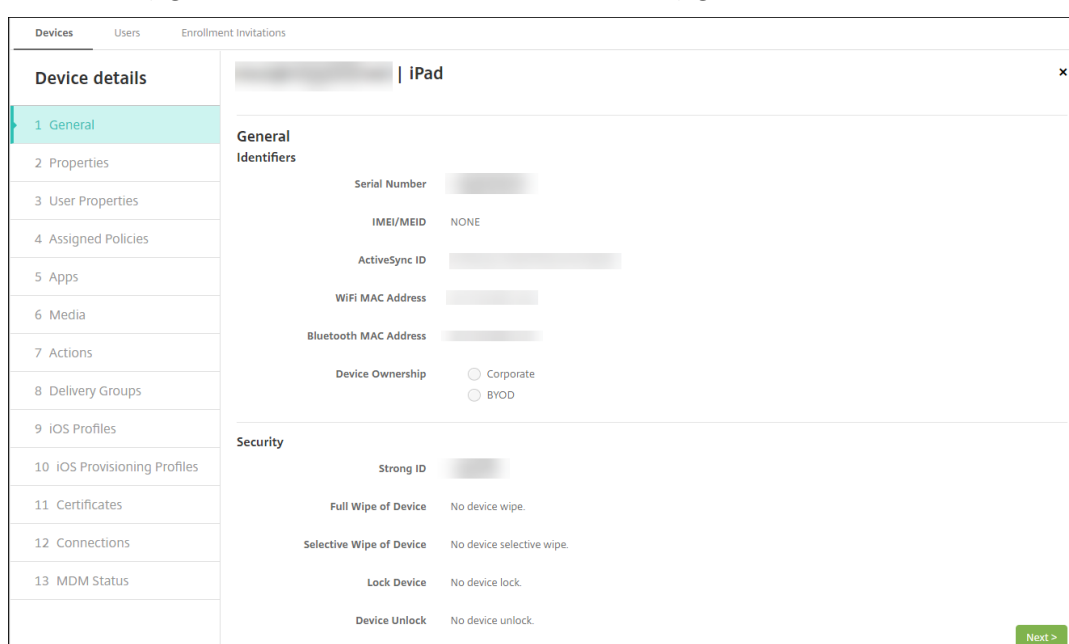
3. Configure these settings:
  - **Select platform:** Click **Android**.
  - **Serial Number:** Type the device serial number.
  - **IMEI/MEID:** Optionally, type the device IMEI/MEID information.
4. Click **Add**. The **Devices** table appears with the device added to the bottom of the list. To view and confirm the device details: Choose the device you added and then, in the menu that appears, click **Edit**.

**Note:**

When you select the check box next to a device, the options menu appears above the device

list. When you click anywhere else in the list, the options menu appears on the right side of the listing.

- LDAP configured
- If using local groups and local users:
  - One or more local groups.
  - Local users assigned to local groups.
  - Delivery groups are associated with local groups.
- If using Active Directory:
  - Delivery groups are associated with Active Directory groups.



5. The **General** page lists device **Identifiers**, such as the serial number and other information for the platform type. For **Device Ownership**, select **Corporate** or **BYOD**.

The **General** page also lists device **Security** properties, such as Strong ID, Lock Device, Activation Lock Bypass, and other information for the platform type. The **Full Wipe of Device** field includes the user PIN code. The user must enter that code after the device is wiped. If the user forgets the code, you can look it up here.

6. The **Properties** page lists the device properties that Endpoint Management is to provision. This list shows any device properties included in the provisioning file used to add the device. To add a property, click **Add** and then select a property from the list. For valid values for each property, see the PDF [Device property names and values](#).

When you add a property, it initially appears under the category where you added it. After you click **Next** and then return to the **Properties** page, the property appears in the appropriate list.

To delete a property, hover over the listing and then click the **X** on the right side. Endpoint Management deletes the item immediately.

7. The remaining **Device Details** sections contain summary information for the device.

- **User Properties:** Displays RBAC roles, group memberships, managed Google Play accounts, and properties for the user. You can retire a managed Google Play account from this page.
- **Assigned Policies:** Displays the number of deployed, pending, and failed policies. Provides the policy name, type, and last deployed information for each policy. Lets you reset the deployment status to pending and redeploy policies that the user removed.
- **Apps:** Displays, for the last inventory, the number of installed, pending, and failed app deployments. Provides the app name, identifier, type, and other information. For a description of iOS and macOS inventory keys, such as **HasUpdateAvailable**, see [Mobile Device Management \(MDM\) Protocol](#).
- **Media:** Displays, for the last inventory, the number of deployed, pending, and failed media deployments.
- **Actions:** Displays the number of deployed, pending, and failed actions. Provides the action name and time of the last deployment.
- **Delivery Groups:** Displays the number of successful, pending, and failed delivery groups. For each deployment, provides the delivery group name and deployment time. Select a delivery group to view more detailed information, including status, action, and channel or user.
- **iOS Profiles:** Displays the last iOS profile inventory, including name, type, organization, and description.
- **iOS Provisioning Profiles:** Displays enterprise distribution provisioning profile information, such as the UUID, expiration date, and managed status.
- **Certificates:** Displays, for valid, expired, or revoked certificates, information such as the type, provider, issuer, serial number, and the number of remaining days before expiration.
- **Connections:** Displays the first connection status and the last connection status. Provides for each connection, the user name, penultimate (next to last) authentication time, and last authentication time.
- **MDM Status:** Displays information such as the MDM status, last push time, and last device reply time.

## Configure Android device policies

Use these policies to configure how Endpoint Management interacts with devices running Android. This table lists all device policies available for Android devices.

---

---

APN	App access	App inventory
App lock	App uninstall	Credentials
Endpoint Management options	Endpoint Management uninstall	Exchange
Files	Launcher configuration	Location
Network	Passcode	Restrictions
Scheduling	Store	Terms and Conditions
Tunnel	VPN	Web clip

---

## Enroll Android devices

1. Go to the Google Play store on your Android device, download the Citrix Secure Hub app, and then tap the app.
2. When prompted to install the app, click **Next** and then click **Install**.
3. After Secure Hub installs, tap **Open**.
4. For devices running Android 6.0 and greater, accept the required permissions:
  - Allow Secure Hub to make and manage phone calls? (required)
  - Allow Secure Hub to access photos, media, and files on your device? (required)
  - Allow Secure Hub to access this device's location? (optional)
5. Enter your corporate credentials, such as your Endpoint Management server name, User Principal Name (UPN), or email address. Then, click **Next**.
6. Choose how to enroll your device:
  - To enroll in MDM+MAM, tap **Yes, enroll**.
  - To enroll in MAM, tap **No**.
7. In the **Activate device administrator** screen, tap **Activate**.
8. Enter your corporate password and then tap **Sign On**.
9. Depending on the way Endpoint Management is configured, you might be asked to create a Citrix PIN. You can use the PIN to sign on to Secure Hub and other Endpoint Management-enabled apps, such as Secure Mail and Citrix Files. You enter your Citrix PIN twice. On the **Create Citrix PIN** screen, enter a PIN.
10. Reenter the PIN. Secure Hub opens. You can then access the app store to view the apps you can install on your Android device.

11. If you configured Endpoint Management to push apps to devices automatically after enrollment, users are prompted to install the apps. In addition, policies that you configure in Endpoint Management are deployed to the device. Tap **Install** to install the apps.

### To unenroll and reenroll an Android device

Users can unenroll from within Secure Hub. When users unenroll by using the following procedure, the device still appears in the device inventory in the Endpoint Management console. You cannot perform actions on the device, however. For example, you cannot track the device or monitor device compliance.

1. Tap to open the Secure Hub app.
2. Depending on whether you have a phone or a tablet, do the following:

On a phone:

- Swipe from the left of the screen to open a settings pane.
- Tap **Preferences**, tap **Accounts**, and then tap **Delete Account**.

On a tablet:

- Tap the arrow next to your email address on the upper-right corner.
- Tap **Preferences**, tap **Accounts**, and then tap **Delete Account**.

3. In the **Delete Account?** window, tap **Yes, delete**.

Secure Hub unenrolls your device. Follow the on-screen instructions to re-enroll your device.

### Security actions

Android supports the following security actions. For a description of each security action, see [Security actions](#).

---

App Lock	App Wipe	Certificate Renewal
Full Wipe	Locate	Lock
Lock and Reset Password	Notify	Revoke
Selective Wipe		

---

**Note:**

For devices running Android 6.0 and greater, the Locate security action requires the user to grant Location permission during enrollment. The user can opt not to grant Location permission. If the user doesn't grant the permission during enrollment, Endpoint Management again requests location permission when sending the Locate command.

## Firebase Cloud Messaging

April 16, 2021

**Note:**

Firebase Cloud Messaging (FCM) was previously known as Google Cloud Messaging (GCM). Some Endpoint Management console labels and messages use the GCM terminology.

Citrix recommends that you use Firebase Cloud Messaging (FCM) to control how and when Android devices connect to Endpoint Management. Endpoint Management, when configured for FCM, sends connection notifications to Android devices that are enabled for FCM. Any security action or deploy command triggers a push notification to prompt the user to reconnect to the Endpoint Management server.

After you complete the configuration steps in this article and a device checks in, the device registers with the FCM service in Citrix Endpoint Management. That connection enables near real-time communication from your Endpoint Management service to your device by using FCM. FCM registration works for new device enrollments and previously enrolled devices.

When Endpoint Management needs to initiate a connection to the device, it connects to the FCM service. Then, the FCM service notifies the device to connect. This type of connection is similar to what Apple uses for its Push Notification Service.

### Prerequisites

- Latest Secure Hub client
- Google developer account credentials
- Google Play services installed on FCM-enabled Android devices

### Firewall ports

- Open port 443 on Endpoint Management to [fcm.googleapis.com](https://fcm.googleapis.com) and [Google.com](https://google.com).
- Open outgoing, Internet communication for device Wi-Fi on ports 5228, 5229, and 5230.

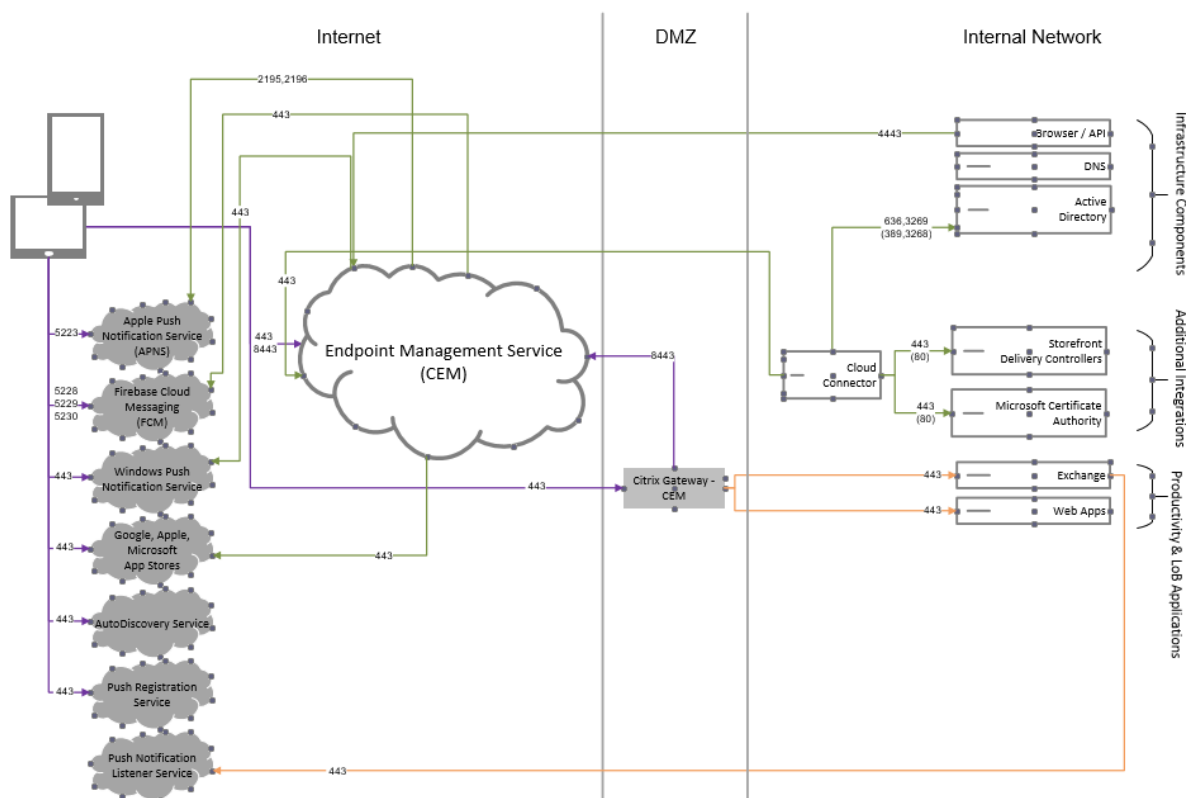


- To allow outgoing connections, FCM recommends adding ports 5228 through 5230 to an allow list, with no IP restrictions. However, if you require IP restrictions, FCM recommends adding all the IP addresses in the IPv4 and IPv6 blocks to an allow list. Those blocks are listed in the Google [ASN of 15169](#). Update that list monthly.

For more information, see [Port requirements](#).

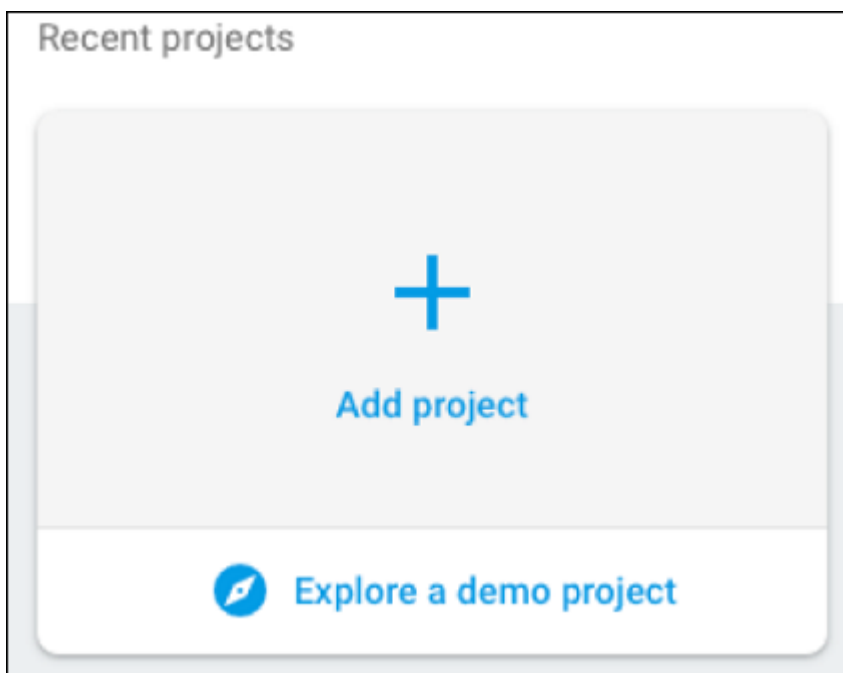
## Architecture

This diagram shows the communication flow for FCM in the external and internal network.

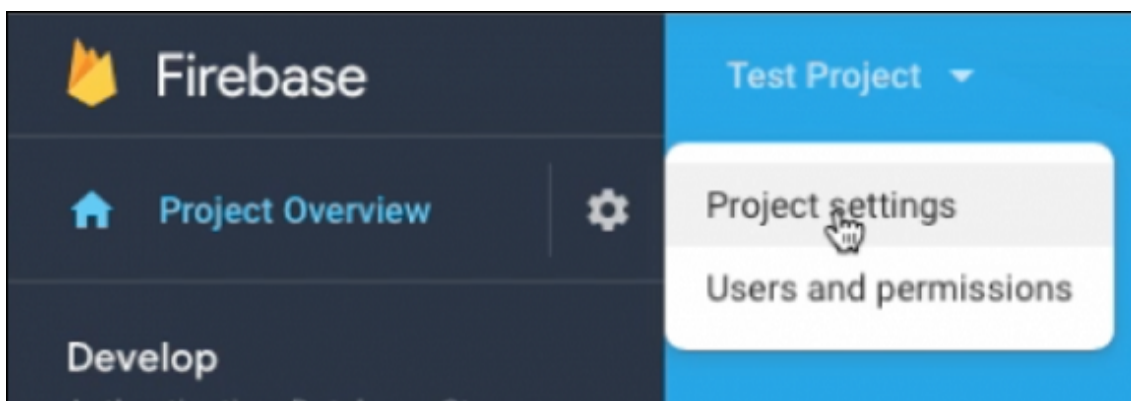


### To configure your Google account for FCM

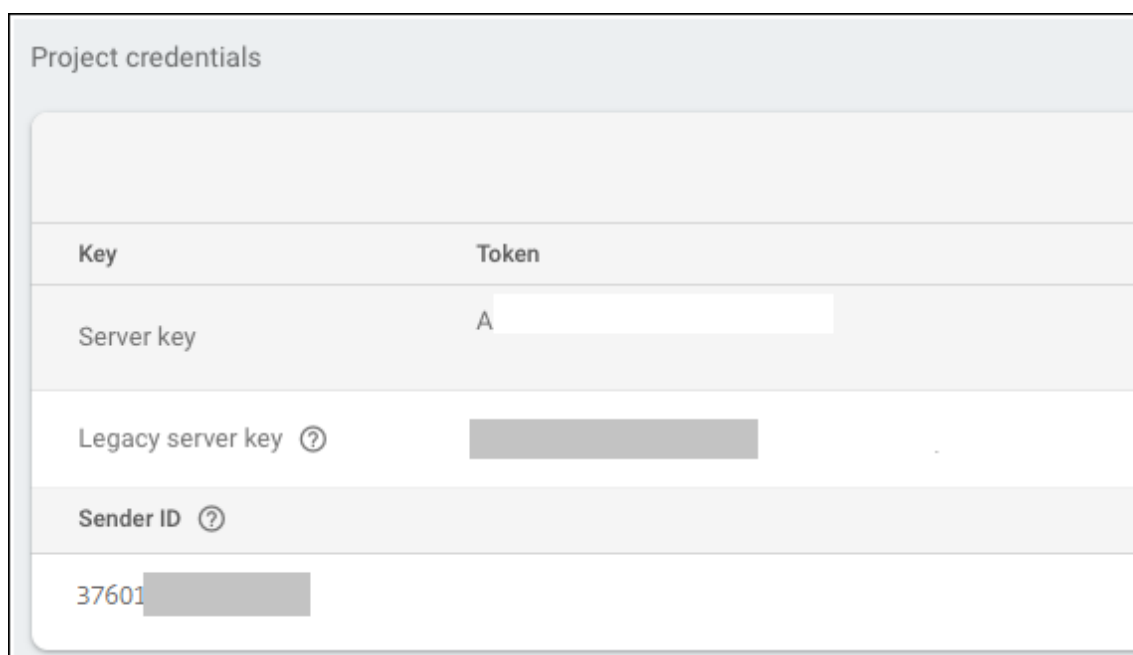
1. Sign in to the following URL using your Google developer account credentials:  
<https://console.firebase.google.com/>
2. Click **Add project**.



3. After you create the project, click **Project settings**.



4. Click the **Cloud Messaging** tab. Copy the **Server key** and **Sender ID** values. In the next procedure, you paste those values in the Endpoint Management console. As of October 2016, you must create Server Keys in the Firebase console.

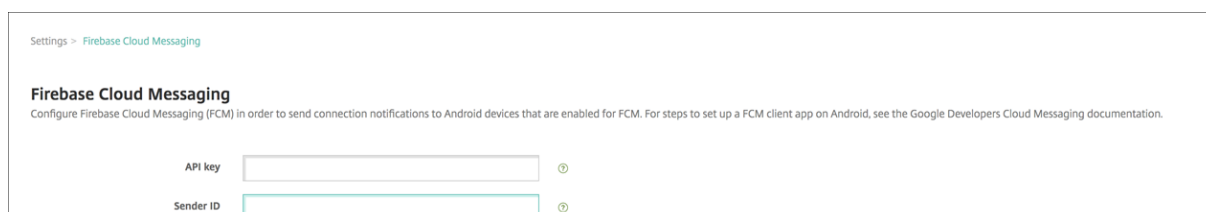


For steps to set up an FCM client app on Android, see this Google Developers Cloud Messaging article: <https://firebase.google.com/docs/cloud-messaging/android/client>.

### To configure Endpoint Management for FCM

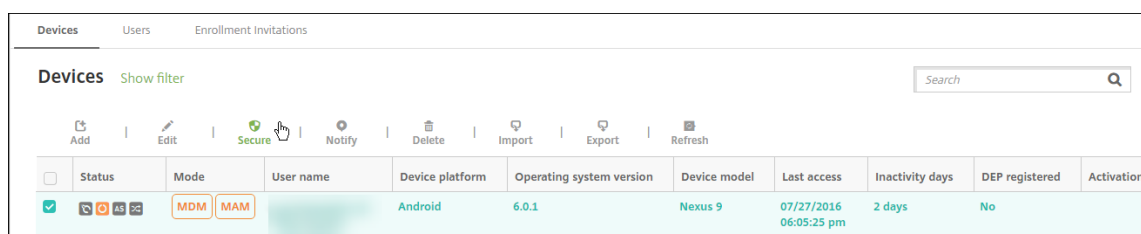
In the Endpoint Management console, go to **Settings > Firebase Cloud Messaging**.

- Edit **API key**, and type the Firebase Cloud Messaging **Server key** that you copied in the last step of Firebase Cloud Messaging configuration.
- Edit **Sender ID**, and type the **Sender ID** value you copied in the previous procedure.



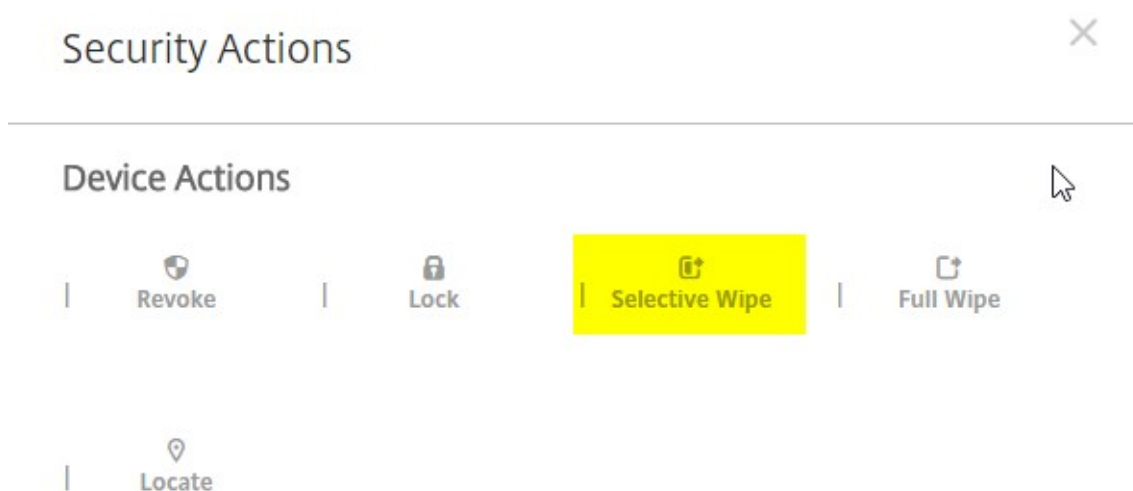
### To test your configuration

1. Enroll an Android device.
2. Leave the device idle for some time, so that it disconnects from Endpoint Management.
3. From the Endpoint Management console, click **Manage**, select the Android device, and then click **Secure**.



	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP registered	Activation
<input checked="" type="checkbox"/>		MDM   MAM		Android	6.0.1	Nexus 9	07/27/2016 06:05:25 pm	2 days	No	

4. Under **Device Actions**, click **Selective Wipe**.



In a successful configuration, selective wipe occurs on the device.

## Android SafetyNet

September 23, 2019

You can use the Android SafetyNet feature to assess the compatibility and security of Android devices that have Secure Hub installed. Android SafetyNet isn't available for MAM deployments.

When this feature is enabled, the SafetyNet Attestation API examines software and hardware information on a device to create a profile of that device. The API then looks for the same profile within a list of device models that have passed Android compatibility testing. The API also uses this information to determine whether Secure Hub has been modified by an unknown source.

When the Android SafetyNet feature is enabled, Secure Hub sends the SafetyNet Attestation API request to Google Play services and the result is reported back to Endpoint Management. Endpoint Management then updates device information with the attestation results. You can set automated actions that use the attestation results to trigger actions on the device.

For more information about how the SafetyNet Attestation API works, see the [Android developers documentation](#).

## Estimate how many SafetyNet Attestation API requests you need

SafetyNet Attestation API requests are sent:

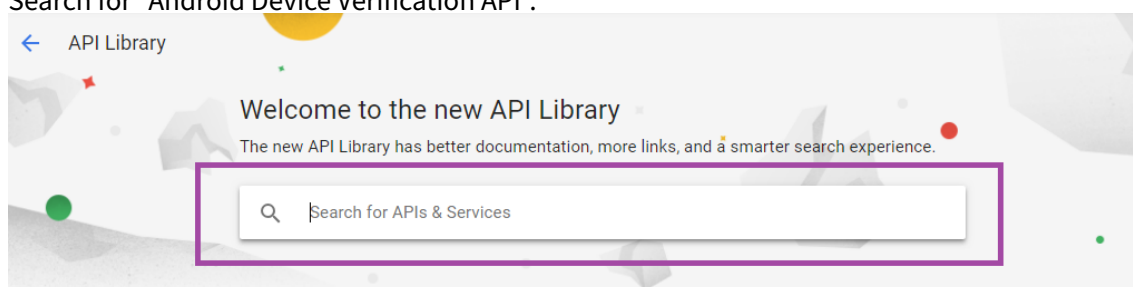
- When a device is enrolled in Endpoint Management.
- When a Secure Hub online authentication occurs. Online authentication occurs when a server session expires or when a user signs off the server and then signs back on. Secure Hub prompts the user to provide credential to authenticate with the server.
- When a device is rebooted.
- At a recurring time interval you configure, between 24 and 1,000 hours.

If your Endpoint Management deployment will make more than 10,000 requests per day, [fill out this quota request form](#).

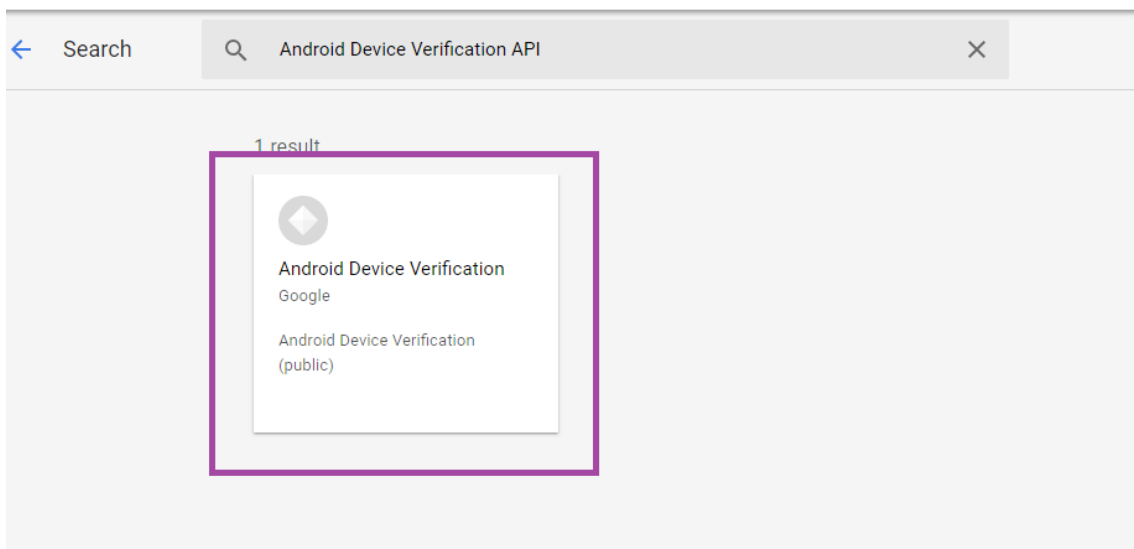
## Get the SafetyNet API key

To enable Android SafetyNet in Endpoint Management, you need the SafetyNet API key.

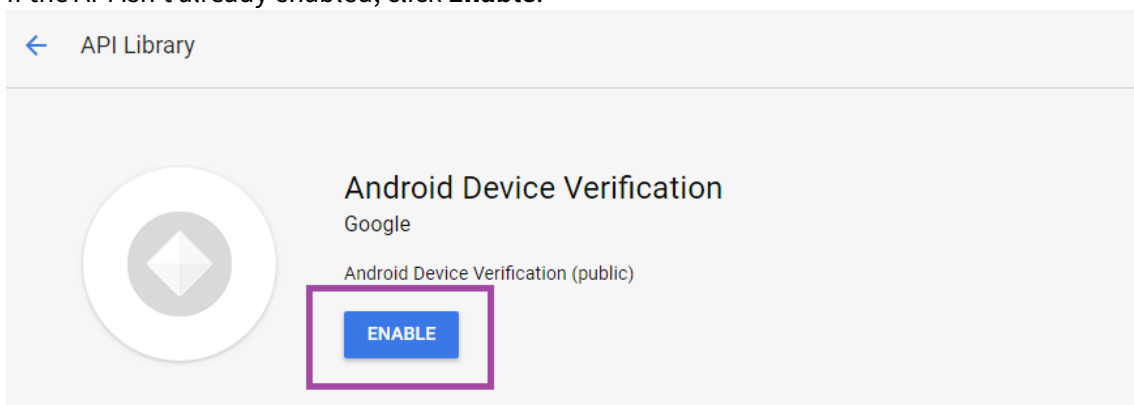
1. Log in to the Google API console with your Google administrator account credentials.
2. Go to the Library page.
3. Search for “Android Device Verification API”.



4. Click **Android Device Verification API**.

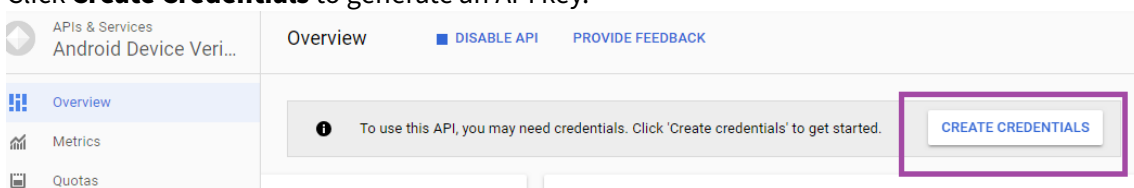


5. If the API isn't already enabled, click **Enable**.

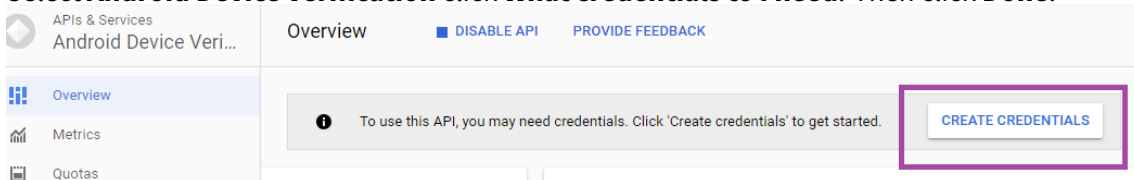


6. Click **Manage**.

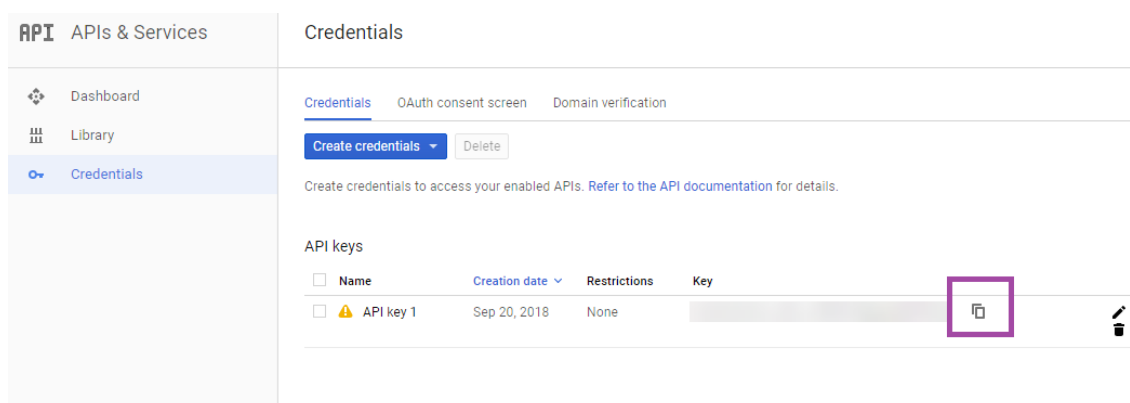
7. Click **Create Credentials** to generate an API key.



8. Select **Android Device Verification** click **What credentials to I need**. Then click **Done**.



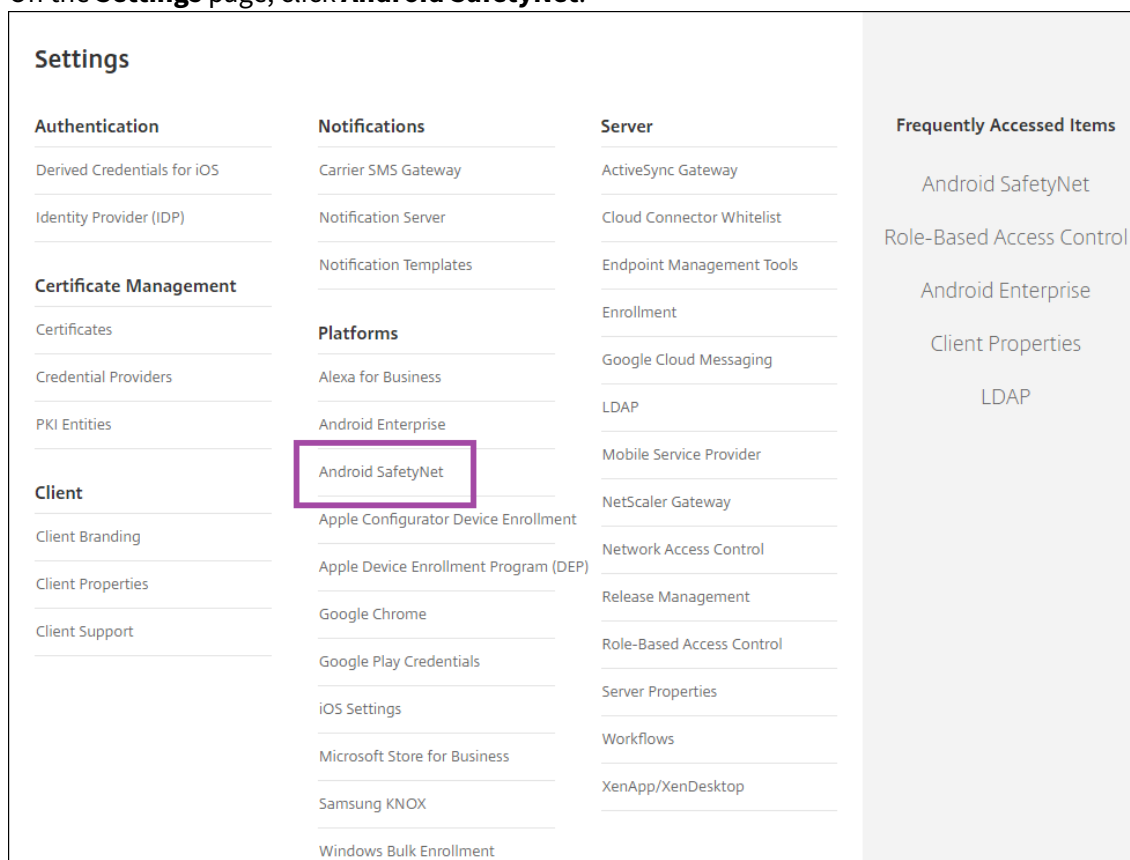
9. In the **Credentials** page, click the copy icon next to the key to copy the key.



10. Save the key so you can paste it into the Endpoint Management console when you enable the Android SafetyNet.

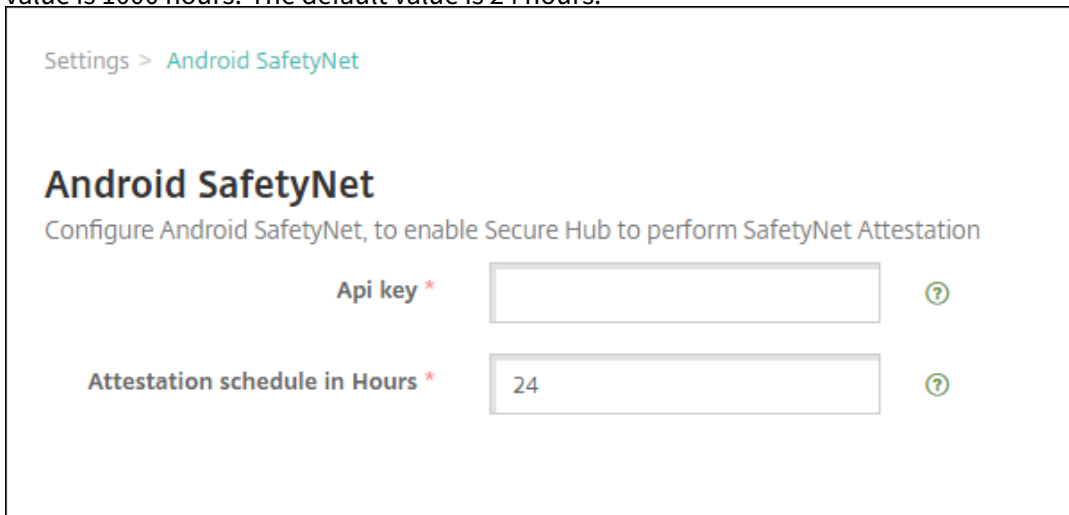
### Enable Android SafetyNet

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. On the **Settings** page, click **Android SafetyNet**.



3. Configure these settings:

- **API Key.** Paste in the SafetyNet API key that you got from the Google API console.
- **Attestation schedule in hours.** Type interval at which the SafetyNet Attestation API assesses your Android devices, in hours. The minimum value is 24 hours. The maximum value is 1000 hours. The default value is 24 hours.

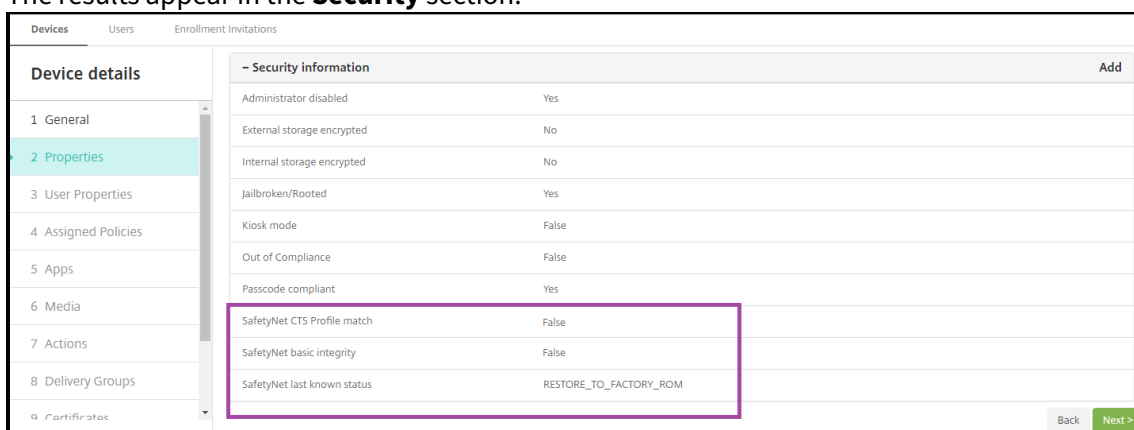


4. Click **Save**.

### View Android SafetyNet results

To view the results of the SafetyNet Attestation API assessment for a device:

1. In the Endpoint Management console, click **Manage > Devices**.
2. Select Android devices to see the SafetyNet Attestation API results. Then click **Show more**.
3. In the **Device details** page, select **Properties**.
4. The results appear in the **Security** section.



The SafetyNet Attestation API returns these statuses for each device:



- **SafetyNet CTS profile match:** If this value is **True**, the device has a profile that matches one that has passed Android Compatibility Test Suite (CTS). If this value is **False**, the device does not have a profile that matches one that has passed Android CTS.
- **SafetyNet basic integrity:** If this value is **True**, the SafetyNet Attestation API found no evidence that Secure Hub on the device has been modified by an unknown source. If this value is **False**, Secure Hub on the device has been modified by an unknown source.
- **SafetyNet last known status:** This value shows the last known SafetyNet status of the device:
  - **Success:** The SafetyNet Attestation API found no evidence that Secure Hub on the device has been modified by an unknown source.
  - **LOCK\_BOOTLOADER:** The user should lock the bootloader of the device. Secure Hub on the device has been modified by an unknown source.
  - **RESTORE\_TO\_FACTORY\_ROM:** The user should restore the device to a clean factory ROM. Secure Hub on the device has been modified by an unknown source.

## Samsung

April 1, 2021

Samsung offers several solutions that are compatible with Citrix Endpoint Management.

- Endpoint Management supports and extends Samsung Knox policies on compatible Samsung devices.
- The Knox Service plug-in (KSP) is an app that supports a subset of Knox Platform for Enterprise (KPE) features. For information from Samsung about KPE, see [Configure Knox Platform for Enterprise](#) and [Overview](#).

To control how and when Android devices connect to the Endpoint Management service, use Firebase Cloud Messaging (FCM). For information, see [Firebase Cloud Messaging](#).

Enrollment profiles determine whether Android devices enroll in MAM, MDM, or MDM+MAM, with the option for users to opt out of MDM. Endpoint Management supports the following authentication types for Android devices enrolled in MDM+MAM. For information, see the following articles:

- [Domain or domain plus security token authentication](#)
- [Client certificate or certificate plus domain authentication](#)
- Identity providers:
  - [Authentication with Azure Active Directory through Citrix Cloud](#)
  - [Authentication with Okta through Citrix Cloud](#)

Another rarely used authentication method is client certificate plus security token. For information, see <https://support.citrix.com/article/CTX215200>.

A general workflow for starting Android device management is as follows:

1. Complete the onboarding process. See [Onboarding and resource setup](#) and [Prepare to enroll devices and deliver resources](#).
2. Choose and configure an enrollment method. See [Supported enrollment methods](#).
3. Deploy Samsung license keys.
4. Enable Knox attestation.
5. Configure Samsung device policies.
6. Set up device and app security actions. See [Security actions](#).

For supported operating systems, see [Supported device operating systems](#).

### Supported enrollment methods

The following table lists the enrollment methods that Endpoint Management supports for Android devices:

Method	Supported
Bulk enrollment	Yes (Knox)
Manual enrollment	Yes
Enrollment invitations	Yes

You can use Knox Mobile Enrollment to enroll multiple Knox devices into Endpoint Management (or any mobile device manager) without manually configuring each device. For information, see [Samsung Knox bulk enrollment](#).

For information about enrolling devices, see [Enroll Android devices](#).

### Deploy Samsung license keys

Samsung has Enterprise License Management (ELM) keys and Knox License Management (KLM) keys. You purchase Samsung licenses from Samsung.

- Knox: The Knox platform requires that you purchase a Knox Workspace license. To enable the Knox APIs and deploy Knox policies and restrictions to devices, first configure the Endpoint Management device policy, Samsung MDM license key. To activate Knox, you must push at least one Restriction device policy specifically for Knox along with the ELM and KLMS key.

- **SAFE:** Deploy the built-in Samsung ELM key to a device before deploying SAFE policies and restrictions. To deploy that key, configure the Endpoint Management device policy, Samsung MDM license key.

### Samsung enterprise Firmware-Over-The-Air (E-FOTA) service

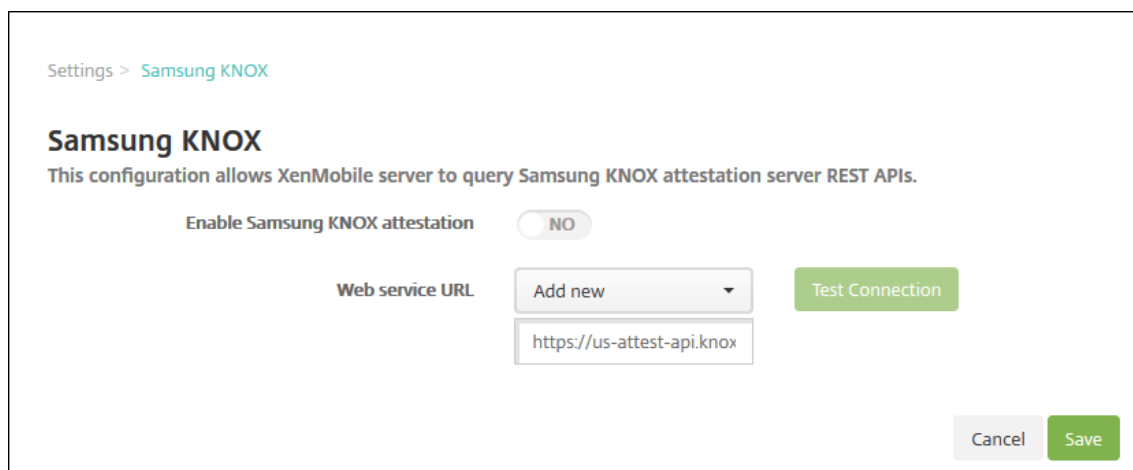
Endpoint Management also supports the Samsung Enterprise Firmware-Over-The-Air (E-FOTA) service. Samsung E-FOTA lets you determine when devices get updated, determine the firmware version to use, and test updates before deploying them. For information, see [Configure Samsung E-FOTA settings](#).

### Enable Knox attestation

You can configure Endpoint Management to query the Knox attestation server REST APIs.

Knox applies hardware security capabilities that provide multiple levels of protection for the operating system and applications. One level of this security resides at the platform through attestation. An attestation server provides verification of the mobile device core system software (for example, the boot loaders and kernel). The verification occurs at runtime based on data collected during a trusted boot.

1. In the Endpoint Management web console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **Samsung Knox**.



Settings > Samsung KNOX

### Samsung KNOX

This configuration allows XenMobile server to query Samsung KNOX attestation server REST APIs.

Enable Samsung KNOX attestation  NO

Web service URL

3. Set **Enable Samsung Knox attestation** to **Yes** to enable Knox attestation. The default is **No**.
4. In the **Web service URL** list, do one of the following:
  - Click the appropriate attestation server.
  - Click **Add new** and then enter the Web service URL.

5. Click **Test Connection** to verify the connection. A success or failure message appears.
6. Click **Save**.

### Configure Samsung device policies

Device policies for Knox:

---

App Restrictions	App Uninstall	Browser
Copy Apps to Samsung Container	Exchange	Knox Platform for Enterprise key
Passcode	Restrictions	Samsung MDM License key
VPN		

---

Device policies for Samsung SAFE:

---

App Uninstall Restrictions	Browser	Exchange
Firewall	Kiosk	Knox Platform for Enterprise
OS update	Restrictions	Samsung MDM License key
Storage Encryption	VPN	

---

### Security actions

Android supports the following security actions. For a description of each security action, see [Security actions](#).

---

App Lock	App Wipe	Certificate Renewal
Full Wipe	Locate	Lock
Lock and Reset Password	Notify	Revoke
Selective Wipe		

---

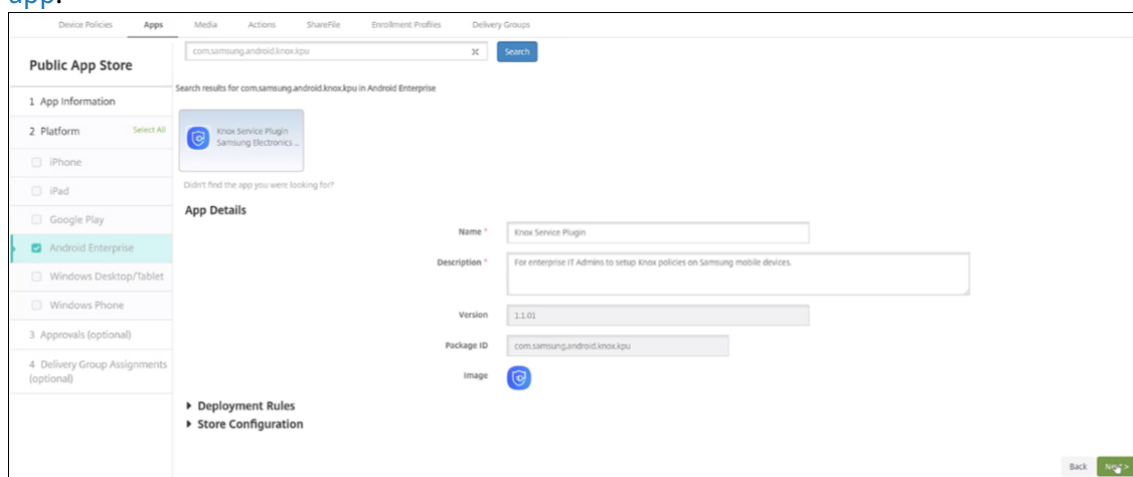
**Note:**

For devices running Android 6.0 and greater, the Locate security action requires the user to grant Location permission during enrollment. The user can opt not to grant Location permissions. If the user doesn't grant the permission during enrollment, Endpoint Management again requests location permissions when sending the Locate command.

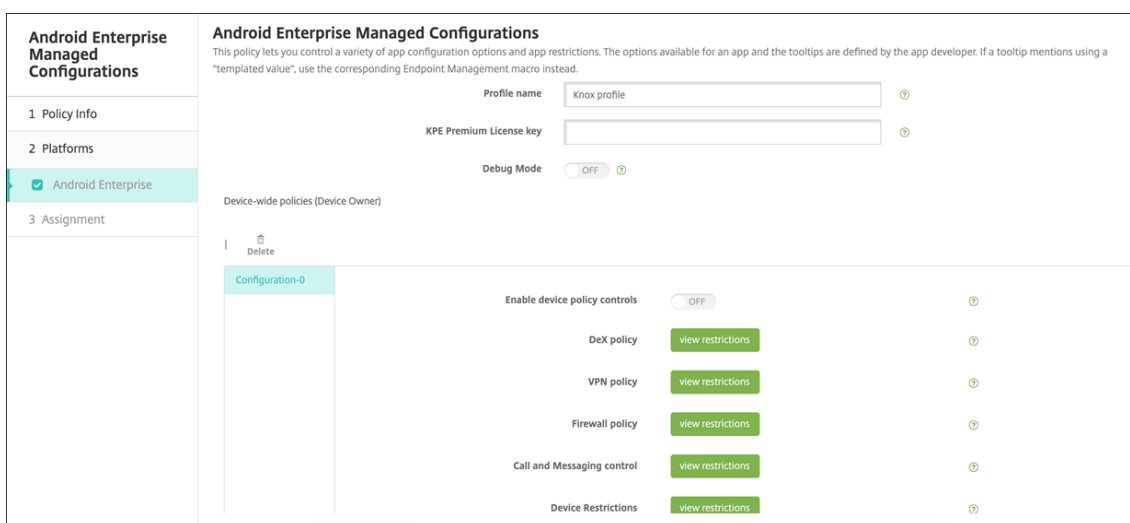
**Add the Knox service plug-in app**

If you plan on using Android Enterprise with Knox, add the Knox service plug-in to Endpoint Management. The KSP app uses AndroidOEMConfig to support features such as security policies, flexible VPN configuration, and biometric authentication controls. AndroidOEMConfig enables OEMs and endpoint mobility managers (EMM) to support custom OEM APIs that cover use cases not supported through Android Enterprise. For more information on KSP, see the [Knox Service Plugin Admin Guide](#).

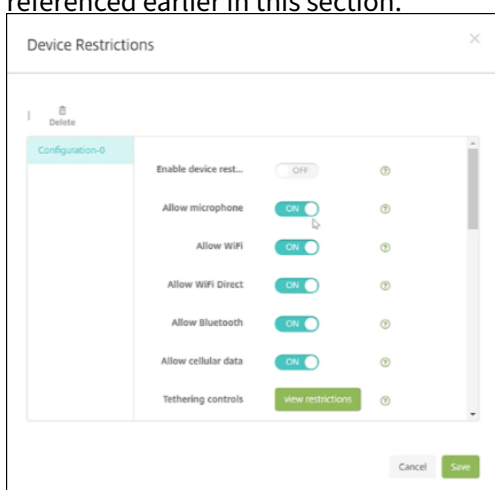
1. Log in to your Google account and navigate to <https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu>. Approve the Knox Service Plugin app.
2. Log in to your Endpoint Management console and add the Knox service plug-in as a public app store app. For more information on adding public app store apps, see [Add a public app store app](#).



3. In your Endpoint Management console, navigate to **Configure > Device policies**. Click **Add**.
4. Click **Android Enterprise Managed Configuration**. In the dialog that comes up, select **Knox Service Plugin** from the menu. For more information on the Android Enterprise managed configuration policy, see [Managed configurations policy](#).
5. Type a name for the policy then continue to the platform page.



6. On the platform page, type a **Profile name** for your Knox profile and input the **KPE Premium License key** from Samsung. The policies that appear below these fields come from your Knox deployment. For more information on Knox policies, see the Knox Service Admin Plugin Guide referenced earlier in this section.



7. Click **Next** and configure deployment rules for the policy.
8. Click **Save**.

## Samsung Knox bulk enrollment

October 18, 2021

To enroll multiple Samsung Knox devices into Endpoint Management (or any mobile device manager) without manually configuring each device, use Knox Mobile Enrollment. The enrollment occurs upon first-time use or after a factory reset. Admins can also pass user names and passwords directly to the device, so users don't need to enter any information upon enrollment.

**Note:**

The setup for Knox Mobile Enrollment is not related to the Endpoint Management Knox container. For more information on Knox Mobile Enrollment, see the [Knox Mobile Enrollment Admin Guide](#).

**Prerequisites for Knox Mobile Enrollment**

- Endpoint Management must be configured (including licenses and certificates) and running.
- Secure Hub APK file. You upload the file when setting up Knox Mobile Enrollment.
- For a list of KME requirements, see the [Knox Mobile Enrollment Introduction](#).
- Samsung Knox Platform for Enterprise (PKE) license, required to apply device policies. Provide the license key in the Endpoint Management device policy, Knox Platform for Enterprise.

**To download the Secure Hub APK file**

Go to the Google Play store to download the Citrix Secure Hub for Android file.

**Configure firewall exceptions**

To access Knox Mobile Enrollment, configure the following firewall exceptions. Some of these firewall exceptions are required for all devices and some are specific the device's geographical region.

Device Region	URL	Port	Destination
All	<a href="https://gslb.secb2b.com">https://gslb.secb2b.com</a>	443	Global load balancer for Knox Mobile Enrollment initiation
All	<a href="https://gslb.secb2b.com">https://gslb.secb2b.com</a>	80	Global load balancer for Knox Mobile Enrollment initiation on some limited legacy devices
All	<a href="https://umc-cdn.secb2b.com">umc-cdn.secb2b.com</a>	443	Samsung agent update servers
All	<a href="https://bulkenrollment.s3.amazonaws.com">bulkenrollment.s3.amazonaws.com</a>	80	Knox Mobile Enrollment customer EULAs
All	<a href="https://eula.secb2b.com">eula.secb2b.com</a>	443	Knox Mobile Enrollment customer EULAs

Device Region	URL	Port	Destination
All	<a href="https://us-be-api-mssl.samsungknox.com">us-be-api-mssl.samsungknox.com</a>	443	Samsung servers for IMEI verification
United States	<a href="https://us-segd-api.secb2b.com">https://us-segd-api.secb2b.com</a>	443	Samsung Enterprise Gateway for US region
Europe	<a href="https://eu-segd-api.secb2b.com">https://eu-segd-api.secb2b.com</a>	443	Samsung Enterprise Gateway for European region
China	<a href="https://china-segd-api.secb2b.com">https://china-segd-api.secb2b.com</a>	443	Samsung Enterprise Gateway for China region

**Note:**

You can find a full list of firewall exceptions in the [Knox Mobile Enrollment Admin Guide](#).

## Getting access to Knox Mobile Enrollment

Follow Samsung documentation to get access to Knox Mobile Enrollment at [Get started with KME](#).

## Setting up Knox Mobile Enrollment

After you get access to Knox Mobile Enrollment, log in to the Knox portal.

The enrollment process follows these general steps.

1. Create an MDM profile with your MDM console information and settings.  
The MDM profile indicates to your devices how to connect to your MDM.
2. Add devices to your MDM profile.  
You can either upload a CSV file with device information or install and use the Knox deployment app from Google Play.
3. Samsung alerts you when device ownership is verified.
4. Provide users with MDM credentials. Instruct them to connect to the Internet using Wi-Fi and to accept the prompt to enroll their device.



## To create an MDM profile

Follow the steps outlined in Samsung documentation on [Profile Configuration](#).

When you encounter the following fields or steps, configure them as described:

- **Pick your MDM:** Select **Citrix** from the menu. Only for device owner profiles.
- **MDM Agent APK:** Only for device owner profiles. Type the Secure Hub APK download URL: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

The APK file can reside on any server that the devices can access during enrollment. During enrollment, a device:

- Downloads Secure Hub from APK download URL
- Installs Secure Hub
- Then opens Secure Hub with the custom JSON data described next.

The capitalization of the .apk file name must match the URL you enter. For example, if the file name is all lowercase, it must also be all lowercase in the URL.

- **MDM Server URI:** Do not specify an MDM server URI. Endpoint Management does not use the Samsung MDM protocol.
- **Custom JSON Data:** Secure Hub needs the Endpoint Management server address plus the user name and password for enrollment. You can provide that data in JSON so that Secure Hub doesn't prompt users for it. Secure Hub prompts users for server address, user name, or password only if the field is omitted from the JSON.

The format for custom JSON data is:

```
{ "serverURL": "URL", "username":"Username", "password":"Password"}
```

In this example, typical for bulk enrollment, Secure Hub doesn't prompt users for the server address or their credentials during enrollment:

```
{ "serverURL":"https://example.com/zdm", "username":"userN", "password":  
:"password1234"}  
{ "serverURL":"https://pmdm.mycorp-inc.net/zdm", "username":"userN2", "  
password":"password7890"}
```

In this example, typical for kiosk-based devices, Secure Hub prompts users for their credentials:

```
{ "serverURL":"https://example.com/zdm"}
```

To enroll devices in the work profile on corporate-owned devices mode, add { `"desiredProvisioningMode": "managedProfile"` } to the custom JSON. See the following example:

```
{ "serverURL":"https://example.com/zdm", "username":"userN", "password"  
:"password1234", "desiredProvisioningMode": "managedProfile"}
```

You can copy the following code block as a starting point for your JSON:

```
1      {
2
3          {
4              "serverURL": "URL", "username": "username", "password": "
5              password"
6          }
7      }
8  }
9
10 <!--NeedCopy-->
```

**Important:**

To enroll devices in the work profile on corporate-owned devices mode, add { `"desiredProvisioningMode": "managedProfile"` } to the custom JSON.

When a device starts enrollment, the device downloads Secure Hub from the given URL, installs Secure Hub, and opens Secure Hub.

You can also use the Android zero-touch enrollment feature to enroll devices. For more information, see [Zero-touch enrollment](#).

**Further configuration**

See the following Samsung documentation pages for more information on configuration:

- [Device configuration](#): Add devices in bulk.
- [Samsung Knox Deployment App](#): Enroll devices through bluetooth, NFC, or Wi-Fi Direct enrollment.
- [Knox Mobile Enrollment](#): Explore Samsung documentation for more information on Samsung Knox.

**To enroll devices running a Knox API earlier than version 2.4**

On devices that have Knox API earlier than version 2.4, bulk enrollment doesn't start during the initial device setup. Instead, users must initiate enrollment. To do that, users go to a Samsung site to download the new Mobile Enrollment client and start the enrollment.

The downloaded enrollment client uses the same MDM profile and APKs configured in the Knox Bulk enrollment portal for the Knox 2.4/2.4.1 devices.

Users typically follow these steps:

1. Turn on the device and connect to Wi-Fi. If the Mobile Enrollment doesn't start or Wi-Fi is not available, do the following:
  - a) Go to [Samsung Knox Mobile Enrollment](#).
  - b) Tap the **Next** button to enroll devices with mobile data.
2. When the prompt **Enroll with Knox** appears, tap **Continue**.
3. Read the EULAs (if available). Tap **Next**.
4. If prompted, enter the **User ID** and **Password** provided by the IT administrator.

At this point, the user credentials are validated and their device is enrolled in your organization's enterprise IT environment.

## Enable and disable biometric authentication for Samsung devices

Endpoint Management supports fingerprint and iris scan authentication, also known as biometric authentication. You can enable and disable biometric authentication for Samsung devices without requiring any action from users. If you disable biometric authentication in Endpoint Management, users and third-party apps cannot enable the feature.

1. In the Endpoint Management console, click **Configure > Device Policies**. The **Device Policies** page appears.
2. Click **Add**. The **Add New Policy** page appears.
3. Click **Passcode**. The **Passcode Policy information** page appears.
4. In the **Policy Information** pane, enter the following information:
  - **Policy Name:** Type a descriptive name for the policy.
  - **Description:** Optionally, type a description of the policy.
5. Click **Next**. The **Platforms** page appears.
6. Under **Platforms**, select **Android** or **Samsung Knox**.
7. Set **Configure biometric authentication** to **On**.
8. If you selected **Android**, under **Samsung SAFE**, select **Allow fingerprint**, **Allow Iris**, or both.

Passcode Policy

1 Policy Info

2 Platforms

iOS

Mac OS X

Android

Samsung KNOX

Android for Work

Windows Phone

Use same passcode across all users  OFF

Changed characters

Number of times a character can occur

Alphabetic sequence length

Numeric sequence length

Allow users to make password visible  ON

Configure biometric authentication  ON

Allow fingerprint

Allow Iris

Forbidden Strings

## Network Access Control

April 28, 2021

You can use your Network Access Control (NAC) solution to extend the Endpoint Management device security assessment for Android and Apple devices. Your NAC solution uses the Endpoint Management security assessment to facilitate and handle authentication decisions. After you configure your NAC appliance, the device policies and NAC filters that you configure in Endpoint Management get enforced.

Using Endpoint Management with a NAC solution adds QoS and more granular control over devices that are internal to your network. For a summary of the advantages of integrating NAC with Endpoint Management, see [Access control](#).

Citrix supports these solutions for integration with Endpoint Management:

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

Citrix doesn't guarantee integration for other NAC solutions.

With a NAC appliance in your network:

- Endpoint Management supports NAC as an endpoint security feature for iOS, Android Enterprise, and Android devices.
- You can enable filters in Endpoint Management to set devices as compliant or non-compliant for NAC, based on rules or properties. For example:
  - If a managed device in Endpoint Management doesn't meet the specified criteria, Endpoint Management marks the device as non-compliant. A NAC appliance blocks non-compliant devices on your network.
  - If a managed device in Endpoint Management has non-compliant apps installed, a NAC filter can block the VPN connection. As a result, a non-compliant user device cannot access apps or websites through the VPN.
  - If you use Citrix Gateway for NAC, you can enable split tunneling to prevent the Citrix Gateway plug-in from sending unnecessary network traffic to Citrix Gateway. For more information on split tunneling, see [Configuring Split Tunneling](#).

### Supported NAC compliance filters

Endpoint Management supports the following NAC compliance filters:

**Anonymous Devices:** Checks if a device is in anonymous mode. This check is available if Endpoint Management can't reauthenticate the user when a device attempts to reconnect.

**Failed Samsung Knox attestation:** Checks if a device failed a query of the Samsung Knox attestation server.

**Forbidden Apps:** Checks if a device has forbidden apps, as defined in an App Access policy. For more information about that policy, see [App access device policies](#).

**Inactive Devices:** Checks if a device is inactive as defined by the **Device Inactivity Days Threshold** setting in **Server Properties**. For details, see [Server properties](#).

**Missing Required Apps:** Checks if a device is missing any required apps, as defined in an App Access policy.

**Non-suggested Apps:** Checks if a device has non-suggested apps, as defined in an App Access policy.

**Noncompliant Password:** Checks if the user password is compliant. On iOS and Android devices, Endpoint Management can determine whether the password currently on the device is compliant with the passcode policy sent to the device. For instance, on iOS, the user has 60 minutes to set a password if Endpoint Management sends a passcode policy to the device. Before the user sets the password, the passcode might be non-compliant.

**Out of Compliance Devices:** Checks whether a device is out of compliance, based on the Out of Compliance device property. Typically, automated actions or third parties using Endpoint Management APIs change that property.

**Revoked Status:** Checks whether the device certificate is revoked. A revoked device cannot re-enroll until it is authorized again.

**Rooted Android and Jailbroken iOS Devices:** Checks whether an Android or iOS device is jailbroken.

**Unmanaged Devices:** Check whether Endpoint Management is managing a device. For example, a device enrolled in MAM or an unenrolled device is not managed.

**Note:**

The Implicit Compliant/Not Compliant filter sets the default value only on devices that Endpoint Management is managing. For example, any devices that have a blocked app installed or are not enrolled, get marked as Not Compliant. The NAC appliance blocks those devices from your network.

## Configuration overview

We recommend that you configure the NAC components in the order listed.

1. Configure device policies to support NAC:

**For iOS devices:** See [Configure the VPN device policy to support NAC](#).

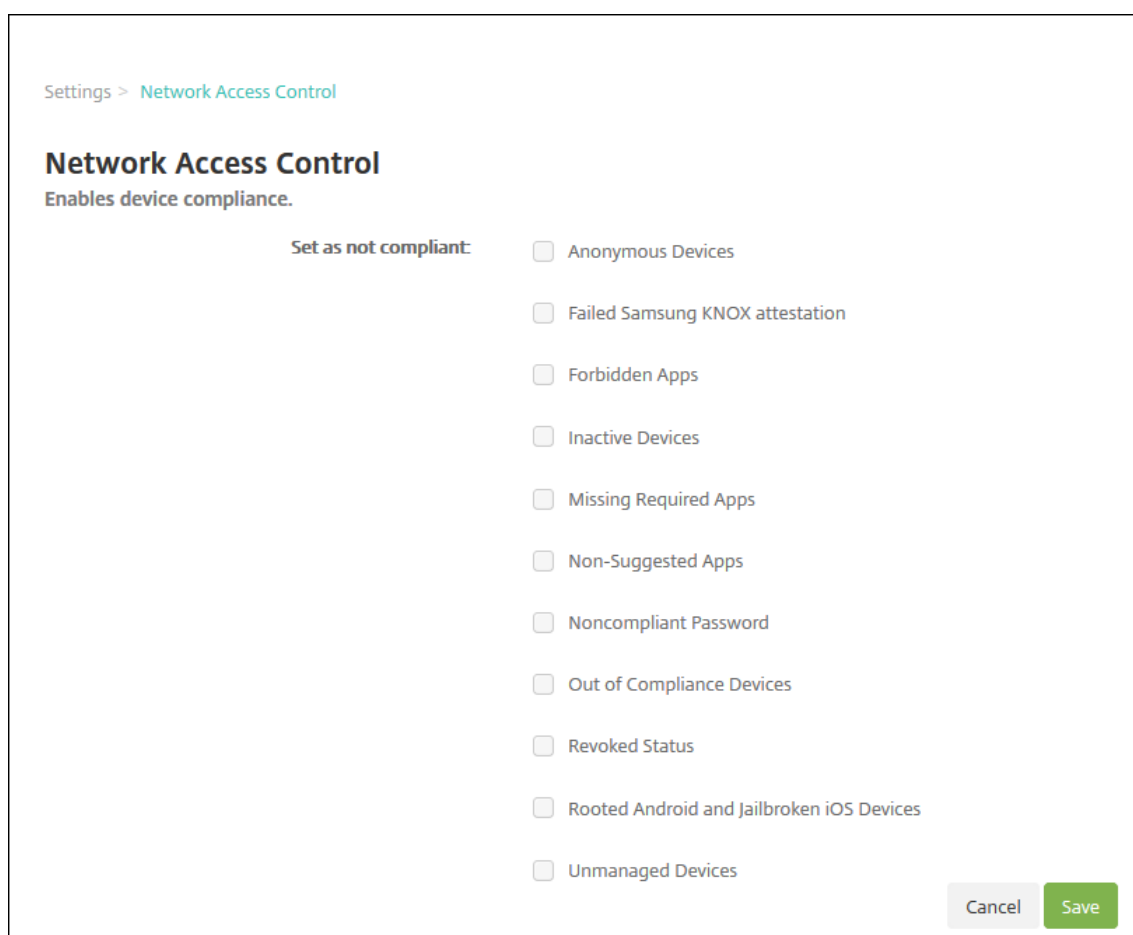
**For Android Enterprise devices:** See [Create an Android Enterprise managed configuration for Citrix SSO](#).

**For Android devices:** See [Configure the Citrix SSO protocol for Android](#).

2. Enable NAC filters in Endpoint Management.
3. Configure a NAC solution:
  - Citrix Gateway, detailed in [Update Citrix Gateway policies to support NAC](#). Requires that you install Citrix SSO on devices. See [Citrix Gateway Clients](#).
  - Cisco ISE: See the Cisco documentation.
  - ForeScout: See the ForeScout documentation.

## Enable NAC filters in Endpoint Management

1. In the Endpoint Management console, go to **Settings > Network Access Control**.



2. Select the check boxes for the **Set as not compliant** filters you want to enable.
3. Click **Save**.

## Update Citrix Gateway policies to support NAC

You must configure advanced (not classic) authentication and VPN sessions policies on your VPN virtual server.

These steps update a Citrix Gateway with either of these characteristics:

- Is integrated with Endpoint Management.
- Or, is set up for VPN, not part of the Endpoint Management environment, and can reach Endpoint Management.

On your virtual VPN server from a console window, do the following. The FQDNs and IP addresses in the commands and examples are fictitious.

1. If you are using classic policies on your VPN virtual server, remove and unbind all classic policies. To check, type:

```
show vpn vserver <VPN_VServer>
```

Remove any result that contains the word Classic. For example: VPN Session Policy Name : PL\_OS\_10.10.1.1 Type: Classic Priority: 0

To remove the policy, type:

```
unbind vpn vserver <VPN_VServer> -policy <policy_name>
```

2. Create the corresponding advanced session policy by typing the following.

```
add vpn sessionPolicy <policy_name> <rule> <session action>
```

For example: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. Bind the policy to your VPN virtual server by typing the following.

```
bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100
```

4. Create an authentication virtual server by typing the following.

```
add authentication vserver <authentication vserver name> <service type>  
<ip address>
```

For example: `add authentication vserver authvs SSL 0.0.0.0`

In the example, 0.0.0.0 means that the authentication virtual server is not public facing.

5. Bind an SSL certificate with the virtual server by typing the following.

```
bind ssl vserver <authentication vserver name> -certkeyName <Webserver  
certificate>
```

Forexample: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Associate an authentication profile to the authentication virtual server from the VPN virtual server. First, create the authentication profile by typing the following.

```
add authentication authnProfile <profile name> -authnVsName <authentication
  vsServer name>
```

For example:

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. Associate the authentication profile with the VPN virtual server by typing the following.

```
set vpn vsServer <vpn vsServer name> -authnProfile <authn profile name>
```

For example:

```
set vpn vsServer _XM_EndpointManagement -authnProfile xm_nac_prof
```

8. Check the connection from Citrix Gateway to a device by typing the following.

```
curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/
Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
```

For example, this query verifies connectivity by obtaining the compliance status for the first device (`deviceid_1`) enrolled in the environment:

```
curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-
Citrix-VPN-Device-ID: deviceid_1"
```

A successful result is similar to the following example.

```
1 HTTP/1.1 200 OK
2 < Server: Apache-Coyote/1.1
3 < X-Citrix-Device-State: Non Compliant
4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
5 <!--NeedCopy-->
```

9. When the preceding step is successful, create the web authentication action to Endpoint Management. First, create a policy expression to extract the device ID from the iOS VPN plug-in. Type the following.
10. Send the request to Endpoint Management by typing the following. In this example, the Endpoint Management IP is 10.207.87.82 and the FQDN is `example.em.cloud.com:4443`.

```
add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).
TYPECAST_NVLIST_T('\='\'','&\'').VALUE(\"deviceidvalue\")"
```

```
add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort
4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n"+ "
Host: example.em.cloud.com:4443\r\n"+ "X-Citrix-VPN-Device-ID: "+
```



```
xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ(\"Compliant\")"
```

The successful output for the Endpoint Management NAC is `HTTP status 200 OK`. The `X-Citrix-Device-State` header must have the value of `Compliant`.

11. Create an authentication policy with which to associate the action by typing the following.

```
add authentication Policy <policy name> -rule <rule> -action <web authentication action>
```

For example: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. Convert the existing LDAP policy to an advanced policy by typing the following.

```
add authentication Policy <policy_name> -rule <rule> -action <LDAP action name>
```

For example: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Add a policy label with which to associate the LDAP policy by typing the following.

```
add authentication policylabel <policy_label_name>
```

For example: `add authentication policylabel ldap_pol_label`

14. Associate the LDAP policy to the policy label by typing the following.

```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
```

15. Connect a compliant device to do a NAC test to confirm successful LDAP authentication. Type the following.

```
bind authentication vserver <authentication vserver> -policy <web authentication policy> -priority 100 -nextFactor <ldap policy label> -gotoPriorityExpression END
```

16. Add the UI to associate with the authentication virtual server. Type the following command to retrieve the device ID.

```
add authentication loginSchemaPolicy <schema policy>-rule <rule> -action lschema_single_factor_deviceid
```

17. Bind the authentication virtual server by typing the following.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority 100 -gotoPriorityExpression END
```

18. Create an LDAP advanced authentication policy enable the Secure Hub connection. Type the following.

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\n\nUser-Agent\n").CONTAINS(\n\n"NAC\n").NOT"-action 10.200.80.60_LDAP\n\nbind authentication vserver authvs -policy ldap_xm_test_pol -priority\n\n110 -gotoPriorityExpression NEXT
```

## iOS

October 21, 2021

To manage iOS devices in Endpoint Management, you set up an Apple Push Notification service (APNs) certificate from Apple. For information, see [APNs certificates](#).

Enrollment profiles determine whether iOS devices enroll in MDM+MAM, with the option for users to opt out of mobile device management (MDM). Endpoint Management supports the following authentication types for iOS devices in MDM+MAM. For information, see the following articles:

- [Domain or domain plus security token authentication](#)
- [Client certificate or certificate plus domain authentication](#)
- Identity providers:
  - [Authentication with Azure Active Directory through Citrix Cloud](#)
  - [Authentication with Okta through Citrix Cloud](#)

### Requirements for trusted certificates in iOS 13:

Apple has new requirements for TLS server certificates. Verify that all certificates follow the new Apple requirements. See the Apple publication, <https://support.apple.com/en-us/HT210176>. For help with managing certificates, see [Upload certificates](#).

A general workflow for starting iOS device management is as follows:

1. Complete the onboarding process. See [Onboarding and resource setup](#) and [Prepare to enroll devices and deliver resources](#).
2. Choose and configure an enrollment method. See [Supported enrollment methods](#).
3. Configure iOS device policies.
4. Enroll iOS devices.
5. Set up device and app security actions. See [Security actions](#).

For supported operating systems, see [Supported device operating systems](#).

## iOS 14 compatibility

Endpoint Management and Citrix mobile apps are compatible with iOS 14 but don't currently support the new iOS 14 features.

For supervised iOS devices, you can postpone software upgrades for up to 90 days. In the restrictions device policy for iOS, use these settings:

- **Force delayed software updates**
- **Enforce software update delay**

See [iOS settings](#). Those settings aren't available for devices in user enrollment mode or unsupervised (full MDM) mode.

## Apple host names that must remain open

Some Apple host names must remain open to ensure proper operation of iOS, macOS, and Apple App Store. Blocking those host names can affect the installation, update, and proper operation of the following: iOS, iOS apps, MDM operation, and device and app enrollment. For more information, see <https://support.apple.com/en-us/HT201999>.

## Supported enrollment methods

You specify how to manage iOS devices in enrollment profiles. You can choose between the following enrollment settings:

- **Apple User Enrollment:** For BYOD devices, offers a balance of privacy for personal data and security for corporate data. This enrollment mode is available as a public preview. To enable this feature, contact your support team.
- **Apple Device Enrollment:** For supervised iOS devices, with separate personal and corporate profiles on the device.
- **Do not manage devices:** Exclude these devices from MDM if you want to manage apps only.

For more information about creating enrollment profiles, see [Enrollment profiles](#).

Endpoint Management supports the following enrollment methods for iOS devices:

---

Method	Supported
Apple Business Manager	Yes
Apple School Manager	Yes
Apple Configurator	Yes
Manual enrollment	Yes

---

Method	Supported
Enrollment invitations	Yes

---

The Apple Deployment Programs include Apple Business Manager (ABM) for business organizations and Apple School Manager (ASM) for educational organizations. For more information, see [Deploy devices through the Apple Deployment Programs](#).

Apple School Manager is a type of Education Apple Deployment Program. See [Integrate with Apple Education features](#).

Use the Apple Deployment Programs to bulk enroll iOS, iPadOS, macOS, and tvOS devices. You can buy those devices directly from Apple, a participating Apple Authorized Reseller, or a carrier. Whether you purchase iOS devices directly from Apple, you can use the Apple Configurator to enroll those devices. See [Enroll Apple devices in bulk](#).

### Managed Apple IDs

User enrollment tightly integrates with Managed Apple IDs. You can create a Managed Apple ID manually using ABM/ASM or dynamically with Azure Active Directory (AAD).

For non-federated authentication, create Managed Apple IDs using ABM/ASM to add an account. For information about adding an account in ABM/ASM, see Apple documentation at <https://support.apple.com/guide/apple-business-manager/welcome/web> and ASM at <https://support.apple.com/guide/apple-school-manager/welcome/web>. We recommend the following to avoid extra steps when users enroll:

- Use an email matching the corporate email address when creating a Managed Apple ID.
- Set the user role to **Staff**.
- Have users manually change their password before enrolling. Let users know that we recommend they use the same password as the corporate account.

To dynamically create Managed Apple IDs, configure Citrix Cloud to use AAD as its identity provider. For more information about configuring Citrix Cloud to use AAD, see [Authentication with Azure Active Directory through Citrix Cloud](#). Also, configure federated authentication in ABM/ASM. To learn more about configuring federated authentication in ABM or ASM, see the [Apple Business Manager User Guide](#) and the [Apple School Manager User Guide](#).

When you manually create Managed Apple IDs, you can configure a custom domain to use in place of the default domain. The custom domain you configure replaces the existing domain. For example, your corporate email addresses follow the format `first.last@company.com`, but you want to use `mycompany.website.com` as the domain for the Managed Apple ID instead. When creating the Managed Apple ID on ABM/ASM, the email address becomes `first.last@mycompany.website.com`.

## Add an iOS device manually

If you want to add an iOS device manually, such as for testing purposes, follow these steps.

1. In the Endpoint Management console, click **Manage > Devices**. The **Devices** page appears.

Status	Mode	User name	Device platform	Operating system version
<input type="checkbox"/>	MDM   MAM	[Redacted]	Android	5.0.2
<input type="checkbox"/>	MDM   MAM	[Redacted]	iOS	8.4.1

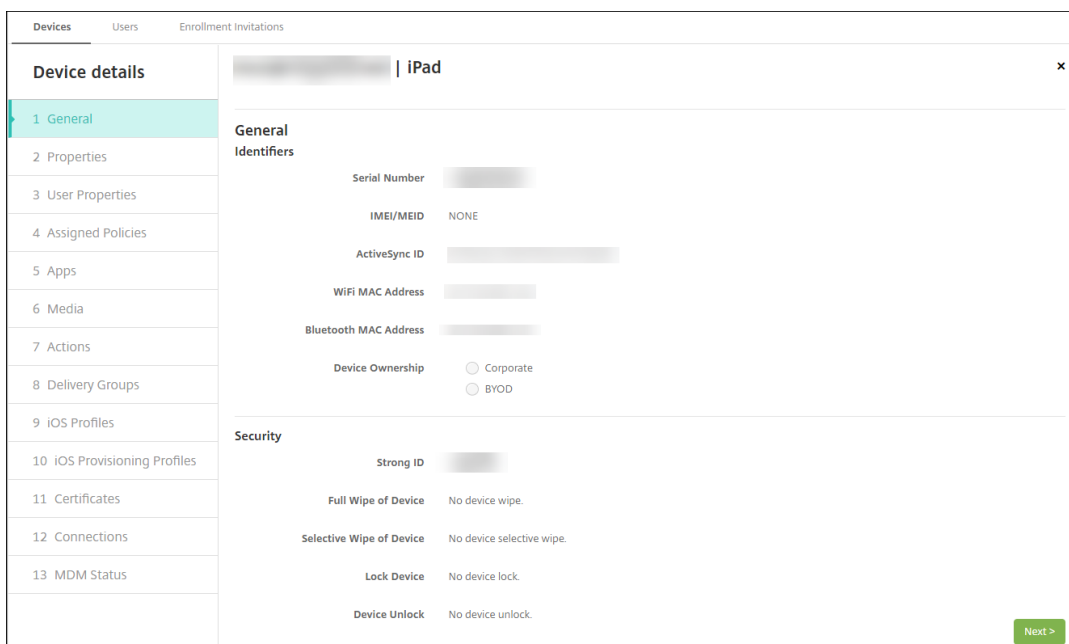
2. Click **Add**. The **Add Device** page appears.

3. Configure these settings:
  - **Select platform:** Click **iOS**.
  - **Serial Number:** Type the device serial number.
4. Click **Add**. The **Devices** table appears with the device added to the bottom of the list. To view and confirm the device details: Choose the device you added and then, in the menu that appears, click **Edit**.

### Note:

When you select the check box next to a device, the options menu appears above the device list. If you click anywhere else in the list, the options menu appears on the right side of the listing.

- LDAP configured
- If using local groups and local users:
  - One or more local groups.
  - Local users assigned to local groups.
  - Delivery groups are associated with local groups.
- If using Active Directory:
  - Delivery groups are associated with Active Directory groups.



5. The **General** page lists device **Identifiers**, such as the serial number and other information for the platform type. For **Device Ownership**, select **Corporate** or **BYOD**.

The **General** page also lists device **Security** properties, such as Strong ID, Lock Device, Activation Lock Bypass, and other information for the platform type. The **Full Wipe of Device** field includes the user PIN code. The user must enter that code after the device is wiped. If the user forgets the code, you can look it up here.

6. The **Properties** page lists the device properties that Endpoint Management provisions. This list shows any device properties included in the provisioning file used to add the device. To add a property, click **Add** and then select a property from the list. For valid values for each property, see the PDF [Device property names and values](#).

When you add a property, it initially appears under the category where you added it. After you click **Next** and then return to the **Properties** page, the property appears in the appropriate list.

To delete a property, hover over the listing and then click the **X** on the right side. Endpoint Management deletes the item immediately.

7. The remaining **Device Details** sections contain summaries for the device.
- **User Properties:** Displays RBAC roles, group memberships, volume purchase accounts, and properties for the user. You can retire a volume purchase account from this page.
  - **Assigned Policies:** Displays the number of deployed, pending, and failed policies. Provides the policy name, type, and last deployed information for each policy. Lets you reset the deployment status to pending and redeploy policies that the user removed.
  - **Apps:** Displays, for the last inventory, the number of installed, pending, and failed app deployments. Provides the app name, identifier, type, and other information. For a descrip-

tion of iOS and macOS inventory keys, such as **HasUpdateAvailable**, see [Mobile Device Management \(MDM\) Protocol](#).

- **Media:** Displays, for the last inventory, the number of deployed, pending, and failed media deployments.
- **Actions:** Displays the number of deployed, pending, and failed actions. Provides the action name and time of the last deployment.
- **Delivery Groups:** Displays the number of successful, pending, and failed delivery groups. For each deployment, provides the delivery group name and deployment time. Select a delivery group to view more detailed information, including status, action, and channel or user.
- **iOS Profiles:** Displays the last iOS profile inventory, including name, type, organization, and description.
- **iOS Provisioning Profiles:** Displays enterprise distribution provisioning profile information, such as the UUID, expiration date, and managed status.
- **Certificates:** Displays, for valid, expired, or revoked certificates, information such as the type, provider, issuer, serial number, and the number of remaining days before expiration.
- **Connections:** Displays the first connection status and the last connection status. Provides for each connection, the user name, penultimate (next to last) authentication time, and last authentication time.
- **MDM Status:** Displays information such as the MDM status, last push time, and last device reply time.

## Configure iOS device policies

Use these policies to configure how Endpoint Management interacts with devices running iOS or iPadOS. This table lists all device policies available for iOS and iPadOS devices.

<a href="#">AirPlay mirroring</a>	<a href="#">AirPrint</a>	<a href="#">APN</a>
<a href="#">App access</a>	<a href="#">App attributes</a>	<a href="#">App configuration</a>
<a href="#">App inventory</a>	<a href="#">App lock</a>	<a href="#">App uninstall</a>
<a href="#">Apps notifications</a>	<a href="#">Calendar (CalDAV)</a>	<a href="#">Cellular</a>
<a href="#">Contacts (CardDAV)</a>	<a href="#">Credentials</a>	<a href="#">Device name</a>
<a href="#">Education configuration</a>	<a href="#">Exchange</a>	<a href="#">Font</a>
<a href="#">Home screen layout</a>	<a href="#">Import iOS &amp; macOS profile</a>	<a href="#">LDAP</a>
<a href="#">Location</a>	<a href="#">Lock screen message</a>	<a href="#">Mail</a>
<a href="#">Managed domains</a>	<a href="#">Maximum resident users</a>	<a href="#">MDM options</a>

---

Network	Network usage	Organization info
OS update	Passcode	Passcode lock grace period
Personal hotspot	Profile removal	Provisioning profile
Provisioning profile removal	Proxy	Restrictions
Roaming	SCEP	SSO account
Store	Subscribed calendars	Terms and conditions
VPN	Wallpaper	Web content filter
Web clip		

---

### Enroll iOS devices

This section shows how users enroll iOS devices (12.2 or later) into Endpoint Management. For more information about the iOS enrollment, watch the following video:

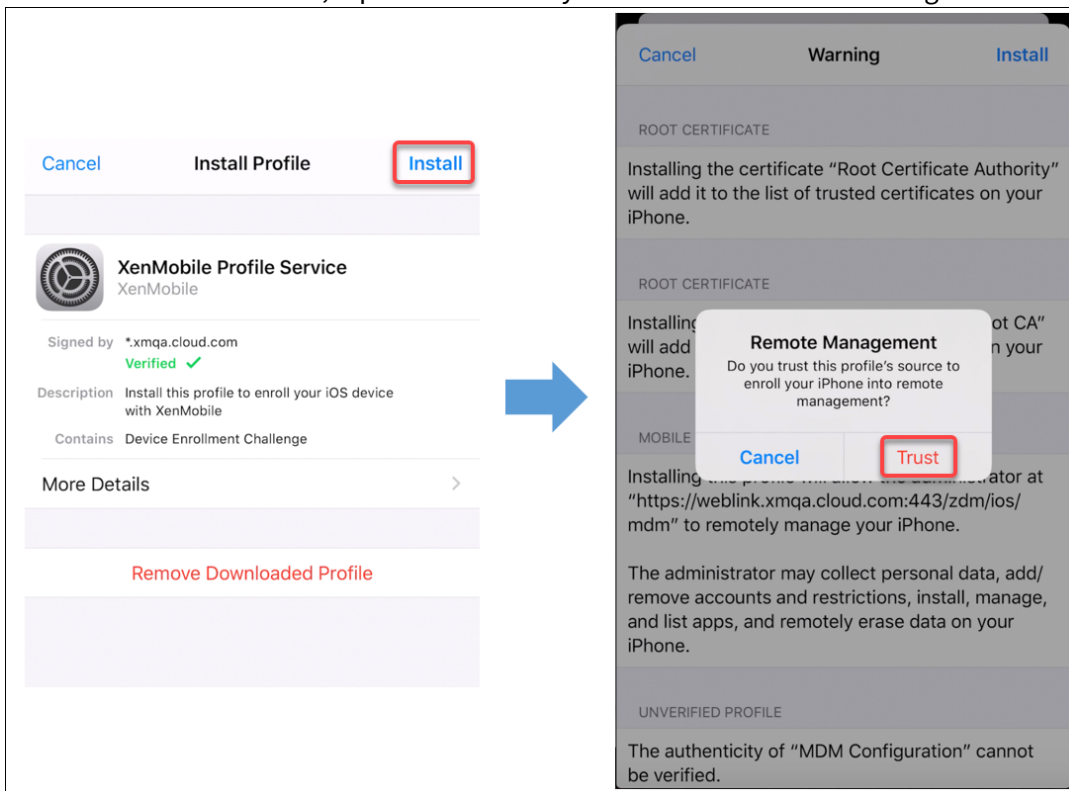


**Enroll using Secure Hub**





1. Go to the Apple store on your iOS device, download the Citrix Secure Hub app, and then tap the app.
2. When prompted to install the app, tap **Next** and then tap **Install**.
3. After Secure Hub installs, tap **Open**.
4. Enter your corporate credentials, such as your Endpoint Management server name, User Principal Name (UPN), or email address. Then, click **Next**.
5. Tap **Yes, Enroll** to enroll your iOS device.
6. A list of the data Endpoint Management collects appears. Click **Next**. An explanation of how an organization uses that data appears. Click **Next**.
7. After you type your credentials, tap **Allow** when prompted, to download the configuration profile. After you download the configuration profile, tap **Close**.
8. In your device settings, install the XenMobile profile.
  - Go to **Settings > General > Profile > XenMobile Profile Service** and tap **Install** to add the profile.
  - In the notification window, tap **Trust** to enroll your device into remote management.



9. Once enrollment succeeds, open Secure Hub. If you are enrolling into MDM+MAM: After your credentials validate, create and confirm your Citrix PIN when prompted.
10. After the workflow completes, the device is enrolled. You can then access the app store to view the apps you can install on your iOS device.

## Security actions

Device enrollment for iOS supports the following security actions. For a description of each security action, see [Security actions](#).

- Activation Lock Bypass
- App Lock
- App Wipe
- ASM Activation Lock
- Certificate Renewal
- Clear Restrictions
- Enable/Disable Lost Mode
- Enable/Disable Tracking
- Full Wipe
- Locate
- Lock
- Ring
- Request/Stop AirPlay Mirroring
- Restart/Shut Down
- Revoke/Authorize
- Selective Wipe
- Unlock

User enrollment for iOS supports the following security actions:

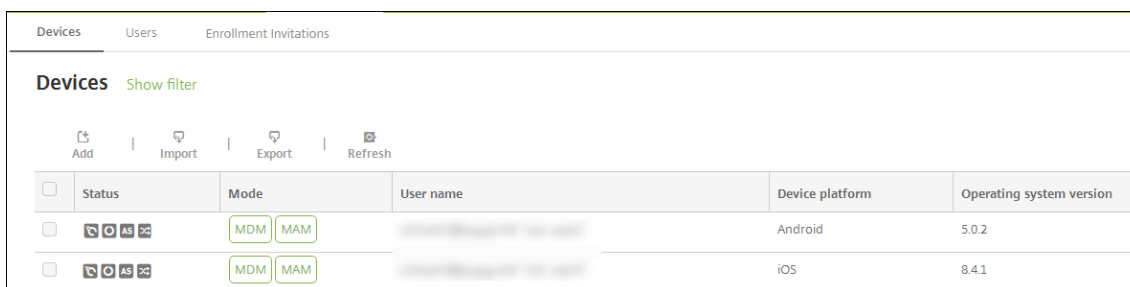
- Revoke
- Lock
- Selective wipe
- Certificate renewal

## Lock iOS devices

You can lock a lost iOS device with an accompanying display of a message and phone number that displays on the device lock screen.

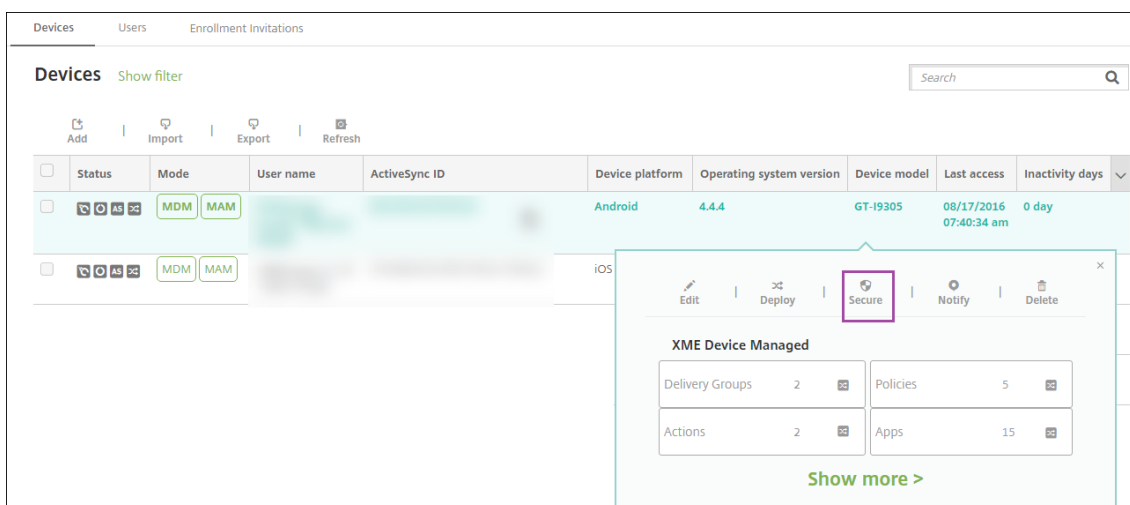
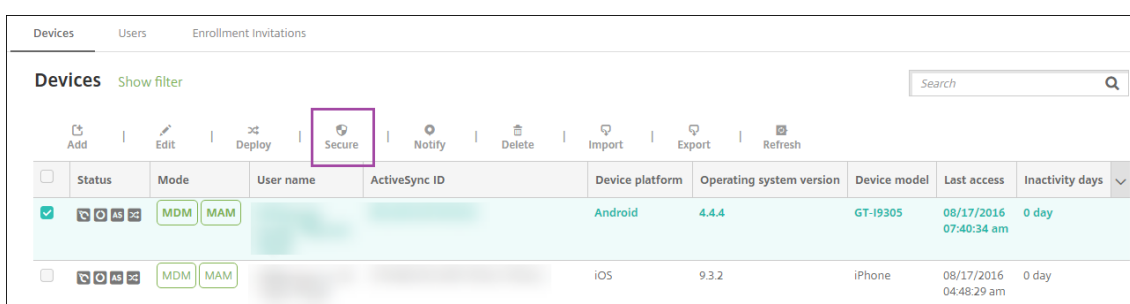
To display a message and phone number on a locked device, set the [Passcode](#) policy to **true** in the Endpoint Management console. Instead users can enable the passcode on the device manually.

1. Click **Manage > Devices**. The **Devices** page appears.

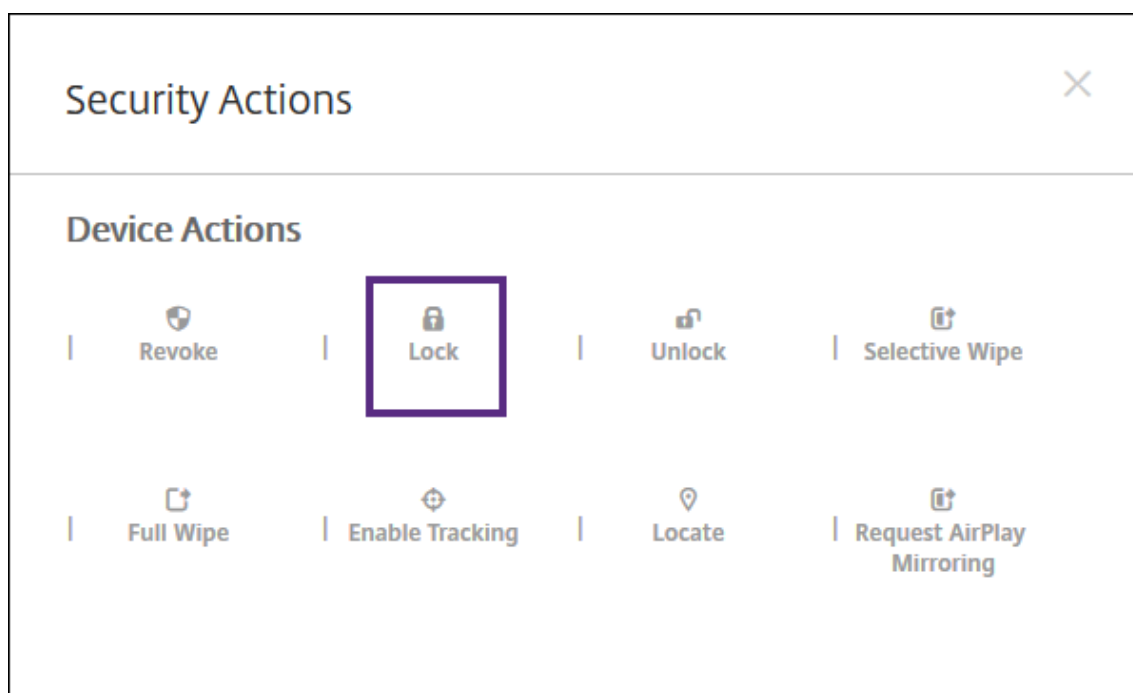


2. Select the iOS device you want to lock.

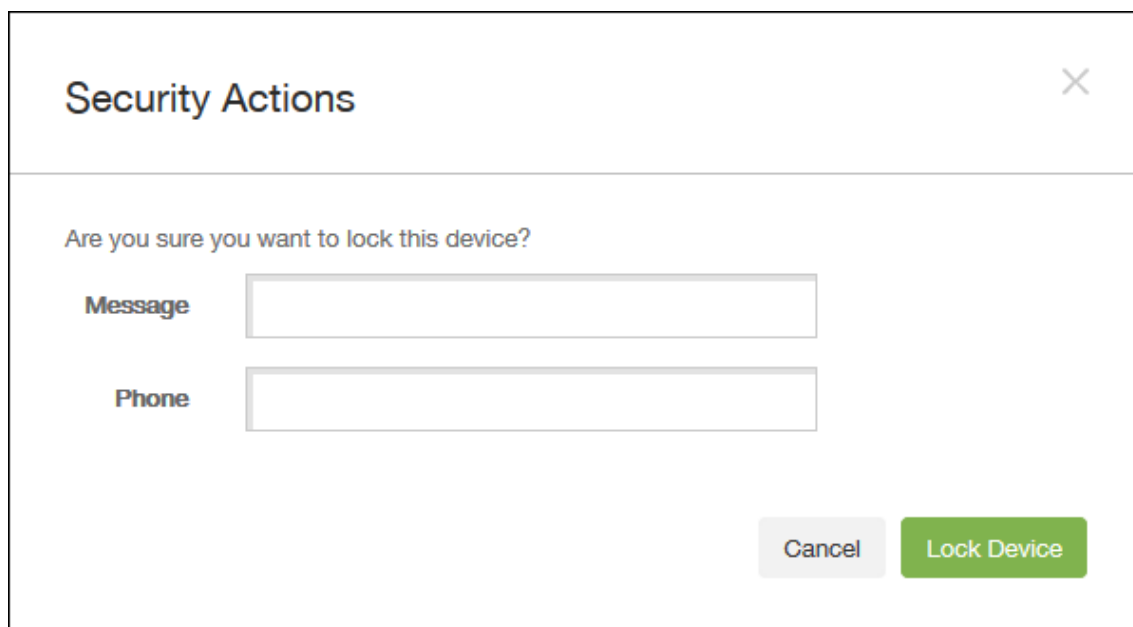
Select the check box next to a device to show the options menu above the device list. Click anywhere else in the list to show the options menu on the right side of the listing.



3. In the options menu, click **Secure**. The **Security Actions** dialog box appears.



4. Click **Lock**. The **Security Actions** confirmation dialog box displays.



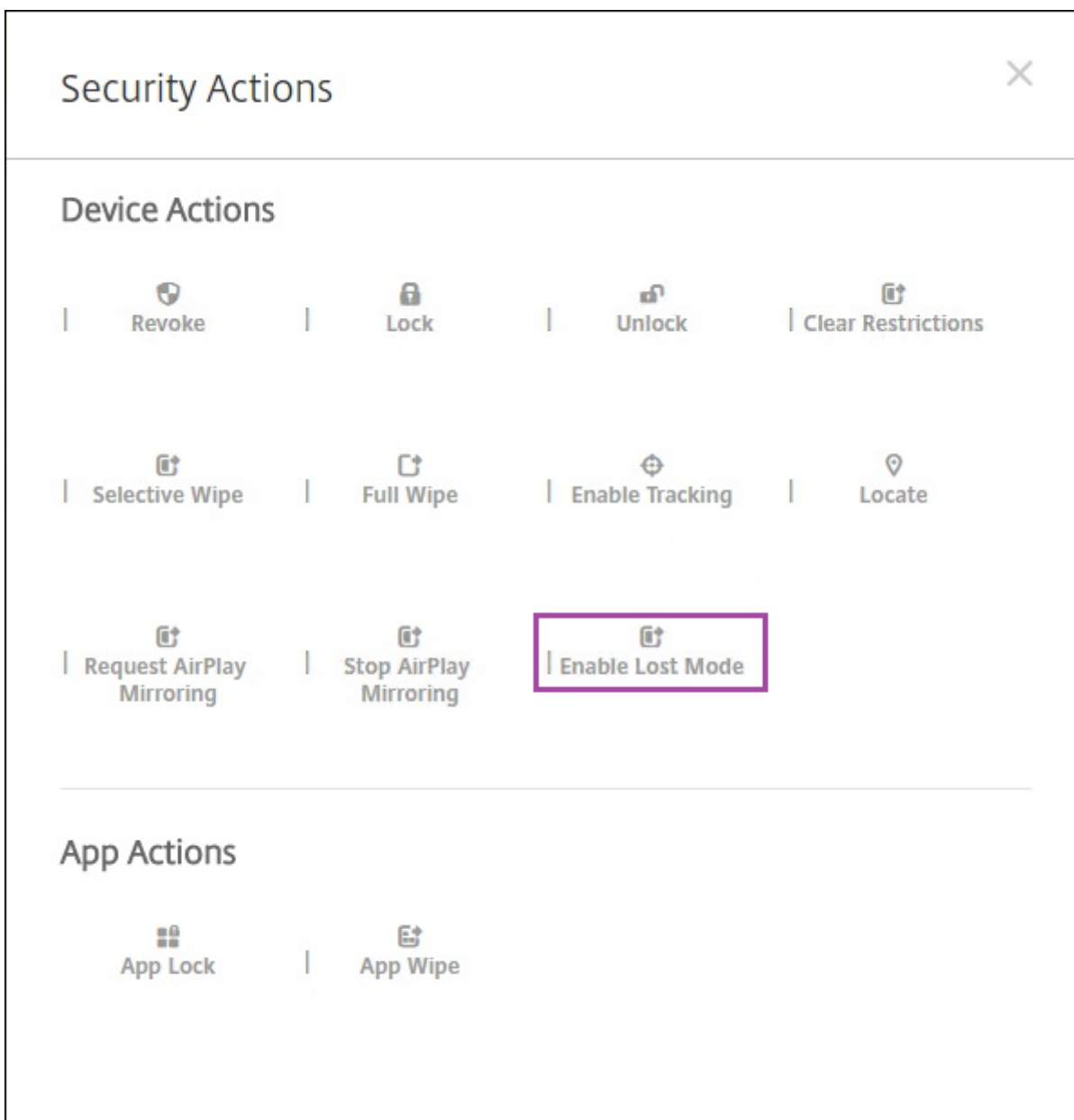
5. Optionally, type a message and phone number that appears on the lock screen of the device.  
iOS appends the words “Lost iPad” to what you type in the **Message** field.  
If you leave the **Message** field empty and provide a phone number, Apple displays the message “Call owner” on the device lock screen.
6. Click **Lock Device**.

### **Put iOS devices in Lost Mode**

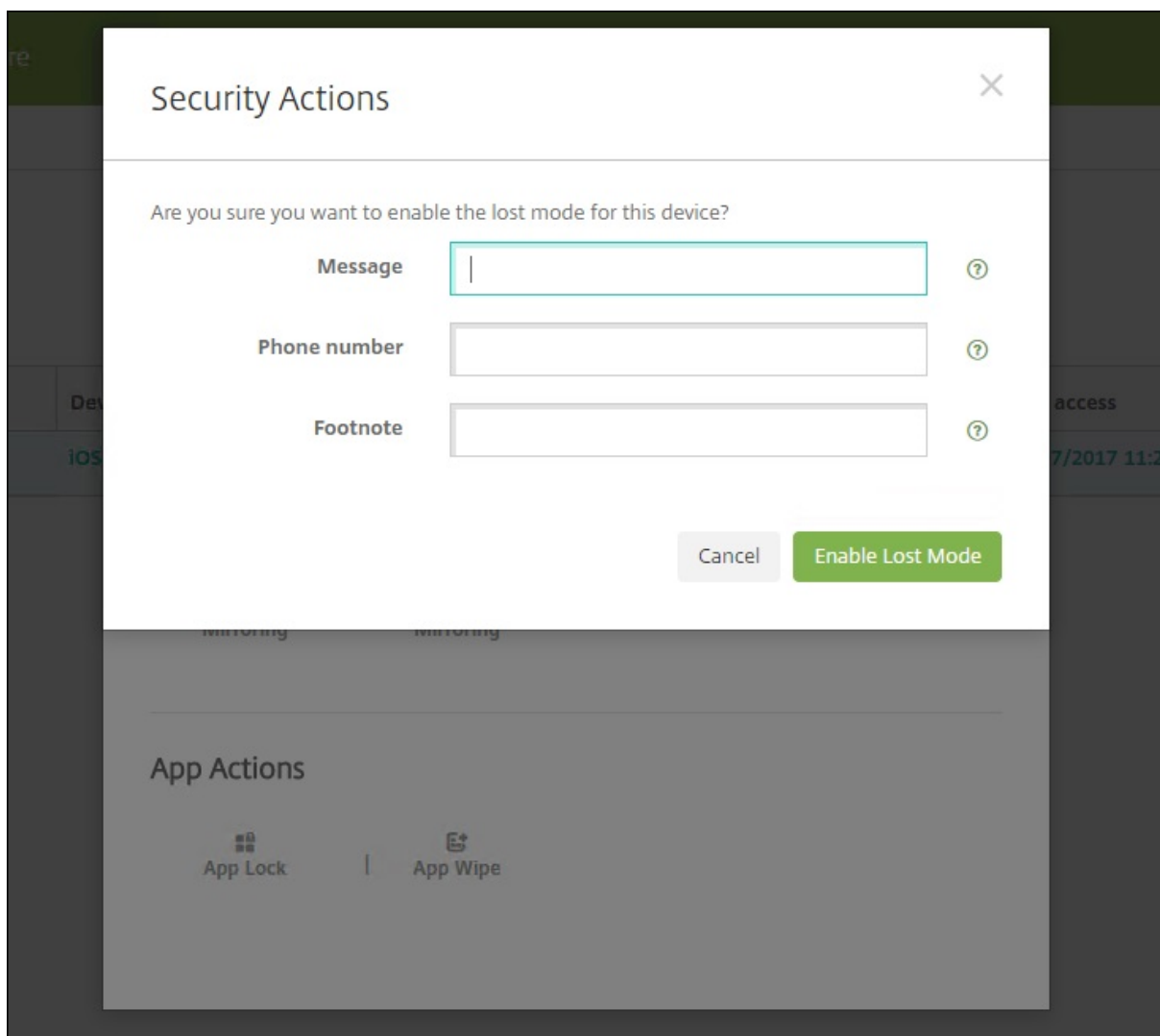
The Endpoint Management Lost Mode device property puts an iOS device in Lost Mode. Unlike Apple Managed Lost Mode, Endpoint Management Lost Mode doesn't require a user to do either of the following actions to enable locating their device: Configure the **Find My iPhone/iPad** setting or enable the Location Services for Citrix Secure Hub.

In Endpoint Management Lost Mode, only Endpoint Management can unlock the device. (In contrast, if you use the Endpoint Management device lock feature, users can unlock the device directly by using a PIN code that you provide.

To enable or disable lost mode: Go to **Manage > Devices**, choose a supervised iOS device, and then click **Secure**. Then, click **Enable Lost Mode** or **Disable Lost Mode**.



If you click **Enable Lost Mode**, type information to appear on the device when it's in lost mode.



Use any of the following methods to check Lost Mode status:

- In the **Security Actions** window, verify if the button is **Disable Lost Mode**.
- From **Manage > Devices**, on the **General** tab under **Security**, see the last Enable Lost Mode or Disable Lost Mode action.

The screenshot shows the 'Device details' page in the Citrix Endpoint Management console. The left sidebar lists various configuration categories, with '1 General' selected. The main content area displays a list of device settings, including 'Device Shutdown', 'Device locate', 'Device Enable Tracking', 'Device Disown', 'DEP Activation Lock', 'Activation Lock Bypass', 'Device Clear Restrictions', 'Device App Wipe', 'Device App Lock', 'Request AirPlay Mirroring', and 'Stop AirPlay Mirroring'. The 'Enable Lost Mode' and 'Disable Lost Mode' settings are highlighted with a red box, both showing the value 'No lost mode enabled.'. A 'Next >' button is visible in the bottom right corner.

- From **Manage > Devices**, on the **Properties** tab, verify that the value of the **MDM lost mode enabled** setting is correct.

The screenshot shows the 'Device details' page in the Citrix Endpoint Management console, with the '2 Properties' tab selected in the left sidebar. The main content area displays a list of device properties, including 'Activation lock enabled', 'Hardware encryption capabilities', 'Internal storage encrypted', 'Jailbroken/Rooted', 'MDM lost mode enabled', 'Passcode compliant', 'Passcode compliant with configuration', 'Passcode present', and 'Supervised'. The 'MDM lost mode enabled' setting is highlighted with a red box, showing the value 'No'. Below this, there are sections for 'Storage space' and 'System information'. A 'Back' button and a 'Next >' button are visible in the bottom right corner.

If you enable Endpoint Management Lost Mode on an iOS device, the Endpoint Management console also changes as follows:



- In **Configure > Actions**, the **Actions** list doesn't include these automated actions: **Revoke the device**, **Selectively wipe the device**, and **Completely wipe the device**.
- In **Manage > Devices**, the **Security Actions** list no longer includes the **Revoke** and **Selective Wipe** device actions. You can still use a security action to perform a **Full Wipe** action, as needed.

iOS appends the words "Lost iPad" to what you type in the **Message** in the **Security Actions** screen.

If you leave the **Message** empty and provide a phone number, Apple shows the message "Call owner" on the device lock screen.

### **Bypass an iOS activation lock**

Activation Lock is a feature of Find My iPhone/iPad that prevents reactivation of a lost or stolen supervised device. Activation Lock requires the user Apple ID and password before anyone can perform these actions: Turn off Find My iPhone/iPad, erase the device, or reactivate the device. For the devices that your organization owns, bypassing an Activation Lock is necessary to, for example, reset or reallocate devices.

To enable Activation Lock, you configure and deploy the Endpoint Management MDM Options device policy. You can then manage a device from the Endpoint Management console without the Apple credentials of the user. To bypass the Apple credential requirement of an Activation Lock, issue the Activation Lock Bypass security action from the Endpoint Management console.

For example, if the user returns a lost phone or to set up the device before or after a Full Wipe: When the phone prompts for the Apple App Store account credential, bypass that step by issuing the Activation Lock Bypass security action.

### **Device requirements for activation lock bypass**

- Supervised through Apple Configurator or Apple Deployment Program
- Configured with an iCloud account
- Find My iPhone/iPad enabled
- Enrolled in Endpoint Management
- MDM Options device policy, with activation lock enabled, is deployed to devices

To bypass an activation lock before issuing a Full Wipe of a device:

1. Go to **Manage > Devices**, select the device, click **Secure**, and then click **Activation Lock Bypass**.
2. Wipe the device. The activation lock screen doesn't appear during device setup.

To bypass an activation lock after issuing a Full Wipe of a device:

1. Reset or wipe the device. The activation lock screen appears during device setup.
2. Go to **Manage > Devices**, select the device, click **Secure**, and then click **Activation Lock Bypass**.
3. Tap the Back button on the device. The home screen appears.

Keep in mind the following:

- Advise your users not to turn off Find My iPhone/iPad. Don't perform a full wipe from the device. In either of those cases, the user is prompted to enter the iCloud account password. After account validation, the user won't see an Activate iPhone/iPad screen after erasing all content and settings.
- For a device that has a generated Activation lock bypass code and has the Activation lock enabled: If you can't bypass the Activate iPhone/iPad page after a Full Wipe, you don't need to delete the device from Endpoint Management. Either you or the user can contact Apple support to unblock the device directly.
- During a hardware inventory, Endpoint Management queries a device for an Activation lock bypass code. If a bypass code is available, the device sends it to Endpoint Management. Then, to remove the bypass code from the device, send the Activation Lock Bypass security action from the Endpoint Management console. At that point, Endpoint Management and Apple have the bypass code required to unblock the device.
- The Activation Lock Bypass security action relies on the availability of an Apple service. If the action doesn't work, you can unblock a device using one of the following ways:
  - On the device, manually enter the credentials of the iCloud account.
  - Leave the user name field empty and type the bypass code in the password field. To look up the bypass code, go to **Manage > Devices**, select the device, click **Edit**, and click **Properties**. The **Activation lock bypass code** is under **Security information**.

## macOS

October 13, 2021

To manage macOS devices in Endpoint Management, you set up an Apple Push Notification service (APNs) certificate from Apple. For information, see [APNs certificates](#).

Endpoint Management enrolls macOS devices into MDM. Endpoint Management supports the following enrollment authentication types for macOS devices in MDM.

- Domain
- Domain plus one-time password
- Invitation URL plus one-time password

### Requirements for trusted certificates in macOS 15:

Apple has new requirements for TLS server certificates. Verify that all certificates follow the new Apple requirements. See the Apple publication, <https://support.apple.com/en-us/HT210176>. For help with managing certificates, see [Upload certificates](#).

A general workflow for starting macOS device management is as follows:

1. Complete the onboarding process. See [Onboarding and resource setup](#) and [Prepare to enroll devices and deliver resources](#).
2. Choose and configure an enrollment method. See [Supported enrollment methods](#).
3. Configure macOS device policies.
4. Enroll macOS devices.
5. Set up device and app security actions. See [Security actions](#).

For supported operating systems, see [Supported device operating systems](#).

### Apple host names that must remain open

Some Apple host names must remain open to ensure proper operation of iOS, macOS, and Apple App Store. Blocking those host names can affect the installation, update, and proper operation of the following: iOS, iOS apps, MDM operation, and device and app enrollment. For more information, see <https://support.apple.com/en-us/HT201999>.

### Supported enrollment methods

The following table lists the enrollment methods that Endpoint Management supports for macOS devices:

Method	Supported
Apple Deployment Program	Yes
Apple School Manager	Yes
Apple Configurator	No
Manual enrollment	Yes
Enrollment invitations	Yes

Apple has device enrollment programs for business and education accounts. For business accounts, you enroll in the Apple Deployment Program to use the Apple Deployment Program for device enrollment and management in Endpoint Management. That program is for iOS, macOS, and Apple TV devices. See [Deploy devices through Apple Deployment Program](#).

For education accounts, you create an Apple School Manager account. Apple School Manager unifies the Deployment Program and volume purchase. Apple School Manager is a type of Education Apple Deployment Program. See [Integrate with Apple Education features](#).

You can use the Apple Deployment Program to bulk enroll iOS, macOS, and Apple TV devices. You can purchase those devices directly from Apple, a participating Apple Authorized Reseller, or a carrier.

## Configure macOS device policies

Use these policies to configure how Endpoint Management interacts with devices running macOS. This table lists all device policies available for macOS devices.

<a href="#">AirPlay mirroring</a>	<a href="#">App inventory</a>	<a href="#">App uninstall</a>
<a href="#">Calendar (CalDAV)</a>	<a href="#">Contacts (CardDAV)</a>	<a href="#">Credentials</a>
<a href="#">Device name</a>	<a href="#">Exchange</a>	<a href="#">FileVault</a>
<a href="#">Firewall</a>	<a href="#">Font</a>	<a href="#">Import iOS &amp; macOS profile</a>
<a href="#">LDAP</a>	<a href="#">Mail</a>	<a href="#">Network</a>
<a href="#">OS update</a>	<a href="#">Passcode</a>	<a href="#">Profile removal</a>
<a href="#">Restrictions</a>	<a href="#">SCEP</a>	<a href="#">VPN</a>
<a href="#">Web clip</a>		

## Enroll macOS devices

Endpoint Management provides two methods to enroll devices that are running macOS. Both methods enable macOS users to enroll over the air, directly from their devices.

- **Send users an enrollment invitation:** This enrollment method enables you to set any of the following enrollment security modes for macOS devices:
  - User name + password
  - User name + PIN
  - Two-factor authentication

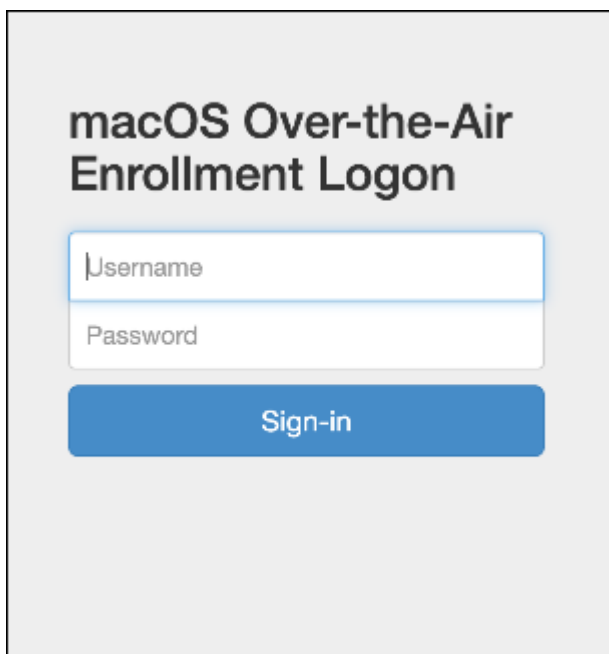
When the user follows the instructions in the enrollment invitation, a sign-on screen with the user name filled in appears.

- **Send users an enrollment link:** This enrollment method for macOS devices sends users an enrollment link, which they can open in Safari or Chrome browsers. A user then enrolls by providing their user name and password.

To prevent the use of an enrollment link for macOS devices, set the server property, **Enable macOS OTAE** to **false**. As a result, macOS users can enroll only by using an enrollment invitation.

### Send macOS users an enrollment invitation

1. Add an invitation for macOS user enrollment. See [Enrollment invitations](#).
2. After users receive the invitation and click the link, the following screen appears in the Safari browser. Endpoint Management fills in the user name. If you chose **Two Factor** for the enrollment security mode, another field appears.



3. Users install certificates as necessary. Whether users see the prompt to install certificates depends on whether you configured the following for macOS: A publicly trusted SSL certificate and a publicly trusted digital signing certificate. For information about certificates, see [Certificates and authentication](#).
4. Users provide the requested credentials.

The Mac device policies install. You can now start managing macOS devices with Endpoint Management just as you manage mobile devices.

### Send macOS users an installation link

1. Send the enrollment link `https://serverFQDN:8443/instanceName/macos/otae`, which users can open in Safari or Chrome browsers.
  - **serverFQDN** is the fully qualified domain name (FQDN) of the server running Endpoint Management.
  - Port **8443** is the default secure port. If you configured a different port, use that port instead of 8443.
  - The **instanceName**, often shown as `zdm`, is the name specified during server installation.

For more information about sending installation links, see [To send an installation link](#).

2. Users install certificates as necessary. If you configured a publicly trusted SSL certificate and digital signing certificate for iOS and macOS, users see the prompt to install certificates. For information about certificates, see [Certificates and authentication](#).
3. Users sign on to their Macs.

The Mac device policies install. You can now start managing macOS devices with Endpoint Management just as you manage mobile devices.

## Security actions

macOS supports the following security actions. For a description of each security action, see [Security actions](#).

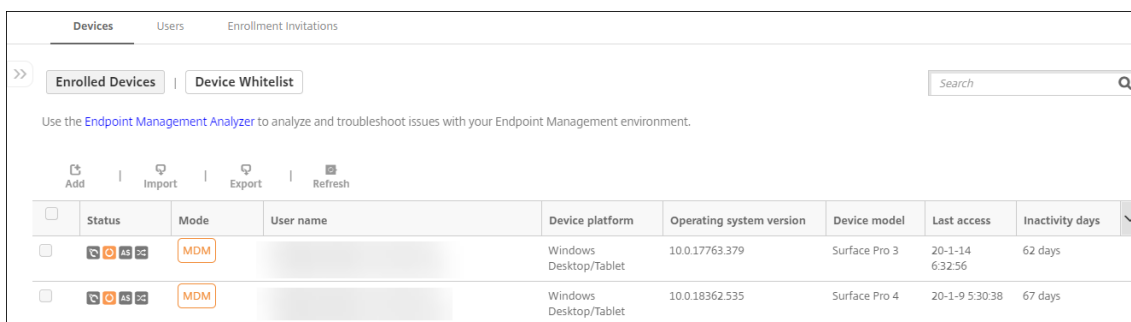
Revoke	Lock	Selective Wipe
Full Wipe	Certificate renewal	Rotate personal recovery key

## Lock macOS devices

You can remotely lock a lost macOS device. Endpoint Management locks the device. It then generates a PIN code and sets it in the device. To access the device, the user types the PIN code. Use **Cancel Lock** to remove the lock from the Endpoint Management console.

You can use the [Passcode](#) device policy to configure more settings associated with the PIN code. For more information, see [macOS settings](#).

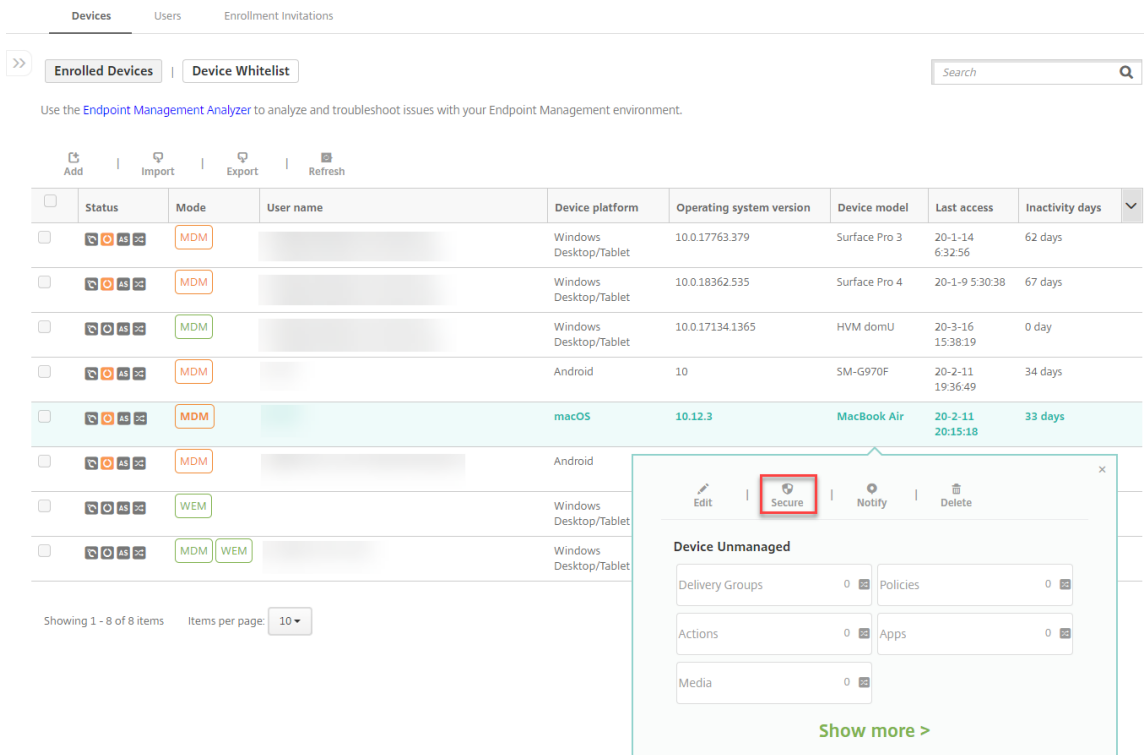
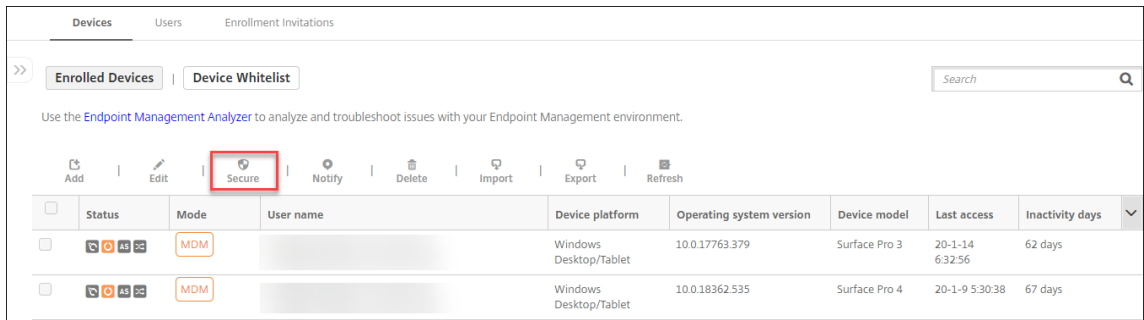
1. Click **Manage > Devices**. The **Devices** page appears.



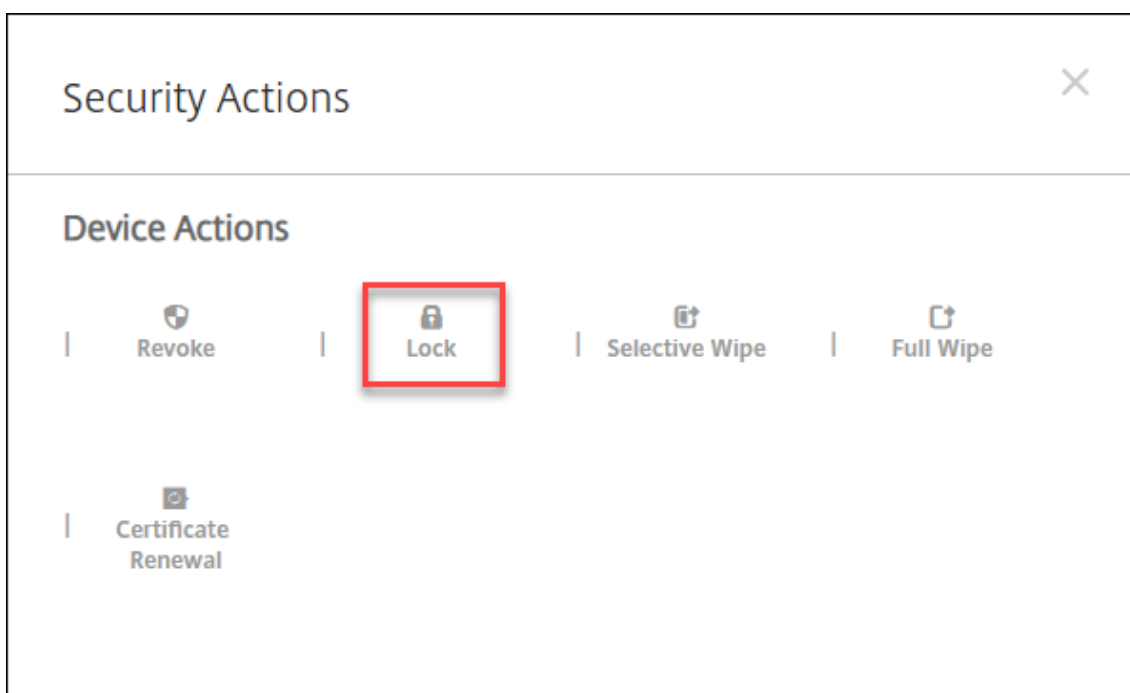
2. Select the macOS device you want to lock.

Select the check box next to a device to show the options menu above the device list. You can also click anywhere else on a listed item to show the options menu on the right side of the list.

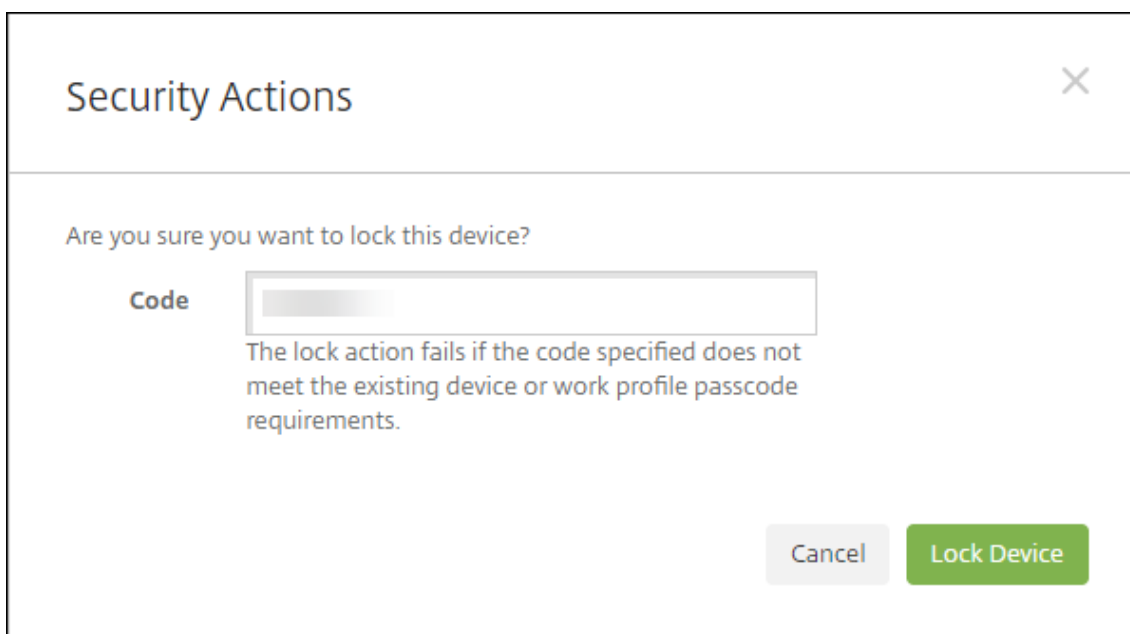
# Citrix Endpoint Management



3. In the options menu, click **Secure**. The **Security Actions** dialog box appears.



4. Click **Lock**. The **Security Actions** confirmation dialog box displays.



5. Click **Lock Device**.

**Important:**

You can also specify a passcode instead of using the code that Endpoint Management generates. The lock action fails if the code specified does not meet the code requirements of the device or existing work profile.



## Bootstrap token

A bootstrap token assists with granting the SecureToken macOS attribute to accounts when you sign on to a macOS device. SecureToken passes down from one trusted account to another. SecureToken-enabled accounts can perform cryptographic operations on the device. Without the bootstrap token, you need to follow complex workflows to create accounts on that device before adding individual user accounts.

Endpoint Management supports escrowing bootstrap tokens for macOS devices that are enrolled through Apple Deployment Program. You use the Apple Deployment Program to enroll macOS devices that you purchase directly from Apple, a participating Apple Authorized Reseller, or a carrier. For information about enrolling in the Apple Deployment Program, see [Deploy devices through Apple Deployment Program](#).

Bootstrap tokens are generated during the Setup Assistant workflow. Specifically, they are generated during local user account creation. The Setup Assistant runs the first time users start their devices. The tokens are saved in the Endpoint Management database and not visible to you and end users. Deleting the devices from your Endpoint Management site deletes the tokens. Performing a factory reset doesn't delete them.

Prerequisites:

- macOS 11.0 or later
- macOS devices that have the Apple T2 Security Chip
- macOS devices enrolled through Apple Deployment Program

One benefit of escrowing bootstrap tokens with Endpoint Management is that remote accounts can be enabled for FileVault and able to unlock the FileVault volume. For information about FileVault, see [FileVault device policy](#).

## Deploy devices through the Apple Deployment Programs

September 10, 2021

The Apple Deployment Programs (ADPs) let you automatically enroll Apple devices in Endpoint Management without having to touch or prepare the devices before users get them. After a user unboxes and activates the device, the device automatically enrolls in Endpoint Management, and all management settings, apps, and books are ready for the user.

The ADPs include Apple Business Manager (ABM) for business organizations and Apple School Manager (ASM) for educational organizations. ABM and ASM are available for iOS, iPadOS, macOS, and tvOS devices. For more information about device eligibility, see [Apple Business Manager User Guide](#) and [Apple School Manager User Guide](#).

**Note:**

ABM and ASM combine the previous Device Enroll Program and Volume Purchase Program from Apple.

This article walks you through the general deployment workflow with ABM or ASM:

1. [Enroll in ABM or ASM](#)
2. [Connect your ABM or ASM account to Endpoint Management](#)
3. [Order devices](#)
4. [Assign devices to Endpoint Management](#)
5. [Buy content in volume and synchronize it with Endpoint Management](#)
6. [Configure deployment rules for device policies and apps](#)
7. Add delivery groups that contain users and resources assigned to them

After you complete this deployment process, the devices are ready to be unboxed and activated for an automated device enrollment.

## Prerequisites

Open required ports for connectivity between Endpoint Management and Apple. For more information, see [Port requirements](#).

## Enroll in ABM or ASM

To begin deploying devices in Apple, enroll in ABM or ASM.

ABM and ASM are available for organizations and not individuals. You must provide many organization details and information to create an account. It might take time to request and receive approval for accounts.

### Enroll in Apple Business Manager

To enroll in ABM, go to [business.apple.com](https://business.apple.com). Click **Enroll now** to apply for a new account.

Best practice is to use an email address for your organization, such as [deployment@company.com](mailto:deployment@company.com). The enrollment process might take a few days. After you receive your logon credentials, follow the steps provided in ABM to create an account.

### Enroll in Apple School Manager

To create your ASM account, go to [Apple School Manager](#) and follow the instructions to enroll. The first time that you log in to ASM, the Setup Assistant opens.

- For information about ASM prerequisites, the Setup Assistant, and management tasks, see the [Apple School Manager User Guide](#).
- When setting up an ASM user account, use a domain name that differs from the domain name for Active Directory. For example, prefix the domain name for ASM with something like `apple.id`.
- When you connect ASM to your roster data, ASM creates Managed Apple IDs for instructors and students. Your roster data includes instructors, students, and classes. For information about adding roster data to ASM, see the Apple School Manager User Guide, linked earlier in this list.
- You can customize the Managed Apple ID format for your institution, as described in the Apple School Manager User Guide, linked earlier in this list.

**Important:**

Don't change Managed Apple IDs after you import ASM information into Endpoint Management.

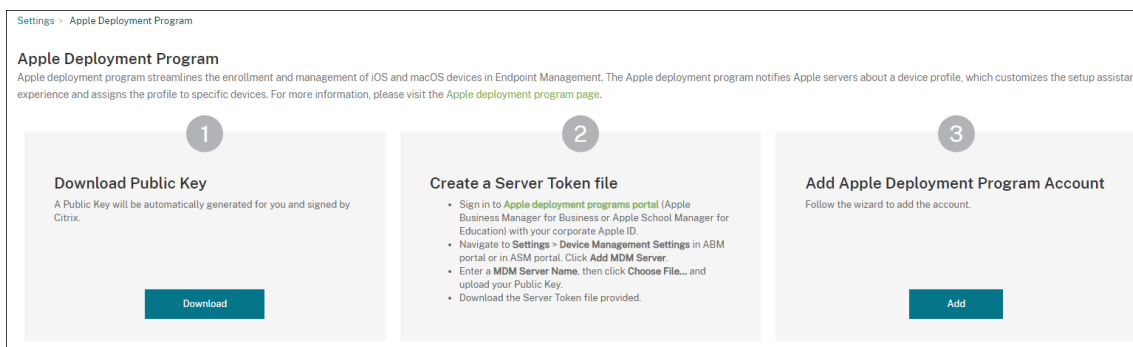
- If you purchased devices through resellers or carriers, link those devices to ASM. For information, see the Apple School Manager User Guide, linked earlier in this list.

## Connect your ABM or ASM account to Endpoint Management

After you create your ABM or ASM account, connect it with your Endpoint Management server deployment.

### Step 1: Download a public key from your Endpoint Management server

1. In the Endpoint Management console, go to **Settings > Apple Deployment Programs**.



2. Under **Download Public Key**, click **Download**.

### Step 2: Create and download a server token file from your Apple account

1. Sign in to [Apple Business Manager](#) or [Apple School Manager](#) using an administrator or device enrollment manager account.

2. At the bottom of the sidebar, click **Settings** and then click **Device Management Settings > Add MDM Server**.
3. In the **MDM Server Name** setting, type a name for the Endpoint Management server. The server name that you type is for your reference. It's not the server URL or name.
4. Under **Upload Public Key**, click **Choose File**. Upload the public key that you downloaded from Endpoint Management and then save the changes.
5. Click **Download Token** to download the server token file to your computer.

You upload the server token file when adding the ABM or ASM account to Endpoint Management. Your token information appears in the Endpoint Management console after you import the token file.

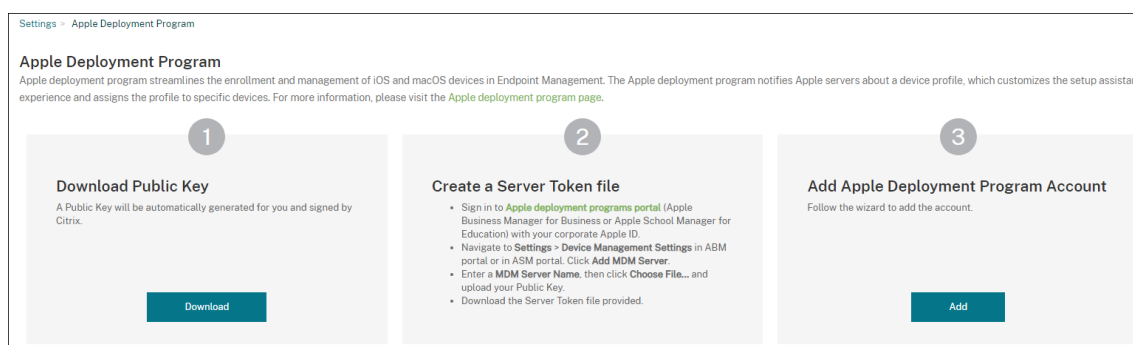
6. Under **Default Device Assignment**, click **Change**. Choose how you want to assign devices and then provide the information requested. For more information, see the [ABM User Guide](#) or [Apple School Manager User Guide](#).

### Step 3: Add your account to Endpoint Management

You can add multiple ABM or ASM accounts to Endpoint Management. This feature enables you to use different enrollment settings and setup assistant options by country, department, and so on. You then associate ABM or ASM accounts with different device policies.

For example, you might centralize all of your ABM or ASM accounts from different countries on the same Endpoint Management server to import and supervise all ABM or ASM devices. You first customize enrollment settings and setup assistant options per department, organizational hierarchy, or other structure. You then configure policies to provide appropriate functionality across your organization and let users receive the appropriate assistance.

1. In the Endpoint Management console, go to **Settings > Apple Deployment Program** and, under **Add Apple Deployment Program Account**, click **Add**.



2. In the **Server Tokens** page, specify your server token file and then click **Upload**.

<p><b>Apple Deployment Program Account</b></p> <ul style="list-style-type: none"> <li>1 Server Tokens</li> <li>2 Account Info</li> <li>3 iOS settings</li> <li>iOS</li> <li>macOS</li> <li>Apple TV</li> <li>4 Setup Assistant Options</li> <li>iOS</li> <li>macOS</li> <li>Apple TV</li> </ul>	<p><b>Server Tokens</b></p> <p>Upload the Server Token file that you downloaded from Apple Business Manager portal or Apple School Manager portal.</p> <p>Select Server Token file * <input type="text"/> <input type="button" value="Upload"/></p> <p>Consumer key <input type="text"/></p> <p>Consumer secret <input type="text"/></p> <p>Access token <input type="text"/></p> <p>Access secret <input type="text"/></p> <p>Access token expiration 7/7/22 4:56:36 pm</p> <p>Server name wj.staging.depidp61</p> <p>Server UUID <input type="text"/></p> <p>Apple admin ID <input type="text"/></p> <p>Organization ID <input type="text"/></p> <p>Organization name <input type="text"/></p> <p>Organization type Business</p> <p>Organization version v2</p> <p>Organization email <input type="text"/></p>
---	--

Your server token information appears.

3. In the **Account Info** page, specify these settings:

<p><b>Apple Deployment Program Account</b></p> <ul style="list-style-type: none"> <li>1 Server Tokens</li> <li>2 Account Info</li> <li>3 iOS settings</li> <li>iOS</li> <li>macOS</li> <li>Apple TV</li> <li>4 Setup Assistant Options</li> <li>iOS</li> <li>macOS</li> <li>Apple TV</li> </ul>	<p><b>Account Info</b></p> <p>Specify your Apple deployment program account information.</p> <p>Apple deployment program account name * <input type="text"/></p> <p>Business/Education unit * <input type="text"/></p> <p>Unique service ID <input type="text"/></p> <p>Support phone number * <input type="text"/></p> <p>Support email address <input type="text"/></p>
---	---

- **Apple Deployment Program account name:** A unique descriptive name for this ADP account, identifying how you organize ADP accounts, such as by country or organizational hierarchy.
- **Business/Education unit:** The business unit or department to which the device is assigned. This field is required.
- **Unique service ID:** An optional unique ID to help you further identify the account.
- **Support phone number:** A support phone number that users call for help during setup. This field is required.

- **Support email address:** An optional support email address available to end users.
- **Education suffix:** For ASM accounts. Type the suffix assigned to devices enrolled through this account.

4. In **iOS Settings**, specify these settings:

Enrollment settings:

- **Require device enrollment:** Whether to require users to enroll their devices. The default is **On**.
- **Require credentials for device enrollment:** Whether to require users to enter their credentials during ABM and ASM setup. We recommend that you require all users to enter their credentials during device enrollment, allowing only authorized users to enroll devices. The default is **On**.

When you enable ABM or ASM before first-time setup and you don't select this option, Endpoint Management creates the ABM or ASM components. This creation includes components such as user, Secure Hub, software inventory, and deployment group. If you select this option, Endpoint Management doesn't create the components. As a result, if you later clear this option, users who haven't entered their credentials can't enroll in ABM or ASM because these components don't exist. To add ABM or ASM components, in that case, disable and then enable the ABM or ASM account.

- **Wait for configuration to complete setup:** Whether to require users' devices to remain in Setup Assistant mode until all MDM resources deploy to the device. This setting is available for devices in supervised mode. The default is **Off**.
- Apple documentation states that the following commands may not work while a device is in Setup Assistant mode:

- InviteToProgram

- InstallApplication
- ApplyRedemptionCode
- InstallMedia
- RequestMirroring
- DeviceLock

Device settings:

- **Supervised mode:** Set to **On** if you are using the Apple Configurator to manage enrolled devices or when **Wait for configuration to complete setup** is enabled. The default is **On**. For details on placing an iOS device in supervised mode, see [Deploy devices using Apple Configurator 2](#).
- **Allow enrollment profile removal:** Whether to allow devices to use a profile that you can remove remotely. The default is **Off**.
- **Allow device pairing:** Whether you can manage enrolled devices through Apple Music and the Apple Configurator. The default is **Off**.

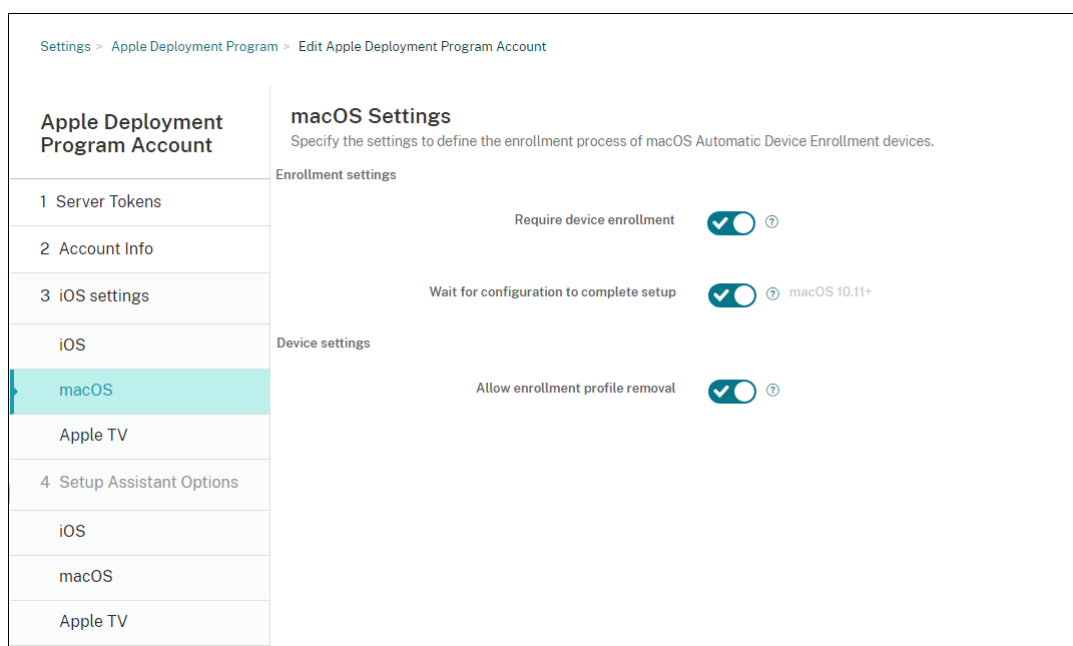
Supervision Identities

If you use the GroundControl tool, you can add a certificate to do the following:

- Override pairing restrictions to avoid the “Trust this host” prompt.
- Escalate managed device actions over USB to perform activities such as profile installation without user interaction. Doing so allows GroundControl to enable single app mode and device lock for checkout.
- Restore a backup to ABM or ASM devices.

For more information on GroundControl, see [The GroundControl website](#).

5. In **macOS Settings**, specify these settings:



Enrollment settings:

- **Require device enrollment:** Whether to require users to enroll their devices. The default is **On**.
- **Wait for configuration to complete setup:** If **On**, the macOS device doesn't continue in the setup assistant until the MDM resource passcode gets deployed to the device. That deployment occurs before the creation of the local account. This setting is available for macOS 10.11 and higher devices. The default is **Off**.

Device settings:

- **Allow enrollment profile removal:** Whether to allow devices to use a profile that you can remove remotely. The default is **Off**.

6. In **Apple TV Settings**, specify these settings:

- **Require device enrollment:** Prevents users from skipping enrollment.
- **Require Credentials for device enrollment:** Challenges for credentials during enrollment. When this setting is off, Apple TV gets enrolled as the default "Device Enrollment Program user".
- **Wait for configuration to complete setup:** The device waits in the **Setup Assistant** screen until all resources deploy.
- **Supervised mode:** Gives more capability to the administrator while configuring restrictions.
- **Allow enrollment profile removal:** Allows users to remove the enrollment profiles.
- **Allow device pairing:** Allows devices enrolled through the Device Enrollment Program to be managed through Apple tools, such as the Apple App Store and the Apple Configurator.



Apple Deployment Program Account	Apple TV Settings
	Specify the settings to define the enrollment process of Apple TV Automatic Device Enrollment devices.
1 Server Tokens	Enrollment settings
2 Account Info	
3 iOS settings	
iOS	
macOS	Device settings
Apple TV	
4 Setup Assistant Options	
iOS	
macOS	
Apple TV	

Require device enrollment  ?

Require credentials for device enrollment  ?

Wait for configuration to complete setup  x ?

Supervised mode  ?

Allow enrollment profile removal  x ?

Allow device pairing  x ?

7. In **iOS Setup Assistant Options**, select the steps that the iOS Setup Assistant skips when users start their devices the first time. When a screen is skipped, the related feature uses default settings. Users can configure the skipped features after setup completes unless you restrict access to those features completely. For more information about restricting access to features, see [Restrictions device policy](#). The default for all items is cleared. The following descriptions explain what occurs when a setting is selected.

Apple Deployment Program Account	iOS Setup Assistant Options
	Select the Setup Assistant items that users won't see when they start their iOS Automatic Device Enrollment devices for the first time.
1 Server Tokens	Skip setup
2 Account Info	
3 iOS settings	
iOS	
macOS	
Apple TV	
4 Setup Assistant Options	
iOS	
macOS	
Apple TV	

Location services

Touch ID iOS 8.0+

Passcode lock

Set up as new or restore

Move from Android iOS 9.0+

Apple ID

Terms and conditions

Apple Pay iOS 8.0+

Siri

App analytics

Display zoom iOS 8.0+

True Tone iOS 10.0+

Home button iOS 10.0+

New feature highlights iOS 11.0+

Privacy iOS 11.3+

Software update iOS 12.0+

Screen Time iOS 12.0+

SIM setup iOS 12.0+

iMessage & FaceTime iOS 12.0+

Appearance iOS 13.0+

Welcome iOS 13.0+

Restore completed iOS 14.0+

- **Location services:** Prevents users from setting up the location service on the device.
- **Touch ID:** Prevents users from setting up Touch ID or Face ID on iOS devices.

- **Passcode lock:** Prevents users from setting up a passcode for the device. If no passcode exists, users can't use Touch ID or Apple Pay.
- **Set up as new or restore:** Prevents users from setting up the device as new or from an iCloud or Apple App Store backup.
- **Move from Android:** Prevents users from transferring data from an Android device to an iOS device. This option is available only when **Set up as new or restore** is selected (that is, the step is skipped).
- **Apple ID:** Prevents users from setting up a Managed Apple ID account for the device.
- **Terms and conditions:** Prevents users from reading and accepting terms and conditions for use of the device.
- **Apple Pay:** Prevents users from setting up Apple Pay. If this setting is cleared, users must set up Touch ID and Apple ID. Ensure that those settings are cleared.
- **Siri:** Prevents the user from configuring Siri.
- **App analytics:** Prevents users from setting up whether to share crash data and usage statistics with Apple.
- **Display zoom:** Prevents users from setting up the display resolution (either standard or zoomed) on iOS devices.
- **True Tone:** Prevents users from setting up four-channel sensors to dynamically adjust the white balance of the display.
- **Home button:** Prevents users from setting up the Home button style of feedback.
- **New feature highlights:** Prevents users from seeing screens that display information about new features of Apple software.
- **Privacy:** Prevent users from seeing the data and privacy pane. For iOS 11.3 and later.
- **Software update:** Prevents users from updating iOS to the latest version. For iOS 12.0 and later.
- **Screen Time:** Prevents users from enabling Screen Time. For iOS 12.0 and later.
- **SIM setup:** Prevents users from setting up a cellular plan. For iOS 12.0 and later.
- **iMessage & FaceTime:** Prevents users from enabling iMessage and FaceTime. For iOS 12.0 and later.
- **Appearance:** Prevents users from selecting the appearance mode. For iOS 13.0 and later.
- **Welcome:** Prevents the user from seeing the **Get Started** screen. For iOS 13.0 and later.
- **Restore completed:** Prevents users from seeing whether a restore completes during setup. For iOS 14.0 and later.
- **Update completed:** Prevents users from seeing whether a software update completes during setup. For iOS 14.0 and later.

The account appears on **Settings > Apple Deployment Program**.

8. In **macOS Setup Assistant Options**, select the steps that the macOS Setup Assistant skips when users start their devices the first time. When a screen is skipped, the related feature uses default settings. Users can configure the skipped features after setup completes unless you restrict ac-

cess to those features completely. For more information about restricting access to features, see [Restrictions device policy](#). The default for all items is cleared. The following descriptions explain what occurs when a setting is selected.

Apple Deployment Program Account	macOS Setup Assistant Options
1 Server Tokens	Select the Setup Assistant items that users won't see when they start their macOS Automatic Device Enrollment devices for the first time.
2 Account Info	
3 iOS settings	
iOS	
macOS	
Apple TV	
4 Setup Assistant Options	
iOS	
macOS	<p><b>Skip setup</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Set up as new or restore</li> <li><input type="checkbox"/> Location services macOS 10.11+</li> <li><input type="checkbox"/> Apple ID</li> <li><input type="checkbox"/> Terms and conditions</li> <li><input type="checkbox"/> Siri macOS 10.12+</li> <li><input type="checkbox"/> FileVault macOS 10.10+ ⓘ</li> <li><input type="checkbox"/> App analytics</li> <li><input type="checkbox"/> Privacy macOS 10.13+</li> <li><input type="checkbox"/> iCloud Analytics macOS 10.13+</li> <li><input type="checkbox"/> iCloud Documents and Desktop macOS 10.13+</li> <li><input type="checkbox"/> Appearance macOS 10.14+</li> <li><input type="checkbox"/> Accessibility macOS 11+</li> <li><input type="checkbox"/> Biometric macOS 10.12.4+</li> <li><input type="checkbox"/> True Tone macOS 10.13.6+</li> <li><input type="checkbox"/> Apple Pay macOS 10.12.4+</li> <li><input type="checkbox"/> Screen Time macOS 10.15+</li> </ul> <p><b>Local account setup options</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Create primary account as a standard user macOS 10.11+</li> </ul> <p>Admin full name <input type="text"/></p> <p>Admin short name <input type="text" value="localadmin"/></p>
Apple TV	

- **Set up as new or restore:** Prevents users from setting up the device as new or from a Time Machine backup or perform a system migration.
- **Location services:** Prevents users from setting up the location service on the device. For macOS 10.11 and later.
- **Apple ID:** Prevents users from setting up a Managed Apple ID account for the device.
- **Terms and conditions:** Prevents users from reading and accepting terms and conditions for use of the device.
- **Siri:** Prevents the user from configuring Siri. For macOS 10.12 and later.
- **FileVault:** Use FileVault to encrypt the startup disk. Endpoint Management only applies the FileVault setting if the system has a single local user account and that account is signed into iCloud.

You can use the macOS FileVault Disk Encryption feature to protect the system volume by encrypting its contents (<https://support.apple.com/en-us/HT204837>). If you run the Setup assistant on a late-model portable Mac that doesn't have FileVault turned on, you might be prompted to turn on this feature. The prompt appears on both new systems and systems upgraded to OS X 10.10 or 10.11, but only if the system has a single local administrator account and that account is signed into iCloud.

- **App analytics:** Prevents users from setting up whether to share crash data and usage statistics with Apple.
- **Privacy:** Prevent users from seeing the Data and privacy pane. For macOS 10.13 and later.
- **iCloud Analytics:** Prevent users from choosing whether to send diagnostic iCloud data to Apple. For macOS 10.13 and later.
- **iCloud Documents and Desktop:** Prevent users from setting up the iCloud Desktop and Documents. For macOS 10.13 and later.
- **Appearance:** Prevents users from selecting the appearance mode. For macOS 10.14 and later.
- **Accessibility:** Prevents the user from hearing Voice Over automatically. Only available if the device is connected to Ethernet. For macOS 11 and later.
- **Biometric:** Prevents the user from setting up Touch ID and Face ID. For macOS 10.12.4 and later.
- **True Tone:** Prevents users from setting up four-channel sensors to dynamically adjust the white balance of the display. For macOS 10.13.6 and later.
- **Apple Pay:** Prevents users from setting up Apple Pay. If this setting is cleared, users must set up Touch ID and Apple ID. Make sure that the **Apple ID** and **Biometric** settings are cleared.
- **Screen Time:** Prevents users from enabling Screen Time. For macOS 10.15 and later.
- **Local account setup options:** Specify the settings to create an account on the device. Endpoint Management first creates the local administrator account by using the information you specify here. When users activate their device, a user account is created as the primary account. The **Create primary account as a standard user** option determines whether the primary account has administrator privileges.

**Important:**

You can select **Create primary account as a standard user** only after you set **Wait for configuration to complete setup** to **On** on the **macOS settings** page.

- **Create primary account as a standard user:** When selected, Endpoint Management creates the user with standard permissions rather than granting the user administrator privileges on the device. Skip this option if you want to grant the user administrator privileges on the device. By default, this option is not selected.
- **Admin full name:** Type the name the system displays for the administrator account.
- **Admin short name:** Type the name that the device displays for the home folder and in the shell.
- **Admin password:** Type a secure password for the administrator account.

- **Show administrator account in Users and Groups:** If cleared, the administrator account doesn't appear in **Users and Groups** in the macOS settings. If you create the primary account as a standard user, enable this setting to hide the administrator account that Endpoint Management first creates.

To enhance security, Endpoint Management checks whether to rotate the password of the administrator account daily. By default, Endpoint Management rotates the password every 7 days. To change the default, update the `mac.dep.admin.passwd.rotate` server property. For more information, see [Server properties](#).

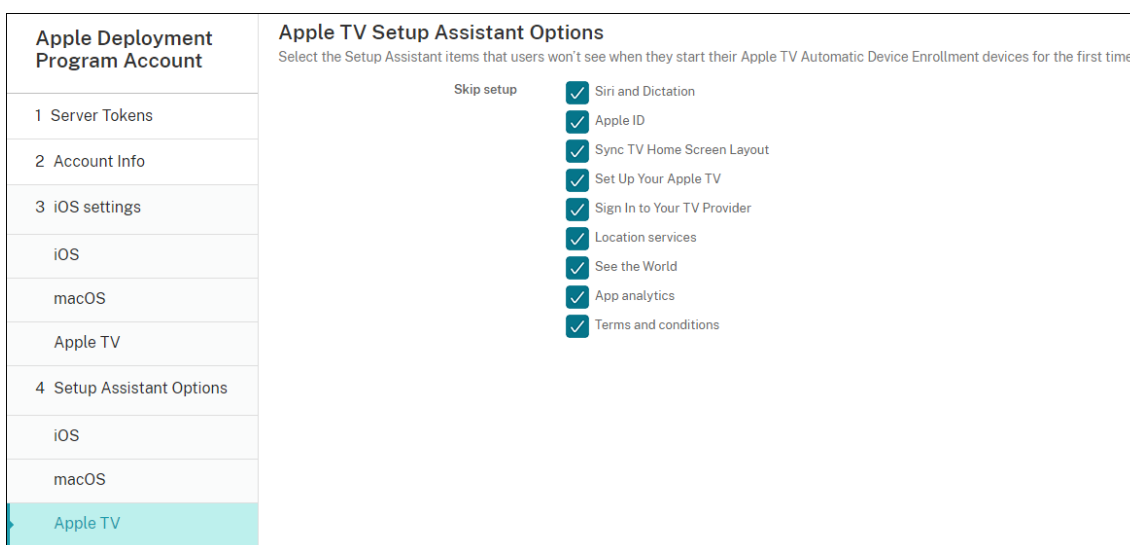
To increase password strength and security, Endpoint Management generates passwords as follows:

- 12 characters long
- 3 upper-case letters
- 3 lower-case letters
- 3 numbers
- 3 special characters: ! \@ \## \\$ % \^ \\* ? + = -

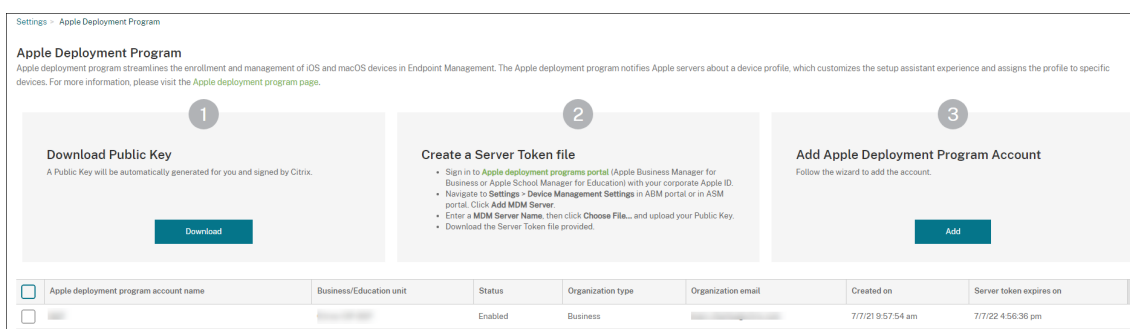
To view the previous password, the current password, and password change status for a device, go to **Manage > Devices**. Click that device, click **Show more**, and then view the **Device details > General** page. The **Security** section displays the following:

- **Previous administrator password:** Lets you view the previous password. Endpoint Management displays only the last password. Click **Show password** to view the password.
- **Current administrator password:** Lets you view the current password.
- **Change administrator password:** Lets you view password change status. The following information might appear, depending on actual status:
  - Password change was requested at <specific time value>.
  - The password was changed at <specific time value>.
  - Attempts to change the password failed at <specific time value>.
  - The password has not yet been changed.

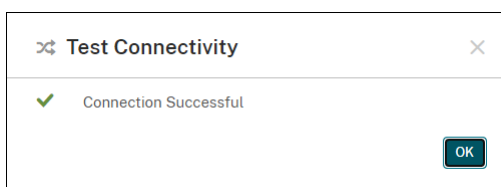
9. In **Apple TV Setup Assistant Options**, select the Apple TV Setup Assistant steps that your users skip when they start their devices the first time. The default for all items is cleared. Save the changes.



10. The account appears on **Settings > Apple Deployment Program**. To test connectivity between Endpoint Management and Apple, select the account and click **Test Connectivity**.



A status message appears.



## Order devices

You can order devices directly from the following channels:

- Apple. Provide your Apple customer numbers to the seller.
- Participating Apple Authorized Reseller or carriers. Provide your Organization ID to the seller and get its Reseller ID.

For more information about managing device suppliers, see [Apple Business Manager User Guide](#) or [Apple School Manager User Guide](#).

After your order ships, the Apple devices that you bought are added to your ABM or ASM account.

## Assign devices to Endpoint Management

In the ABM or ASM portal, search for an order number and use it to assign devices in this order to your Endpoint Management. You can also add iPhone, iPad, iPod touch, and Apple TV devices to ABM or ASM by using Apple Configurator 2, regardless of where the devices were bought.

For more information, see the [Apple Business Manager User Guide](#) or [Apple School Manager User Guide](#).

## Buy content in volume and synchronize it to Endpoint Management

ABM and ASM let you buy, distribute, and manage licenses of apps and books in volume from a single organization account. To enable your Endpoint Management to communicate with ABM or ASM to get the license information for distribution, complete the following steps:

1. In the ABM or ASM portal, buy public apps and books from the **Apps and Books** and buy custom apps that are developed for your Endpoint Management from **Custom Apps**.

**Note:**

If Endpoint Management is integrated with Citrix Workspace, buy the **Workspace** App and configure it as a required app in Endpoint Management.

2. In the ABM or ASM portal, download the content token assigned to your Endpoint Management.

For more information about Steps 1 and 2, see the [Apple Business Manager User Guide](#) or [Apple School Manager User Guide](#).

3. In the Endpoint Management console, create a volume purchase account based on the content token you downloaded.

For more information, see [Adding apps through Apple volume purchase](#).

After the volume purchase account is created, the apps and books that you bought appear in **Manage > Apps**, and the devices that you assigned to the Endpoint Management server appear in **Manage > Devices**.

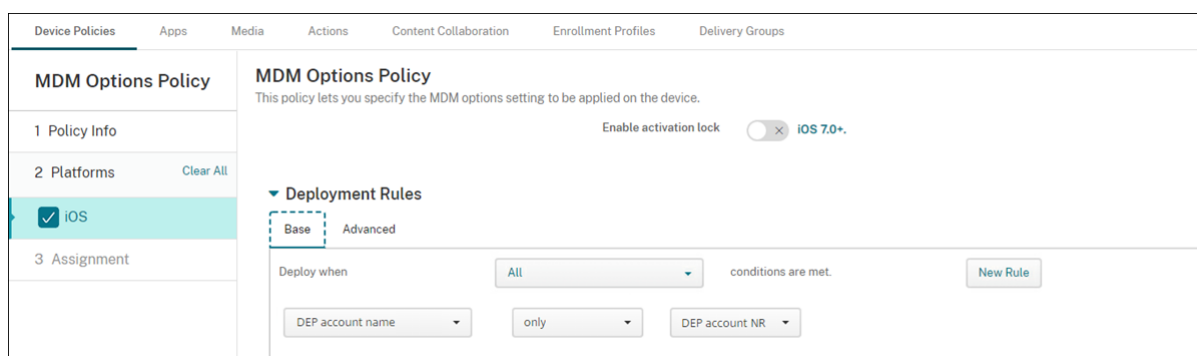
## Configure deployment rules for device policies and apps

You can associate ABM or ASM accounts with different device policies and apps when configuring device policies and apps.

1. On the **Configure > Device Policies** and **Configure > Apps** pages, expand **Deployment Rules**.
2. Specify that a policy or app deploys for a particular ABM account or for all ABM accounts except the one selected.

The list of ABM accounts includes only those accounts with a status of enabled or disabled. If the ABM account is disabled, the ABM device doesn't belong to this account. Therefore, Endpoint Management doesn't deploy the app or policy to the device.

In the following example, a device policy deploys only for devices with the ABM account name "ABM Account NR."



## Enroll Apple devices in bulk

September 22, 2021

You can enroll large numbers of iOS, iPadOS, macOS, and tvOS devices in Endpoint Management in two ways:

- Use the Apple Deployment Programs (ADP) to enroll Apple devices that you buy directly from Apple or from a participating Apple Authorized Reseller or a carrier.

For more information about deploying ADP-enabled devices, see [Deploy devices through the Apple Deployment Programs](#). This article describes how users enroll ADP-enabled devices and how to reenroll the devices.

- Use Apple Configurator 2 to enroll iOS devices regardless of whether you buy them directly from Apple.

This article describes how to deploy devices in bulk using Apple Configurator 2.

### About bulk enrollment

The ADPs include Apple Business Manager (ABM) for business and Apple School Manager (ASM) for Education. Bulk enrollment through the ADPs features the following:

- You don't have to touch or prepare the devices.
- After you complete deployment settings in Endpoint Management, you can give the devices to users who can start using them right away.



- You can simplify the setup process for users by eliminating some of the Setup Assistant steps.
- For more information about setting up ABM and ASM, see the documentation available from [Apple Business Manager](#) and [Apple School Manager](#).

Bulk enrollment through Apple Configurator 2 features the following:

- You attach iOS devices to a Mac running macOS 10.7.2 or later and the Apple Configurator 2 app. You prepare the iOS devices and configure policies through Apple Configurator 2.
- Devices automatically enroll in Endpoint Management during the setup process. Once setup is completed, Endpoint Management pushes policies, apps, and other resources to devices. You can then start managing the devices.
- For more information about using Apple Configurator 2, see the [Apple Configurator Help](#).

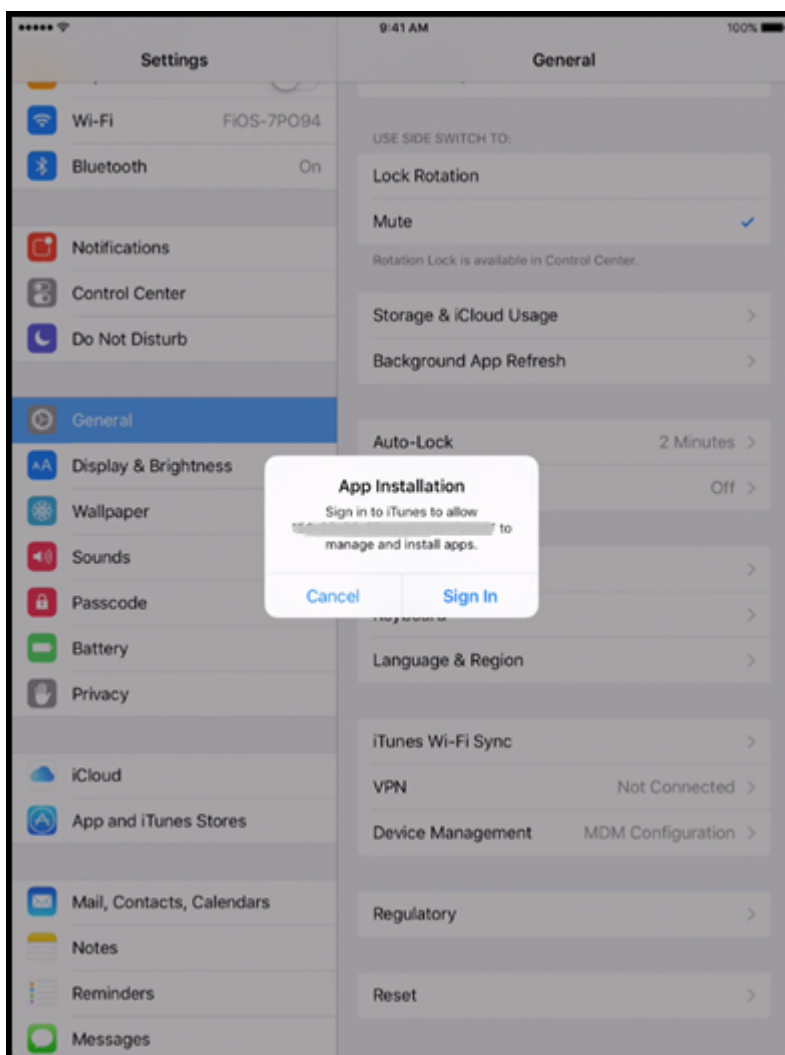
### **How users enroll ADP-enabled devices**

Users enroll their devices in Endpoint Management as follows:

1. Users start their device.
2. Endpoint Management delivers the ADP settings that you configured on the **Settings > Apple Deployment Programs** page to the device.
3. Users configure the initial settings on their device.
4. The device automatically starts the Endpoint Management device enrollment process.
5. If you integrate Endpoint Management with Citrix Workspace, the Deployment Program deployment package includes the Workspace App as a required app. In that case, Secure Hub prompts users to enroll the device in Citrix Workspace before enrolling in Endpoint Management.
6. Users continue to configure the other initial settings on their device.
7. In the home screen, users might be prompted to sign in to the Apple App Store so that they can download Citrix Secure Hub.

**Note:**

This step is optional if you configure Endpoint Management to deploy the Secure Hub app using the device-based volume purchase app assignment. In this case, you don't need to create an Apple App Store account or use an existing account.



8. Users open Secure Hub and type their credentials. If required by the policy, users might be prompted to create and verify a Citrix PIN.

Endpoint Management deploys any remaining required apps to the device.

### Reenroll the ADP-enabled devices

ADP-enabled devices enroll from a factory reset condition. To reenroll an ADP-enabled device, you must first complete a full wipe to unenroll the device. Detailed steps are as follows:

1. On the **Manage > Devices** page, select the device.
2. Click **Security**.
3. Click **Full Wipe** to unenroll the device to the factory reset condition.
4. Start the device.

**Important:**

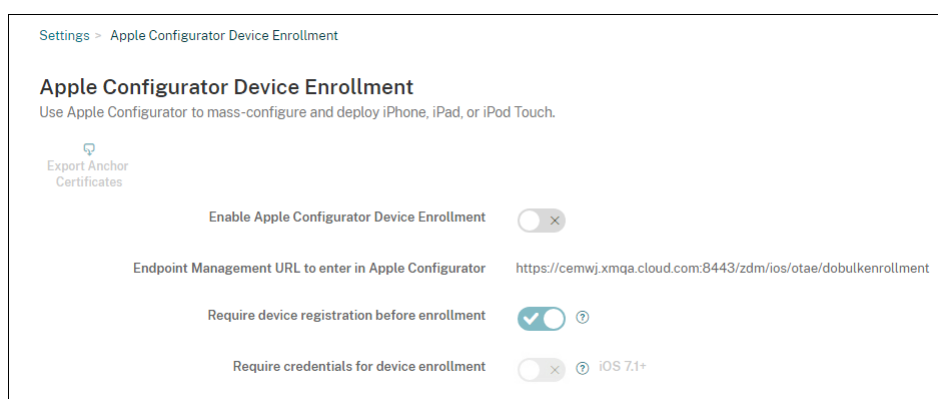
Do not use **Selective Wipe** to unenroll an ADP-enabled device because ADP enrollment requires the device in the factory reset condition.

**Deploy devices using Apple Configurator 2**

You can use Apple Configurator 2 to deploy large numbers of devices with settings, apps, and data and enroll these devices in Endpoint Management.

**Step 1: Configure settings in Endpoint Management**

1. In the Endpoint Management console, go to **Settings > Apple Configurator Device Enrollment**.

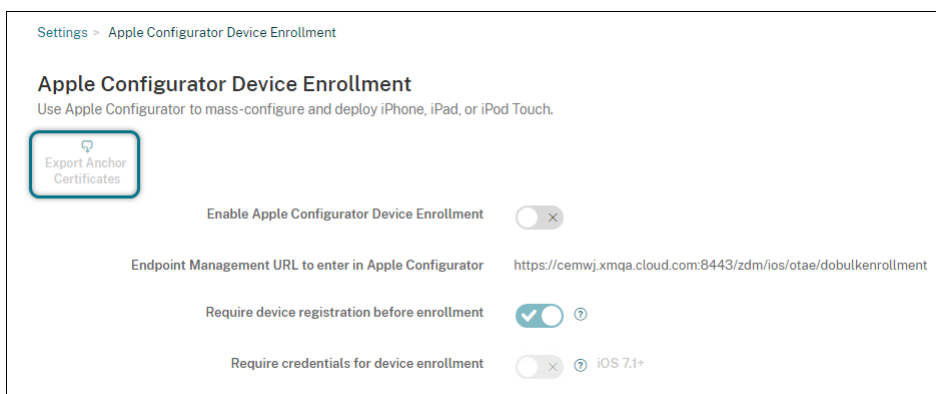


2. Set **Enable Apple Configurator device enrollment** to **Yes**.
3. Copy the **Enrollment URL to enter in Apple Configurator** setting and paste this URL when you configure settings in Apple Configurator 2. This setting provides the URL for the Endpoint Management server that communicates with Apple. The enrollment URL is the Endpoint Management server fully qualified domain name (FQDN), such as `mdm.server.url.com`, or the IP address.
4. To prevent unknown devices from enrolling, set **Require device registration before enrollment** to **Yes**. Note: If this setting is **Yes**, you must add the configured devices to **Manage > Devices** in Endpoint Management manually or through a CSV file before enrollment.
5. To require users of iOS devices to enter their credentials when enrolling, set **Require credentials for device enrollment** to **Yes**. The default is **No**.

**Note:**

If the Endpoint Management server is using a trusted SSL certificate, skip this step. Click **Export anchor certs** and save the certchain.pem file to the macOS keychain (login or Sys-

tem).



## Step 2: Configure settings in Apple Configurator 2

1. Prepare a Mac that runs macOS 10.7.2 or later and has Apple Configurator 2 installed.
2. Use a Dock Connector-to-USB cable to connect Apple devices to the Mac. You can configure up to 30 connected devices simultaneously. If you do not have a Dock Connector, use one or more powered USB 2.0 high-speed hubs to connect the devices.
3. Start Apple Configurator 2. The configurator shows any devices that you can prepare for supervision.
4. To prepare a device for supervision:
  - Select **Supervise devices** if you intend to maintain control of the device by reapplying a configuration regularly. Click **Next**.

### Important:

Placing a device into Supervised mode installs the selected version of iOS on the device, completely wiping the device of any previously stored user data or apps.

- In iOS, click **Latest** for the latest version of iOS that you want to install.
5. In **Enroll in MDM Server**, choose an MDM server. To add a server, click **Next**.
  6. In **Define an MDM server**, provide a name for the server and paste the MDM server URL from the Endpoint Management console.
  7. In **Assign to organization**, choose an organization to supervise the device.

For more information on preparing devices with Apple Configurator 2, see the Apple Configurator help page, [Prepare devices](#).

8. As each device is prepared, turn it on to start the iOS Setup Assistant, which prepares the device for first-time use.

## Add devices to ABM or ASM using Apple Configurator 2

You can add iPhone, iPad, and Apple TV devices to your ABM or ASM account using Apple Configurator 2 regardless of where the devices were bought.

After you add devices, they appear in the **Devices** section. These devices no longer include enrollment settings assigned through Apple Configurator 2. For more information, see the [Apple Business Manager User Guide](#) or [Apple School Manager User Guide](#).

## Renew the ADP token

Endpoint Management displays a license expiration warning when your ADP token expires. Replace the token from ASM or ABM.

### Step 1: Download a public key from your Endpoint Management server

1. In the Endpoint Management console, go to **Settings > Apple Deployment Program** to download a new public key.

### Step 2: Create and download a server token file from your Apple account

1. Sign in to ABM to download the token.
2. Open **Settings** and select the server from which you need a token. Click **Edit**.
3. Under **MDM Server Settings**, upload the new public key you downloaded from Endpoint Management and save the changes.
4. Click **Download Token** to download the new token.

### Step 3: Upload a server token file in Endpoint Management

1. In Citrix Endpoint Management, go to **Settings > Apple Deployment Program**.
2. Select the Deployment Program account, click **Edit**, and upload your server token file.
3. Click **Next** and save the changes.

## Integrate with Apple Education features

April 29, 2021

You can use Endpoint Management as your mobile device management (MDM) solution in an environment that uses Apple Education. Endpoint Management support includes Apple School Manager

(ASM) and Classroom app for iPad. The Endpoint Management Education Configuration device policy configures instructor and student devices for use with Apple Education.

You provide preconfigured and supervised iPads to instructors and students. That configuration includes ASM enrollment in Endpoint Management, a Managed Apple ID account configured with a new password, and required volume purchase apps and eBooks.

For more information about Apple Education features, see the Apple [Education](#) site and the Apple Education Deployment Guide from the same site.

## Apple School Manager

Follow these general steps to integrate Endpoint Management with ASM.

1. Create an account for your institution in ASM to enroll your institution in ASM.
2. Configure an Education volume purchase account for Apple School Manager.
3. Add passwords for Apple School Manager users.
4. Plan and add resources and delivery groups to Endpoint Management.
5. Test instructor and student device enrollments.
6. Provide the preconfigured devices to instructors and students.
7. Manage instructor, student, and class data
8. If a device is lost or stolen, you can lock and locate the device.

For information on enrolling in ASM and connecting your account to Endpoint Management, see [Deploy devices through the Apple Deployment Program](#).

## Prerequisites

- Citrix Gateway
- Enrollment profile configured for MDM+MAM.
- Apple iPad 3rd generation (minimum version) or iPad Mini, with iOS 9.3 (minimum version)

### Note:

Endpoint Management doesn't validate ASM user accounts against LDAP or Active Directory. However, you can connect Endpoint Management to LDAP or Active Directory for management of users and devices not related to ASM instructors or students. For example, you can use Active Directory to provide Secure Mail and Secure Web to other ASM members, such as IT administrators and managers.

Because ASM instructors and students are local users, there is no need to deploy Citrix Secure Hub to their devices.

MAM enrollment that includes Citrix Gateway authentication doesn't support local users (only Ac-

tive Directory users). Therefore, Endpoint Management deploys only required volume purchase apps and iBooks to instructor and student devices.

### **Classroom app for iPad**

The Classroom app for iPad enables instructors to connect to and manage student devices. You can view device screens, open apps on iPads, share and open web links, and present a student screen on Apple TV.

Classroom is free in the App Store. You upload the app to the Endpoint Management console. You then use the Education Configuration device policy to configure the Classroom app, which you deploy to instructor devices.

For more information on how to deploy the Classroom app, see [Distribute Apple apps](#).

For more information on Classroom app requirements, setup, and features, see the [Classroom user guide](#) on the Apple support site.

### **Add passwords for Apple School Manager users**

After you add an ASM account, Endpoint Management imports classes and users from ASM. Endpoint Management treats classes as local groups and uses the term “group” in the console. If a class has a group name in ASM, Endpoint Management assigns the group name to the class. Otherwise, Endpoint Management uses the source system ID for the group name. Endpoint Management doesn’t use the course name for the class name because course names in ASM aren’t unique.

Endpoint Management uses the Managed Apple IDs to create local users with the user type **ASM**. The users are local because ASM creates the credentials independently of all external data sources. As a result, Endpoint Management doesn’t use a directory server to authenticate these new users.

ASM doesn’t send temporary user passwords to Endpoint Management. You can import them from a CSV file or add them manually. To import temporary user passwords:

1. Obtain the CSV file generated by ASM when creating the Managed Apple ID temporary passwords.
2. Edit the CSV file, replacing the temporary passwords with new passwords that users provide to enroll to Endpoint Management. There is no constraint on the password type for this purpose.

The format of an entry in the CSV file is as follows: `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`

Where:

User: `user@appleid.citrix.com`

First name: `Firstname`

Middle name: `Middle`

Last name: `Lastname`

Password: `Password123!`

- In the Endpoint Management console, click **Manage > Users**. The **Users** page appears.

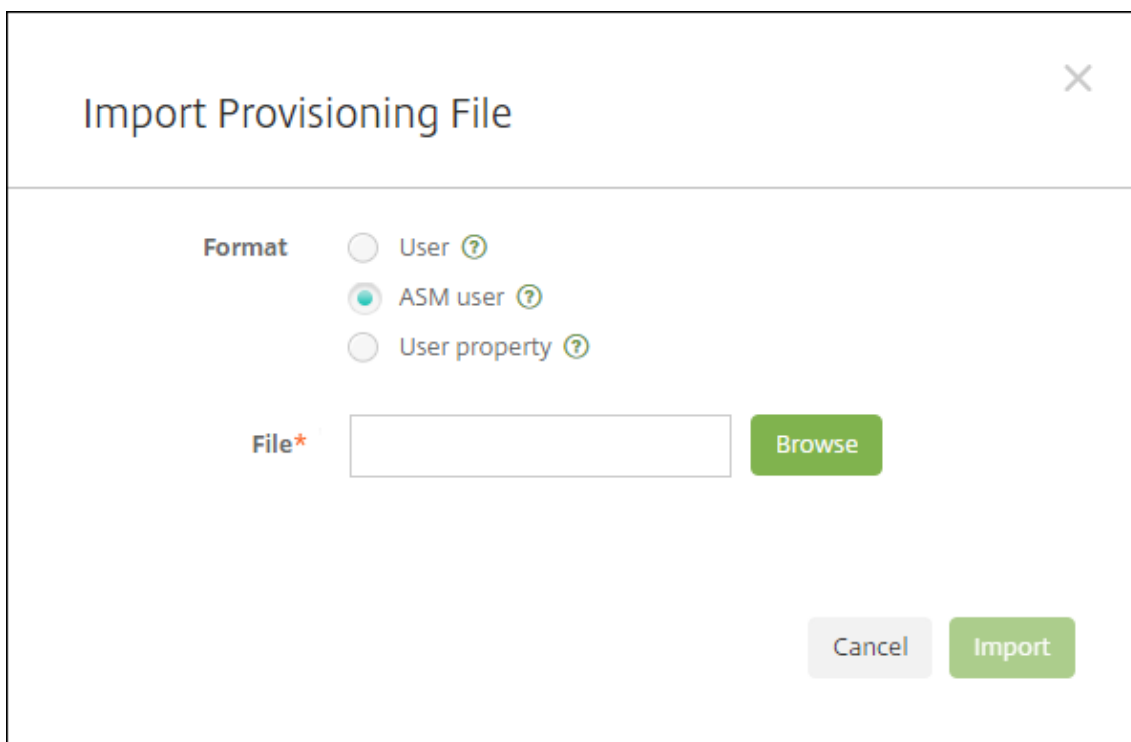
The following **Manage > Users** screen sample shows a list of users imported from ASM. In the **Users** list:

- User name** shows the managed Apple ID.
- User type is **ASM**, to indicate the account originated from ASM.
- Groups** show the classes.

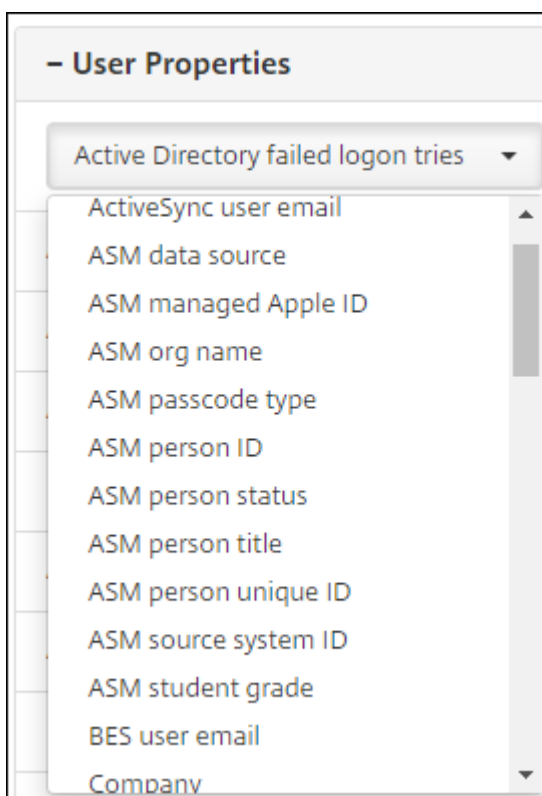
User name	First name	Last name	User type	Roles	Groups	Domain	Created
[Redacted]	Julia	Romero	ASM	USER	SAMPLE-CLASS-1013 - HS.SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00
[Redacted]	Kaelyn	Lazzara	ASM	USER	SAMPLE-CLASS-1013 - HS.SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00
[Redacted]	Brooklyn	Baily	ASM	USER	SAMPLE-CLASS-1010 - HS.SAMPLE-CLASS-1014 - HS	local	21/07/2017 14:43:00

- Click **Import Local Users**. The **Import Provisioning File** dialog box appears.
- For Format, choose **ASM user**, navigate to the CSV file you prepared in step 2, and then click **Import**.





6. To view the properties for a local user, select the user and then click **Edit**.



In addition to the name properties, these ASM properties are available:

- **ASM data source:** The data source of the class, such as **CSV** or **SFTP**.
- **ASM managed Apple ID:** A Managed Apple ID might include your institution name and `appleid`. For example, the ID might resemble `johnappleseed@appleid.myschool.edu`. Endpoint Management requires a Managed Apple ID for authentication.
- **ASM org name:** The name you gave the account in Endpoint Management.
- **ASM passcode type:** Password policy of the person: **complex** (a non-student password of eight or more numbers and letters), **four** (digits), or **six** (digits).
- **ASM person unique ID:** Identifier for the user.
- **ASM person status:** Specifies whether the Managed Apple ID is **Active** or **Inactive**. This status becomes active after the user provides their new password for the Managed Apple ID account.
- **ASM person title:** Either Instructor, Student or Other.
- **ASM person unique ID:** Unique identifier for the user.
- **ASM source system ID:** Identifier for the system source.
- **ASM student grade:** Student grade information (not used by instructors).

## Plan and add resources and delivery groups to Endpoint Management

A delivery group specifies the resources to deploy to categories of users. For example, you might create one delivery group for instructors and students. Alternatively, you might create multiple delivery groups so you can customize the apps, media, and policies sent to various instructors or students. You might create one or more delivery groups per class. You can also create one or more delivery groups for managers (other staff in your educational institution).

Resources that you deploy to user devices include device policies, volume purchase apps, and iBooks.

- Device policies:

If instructors use the Classroom app, the Education Configuration device policy is required. Be sure to review other device policies to determine how you want to configure and restrict instructor and student iPads.

- Volume purchase apps:

Endpoint Management requires that you deploy volume purchase apps as required apps for education users. Endpoint Management doesn't support deploying such volume purchase apps as optional.

If you use the Apple Classroom app, deploy it only to instructor devices.

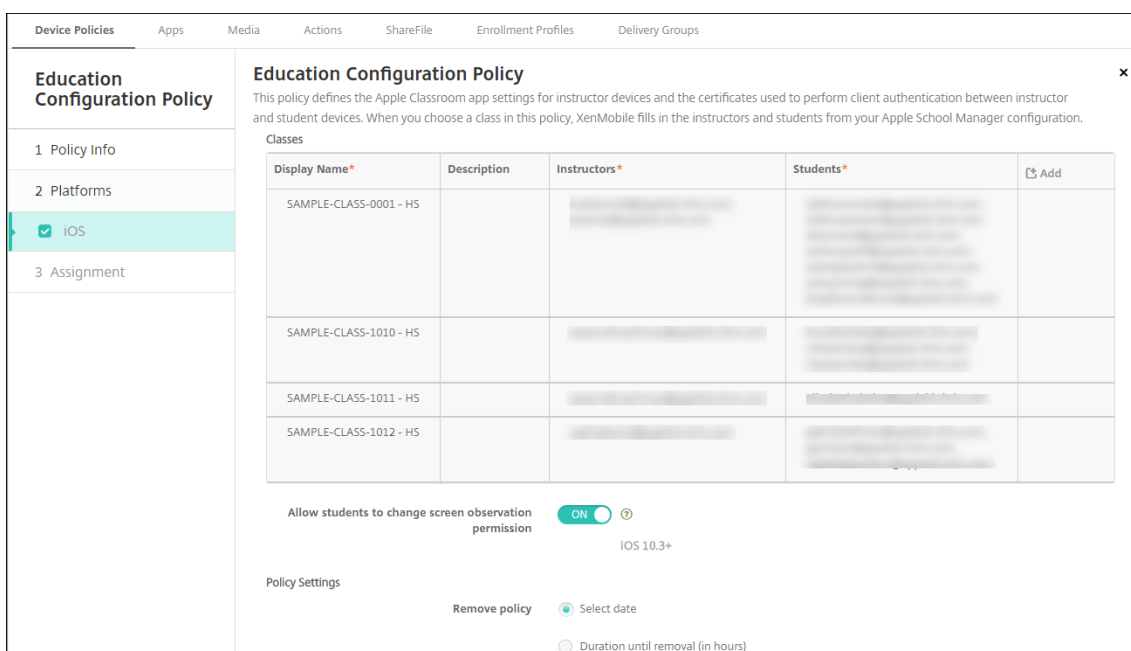
Deploy any other apps that you want to provide to instructors or students. This solution doesn't use Citrix Secure Hub app, so there's no need to deploy it to instructors or students.

- Volume purchase iBooks:

After Endpoint Management connects to your ASM account, your purchased iBooks appear in the Endpoint Management console, in **Configure > Media**. The iBooks listed on that page are available to add to delivery groups. Endpoint Management supports adding iBooks as required media only.

After you plan the resources and delivery groups for instructors and students, you can create those items in the Endpoint Management console.

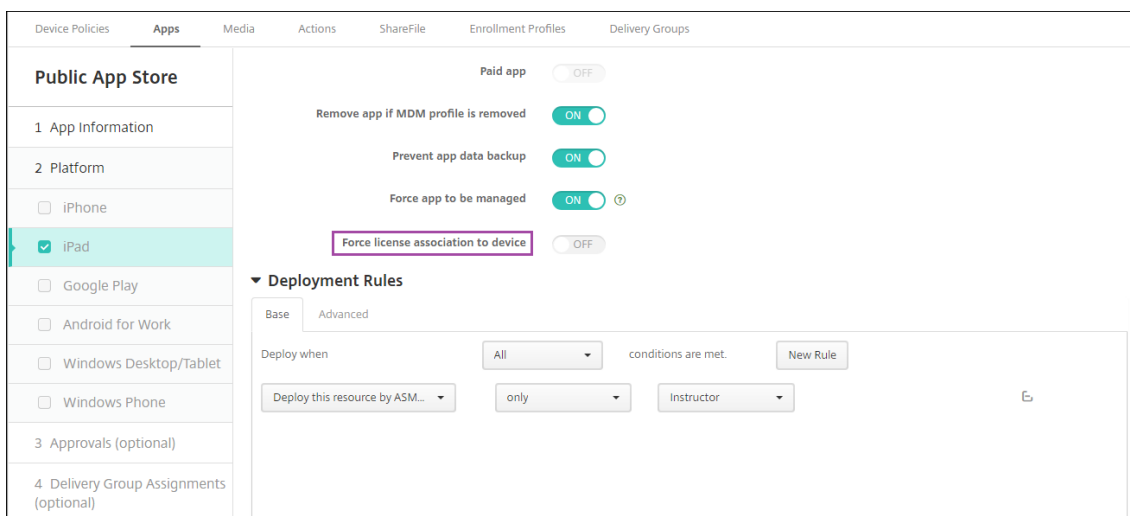
1. Create any device policies that you want to deploy to instructor or student devices. For information about the Education Configuration device policy, see [Education Configuration device policy](#).



For information about device policies, see [Device policies](#) and the individual policy articles.

2. Configure apps (**Configure > Apps**) and iBooks (**Configure > Media**):
  - By default, Endpoint Management assigns apps and iBooks at the user level. During first-time deployment, instructors and students receive a prompt to register to ASM. After accepting the invitation, users receive their ASM apps and iBooks at the next deployment (within six hours). Citrix recommends that you force the deployment of apps and iBooks to new ASM users. To do that, select the delivery group and click **Deploy**.

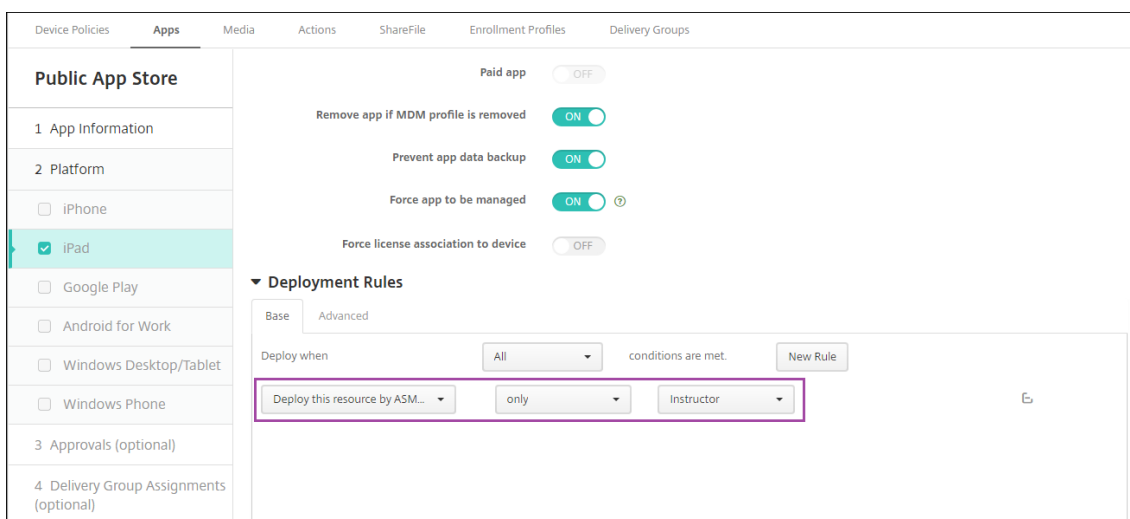
You can choose to assign apps (but not iBooks) at the device level. To do that, change the setting **Force license association to device** to **On**. When you assign apps at the device level, users don't receive an invitation to join the volume purchase program.



- To deploy an app only to instructors, select a delivery group that includes only instructors or use the following deployment rule:

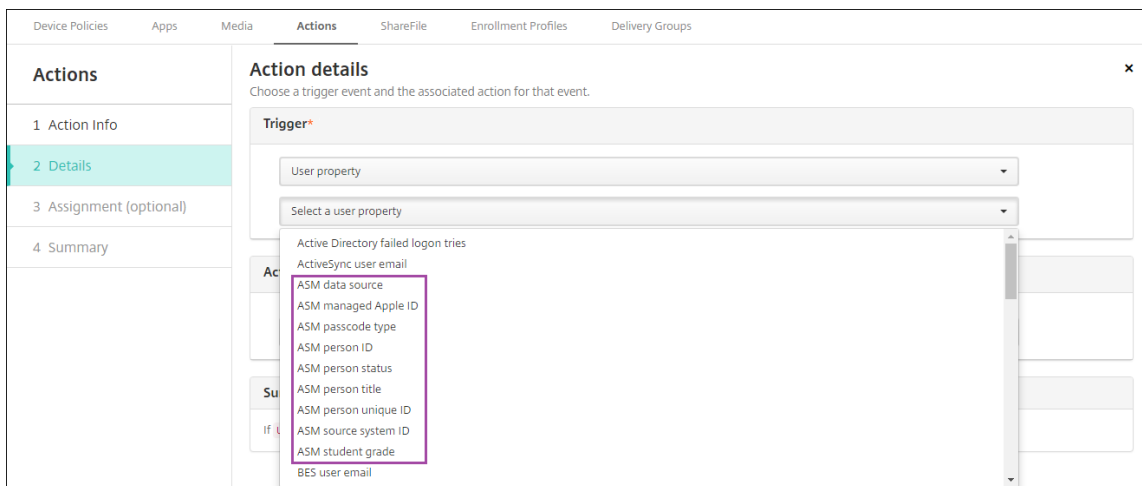
```

1 Deploy this resource by ASM device type
2 only
3 Instructor
4 <!--NeedCopy-->
    
```



- For help with adding volume purchase apps, see [Add a Public App Store app](#).

3. Optional. Create actions based on ASM user properties. For example, you might create an action to send a notification to student devices when a new app installs. Alternatively, you can create an action that a user property triggers, as shown in the following example.

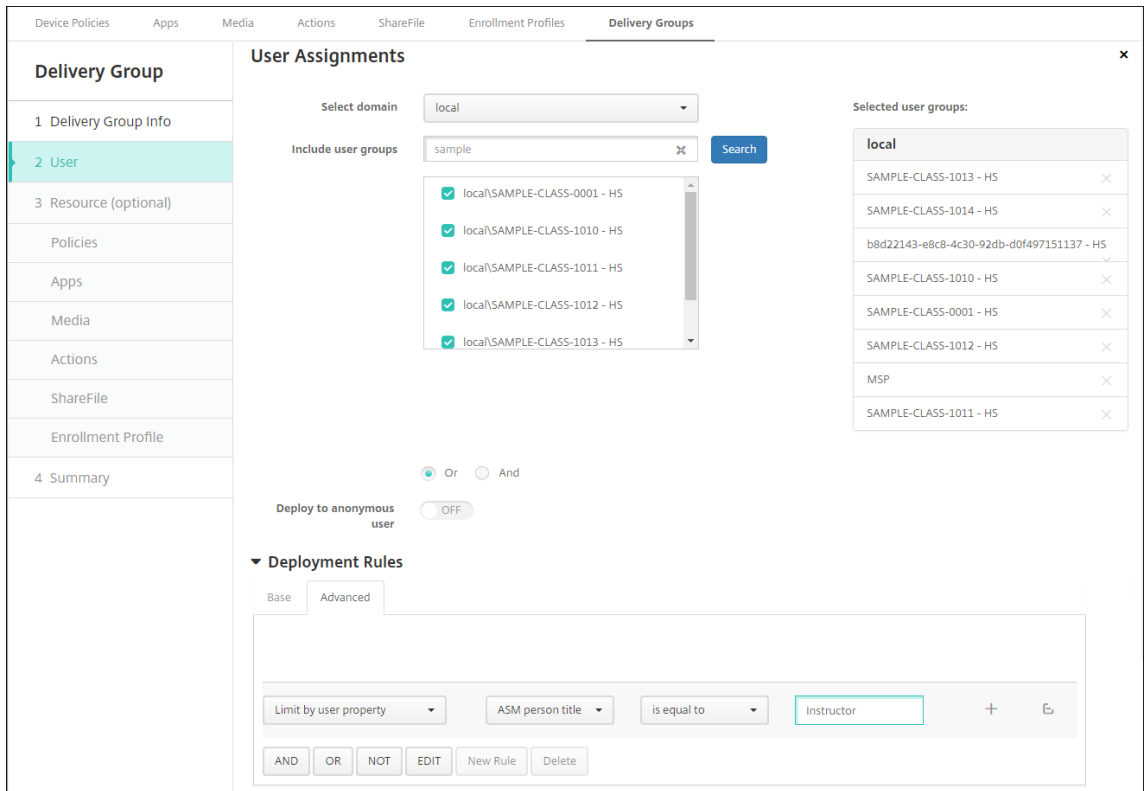


To create an action, go to **Configure > Actions**. For information about configuring actions, see [Automated actions](#).

4. In **Configure > Delivery Groups**, create delivery groups for instructors and for students. Choose the classes that were imported from ASM. Also, create a deployment rule for instructors and students.

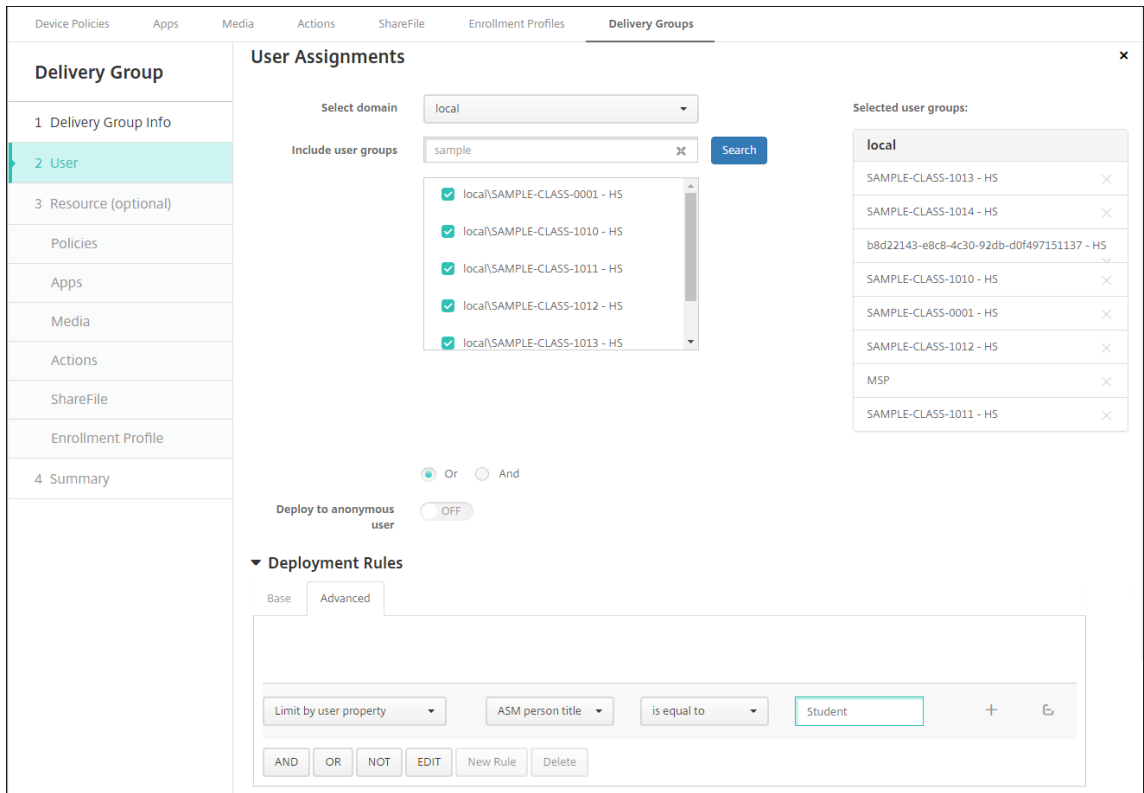
For example, the following user assignments are for instructors. The deployment rule is:

```
1 Limit by user property
2 ASM person title
3 is equal to
4 Instructor
5 <!--NeedCopy-->
```

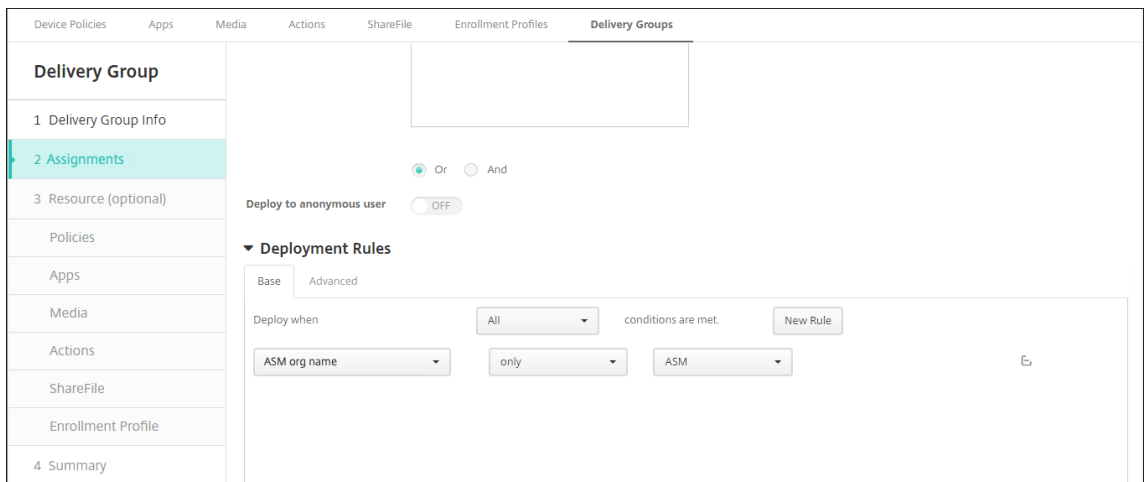


The following user assignments are for students. The deployment rule is:

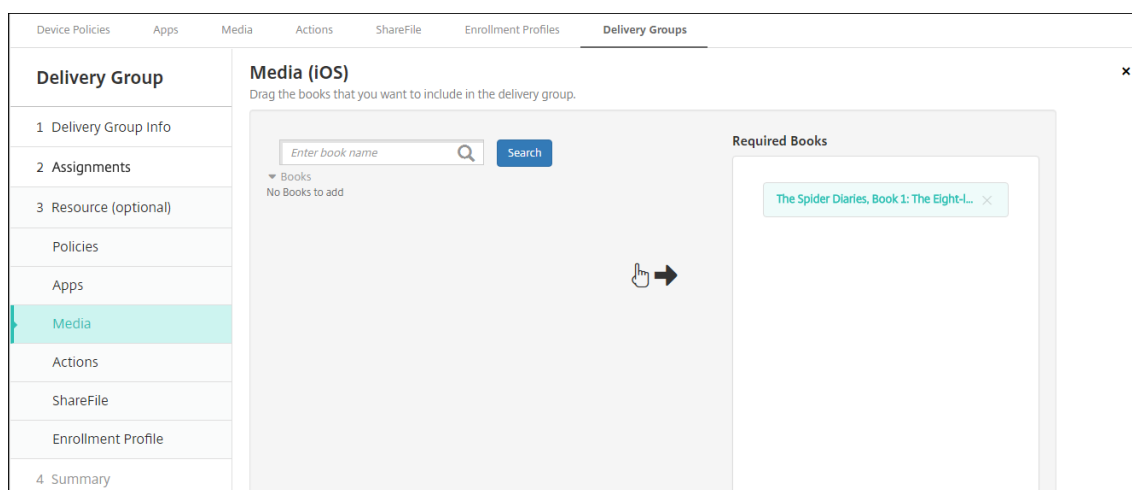
- 1 Limit by user property
- 2 ASM person title
- 3 is equal to
- 4 Student
- 5 <!--NeedCopy-->



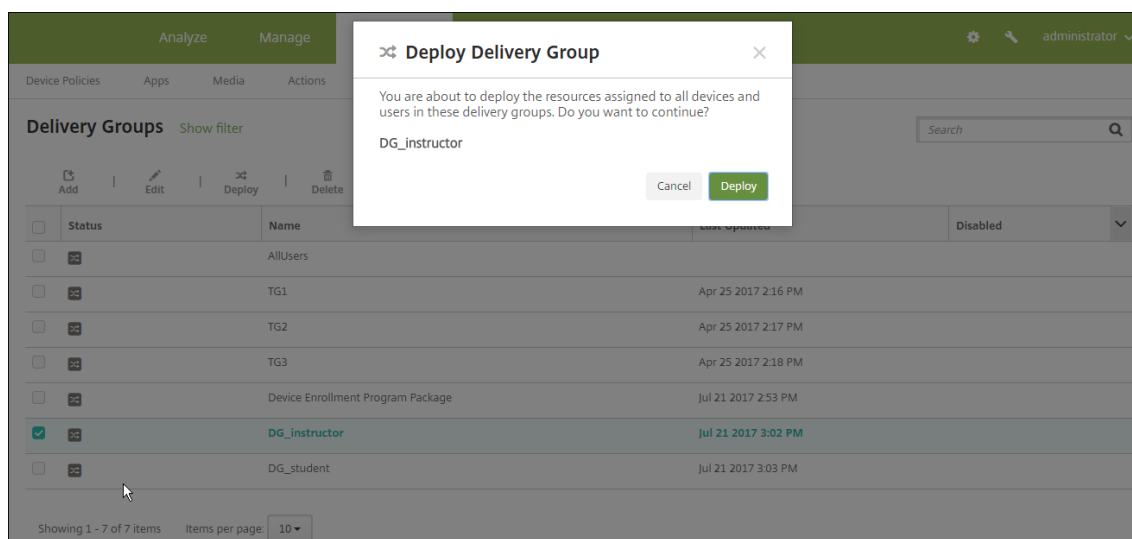
You can also filter a delivery group by using a deployment rule based on the ASM org name.



5. Assign the resources to delivery groups. The following example shows an iBook contained in a delivery group.



The following example shows the confirmation dialog that appears when you select a delivery group and click **Deploy**.



For more information, see “To edit a delivery group” and “To deploy to delivery groups” in [Deploy resources](#).

## Test instructor and student device enrollments

You can enroll devices through either of the following methods:

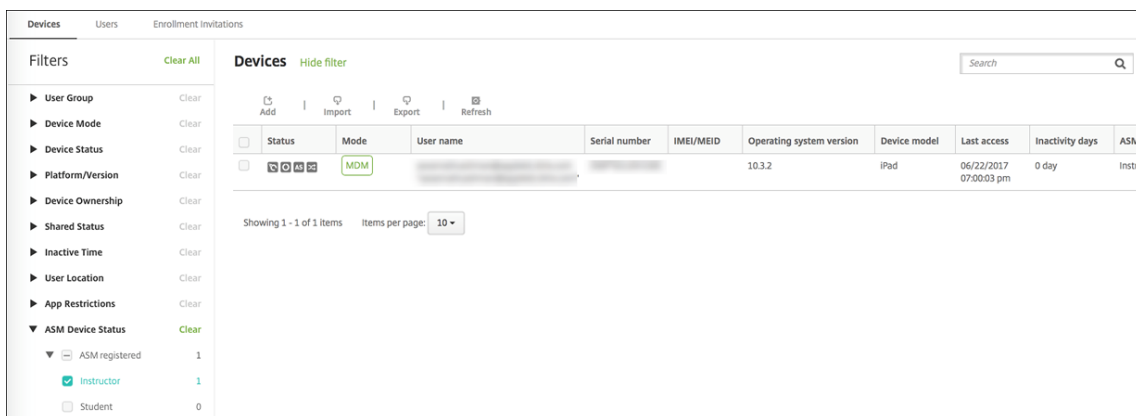
- A school administrator can enroll instructor and student devices by using the user password you can set in the Endpoint Management console. As a result, you can provide users with devices that are already set up with apps and media.
- When users receive the devices, they enroll using the user password that you provide to them. After enrollment completes, Endpoint Management sends device policies, apps, and media to the devices.



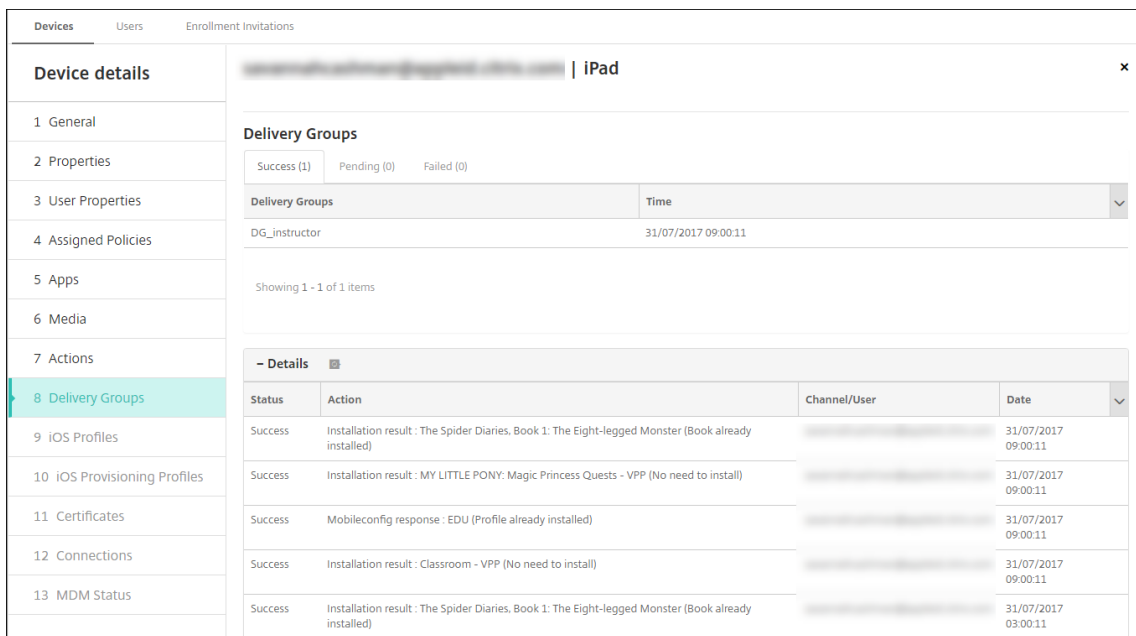
To test enrollment, use Apple Deployment Program devices that are linked to ASM.

1. If the devices aren't linked to ASM, erase the device contents and settings by performing a hard reset.
2. Enroll an ASM device with an instructor. Then, enroll an ASM device with a student.
3. In the **Manage > Devices** page, check that both ASM devices are enrolled in MDM only.

You can filter the **Devices** page by the ASM device status: **ASM registered**, **ASM shared**, **Instructor**, and **Student**.



4. To verify that MDM resources deployed correctly for each device: Select the device, click **Edit**, and check the various pages.



## Distribute devices

Apple recommends that you host an event so you can distribute devices to instructors and students.

If you don't distribute pre-enrolled devices, also provide the following to these users:

- Endpoint Management passwords for enrollment
- ASM temporary passwords for Managed Apple IDs.

The first-time user experience is as follows.

1. The first time that a user starts their device after a hard-reset, Endpoint Management prompts them in the enrollment screen to enroll their device.
2. The user provides their Managed Apple ID and Endpoint Management password used to authenticate to Endpoint Management.
3. In the Apple ID setup step, the device prompts the user to provide their Managed Apple ID and ASM temporary password. Those items authenticate the user to Apple services.
4. The device prompts the user to create a password for their Managed Apple ID, used to protect their data in iCloud.
5. At the end of the Setup Assistant, Endpoint Management starts installing the policies, apps, and media to the device. For apps and iBooks assigned at the user level, the assistant prompts instructors and students to register to volume purchase. After accepting the invitation, users receive their volume purchase apps and iBooks at the next deployment (within six hours).

### **Manage instructor, student, and class data**

When managing instructor, student, and class data, note the following:

- Don't change Managed Apple IDs after you import ASM information into Endpoint Management. Endpoint Management also uses ASM user identifiers to identify users.
- If you add or change class data in ASM after you create one or more Education Configuration device policies: Edit the policies and then redeploy them.
- If the instructor for a class changes after you deploy the Education Configuration device policy: Review the policy to ensure it updates in the Endpoint Management console and then redeploy the policy.
- If you update user properties in the ASM portal, Endpoint Management also updates those properties in the console. However, Endpoint Management doesn't receive the ASM person title property (Instructor, Student, or Other) in the same way it receives other properties. Thus, if you change the ASM person title in ASM, complete the following steps to reflect that change in Endpoint Management.

To manage the data:

1. In the ASM portal, update the student grade and clear the instructor grade.

2. If you changed a student account to an instructor account, remove the user from the list of students in the class. Then, add the user to the list of instructors in the same or another class.

If you changed an instructor account to a student account, remove the user from the class. Then, add the user to the list of students in the same or another class. Your updates appear in the Endpoint Management console during the next sync (every five minutes by default) or fetch (every 24 hours by default).

3. Edit the Education Configuration device policy to apply the change and redeploy it.
  - If you delete a user from the ASM portal, Endpoint Management also deletes that user from the Endpoint Management console after a fetch.

You can reduce the interval between two baselines by changing this server property value: **bulk.enrollment.fetchRosterInfoDelay** (default is **1440** minutes).

- After you deploy resources: If a student joins a class, create a delivery group with just that student and deploy the resources to the student.
- If a student or instructor loses their temporary password, have them contact the ASM administrator. The administrator can provide the temporary password or generate a new one.

## Manage a lost or stolen device

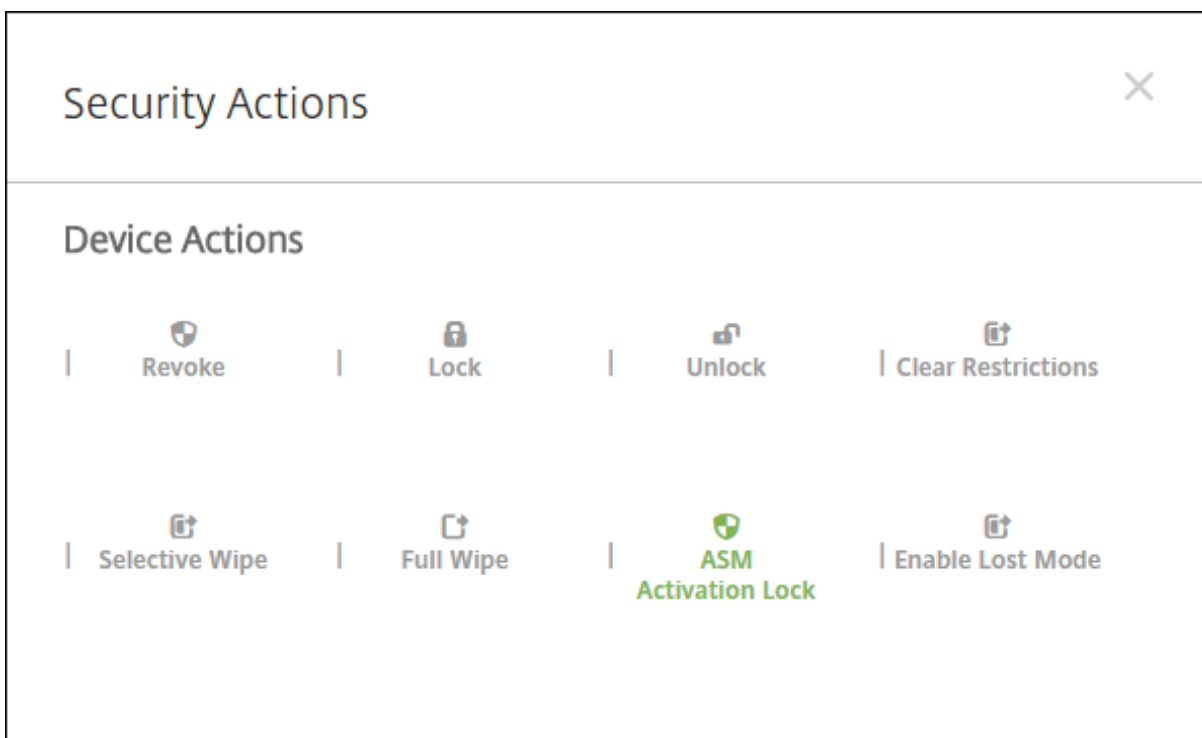
The Apple Find My iPhone/iPad service includes an Activation Lock feature. Activation Lock prevents non-authorized users from using or reselling a lost or stolen device that's enrolled in Apple Deployment Program.

Endpoint Management includes an **ASM Activation Lock** security action that enables you to send a lock code to an ASM Apple Deployment Program enrolled device.

When you use the **ASM Activation Lock** security action, Endpoint Management can locate devices without requiring users to enable the Find My iPhone/iPad service. When an ASM device is hard-reset or fully wiped, the user provides their Managed Apple ID and password to unlock the device.

To release the lock from the console, click the security action **Activation Lock Bypass**. For information about bypassing an activation lock, see [Bypass an iOS activation lock](#). The user also can leave the login blank and type the **ASM activation lock bypass code** as the password. That information is available in **Device Details**, on the **Properties** tab.

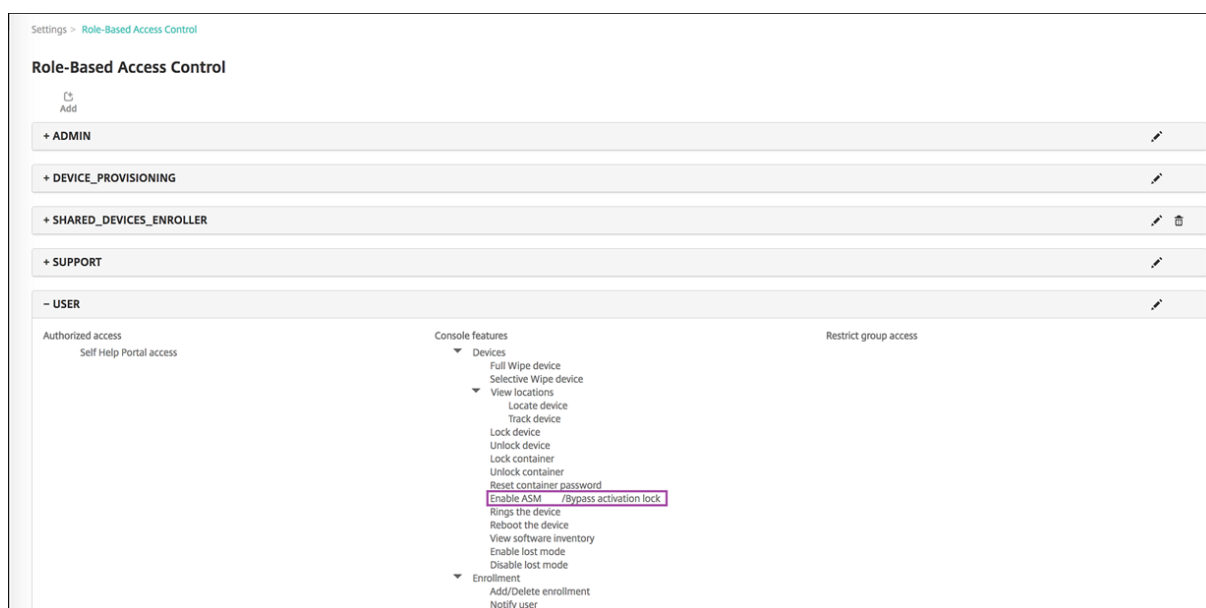
To set the activation lock, go to **Manage > Devices**, select the device, click **Security**, and then click **ASM Activation Lock**.



The properties **ASM escrow key** and **ASM activation lock bypass code** appear in **Device details**.

Devices	Users	Enrollment Invitations												
<b>Device details</b>														
1 General	<table border="1"> <thead> <tr> <th colspan="2">- Security information</th> <th>Add</th> </tr> </thead> <tbody> <tr> <td>ASM Automated Device Enrollment escrow key</td> <td></td> <td></td> </tr> <tr> <td>ASM Automated Device Enrollment activation lock bypass code</td> <td></td> <td></td> </tr> <tr> <td>Activation lock bypass code</td> <td></td> <td></td> </tr> </tbody> </table>		- Security information		Add	ASM Automated Device Enrollment escrow key			ASM Automated Device Enrollment activation lock bypass code			Activation lock bypass code		
- Security information		Add												
ASM Automated Device Enrollment escrow key														
ASM Automated Device Enrollment activation lock bypass code														
Activation lock bypass code														
2 Properties	<table border="1"> <tbody> <tr> <td>Activation lock enabled</td> <td>No</td> </tr> </tbody> </table>		Activation lock enabled	No										
Activation lock enabled	No													
3 User Properties	<table border="1"> <tbody> <tr> <td>Hardware encryption capabilities</td> <td>Block and file levels encryption</td> </tr> </tbody> </table>		Hardware encryption capabilities	Block and file levels encryption										
Hardware encryption capabilities	Block and file levels encryption													
4 Assigned Policies	<table border="1"> <tbody> <tr> <td>Internal storage encrypted</td> <td>No</td> </tr> </tbody> </table>		Internal storage encrypted	No										
Internal storage encrypted	No													
5 Apps	<table border="1"> <tbody> <tr> <td>Jailbroken/Rooted</td> <td>No</td> </tr> </tbody> </table>		Jailbroken/Rooted	No										
Jailbroken/Rooted	No													
6 Media	<table border="1"> <tbody> <tr> <td>MDM lost mode enabled</td> <td>No</td> </tr> </tbody> </table>		MDM lost mode enabled	No										
MDM lost mode enabled	No													
7 Actions	<table border="1"> <tbody> <tr> <td>Passcode compliant</td> <td>Yes</td> </tr> </tbody> </table>		Passcode compliant	Yes										
Passcode compliant	Yes													
8 Delivery Groups	<table border="1"> <tbody> <tr> <td>Passcode compliant with configuration</td> <td>Yes</td> </tr> </tbody> </table>		Passcode compliant with configuration	Yes										
Passcode compliant with configuration	Yes													
9 iOS Profiles	<table border="1"> <tbody> <tr> <td>Passcode present</td> <td>No</td> </tr> </tbody> </table>		Passcode present	No										
Passcode present	No													
10 iOS Provisioning Profiles	<table border="1"> <tbody> <tr> <td>Supervised</td> <td>Yes</td> </tr> </tbody> </table>		Supervised	Yes										
Supervised	Yes													
11 Certificates	<table border="1"> <thead> <tr> <th colspan="2">- Storage space</th> <th>Add</th> </tr> </thead> <tbody> <tr> <td>Available storage space</td> <td>25.58 GB</td> <td></td> </tr> <tr> <td>Total storage space</td> <td>27.05 GB</td> <td></td> </tr> </tbody> </table>		- Storage space		Add	Available storage space	25.58 GB		Total storage space	27.05 GB				
- Storage space		Add												
Available storage space	25.58 GB													
Total storage space	27.05 GB													
12 Connections														
13 MDM Status														

The RBAC permission for an ASM Activation Lock is **Devices > Enable ASM Bypass activation lock**.



## Shared iPads

June 11, 2021

The shared iPad feature allows multiple users to use an iPad. The user experiences can be personalized even though the devices are shared. You can use shared iPads for education or business. Apple School Manager (ASM) supports the instructor and student roles in addition to the roles Apple Business Manager (ABM) supports.

### Prerequisites for Shared iPads

- Apple School Manager or Apple Business Manager
- Citrix Endpoint Management
- Any iPad Pro, iPad 5th generation, iPad Air 2 or later, and iPad mini 4 or later
- At least 32 GB of storage
- Supervised devices

### Configure Shared iPads

Multiple students or employees can share an iPad for different purposes.

Either you or device owners enroll Shared iPads and then deploy device policies, apps, and media to the devices. After that, users provide their managed Apple ID credentials to sign in to a Shared iPad.

If you previously deployed an Education Configuration policy to students, they no longer sign in as an “Other User” to share devices.

Endpoint Management uses two communications channels for Shared iPads: The system channel for the device owner (instructor or supervisor) and the user channel for the current resident user (student or employee). Endpoint Management uses those channels to send the appropriate MDM commands for the resources supported by Apple.

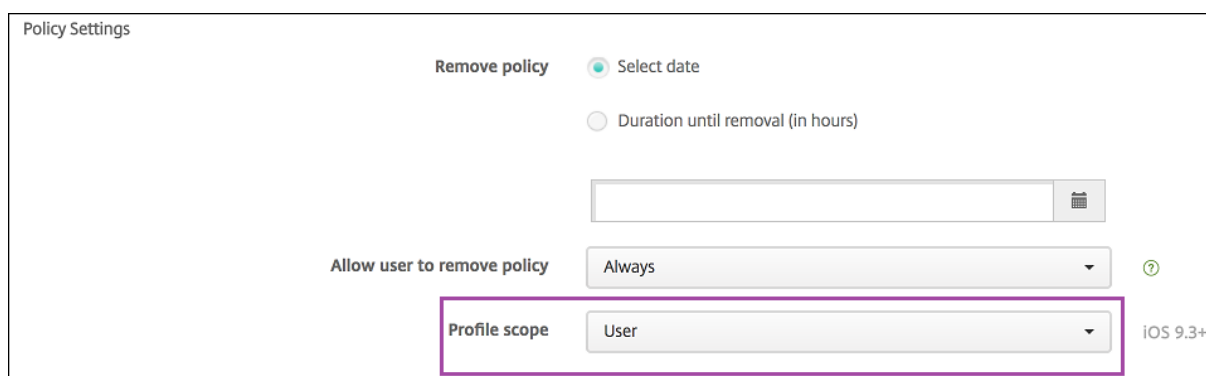
Resources that deploy over the system channel are:

- Device policies, such as [Education Configuration](#), [Lock Screen Message](#), [Maximum Resident Users](#), and [Passcode Lock Grace Period](#)
- Device-based volume purchase apps  
Apple doesn’t support Enterprise apps or user-based volume purchase apps on Shared iPads. Apps installed on a Shared iPad are global to the device and not per user.
- User-based volume purchase iBooks  
Apple supports assignment of user-based volume purchase iBooks on Shared iPads.

Resources that deploy over the user channel are:

- Device policies: Apps Notifications, Home Screen Layout, and Restrictions  
Endpoint Management supports only these device policies over the user channel.

When configuring device policies, you specify the deployment channel in the policy setting **Profile scope**.



To remove device policies that you deployed over the user channel, be sure to choose a **Deployment scope of User** for the Profile Removal policy.

### General workflow

Typically, you provide preconfigured and supervised Shared iPads to device owners. Those individuals then distribute the devices to students or employees. If you don’t distribute pre-enrolled Shared iPads: Be sure to provide the device owners with their Endpoint Management server passwords so they can enroll their devices.

The general workflow for configuring and enrolling Shared iPads is as follows.

1. Use the Endpoint Management server console to add ASM or ABM accounts (**Settings > Apple Deployment Program**) with **Shared mode** enabled. For more information, see “Manage accounts for Shared iPads” next.
2. As described in this section, add the required device policies, apps, and media to Endpoint Management. Assign those resources to delivery groups.
3. Have the device owners perform a hard reset on the Shared iPads. The Remote Management screen for enrollment appears.
4. The device owners enroll the Shared iPads.  
Endpoint Management deploys configured resources to each enrolled Shared iPad. After an automatic restart, device owners can share the devices with users. A sign-in page appears on the iPad.
5. A device user enters their Managed Apple ID and temporary ASM password.  
The Shared iPad authenticates to ASM and prompts the user to create an ASM password. For the next sign into the Shared iPad, the device user provides the new ASM password.
6. Another device user who shares the iPad can then sign in by repeating the previous step.

### **Manage accounts for Shared iPads**

If you already use Endpoint Management with Apple Education or Apple Business: You have an existing ASM/ABM account configured in Endpoint Management for devices that aren't shared, such as the devices used by device owners. You can use the same ASM/ABM account and the same Endpoint Management server for both shared and non-shared devices.

### **Organize Shared iPads into device groups**

ASM/ABM lets you organize devices into groups by creating multiple MDM servers. When you assign the Shared iPads to an MDM server, create a device group for each group of Shared iPads:

- Group 1 of Shared iPads > Device Group 1 MDM Server
- Group 2 of Shared iPads > Device Group 2 MDM Server
- Group N of Shared iPads > Device Group N MDM Server

### **Add ASM accounts for each device group**

When you create multiple ASM/ABM accounts from the Endpoint Management server console, you automatically import groups of Shared iPads:

- Device Group 1 MDM Server > Device Group 1 account
- Device Group 2 MDM Server > Device Group 2 account
- Device Group N MDM Server > Device Group N account

Requirements specific to Shared iPads are as follows:

- One ASM/ABM account for each device group with these settings enabled:
  - **Require device enrollment**
  - **Supervised mode**
  - **Shared mode**
- For a given educational organization, be sure to use the same **Education suffix** for all ASM accounts.

### Apps for Shared iPads

Shared iPads support assignment of device-based volume purchase apps. Before deploying an app on a Shared iPad, Endpoint Management sends a request to the Apple volume purchase server to assign volume purchase licenses to the devices. To check the volume purchase assignments, go to **Configure > Apps > iPad** and expand **Volume Purchase**.

### Media for Shared iPads

Shared iPads support assignment of user-based volume purchase iBooks. Before deploying iBooks on a Shared iPad, Endpoint Management sends a request to the Apple volume purchase server to assign volume purchase licenses to users. To check the volume purchase assignments, go to **Configure > Media > iPad** and expand **Volume Purchase**.

The screenshot displays the configuration page for an iBook on an iPad. The left sidebar shows the navigation menu with 'iPad' selected under 'Media'. The main content area is divided into three sections:

- Deployment Rules:** Shows a rule configuration for deployment. The 'Deploy when' section is set to 'All conditions are met'. The rule criteria include:
  - Deploy this resource by device model: only iPad
  - Device operating system version: is greater than or equal to 9.3
  - Supervised: True
  - Apple Deployment Program account name: only ASM Automated Device Enrollment
- Volume Purchase:** Shows configuration for volume purchase. The 'Volume purchase License' is set to 'Use Volume purchase company token' and the 'Volume purchase Account' is set to 'test'.
- Volume purchase ID Assignment:** A table showing license usage. The table has columns for License ID, Usage Status, and Associated User. Two licenses are listed, both with a status of 'Used'.
 

License ID	Usage Status	Associated User
7545903139	Used	[Redacted]
7545903138	Used	[Redacted]

At the bottom right, there are 'Back' and 'Next >' buttons. A 'License Usage: 2 of 5' indicator is also visible.



### Deployment rules for Shared iPads

For Shared iPad deployment, the rules at the delivery group level don't apply because they relate to user properties. To filter the policies, apps, and media for each group of devices: Add a deployment rule for the resources based on the account name. For example:

- For the Device Group 1 account, set this deployment rule:

```
1 Apple Deployment Program account name
2 Only
3 Device Group 1 account
4
5 <!--NeedCopy-->
```

- For the Device Group 2 account, set this deployment rule:

```
1 Apple Deployment Program account name
2 Only
3 Device Group 2 account
4
5 <!--NeedCopy-->
```

- For the Device Group N account, set this deployment rule:

```
1 Apple Deployment Program account name
2 Only
3 Device Group N account
4
5 <!--NeedCopy-->
```

Calendar	True	True	True	True	True	True	None
Mail	True	True	True	True	True	True	None
Maps	True	True	True	True	True	True	None
Wallet	True	True	True	True	True	True	None

To deploy the Apple Classroom app only to device owners (using unshared iPads), filter the resources by ASM shared status with these deployment rules:

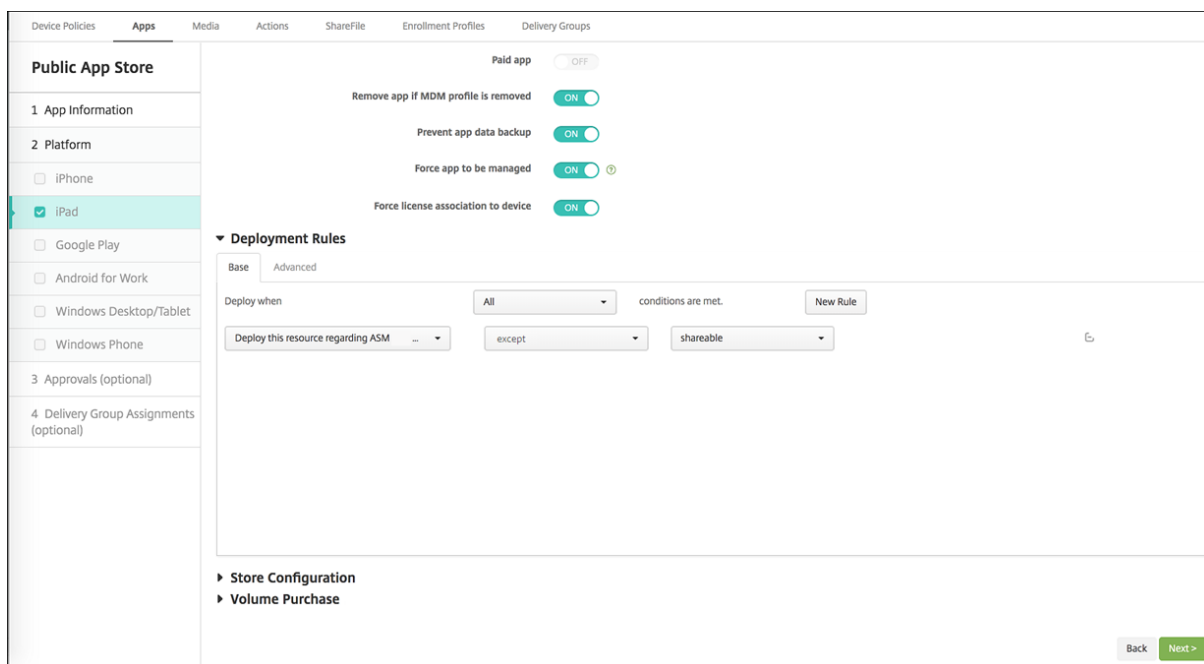
```

1 Deploy this resource regarding ASM/ABM shared mode
2 only
3 unshared
4
5 <!--NeedCopy-->
    
```

Or:

```

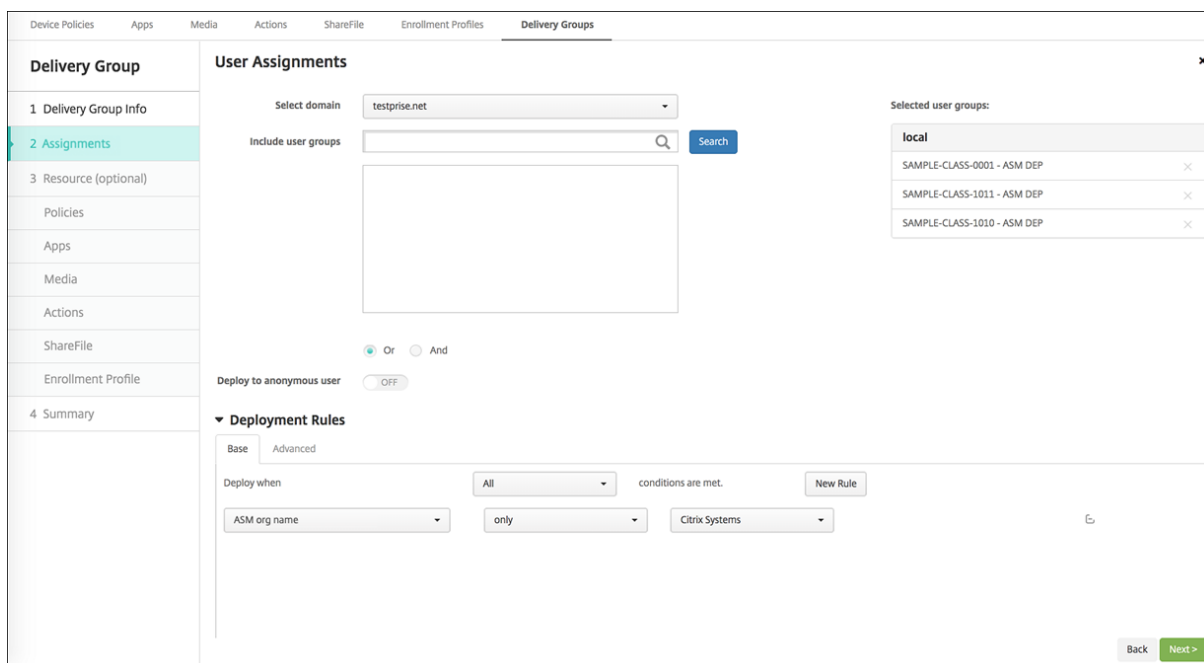
1 Deploy this resource regarding ASM/ABM shared mode
2 except
3 shareable
4
5 <!--NeedCopy-->
    
```



### Delivery groups for Shared iPads

For the device group:

- Configure one delivery group. For instructors, assign all the classes that the Education Configuration policy defines.



- That delivery group must include these MDM resources:
  - Device policies:

- \* Education Configuration (for ASM)
- \* Lock Screen Message
- \* Apps Notifications
- \* Home Screen Layout
- \* Restrictions
- \* Maximum Resident Users
- \* Passcode Lock Grace Period
- Required volume purchase apps
- Required volume purchase iBooks

The screenshot displays the 'Delivery Groups' configuration page in the Citrix Endpoint Management console. The left sidebar shows a navigation menu with options: Device Policies, Apps, Media, Actions, ShareFile, Enrollment Profiles, and Delivery Groups. The main content area is titled 'Summary' and includes a sub-section 'General' with the following details:

- Name:** iOS Education DG
- Description:** (empty)
- User:** Include local user groups: local\SAMPLE-CLASS-1011 - ASM, local\SAMPLE-CLASS-0001 - ASM, local\SAMPLE-CLASS-1010 - ASM
- Resource:** Logic: OR

Below the 'Resource' section, there are several categories of resources assigned to the delivery group:

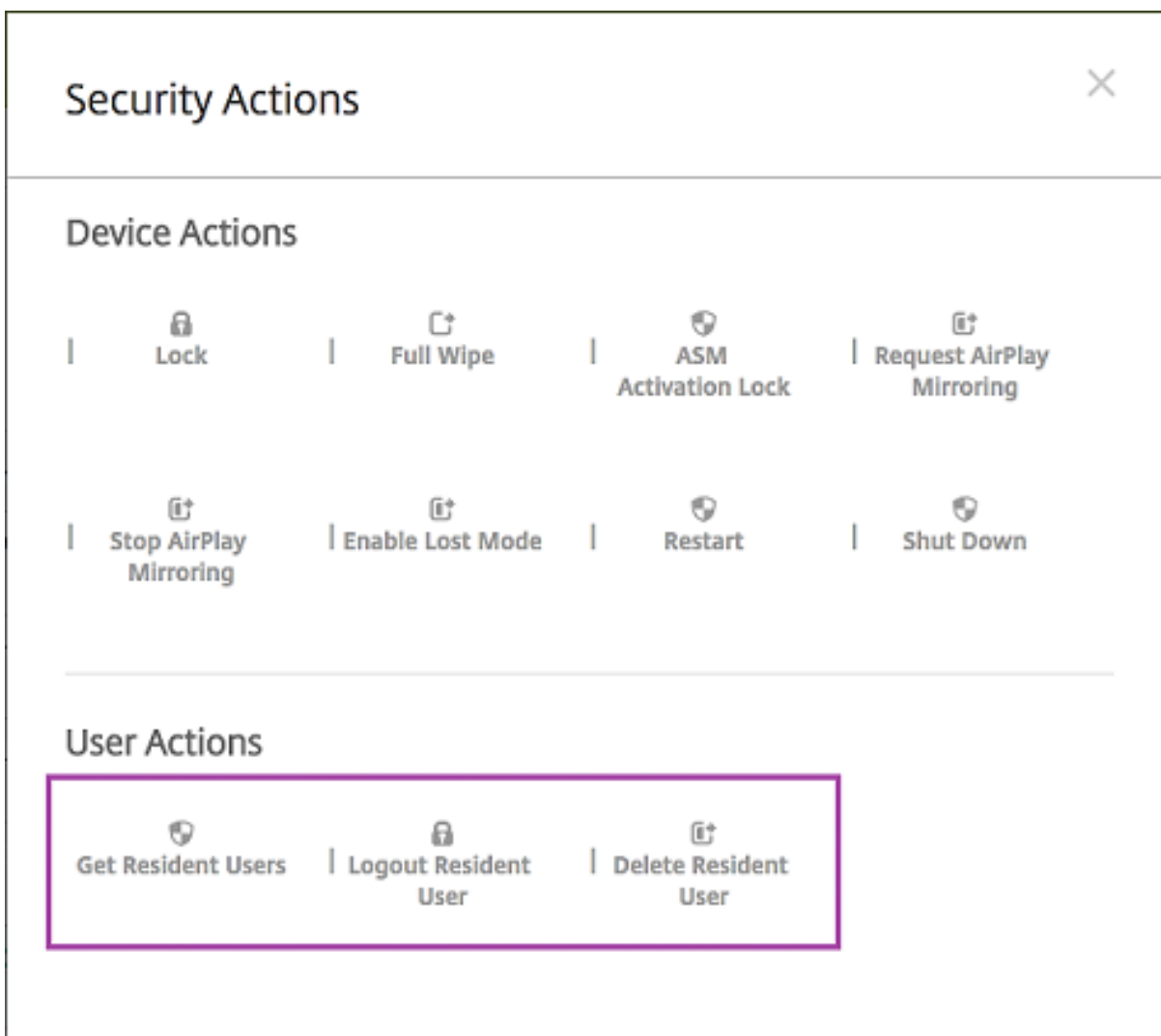
- Policies (7):** DEP Software Inventory, Test 1 HSL, Test 1 Notifications, SAMPLE CLASS 0001 Restrictions, Test Maximum Resident Users, ASM DEP Edu Config, Test Passcode Lock Grace Period.
- Apps (2):** MY LITTLE PONY: MAGIC PRINCESS - ASM, Classroom - ASM.
- Media (2):** Rome - ASM, The Spider Diaries, Book 1: The Eight-leg... - ASM.
- Actions (0):** (None listed)
- ShareFile:** Disabled
- Enrollment Profile:** Global

At the bottom right of the configuration area, there are 'Back' and 'Save' buttons. A 'Deployment Order' button is also visible in the top right corner of the main content area.

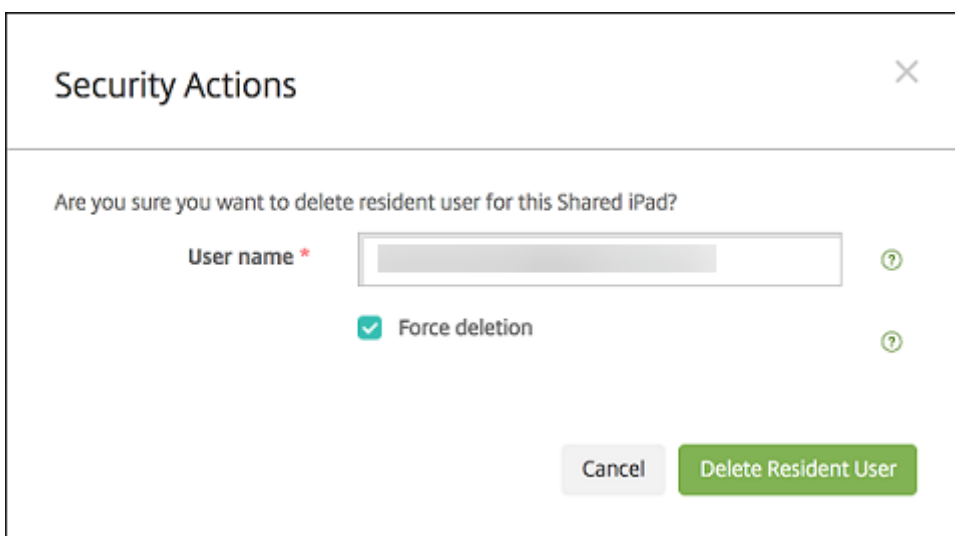
## Security actions for Shared iPads

In addition to existing security actions, you can use these security actions for Shared iPads:

- **Get Resident Users:** Lists the users that have active accounts on the current device. This action forces a sync between the device and the Endpoint Management console.
- **Logout Resident User:** Forces a log out of the current user.
- **Delete Resident User:** Deletes the current session for a specific user. The user can sign in again.
- **Delete All Users:** Deletes all users on the device.



After you click **Delete Resident User**, you can specify the user name.



Results of security actions appear on the **Manage > Devices > General** and **Manage > Devices > Delivery Groups** pages.

### Get information about Shared iPads

Find information specific to Shared iPads on the **Manage > Devices** page:

- Look up:
  - Whether a device is shared (**ASM/ABM shared**)
  - Who is logged in to the shared device (**ASM/ABM logged-in user**)
  - All users assigned to the shared device (**ASM/ABM resident users**)

The screenshot shows the 'Devices' page with a search bar and a table of device details. The table has the following columns: Serial number, Device platform, Operating system version, Device model, ASM device type, ASM shared, ASM logged-in user, and ASM resident users. A single device is listed with the following details:

Serial number	Device platform	Operating system version	Device model	ASM device type	ASM shared	ASM logged-in user	ASM resident users
leid.citrix.com leid.citrix.com*	iOS	11.2.2	iPad	Instructor	Yes	[Redacted]	[Redacted]

- Filter the device list by its **ASM/ABM Device Status**:

The screenshot shows the 'Devices' page with a left-hand filter pane. The 'ASM Device Status' filter is expanded, showing 'ASM shared' selected with a count of 1. The main table displays the following device details:

platform	Operating system version	Device model	ASM device type	ASM shared	ASM logged-in user	ASM resident users
	11.2.2	iPad	Instructor	Yes	[Redacted]	[Redacted]

- View details about the user logged in to a Shared iPad, on the **Manage > Devices > Logged-in User Properties** page.

Devices Users Enrollment Invitations

**Device details** | iPad

- 1 General
- 2 Properties
- 3 User Properties
- 4 Logged-in User Properties**
- 5 Assigned Policies
- 6 Apps
- 7 Media
- 8 Actions
- 9 Delivery Groups
- 10 iOS Profiles
- 11 iOS Provisioning Profiles
- 12 Certificates
- 13 Connections
- 14 MDM Status

**User Properties**

User name:

Password:

Role:

Membership:

- local\Android Default Group [Manage Groups](#)
- local\Android SD Enroller Group
- local\Android SD Group
- local\Apple Configurator Group
- local\CWC GRP

VPP Accounts:

- ASM VPP [Retire](#)

[Back](#) [Next >](#)

Devices Users Enrollment Invitations

**Device details**

- 1 General
- 2 Properties
- 3 User Properties
- 4 Logged-in User Properties**
- 5 Assigned Policies
- 6 Apps
- 7 Media
- 8 Actions
- 9 Delivery Groups
- 10 iOS Profiles
- 11 iOS Provisioning Profiles
- 12 Certificates
- 13 Connections
- 14 MDM Status

**- User Properties** [Add](#)

ASM DEP org name	Citrix Systems
ASM person title	Student
ASM person unique ID	<input type="text"/>
Name	Brayden Anderson
ASM source system ID	S25-008
ASM person status	Active
First name	Brayden
ASM person ID	SAMPLE-STUDENT-0008
ASM managed Apple ID	<input type="text"/>
Surname	Anderson
ASM student grade	4
ASM passcode type	four
ASM data source	SFTP

[Back](#) [Next >](#)

- See the channel used to deploy resources to device owners and users in a delivery group on the **Manage > Devices > Delivery Groups** page. The **Channel/User** column shows the type (**System** or **User**) and the recipient.

The screenshot shows the 'Device details' page for an iPad. The 'Delivery Groups' section is active, displaying a list of actions. The actions table is as follows:

Status	Action	Channel/User	Date
Failure	NotNow response : Securityinfo MDM command (PARK)		11/30/17 5:48:04 pm
Success	Mobileconfig response : Test 1 Notifications (Profile already installed)		11/30/17 5:48:04 pm
Success	Package deploy end : SAMPLE CLASS 0001 DG		11/30/17 5:48:04 pm
Success	Mobileconfig response : Test 1 HSL (Profile already installed)		11/30/17 5:48:04 pm
Success	Mobileconfig response : SAMPLE CLASS 0001 Restrictions (Profile already installed)		11/30/17 5:48:03 pm
Success	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster (Installed)		11/30/17 4:51:22 pm
Success	Installation result : Rome (Installed)		11/30/17 4:51:22 pm
Done	Software inventory requested		11/30/17 4:50:49 pm
Success	Software inventory response		11/30/17 4:50:49 pm
Done	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster - ASM (Installing)		11/30/17 4:50:49 pm

- Get information about resident users:
  - **Has data to sync:** Whether the user has data to be synchronized to the cloud.
  - **Data quotas:** The data quota set for the user in bytes. A quota might not appear if user quotas are temporarily off or aren't enforced for the user.
  - **Data used:** The amount of data used by the user in bytes. A value might not appear if an error occurs as the system gathers the information.
  - **Is logged in:** Whether the user is logged on to the device.

The screenshot shows the 'Device details' page for an iPad, with the 'Connections' section active. It displays connection statistics and a table of user connections.

Connection Summary:

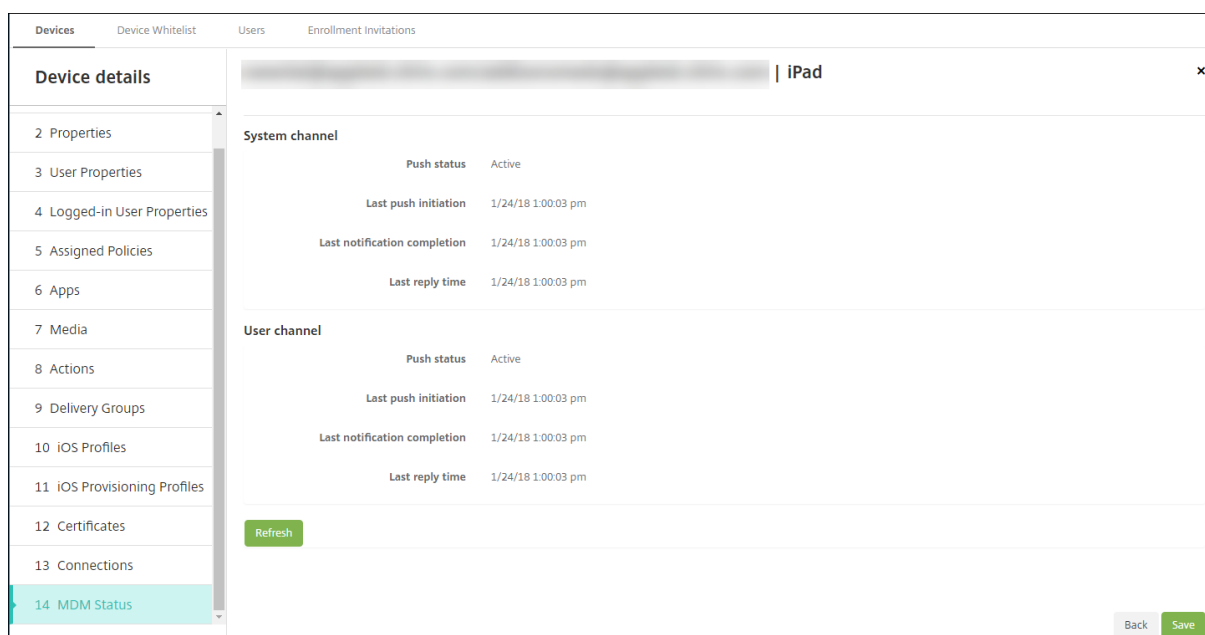
- First connection: 8/30/17 12:42:38 pm
- Status: Active
- Last connection: 11/30/17 5:48:04 pm

User Connections Table:

User name	Penultimate authentication	Last authentication	Has data to sync	Data quota	Data used	Is logged-in
[Redacted]	10/12/17 10:15:34 am	10/12/17 10:19:00 am				
[Redacted]	11/23/17 3:45:28 pm	11/23/17 3:45:29 pm				
[Redacted]	11/23/17 5:48:03 pm	11/23/17 5:48:03 pm				
[Redacted]	11/30/17 5:48:03 pm	11/30/17 5:48:04 pm				
[Redacted]	11/30/17 5:48:03 pm	11/30/17 5:48:04 pm	Yes			Yes
[Redacted]	11/29/17 7:02:32 pm	11/29/17 7:02:32 pm	No		120.82 MB	No

- View the push status for both channels.





## Distribute Apple apps

October 7, 2021

Endpoint Management manages apps deployed to devices. You can organize and deploy the following types of iOS/iPadOS and macOS apps.

- **Public App Store (iOS/iPadOS only):** These apps include free or paid apps available in a public app store, such as the Apple App Store or Google Play. For example, GoToMeeting.
- **Enterprise (iOS/iPadOS/macOS):** Native apps that aren't MDX-enabled and don't contain the policies associated with MDX apps.
- **MDX (iOS/iPadOS only):** Apps prepared with the MAM SDK or wrapped with the MDX Toolkit. These apps include MDX policies. You get MDX apps from internal sources and public stores.
- **Volume purchase (iOS/iPadOS/macOS):** Apps with licenses managed through the Apple volume purchase program.
- **iOS custom apps (iOS/iPadOS only):** Proprietary business-to-business apps developed in-house or by a third-party.

For more information about different types of apps, see [Add apps](#).

Some deployments require an Apple Business Management (ABM) or Apple School Management (ASM) account. See the following sections for more information.

For each type of app and distribution method, Citrix recommends a set of configuration practices. For information about distributing apps for other platforms, see [Add Apps](#). The following sections provide more in depth information for iOS app configuration.

## General steps for app distribution

Scenario	Step 1: Link accounts	Step 2: Add and configure apps	Step 3: Configure delivery groups and deploy apps
Public app store apps, including Citrix mobility apps	Not applicable	<b>In Endpoint Management: Configure &gt; Apps,</b> add <b>Public App Store</b> apps for iPhone or iPad. Configure the apps and assign them to delivery groups.	<b>In Endpoint Management:</b> Configure and deploy apps using delivery groups.
Public app store apps delivered with Apple volume purchase, including Citrix mobility apps	Enroll in an Apple deployment program. <b>In Endpoint Management:</b> Go to <b>Settings &gt; Volume purchase</b> to add your volume purchase account.	<b>In ABM or ASM:</b> Purchase and add apps from Apps and Books. <b>In Endpoint Management:</b> Go to <b>Configure &gt; Apps,</b> configure the apps, and assign them to delivery groups.	<b>In Endpoint Management:</b> Configure and deploy apps using delivery groups.
Enterprise apps	Not applicable	<b>In Endpoint Management:</b> Go to <b>Configure &gt; Apps.</b> Click <b>Add</b> then click <b>Enterprise.</b> Upload the IPA file. Configure the apps and assign them to delivery groups.	<b>In Endpoint Management:</b> Configure and deploy apps using delivery groups.

Scenario	Step 1: Link accounts	Step 2: Add and configure apps	Step 3: Configure delivery groups and deploy apps
MDX apps	Not applicable	<p><b>In Endpoint Management:</b> Go to <b>Configure &gt; Apps</b>. Click <b>Add</b> then click <b>MDX</b>. Ensure that you select <b>iPad/iPhone</b> for the platform. Upload the MDX file. Configure the apps and assign them to delivery groups.</p>	<p><b>In Endpoint Management:</b> Configure and deploy apps using delivery groups.</p>
MDX apps distributed using Apple volume purchase	<p>Enroll in an Apple deployment program. <b>In Endpoint Management:</b> Go to <b>Settings &gt; Volume purchase</b> to add your volume purchase account.</p>	<p><b>In ABM:</b> Purchase and add MDX apps from Apps and Books. Link the app to your ABM account. <b>In Endpoint Management:</b> Go to <b>Configure &gt; Apps</b>, configure the apps, and assign them to delivery groups.</p>	<p><b>In Endpoint Management:</b> Configure and deploy apps using delivery groups.</p>
Custom apps	<p>Enroll in an Apple deployment program. <b>In Endpoint Management:</b> Go to <b>Settings &gt; Volume purchase</b> to add your volume purchase account.</p>	<p><b>In ABM:</b> Add your app to the App Store as a private app. Link the app to your ABM account. <b>In Endpoint Management:</b> Go to <b>Configure &gt; Apps</b>, configure the apps, and assign them to delivery groups.</p>	<p><b>In Endpoint Management:</b> Configure and deploy apps using delivery groups.</p>

Scenario	Step 1: Link accounts	Step 2: Add and configure apps	Step 3: Configure delivery groups and deploy apps
MDX-enabled custom apps	Enroll in an Apple deployment program. <b>In Endpoint Management:</b> Go to <b>Settings &gt; Volume purchase</b> to add your volume purchase account.	<b>In ABM:</b> Add your app to the app store as a private app. Link the app to your ABM account. <b>In Endpoint Management:</b> Go to <b>Configure &gt; Apps</b> and upload the MDX file. Configure the apps and assign them to delivery groups.	<b>In Endpoint Management:</b> Configure and deploy apps using delivery groups.

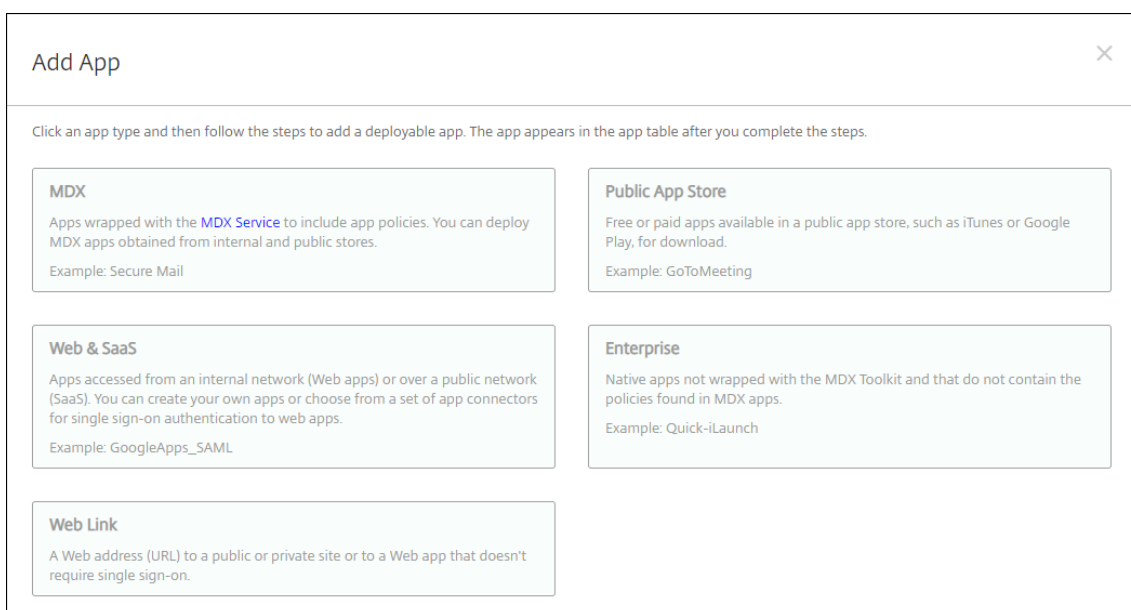
### Public app store apps

You can add free and paid apps available on the App Store to Citrix Endpoint Management.

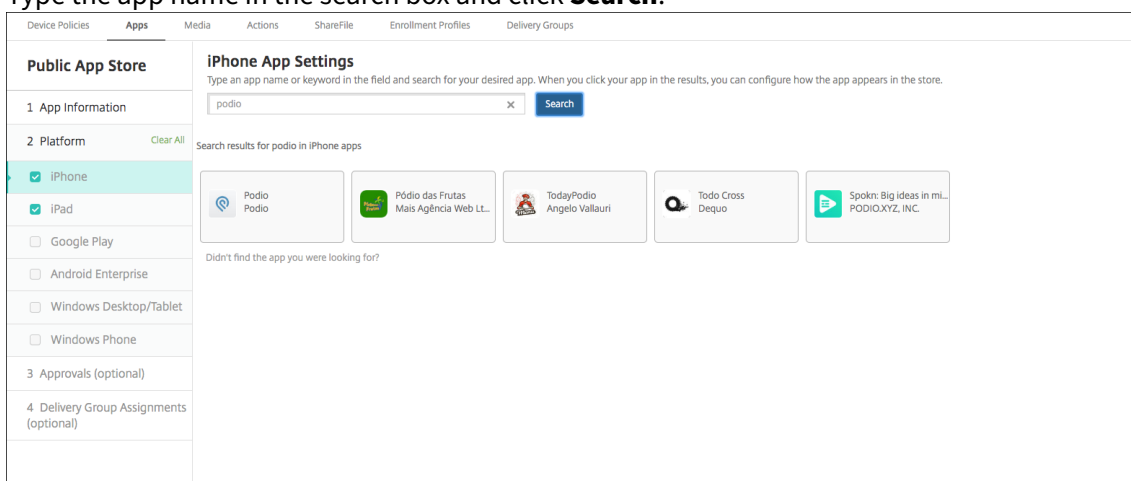
Feature availability	
Requires device supervision	No
Available for user enrollment mode	No
Available on	iOS/iPadOS

#### Step 1: Add and configure apps

1. In the Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.
2. Click **Public App Store**.



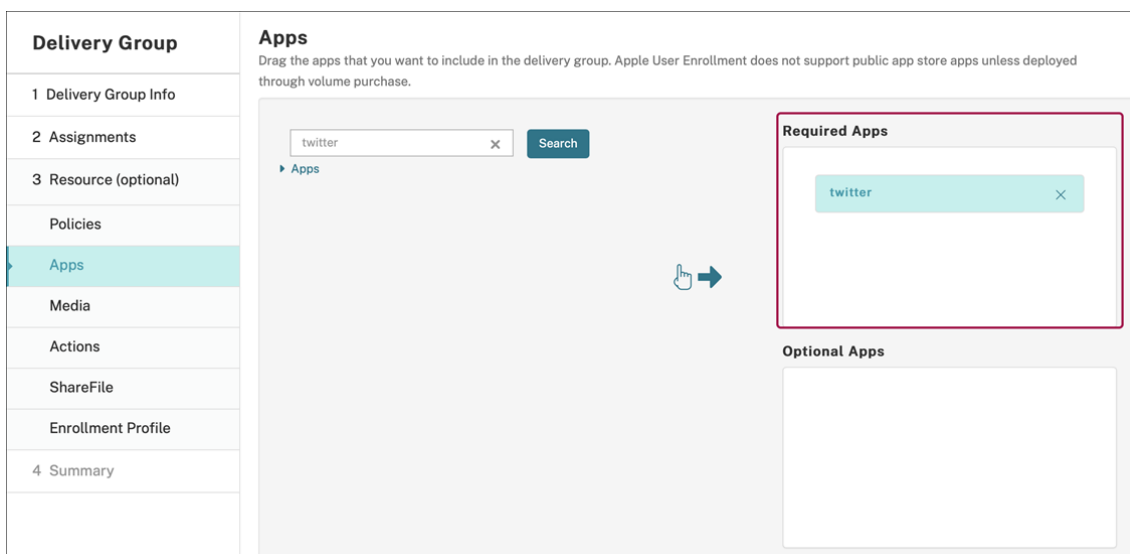
3. Select **iPhone** or **iPad** for platforms
4. Type the app name in the search box and click **Search**.



5. Apps matching the search criteria appear. Click the desired app.
6. Assign a delivery group to the app and click **Save**.

## Step 2: Configure app deployment

1. In the Endpoint Management console, navigate to **Configure > Apps**.
2. Select the app you want to configure and click **Edit**.
3. Citrix recommends enabling the **Force app to be managed** feature.
4. Assign any delivery groups and click **Save**.
5. Navigate to **Configure > Delivery Groups** and click **Add**.
6. In the **Apps** section, drag the desired apps to the **Required Apps** box.



7. Navigate back up to **Configure > Delivery Groups**.
8. Select the delivery group and click **Deploy**.
9. Users receive a request to install the app and the app installs in the background after they accept.



## Public app store apps delivered with Apple volume purchase

You can manage iOS/iPadOS app licenses through the Apple volume purchase program. Follow these steps to add volume purchase apps to Endpoint Management.

---

### Feature availability

---

Requires device supervision	No
Available for user enrollment mode	Yes
Available on	iOS/iPadOS/macOS

---

### Step 1: Link accounts

1. Set up and enroll in Apple Business Manager (ABM) or Apple School Manager (ASM). For more information about these programs, see [Apple documentation](#).
2. Link your ABM/ASM account with Endpoint Management. For more information on linking volume purchase accounts, see [Apple Volume Purchase](#).
3. When you add your volume purchase account, enable **App Auto Update**. This setting ensures that apps on user devices automatically update when an update appears in the Apple store. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens regardless of whether the app is required or optional.

To use the **Force app to be managed** and **App Auto Update** settings, enable the `apple.app.force.managed` server property. See [Server properties](#).

### Step 2: Get apps and licenses from Apple

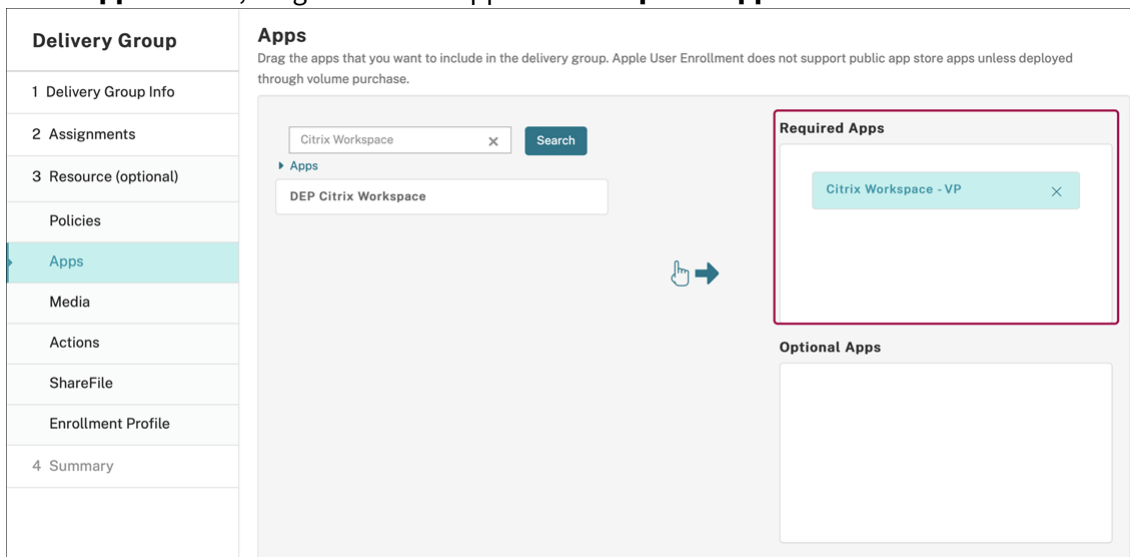
Purchase apps on your ABM/ASM account. You can make purchases in Apple Books (for iOS/iPadOS only) and the Apple App Store. Keep in mind that you must purchase all apps, even if they are free. Once you purchase licenses on ABM/ASM, Endpoint Management shows the app automatically.

For information about how to make apps available to your business, see [Apple documentation](#).

### Step 3: Configure app deployment

1. In the Endpoint Management console, navigate to **Configure > Apps**.
2. Select the volume purchase app you want to configure and click **Edit**.
3. Select the platforms: **iPhone**, **iPad**, or **macOS**.
4. Citrix recommends enabling the **Force app to be managed** feature (iOS/iPadOS only).
5. Assign any delivery groups and click **Save**.

6. Navigate to **Configure > Delivery Groups** and click **Add**.
7. In the **Apps** section, drag the desired apps to the **Required Apps** box.



8. Navigate back to **Configure > Delivery Groups**.
9. Select the delivery group and click **Deploy**.
10. Users receive a request to install the app and the app installs in the background after they accept.





## Enterprise apps

You can also add native apps that don't have any MDX policies associated with them. Follow these steps to add apps that don't exist on the App Store.

### Feature availability

Requires device supervision	No
Available for user enrollment mode	Yes
OS	iOS/iPadOS/macOS

### Step 1: Add and configure apps

1. In the Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.
2. Click **Enterprise**.

Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

**MDX**

Apps wrapped with the [MDX Service](#) to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: Secure Mail

**Public App Store**

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

**Web & SaaS**

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps\_SAML

**Enterprise**

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

**Web Link**

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. On the **App information** page, configure the following:
  - **Name:** Type a descriptive name for the app. The name appears under App Name on the Apps table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app.
4. Click **Next**. The **App Platforms** page appears.
5. Select the platforms: **iPhone**, **iPad**, or **macOS**.
6. Upload the IPA file (iOS/iPadOS) or upload the PKG file (macOS)

7. Click **Next**. The **App details** page appears.

8. Configure these settings:

- **File name:** Optionally, type a new name for the app.
- **App description:** Optionally, type a new description for the app.
- **App version:** You can't change this field.
- **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
- **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
- **Excluded devices:** Optionally, type the manufacturer or models of devices that cannot run the app.
- **Remove app if MDM profile is removed:** Select whether to remove the app from a device when the MDM profile is removed. The default is On. (iOS/iPadOS only)
- **Prevent app data backup:** Select whether to prevent the app from backing up data. The default is On. (iOS/iPadOS only)
- **Force app to be managed:** If you install an unmanaged app, select **On** if you want users on unsupervised devices see a prompt to allow management of the app. If they accept the prompt, the app is managed. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens regardless of whether the app is required or optional. (iOS/iPadOS only)

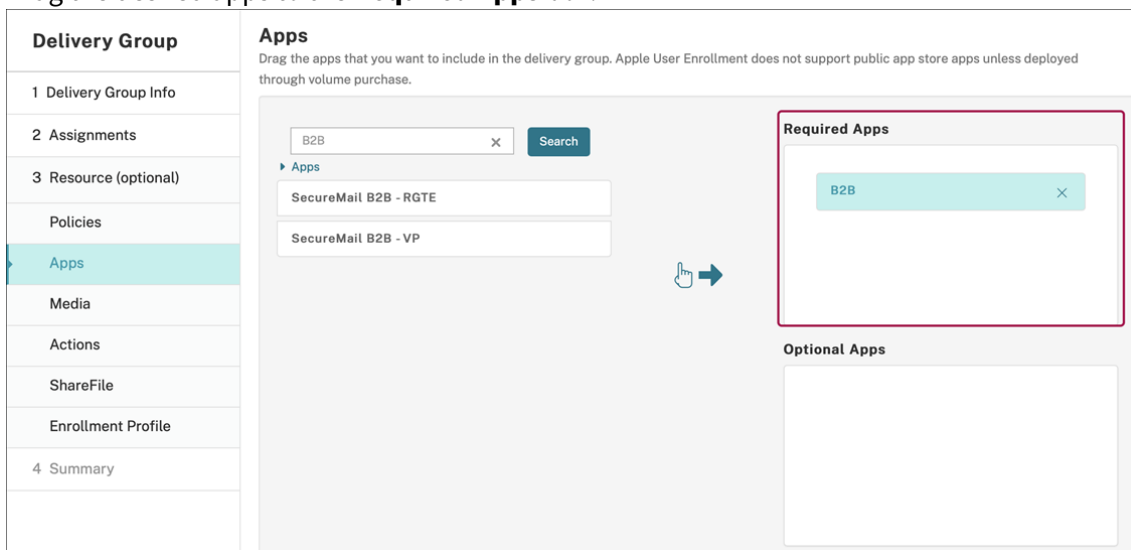
To use the **Force app to be managed** and **App Auto Update** settings, enable the `apple.app.force.managed` server property. See [Server properties](#).

Enterprise	iOS Enterprise App
1 App Information	Upload an .ipa file <input type="button" value="Upload"/>
2 Platform	App name * <input type="text" value="Hello Cordova"/>
<input checked="" type="checkbox"/> iOS	Description * <input type="text" value="Hello Cordova"/>
<input type="checkbox"/> macOS	App version <input type="text" value="2.0.0"/>
<input type="checkbox"/> Android (legacy DA)	Minimum OS version <input type="text" value="8.0"/>
<input type="checkbox"/> Samsung KNOX	Maximum OS version <input type="text"/>
<input type="checkbox"/> Android Enterprise	Excluded devices <input type="text" value="example: manufacturer or model, ..."/>
<input type="checkbox"/> Windows Phone	Package ID <input type="text" value="com.citrix.hellocordova"/>
<input type="checkbox"/> Windows Desktop/Tablet	Remove app if MDM profile is removed <input checked="" type="checkbox"/>
<input type="checkbox"/> Workspace Hub	
3 Approvals (optional)	

9. Assign a delivery group to the app and click **Save**.

## Step 2: Configure app deployment

1. In the Endpoint Management console, navigate to **Configure > Delivery Groups**. Select the delivery group to configure and click the **Apps** page.
2. Drag the desired apps to the **Required Apps** box.



3. Navigate to **Configure > Delivery Groups**.
4. Select the delivery group and click **Deploy**.
5. Users receive a request to install the app and the app installs in the background after they accept.



## MDX apps

To use MDX policies and security features, add apps that are MAM SDK enabled or MDX-wrapped. You can deploy MDX apps using volume purchase or without it.

---

### Feature availability

Requires device supervision	No
Available for user enrollment mode	Yes
Available On	iOS/iPadOS

---

To add the MDX version of a public app store app, follow the steps under Public app store apps, and then follow the steps in this section.

### Step 1: Add and configure apps

1. In the Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.
2. Click **MDX**.

### Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

**MDX**

Apps wrapped with the [MDX Service](#) to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: Secure Mail

**Public App Store**

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

**Web & SaaS**

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps\_SAML

**Enterprise**

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

**Web Link**

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Select **iPhone** or **iPad** for platforms.
4. Upload the MDX file.
5. Configure the app details. Set **App deployed via Volume purchase** to **Off**. Citrix also recommends enabling the **Force app to be managed** feature.

Use the [MDX Service](#) on Citrix Cloud to wrap an app for delivery.

**File name \***

**App Description \***

**App version**

**Package ID**

**Minimum OS version**

**Maximum OS version**

**Excluded devices**

**Remove app if MDM profile is removed**

**Prevent app data backup**

**Force app to be managed**

**App deployed via Volume purchase**

**MDX Policies**

Authentication

**Device passcode**

6. Configure the MDX policies. Set **Disable required upgrade** to **On**.

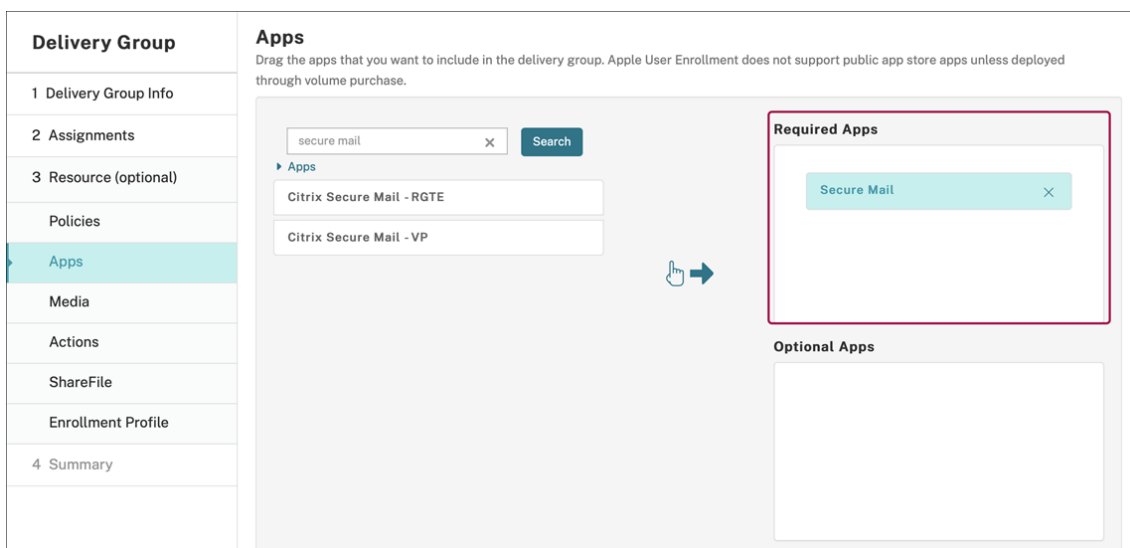
The screenshot shows a configuration page with three main sections: Miscellaneous Access, Encryption, and App Interaction. Each section contains several settings with input fields, toggle switches, or dropdown menus. A question mark icon is present to the right of each setting.

Section	Setting	Value
Miscellaneous Access	Disable required upgrade	ON
	App update grace period (hours)	168
	Erase app data on lock	OFF
	Active poll period (minutes)	60
Encryption	Enable encryption	On
	Database encryption exclusions	
	File encryption exclusions	
App Interaction	Cut and copy	Restricted
	Paste	Unrestricted

7. Assign a delivery group to the app and click **Save**.

### Step 2: Configure app deployment

1. In the Endpoint Management console, navigate to **Configure > Delivery Groups** and click **Add**.
2. In the **Apps** section, drag the desired apps to the **Required Apps** box.



3. Navigate to **Configure > Delivery Groups**.
4. Select the delivery group and click **Deploy**.
5. Users receive a request to install the app and the app installs in the background after they accept.



## MDX apps distributed using Apple volume purchase

To use MDX policies and security features, add apps that are MAM SDK enabled or MDX-wrapped. To deploy apps using volume purchase, the apps must exist on the app store.

---

### Feature availability

---

Requires device supervision	No
Available for user enrollment mode	Yes
Available on	iOS/iPadOS

---

### Step 1: Link accounts

1. Set up and enroll in Apple Business Manager (ABM) or Apple School Manager (ASM). For more information about these programs, see [Apple documentation](#).
2. Link your ABM/ASM account with Endpoint Management. For more information on linking volume purchase accounts, see [Apple Volume Purchase](#).
3. When you add your volume purchase account, enable **App Auto Update**. This setting ensures that apps on user devices automatically update when an update appears in the Apple store. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens regardless of whether the app is required or optional.

To use the **Force app to be managed** and **App Auto Update** settings, enable the `apple.app.force.managed` server property. See [Server properties](#).

### Step 2: Get apps and licenses from Apple

Purchase apps on your ABM/ASM account. You can make purchases in Apple Books (for iOS/iPadOS only) and the Apple App Store. Keep in mind that you must purchase all apps, even if they are free. Once you purchase licenses on ABM/ASM, Endpoint Management shows the app automatically.

For information about how to make apps available to your business, see [Apple documentation](#).

### Step 3: Add and configure apps

1. In the Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.
2. Click **MDX**.



### Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

**MDX**

Apps wrapped with the [MDX Service](#) to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: Secure Mail

**Public App Store**

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

**Web & SaaS**

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps\_SAML

**Enterprise**

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

**Web Link**

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Select **iPhone** or **iPad** for platforms.
4. Upload the MDX file.
5. Configure the app details. Set **App deployed via Volume purchase** to **On**. Citrix also recommends enabling the **Force app to be managed** feature.

**File name \***

**App Description \***

**App version**

**Package ID**

**Minimum OS version**

**Maximum OS version**

**Excluded devices**

**Remove app if MDM profile is removed**

**Prevent app data backup**

**Force app to be managed**  ⓘ

**App deployed via Volume purchase**  ⓘ

**▼ MAM SDK Policies**

**Authentication**

**Device passcode**  ⓘ

6. Configure the MDX policies. Set **Disable required upgrade** to **On**.

The screenshot displays the configuration interface for MDX policies, organized into three sections:

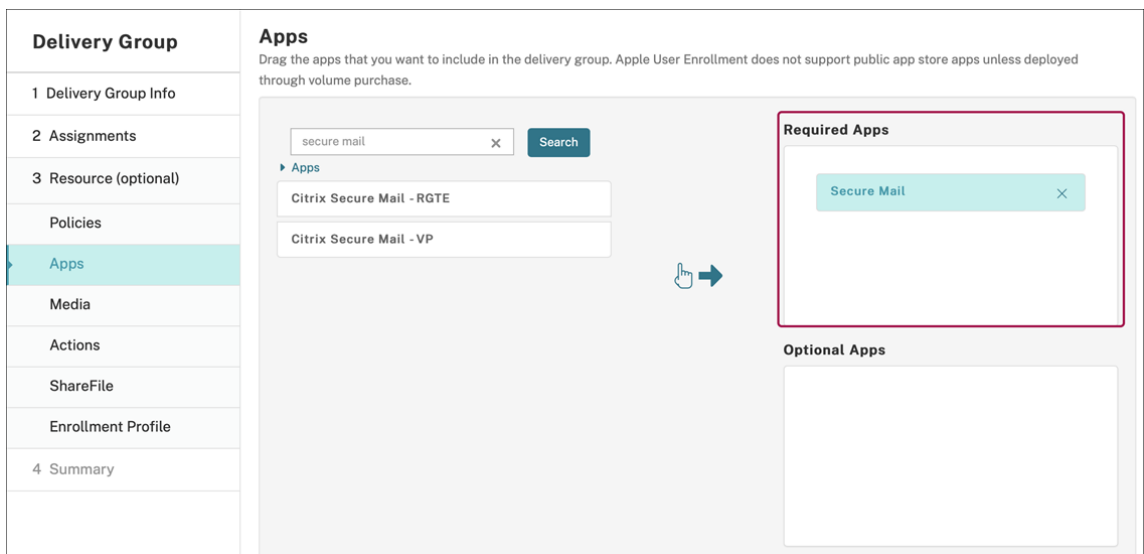
- Miscellaneous Access:**
  - Disable required upgrade:** A toggle switch is set to **ON**.
  - App update grace period (hours):** A text input field contains the value **168**.
  - Erase app data on lock:** A toggle switch is set to **OFF**.
  - Active poll period (minutes):** A text input field contains the value **60**.
- Encryption:**
  - Enable encryption:** A dropdown menu is set to **On**.
  - Database encryption exclusions:** An empty text input field.
  - File encryption exclusions:** An empty text input field.
- App Interaction:**
  - Cut and copy:** A dropdown menu is set to **Restricted**.
  - Paste:** A dropdown menu is set to **Unrestricted**.

7. Assign a delivery group to the app for each platform and click **Save**.

This configuration results in two entries listed for this app in the apps list. When you select an app to configure, select the app with **Type MDX**.

#### Step 4: Configure app deployment

1. In the Endpoint Management console, navigate to **Configure > Delivery Groups** and click **Add**.
2. In the **Apps** section, drag the desired MDX apps to the **Required Apps** box.



3. Navigate to **Configure > Delivery Groups**.
4. Select the delivery group and click **Deploy**.
5. Users receive a request to install the app and the app installs in the background after they accept.



## Custom apps

Custom apps are proprietary business-to-business apps. You can use Endpoint Management and Apple volume purchase to distribute proprietary apps privately and securely. You can distribute the apps to specific partners, clients, franchisees, and internal employees.

---

### Feature availability

---

Requires device supervision	No
Available for user enrollment mode	Yes
Available on	iOS/iPadOS

---

## Requirements for custom apps

- Apple Business Manager or Apple School Manager account
- Apple volume purchase account (requires devices with iOS 7 or later)
- Enroll devices in Endpoint Management, using one of the following Apple enrollment modes:
  - Automated Device Enrollment
  - Device enrollment
  - User enrollment

## Step 1: Link accounts

To deploy custom apps using volume purchase, link your volume purchase account to Endpoint Management.

1. Set up and enroll in Apple Business Manager (ABM). For more information about these programs, see [Apple documentation](#).
2. Link your ABM account with Endpoint Management. For more information on linking volume purchase accounts, see [Apple Volume Purchase](#).
3. When you add your volume purchase account, enable **App Auto Update**. This setting ensures that apps on user devices automatically update when an update appears in the Apple store. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens regardless of whether the app is required or optional.

To use the **Force app to be managed** and **App Auto Update** settings, enable the `apple.app.force.managed` server property. See [Server properties](#).

## Step 2: Configure apps on ABM

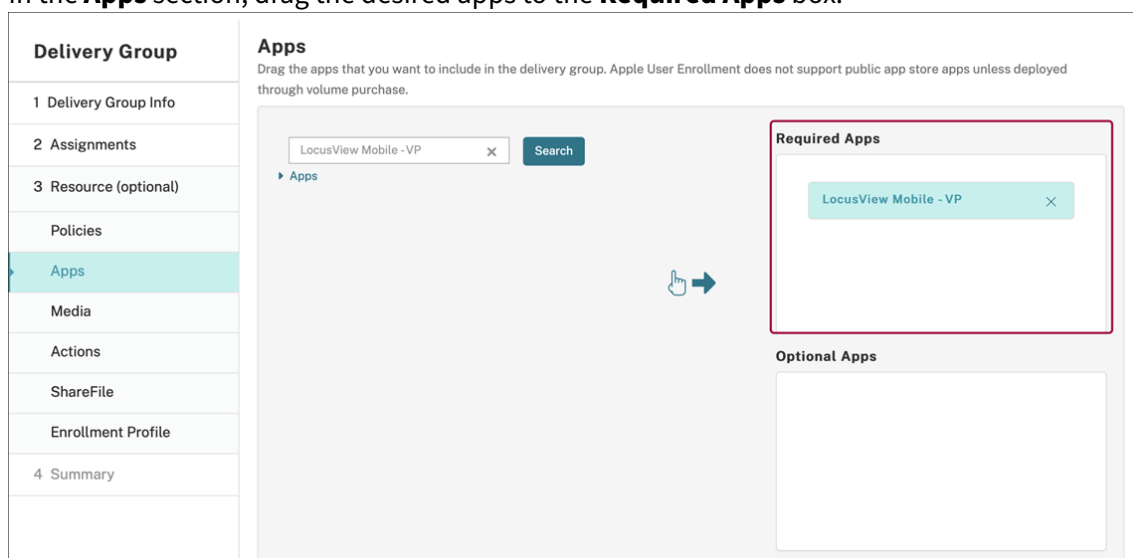
Add apps on your ABM account. You can upload and distribute your own custom apps or buy licenses for custom apps from other organizations. For more information on adding and enabling custom apps on ABM, see [Apple documentation](#).

## Step 3: Add and configure apps in Endpoint Management

1. In the Endpoint Management console, navigate to **Configure > Apps**. Volume purchase apps appear in the list of apps.
2. Select the app you want to configure. Click **Edit**.
3. Select the platforms: **iPhone, iPad, or macOS**.
4. Choose the delivery groups to which you want the app distributed. Click **Save**.

## Step 4: Configure app deployment

1. In the Endpoint Management console, navigate to **Configure > Delivery Groups** and click **Add**.
2. In the **Apps** section, drag the desired apps to the **Required Apps** box.



3. Navigate back to **Configure > Delivery Groups**.
4. Select the delivery group you want deployed and click **Deploy**.
5. Users receive a request to deploy apps. Apps install in the background after users accept them.



### MDX enabled custom apps

To use MDX policies and security features, add custom apps that are MAM SDK enabled or MDX-wrapped.

---

#### Feature availability

Requires device supervision	No
Available for user enrollment mode	Yes
Available on	iOS/iPadOS

### Step 1: Link accounts

To deploy custom apps using volume purchase, link your volume purchase account to Endpoint Management.

1. Set up and enroll in Apple Business Manager (ABM). For more information about these programs, see [Apple documentation](#).
2. Link your ABM account with Endpoint Management. For more information on linking volume

purchase accounts, see [Apple Volume Purchase](#).

3. When you add your volume purchase account, enable **App Auto Update**. This setting ensures that apps on user devices automatically update when an update appears in the Apple store. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens regardless of whether the app is required or optional.

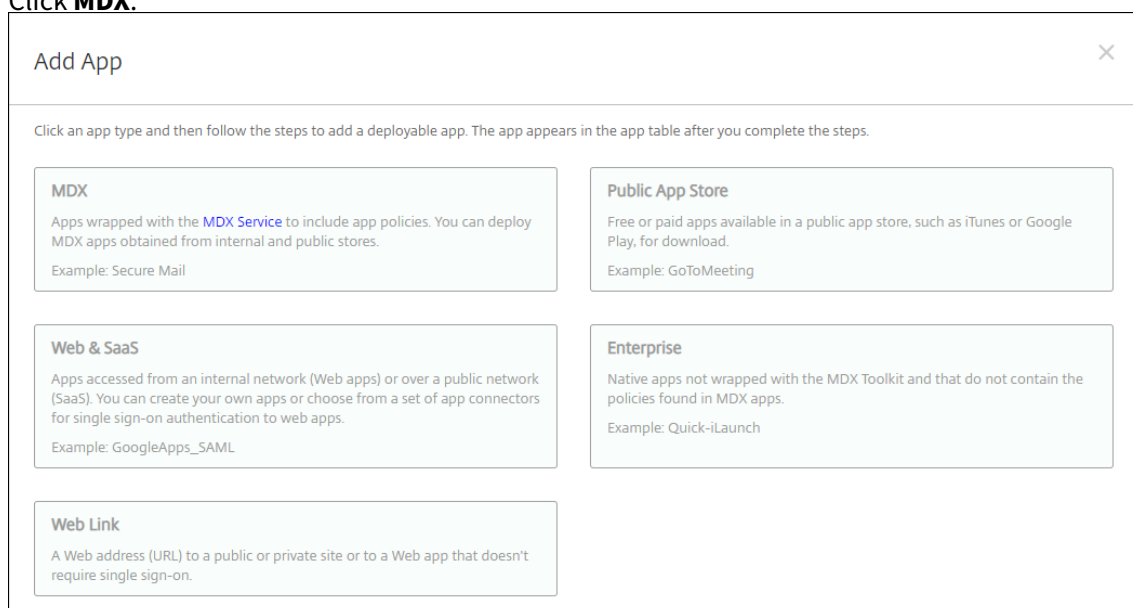
To use the **Force app to be managed** and **App Auto Update** settings, enable the `apple.app.force.managed` server property. See [Server properties](#).

## Step 2: Configure apps on ABM

Add apps on your ABM account. You can upload and distribute your own custom apps or buy licenses for custom apps from other organizations. For more information on adding and enabling custom apps on ABM, see [Apple documentation](#).

## Step 3: Add and configure apps in Endpoint Management

1. In the Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.
2. Click **MDX**.



3. Select the **iPhone** or **iPad** platforms.
4. Upload the MDX file for the app you want to add.
5. Configure the app details. Set **App deployed via Volume purchase** to **On**. Citrix also recommends enabling the **Force app to be managed** feature.

<b>File name *</b>	<input type="text" value="Secure Mail"/>
<b>App Description *</b>	<input type="text" value="Managed Enterprise Application"/>
<b>App version</b>	<input type="text" value="19.3.5"/>
<b>Package ID</b>	<input type="text" value="XGFUKY3NSP.com.citrix.mail.ios"/>
<b>Minimum OS version</b>	<input type="text" value="10.0"/>
<b>Maximum OS version</b>	<input type="text"/>
<b>Excluded devices</b>	<input type="text" value="example: manufacturer or model, ..."/>
<b>Remove app if MDM profile is removed</b>	<input checked="" type="checkbox"/>
<b>Prevent app data backup</b>	<input checked="" type="checkbox"/>
<b>Force app to be managed</b>	<input checked="" type="checkbox"/>
<b>App deployed via Volume purchase</b>	<input checked="" type="checkbox"/>
<b>▼ MAM SDK Policies</b>	
Authentication	
<b>Device passcode</b>	<input type="checkbox"/>

6. Configure the MDX policies. Set **Disable required upgrade** to **On**.



**Miscellaneous Access**

**Disable required upgrade**  ON ⓘ

**App update grace period (hours)**  ⓘ

**Erase app data on lock**  OFF ⓘ

**Active poll period (minutes)**  ⓘ

**Encryption**

**Enable encryption**  ⓘ

**Database encryption exclusions**  ⓘ

**File encryption exclusions**  ⓘ

**App Interaction**

**Cut and copy**  ⓘ

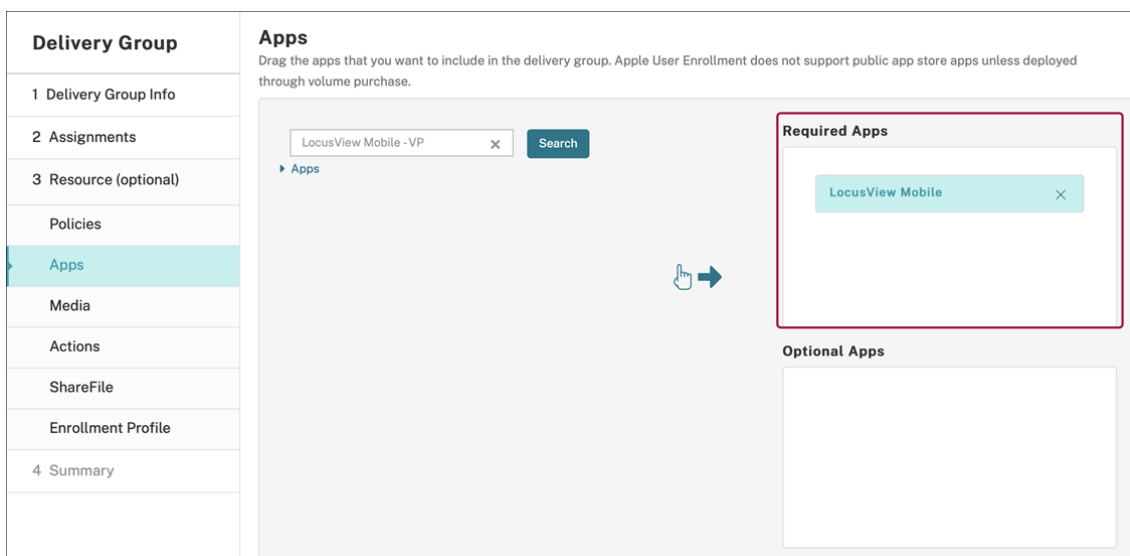
**Paste**  ⓘ

7. Assign a delivery group to the app and click **Save**.

This configuration results in two entries listed for this app in the apps list. When you select an app to configure, select the app with **Type MDX**.

#### Step 4: Configure app deployment

1. In the Endpoint Management console, navigate to **Configure > Apps**. Volume purchase apps appear in the list of apps.
2. Select the app you want to configure. Click **Edit**.
3. Choose the delivery groups to which you want the app distributed on each platform. Click **Save**.
4. Navigate to **Configure > Delivery Groups** and click **Add**.
5. In the **Apps** section, drag the desired MDX apps to the **Required Apps** box.



6. Navigate back to **Configure > Delivery Groups**.
7. Select the delivery group you want deployed and click **Deploy**.
8. Users receive a request to deploy apps. Apps install in the background after they accept.

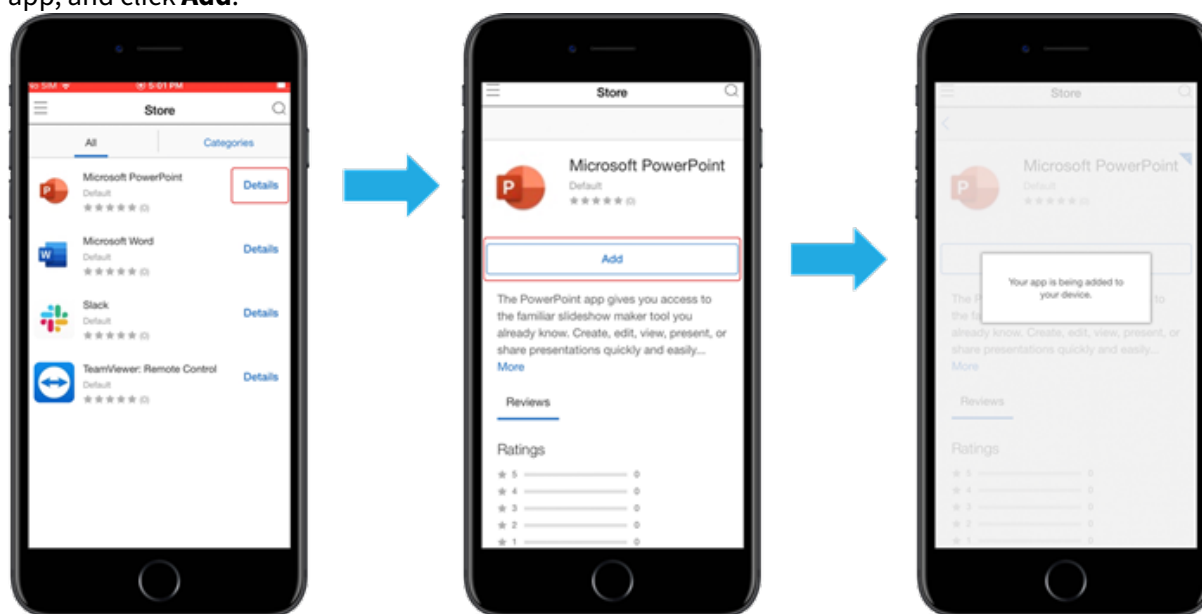


### Optional apps (iOS/iPadOS only)

Citrix recommends deploying apps as **Required**. Required apps install silently on user devices, minimizing interaction. Having this feature enabled also allows apps to update automatically.

Optional apps allow users to choose what apps to install, but users must initiate the installation manually through Secure Hub.

To install optional apps, users must launch Secure Hub, go to **Store**, select **Details** for the desired app, and click **Add**.



## Network Access Control

April 28, 2021

You can use your Network Access Control (NAC) solution to extend the Endpoint Management device security assessment for Android and Apple devices. Your NAC solution uses the Endpoint Management security assessment to facilitate and handle authentication decisions. After you configure your NAC appliance, the device policies and NAC filters that you configure in Endpoint Management get enforced.

Using Endpoint Management with a NAC solution adds QoS and more granular control over devices that are internal to your network. For a summary of the advantages of integrating NAC with Endpoint Management, see [Access control](#).

Citrix supports these solutions for integration with Endpoint Management:

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

Citrix doesn't guarantee integration for other NAC solutions.

With a NAC appliance in your network:

- Endpoint Management supports NAC as an endpoint security feature for iOS, Android Enterprise, and Android devices.
- You can enable filters in Endpoint Management to set devices as compliant or non-compliant for NAC, based on rules or properties. For example:
  - If a managed device in Endpoint Management doesn't meet the specified criteria, Endpoint Management marks the device as non-compliant. A NAC appliance blocks non-compliant devices on your network.
  - If a managed device in Endpoint Management has non-compliant apps installed, a NAC filter can block the VPN connection. As a result, a non-compliant user device cannot access apps or websites through the VPN.
  - If you use Citrix Gateway for NAC, you can enable split tunneling to prevent the Citrix Gateway plug-in from sending unnecessary network traffic to Citrix Gateway. For more information on split tunneling, see [Configuring Split Tunneling](#).

### Supported NAC compliance filters

Endpoint Management supports the following NAC compliance filters:

**Anonymous Devices:** Checks if a device is in anonymous mode. This check is available if Endpoint Management can't reauthenticate the user when a device attempts to reconnect.

**Failed Samsung Knox attestation:** Checks if a device failed a query of the Samsung Knox attestation server.

**Forbidden Apps:** Checks if a device has forbidden apps, as defined in an App Access policy. For more information about that policy, see [App access device policies](#).

**Inactive Devices:** Checks if a device is inactive as defined by the **Device Inactivity Days Threshold** setting in **Server Properties**. For details, see [Server properties](#).

**Missing Required Apps:** Checks if a device is missing any required apps, as defined in an App Access policy.

**Non-suggested Apps:** Checks if a device has non-suggested apps, as defined in an App Access policy.

**Noncompliant Password:** Checks if the user password is compliant. On iOS and Android devices, Endpoint Management can determine whether the password currently on the device is compliant with the passcode policy sent to the device. For instance, on iOS, the user has 60 minutes to set a password if Endpoint Management sends a passcode policy to the device. Before the user sets the password, the passcode might be non-compliant.

**Out of Compliance Devices:** Checks whether a device is out of compliance, based on the Out of Compliance device property. Typically, automated actions or third parties using Endpoint Management APIs change that property.

**Revoked Status:** Checks whether the device certificate is revoked. A revoked device cannot re-enroll until it is authorized again.

**Rooted Android and Jailbroken iOS Devices:** Checks whether an Android or iOS device is jailbroken.

**Unmanaged Devices:** Check whether Endpoint Management is managing a device. For example, a device enrolled in MAM or an unenrolled device is not managed.

**Note:**

The Implicit Compliant/Not Compliant filter sets the default value only on devices that Endpoint Management is managing. For example, any devices that have a blocked app installed or are not enrolled, get marked as Not Compliant. The NAC appliance blocks those devices from your network.

## Configuration overview

We recommend that you configure the NAC components in the order listed.

1. Configure device policies to support NAC:

**For iOS devices:** See [Configure the VPN device policy to support NAC](#).

**For Android Enterprise devices:** See [Create an Android Enterprise managed configuration for Citrix SSO](#).

**For Android devices:** See [Configure the Citrix SSO protocol for Android](#).

2. Enable NAC filters in Endpoint Management.

3. Configure a NAC solution:

- Citrix Gateway, detailed in [Update Citrix Gateway policies to support NAC](#). Requires that you install Citrix SSO on devices. See [Citrix Gateway Clients](#).
- Cisco ISE: See the Cisco documentation.
- ForeScout: See the ForeScout documentation.

## Enable NAC filters in Endpoint Management

1. In the Endpoint Management console, go to **Settings > Network Access Control**.

Settings > Network Access Control

## Network Access Control

Enables device compliance.

**Set as not compliant:**

- Anonymous Devices
- Failed Samsung KNOX attestation
- Forbidden Apps
- Inactive Devices
- Missing Required Apps
- Non-Suggested Apps
- Noncompliant Password
- Out of Compliance Devices
- Revoked Status
- Rooted Android and Jailbroken iOS Devices
- Unmanaged Devices

Cancel Save

2. Select the check boxes for the **Set as not compliant** filters you want to enable.
3. Click **Save**.

### Update Citrix Gateway policies to support NAC

You must configure advanced (not classic) authentication and VPN sessions policies on your VPN virtual server.

These steps update a Citrix Gateway with either of these characteristics:

- Is integrated with Endpoint Management.
- Or, is set up for VPN, not part of the Endpoint Management environment, and can reach Endpoint Management.

On your virtual VPN server from a console window, do the following. The FQDNs and IP addresses in the commands and examples are fictitious.

1. If you are using classic policies on your VPN virtual server, remove and unbind all classic policies. To check, type:

```
show vpn vserver <VPN_VServer>
```

Remove any result that contains the word Classic. For example: VPN Session Policy Name : PL\_OS\_10.10.1.1 Type: Classic Priority: 0

To remove the policy, type:

```
unbind vpn vserver <VPN_VServer> -policy <policy_name>
```

2. Create the corresponding advanced session policy by typing the following.

```
add vpn sessionPolicy <policy_name> <rule> <session action>
```

For example: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. Bind the policy to your VPN virtual server by typing the following.

```
bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100
```

4. Create an authentication virtual server by typing the following.

```
add authentication vserver <authentication vserver name> <service type>  
<ip address>
```

For example: `add authentication vserver authvs SSL 0.0.0.0`

In the example, 0.0.0.0 means that the authentication virtual server is not public facing.

5. Bind an SSL certificate with the virtual server by typing the following.

```
bind ssl vserver <authentication vserver name> -certkeyName <Webserver  
certificate>
```

Forexample: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Associate an authentication profile to the authentication virtual server from the VPN virtual server. First, create the authentication profile by typing the following.

```
add authentication authnProfile <profile name> -authnVsName <authentication  
vserver name>
```

For example:

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. Associate the authentication profile with the VPN virtual server by typing the following.

```
set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
```

For example:

```
set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof
```

8. Check the connection from Citrix Gateway to a device by typing the following.

```
curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/  
Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
```

For example, this query verifies connectivity by obtaining the compliance status for the first device (`deviceid_1`) enrolled in the environment:

```
curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"
```

A successful result is similar to the following example.

```
1 HTTP/1.1 200 OK
2 < Server: Apache-Coyote/1.1
3 < X-Citrix-Device-State: Non Compliant
4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
5 <!--NeedCopy-->
```

9. When the preceding step is successful, create the web authentication action to Endpoint Management. First, create a policy expression to extract the device ID from the iOS VPN plug-in. Type the following.

```
add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).
TYPECAST_NVLIST_T('\='\'','&\'').VALUE(\"deviceidvalue\")"
```

10. Send the request to Endpoint Management by typing the following. In this example, the Endpoint Management IP is `10.207.87.82` and the FQDN is `example.em.cloud.com:4443`.

```
add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort
4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n"+ "
Host: example.em.cloud.com:4443\r\n"+ "X-Citrix-VPN-Device-ID: "+
xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.
RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ
(\"Compliant\")"
```

The successful output for the Endpoint Management NAC is `HTTP status 200 OK`. The `X-Citrix-Device-State` header must have the value of `Compliant`.

11. Create an authentication policy with which to associate the action by typing the following.

```
add authentication Policy <policy name> -rule <rule> -action <web
authentication action>
```

For example: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. Convert the existing LDAP policy to an advanced policy by typing the following.

```
add authentication Policy <policy_name> -rule <rule> -action <LDAP
action name>
```

For example: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`



13. Add a policy label with which to associate the LDAP policy by typing the following.

```
add authentication policylabel <policy_label_name>
```

For example: `add authentication policylabel ldap_pol_label`

14. Associate the LDAP policy to the policy label by typing the following.

```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol  
-priority 100 -gotoPriorityExpression NEXT
```

15. Connect a compliant device to do a NAC test to confirm successful LDAP authentication. Type the following.

```
bind authentication vserver <authentication vserver> -policy <web  
authentication policy> -priority 100 -nextFactor <ldap policy label> -  
gotoPriorityExpression END
```

16. Add the UI to associate with the authentication virtual server. Type the following command to retrieve the device ID.

```
add authentication loginSchemaPolicy <schema policy>-rule <rule> -  
action lschema_single_factor_deviceid
```

17. Bind the authentication virtual server by typing the following.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority  
100 -gotoPriorityExpression END
```

18. Create an LDAP advanced authentication policy enable the Secure Hub connection. Type the following.

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"  
User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP  
  
bind authentication vserver authvs -policy ldap_xm_test_pol -priority  
110 -gotoPriorityExpression NEXT
```

## Chrome OS

October 13, 2021

Endpoint Management support for Chrome OS devices includes the ability to run Chrome OS devices in a public session. A public session doesn't require a user to sign on and doesn't have permanent data. Public sessions are useful for libraries, public schools, and other situations where session data isn't permanent. You can also configure a Chrome OS device in kiosk mode. Kiosk mode locks down a device per user.

To manage Chrome OS devices, Endpoint Management uses a Secure Hub extension installed in the Chrome device browser. Before enrolling Chrome OS devices in Endpoint Management, you configure Google Workspace to install the Secure Hub extension on the device. Then, you connect Google Workspace to Endpoint Management.

Endpoint Management enrolls Chrome OS devices into MDM. Endpoint Management doesn't support MAM-only registration for Chrome OS devices. Endpoint Management supports user name and password authentication on Chrome OS devices.

A general workflow for starting Chrome OS device management is as follows:

1. Complete the onboarding process. See [Onboarding and resource setup](#) and [Prepare to enroll devices and deliver resources](#).
2. Choose and configure an enrollment method. See [Supported enrollment methods](#).
3. Configure Google Workspace to install Secure Hub on the Chrome OS device.
4. Connect Endpoint Management to Google Workspace.
5. Configure Chrome OS device policies.
6. Enroll Chrome OS devices in Google Workspace and then Enroll Chrome devices in Endpoint Management.

For supported operating systems, see [Supported device operating systems](#).

### Supported enrollment methods

The following table indicates the enrollment methods that Endpoint Management supports for Chrome OS devices:

Method	Supported
Bulk enrollment	No
Manual enrollment	Yes (user name + password only)
Enrollment invitations	No

For more information, see the Google Workspace configuration sections in this article.

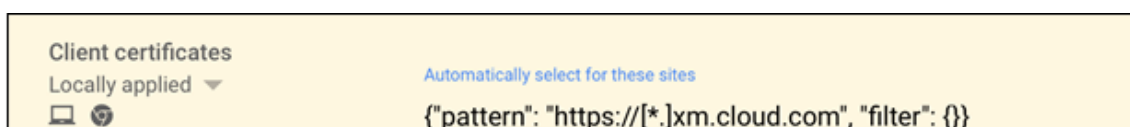
### Configure Google Workspace to install Secure Hub on the Chrome OS device

You configure forced installation of the Secure Hub extension on the Chrome OS device and prevent the extension from being disabled or deleted.

1. Go to the [Google Admin site](#) and log in to your Google Workspace account.
2. Verify that you've completed the configuration described in [Enable partner access for devices and users in your Google Workspace domain](#).
3. In the Google administrator console, select **Devices > Chrome > Settings > Users & Browsers**.
4. In the **User & Browsers** settings page, search for Client certificates. Add this pattern:

```
{ "pattern": "https://[*.]xm.cloud.com", "filter": { } }
```

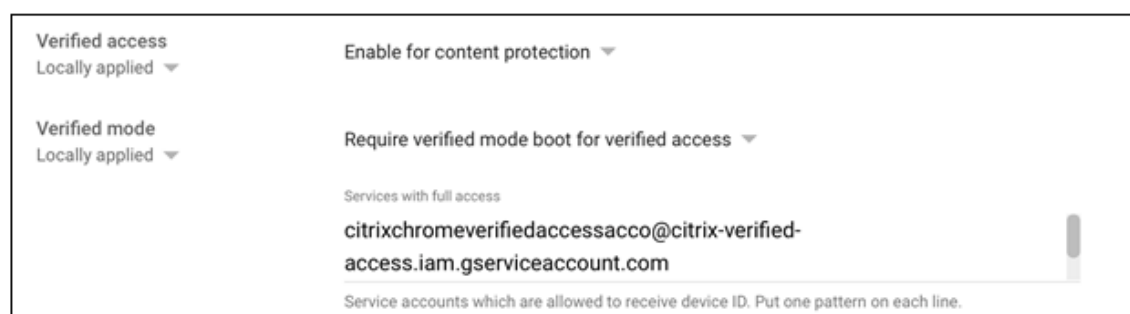
When you add this pattern to Client certificates, device certificates pushed from Endpoint Management to the device are selected automatically. The user isn't prompted to select certificates.



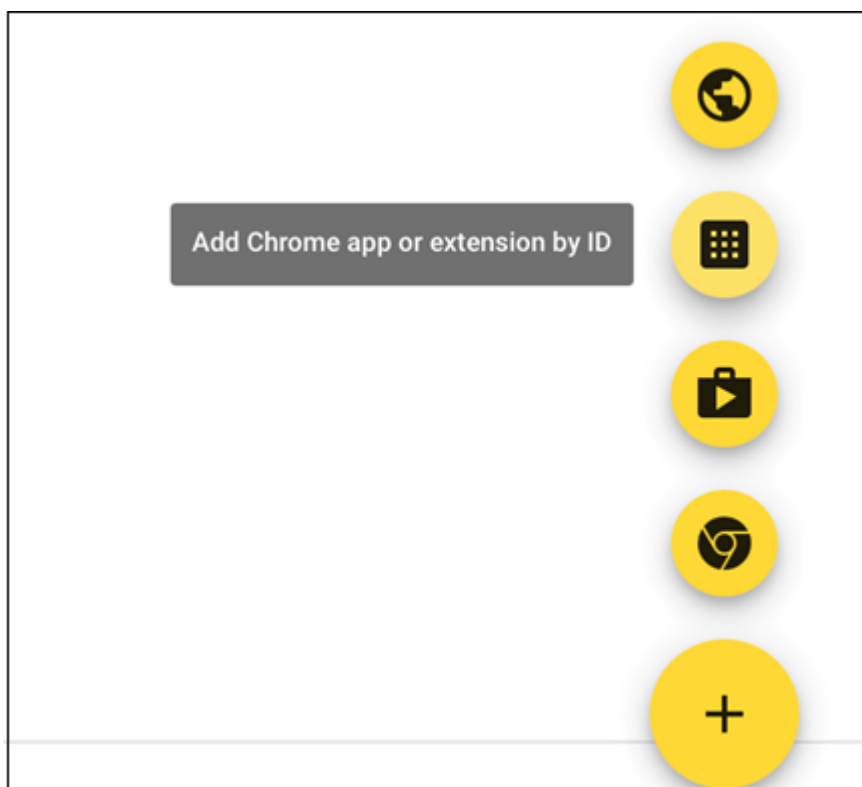
5. Click **Save**.
6. Click the Device Settings tab (**Devices > Chrome > Settings > Device**). In the Device settings page:
  - a) Search for Verified Access.
  - b) Select the option for **Enable for content protection**.
  - c) On the Verified Mode option, select the option for **Require verified mode boot for verified access**.
  - d) Add the following e-mail address for Service with full access.

```
citrixchromeverifiedaccessacco@citrix-verified-access.iam.gserviceaccount.com
```

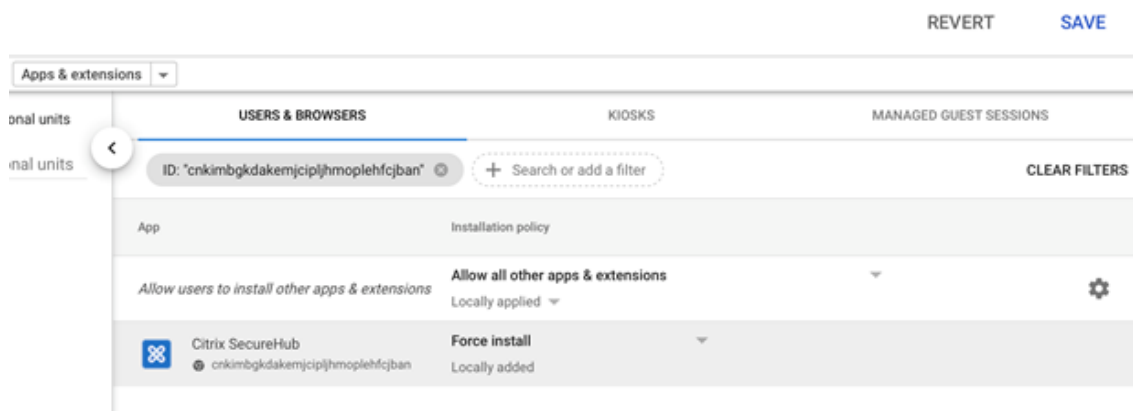
When you add the address to Verified Mode, it fulfills the requirement for Citrix Endpoint Management to be able to enable Verified Access for device security.



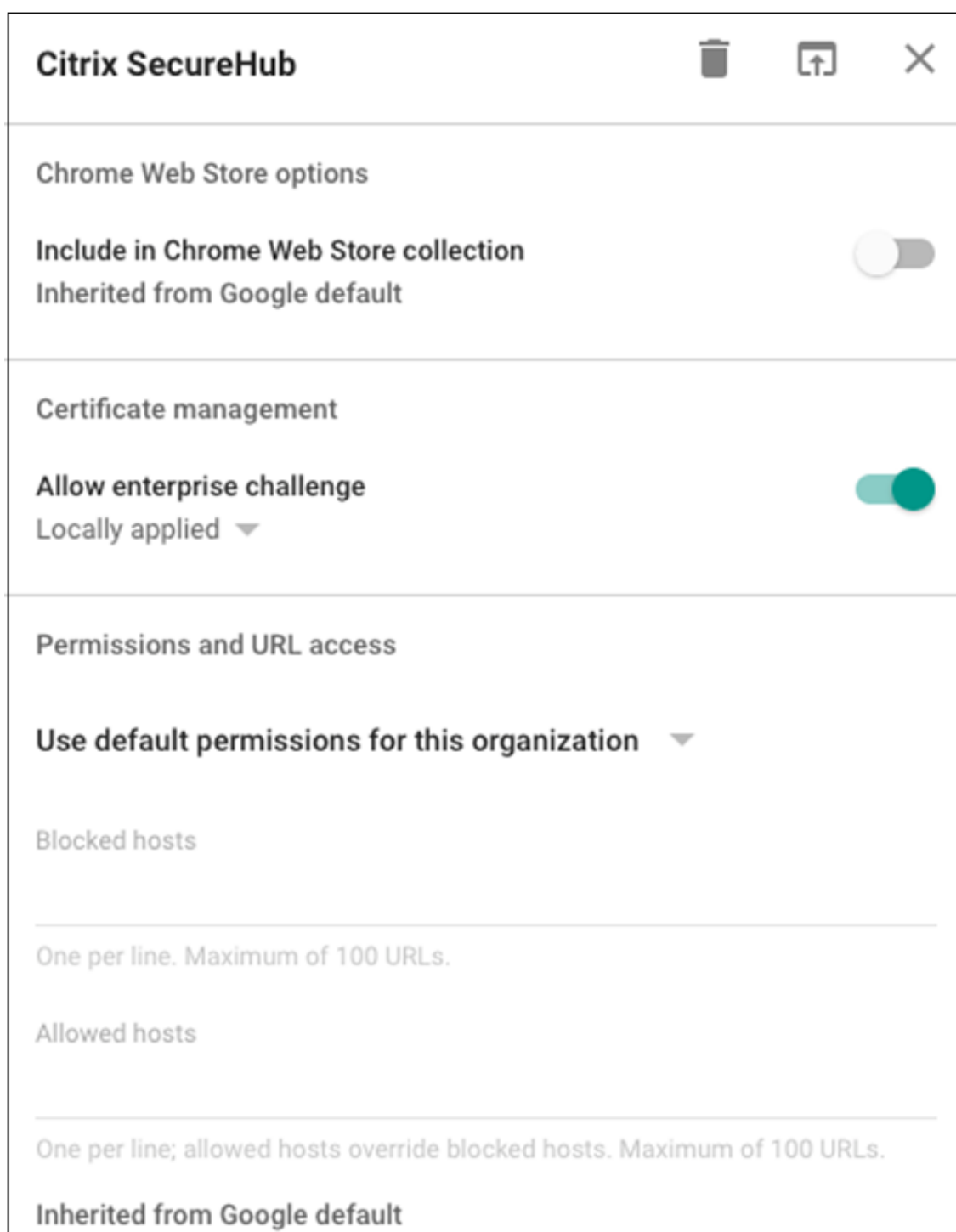
7. Navigate to **Devices > Chrome > Apps & Extensions > Users & browsers**. Click + and select **Add Chrome app or extension by ID**, as shown in the figure.



8. On the Add Chrome app or extension by ID popup, enter `cnkimbgkdakemjcipljhmoplehfcjban` in the **Extension ID field** and click **Save**.
9. Change the installation policy for the Citrix Secure Hub Extension to **Force Install**.



10. Click the Citrix SecureHub row to open the Secure Hub dialog on the right. Under **Certificate management**, enable **Allow enterprise challenge**.



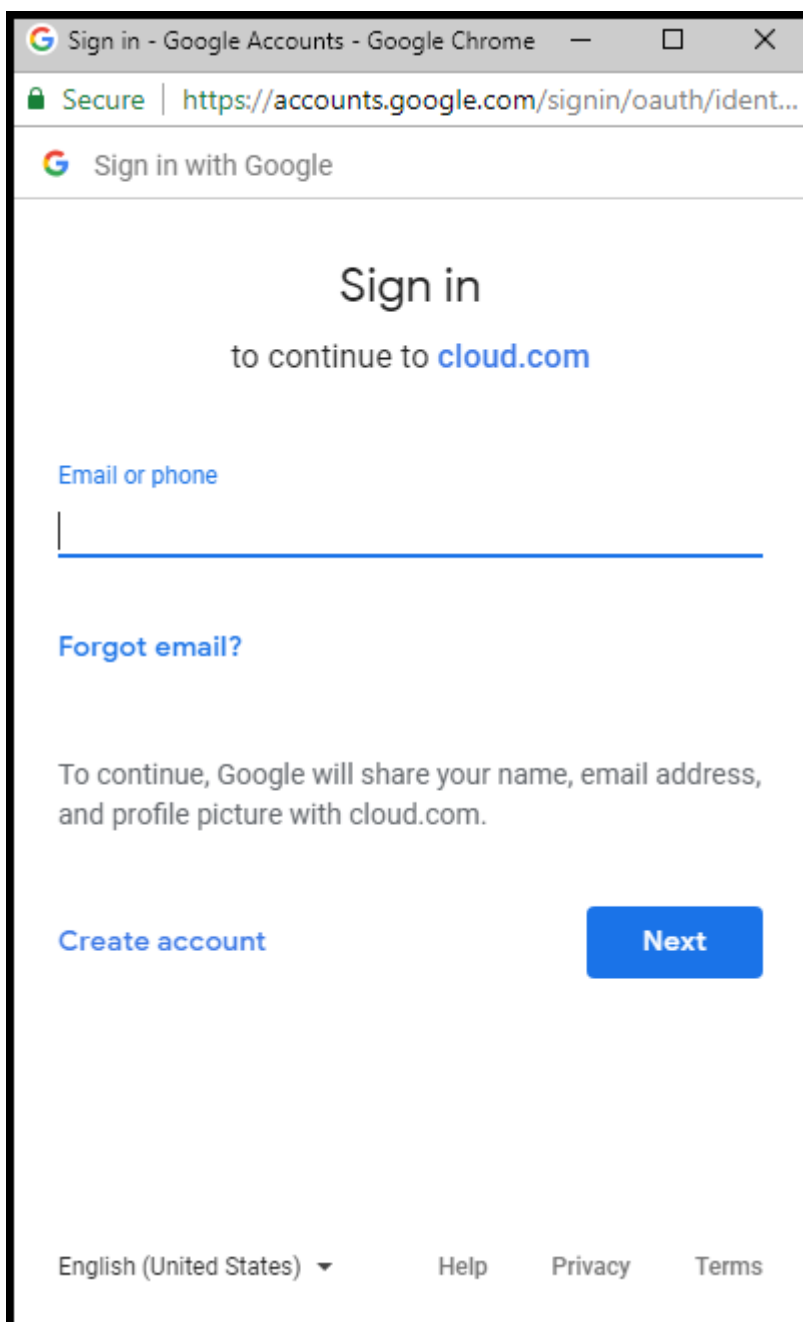
11. Click **Save**.

### **Connect Endpoint Management to Google Workspace**

1. In the Endpoint Management console, click the gear icon in the upper-right corner and then click **Settings > Google Chrome**.

<b>G-Suite Domain *</b>	<input type="text" value="xms"/>
<b>G-Suite Admin *</b>	<input type="text" value="ma@xms"/>
<b>G-Suite Client ID</b>	<input type="text" value="105"/>
<b>G-Suite Enterprise ID</b>	<input type="text" value="C01"/>

2. Click **Connect**. A Google account sign-in window appears.



3. Sign in with your Google account credentials and click **Next**.
4. Endpoint Management fills in your Google Workspace domain and Google Workspace account administrator name. The **Connect** button has change to **Disconnect**. Endpoint Management is connected to Google Workspace.

Settings > Google Chrome

## Google Chrome

Configures Endpoint Management to communicate with your G Suite account.

**G Suite domain \***

**G Suite admin account \***

**G Suite client ID**

[Disconnect](#)

### Configure Chrome OS device policies

Use these policies to configure how Endpoint Management interacts with devices running Chrome OS. These device policies are available for Chrome OS devices.

- [App restrictions](#)
- [Connection scheduling](#)
- [Content](#)
- [Credentials](#)
- [Kiosk](#)
- [Managed bookmarks](#)
- [Network](#)
- [Power management](#)
- [Public session](#)
- [Restrictions](#)
- [OS update](#)
- [VPN](#)

### Enroll Chrome OS devices in Google Workspace

Device enrollment in your Google Workspace domain is a prerequisite for enrolling a Chrome OS device in Endpoint Management. For information on Google Workspace domain enrollment, see the Google article, [Enroll Chrome devices](#).



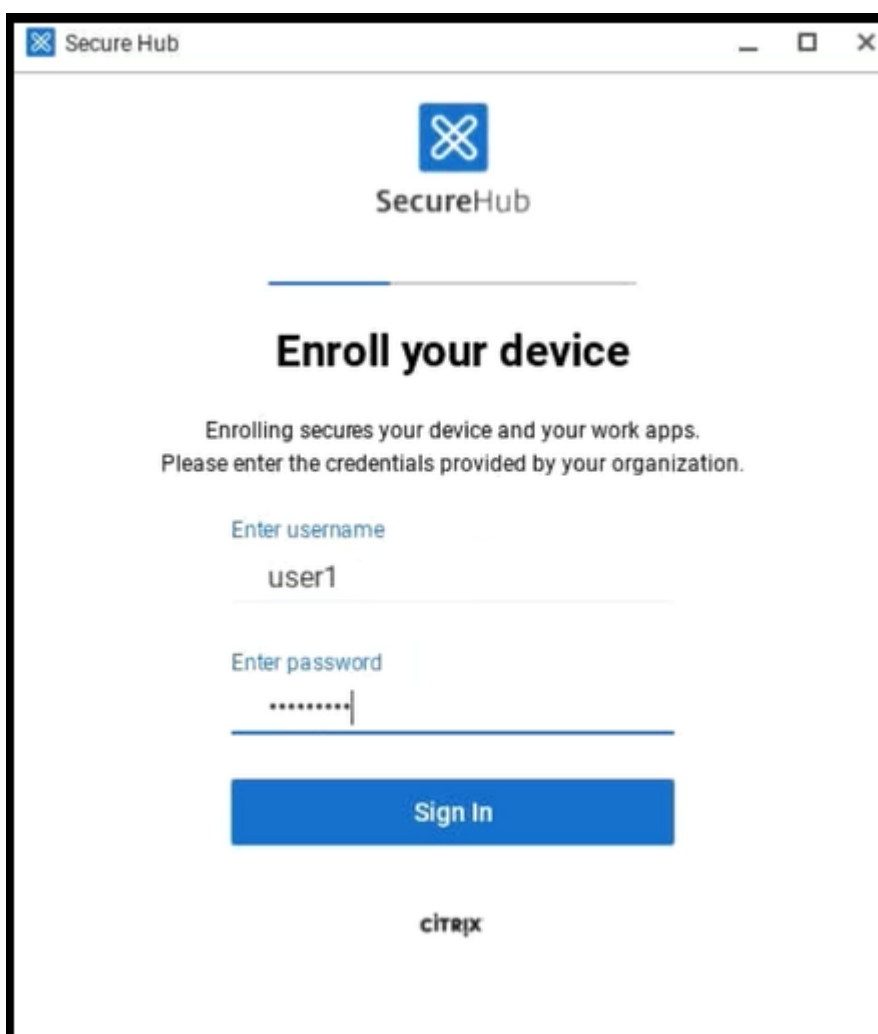
## Enroll Chrome devices in Endpoint Management

A Citrix PIN must be created when a Chrome OS device is enrolled in Endpoint Management. The Citrix PIN is separate from the Endpoint Management passcode. The Citrix PIN secures a certificate from the Endpoint Management server. This PIN cannot be reset. If a user forgets this PIN, the Chrome OS device must be unenrolled and re-enrolled.

1. Sign in to your Chrome OS device by using your Google Workspace credentials.
2. Click the Secure Hub extension in Chrome. The Secure Hub extension appears next to your browser address bar, is grayed out, and looks like the following image:



3. The Secure Hub enrollment window appears. Click **Enroll**.
4. Type your corporate credentials, such as your Endpoint Management server name, User Principal Name (UPN), or email address. Then, click **Next**.
5. If prompted, type your corporate user name. Type your corporate password. Then, click **Sign In**.



6. Create a Citrix PIN. This PIN must be 6 characters long. It can contain only letters and numbers. Type your Citrix PIN twice and then click **Finish**.

When the enrollment is complete, the Secure Hub extension icon is active.

### **Sign in to an enrolled Chrome OS device**

To sign in to a Chrome OS device that is enrolled in Endpoint Management:

1. Sign in using your Google Workspace credentials.
2. When prompted, enter your Citrix PIN. This PIN was created when the device was enrolled in Endpoint Management.

If you do not type your Citrix PIN:

- You are prompted to type your Citrix PIN every minute until you type the PIN.
- After five minutes, access is blocked to all websites except google.com, citrix.com, gotomeeting.com, cloud.com.

- If you try to access any other website, an error message appears and you are prompted to sign in using your Citrix PIN.

### **Unenroll and reenroll a Chrome OS device**

To unenroll a Chrome OS device from Endpoint Management, users delete their account.

1. In the Chrome browser, click the Secure Hub extension icon.
2. In the Secure Hub enrollment window, click **Delete**.
3. Click **Yes, Delete** to confirm the deletion.

The Secure Hub enrollment window closes and the Secure Hub extension icon is grayed out.

To re-enroll:

1. Log out of your Chrome OS device and log back in using your Google Workspace credentials.
2. Click **Enroll** and follow the prompts to re-enroll.

### **Security actions**

Chrome OS doesn't support security actions.

## **Windows Desktop and Tablet**

October 13, 2021

Endpoint Management enrolls Windows 10 and Windows 11 devices in MDM. Endpoint Management supports the following authentication types for Windows 10 and Windows 11 devices enrolled in MDM:

- Domain-based authentication
  - Active Directory
  - Azure Active Directory
- Identity providers:
  - Azure Active Directory
  - Citrix identity provider

For more information about the supported authentication types, see [Certificates and authentication](#).

A general workflow for starting Windows 10 or Windows 11 device management is as follows:

1. Complete the onboarding process. See [Onboarding and resource setup](#) and [Prepare to enroll devices and deliver resources](#).

If you plan to enroll Windows devices using the AutoDiscovery service, you must configure the Citrix AutoDiscovery service. Request Citrix Technical Support for assistance. For more information, see [Request AutoDiscovery for Windows devices](#).

2. Choose and configure an enrollment method. See Supported enrollment methods.
3. Configure Windows Desktop and Tablet device policies.
4. Users enroll Windows 10 and Windows 11 devices.
5. Set up device and app security actions. See Security actions.

For supported operating systems, see [Supported device operating systems](#).

### Supported enrollment methods

You specify how to manage Windows 10 and Windows 11 devices in enrollment profiles. Two options are available:

- Fully managed (MDM enrollment)
- Do not manage devices (no MDM enrollment)

To configure enrollment settings for Windows 10 and Windows 11 devices, go to **Configure > Enrollment Profiles > Windows**. For more information about enrollment profiles, see [Enrollment profiles](#).

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<p><b>Device management</b> ?</p> <p><b>Management</b> <input checked="" type="radio"/> Fully managed ? <input type="radio"/> Do not manage devices ?</p>
Android	<p><b>User consent</b></p> <p>Allow users to decline device management <input checked="" type="checkbox"/> On ?</p>
Windows	<p><b>Workspace integration</b> ?</p> <p>Enrollment through Workspace app <input type="checkbox"/> Off ?</p>
3 Assignment (optional)	

The following table lists the enrollment methods that Endpoint Management supports for Windows 10 and Windows 11 devices:

Method	Supported
Azure Active Directory enrollment	Yes

Method	Supported
Citrix Workspace app enrollment	Yes
AutoDiscovery service enrollment	Yes
Windows bulk enrollment	Yes
Manual enrollment	Yes
Enrollment invitations	No

**Note:**

- Manual enrollment requires users to enter a fully qualified domain name (FQDN) of the Endpoint Management server. We do not recommend using manual enrollment. Instead, use other methods to simplify the enrollment process for users.
- You cannot send enrollment invitations to Windows devices. Windows users enroll directly through their devices.

### Configure Windows Desktop and Tablet device policies

Use these policies to configure how Endpoint Management interacts with desktop and tablet devices running Windows 10 or Windows 11. This table lists all device policies available for Windows desktop and tablet devices.

App configuration	App inventory	App lock
App uninstall	Application Guard	BitLocker
Credentials	Custom XML	Defender
Device Guard	Device Health Attestation	Exchange
Firewall	Kiosk	Network
Office	OS update	Passcode
Restrictions	Store	Terms and Conditions
VPN	Web clip	Windows Agent
Windows GPO configuration	Windows Hello for Business	Windows Information Protection

## Enroll Windows 10 and Windows 11 devices through Azure Active Directory

### Important:

Before users can enroll, you must configure Azure Active Directory (AD) settings in Azure and then configure Endpoint Management. For details, see [Connect Endpoint Management to Azure AD](#).

Windows 10 and Windows 11 devices can enroll with Azure as a federated means of AD authentication. This enrollment requires an Azure AD Premium subscription. For more information, see <https://docs.microsoft.com/en-us/azure/active-directory/devices/overview#license-requirements>.

You can join Windows 10 and Windows 11 devices to Microsoft Azure AD by using any of the following methods:

- For company-owned devices:
  - Enroll in MDM when joining the device to Azure AD the first time the devices are powered on. In this scenario, users complete the enrollment as described in this article: <https://docs.microsoft.com/en-us/azure/active-directory/devices/azuread-joined-devices-frx>.  
For Windows devices that you enroll with this method, you can use Windows AutoPilot to set up and pre-configure the devices. For more information, see [Use Windows AutoPilot to set up and configure devices](#).
  - Enroll in MDM when joining the device to Azure AD from the Windows **Settings** page after configuring the device. In this scenario, users complete the enrollment as described in [Enroll in MDM when joining Azure AD after configuring devices](#).
- For personal devices (BYOD or mobile devices):
  - Enroll in MDM when registering to Azure AD while adding the Microsoft work account to Windows. In this scenario, users complete the enrollment as described in [Enroll in MDM when registering to Azure AD](#).

### Enroll in MDM when joining Azure AD after configuring devices

1. On a device, from the Start menu, navigate to **Settings > Accounts > Access work or school** and click **Connect**.
2. In the **Set up a work or school account** dialog box, under **Alternate actions**, click **Join this device to Azure Active Directory**.
3. Enter Azure AD credentials and click **Sign in**.
4. Accept the terms and conditions that the organization requires.
  - If users click **Decline**, the device neither joins Azure AD nor enrolls in Endpoint Management.
5. Click **Join** to proceed with the enrollment process.

6. Click **Done** to complete the enrollment process.

### **Enroll in MDM when registering to Azure AD**

1. On a device, from the Start menu, navigate to **Settings > Accounts > Access work or school** and click **Connect**.
2. In the **Set up a work or school account** dialog box, enter Azure AD credentials and click **Sign in**.
3. Accept the terms and conditions that the organization requires. The device is registered to Azure AD and enrolls in Endpoint Management.
  - If users click **Decline**, the device is registered to Azure AD but not enrolled into Endpoint Management. There is no **Info** button on the account.
4. Click **Join** to proceed with the enrollment process.
5. Click **Done** to complete the enrollment process.

### **Enroll Windows 10 and Windows 11 devices through Citrix Workspace app (preview)**

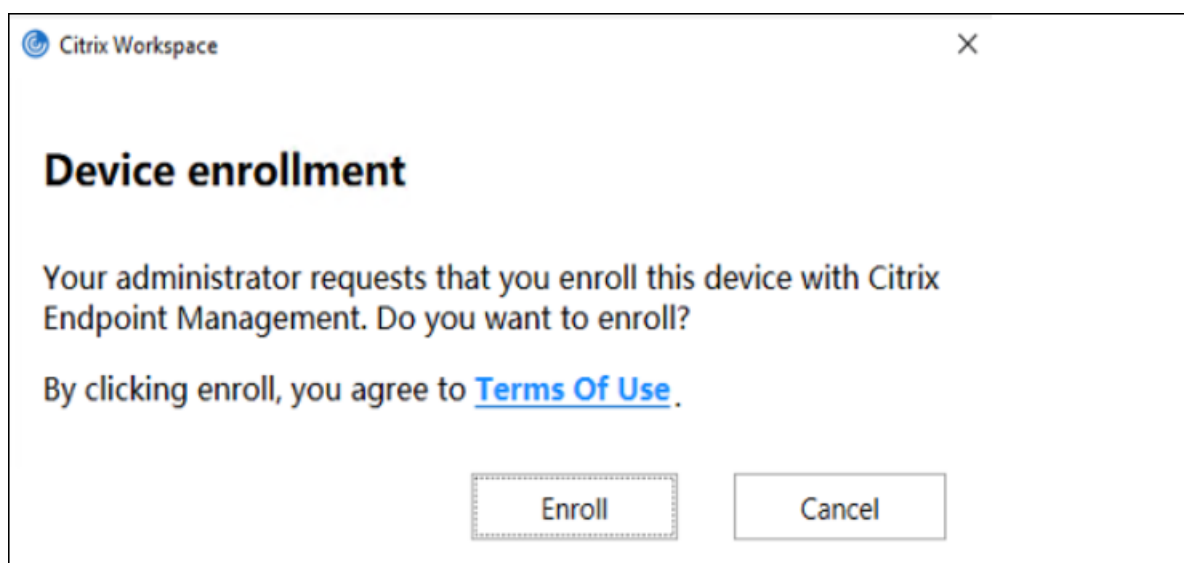
Endpoint Management supports automatically enrolling Windows 10 and Windows 11 devices through Citrix Workspace app. This support means that users can enroll supported Windows 10 and Windows 11 devices.

Prerequisites:

- Cloud-based deployment
- Citrix Workspace app 1911 or later
- Citrix Endpoint Management 20.1.0 or later
- Citrix Endpoint Management integrated with Citrix Workspace

For information about Endpoint Management integration with Citrix Workspace, see [Integration with Citrix Workspace experience](#). For information about enabling Workspace integration for Endpoint Management in Citrix Cloud, see Endpoint Management in the [Citrix Workspace documentation](#).

The following enrollment prompt appears when users enter their credentials to add a store in Citrix Workspace app:



The enrollment prompt appears only when the following conditions are met:

- The device is not MDM-enrolled.
- The user is a member of the local administrators group on the endpoint.
- An enrollment profile is present for Windows 10 and Windows 11 devices.

### Enroll Windows devices by using the AutoDiscovery service

To configure the AutoDiscovery service for Windows devices, request Citrix Technical Support for assistance. For more information, see [Request AutoDiscovery for Windows devices](#).

#### Note:

For Windows devices to enroll, the SSL listener certificate must be a public certificate. Enrollment fails for self-signed SSL certificates.

Users perform the following steps to complete the enrollment:

1. On a device, from the Start menu, navigate to **Settings > Accounts > Access work or school** and click **Enroll only in device management**.
2. In the **Set up a work or school account** dialog box, enter a corporate email address and click **Next**.

To enroll as a local user, enter a nonexistent email address with the correct domain name (for example, `foo\@mydomain.com`). That step lets a user bypass a known Microsoft limitation where the built-in Device Management on Windows performs enrollment. In the **Connecting to a service** dialog box, enter the user name and password associated with the local user. The device then discovers an Endpoint Management server and starts the enrollment process.



3. Enter the credential and click **Continue**.
4. In the **Terms of use** dialog box, agree to have the device managed and then click **Accept**.

Enrolling domain-joined Windows devices through the AutoDiscovery service fails if the domain policy disables MDM enrollment. Users can use either of the following methods instead:

- Remove the devices from the domain, enroll, and then rejoin them.
- Enter the FQDN of the Endpoint Management server to proceed.

### Windows bulk enrollment

With Windows bulk enrollment, you can set up many devices for an MDM server to manage without the need to reimage devices. You use a provisioning package for bulk enrollment for Windows 10 and Windows 11 Desktop and Laptop devices. For information, see [Enroll Windows devices in bulk](#).

### Security actions

Windows 10 and Windows 11 devices support the following security actions. For a description of each security action, see [Security actions](#).

---

Locate	Lock	Reboot
Revoke	Selective Wipe	Wipe

---

### Connect Endpoint Management to Azure AD

Windows 10 and Windows 11 devices can enroll with Azure. Users created in Azure AD can have access to the devices. Endpoint Management is deployed in Microsoft Azure as an MDM service. Connecting Endpoint Management to Azure AD enables users to automatically enroll their devices into Endpoint Management when they enroll the devices into Azure AD.

To connect Endpoint Management to Azure AD, perform the following steps:

1. In the Azure portal, navigate to **Azure Active Directory > Mobility (MDM and MAM) > Add application** and click **On-premises MDM application**.
2. Provide a name for the application and click **Add**.
3. Select the application you created, configure the following, and then click **Save**.
  - **MDM user scope**. Select **All**.

- **MDM terms of use URL.** Enter in the format, <https://<Endpoint Management Enrollment FQDN>:8443/zdm/wpe/tou>.
  - **MDM discovery URL.** Enter in the format, <https://<Endpoint Management Enrollment FQDN>:8443/zdm/wpe>.
4. Click **On-premises MDM application settings**.
    - In the **Properties** pane, set **APP ID URI** in the format, <https://< Endpoint Management Enrollment FQDN>:8443>. This App ID URI is a unique ID that you cannot use again in any other app.
    - In the **Required permissions** pane, select **Microsoft Graph** and **Windows Azure Active Directory**.
    - In the **Keys** pane, create the authentication key. Click **Save** to view the key value. The key value appears only once. Save the key for later use. You need the key in step 7.
  5. In the Endpoint Management console, go to **Settings > Identity Provider (IDP)** and then click **Add**.
  6. On the **Discovery URL** page, configure the following and click **Next**.
    - **IDP Name.** Enter a unique name to identify the IdP connection that you are creating.
    - **IDP Type.** Select **Azure Active Directory**.
    - **Tenant ID.** The **Directory ID** in Azure. You see it when you navigate to **Azure Active Directory > Properties** in Azure.
  7. On the **Windows MDM Info** page, configure the following and click **Next**.
    - **App ID URI.** The APP ID URI value you typed in Azure.
    - **Client ID.** The Application ID you see in the **Properties** pane in Azure.
    - **Key.** The key value you created and saved in step 4 above.
  8. On the **IDP Claims Usage** page, configure the following and click Next.
    - **User Identifier type.** Select **userPrincipalName**.
    - **User Identifier string.** Enter `${ id_token } .upn`.
  9. Click **Save**.
  10. Add an Azure AD user as a local user and assign it to a local user group.
  11. Create a terms and conditions device policy and a delivery group that includes that local user group.

## Device management when integrated with Workspace Environment Management

With Workspace Environment Management (WEM) alone, MDM deployments aren't possible. With Endpoint Management alone, you're limited to managing Windows 10 and Windows 11 devices. By

integrating the two, WEM can access MDM features and you can manage a wider spectrum of Windows operating systems through Endpoint Management. That management takes the form of configuring Windows GPOs. Currently, administrators import an ADMX file to Citrix Endpoint Management and push it to Windows 10 and Windows 11 desktops and tablets to configure specific applications. Using the Windows GPO Configuration device policy, you can configure GPOs and push changes to the WEM service. The WEM Agent then applies the GPOs to devices and their apps.

MDM management isn't a requirement for WEM integration. Any device that WEM supports can have GPO configurations pushed to it, even if Endpoint Management doesn't support that device natively.

For a list of the devices supported, see [Operating System requirements](#).

Devices which receive the Windows GPO Configuration device policy run in a new Endpoint Management mode called WEM. In the **Manage > Devices** list of enrolled devices, the **Mode** column for WEM-managed devices lists **WEM**.

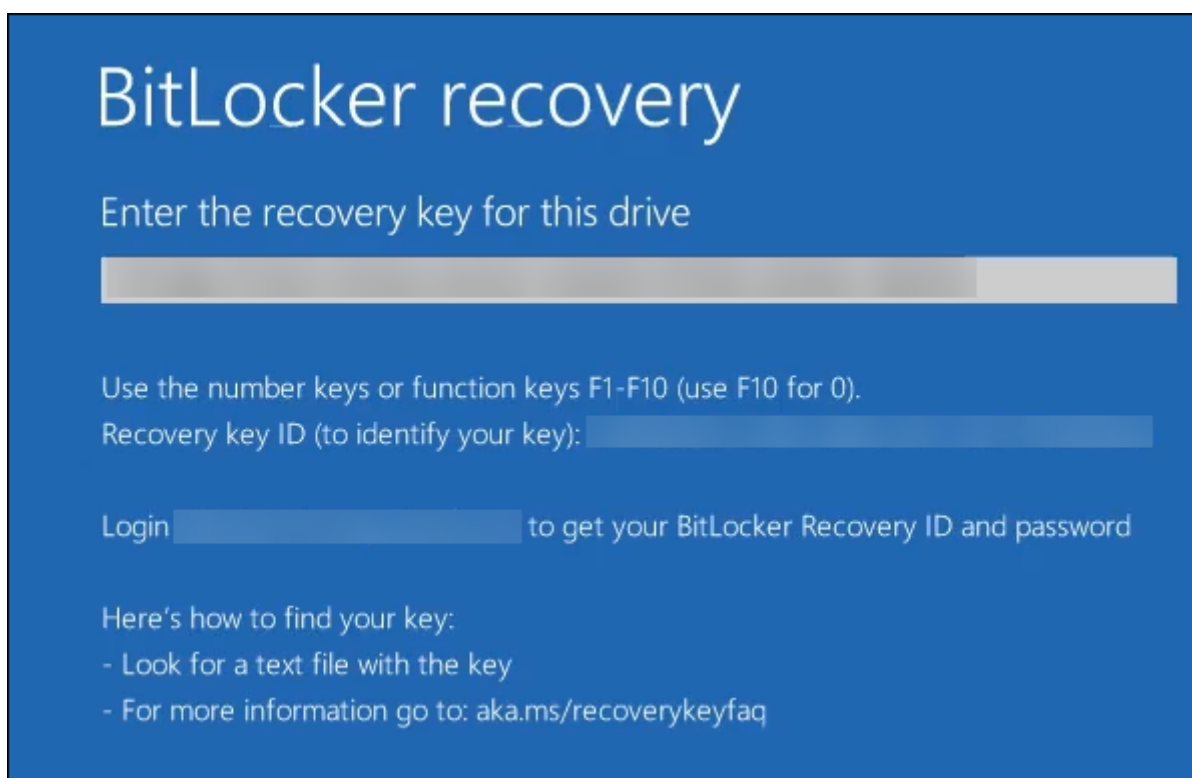
For more information, see [Windows GPO Configuration device policy](#).

### **BitLocker recovery key**

Encrypting disks using BitLocker is a useful security feature. However, unlocking devices can be a challenge if the user loses their BitLocker recovery key. Endpoint Management can now automatically, securely save BitLocker recovery keys for users. Users can find their BitLocker recovery key on the Self-Help Portal. To enable and find the BitLocker recovery key:

1. In the Endpoint Management console, navigate to **Settings > Server Properties**.
2. Search for `shp` and enable the `shp.console.enable` feature. Ensure that `enable.new.shp` remains disabled. For more information on enabling the Self-Help Portal, see [Configure enrollment security modes](#).
3. Navigate to **Configure > Device policies**. Find your BitLocker policy or create one and enable the **BitLocker Recovery backup to Endpoint Management** setting.

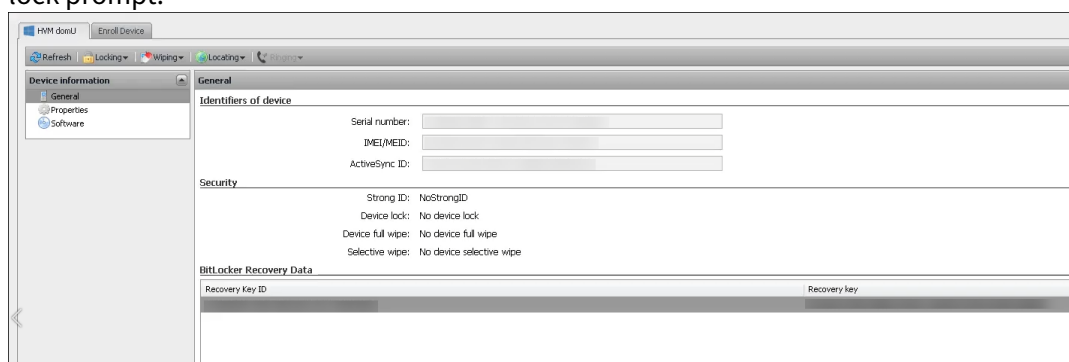
When unlocking their device, end users see a message asking them to enter their key. The message displays the Recovery key ID as well.



To find their BitLocker recovery key, users navigate to the Self-Help Portal.

1. Under the **General** details, see the **BitLocker Recovery Data**.

- **Recovery key ID:** The identifier for the BitLocker recovery key used to encrypt the disk. This ID must match the key ID given in the previous message.
- **Recovery key:** The key the user must enter to unlock their disk. Enter this key at the unlock prompt.



For more information about the BitLocker device policy, see [BitLocker device policy](#).

## Windows Phone

October 13, 2021

**Note:**

If you use Microsoft Endpoint Manager, this article doesn't apply to your setup. See [Citrix Endpoint Management integration with Microsoft Endpoint Manager](#).

Microsoft moved Windows Phone 8.1 devices to End of Support on July 11, 2017. Endpoint Management supports Windows Phone 8.1 devices for MDM enrollment only.

To manage Windows 10 Phone devices in Endpoint Management, configure the Citrix AutoDiscovery service. Request Citrix Technical Support for assistance. For more information, see [Request AutoDiscovery for Windows devices](#).

Endpoint Management enrolls Windows 10 Phone devices into MDM. Endpoint Management supports the following authentication types for Windows Phone devices:

- Domain-based authentication
  - Active Directory
  - Azure Active Directory
- Identity providers:
  - Azure Active Directory
  - Citrix identity provider

**Tip:**

- For more information about the supported authentication types, see [Certificates and authentication](#).

A general workflow for starting Windows 10 Phone device management is as follows:

1. Complete the onboarding process. See [Onboarding and resource setup](#) and [Prepare to enroll devices and deliver resources](#).
2. Choose and configure an enrollment method. See [Supported enrollment methods](#).
3. Configure Windows Phone device policies.
4. Enroll Windows Phone devices.
5. Set up device and app security actions. See [Security actions](#).

For supported operating systems, see [Supported device operating systems](#).

## Supported enrollment methods

The following table lists the enrollment methods that Endpoint Management supports for Windows Phone devices:

Method	Supported
Azure Active Directory enrollment	Yes
Windows bulk enrollment	No
Manual enrollment	Yes
Enrollment invitations	No

## Azure enrollment

Devices running Windows 10 Enterprise can enroll with Azure as a federated means of Active Directory authentication. This setup requires an Azure Active Directory Premium subscription.

You can join Windows 10 devices to Microsoft Azure AD in any of the following ways:

- Enroll in MDM as part of Azure AD Join setup the first time the device is powered on.
- Enroll in MDM as part of Azure AD Join from the Windows Settings page after configuring the device.
- Enroll in MDM as part of Azure AD Join when you add a work account on a personal device.

Before users can enroll, you must configure Azure Active Directory (AD) settings in Azure and then configure Endpoint Management. For details, see [Connect Endpoint Management to Azure AD](#).

## Configure Windows Phone device policies

Use these policies to configure how Endpoint Management interacts with phone devices running Windows 10. This table lists all device policies available for Windows 10 Phone devices.

<a href="#">App configuration</a>	<a href="#">App inventory</a>	<a href="#">App uninstall</a>
<a href="#">BitLocker</a>	<a href="#">Credentials</a>	<a href="#">Custom XML</a>
<a href="#">Device Health Attestation</a>	<a href="#">Enterprise Hub</a>	<a href="#">Exchange</a>
<a href="#">Maps</a>	<a href="#">Network</a>	<a href="#">Passcode</a>
<a href="#">Restrictions</a>	<a href="#">Storage encryption</a>	<a href="#">Terms and Conditions</a>

VPN

Windows Hello for  
Business

Windows Information  
Protection

---

## Enroll Windows Phone devices by using Azure Active Directory

1. Sign on to a Windows Enterprise edition computer. Open **Settings > Accounts > Access work or school** and then click **Connect**.
2. From **Set up a work or school account**, under **Alternative actions**, click **Join this device to Azure Active Directory**.
3. Provide your Azure Active Directory credentials and then click **Sign in**.
4. Accept the Terms and Conditions set by your organization.
5. Click **Join** to proceed with the enrollment process.
6. Click **Done** to complete the enrollment process.

## Enroll Windows Phone devices

To enroll Windows Phone devices in Endpoint Management, users need their Active Directory or internal network email address, and password. If AutoDiscovery is not set up, users also need the server web address for the Endpoint Management server. Then, they follow this procedure on their devices to enroll.

### Note:

If you plan to deploy apps through the Windows Phone company store: Before your users enroll, configure an [Enterprise Hub device policy](#). In that policy, you upload a signing certificate from DigiCert and a signed Citrix Company Hub app.

1. On the main screen of the Windows phone, tap the **Settings** icon.
2. Depending on your version, either tap **Accounts > Access work or school > Connect to work or school** or tap **Accounts > Work access > Enroll in to device management**.
3. On the next screen, enter an email address and password and then tap **sign in**.

If AutoDiscovery is configured for your domain, the information requested in the next several steps is automatically populated. Proceed to the last step in this procedure.

If AutoDiscovery is not configured for your domain, continue with the next step. To enroll as a local user, enter a non-existent email address with the correct domain name (for example, [foo@mydomain.com](#)). Using a non-existent address permits you to bypass a known Microsoft

limitation. In the **Connecting to a service** screen, enter the user name and password associated with the local user.

4. On the next screen, type the web address of the Endpoint Management server, such as: `https://<xenmobile_server_fqdn>:<enrollment_port>/<instance_name>/wpe`. For example, `https://mycompany.mdm.com:8443/zdm/wpe`.

**Note:**

The port number must be the same port that you used for an iOS enrollment.

5. If authentication is validated through a user name and domain, type the user name and domain and then tap **sign in**.
6. If a message indicates a problem with the certificate, the error is the result of using a self-signed certificate. If the server is trusted, tap **continue**. Otherwise, tap **Cancel**.
7. To force a connection to the server, tap the refresh icon. If the device does not manually connect to the server, Endpoint Management attempts to reconnect.

Endpoint Management connects to the device every three minutes for five successive times, then every two hours afterward. You can alter this connection rate in the **Windows WNS Heart-beat Interval** located in **Server properties**.

Once enrollment is complete, Secure Hub enrolls in the background. No indicator appears when the installation is complete. Tap Secure Hub from the **All Apps** screen.

## Security actions

Windows 10 Phone devices support the following security actions. For a description of each security action, see [Security actions](#).

Locate	Lock	Lock and Reset Password
Reboot	Revoke	Ring
Selective Wipe	Wipe	

## Enroll Windows devices in bulk

September 9, 2021

Endpoint Management supports bulk enrollment of Windows 10 and Windows 11 desktop and tablet



devices. With bulk enrollment, you can set up many devices for Endpoint Management to manage without reimaging devices. You use the provisioning package for bulk enrollment.

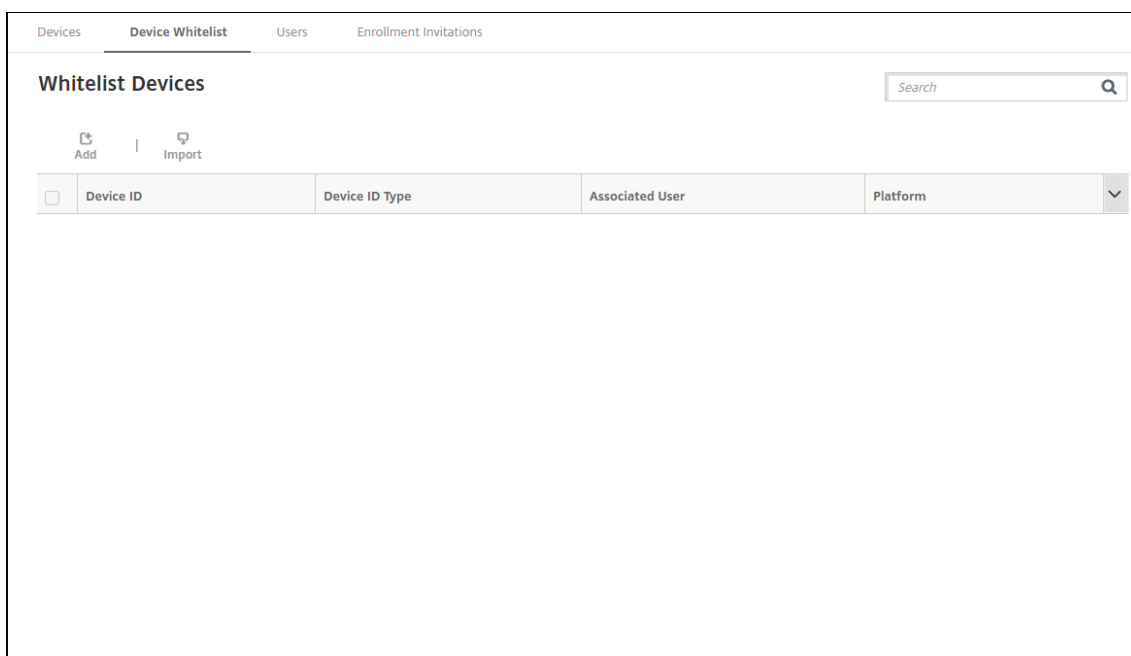
A general workflow to bulk enroll Windows 10 and Windows 11 devices is as follows:

1. Assign devices. You can assign devices either on a per-device basis or in bulk.
2. Configure bulk enrollment.
3. Create a provisioning package and apply that package per device.

Before running bulk enrollment, ensure that you assign all devices to the correct users. Perform this assignment by adding the devices on a per-device basis or in bulk.

### Assign devices on a per-device basis

1. In the Endpoint Management console, navigate to **Manage > Devices > Device Allow List**.



2. To add each device, click **Add**.

The screenshot shows a web form titled "Add Whitelist Device" with the following fields and controls:

- Device platform \***: A dropdown menu with "-- Select --" selected.
- Device ID Type \***: A dropdown menu with "-- Select --" selected.
- Device ID \***: A text input field with a copy icon and a help icon.
- Associated User**: A text input field.
- Select domain \***: A dropdown menu.
- Search for user \***: A text input field with a search icon and a "Search" button.
- Cancel** and **Save** buttons at the bottom right.

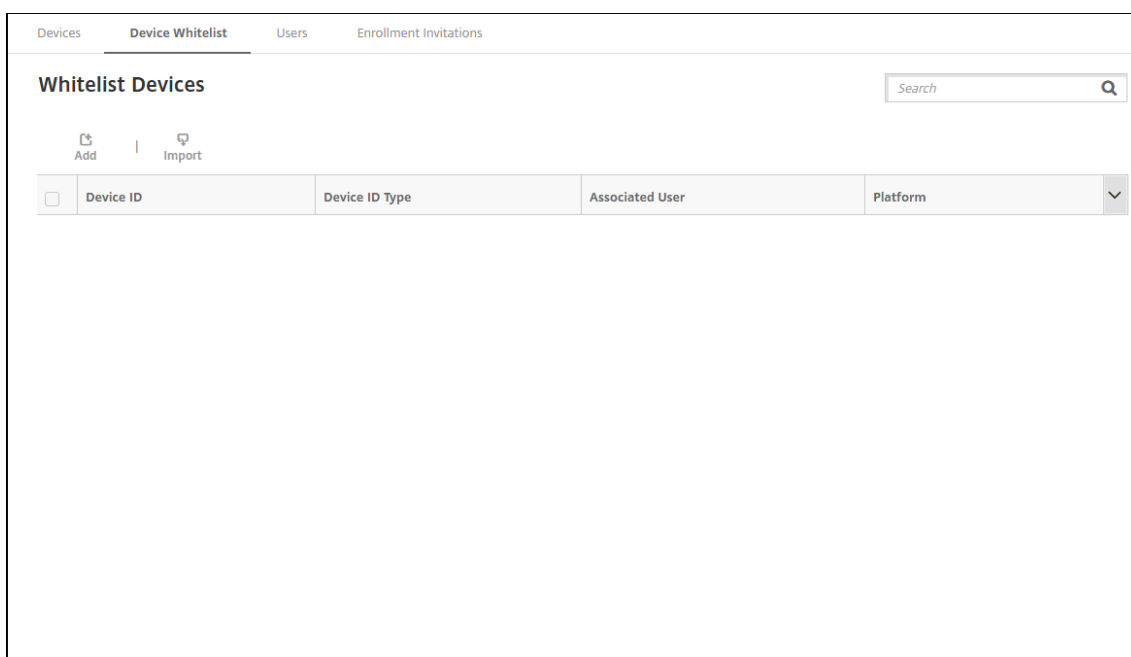
3. Type the following information:

- **Device platform:** Select **Windows**.
- **Device ID Type:** Select an ID that identifies the device. Endpoint Management supports **Hardware ID** and **Device Name** for Windows devices.
- **Device ID:** Type the ID corresponding to the type you selected previously for the device.
- **Associated User:** Displays the associated user for this device. This field automatically populates with the user you select.
- **Select domain:** Select the domain from which you want to search for an associated user.
- **Search for user** Type a full or partial user name in this field and click **Search** to find a user to associate with this device.

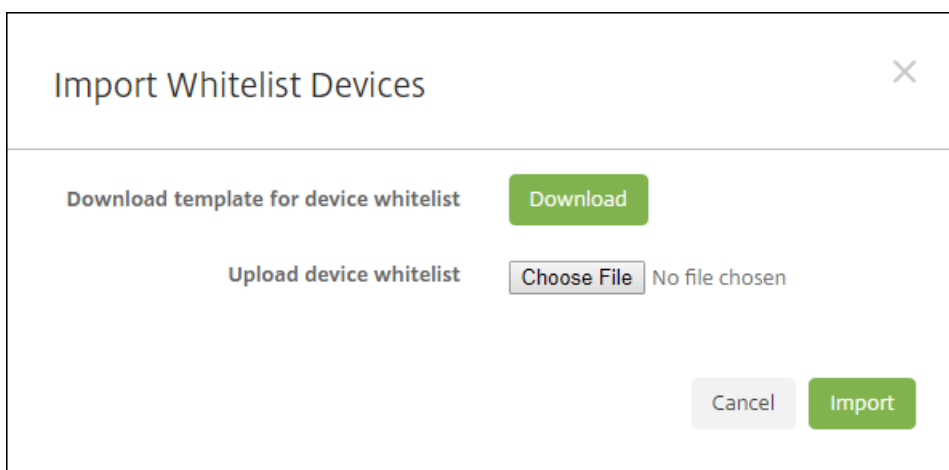
4. Click **Save**.

### Add devices in bulk

1. In the Endpoint Management console, navigate to **Manage > Devices > Device Allow List**.



2. Click **Import**.



3. Click **Download** to download a template (spreadsheet) for the device allow list. Fill out that spreadsheet and then upload the spreadsheet using **Choose File** and **Import**.

### Configure bulk enrollment

1. In the Endpoint Management console, navigate to **Settings > Windows Bulk Enrollment**.
2. In the **UPN** field, type a user name through which to deploy all devices. The UPN must be a valid user in Endpoint Management that has the enrollment permissions. You can provide a UPN that is different from the associated user you selected previously.

Settings > Windows Bulk Enrollment

## Windows Bulk Enrollment

Configure Windows bulk enrollment settings

Authentication policy OnPremise

UPN \*  ?

Discovery service URL

Enrollment service URL

Policy service URL

URLs appear here

You need the URLs when creating a provisioning package in the Windows Configuration Designer.

3. Click **Save**.

### Create and apply a provisioning package

To bulk provision devices, download the Windows Configuration Designer from the Microsoft Store. The Windows Configuration Designer creates provisioning packages used to image devices. As part of these packages, you can include Endpoint Management bulk enrollment configuration settings so that provisioned devices automatically enroll into Endpoint Management.

For information about using a provisioning package, see <https://docs.microsoft.com/en-us/windows/client-management/mdm/bulk-enrollment-using-windows-provisioning-tool>. Follow the steps described in the *Create and apply a provisioning package for on-premises authentication* section in that document. You follow those steps to include the following Endpoint Management bulk enrollment configuration settings and to apply the package to each device.

- **Discovery service URL.**
- **Enrollment service URL.**
- **Policy service URL.**
- **Secret.** Password of the UPN. You previously typed the user name in the UPN field.

## Bulk enroll devices out of the box

Endpoint Management supports bulk enrollment of Windows devices out of the box. Follow these steps to set up and perform bulk enrollment:

1. Use the Endpoint Management console to add devices (on a per-device basis or in bulk) and to configure bulk enrollment. For more information, see [Add devices in bulk](#) and [Configure bulk enrollment](#).
2. Create a provisioning package, as described in [Create and apply a provisioning package](#).

**Note:**

You need to configure the device name for each device when creating a provisioning package. To do so, in Windows Configuration Designer, navigate to **Runtime settings > Accounts > ComputerAccount > ComputerName** and specify the name of the device. The device name you specify for each device must align with the name you used when importing allow list devices.

3. Place that provisioning package into a USB stick.
4. Insert the USB stick into the target device the first time the user turns on the device.

Windows device automatically discovers the provisioning package (.ppkg) on the USB stick. For detailed instructions, see the Microsoft documentation at <https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package?redirectedfrom=MSDN#during-initial-setup-from-a-usb-drive>.

The device automatically enrolls into Endpoint Management.

For devices running Windows 10 (version 2004 or later) or Windows 11, you can simplify the enrollment process by creating only one provisioning package. The package can then be applied to all devices. As a result, you no longer need to create a provisioning package on a per-device basis.

To simplify the enrollment process, perform these steps when creating a provisioning package:

1. In Windows Configuration Designer, navigate to **Runtime settings > Accounts > ComputerAccount > ComputerName**.
2. In the **ComputerName** field, include the following string as part of the device name: %SERIAL%. For example: *Surface-%SERIAL%*. The string expands to the BIOS serial number of each device.

## Workspace hub device management

March 17, 2021

Citrix Ready workspace hub devices let users move virtual app and desktop sessions from a mobile device running Citrix Workspace app to a Citrix Ready workspace hub. The Citrix Ready workspace hub is a Raspberry Pi device that has a keyboard, mouse, monitor, and any other accessory attached to it. You can manage Citrix Ready workspace hub devices from your Endpoint Management console. For more information about Citrix Ready workspace hub, see [Citrix Ready workspace hub](#) and this [Citrix blog post](#).

By using Endpoint Management to manage Citrix Ready workspace hub, you can keep your devices updated with the latest features and security patches. You can also perform security actions, such as full wipes or restarts. For more details about the unified endpoint management (UEM) and data protection benefits of Endpoint Management, see this [use case on the Citrix website](#).

A general workflow for the workspace hub device management is as follows:

1. Complete the onboarding process. See [Onboarding and resource setup](#) and [Prepare to enroll devices and deliver resources](#).
2. Add Citrix Ready workspace hubs to the Device Allow List table in the Endpoint Management Console, using either of the following methods:
  - To add Citrix Ready workspace hubs to Endpoint Management manually
  - To import or export Citrix Ready workspace hub devices in bulk
3. Configure a Citrix Ready workspace hub.
4. Deploy custom configurations to Citrix Ready workspace hub devices.
5. Deploy the Citrix Workspace configuration to Citrix Ready workspace hub devices.
6. Configure Citrix Ready workspace hub device policies.
7. Deploy and update apps for Citrix Ready workspace hub.
8. Set up security actions. See [Security actions](#).

For supported operating systems, see [Supported device operating systems](#).

### **To add Citrix Ready workspace hubs to Endpoint Management manually**

To enroll a Citrix Ready workspace hub in Endpoint Management, you can manually add the device to the Device Allow List table in the Endpoint Management console.

A workspace hub device must enroll from the same region where Citrix Endpoint Management is located. For example, if your home region is European Union, the device must enroll while in that region. After a workspace hub device enrolls from your home region and the device roams to a different geographical region, workspace hub works as usual.

If a workspace hub device has to enroll when outside of the home region, the Service URL will contain an incorrect home region. You can change the Service URL in the Stratodesk configuration to point to the correct home region, as follows.

1. On the Stratodesk system: Go to **Services > NoTouch Center > Central Management URL**.
2. Change the **Management URL** to include the URL for your home region.
  - Asia Pacific South (Asia, Australia/Pacific, Middle East): `manageiot-apse.xm.cloud.com`
  - European Union: `manageiot-eu.xm.cloud.com`
  - United States (Africa, Antarctica, Caribbean, Central America, North America, South America): `manageiot-us.xm.cloud.com`
3. Save the configuration.
4. Go to **Information > NoTouch Center** and then click **Announce**.

For example, if your home region is in the U.S. and the Workspace hub device has to enroll while in the U.K.: Change the Service URL in Stratodesk from `https://manageiot-eu.xm.cloud.com:443/easyadmin/servlet/XmlRPC` to `https://manageiot-us.xm.cloud.com:443/easyadmin/servlet/XmlRPC`.

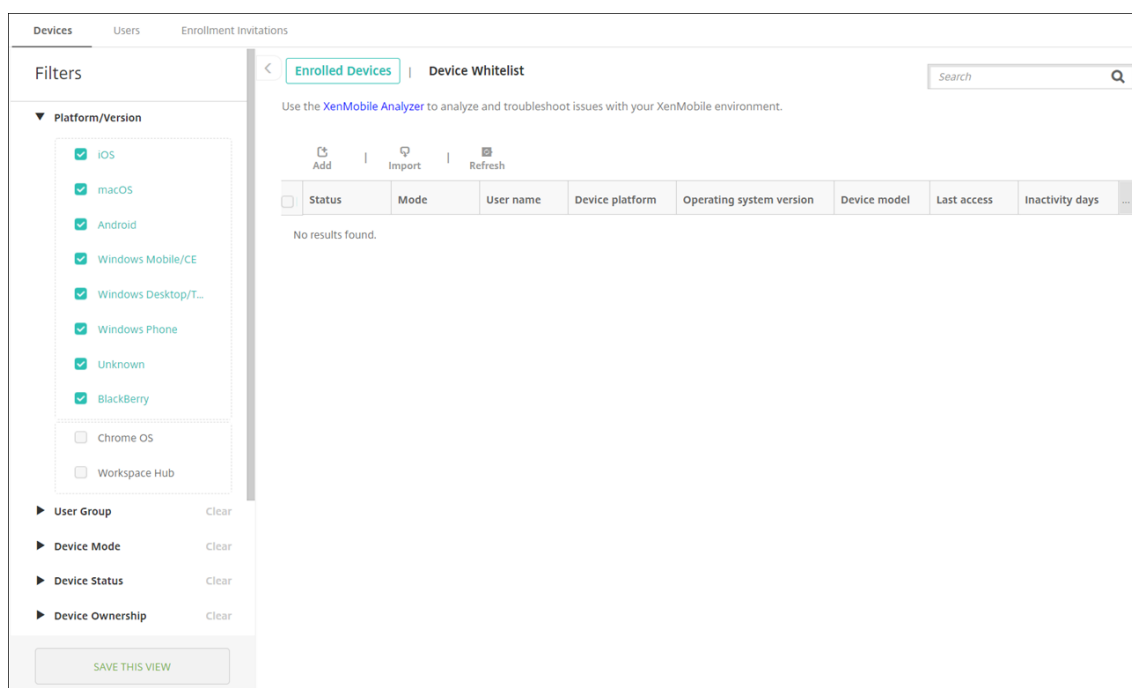
### Prerequisite

The configuration steps in this section include specifying a domain for Citrix Ready workspace hub users. Workspace hub uses email-based management server lookup. The lookup requires that you create a DNS SRV record named `_tcmgr._tcp.mycompany.com`, where `mycompany.com` is your domain name.

For more information, see the NComputing documentation article, [E-mail based management server lookup](#).

### To add a device to the Device Allow List table

1. In the Endpoint Management console, navigate to **Manage > Devices**.



2. Click **Device Allow List** at the top.



3. Click **Add**. On the page that opens, type the following information.

- **Device platform:** Select **Workspace Hub**.
- **Device ID Type:** Select the method to identify devices. Citrix Ready workspace hub only supports **MAC address**. For the device registration process, the eth0 MAC address is used, regardless of which connection type you choose.
- **Device ID:** Type the appropriate identifier you selected previously.
- **Associated User:** User to associate with the Citrix Ready workspace hub. The user associated with the device can be a pseudo user, such as a service account. The selected user is used for enrollment, policy pushing, and applying security actions. A single user can associate with multiple devices. This user can be a Local user or LDAP user already configured in your Endpoint Management console. If you want to associate the Citrix Ready workspace hub with a local user, choose **Local** from **Select domain**. Enter the user name in **Search for user** and select the user. If you want to associate the Citrix Ready workspace hub with an LDAP user, choose the appropriate domain from **Select domain**. Search for a user in **Search for user** and select the user.
- **Select domain:** Select the domain to use when searching for users.



- **Search for user:** Type the user name you want to associate with this device and click **Search**. Select the user from the result box. The user appears in the **Associated User** box.

The screenshot shows the 'Devices' tab in the Citrix Endpoint Management console. The form contains the following fields and controls:

- Device platform \***: A dropdown menu with "-- Select --" as the selected option.
- Device ID Type \***: A dropdown menu with "-- Select --" as the selected option.
- Device ID \***: A text input field with a lock icon on the right.
- Associated User**: A text input field that is currently empty.
- Select domain \***: A dropdown menu.
- Search for user \***: A text input field with a search icon on the right.
- Search**: A blue button located to the right of the search input field.

4. Click **Save**. The device is added to the table.

### To import or export Citrix Ready workspace hub devices in bulk

To enroll a Citrix Ready workspace hub in Endpoint Management, you can import or export the devices in bulk to the Device Allow List table.

1. In the Endpoint Management console, navigate to **Manage > Devices**. Click **Device Allow List** and then click **Import**.

The screenshot shows the 'Import Whitelist Devices' dialog box. It contains the following elements:

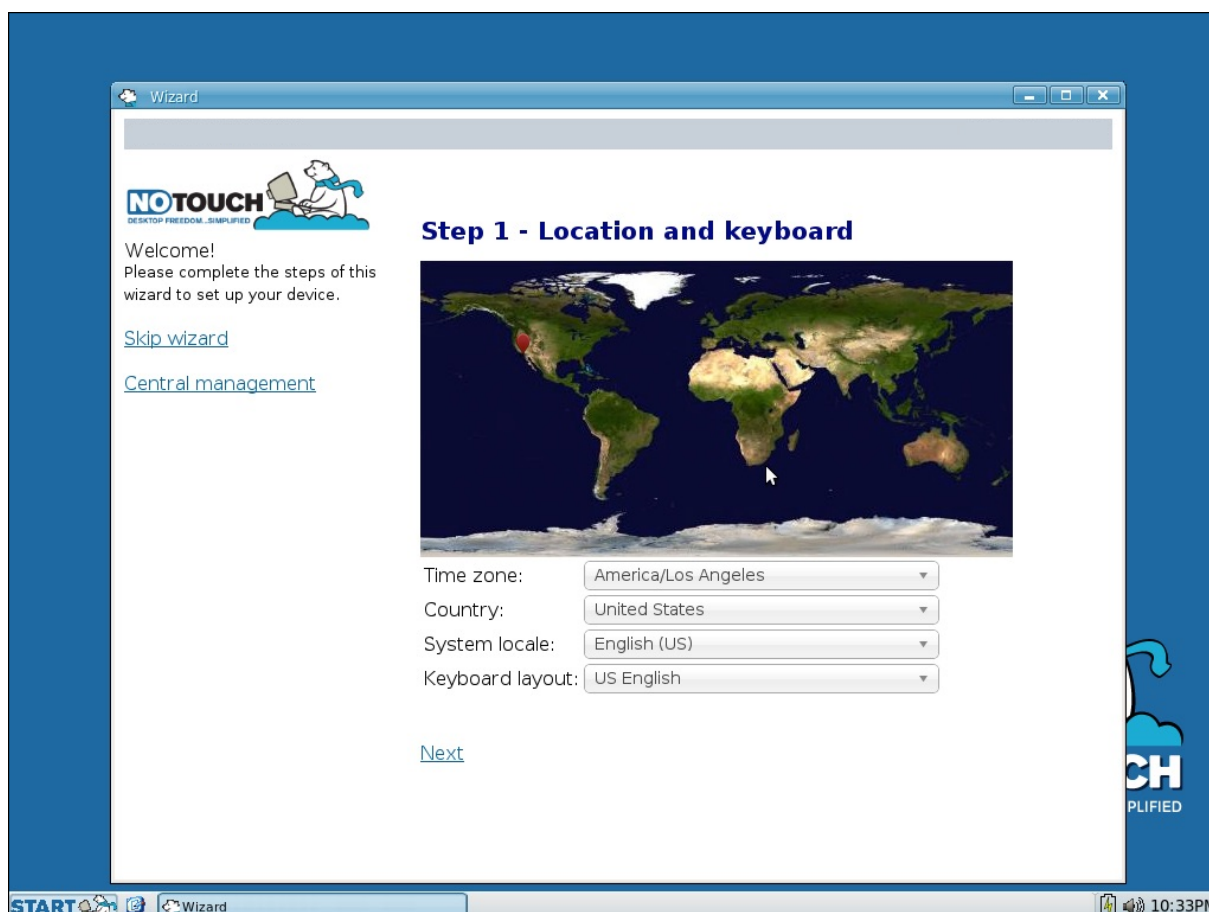
- Download template for device whitelist**: A text label next to a green **Download** button.
- Upload device whitelist**: A text label next to a **Choose File** button and the text "No file chosen".
- Cancel**: A grey button at the bottom right.
- Import**: A green button at the bottom right.

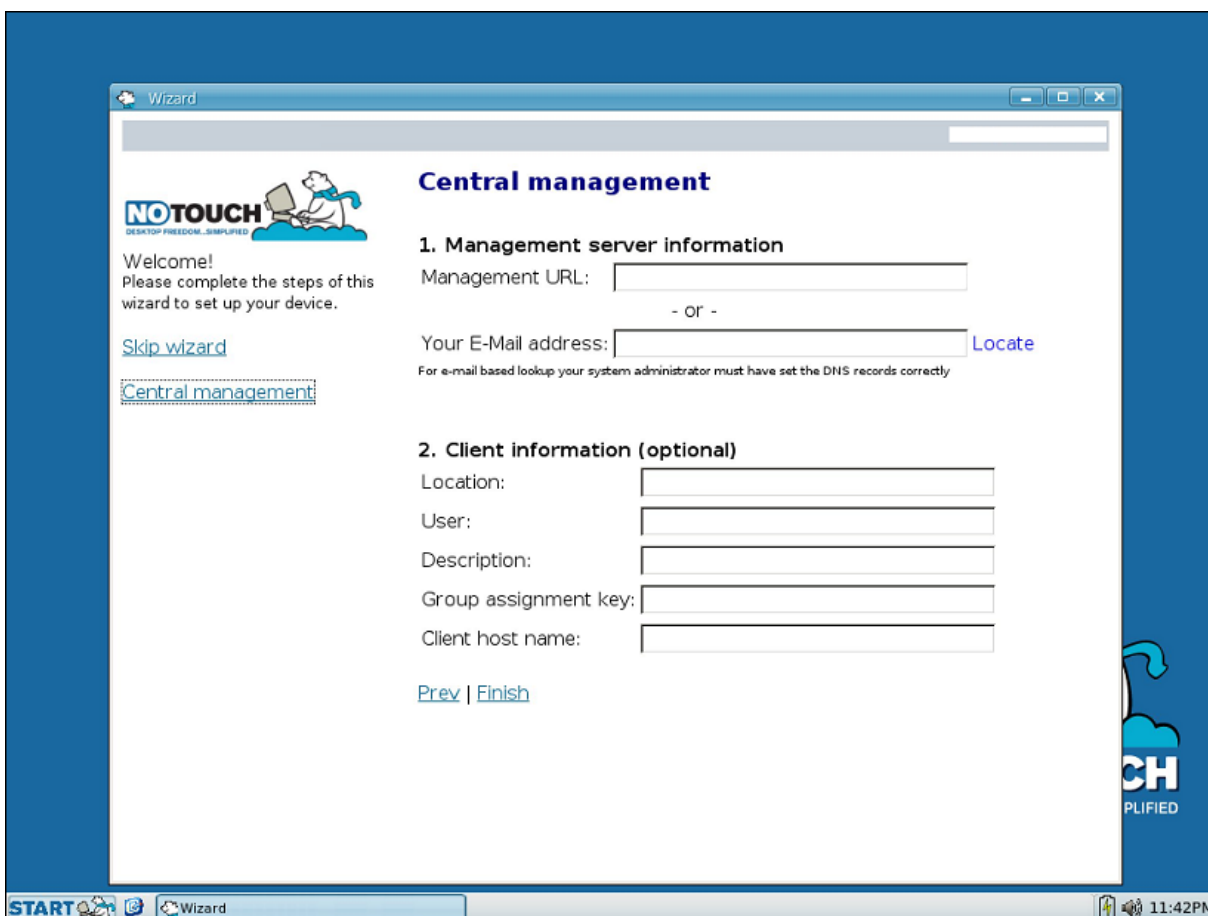
2. Click **Download** to download a .csv template for importing devices. The columns in the file are the same as the fields in the previous workflow.
3. Fill out the form and save it. When finished, click **Choose File** and select the template.
4. Click **Import**. All Citrix Ready workspace hubs in the template file are added to the table.
5. To export the list of Citrix Ready workspace hubs for editing, click **Export**.

## Configure a Citrix Ready workspace hub

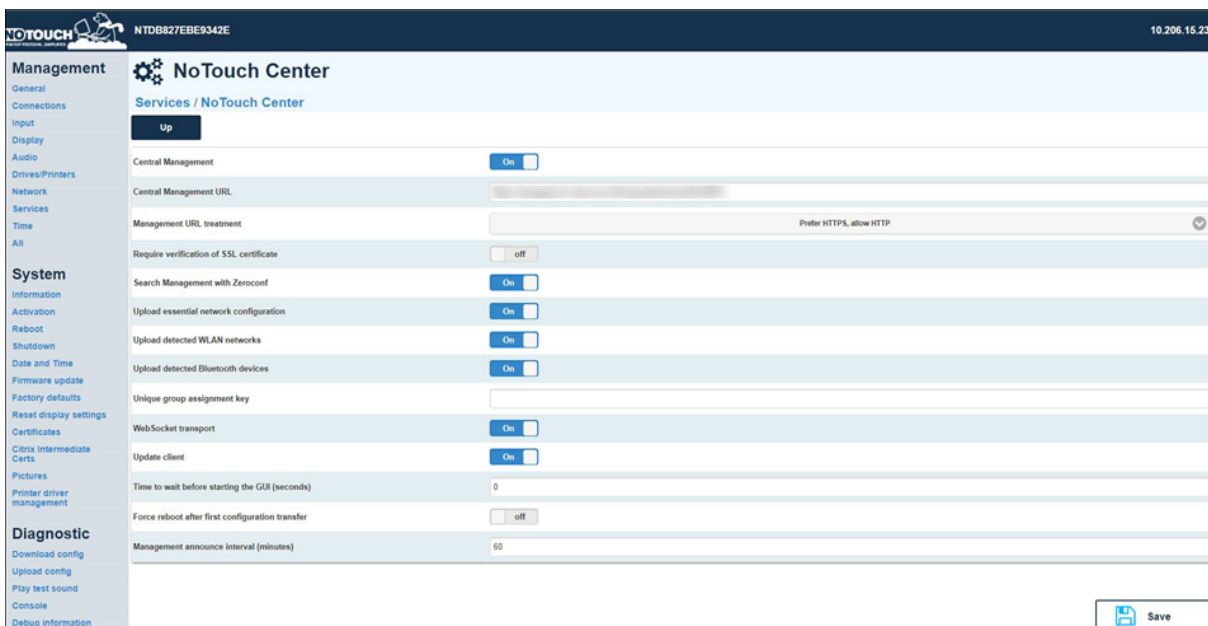
After configuring Endpoint Management to enroll your Citrix Ready workspace hub devices, configure the workspace hub device itself. For more information on configuring the device, see the Stratodesk Knowledge Base.

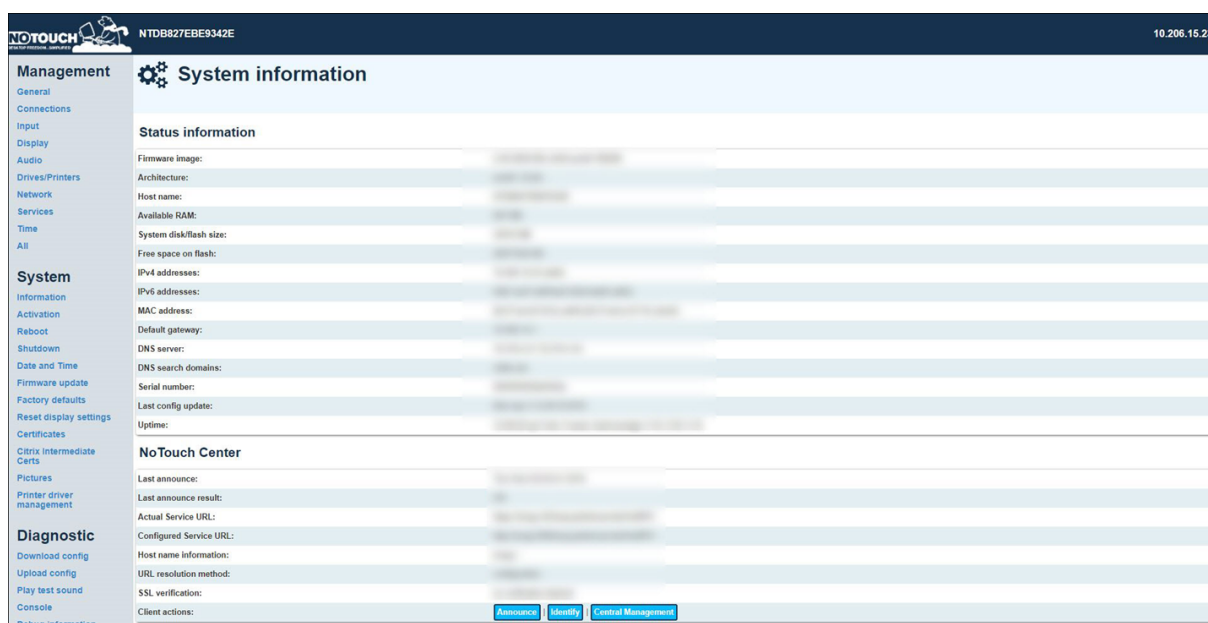
For first-time device use, configure Central Management during the first time wizard. Enter <https://manageiot.xm.cloud.com:443/easyadmin/servlet/XMLRPC> as the **Management URL** and then click **Finish**. The device performs an Announce and enrolls in Endpoint Management.





If the device was configured, or if you don't want to use the wizard, navigate to **Services > No Touch Center**. Configure the **Management URL** as you did previously and **Save**. Do a manual Announce by navigating to **Information** on the left pane and clicking **Announce**.





## Deploy custom configurations to Citrix Ready workspace hub devices

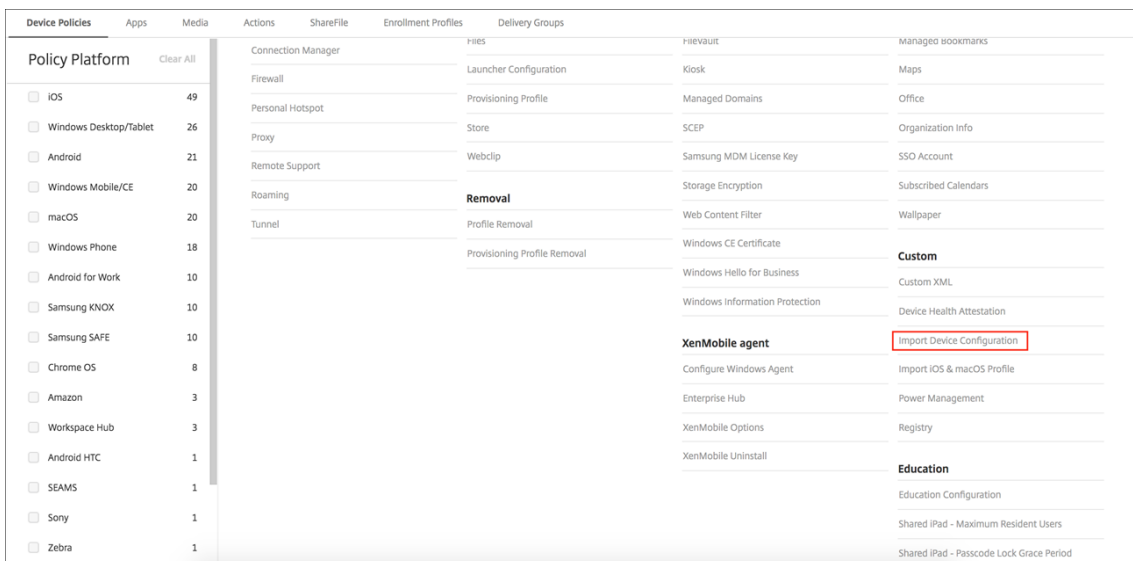
You can deploy custom configurations to Citrix Ready workspace hub devices. After manually configuring your first workspace hub device, you then download the configuration from the device and deploy the configuration to all other devices.

Requirements:

- Workspace hub device running Stratodesk NoTouch OS v2.40.3512 (minimum version)

To set up and deploy custom configurations:

1. Configure your Citrix Ready workspace hub device and download the configuration file.
  - a) Log in to the Workspace Hub console from a remote machine.
  - b) Set up network shares, printer configuration, and any other settings you want shared across devices on your Citrix Ready workspace hub device.
  - c) In the left pane of your workspace hub console, click **Download config**.
  - d) The .config file downloads to the remote machine where you're logged in.
2. Host the configuration file on a file sharing web server. Ensure that the file share isn't protected with any authentication.
3. On your Endpoint Management console, navigate to **Configure > Device Policies** and select **Import Device Configuration**.



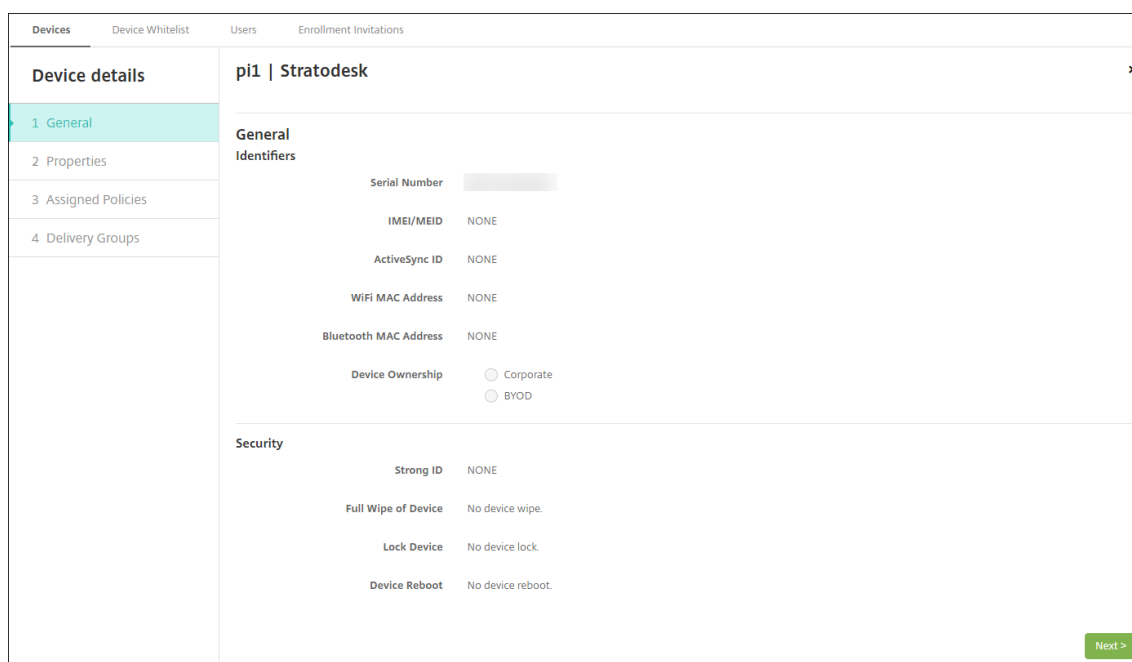
4. Type a **Policy Name** and, optionally, a **Description**. Click **Next**.
5. Paste the URL for the configuration file and click **Next**.
6. Configure your deployment rules. For information on configuring those rules, see [Device policies](#). Click **Save**.
7. Within a few minutes after the policy pushes to devices, enrolled devices show the configured settings. Those settings include network shares, desktop wallpapers, and connections.

If the device doesn't reflect the configuration, check the configuration URL in your Citrix Ready workspace hub device console. Navigate to **Services > NoTouch Center**. Then confirm that the **Configuration archive URL** is the URL where you hosted the configuration file.

### To manage Citrix Ready workspace hub devices

1. To view and manage Citrix Ready workspace hubs in Endpoint Management after enrollment, navigate to **Manage > Devices**. The **Devices** table appears. Select **Workspace Hub** on the left to see the newly enrolled device. Choose the Citrix Ready workspace hub you want to manage, and then click **Edit** to view and confirm the device details.

When you select the check box next to a device, the options menu appears above the device list. If you click anywhere else in the list, the options menu appears on the right side of the listing.



- The **General** page lists device **Identifiers** for the platform type, such as the serial number, ActiveSync ID, and other information. For **Device Ownership**, select **Corporate** or **BYOD**.

The **General** page also lists device **Security** properties, such as Strong ID, Lock Device, Activation Lock Bypass, and other information for the platform type.

- The remaining **Device Details** sections contain summary information for the device.
  - **Assigned Policies:** Displays the number of assigned policies including the number of deployed, pending, and failed policies. Provides the policy name, type and last deployed information for each policy.
  - **Apps:** Displays the apps that are installed, pending, or failed.
  - **Delivery Groups:** Displays the number of successful, pending, and failed delivery groups. For each deployment, provides the delivery group name and deployment time.

You can also perform security actions, such as full wipe or restart. For more information on security actions, see [Security actions](#).

## Deploy the Citrix Workspace configuration to Citrix Ready workspace hub devices

Use the App Configuration device policy to deploy the Citrix Workspace configuration to Citrix Ready workspace hub devices. Go to **Configure > Device Policies**, add the **App Configuration** policy, and, under **Platforms**, select **Workspace Hub**. Configure the following Workspace Hub settings:

- **Connection Mode:** Select **Citrix Receiver**.
- **Connection Name:** Type a descriptive name for your connection.
- **Connection Target:** Type a URL to load upon connection.

Some apps might require extra parameters to function. For each configuration parameter you want to add, click **Add** and then do the following:

- **Parameter name:** Type the key name of an application setting for the Citrix Ready workspace hub device.
- **Value:** Type the value for the specified parameter.

After you complete the configuration, choose delivery groups. For more information, see [Device policies](#).

## Configure Citrix Ready workspace hub device policies

Use these policies to configure how Endpoint Management interacts with the workspace hub devices. This table lists all device policies available for Citrix Ready workspace hub devices.

<a href="#">App Configuration</a>	<a href="#">Credentials</a>	<a href="#">Import Device Configuration</a>
<a href="#">Control OS Update</a>	<a href="#">Network</a>	

## Deploy and update apps for Citrix Ready workspace hub

1. Because Citrix Ready workspace hub devices only allow for deploying and updating a single file, first package all of your apps into a Squash FS file.

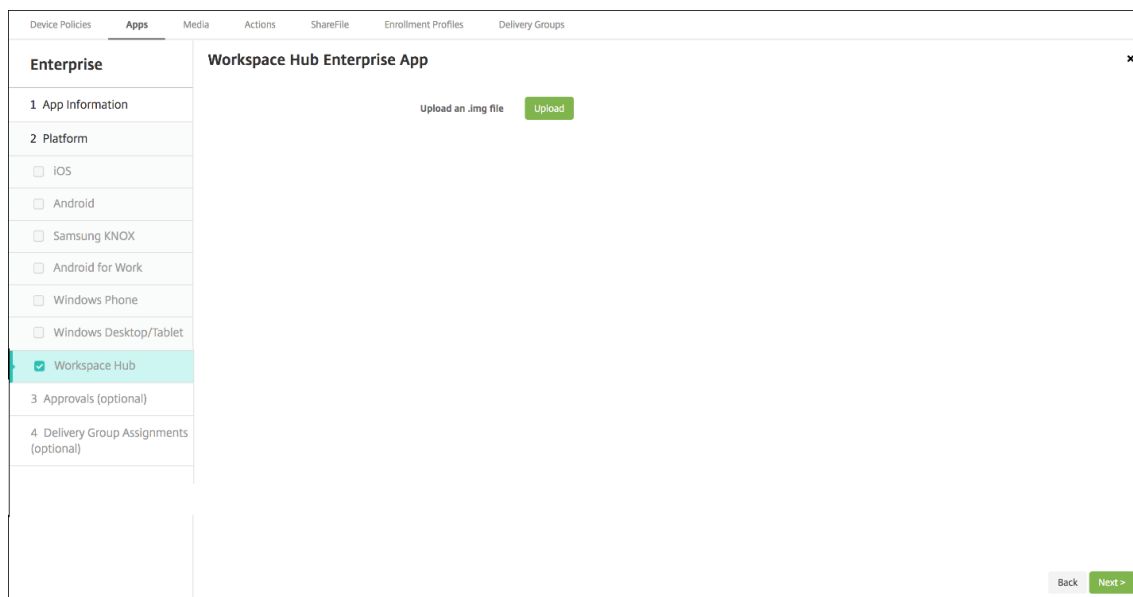
For more information on creating a Squash FS file, see the Squash FS documentation.

**Note:**

When creating the file, ensure that you output an .img file.

2. In the Endpoint Management console, navigate to **Configure > Apps** and click **Add**. Click **Enterprise**.

3. Type a name and description for your app, and then deselect all platforms except **Workspace Hub**. Click **Next**.
4. On the Workspace Hub Enterprise App page, click **Upload**. Navigate to the .img file you created previously and click **Open**.



5. Click **Next**. The **Approvals** page does not function for Citrix Ready workspace hub.
6. Click **Next**. The **Delivery Group Assignment** page appears.
7. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.

**Note:**

Apps are always delivered to the device assigned to the delivery group. It doesn't matter whether the app is optional or required because there is no store for Citrix Ready workspace hub devices.

8. Click **Save**.

After the apps upload to Endpoint Management, the workspace hub devices receive the update when restarted.

### Security actions

Workspace hub supports Full Wipe and Restart security actions. For a description of each security action, see [Security actions](#).



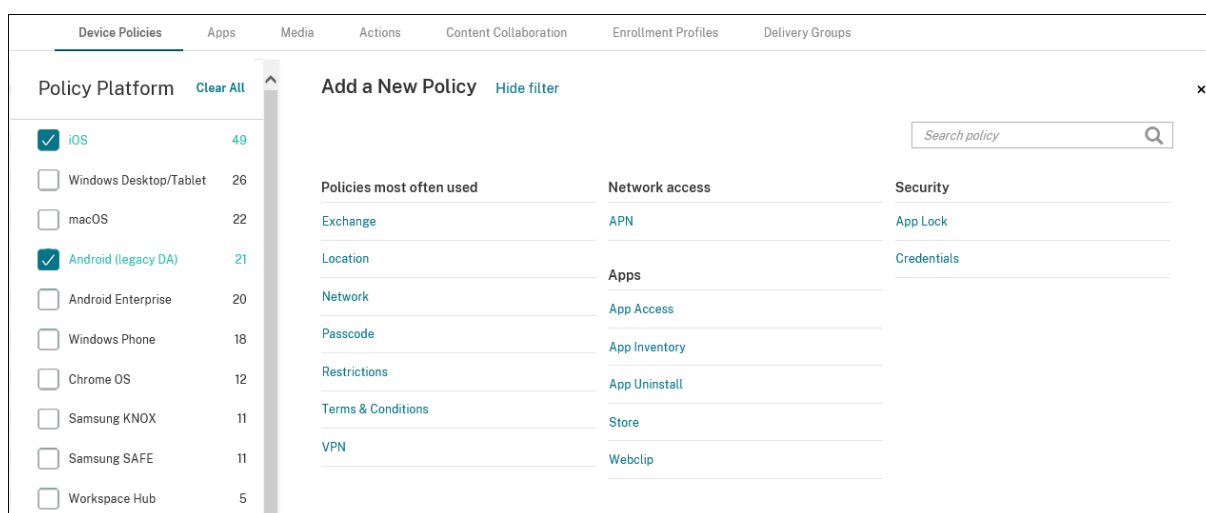
## Device policies

October 13, 2021

You can configure how Endpoint Management interacts with your devices by creating policies. Although many policies are common to all devices, each device has a set of policies specific to its operating system. As a result, you might find differences between platforms, and even between different manufacturers of Android devices.

To view the policies that are available per platform:

1. In the Endpoint Management console, go to **Configure > Device Policies**.
2. Click **Add**.
3. Each device platform appears in a list in the **Policy Platform** pane. If that pane isn't open, click **Show filter**.
4. To see a list of all policies available for a platform, select that platform. To see a list of the policies that are available for multiple platforms, select each of those platforms. A policy appears in the list only if it applies to each platform selected.



For a summary description of each device policy, see [Device policy summaries](#) in this article.

### Note:

If your environment is configured with Group Policy Objects (GPOs):

When you configure Endpoint Management device policies for Windows 10 and Windows 11, keep the following rule in mind. If a policy on one or more enrolled devices conflicts, the policy aligned with the GPO takes precedence.

To see which policies the Android Enterprise container supports, see [Android Enterprise](#).

## Prerequisites

- Create any delivery groups you plan to use.
- Install any necessary CA certificates.

## Add a device policy

The basic steps to create a device policy are as follows:

1. Name and describe the policy.

### Important:

Do not use a forward slash (/) in a policy name. If you do, an error might occur when you edit the policy later.

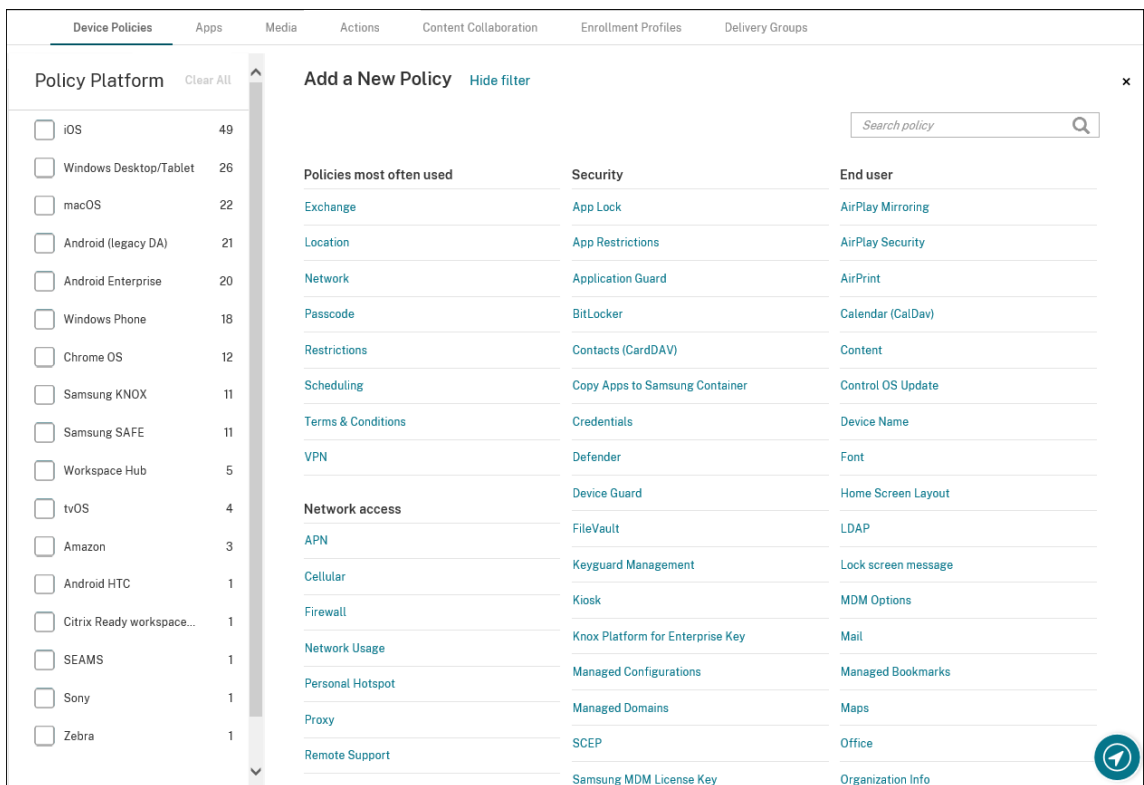
2. Configure the policy for one or more platforms.
3. Create deployment rules (optional).
4. Assign the policy to delivery groups.
5. Configure the deployment schedule (optional).

To create and manage device policies, go to **Configure > Device Policies**.

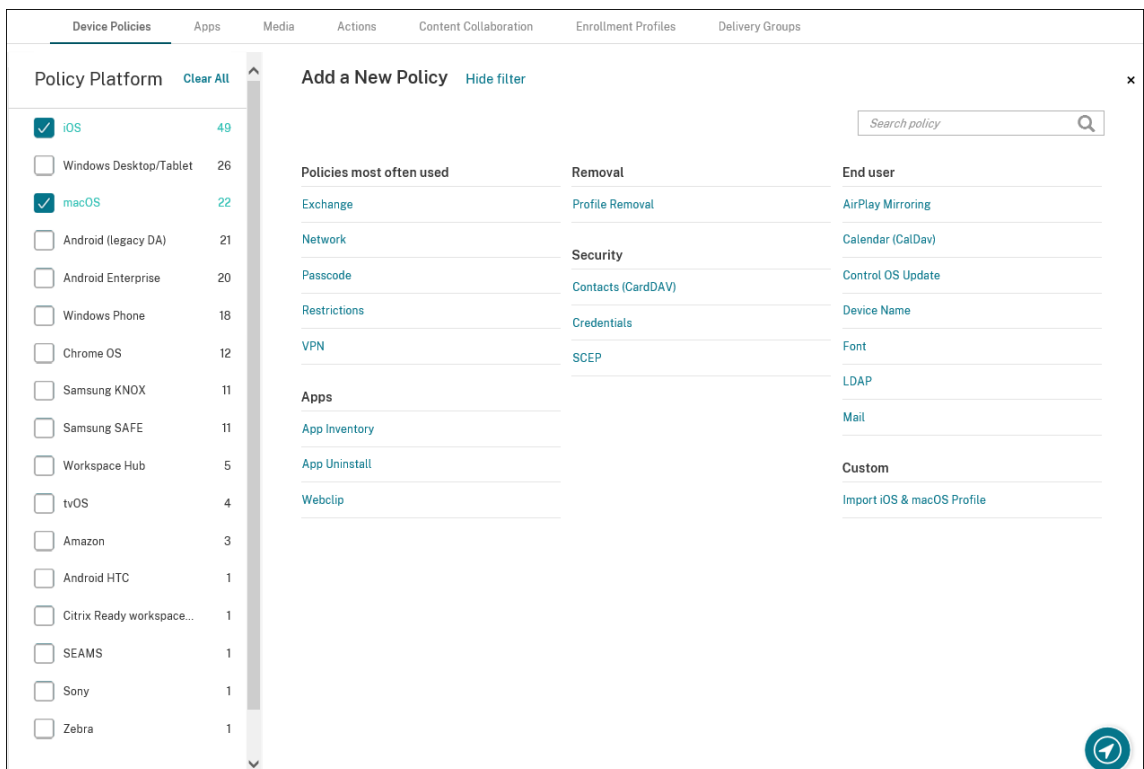
<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status
<input type="checkbox"/>	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM	
<input type="checkbox"/>	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM	
<input type="checkbox"/>	K--Webclip	Mdm Weblink	8/12/17 6:46 AM	8/12/17 6:46 AM	
<input type="checkbox"/>	K--Passcode	Password	8/12/17 6:47 AM	8/12/17 6:47 AM	
<input type="checkbox"/>	K--Wifi	Wifi	8/12/17 6:47 AM	8/12/17 6:47 AM	
<input type="checkbox"/>	K--T&C	Terms Conditions	8/12/17 6:48 AM	8/12/17 6:48 AM	

To add a policy:

1. On the **Device Policies** page, click **Add**. The **Add a New Policy** page appears.



2. Click one or more platforms to view a list of the device policies for the selected platforms. Click a policy name to continue with adding the policy.



You can also type the name of the policy in the search box. As you type, potential matches appear. If your policy is in the list, click it. Only your selected policy remains in the results. Click it to open the **Policy Information** page for that policy.

3. Select the platforms you want to include in the policy. Configuration pages for the selected platforms appear in Step 5.
4. Complete the **Policy Information** page and then click **Next**. The **Policy Information** page collects information, such as the policy name, to help you identify and track your policies. This page is similar for all policies.
5. Complete the platform pages. Platform pages appear for each platform you selected in Step 3. These pages are different for each policy. A policy might differ among platforms. Not all policies apply to all platforms.

Some pages include tables of items. To delete an existing item, hover over the line containing the listing and click the trash can icon on the right side. In the confirmation dialog, click **Delete**.

To edit an existing item, hover over the line containing the listing and click the pen icon on the right side.

### To configure deployment rules, assignments, and schedule

For more information about configuring deployment rules, see [Deploy resources](#).

1. On a platform page, expand **Deployment Rules** and then configure the following settings. The **Base** tab appears by default.
  - In the lists, click options to specify the deployment conditions. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is **All**.
  - Click **New Rule** to define the conditions.
  - In the lists, click the conditions, such as **Device ownership** and **BYOD**.
  - Click **New Rule** again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the **Advanced** tab to combine the rules with Boolean options. The conditions you chose on the **Base** tab appear.
3. You can use more advanced Boolean logic to combine, edit, or add rules.
  - Click **AND**, **OR**, or **NOT**.
  - In the lists, choose the conditions that you want to add to the rule. Then, click the Plus sign (+) on the right side to add the condition to the rule.

At any time, you can click to select a condition and then click **EDIT** or **Delete**.

- Click **New Rule** to add another condition.
4. Click **Next** to move to the next platform page or, when all the platform pages are complete, to the **Assignments** page.
  5. On the **Assignments** page, select the delivery groups to which you want to apply the policy. If you click a delivery group, the group appears in the **Delivery groups to receive app assignment** box.

**Delivery groups to receive app assignment** doesn't appear until you select a delivery group.

6. On the **Assignments** page, expand **Deployment Schedule** and then configure the following settings:
  - Next to **Deploy**, click **On** to schedule deployment or click **Off** to prevent deployment. The default option is **On**.
  - Next to **Deployment schedule**, click **Now** or **Later**. The default option is **Now**.
  - If you click **Later**, click the calendar icon and then select the date and time for deployment.
  - Next to **Deployment condition**, click **On every connection** or click **Only when previous deployment has failed**. The default option is **On every connection**.
  - Next to **Deploy for always-on connection**, click **On** or **Off**. The default option is **Off**.

**Note:**

This option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.

The always-on option:

- Is not available for iOS devices
- Is not available for Android, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with version 10.18.19 or later
- Is not recommended for Android, Android Enterprise, and Chrome OS to cus-

tomers who began using Endpoint Management with before version 10.18.19

The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

▼ **Deployment Schedule** ?

**Deploy**  ON

**Deployment Schedule**  Now  Later

**Deployment condition**  On every connection  Only when previous deployment has failed

**Deploy for always-on connections**  OFF ?

7. Click **Save**.

The policy appears in the **Device Policies** table.

## Remove a device policy from a device

The steps to remove a device policy from a device depends on the platform.

- Android

To remove a device policy from an Android device, use the Endpoint Management Uninstall device policy. For information, see [Endpoint Management uninstall device policy](#).

- iOS and macOS

To remove a device policy from an iOS or macOS device, use the Profile Removal device policy. On iOS and macOS devices, all policies are part of the MDM profile. Thus, you can create a Profile Removal device policy for just the policy that you want to remove. The rest of the policies and the profile remain on the device. For information, see [Profile Removal device policy](#).

- Windows 10 and Windows 11

You can't directly remove a device policy from a Windows Desktop or Tablet device. However, you can use either of the following methods:

- Unenroll the device and then push a new set of policies to the device. Users then re-enroll to continue.
- Push a security action to selectively wipe the specific device. That action removes all corporate apps and data from the device. You then remove the device policy from a delivery

group that contains just that device and push the delivery group to the device. Users then re-enroll to continue.

- Chrome OS

To remove a device policy from a Chrome OS device, you can remove the device policy from a delivery group that contains just that device. You then push the delivery group to the device.

## Edit a device policy

To edit a policy, select the check box next to a policy. The options menu appears above the policy list. Or, click a policy in the list to show more controls.

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status	▼
<input type="checkbox"/>	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM		
<input checked="" type="checkbox"/>	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM		
<input type="checkbox"/>	K--Webclip	Mdm Weblink				
<input type="checkbox"/>	K--Passcode	Password				
<input type="checkbox"/>	K--Wifi	Wifi				
<input type="checkbox"/>	K--T&C	Terms Conditions				
<input type="checkbox"/>	K--Location	Locationservices				
<input type="checkbox"/>	K--EAS	Exchange				
<input type="checkbox"/>	K--AppLock	Applock				

Edit
Delete

---

**Deployment**

0  
 Installed

0  
 Pending

0  
 Failed

Show more >

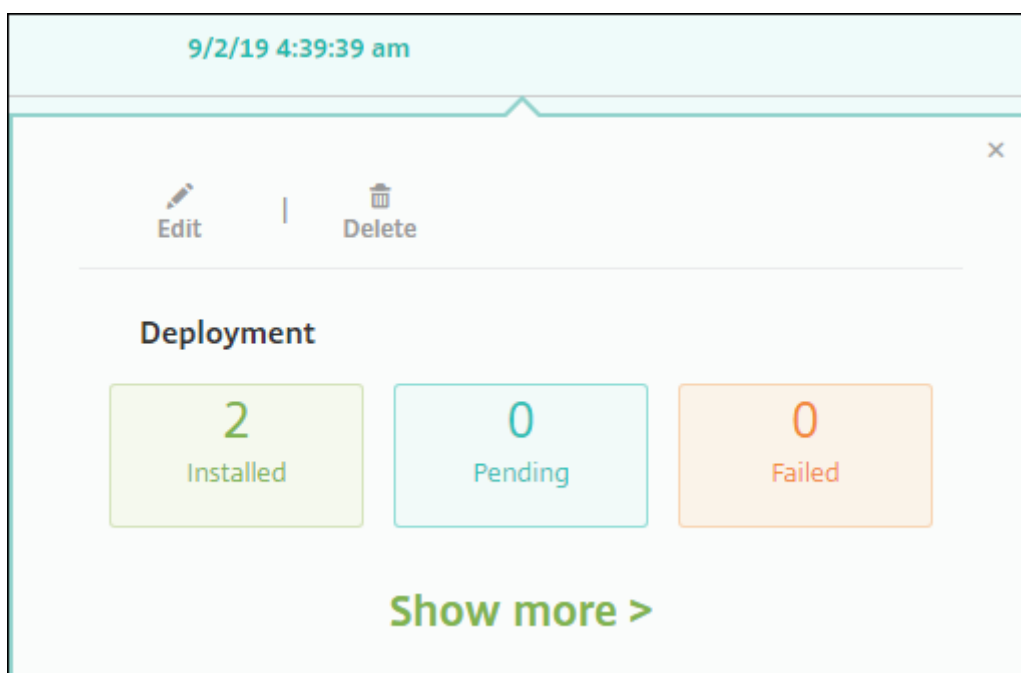
To view policy details, click **Show more**.

To edit all settings for a device policy, click **Edit**.

If you click **Delete**, a confirmation dialog box appears. Click **Delete** again to delete the policy.

## Check policy deployment status

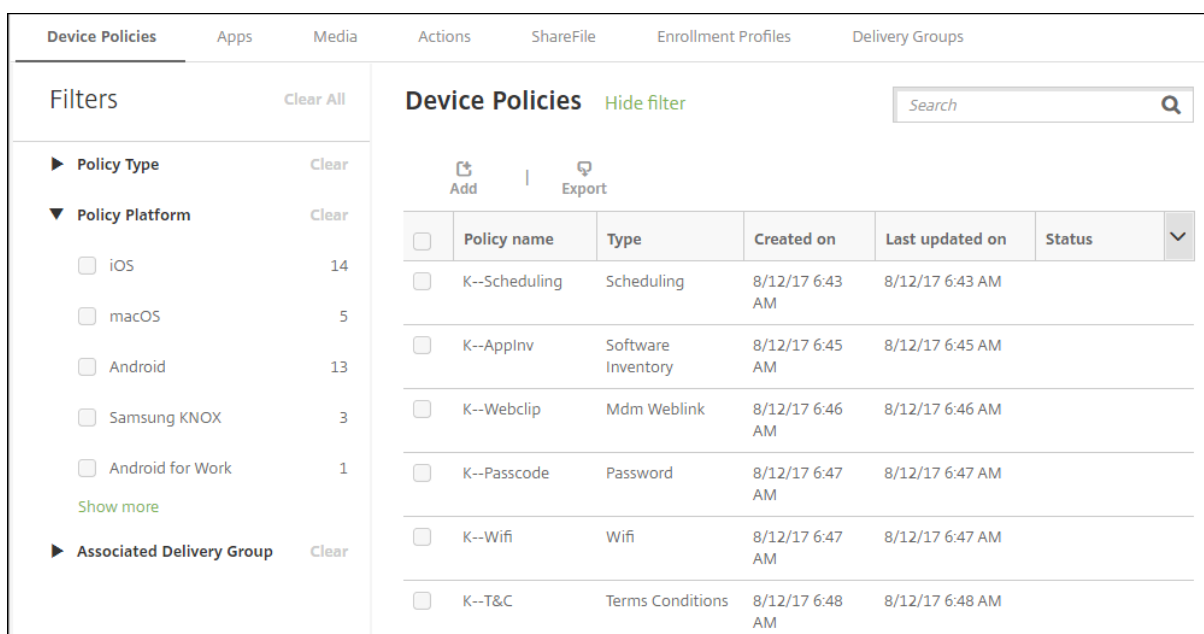
Click a policy row on the **Configure > Device Policies** page to check its deployment status.



When a policy deployment is pending, users can refresh the policy from Secure Hub by tapping **Preferences > Device Information > Refresh policy**.

### Filter the list of added device policies

You can filter the list of added policies by policy types, platforms, and associated delivery groups. On the **Configure > Device Policies** page, click **Show filter**. In the list, select the check boxes for the items you want to see.





Click **SAVE THIS VIEW** to save a filter. The name of the filter then appears in a button below the **SAVE THIS VIEW** button.

## Device policy summaries

Device Policy Name	Device Policy Description
AirPlay Mirroring	Adds specific AirPlay devices (such as Apple TV or another Mac computer) to iOS devices. You can also add devices to an allow list for supervised devices. That option limits users to only the AirPlay devices on the allow list.
AirPrint	Adds AirPrint printers to the AirPrint printer list on iOS devices. This policy makes it easier to support environments where the printers and the devices are on different subnets.
APN	Determines the settings used to connect your devices to the General Packet Radio Service (GPRS) of a specific phone carrier. This setting is already defined in most new phones. Use this policy if your organization doesn't use a consumer APN to connect to the internet from a mobile device.
App Access	Defines a list of the apps that are required, optional, or prevented on the device. You can then create an automated action to react to the device compliance with that list of apps.
App Attributes	Specifies attributes, such as a managed app bundle ID or per-app VPN identifier, for iOS devices.
App Configuration	Remotely configures various settings and behaviors of apps that support managed configuration. To do that, you deploy an XML configuration file (called a property list, or <code>plist</code> ) to iOS devices. Or, you deploy key/value pairs to Windows 10 phone, desktop, or tablet devices.

<b>Device Policy Name</b>	<b>Device Policy Description</b>
App Inventory	Collects an inventory of the apps on managed devices. Endpoint Management then compares the inventory to any app access policies deployed to those devices. In this way, you can detect apps that are on an allow list or block list for app access and then act accordingly.
App Lock	Defines a list of apps that users either can or can't run on iOS or certain Android devices. Can turn an iPad into a kiosk.
App Permissions	Configures how requests to Android Enterprise apps within work profiles handle what Google calls "dangerous" permissions.
App Restrictions	Creates block lists for apps you want to prevent users from installing on Samsung Knox devices. You can also create allow lists for the apps you permit users to install.
App Uninstall	Remove apps from user devices.
App Uninstall Restrictions	Specifies the apps that users can or can't uninstall.
Application Guard	For the Microsoft Edge browser only, this policy specifies Windows Defender Application Guard settings. The settings include whether to block external content on enterprise sites.
Apps Notifications	Controls how iOS users receive notifications from specified apps.
Automatically update managed apps	Controls how installed managed apps are updated on Android Enterprise devices.
BitLocker	Configures the settings available in the BitLocker interface on Windows 10 and Windows 11 devices.
Browser	Defines whether user devices can use the browser or which browser functions the devices can use.

<b>Device Policy Name</b>	<b>Device Policy Description</b>
Calendar (CalDAV)	Adds a calendar (CalDAV) account to iOS or macOS devices. The CalDAV account enables users to synchronize scheduling data with any server that supports CalDAV.
Cellular	Configures cellular network settings.
Connection scheduling	Required for Android devices to connect back in to Endpoint Management for MDM management, app push, and policy deployment. If you don't send this policy to devices and don't enable Google FCM, a device can't connect back to the server.
Contacts (CardDAV)	Adds an iOS contact (CardDAV) account to iOS or macOS devices. The CardDAV account enables users to synchronize contact data with any server that supports CardDAV.
Content	Controls various web content options for Chrome OS, including what home page to show and how popups are handled.
Copy apps to Samsung Container	Copies the apps already installed on a device to a Knox container on supported Samsung devices. Apps copied to the Knox container are available only when users sign in to the Knox container.
Credentials	Enables integrated authentication with your PKI configuration in Endpoint Management. For example, with a PKI entity, a keystore, a credential provider, or a server certificate.
Custom XML	Customizes features such as provisioning devices, enabling device features, configuring devices, and managing faults.
Defender	Configures Windows Defender settings for Windows 10 and Windows 11 for desktop and tablet.
Device Guard	Enable security features such as secure boot, UEFI lock, and virtualization.

<b>Device Policy Name</b>	<b>Device Policy Description</b>
Device Health Attestation	Requires that Windows 10 and Windows 11 devices report the state of their health. To do that they send specific data and runtime information to the Health Attestation Service (HAS) for analysis. The HAS creates and returns a Health Attestation Certificate that the device then sends to Endpoint Management. When Endpoint Management receives the Health Attestation Certificate, based on the contents of that certificate, it can deploy automatic actions that you configured.
Device Name	Sets the names on iOS and macOS devices so that you can identify the devices. You can use macros, text, or a combination of both to define a device name.
Education Configuration	Configures instructor and student devices for use with Apple Education. If instructors use the Classroom app, the Education Configuration device policy is required. Supported for iOS (iPadOS) devices.
Endpoint Management Options	Configures the Secure Hub behavior when connecting to Endpoint Management from Android devices.
Endpoint Management Uninstall	Uninstalls Endpoint Management from Android devices. When deployed, this policy removes Endpoint Management from all devices in the deployment group.
Enterprise Hub	Distributes apps to Windows Phones through the Enterprise Hub Company store. Endpoint Management supports only one Enterprise Hub policy for one mode of Windows Phone Secure Hub. For example, don't create multiple Enterprise Hub policies with different versions of Secure Home for Endpoint Management. You can deploy the initial Enterprise Hub policy only during device enrollment.

<b>Device Policy Name</b>	<b>Device Policy Description</b>
Exchange	Enables ActiveSync email for the native email client on the device.
Files	Adds script files to Endpoint Management that perform certain functions for users. Or, you can add document files that you want Android device users to be able to access on their devices. When you add the file, you can also specify the directory in which you want the file to be stored on the device.
FileVault	This policy lets you enable FileVault device encryption on enrolled macOS devices. You can also control how many times a user can skip FileVault setup during login. Available for macOS 10.7 or later.
Firewall	Configures the firewall settings. You provide the IP addresses, ports, and host names that you want to allow or block on devices. You can also configure the proxy and proxy reroute settings.
Font	Adds fonts to iOS and macOS devices. Fonts must be TrueType (.TTF) or OpenType (.OFT) fonts. Endpoint Management doesn't support font collections (.TTC, .OTC).
Home screen layout	Specifies the layout of apps and folders for the iOS Home screen on supervised iOS devices.
Import Device Configuration	Imports a template configuration file from Workspace Hub devices.
Import iOS & macOS Profile	Imports device configuration XML files for iOS and macOS devices into Endpoint Management. The file contains device security policies and restrictions that you prepare by using the Apple Configurator.

<b>Device Policy Name</b>	<b>Device Policy Description</b>
Keyguard Management	Controls the features available to users before they unlock the device keyguard and the work challenge keyguard. You can also control device keyguard features for fully managed and dedicated devices. For example, you can disable lock screen features such as fingerprint unlock, trust agents, and notifications.
Kiosk	Restricts app usage on Samsung SAFE devices. You can limit available apps to a specific app or apps. This policy is useful for corporate devices that are intended to run only a specific type or class of apps. This policy also lets you choose custom images for the device home screen and lock screen wallpapers for kiosk mode.
Knox Platform for Enterprise	Specifies the Knox Platform for Enterprise (KPE) Premium license key.
Launcher Configuration	Specifies settings for Citrix Launcher on Android devices, such as the apps allowed and a custom logo image for the Launcher icon.
LDAP	Provides information about an LDAP server to use for iOS devices, including any necessary account information such as the LDAP server host name. The policy also provides a set of LDAP search policies to use when querying the LDAP server.
Location	Lets you geo-locate devices on a map, assuming that the device has GPS enabled for Secure Hub. After deploying this policy to the device, you can send a locate command from Endpoint Management. The device then responds with its location coordinates. Endpoint Management also supports geofencing and tracking policies.

<b>Device Policy Name</b>	<b>Device Policy Description</b>
Lock screen message	Sets messages to appear on the following devices when they are lost: The login window of shared iPads and the lock screen of supervised iOS devices.
Mail	Configures an email account on iOS or macOS devices.
Managed Bookmarks	Deploys a folder of bookmarks to Chrome OS devices.
Managed Configurations	Controls various app configuration options and app restrictions for Android Enterprise devices.
Managed Domains	Defines managed domains that apply to email and the Safari browser. Managed domains help you protect corporate data by controlling which apps can open documents downloaded from domains using Safari. For iOS supervised devices, you can specify URLs or subdomains to control how users can open documents, attachments, and downloads from the browser.
Maps	Specifies which maps to download to supervised Windows 10 phone devices. The Microsoft Maps configuration service provider (CSP) only supports maps of Germany, the United Kingdom, and the United States.
Maximum resident users	Specifies the maximum number of users for a Shared iPad. Supported for iOS and iPadOS devices.
MDM Options	Manages Find My Phone and iPad Activation Lock on supervised iOS devices.
Network	Allows administrators to deploy Wi-Fi router details to managed devices. The router details include SSID, authentication data, and configuration data.

<b>Device Policy Name</b>	<b>Device Policy Description</b>
Network Usage	Sets network usage rules to specify how managed apps use networks, such as cellular data networks, on iOS devices. The rules only apply to managed apps. Managed apps are apps that you deploy to user devices through Endpoint Management.
Office	Deploy Microsoft Office apps to any devices running Windows 10 (version 1709 or later) or Windows 11.
Organization Info	Specifies organization information for alert messages that Endpoint Management deploys to iOS devices.
OS Update	Deploys the latest OS updates to devices that are supported and supervised.
Passcode	Enforces a PIN code or password on a managed device. You can set the complexity and timeouts for the passcode on the device.
Passcode lock grace period	Specifies the number of minutes that a Shared iPad screen stays locked before the user must enter a passcode to unlock the screen. Supported for iOS and iPadOS devices.
Personal Hotspot	Allows users to connect to the internet when they are not in range of a Wi-Fi network. Users connect through the cellular data connection on their iOS device, using personal hotspot functionality.
Power management	Controls how Chrome OS devices respond to idle periods when using AC or battery power.
Profile Removal	Removes the app profile from macOS devices.



---

<b>Device Policy Name</b>	<b>Device Policy Description</b>
Provisioning Profile	Specifies an enterprise distribution provisioning profile to send to devices. When you develop and code sign an iOS enterprise app, you usually include a provisioning profile. Apple requires the profile for the app to run on an iOS device. If a provisioning profile is missing or has expired, the app crashes when a user taps to open it.
Provisioning Profile Removal	Removes iOS provisioning profiles.
Proxy	Specifies global HTTP proxy settings for devices running iOS. You can deploy only one global HTTP proxy policy per device.
Public Session	Configure a Chrome OS device to act as a public device in guest mode.
Restrictions	Provides hundreds of options to lock down and control features and functionality on managed devices. Examples of restriction options: Disable the camera or microphone, enforce roaming rules, and enforce access to third-party services, such as app stores.
Roaming	Configures whether to allow voice and data roaming on iOS devices. If voice roaming is disabled, data roaming is automatically disabled.
Samsung MDM License Key	Specifies the built-in Samsung Enterprise License Management (ELM) key that you must deploy to a device before you can deploy SAFE policies and restrictions. Endpoint Management also supports the Samsung Enterprise Firmware-Over-The-Air (E-FOTA) service. Endpoint Management supports and extends both Samsung for Enterprise (SAFE) and Samsung Knox policies.

---

SCEP	Configures iOS and macOS devices to retrieve a certificate from an external SCEP server. You can also deliver a certificate to the device using SCEP from a PKI that is connected to Endpoint Management. To do that, create a PKI entity and a PKI provider in distributed mode.
Single sign-on (SSO) Account	Creates SSO accounts so users sign on one-time only to access Endpoint Management and your internal company resources. Users do not need to store any credentials on the device. Endpoint Management uses the enterprise user credentials for an SSO account across apps, including apps from the App Store. This policy is compatible with Kerberos authentication. Available for iOS.
Storage Encryption	Encrypts internal and external storage. For some devices, this policy prevents users from using a storage card on their devices.
Store	Specifies whether an app store web clip appears on the home screen of user devices.
Subscribed Calendars	Adds a subscribed calendar to the calendars list on iOS devices. Ensure that you subscribe to a calendar before you add it to the subscribed calendars list on user devices.
Terms and Conditions	Requires that users accept the specific policies of your company that govern connections to the corporate network. When users enroll their devices with Endpoint Management, they must accept the terms and conditions to enroll their devices. Declining the terms and conditions cancels the enrollment process.
Tunnel	Define proxy parameters between the client component of any mobile device app and the app server component.

VPN	Provides access to back end systems that use legacy VPN gateway technology. This policy provides VPN gateway connection details that you can deploy to devices. Endpoint Management supports several VPN providers, including Cisco AnyConnect, Juniper, and Citrix VPN. If your VPN gateway supports this option, you can link this policy to a CA and enable VPN on-demand.
Wallpaper	Adds a .png or .jpg file to set the wallpaper on an iOS device lock screen, home screen, or both. To use a different wallpaper on iPads and iPhones, create different wallpaper policies and deploy them to the appropriate users.
Web clip	Places shortcuts, or web clips, to websites so that they appear alongside apps on user devices. You can specify your own icons to represent the web clips for iOS, macOS, and Android devices. Windows tablet only requires a label and a URL.
Web Content Filter	Filters web content on iOS devices. Endpoint Management uses the Apple auto-filter function and the sites that you add to allow lists and block lists. Available only for iOS supervised devices.
Windows Agent	Enable this policy to run uploaded PowerShell scripts on Windows desktops and tablets.
Windows GPO configuration	Configure Group Policy Objects (GPOs) for any Windows device supported by Citrix Workspace Environment Management.
Windows Hello for Business	Enable the Windows feature so users can provision Windows Hello for Business on their device. The policy also lets you configure passcode limitations and other security features.

Windows Information Protection	Specifies the apps that require Windows Information Protection at the enforcement level you set for the policy. The policy is for Windows 10 and Windows 11 supervised devices.
--------------------------------	---

### Device policies by platform

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
AirPlay mirroring device policy	X	X						
AirPrint device policy	X							
APN device policy	X			X				
App access device policy	X			X				
App attributes device policy	X							
App configuration device policy	X					X	X	

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
App inventory device policy	X	X	X	X		X	X	
App lock device policy	X			X		X		
App permissions device policy			X					
App restrictions device policy					X			
App uninstall device policy	X	X	X	X			X	
App uninstall restrictions device policy								X
Application Guard device policy						X		

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
Apps notifications device policy	X							
Automated update managed apps			X					
BitLocker device policy						X	X	
Browser device policy								X
Calendar (Cal-Dav) device policy	X	X						
Cellular device policy	X							
Connection scheduling device policy			X	X	X			
Contacts (Card-DAV) device policy	X	X						

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
Content device policy					X			
Copy Apps to Samsung Container device policy								X
Credential device policy	X	X	X	X	X	X	X	
Custom XML device policy			X			X	X	
Defender device policy						X	X	
Device Guard device policy						X		
Device Health Attestation device policy						X		

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
Device name device policy	X	X						
Education Configuration device policy	X							
Endpoint Management options device policy			X	X				
Endpoint Management uninstall device policy				X				
Enterprise Hub device policy							X	
Exchange device policy	X	X	X	X		X	X	
Files device policy			X	X				



Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
FileVault device policy		X						
Firewall device policy		X				X		
Font device policy	X	X						
Home screen layout device policy	X							
Import Device Configuration device policy								X
Import iOS & macOS Profile device policy	X	X						
Keyguard Management device policy			X					

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
Kiosk device policy			X		X	X		
Knox Platform for Enterprise device policy			X					
Launcher configuration device policy			X	X				
LDAP device policy	X	X						
Location device policy	X		X	X				
Lock screen message device policy	X							
Mail device policy	X	X						

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
Managed bookmarks device policy					X			
Managed configurations device policy			X					
Managed domains device policy	X							
Maps device policy							X	
Maximum resident users device policy	X							
MDM options device policy	X							
Network device policy	X		X	X	X		X	

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
Network usage device policy	X							
Office device policy						X		
Organizational information device policy	X							
OS Update device policy	X	X	X		X	X		
Passcode device policy	X	X	X	X		X	X	
Passcode lock grace period device policy	X							
Personal hotspot device policy	X							

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
Power management device policy					X			
Profile Removal device policy	X	X						
Provisioning profile device policy								
Provisioning profile removal device policy	X							
Proxy device policy	X							
Public session device policy					X			
Restrictions device policy	X	X		X	X	X	X	
Roaming device policy	X							

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
Samsung MDM license key device policy			X					
SCEP device policy	X	X						
Siri and dictation policies	X							
SSO account device policy	X							
Storage encryption device policy							X	
Store device policy	X			X		X		
Subscribed calendars device policy								

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
Terms and conditions device policy	X			X		X	X	
Tunnel device policy				X				
VPN device policy	X	X		X	X	X	X	
Wallpaper device policy	X							
Web clip device policy	X	X		X		X		
Web content filter device policy	X							
Windows Agent device policy						X		
Windows GPO configuration device policy						X		

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Chrome OS	Windows Desktop/Tablet	Windows Phone	Other
Windows Hello for Business device policy						X	X	
Windows Information Protection device policy						X	X	

## AirPlay mirroring device policy

September 2, 2021

The Apple AirPlay feature allows users to wirelessly stream content from an iOS device to a TV screen through Apple TV, or to mirror exactly what’s on a device display to a TV screen or another Mac computer.

You can add a device policy in Endpoint Management to add specific AirPlay devices (such as Apple TV or another Mac computer) to iOS devices. You also have the option of adding devices to an allow list for supervised devices, which limits users to only those AirPlay devices. For information about placing a device into Supervised mode, see [Deploy devices using Apple Configurator 2](#).

**Note:**

Before proceeding, be sure to have the device IDs and any passwords for all the devices you want to add.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).



## iOS settings

AirPlay mirroring policy				
1 Policy Info	<b>AirPlay mirroring policy</b> <small>This policy lets you configure specific AirPlay devices to add to iOS and macOS devices. For supervised devices, you can also add a list of allowed AirPlay devices.</small>			
2 Platforms <span>Clear All</span>	<b>AirPlay password</b> <table border="1"> <tr> <td>Device name *</td> <td>Password *</td> <td>Add</td> </tr> </table>	Device name *	Password *	Add
Device name *	Password *	Add		
<input checked="" type="checkbox"/> iOS	<b>Allow list ID</b> <table border="1"> <tr> <td>Device ID *</td> <td>Add</td> </tr> </table>	Device ID *	Add	
Device ID *	Add			
<input checked="" type="checkbox"/> macOS	<b>Policy Settings</b> Remove policy <input checked="" type="radio"/> Select date <input type="radio"/> Duration until removal (in hours) <input type="text"/>			
3 Assignment				

- **AirPlay Password:** For each device you want to add, click **Add** and then do the following:
  - **Device name:** Enter the hardware address (Mac address) in xx:xx:xx:xx:xx:xx format. This field is not case-sensitive.
  - **Password:** Enter an optional password for the device.
  - Click **Add** to add the device or click **Cancel** to cancel adding the device.
- **Allow list ID:** This list is ignored for unsupervised devices. The device IDs in this list are the only AirPlay devices available to users devices. For each AirPlay device you want to add to the list, click **Add** and then do the following:
  - **Device ID:** Type the device ID in xx:xx:xx:xx:xx:xx format. This field is not case-sensitive.
  - Click **Add** to add the device or click **Cancel** to cancel adding the device.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

## macOS settings

- **AirPlay Password:** For each device you want to add, click **Add** and then do the following:
  - **Device name:** Enter the hardware address (Mac address) in xx:xx:xx:xx:xx:xx format. This field is not case-sensitive.
  - **Password:** Enter an optional password for the device.
  - Click **Add** to add the device or click **Cancel** to cancel adding the device.
- **Allow list ID:** This list is ignored for unsupervised devices. The device IDs in this list are the only AirPlay devices available to users devices. For each AirPlay device you want to add to the list, click **Add** and then do the following:
  - **Device ID:** Type the device ID in xx:xx:xx:xx:xx:xx format. This field is not case-sensitive.
  - Click **Add** to add the device or click **Cancel** to cancel adding the device.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

## AirPrint device policy

March 24, 2020

The AirPrint device policy adds AirPrint printers to the AirPrint printer list on iOS devices. This policy makes it easier to support environments where the printers and the devices are on different subnets.

### Note:

To configure the AirPrint device policy, you need the IP address and resource path for each printer.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### iOS settings

- **AirPrint Destination:** For each AirPrint destination you want to add, click **Add** and then do the following:
  - **IP Address:** Enter the AirPrint printer IP address.
  - **Resource Path:** Enter the Resource Path associated with the printer. This value corresponds to the parameter of the `_ipps.tcp` Bonjour record. For example, `printers/Canon_MG5300_series` or `printers/Xerox_Phaser_7600`.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 or later.

## App permissions device policy

June 23, 2021

For Android Enterprise apps that are within work profiles: You can configure how requests to those apps handle what Google calls “dangerous” permissions. You control whether the user is prompted to grant or deny the permission request from the app. This feature applies to devices running Android 7.0 and later.

This policy applies to Android for Workspace (Preview) devices as well.

Google defines dangerous permissions as permissions that:

- Give the app access to data or resources that involve the user's private information.
- Or, can potentially affect the user's stored data or the operation of other apps. For example, the ability to read user contacts is a dangerous permission.

You can configure a global status to control the behavior of all dangerous permission requests. The scope of this configuration is Android Enterprise apps that are within work profiles. You can also control the behavior of dangerous permission request for individual permission groups, as defined by Google, for each app. These individual settings override the global status.

For information on how Google defines permission groups, see the [Android developers guide](#).

By default, users are prompted to grant or deny dangerous permission requests.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Android Enterprise settings

**Android Enterprise App Permissions**

This policy lets you specify the behavior when Android Enterprise apps request dangerous permissions.

Global State \* Prompt

App *	Grant Status	⊞ Add
Gmail	Deny	

**Calendar**

App *	Grant Status	⊞ Add
com.sec.android.gallery3d	Deny	

**Camera**

App *	Grant Status	⊞ Add
com.sec.android.gallery3d	Deny	

**Contacts**

App *	Grant Status	⊞ Add
com.sec.android.gallery3d	Deny	

**Location**

App *	Grant Status	⊞ Add

**Microphone**

App *	Grant Status	⊞ Add

**Phone**

App *	Grant Status	⊞ Add

**Sensors**

App *	Grant Status	⊞ Add

Back Next >

- **Global State:** Controls the behavior of all dangerous permission requests. In the list, click **Prompt, Grant, or Deny**.
  - **Prompt:** Users are prompted to grant or deny dangerous permission requests.
  - **Grant:** All dangerous permission requests are granted. The user is not prompted.
  - **Deny:** All dangerous permission requests are denied. The user is not prompted.

Default is **Prompt**.

- Set an individual behavior for each permission group, for each app. To configure the behavior for a permission group: Click **Add** and then under **App**, choose an app from the list. If you con-

figure Android Enterprise system apps, click **Add new** and enter the application package name you enabled in the Restrictions device policy. Under Grant Status, choose **Prompt**, **Grant**, or **Deny**. This grant status overrides the global status.

- **Prompt:** Users are prompted to grant or deny dangerous permission requests from this permission group for this app.
- **Grant:** Dangerous permission requests from this permission group for this app are granted. The user is not prompted.
- **Deny:** Dangerous permission requests from this permission group for this app are denied. The user is not prompted.

Default is **Prompt**.

- Click **Save** next to the app and grant status.
- To add more apps for the permission group, click **Add** again and repeat these steps.
- When you have finished setting the **Grant Status** for permission groups, click **Next**.

## APN device policy

April 7, 2020

You can add a custom Access Point Name (APN) device policy for iOS and Android devices. You use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device. An APN policy determines the settings used to connect your devices to a specific phone carrier's General Packet Radio Service (GPRS). This setting is already defined in most newer phones.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

**APN Policy** ✕

This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

APN \*

User name

Password

Server proxy address

Server proxy port

Policy Settings

Remove policy  Select date  
 Duration until removal (in hours)

- **APN:** Type the name of the access point. The name must match an accepted iOS APN or the policy doesn't work.
- **User name:** This string specifies the user name for this APN. If the user name is missing, the device prompts for the string during profile installation.
- **Password:** The password for the user for this APN. For obfuscation purposes, the password is encoded. If it is missing from the payload, the device prompts for the password during profile installation.
- **Server proxy address:** The IP address or URL of the APN proxy.
- **Server proxy port:** The port number for the APN proxy. The port number is required if you entered a server proxy address.
- Under **Policy Settings**, next to **Remove policy**, click either **Select date** or **Duration until removal (in hours)**.
  - For the option **Select date**, click the calendar to select the specific date for removal.
  - For the option **Password required**, type the password.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 or later.

## Android settings

**APN Policy** ✕

This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

APN *	<input type="text"/>
User name	<input type="text" value="administrator"/>
Password	<input type="password" value="*****"/>
Server	<input type="text"/>
APN type	<input type="text"/>
Authentication type	<input type="text" value="None"/>
Server proxy address	<input type="text"/>
Server proxy port	<input type="text"/>
MMSC	<input type="text"/>

- **APN:** Type the name of the access point. The name must match an accepted Android APN or the policy doesn't work.
- **User name:** This string specifies the user name for this APN. If the user name is missing, the device prompts for the string during profile installation.
- **Password:** The password for the user for this APN. For obfuscation purposes, the password is encoded. If it is missing from the payload, the device prompts for the password during profile installation.
- **Server:** This setting, which predates smart phones, is usually empty. It references a Wireless Application Protocol (WAP) gateway server for phones that can't access or render standard web sites.
- **APN type:** This setting must match the carrier's intended use for the access point. It is a comma separated string of APN service specifiers and must match the wireless carrier's published definitions. Examples include:
  - \\*: All traffic goes through this access point.
  - mms: Multimedia traffic goes through this access point.
  - default: All traffic, including multimedia, goes through this access point.
  - supl: Secure User Plane Location is associated with assisted GPS.
  - dun: Dial Up Networking is outdated and rarely used.
  - hipri.: High priority networking.
  - fota: Firmware over the air is used for receiving firmware updates.
- **Authentication type:** In the list, click the type of authentication to be used. Defaults to None.
- **Server proxy address:** The IP address or URL of the carrier's APN HTTP proxy.
- **Server proxy port:** The port number for the APN proxy. The port is required if you entered a server proxy address.

- **MMSC:** The MMS Gateway Server address provided by the carrier.
- **Multimedia Messaging Server (MMS) proxy address:** The address for the multimedia messaging service server for MMS traffic. MMS succeeded SMS for sending larger messages with multimedia content, such as pictures or videos. These servers require specific protocols (such as MM1, ... MM11).
- **MMS port:** The port used for the MMS proxy.

## App access device policy

March 3, 2021

The app access device policy allows you to define a list of apps that must be installed, can be installed, or must not be installed. If the apps on a device contradict this policy, Endpoint Management marks the device as out of compliance. You can then create an automated action to react to that device compliance.

### Important:

The app access device policy does not prevent a user from installing a forbidden app or uninstalling a required app.

You can only configure one type of access policy at a time. Each policy contains a list of required apps, suggested apps, or forbidden apps, but not a mix within the same app access policy. If you create a policy for each type of list, name each policy carefully, so you know which policy applies to which list of apps.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS and Android (legacy DA) settings

- **Access policy:** Select the type of list to configure for this policy.
  - **Required:** The app must exist on the device. If the app doesn't exist, the device is marked as out of compliance. **Required** is the default option.
  - **Forbidden:** The app must not exist on the device. If the app does exist, the device is marked as out of compliance.
- To add one or more apps to the list:
  1. Click **Add** and then configure the following:
    - **App name:** Enter an app name.
    - **App Identifier:** Enter an optional app identifier.
  2. Click **Save**.

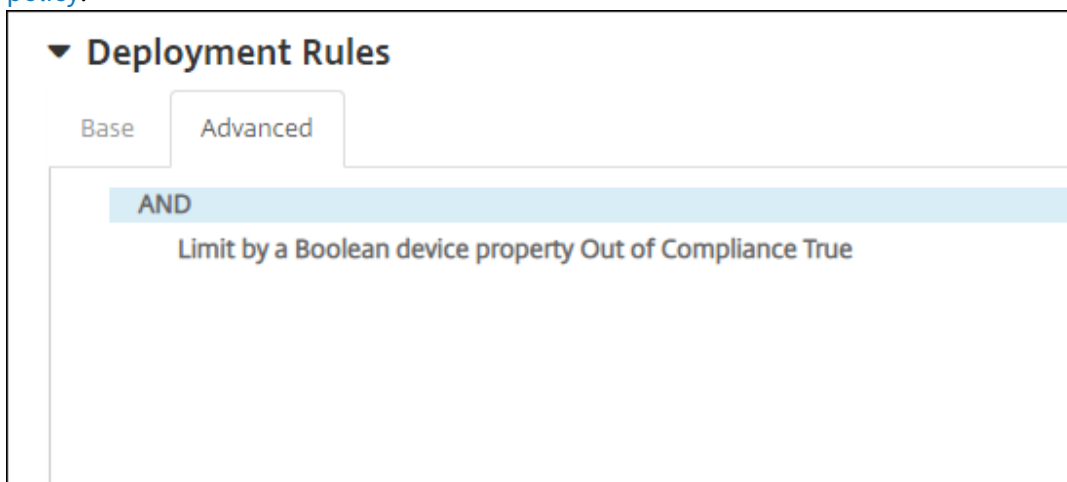


3. Repeat these steps for each app you want to add.

### Configure automated actions based on app access compliance

1. Add an app access policy to require or forbid apps.
2. Configure two automated actions based on whether the apps in question are required or forbidden:
  - Required
    - Mark a device as out of compliance if a required app doesn't exist on the device.
    - Mark a device as compliant once that required app is installed.
  - Forbidden
    - Mark a device as out of compliance if a forbidden app exists on the device.
    - Mark a device as compliant once that forbidden app is no longer installed.

For information on setting up automated actions, see [Automated actions](#).
3. Create a restriction policy with the settings you want to implement on out of compliance devices.
  - a) As part of the restriction policy, add an advanced deployment rule with the options **Limit by a Boolean device property**, **Out of Compliance**, and **True**. See [Restrictions device policy](#).



4. Create a profile removal policy to remove the restriction policy once the device is back in compliance.
5. Add an advanced deployment rule with the options **Limit by a Boolean device property**, **Out of Compliance**, and **False**. See [Profile removal device policy](#).

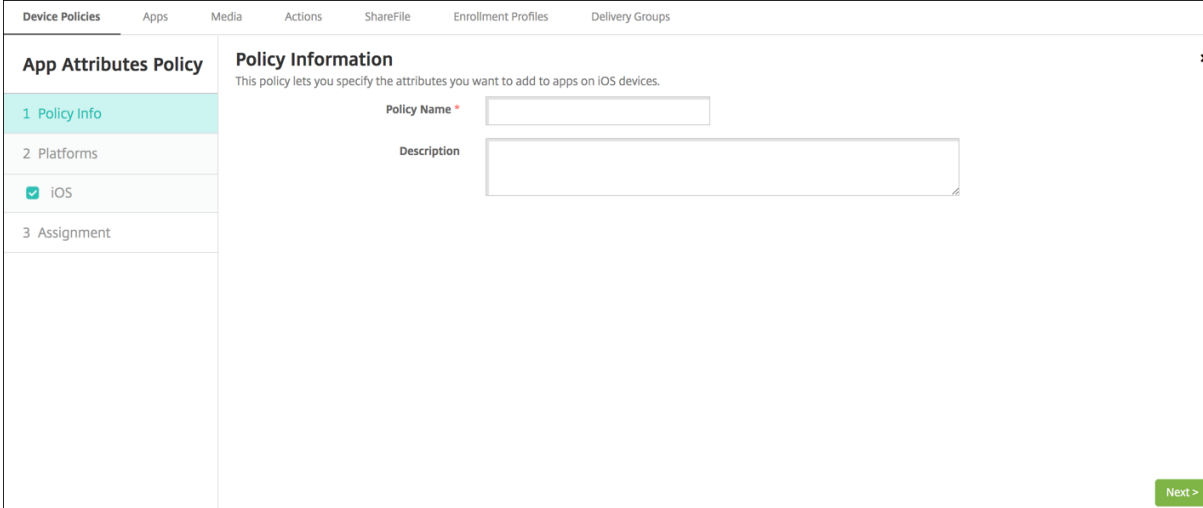
### App attributes device policy

August 26, 2019

The App attributes device policy lets you specify attributes, such as a managed app bundle ID or per-app VPN identifier, for iOS devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings



- **Managed app bundle ID:** In the list, click an app bundle ID or click **Add new**.
  - If you click **Add new**, type the app bundle ID in the field that appears.
- **Per-app VPN identifier:** In the list, click per-app VPN identifier.

## App configuration device policy

September 9, 2021

You can remotely configure apps that support managed configuration by deploying:

- An XML configuration file (.plist, also called a property list) to iOS devices
- Key/value pairs for Phone, Desktop, or Tablet devices running Windows 10 or Windows 11
- Citrix Workspace connection information to Workspace hub devices

The configuration specifies various settings and behaviors in the app. Endpoint Management pushes the configuration to devices when the user installs the app. The actual settings and behaviors that you can configure depend on the app and are beyond the scope of this article.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

- **Identifier:** In the list, click the app you want to configure or click **Add new** to add an app to the list.
  - If you click **Add new**, type the app identifier in the field that appears.
- **Dictionary content:** Type, or copy and paste, the XML property list (.plist) configuration information.
- Click **Check dictionary**. Endpoint Management verifies the XML. If there are no errors, you see **Valid XML** below the content box. If any syntax errors appear below the content box, you must correct them before you can continue.

## Windows Phone settings

- In the **Make a selection** list, click the app you want to configure or click **Add new** to add an app to the list.
  - If you click **Add new**, type the package family name in the field that appears.
- For each configuration parameter you want to add, click **Add** and then do the following:
  - **Parameter name:** Enter the key name of an application setting for the Windows device. For information about Windows app settings, refer to the Microsoft documentation.
  - **Value:** Enter the value for the specified parameter.
  - Click **Add** to add the parameter or click **Cancel** to cancel adding the parameter.

## Windows Desktop/Tablet settings

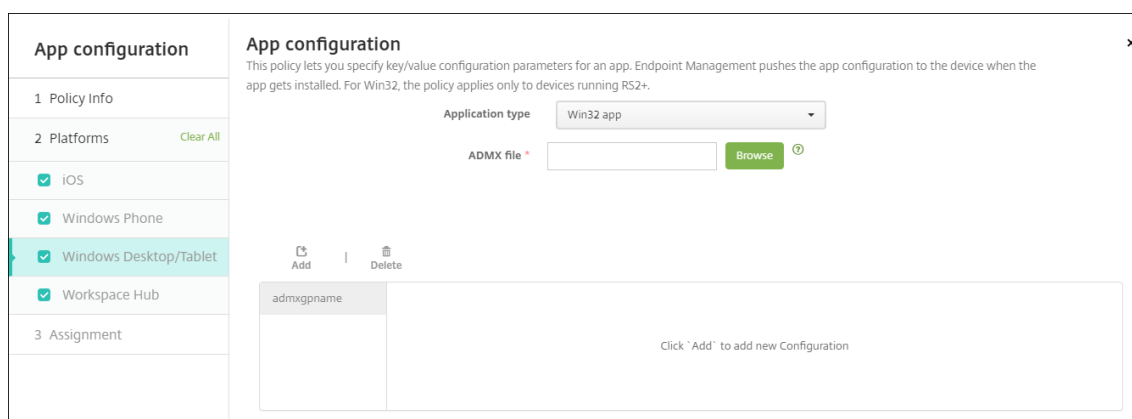
You can configure either Universal Windows Platform (UWP) apps or Win32 apps. To import Microsoft Administrative Template (ADMX) policy settings, configure Win32 apps.

### Note:

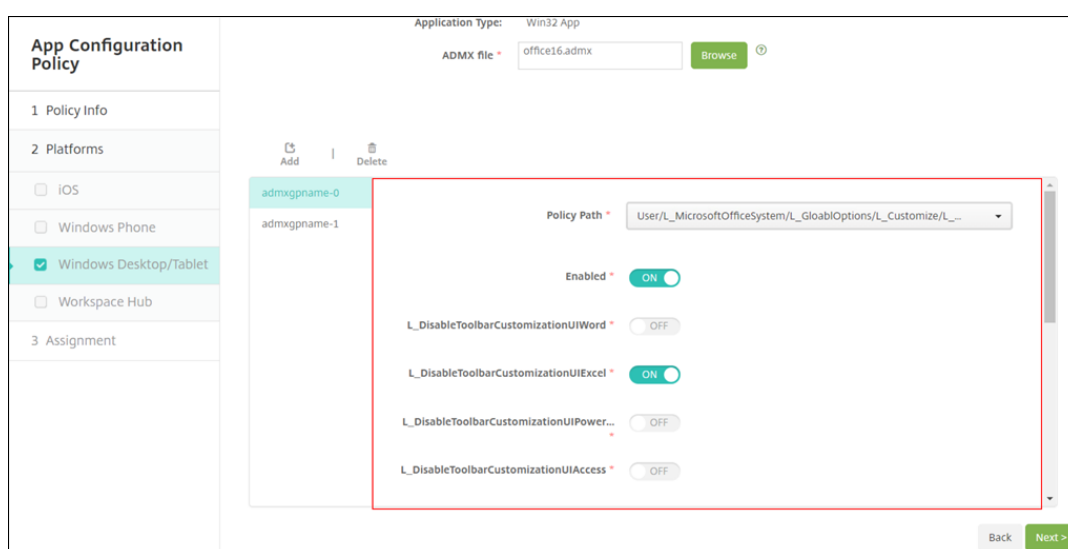
The App Configuration device policy supports third-party ADMX files for third-party applications such as Office. Not supported are Microsoft ADMX templates for Windows that are provided as operating system Group Policies available under `%SystemRoot%\PolicyDefinitions\NeedCopy`.

- If you choose **UWP App**: In the **Make a selection** list, click the app you want to configure or click **Add new** to add an app to the list.

- If you click **Add new**, type the package family name in the field that appears.
- For each configuration parameter you want to add, click **Add** and then do the following:
  - \* **Parameter name**: Enter the key name of an application setting for the Windows device. For information about Windows app settings, refer to the Microsoft documentation.
  - \* **Value**: Enter the value for the specified parameter.
  - \* Click **Add** to add the parameter or click **Cancel** to cancel adding the parameter.
- If you choose **Win32 App**: Click **Browse** and navigate to the ADMX file you want to use to configure the policy.



- Click **Add**. Configuration options from the ADMX file appear on the right side of the page.



- Choose a policy path. If you choose the same path more than once, the configuration associated with the most recently version is enforced.
- Set **Enable** to **On**.
- Input any required list element values as key-value pairs. Use the text string **&#xFO00** to separate each key-value pair and the value and key within the pair.
- Element values that include a decimal might require values within a specific range.

### Workspace Hub settings

Use the App Configuration device policy to deploy the Citrix Workspace configuration to Citrix Ready workspace hub devices. Configure the following settings:

**App configuration**

1 Policy Info

2 Platforms [Clear All](#)

- iOS
- Windows Phone
- Windows Desktop/Tablet
- Workspace Hub**

3 Assignment

**App configuration**

This policy lets you specify key/value configuration parameters for an app. Endpoint Management pushes the app configuration to the device when the app gets installed. For iOS devices, after you enter the dictionary content, you can check the syntax.

Connection mode: Citrix Receiver

Connection name:

Connection target:

Parameter name	Value	<a href="#">Add</a>
----------------	-------	---------------------

- **Connection mode:** Select **Citrix Receiver**.
- **Connection name:** Type a descriptive name for your connection.
- **Connection target:** Type a URL to load upon connection.

Some apps might require extra parameters to function. For each configuration parameter you want to add, click **Add** and then configure the following:

- **Parameter name:** Type the key name of an application setting for the Citrix Ready workspace hub device.
- **Value:** Type the value for the specified parameter.

For more information about configuring Citrix Ready workspace hub devices, see [Workspace hub device management](#).

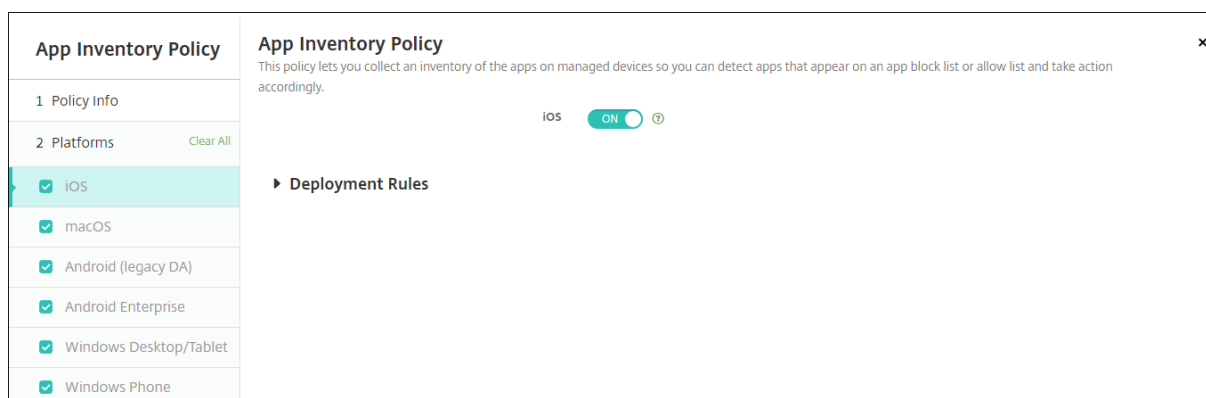
## App inventory device policy

September 8, 2021

The App inventory policy lets you collect an inventory of the apps on managed devices. Endpoint Management can then compare the inventory to any app access policies deployed to those devices. In this way, you can detect apps that appear on an app allow or block list and act accordingly. Use an App access policy to define allow or block lists.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS, macOS, Android (legacy DA), Android Enterprise, Windows Desktop/Tablet, and Windows Phone



- For each platform you select, leave the default setting or change the setting to **Off**. The default is **On**.

### Inventory and delete Win32 apps

You can determine whether the Win32 apps on user devices comply with your App access device policy. To view an inventory of Win32 apps on managed Windows 10 and Windows 11 Desktop and Tablet devices:

1. Go to **Configure > Device Policies** and add an App Inventory policy for the **Windows Desktop/Tablet** platform. Deploy the policy.
2. Go to **Manage > Devices**, select the Windows 10 and Windows 11 device that you want to view, click **Edit**, and then click the **Apps** tab.

The results of the inventory appear.

Device details		Apps							
1 General		Last inventory: 11/13/17 4:26:56 am							
2 Properties		Installed (55)   Pending (0)   Failed (0)							
3 User Properties		Name	Ownership	Version	Author	Size	Installed	Identifier	Type
4 Assigned Policies		Microsoft.BingNews	Personal	4.21.2212.0			11/13/17 4:21:50 am	Microsoft.BingNews_8wekyb3d8bbwe	
5 Apps		Microsoft.BingWeather	Personal	4.21.2212.0			11/13/17 4:21:50 am	Microsoft.BingWeather_8wekyb3d8bbwe	
6 Media		Microsoft.DesktopAppInstaller	Personal	1.0.10332.0			11/13/17 4:21:50 am	Microsoft.DesktopAppInstaller_8wekyb3d8bbwe	
7 Actions		Microsoft.Getstarted	Personal	5.12.2691.0			11/13/17 4:21:50 am	Microsoft.Getstarted_8wekyb3d8bbwe	
8 Delivery Groups		Microsoft.MSPaint	Personal	3.1710.30027.0			11/13/17 4:21:50 am	Microsoft.MSPaint_8wekyb3d8bbwe	
9 Certificates		Microsoft.Messaging	Personal	3.34.25004.0			11/13/17 4:21:50 am	Microsoft.Messaging_8wekyb3d8bbwe	
10 Connections		Microsoft.Microsoft3DViewer	Personal	2.1710.12012.0			11/13/17 4:21:50 am	Microsoft.Microsoft3DViewer_8wekyb3d8bbwe	
		Microsoft.MicrosoftOfficeHub	Personal	17.8809.7600.0			11/13/17 4:21:50 am	Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe	

3. Compare the app inventory to your App access device policy. If the device has apps installed that are on the block list, you can delete them from devices.

### **App install and uninstall issues caused by an incorrect Product Code**

If a Win32 app is configured with the incorrect Product Code, the app initially installs, however Microsoft doesn't return the app status to Endpoint Management. As a result:

- The App Uninstall device policy doesn't uninstall the app.
- Endpoint Management continues to deploy the app because it doesn't have confirmation that the app installed. With each deployment, the device generates an error code because the app is already installed. The error shown in **Manage > Device > Delivery Group Details** is:  
`Msi Application received: Reporting:AppPush id:7z1701-x64.msi: Command execution failed -2147023293`

To correct the Product Code:

1. Manually remove the app from the device.
2. In the Endpoint Management console, go to **Configure > Apps** and correct the Product Code for the Win32 app.
3. Deploy the Win32 app.

## **Application Guard device policy**

September 9, 2021

The Application Guard policy specifies Windows Defender Application Guard settings. The settings include whether to enable Application Guard and controls for clipboard behavior.

Windows Defender Application Guard protects your environment from sites that haven't been defined as trusted by your organization. When users visit sites that aren't listed in your isolated network boundary: The sites open in a virtual browsing session in Hyper-V. Enterprise cloud resources define trusted sites.

### **Requirements**

- Devices running Windows 10 Enterprise (64-bit) or Windows 11 Enterprise (64-bit). A device restart is required to install the Windows Defender Application Guard.
- Microsoft Edge browser



## Windows Desktop and Tablet settings

The screenshot shows the 'Application Guard policy' configuration page. The left sidebar has a navigation menu with the following items: 'Application Guard policy', '1 Policy Info', '2 Platforms' (with a 'Clear All' link), '3 Assignment', and '4 Deployment Rules'. The '2 Platforms' section is expanded to show 'Windows Desktop/Tablet' selected. The main content area is titled 'Application Guard policy' and includes a descriptive paragraph: 'This policy lets you enable Windows Defender Application Guard and configure clipboard controls. Use this policy to protect your environment from sites not trusted by Microsoft Edge. When users visit untrusted sites, the sites open in a Hyper-V virtual browsing session. Enterprise cloud resources define trusted sites. This policy is available to devices running Windows 10 Enterprise (64-bit) version 1709 or later. To install Windows Defender Application Guard, the device must restart.' Below this are four configuration options, each with a toggle switch and an information icon: 'Application guard' (set to Off), 'Clipboard behavior' (set to 'No restriction'), 'Block external content on enterprise sites' (set to Off), and 'Retain user-generated browser data' (set to Off). At the bottom right, there are 'Back' and 'Next >' buttons.

- **Application guard:** Enables Application Guard. Default is **Off**.
  - **Enterprise cloud resources:** A comma-separated list of enterprise cloud domains.
- **Clipboard behavior:** Controls which directions content can be copied and pasted. The options are as follows:
  - **Not configured**
  - **Allow copy and paste only from browser to PC:** Allows users to copy and paste content only from their browser to their PC.
  - **Allow copy and paste only from PC to browser:** Allows users to copy and paste content only from their PC to their browser.
  - **Allow copy and paste between PC and browser:** Allows users to copy and paste content freely between their PC and browser.
  - **Block copy and paste between PC and browser:** Does not allow users to copy and paste content between their PC and browser.
- **Clipboard content:** Controls which content users can copy and paste. The options are as follows:
  - **No restriction**
  - **Allow text copying:** Allows users to copy text only.
  - **Allow image copying:** Allows users to copy images only.
  - **Allow both text and image copying:** Allows users to copy both text and images.

- **Block external content on enterprise sites:** If **On**, Windows Defender Application Guard prevents content from unapproved sites from loading on enterprise sites. Default is **Off**.
- **Retain user-generated browser data:** If **On**, allows saving user data created during an Application Guard virtual browsing session. This data includes things like passwords, favorites, and cookies. Default is **Off**.

## App lock device policy

September 8, 2021

The App lock device policy defines a list of apps that are either:

- Allowed to run on a device.
- Blocked from running on a device.

The exact way the policy works differs for each supported platform. For example, you cannot block multiple apps on an iOS device.

Likewise, for iOS devices, you can select only one iOS app per policy. Users are only able to use their device to run a single app. They cannot do any other activities on the device except for the options you specifically allow when the App lock device policy is enforced.

In addition, iOS devices must be supervised to push app lock policies.

Although the device policy works on most Android L and M devices, app lock doesn't function on Android N or later devices. It doesn't work because Google deprecated the required API.

For managed Windows Desktops and Tablets, you can create an App lock device policy that defines the list of apps on the allow and block lists. You can allow or block executables, MSI installers, store apps, DLLs, and scripts.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

<p><b>App lock</b></p> <p>1 Policy Info</p> <p>2 Platforms <span style="color: green;">Clear All</span></p> <p><input checked="" type="checkbox"/> iOS</p> <p><input checked="" type="checkbox"/> Android (legacy DA)</p> <p><input checked="" type="checkbox"/> Windows Desktop/Tablet</p> <p>3 Assignment</p>	<p><b>App lock</b></p> <p>This policy lets you define allowed or blocked apps on a managed device. For Windows Desktop and Tablets: You can allow or block executables, MSI installers, store apps, DLLs, and scripts. First, you configure rules in the Local Security Policy App on the Windows Desktop and export the XML configuration file. Then, use this policy to upload the XML file to Endpoint Management.</p> <p>App bundle ID * <input type="text" value="Make a selection"/></p> <p><b>Options</b></p> <p>Disable touch screen <input checked="" type="checkbox"/> ON iOS 6.0+</p> <p>Disable device rotation sensing <input type="checkbox"/> OFF iOS 6.0+</p> <p>Disable volume buttons <input type="checkbox"/> OFF iOS 6.0+</p> <p>Disable ringer switch <input type="checkbox"/> OFF iOS 6.0+</p> <p>Disable sleep/wake button <input type="checkbox"/> OFF iOS 6.0+</p> <p>Disable auto-lock <input type="checkbox"/> OFF iOS 6.0+</p> <p>Enable VoiceOver <input type="checkbox"/> OFF iOS 6.0+</p> <p>Enable zoom <input type="checkbox"/> OFF iOS 6.0+</p>
---	---

- **App bundle ID:** In the list, click the app to which this policy applies or click **Add new** to add an app to the list. If you select **Add new**, type the app name in the field that appears.
- **Options:** For each option, the default is **Off** except for **Disable touch screen**, which defaults to **On**.
  - Disable touch screen
  - Disable device rotation sensing
  - Disable volume buttons
  - Disable ringer switch
    - When **Disable ringer switch** is **On**, the ringer behavior depends on what position the switch was in when it was first disabled.
  - Disable sleep/wake button
  - Disable auto lock
  - Disable VoiceOver
  - Enable zoom
  - Enable invert colors
  - Enable AssistiveTouch
  - Enable speak selection
  - Enable mono audio
  - Enable voice control
- **User Enabled Options:** For each option, the default is **Off**.
  - Allow VoiceOver adjustment
  - Allow zoom adjustment
  - Allow invert colors adjustment

- Allow AssitiveTouch adjustment
- Allow voice control adjustment
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 or later.

### Configure an iPad as a kiosk

You can use the App lock device policy to run a supervised iPad as a kiosk. Apple refers to this feature as Single App Mode. For more information about this feature, see [Apple documentation](#). Ensure that you deploy the app you want to run before deploying this policy.

1. Navigate to **Configure > Device policies** and click **Add**.
2. Select the **App Lock** policy.
3. Type a **Policy Name** and optional **Description**.
4. Select only the **iOS** platform.
5. For **App bundle ID**, select the app you want to run on the iPad.
6. Configure any options you want, as described previously, and save the policy.
7. Add the policy to the same delivery group as your iPad and deploy the policy.

### Android (legacy DA) settings

**Note:**

You can't block the Android Settings app by using the App Lock device policy.

The screenshot shows the 'App lock' configuration page. On the left, a sidebar lists '1 Policy Info', '2 Platforms' (with 'Clear All' and checkboxes for 'iOS', 'Android (legacy DA)', and 'Windows Desktop/Tablet'), and '3 Assignment'. The main panel is titled 'App lock' and contains a description: 'This policy lets you define allowed or blocked apps on a managed device. For Windows Desktop and Tablets: You can allow or block executables, MSI installers, store apps, DLLs, and scripts. First, you configure rules in the Local Security Policy App on the Windows Desktop and export the XML configuration file. Then, use this policy to upload the XML file to Endpoint Management.' Below this is the 'App lock parameters' section with fields for 'Lock message', 'Unlock password', 'Prevent uninstall' (set to OFF), and 'Lock screen' (with a 'Browse' button). The 'Enforce' section has radio buttons for 'Block list' (selected) and 'Allow list'. At the bottom, there is an 'Apps' section with a table header 'App name' and an 'Add' button.

- **App Lock parameters**
  - **Lock message:** Type a message that users see when they attempt to open a locked app.
  - **Unlock password:** Type the password to unlock the app.
  - **Prevent uninstall:** Select whether users are allowed to uninstall apps. The default is **Off**.
  - **Lock screen:** Select the image that appears on the device’s lock screen by clicking **Browse** and navigating to the file’s location.
  - **Enforce:** Click **Block list** to create a list of apps that are not allowed to run on devices. Click **Allow list** to create a list of apps that are allowed to run on devices.
- **Apps:** Click **Add** and then do the following:
  - **App name:** In the list, click the name of the app to add to the allow or block list. Alternatively, click **Add new** to add an app to the list of available apps.
  - If you select **Add new**, type the app name in the field that appears.
  - Click **Save** or **Cancel**.
  - Repeat these steps each app you want to add to the allow or block list.

## Windows Desktop and Tablet settings

<b>App lock</b>	<p><b>App lock</b> This policy lets you define allowed or blocked apps on a managed device. For Windows Desktop and Tablets: You can allow or block executables, MSI installers, store apps, DLLs, and scripts. First, you configure rules in the Local Security Policy App on the Windows Desktop and export the XML configuration file. Then, use this policy to upload the XML file to Endpoint Management.</p> <p>AppLocker policy file <input type="text"/> <span style="background-color: #4CAF50; color: white; padding: 2px 5px;">Browse</span> <span style="font-size: 1em;">?</span></p> <p>► <b>Deployment Rules</b></p>
1 Policy Info	
2 Platforms <span style="float: right; color: #4CAF50;">Clear All</span>	
<input checked="" type="checkbox"/> iOS	
<input checked="" type="checkbox"/> Android (legacy DA)	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	

### Prerequisites for App lock

- In Windows, configure rules in the Local Security Policy editor on a Windows 10 or Windows 11 desktop.
- Export the policy XML file. Citrix recommends that you create default rules in Windows to avoid locking the default configuration or causing issues on devices.
- Then, upload the XML file to Endpoint Management by using the App Lock device policy. For more information about creating rules, see this Microsoft article: <https://docs.microsoft.com/en-us/windows/security/threat-protection/applocker/applocker-overview>

### To configure and export the policy XML file from Windows

**Important:**

When configuring the policy XML file through the Windows policy editor, use Audit Only mode.

1. On the Windows computer, start the **Local Security Policy** editor. Click **Start**, type **local security policy** and then click **Local Security Policy**.
2. In the console tree, expand **Application Control Policies**.
3. Click **AppLocker** and then in the center pane, click **Configure rule enforcement**.
4. Select **Configured** and then **Enforce rules**. When you enable a rule, **Enforce rules** is the default.
5. Right-click **AppLocker**, click **Export Policy**, and then save the XML file.

**Note:**

You can create **Executable Rules**, **Windows Installer Rules**, **Script Rules**, and **Packaged App Rules**. To do so, right-click the folder and then click **Create New Rule**.

### **To import the policy XML file into Endpoint Management**

Create an App Lock policy. Across from the **App Lock policy file** setting, click **Browse** and navigate to the XML file.

### **To stop applying an App Lock policy**

After you deploy an App Lock policy in Endpoint Management: To stop applying that App Lock policy, create an empty XML file. Then, create another App Lock policy, upload the file, and deploy the policy. Devices that have an App Lock enabled are not affected. Devices receiving the policy for the first time do not have the App Lock policy in place.

## **Apps notifications device policy**

April 20, 2020

The Apps notifications policy lets you control how iOS users receive notifications from specified apps. The policy is supported only on supervised iOS devices running iOS 9.3 and later.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

The screenshot displays the 'Apps Notifications Policy' configuration interface. It features a top navigation bar with tabs for 'Device Policies', 'Apps', 'Media', 'Actions', 'Sharefile', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar contains a tree view with 'Apps Notifications Policy' selected, and sub-items for '1 Policy Info', '2 Platforms', '3 Assignment', and 'Policy Settings'. The main content area is titled 'Apps Notifications Policy' and includes a sub-header 'Notifications Settings'. Below this is a table of settings with columns: 'App Bundle Identifier' (set to 'App Store'), 'Allow Notifications' (ON), 'Show in Notification Center' (ON), 'Badge App Icon' (ON), 'Sounds' (ON), 'Show on Lock Screen' (ON), 'Show in Car Play' (ON), 'Enable Critical Alert' (OFF), and 'Unlocked Alert Style' (Alerts). Below the table is the 'Policy Settings' section, which includes a 'Remove policy' section with radio buttons for 'Select date' and 'Duration until removal (in hours)', a text input field, an 'Allow user to remove policy' dropdown set to 'Always', and a 'Profile scope' dropdown set to 'System'.

- **App bundle identifier:** Specify the apps you want to add. If you click **Add new**, type the app bundle ID in the field that appears. To find a bundle ID: Locate the app in the App Store and copy the number at the end of the URL. For example, 363501921 is the app ID for Citrix Workspace app. Then go to <https://itunes.apple.com/lookup?id=> and paste the number at the end. After a .txt file downloads, search for bundleid. For example, the bundle ID for Citrix Workspace app is `com.citrix.ReceiveriPad`.
- **Allow notifications:** Select **On** to allow notifications.
- **Show in notification center:** Select **On** to show notifications in the notification center of the user devices.
- **Badge app icon:** Select **On** to show a badge app icon with notifications.
- **Sounds:** Select **On** to include sounds with notifications.
- **Show on lock screen:** Select **On** to show notifications on the lock screen of the user devices.
- **Show in CarPlay:** If **On**, notifications display in Apple CarPlay. Available in iOS 12 and later. Default is **On**.
- **Enable Critical Alert:** If **On**, an app can mark a notification as a critical notification that ignores Do Not Disturb and ringer settings. Available in iOS 12 and later. Default is **Off**.
- **Unlocked Alert Style:** In the list, select **None**, **Banner**, or **Alerts** to configure the appearance of unlocked alerts.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 or later.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on iOS 9.3 and later.

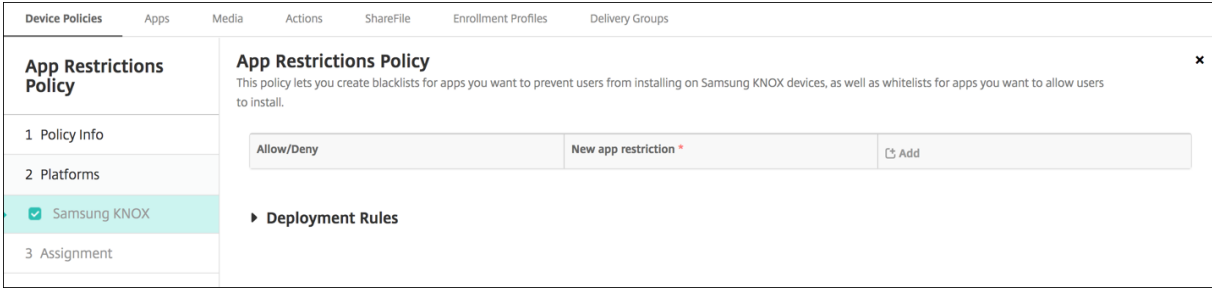
## App restrictions device policy

June 23, 2021

You use the App Restrictions device policy to specify allowed or blocked Chrome apps, Android apps running on Chrome OS, and Samsung Knox apps. If you enable App Runtime for Chrome (ARC) in the Restrictions device policy, you configure Android app restrictions under **Android apps** in the App Restrictions device policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Samsung Knox settings



The screenshot shows the configuration page for the 'App Restrictions Policy'. The top navigation bar includes 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar lists 'App Restrictions Policy', '1 Policy Info', '2 Platforms', '3 Assignment', and 'Samsung KNOX' (which is selected). The main content area is titled 'App Restrictions Policy' and includes a description: 'This policy lets you create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.' Below this is an 'Allow/Deny' section with a 'New app restriction' button and an 'Add' button. A 'Deployment Rules' section is also visible.

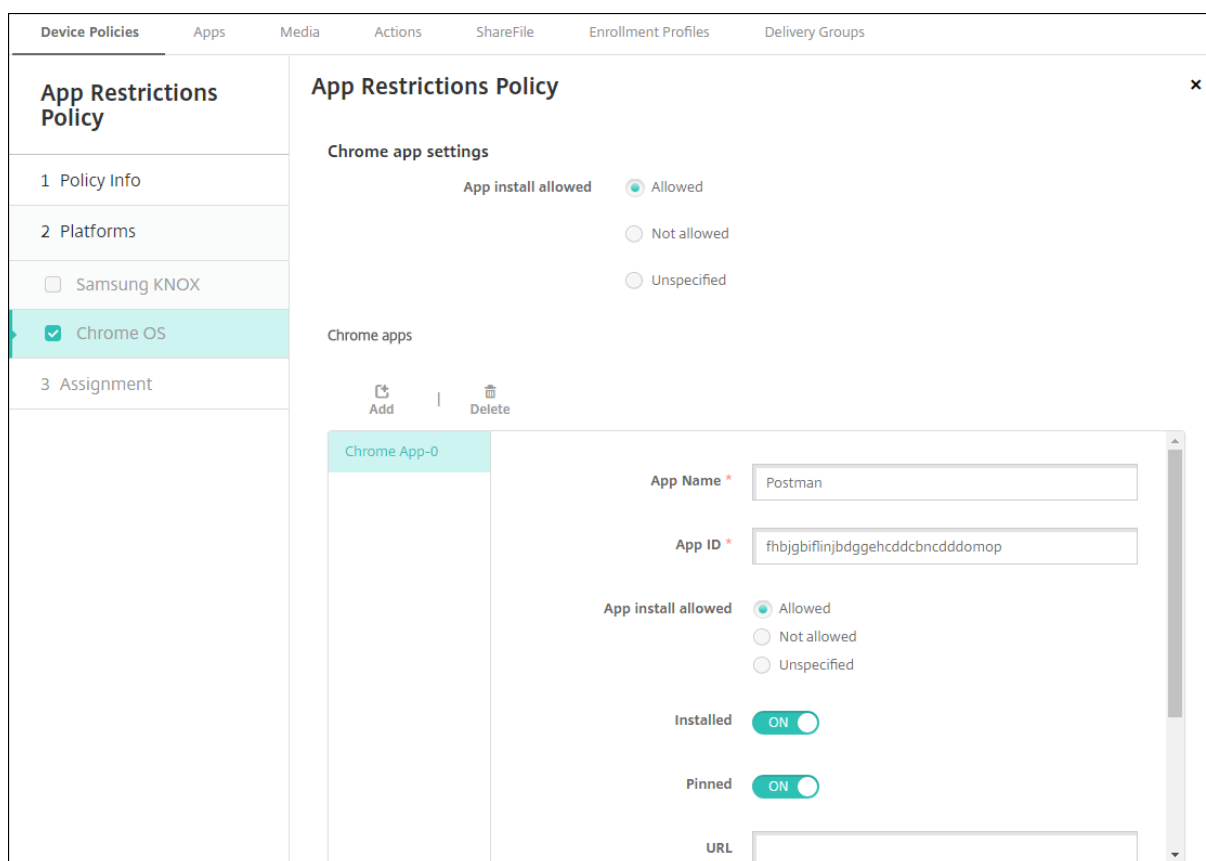
For each app you want to add to the Allow/Deny list, click **Add** and then do the following:

- **Allow/deny:** Select whether users are allowed to install the app.
- **App package ID:** Type the app package ID; for example, com.kmdm.af.crackle.
- Click **Save** to save the app to the Allow/Deny list or click **Cancel** to not save the app to the Allow/Deny list.

### Chrome app settings

Chrome apps are both apps and extensions.





- **App install allowed:** A global setting to allow or block the installation of all Chrome apps on Chrome OS devices. If you choose **Allowed**, you can create a list of specific blocked apps. If you choose **Not allowed**, you can create a list of specific allowed apps. To do that, click **Add** under **Chrome apps**. To use the settings specified in your Chrome account, select **Unspecified**. Default is **Allowed**.
- **Chrome apps:** To add Chrome apps that are exceptions to your selection for the **App install allowed** setting, click **Add** and then specify these settings:

- **App name:** A name used to identify an app in the Endpoint Management console.
- **App ID:** The unique identifier for a Chrome app. Don't include the prefix "app:".

To look up a Chrome app ID: Go to the Chrome web store. Then, search for the app. Click the app to view the URL and app ID in the address bar. The last portion of the address is the app ID. For example, if the URL is <https://chrome.google.com/webstore/detail/example/abcdefghijkl>, the app id is `abcdefghijkl`.

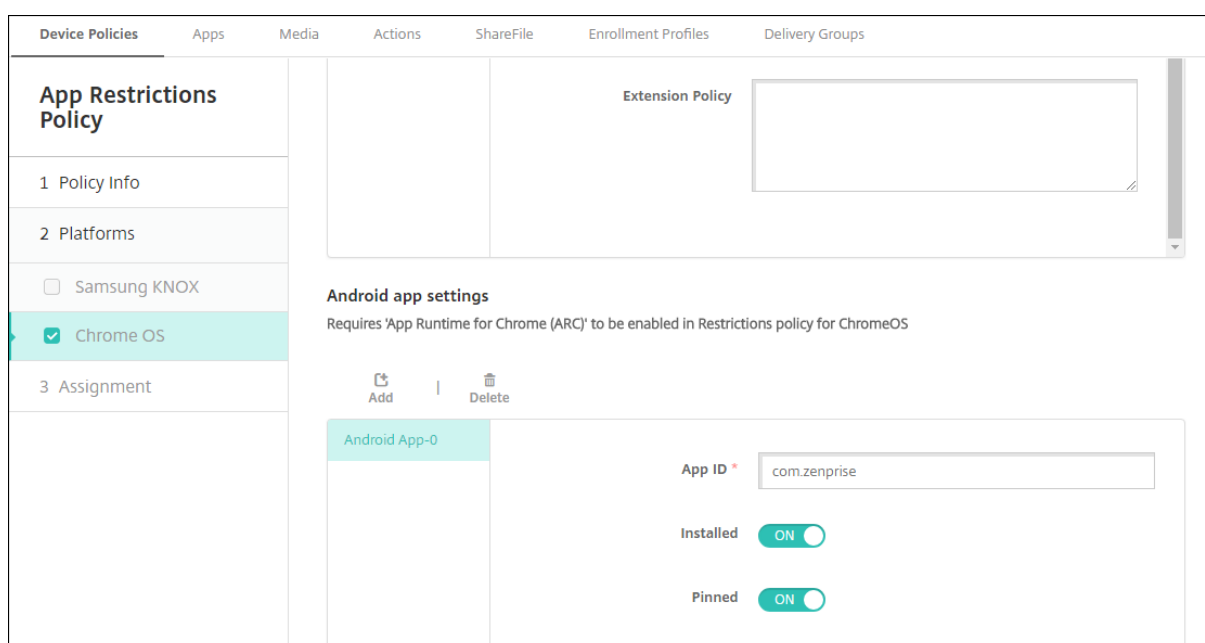
You can look up Chrome apps only from Chromebook. You can look up Chrome extensions from any platform.

- **App install allowed:** Creates an exception to the global setting above. This setting allows or blocks the specified Chrome app.

- **Installed:** If **On**, forces the Chrome app to install for enrolled Chrome OS device users. If **Off** and an app is installed, the app is uninstalled. If **Off** and the app is no longer configured by the policy, the app remains installed. Default is **Off**.
- **Pinned:** If **On**, pins the app to the Chromebook task bar. Default is **Off**.
- **URL:** Specifies the URL from which users can download an app that isn't hosted in the Chrome Web Store.
- **Extension policy:** Defines, in JSON format, the app-specific policy defined by this app. For information, see [Manifest for storage areas](#).

### Android app settings

To enable enrolled Chrome OS device users to run Android apps, configure the Restrictions device policy as noted in the next section “Enable enrolled Chrome OS device users to run Android apps.” To configure ARC app restrictions, click **Add** under Android apps and then specify these settings.



- **App ID:** A unique app identifier for an Android app running on Chrome OS. For example: com.android.camera. Don't include the prefix “app:”.

To look up an Android app ID: Go to the Google Play store. Then, search for the app. Click the app to view the app ID in the address bar. The portion after **id=** is the app ID. For example, if the URL is <https://play.google.com/store/apps/details?id=com.citrix.mail>, the app id is **id=com.citrix.mail**.

- **Installed:** Specifies whether to force the Android app to install for enrolled Chrome OS device users. If **Off** and an app is installed, the app is uninstalled. If **Off** and the app is no longer configured by the policy, the app remains installed. Default is **Off**.

- **Pinned:** If **On**, pins the Android app to the Chromebook task bar. Default is **Off**.

### **Enable enrolled Chrome OS device users to run Android apps**

To enable enrolled Chrome OS device users to run Android apps: Go to **Configure > Device Policies** and add a Restrictions device policy for Chrome OS with the setting **Enable App Runtime for Chrome (ARC)** enabled.

- **Enable App Runtime for Chrome (ARC):** If **On**, allows enrolled Chrome OS device users to run Android apps. Specify ARC apps in the App Restrictions device policy. Requires Google Workspace Chrome configuration. ARC isn't available if either Ephemeral mode or multiple sign-on is enabled in the current user session. If **Off**, enterprise Chrome OS device users can't run Android apps. The default is **On**.

## **App uninstall device policy**

September 9, 2021

The App uninstall policy lets you remove apps from user devices. You might remove an app if you no longer want to support it or if you want to replace it with a similar app from a different vendor.

The app is removed when this policy is deployed to user devices. Except for Samsung Knox devices, users receive a prompt to uninstall the app. Samsung Knox device users do not receive a prompt and the app uninstalls automatically.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS and macOS settings

- **Managed app bundle ID:** In the list, select an existing managed app or **Add new**. If there are no apps configured for this platform, the list is empty, and you must add a new managed app. When you select **Add new**, a field appears where you can type a managed app name. Available for iOS 5.0 and later and macOS 11.0 and later.

## Android (legacy DA), Samsung Knox, Android Enterprise, Windows Phone, and Windows Desktop/Tablet settings

- **Apps to uninstall:** For each app you want to add, click **Add** and then do the following:
  - **App name:** In the list, click an existing app or click **Add new** to enter a new app name. If there are no apps configured for this platform, the list is empty and you must add new apps.
  - Click **Add** to add the app or click **Cancel** to cancel adding the app.

For Android Enterprise apps, also enable the App inventory device policy. See [App inventory device policy](#).

## Automatically uninstall an Enterprise app after the corresponding public app store app installs

You can configure Endpoint Management to remove the Enterprise version of Citrix apps upon installation of the public app store version. This feature prevents user devices from having two identical app icons after the public app store version installs.

A deployment condition for the App Uninstall device policy triggers Endpoint Management to remove older apps from user devices upon installation of the new version. This feature is available only for managed iOS devices connected to an Endpoint Management server in enterprise mode (XME).

To configure a deployment rule with the Installed app name condition:

- Specify the **Managed app bundle ID** for the Enterprise app.
- Add a rule: Click **New Rule** and then, as shown in the sample, choose **Installed app name** and **is equal to**. Type the app bundle ID for the public app store app.

In the example, when the public app store app (com.citrix.mail.ios) installs on a device in the delivery groups specified, Endpoint Management removes the Enterprise version (com.citrix.mail).

## App uninstall restrictions device policy

August 21, 2018

You can specify the apps users can or cannot uninstall on a Samsung SAFE or Amazon device.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Samsung SAFE or Amazon settings

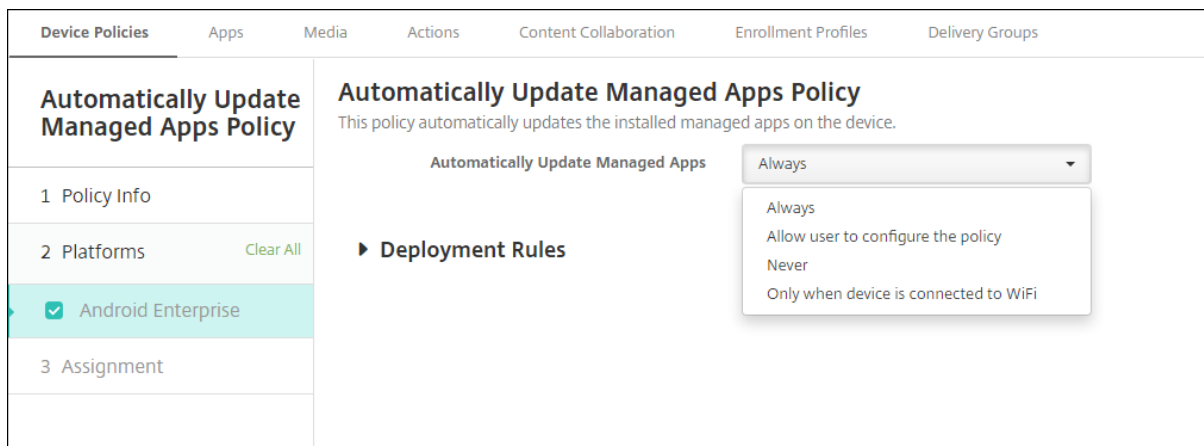
- **App Uninstall Restrictions Settings:** For each app rule you want to add, click **Add** and then do the following:
  - **App Name:** In the list, click an app or **Add new** to add a new app.
  - **Rule:** Select whether users can uninstall the app. The default is to allow uninstallation.
  - Click **Save** or **Cancel**.

## Automatically update managed apps device policy

June 23, 2021

This policy controls how installed managed apps are updated on Android Enterprise devices and Android for Workspace (Preview) devices. You can restrict the ability of users to allow automatic updates of apps on their devices. If you allow users to control automatic updates for apps on their devices, they set automatic app update policies in the managed Google Play store.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).



**Set Automatically Update Managed Apps.**

- **Always:** Enables automatic app updates. **Always** is the default.
- **Allow user to configure policy:** Allows the user to configure the automatic app update policy for the device in the managed Google Play store.
- **Never:** Disables automatic app updates.
- **Only when device is connected to Wi-Fi:** Allows automatic app updates only when the device is connected to Wi-Fi.

## BitLocker device policy

September 8, 2021

Windows 10 and Windows 11 include a disk encryption feature called BitLocker, which provides extra file and system protections against unauthorized access of a lost or stolen Windows device. For more protection, you can use BitLocker with Trusted Platform Module (TPM) chips, version 1.2 or later. A TPM chip handles cryptographic operations and generates, stores, and limits the use of cryptographic keys.

Starting with Windows 10, build 1703, MDM policies can control BitLocker. You use the BitLocker device policy in Endpoint Management to configure the settings available in the BitLocker wizard on Windows 10 and Windows 11 devices. For example, on a device with BitLocker enabled, BitLocker prompt users with several options:

- How they want to unlock their drive at startup
- How to back up their recovery key
- How to unlock a fixed drive.

BitLocker device policy setting also configure whether to:

- Enable BitLocker on devices without a TPM chip.

- Show recovery options in the BitLocker interface.
- Deny write access to a fixed or removable drive when BitLocker isn't enabled.
- Securely save an encrypted BitLocker recovery key for users to access in case they forget or misplace the key. This key can be found on the Self-Help Portal.

Note

After BitLocker encryption starts on a device, you can't change the BitLocker settings on the device by deploying an updated BitLocker device policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Requirements

- The BitLocker device policy requires Windows 10 Enterprise or Windows 11 Enterprise edition.
- Before deploying the BitLocker device policy, prepare your environment for BitLocker use. For detailed information from Microsoft, including BitLocker system requirements and setup, see the articles in [BitLocker](#).

### Windows Phone settings

<b>BitLocker policy</b>	<b>BitLocker policy</b> This policy lets you enable BitLocker on an enrolled machine and specify the encryption mechanism to use.
1 Policy Info	<b>BitLocker settings</b>
2 Platforms <span style="float: right;">Clear All</span>	<p>Require device to be encrypted <input type="checkbox"/> OFF</p> <p>Require storage card encryption <input type="checkbox"/> OFF ⓘ</p>
<input checked="" type="checkbox"/> Windows Phone	<b>► Deployment Rules</b>
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	

- **Require device to be encrypted:** Determines whether to prompt users to enable BitLocker encryption on a Windows Phone system card. If **On**, devices show a message after enrollment completes, indicating that the enterprise requires device encryption. If the user opts out of device encryption, the user isn't granted write access to the system card. If **Off**, the user isn't prompted and the BitLocker policy determines whether the device is encrypted. Defaults to **Off**.
- **Require storage card encryption:** Determines whether to prompt users to enable BitLocker encryption on a Windows Phone storage card. If **On**, storage card encryption is required to gain write permission on the card. Defaults to **Off**.





## Windows Desktop and Tablet settings

**BitLocker policy**  
This policy lets you enable BitLocker on an enrolled machine and specify the encryption mechanism to use.

**BitLocker settings**

Require device to be encrypted

**Encryption settings**

Configure encryption methods  ⓘ

Operating system drive  ⓘ

Fixed drive  ⓘ

Removable drive  ⓘ

**OS drive settings**

Require additional authentication at startup

Block BitLocker on devices without TPM chip  ⓘ

TPM startup  ⓘ

TPM startup PIN  ⓘ

TPM startup key  ⓘ

TPM startup key and PIN  ⓘ

**PIN length**

Minimum PIN length  ⓘ

**BitLocker password recovery settings**

BitLocker Recovery backup to Endpoint Management  
The Self-Help Portal displays the recovery key on the Devices page. Enable the server property shp.console.enable to provide access to the portal. [Learn more](#)

BitLocker Recovery backup to Endpoint Management  ⓘ

**OS drive recovery settings**

Enable OS drive recovery

Allow certificate based data recovery agent

48-bit recovery password  ⓘ

256-bit recovery key  ⓘ

Hide OS drive recovery options

Save recovery info to Active Directory Domain Services

Recovery info stored in Active Directory Domain Services  ⓘ

Enable BitLocker after storing recovery info in Active Directory Domain Services

Customize preboot recovery message and URL

Preboot recovery message and URL  ⓘ

**Fixed drive recovery settings**

Save recovery info to Active Directory Domain Services

Allow certificate based data recovery agent

48-bit recovery password  ⓘ

256-bit recovery password  ⓘ

Hide fixed drive recovery options

Save fixed drive recovery info to Active Directory Domain Services

Recovery info stored in Active Directory Domain Services  ⓘ

Enable BitLocker after storing recovery info in Active Directory Domain Services

**Fixed drive settings**

Block write access to fixed drives not using BitLocker

**Removable drive settings**

Block write access to removable drives not using BitLocker

Block write access to other organization device

**Other drive settings**

Prompt for other disk encryption

▶ **Deployment Rules**

- **BitLocker settings**

- **Require device to be encrypted:** Determines whether to prompt users to enable BitLocker encryption on the Windows Desktop or Tablet. If **On**, devices show a message after enrollment completes, indicating that enterprise requires device encryption. If **Off**, the user isn't prompted and BitLocker uses the policy settings. Defaults to **Off**.

- **Encryption settings**

- **Configure encryption methods:** Determines the encryption methods to use for specific drive types. If **Off**, the BitLocker wizard prompts the device user for the encryption method to use for a drive type. The encryption method for all drives defaults to XTS-AES 128 bit. The encryption method for removable drives defaults to AES-CBC 128-bit. If **On**, BitLocker uses the encryption method specified in the policy. If **On**, these extra settings appear: **Operating system drive**, **Fixed drive**, and **Removable drive**. Choose the default encryption method for each drive type. Defaults to **Off**.

- **OS drive settings**

- **Require additional authentication at startup:** Specifies the additional authentication required during device startup. Also specifies whether to allow BitLocker on devices that don't have a TPM chip. If **Off**, devices without TPM can't use BitLocker encryption. For information about TPM, see the Microsoft article, [Trusted Platform Module Technology Overview](#). If **On**, the following extra settings appear. Defaults to **Off**.
- **Block BitLocker on devices without a TPM chip:** On a device with no TPM chip, BitLocker requires users to create an unlock password or startup key. The startup key is stored in a USB drive, which the user must connect to the device before startup. The unlock password is a minimum of eight characters. Defaults to **Off**.
- **TPM startup:** On a device with TPM, there are four unlock modes: TPM-only, TPM + PIN, TPM + Key, and TPM + PIN + Key. TPM startup is for the TPM-only mode, in which encryption keys are store in the TPM chip. This mode doesn't require a user to provide extra unlock data. The user device automatically unlocks during restart, using the encryption key from the TPM chip. Defaults to **Allow TPM**.
- **TPM startup PIN:** This setting is the TPM + PIN unlock mode. A PIN can have up to 20 digits. Use the **Minimum PIN length** setting to specify the minimum PIN length. A user configures a PIN during BitLocker setup and provides the PIN during device startup.
- **TPM startup key:** This setting is the TPM + Key unlock mode. The startup key is stored in a USB or other removable drive, which the user must connect to the device before startup.
- **TPM startup key and PIN:** This setting is the TPM + PIN + Key unlock mode.  
  
If the unlock succeeds, the operating system starts loading. Otherwise, the device enters recovery mode.

- **PIN length**
  - **Minimum PIN length:** The minimum length of the TPM startup PIN. Defaults to **6**.
- **BitLocker password recovery settings**
  - **BitLocker Recovery backup to Endpoint Management:** If this option is enabled, users who must unlock their devices can find their BitLocker recovery key on the Self-Help Portal. The Endpoint Management administrator can't see a user's BitLocker recovery key. For more information on seeing your BitLocker recovery key, see [BitLocker recovery key](#).
- **OS drive recovery settings:** Configures the recovery options to users for a BitLocker-encrypted OS drive.
  - **Enable OS drive recovery:** If the unlock step fails, BitLocker prompts the user for the configured recovery key. This setting configures the operating system drive recovery options available to users if they don't have the unlock password or USB startup key. Default is **Off**.
  - **Allow certificate based data recovery agent:** Specifies whether to allow a certificate-based data recovery agent. Add a data recovery agent from Public Key Policies, which is located in the Group Policy Management Console (GPMC) or in the Local Group Policy Editor. For more information about data recovery agents, see the Microsoft article, [BitLocker Group Policy settings](#). Default is **Off**.
  - **48-bit recovery password:** Specifies whether to allow or require users to use a recovery password. BitLocker generates the password and stores it in a file or Microsoft Cloud account. Default is **Allow 48 bit password**.
  - **256-bit recovery key:** Specifies whether to allow or require users to use a recovery key. A recovery key is a BEK file, which is stored on a USB drive. Default is **Allow 256-bit recovery key**.
  - **Hide OS drive recovery options:** Specifies whether to show or hide recovery options in the BitLocker interface. If **On**, no recovery options appear in the BitLocker interface. In that case, register the devices to Active Directory, save the recovery options to Active Directory, and set **Save recovery info to AD DS** to **On**. Default is **Off**.
  - **Save recovery info to Active Directory Domain Services:** Specifies whether to save the recovery options to Active Directory Domain Services. Default is **Off**.
  - **Recovery info stored in Active Directory Domain Services:** Specifies whether to store the BitLocker recovery password or the recovery password and the key package in Active Directory Domain Services. Storing the key package supports recovering data from a drive that is physically corrupted. Default is **Backup recovery password**.
  - **Enable BitLocker after storing recovery info in Active Directory Domain Services:** Specifies whether to prevent users from enabling BitLocker unless the device is domain-

connected and the backup of BitLocker recovery information to Active Directory succeeds. If **On**, a device must be domain-joined before starting BitLocker. Default is **Off**.

- **Preboot recovery message and URL:** Specifies whether BitLocker shows a customized message and URL on the recovery screen. If **On**, the following extra settings appear: **Use default recovery message and URL**, **Use empty recovery message and URL**, **Use custom recovery message**, **Use custom recovery URL**, and **Use Endpoint Management recovery message and URL**. If **Off**, the default recovery message and URL display. Default is **Off**.
- **Fixed drive recovery settings:** Configures the recovery options for users for a BitLocker-encrypted fixed drive. BitLocker doesn't display a message to users about fixed drive encryption. To unlock a drive during startup, a user provides a password or smart card. The startup unlock settings, which aren't in this policy, appear in the BitLocker interface when a user enables BitLocker encryption on a fixed drive. For information about the related settings, see **Configure OS drive recovery**, earlier in this list. Default is **Off**.
- **Fixed drive settings**
  - **Block write access to fixed drives not using BitLocker:** If **On**, users can write to fixed drives only when those drives are encrypted with BitLocker. Default is **Off**.
- **Removable drive settings**
- **Block write access to removable drives not using BitLocker:** If **On**, users can write to removable drives only when those drives are encrypted with BitLocker. Configure this setting according to whether your organization allows write access on other organization removable drives. Default is **Off**.
- **Block write access to other organization device:** If **On**, users can't write to other devices within their organization, such as a network drive.
- **Other drive settings**
- **Prompt for other disk encryption:** Allows you to disable the warning prompt for other disk encryption on devices. Defaults to **Off**.

## Browser device policy

March 21, 2019

You can create browser device policies for Samsung SAFE or Samsung Knox devices to define whether user devices can use the browser or to limit the browser functions that the devices can use.

On Samsung devices, you can completely disable the browser, or you can enable or disable pop-ups, JavaScript, cookies, autofill, and whether to force fraud warnings.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Samsung SAFE and Samsung Knox settings

- **Disable browser:** Select whether to completely disable the Samsung browser on users' devices. The default is **Off**, which lets users use the browser. When you disable the browser, the following options disappear.
- **Disable pop-up:** Select whether to allow pop-up messages on the browser.
- **Disable Javascript:** Select whether to allow JavaScript to run on the browser.
- **Disable cookies:** Select whether to allow cookies.
- **Disable autofill:** Select whether to allow users to turn on the browser's autofill function.
- **Force fraud warning:** Select whether to display a warning when users visit a fraudulent or compromised website.

### Calendar (CalDav) device policy

March 24, 2020

You can add a device policy in Endpoint Management to add a calendar (CalDAV) account to users' iOS or macOS devices to enable them to synchronize scheduling data with any server that supports CalDAV.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### iOS settings

- **Account description:** Type an account description. This field is required.
- **Host name:** Type the address of the CalDAV server. This field is required.
- **Port:** Type the port on which to connect to the CalDAV server. This field is required. The default is **8443**.
- **Principal URL:** Type the base URL to the user's calendar.
- **User name:** Type the user's logon name. This field is required.
- **Password:** Type an optional user password.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the CalDAV server. The default is **On**.

- **Policy settings**

- **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
  - \* **Select date:** Click the calendar to select the specific date for removal.
  - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 or later.

## macOS settings

- **Account description:** Type an account description. This field is required.
- **Host name:** Type the address of the CalDAV server. This field is required.
- **Port:** Type the port on which to connect to the CalDAV server. This field is required. The default is **8443**.
- **Principal URL:** Type the base URL to the user's calendar.
- **User name:** Type the user's logon name. This field is required.
- **Password:** Type an optional user password.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the CalDAV server. The default is **On**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

## Cellular device policy

March 24, 2020

This policy allows you to configure cellular network settings on an iOS device.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

You can use macros in non-string fields, such as **Proxy server port**.

For example, you can use a macro such as `${ device.xyz }` or `${ setting.xyz }`, which expands into an integer. You can also use the macros in a device configuration XML file that you import into Endpoint Management by using the Import iOS & macOS Profile device policy.

- **Attach APN**
  - **Name:** A name for this configuration.
  - **Authentication type:** In the list, click Challenge Handshake Authentication Protocol (**CHAP**) or Password Authentication Protocol (**PAP**). The default is **PAP**.
  - **User name** and **Password:** The user name and password to use for authentication.
- **APN**
  - **Name:** A name for the Access Point Name (APN) configuration.
  - **Authentication type:** In the list, click **CHAP** or **PAP**. The default is **PAP**.
  - **User name** and **Password:** The user name and password to use for authentication.
  - **Proxy server:** The proxy server network address.
  - **Proxy server port:** The proxy server port.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

## Connection scheduling device policy

August 24, 2020

### Important:

Citrix recommends that you use Firebase Cloud Messaging (FCM) to control connections from Android, Android Enterprise, and Chrome OS devices to Endpoint Management. For information on using FCM, see [Firebase Cloud Messaging](#).

If you choose to not use FCM, you can create connection scheduling policies to control how and when user devices connect to Endpoint Management. If you choose to use FCM, you must also create a

connection scheduling policy.

You can specify that users connect their devices manually or that devices connect within a defined time frame.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Android and Android Enterprise settings

- **Require devices to connect:** Click the option you want to set for this schedule.
  - **Never:** Connect manually. Users must initiate the connection from Endpoint Management on their devices. Citrix doesn't recommend this option for production deployments because it prevents you from deploying security policies to devices, which means users never receive any new apps or policies. The **Never** option is enabled by default.
  - **Every:** Connect at the designated interval. When this option is in effect and you send a security policy such as a lock or a wipe, Endpoint Management processes the action on the device the next time the device connects. When you select this option, the **Connect every N minutes** field appears where you must enter the number of minutes after which the device must reconnect. The default, and minimum value, is **120**.
  - **Define schedule:** Endpoint Management on the user device attempts to reconnect to the Endpoint Management server after a network connection loss. Endpoint Management and monitors the connection by transmitting control packets at regular intervals within the time frame you define. See *Defining a connection time frame*, next, for how to define a connection time frame.
    - \* **Require a connection within each of these ranges:** Users' devices must be connected at least once in any of the defined time frames.
    - \* **Use local device time rather than UTC:** Synchronize the defined time frames to local device time rather than Coordinated Universal Time (UTC).

## Defining a connection time frame

When you enable the following options, a timeline appears where you can define the time frames you want. You can enable either or both options to require a permanent connection during specific hours or to require a connection within certain time frames. Each square in the timeline is 1 hour. To specify a connection between 8:00 AM and 9:00 AM every weekday, you click the square on the timeline between 8 AM and 9 AM every weekday.

For example, the two timelines in the following figure require:

- A permanent connection between 8:00 AM and 10:00 AM every weekday
- A permanent connection between 1:00 AM Saturday and 2:00 AM Sunday



- At least one connection every weekday between 5:00 AM and 8:00 AM or between 10:00 AM and 12:00 AM

The screenshot shows a configuration window for defining a schedule. At the top, there is a radio button labeled "Define schedule" which is selected. Below it, a toggle switch for "Maintain permanent connection during these hours" is turned "ON". The main area contains two grids representing weekly schedules. The first grid, corresponding to the "ON" toggle, shows a 7x24 grid with days Mon-Sun on the y-axis and hours 1 AM to 12 AM on the x-axis. Green blocks indicate connection requirements: a 2x2 block (Mon-Fri, 8 AM-10 AM), a 2x2 block (Mon-Fri, 10 AM-12 PM), a 1x1 block (Sun, 1 AM), and a 1x1 block (Sat, 12 AM). The second grid, corresponding to the "Require a connection within each of these ranges" toggle (also "ON"), shows a similar 7x24 grid. Green blocks indicate connection requirements: a 3x3 block (Mon-Fri, 5 AM-8 AM), a 3x3 block (Mon-Fri, 10 AM-12 PM), and a 5x12 block (Mon-Fri, 10 AM-12 PM, Sat-Sun, 10 AM-12 AM). At the bottom, a toggle switch for "Use local device time rather than UTC" is turned "OFF".

## Chrome OS settings

- **Require devices to connect:** Specify the connection frequency in **Connect every N minutes**. Default is **120** minutes (2 hours).

## Contacts (CardDAV) device policy

March 24, 2020

You can add a device policy in Endpoint Management to add an iOS contacts (CardDAV) account to users' iOS or macOS devices to enable them to synchronize contact data with any server that supports CardDAV.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### iOS settings

- **Account description:** Type an account description. This field is required.
- **Host name:** Type the address of the CardDAV server. This field is required.
- **Port:** Type the port on which to connect to the CardDAV server. This field is required. The default is **8443**.
- **Principal URL:** Type the base URL to the user's calendar.
- **User name:** Type the user's logon name. This field is required.
- **Password:** Type an optional user password.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the CardDAV server. The default is **On**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

### macOS settings

- **Account description:** Type an account description. This field is required.
- **Host name:** Type the address of the CardDAV server. This field is required.
- **Port:** Type the port on which to connect to the CardDAV server. This field is required. The default is **8443**.
- **Principal URL:** Type the base URL to the user's calendar.
- **User name:** Type the user's logon name. This field is required.
- **Password:** Type an optional user password.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the CardDAV server. The default is **On**.
- **Policy settings**

- **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
  - \* **Select date:** Click the calendar to select the specific date for removal.
  - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
- **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
- **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

## Content device policy

June 19, 2020

You can control various web content options for Chrome OS, including what homepage to show and how popups are handled.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Chrome OS Settings

The screenshot displays the 'Content' configuration page for a Chrome OS policy. On the left, a sidebar lists 'Policy Info', 'Platforms' (with a 'Clear All' link), 'Chrome OS' (selected), and 'Assignment'. The main content area is titled 'Content' and contains the following settings:

- Home Page Settings:** A dropdown menu set to 'New tab page'.
- Pop-up default settings:** A dropdown menu set to 'Allow pop-ups'.
- Pop-ups allowed from these sites:** A text input field labeled 'URLs allowed' with an 'Add' button.
- Pop-ups not allowed from these sites:** A text input field labeled 'URLs not allowed' with an 'Add' button.
- Pages to load on startup:** A text input field labeled 'Start-up URL' with an 'Add' button.

- **Home Page Settings:** Select whether the home page should be a new tab or a specified URL.
- **Homepage URL:** If you selected a Homepage URL for the Homepage settings, type the URL here.
- **Pop-up default settings:** Select whether to allow or block popups by default. You can then allow or block specific URLs from opening popups.
- **Pop-ups allowed from these sites:** Specify a list of URLs allowed to open popups.

- **Popup not allowed from these sites:** Specify a list of URLs blocked from opening popups.
- **Pages to load on startup:** Specify a list of URLs to be opened on browser startup.

## Copy Apps to Samsung Container device policy

October 1, 2020

For apps that are already installed on a device, you can specify to copy the apps to a Knox container on supported Samsung devices. For information about supported devices, see the Samsung article, [Samsung Knox Supported Devices](#).

Apps copied to the Knox container are only available when users sign in to the Knox container.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Prerequisites

- Enroll the device in Endpoint Management.
- Deploy the Samsung MDM keys (ELM and KLM). For how to do this, see [Samsung MDM License Key device policy](#).
- Install apps on the device.
- Initialize Knox on the device to copy apps to the Knox container.

### Samsung Knox settings

- **New app:** For each app you want to add to the list, click **Add** and then do the following:
  - Type a package ID; for example, com.mobiwolf.lacingart for the LacingArt app.
  - Click **Save** or **Cancel**.

## Credentials device policy

September 20, 2021

Credentials device policies point to a PKI configured in Endpoint Management. For example, your PKI configuration might include a PKI entity, a keystore, a credential provider, or a server certificate. For more information about credentials, see [Certificates and authentication](#).

Each supported platform requires a different set of values, which are described in this article.

**Note:**

Before you can create this policy, you need the credential information you plan to use for each platform, plus any certificates and passwords.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

**iOS and tvOS settings**

### Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

**Credential type** Certificate (.cer, .crt, .der and .pem)

**Credential name \***

**The credential file path**

Policy Settings

**Remove policy**  Select date  
 Duration until removal (in hours)

► **Deployment Rules**

Configure the following settings:

- **Credential type:** In the list, click the type of credential to use with this policy, and then enter the following information for the selected credential:
  - **Certificate**
    - \* **Credential name:** Enter a unique name for the credential.
    - \* **The credential file path:** Select the credential file by clicking Browse and navigating to the file's location.
  - **Keystore**
    - \* **Credential name:** Enter a unique name for the credential.
    - \* **The credential file path:** Select the credential file by clicking Browse and navigating to the file's location.
    - \* **Password:** Enter the keystore password for the credential.
  - **Server certificate**
    - \* **Server certificate:** In the list, click the certificate to use.

- **Credential provider**
  - \* **Credential provider:** In the list, click the name of the credential provider.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field. Not available for iOS.

## macOS settings

### Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

**Credential type** Certificate (.cer, .crt, .der and .pem) ▼

**Credential name \***

**The credential file path**  Browse

**Policy Settings**

**Remove policy**  Select date  Duration until removal (in hours)

📅

**Allow user to remove policy** Always ▼ ?

**Profile scope** User ▼ macOS 10.7+

Configure the following settings:

- **Credential type:** In the list, click the type of credential to use with this policy, and then enter the following information for the selected credential:
  - **Certificate**
    - \* **Credential name:** Enter a unique name for the credential.
    - \* **The credential file path:** Select the credential file by clicking **Browse** and navigating to the file's location.
  - **Keystore**
    - \* **Credential name:** Enter a unique name for the credential.

- \* **The credential file path:** Select the credential file by clicking **Browse** and navigating to the file's location.
- \* **Password:** Enter the keystore password for the credential.
- **Server certificate**
  - \* **Server certificate:** In the list, click the certificate to use.
- **Credential provider**
  - \* **Credential provider:** In the list, click the name of the credential provider.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

## Android settings

**Credentials Policy**

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Credential type Certificate (.cer, .crt, .der and .pem) ▼

The credential file path  Browse

▶ **Deployment Rules**

Configure the following settings:

- **Credential type:** In the list, click the type of credential to use with this policy, and then enter the following information for the selected credential:
  - **Certificate**

- \* **Credential name:** Type a unique name for the credential.
- \* **The credential file path:** Select the credential file by clicking Browse and then navigating to the file's location.
- **Keystore**
  - \* **Credential name:** Type a unique name for the credential.
  - \* **The credential file path:** Select the credential file by clicking **Browse** and then navigating to the file location.
  - \* **Password:** Type the keystore password for the credential.
- **Server certificate**
  - \* **Server certificate:** In the list, click the certificate to use.
- **Credential provider**
  - \* **Credential provider:** In the list, click the name of the credential provider.

## Android Enterprise settings

**Credentials Policy** ✕

This policy lets you deliver certificates to devices. On iOS, certificates such as a certificate for wi-fi authentication can also be used as part of another policy. For Windows phones, only Windows 10 and later supervised devices support the policy.

Remove credentials  OFF

Apply To COPE  OFF

Credential type

The credential file path

Certificate Alias

▶ Deployment Rules

Configure these settings to determine how credentials settings are applied:

- **Remove credentials:** Set to **On** to configure the following settings. Default is **Off**.
  - **Remove user credentials:** Removes certificates from the managed keystore. Default is **Off**.
  - **Remove trusted root certificates:** Uninstalls all non-system CA certificates. Default is **Off**.
- **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices:** Allows you to configure credentials policy settings for fully managed devices with work profiles. When this setting is **On**, select one of these settings. This policy applies to the work profile on devices only.



Configure the credential settings:

- **Credential type:** In the list, click the type of credential to use with this policy, and then enter the following information for the selected credential:
  - **Certificate**
    - \* **Credential name:** Type a unique name for the credential.
    - \* **The credential file path:** Select the credential file by clicking **Browse** and then navigating to the file location.
  - **Keystore**
    - \* **Credential name:** Type a unique name for the credential.
    - \* **The credential file path:** Select the credential file by clicking **Browse** and then navigating to the file location.
    - \* **Password:** Type the keystore password for the credential.
    - \* **Certificate Alias:** A certificate alias makes it easier for apps to access the certificate. Configure a certificate alias in the Android Enterprise Managed Configuration device policy. Then, type the alias in the **Certificate Alias** field in the Credentials device policy. Apps retrieve the certificate and authenticate the VPN without any action by users.
  - **Server certificate**
    - \* **Server certificate:** In the list, click the certificate to use.
  - **Credential provider**
    - \* **Credential provider:** In the list, click the name of the credential provider.
    - \* **Apps to use certificates:** To specify apps that have silent access to the credentials from this provider: Click **Add**, select an app, and click **Save**.
    - \* **Certificate Alias:** A certificate alias makes it easier for apps to access the certificate. Configure a certificate alias in the Android Enterprise Managed Configuration device policy. Then, type the alias in the **Certificate Alias** field in the Credentials device policy. Apps retrieve the certificate and authenticate the VPN without any action by users.

## Chrome OS settings

In this preview, Chromebook devices can use the credential policy to take advantage of the Chrome operating system's built-in certificate management. Administrators can upload a certificate authority's private certificate for signing and issuing the client certificates. This certificate allows Citrix Endpoint Management to create and push certificates to Chromebook devices.

### Credentials Policy

This policy lets you deliver certificates to devices. On iOS, certificates such as a certificate for wi-fi authentication can also be used as part of another policy. For Windows phones, only Windows 10 and later supervised devices support the policy.

Credential type:

The credential file path:

Password \*

- **Credential type:** In the list, click the type of credential to use with this policy and then enter the following information for the selected credential:
  - **Keystore**
    - \* **The credential file path:** Select the credential file by clicking Browse and navigating to the file's location
    - \* **Password:** Enter the keystore password for the credential.

## Windows Desktop/Tablet settings

### Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Certificate Type:

Store device:

Location:

Credential type:

Credential file path \*

▶ Deployment Rules

- **Certificate Type:** In the list, click either **ROOT** or **CLIENT**.
- If you click **ROOT**, configure these settings:
  - **Store device:** In the list, click **root**, **My**, or **CA** for the location of the certificate store for the credential. **My** stores the certificate in users' certificate stores.
  - **Location:** For Windows 10 and Windows 11 tablets, **System** is the only location.
  - **Credential type:** For Windows 10 and Windows 11 tablets, **Certificate** is the only credential type.

- **Credential file path:** Select the certificate file by clicking **Browse** and navigating to the file's location.
- If you click **CLIENT**, configure these settings:
  - **Location:** For Windows 10 and Windows 11 tablets, **System** is the only location.
  - **Credential type:** For Windows 10 and Windows 11 tablets, **Keystore** is the only credential type.
  - **Credential name:** Type the name of the credential. This field is required.
  - **Credential file path:** Select the certificate file by clicking **Browse** and navigating to the file's location.
  - **Password:** Type the password associated with the credential. This field is required.

## Windows Phone settings

**Credentials Policy** ✕

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Certificate Type:

Store device:

Location:

Credential type:

The credential file path \*

► Deployment Rules

- **Certificate Type:** In the list, click either **ROOT** or **CLIENT**.
- If you click **ROOT**, configure these settings:
  - **Store device:** In the list, click **root**, **My**, or **CA** for the location of the certificate store for the credential. **My** stores the certificate in users' certificate stores.
  - **Location:** The **System** value is the only location for Windows phones.
  - **Credential type:** Certificate is the only credential type for Windows phones.
  - **Credential file path:** Select the certificate file by clicking **Browse** and navigating to the file's location.
- If you click **CLIENT**, configure these settings:
  - **Location:** For Windows phones, **System** is the only location.
  - **Credential type:** For Windows phones, **Keystore** is the only credential type.
  - **Credential name:** Type the name of the credential. This field is required.

- **Credential file path:** Select the certificate file by clicking **Browse** and navigating to the file's location.
- **Password:** Type the password associated with the credential. This field is required.

## Workspace Hub settings

### Credentials Policy ×

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

The credential file path  **Browse** ?

- **The credential file path:** Browse for the CA certificate file or .zip file containing the certificates to upload. This policy supports .cer, .crt, .pem, and .der certificate files.

## Custom XML device policy

September 8, 2021

You can create custom XML policies in Endpoint Management to customize the following features on supported Windows, Zebra Android, and Android Enterprise devices:

- Provisioning, which includes configuring the device, and enabling or disabling features
- Device configuration, which includes allowing users to change settings and device parameters
- Software upgrades, which include providing new software or bug fixes to be loaded onto the device, including apps and system software
- Fault management, which includes receiving error and status reports from the device

### Note:

When creating your XML content, use the \% character with caution. The \% character is an XML reserved character, used only to escape XML special characters. To use \% in a name, encode it as \%25.

For Windows devices: You create your custom XML configuration by using the Open Mobile Alliance Device Management (OMA DM) API in Windows. Creating custom XML with the OMA DM API is beyond the scope of this topic. For more information about using the OMA DM API, see [OMA DM protocol support](#) on the Microsoft Developer Network site.

**Note:**

For Windows 10 RS2 Phone: After a Custom XML policy or Restrictions policy that disables Internet Explorer deploys to the phone, the browser remains enabled. To work around this issue, restart the phone. This is a third-party issue.

For Zebra Android and Android Enterprise devices: You create your custom XML configuration by using the MX Management System (MXMS). Creating custom XML with the MXMS API is beyond the scope of this article. For more information about using MXMS, see the Zebra product documentation.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## **Windows Phone, Windows Desktop/Tablet, Zebra Android, and Android Enterprise settings**

**XML content:** Type, or cut and paste, the custom XML code you want to add to the policy.

After you click **Next**, Endpoint Management checks the XML content syntax. Any syntax errors appear below the content box. Fix any errors before you continue.

If there are no syntax errors, the **Custom XML Policy** assignment page appears.

## **Use Windows AutoPilot to set up and configure devices**

Windows AutoPilot is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use. You can use Windows AutoPilot to reset, repurpose, and recover devices. AutoPilot helps to remove some of the complexity of your current operating system deployment. Using AutoPilot reduces the task to a set of simple settings and operations that can get your devices ready to use quickly and efficiently.

### **Prerequisites**

- Devices registered to the organization in the Microsoft Store for Business portal.
- Company branding configured in the Azure Active Directory portal.
- Company has an Azure Active Directory Premium P1 or P2 subscription.
- Configure Azure Active Directory as the IdP type for Endpoint Management. In the Endpoint Management console, go to **Settings > Identity Provider (IDP)**.
- Network connectivity to cloud services used by Windows AutoPilot.
- Devices pre-installed with Windows 10 Professional, Enterprise or Education (version 1703 or later) or Windows 11 Professional, Enterprise or Education.
- Devices have access to the internet.

For more information about configuring prerequisites, see the Microsoft Windows documentation on AutoPilot: <https://docs.microsoft.com>.

### To configure Windows Automatic Redeployment in Endpoint Management for AutoPilot devices

1. Follow the steps to add a custom XML policy at Custom XML Device Policy. Add the following in **XML Content**:

```
1 <Add>
2 <CmdID>_cmdid_</CmdID>
3 <Item>
4 <Target>
5 <LocURI>./Vendor/MSFT/Policy/Config/CredentialProviders/
   DisableAutomaticReDeploymentCredentials</LocURI>
6 </Target>
7 <Meta>
8 <Format xmlns="syncml:metinf">int</Format>
9 </Meta>
10 <Data>0</Data>
11 </Item>
12 </Add>
13
14 <!--NeedCopy-->
```

2. On the Windows lock screen, type the keystroke **CTRL + Windows key + R**.
3. Log in with an Azure Active Directory account.
4. The device verifies that the user has rights to redeploy the device. The device then redeploys.
5. After the device updates with the AutoPilot configuration, the user can then log into the freshly configured device.

## Defender device policy

September 8, 2021

Windows Defender is malware protection included with Windows 10 and Windows 11. You can use the Endpoint Management device policy, Defender, to configure the Microsoft Defender policy for Windows 10 and Windows 11 desktop and tablet devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Windows Desktop and Tablet settings

The screenshot shows the 'Defender policy' configuration page in the Citrix Endpoint Management console. The left sidebar contains a navigation menu with the following items: '1 Policy Info', '2 Platforms' (with a 'Clear All' link), '3 Assignment', and '4 Windows Desktop/Tablet' (which is selected and highlighted in blue). The main content area is titled 'Defender policy' and includes a subtitle: 'This policy configures Windows Defender settings for Windows 10 desktop and tablet devices.' The settings are as follows:

- Allow scans of archived files:  (Off)
- Allow cloud protection:  (On)
- Allow a full scan of removable drives:  (On)
- Allow real-time monitoring:  (On)
- Allow scans of network files:  (On)
- Allow access to the Windows Defender UI:  (On)
- Excluded extensions:  (with a help icon)
- Excluded paths:  (with a help icon)
- Excluded processes:  (with a help icon)
- Submit samples for further analysis:  (dropdown menu)

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

- **Allow scanning of archived files:** Allows or blocks Defender to scan archived files. Defaults to **Off**.
- **Allow cloud protection:** Allows or blocks Defender to send information to Microsoft about malware activity. Defaults to **On**.
- **Allow a full scan of removable drives:** Allows or blocks Defender to scan removable drives such as USB sticks. Defaults to **On**.
- **Allow real-time monitoring:** Defaults to **On**.
- **Allow scans of network files:** Allows or blocks Defender to scan network files. Defaults to **On**.
- **Allow access to the Windows Defender UI:** Specifies whether users can access the Windows Defender user interface. This setting takes effect the next time the user device starts. If this setting is **Off**, users don't receive any Windows Defender notifications. Defaults to **On**.
- **Excluded extensions:** The extensions to exclude from real-time or scheduled scans. To separate extensions, use the | character. For example, `lib\|obj`.
- **Excluded paths:** The paths to exclude from real-time or scheduled scans. To separate paths, use the | character. For example, `C:\Example|C:\Example1`.
- **Excluded processes:** The processes to exclude from real-time or scheduled scans. To separate processes, use the | character. For example, `C:\Example.exe|C:\Example1.exe`.
- **Submit samples for further analysis:** Controls whether to send to Microsoft files that might require further analysis to determine if they are malicious. Options: **Always prompt**, **Send safe samples**, **Never send**, **Send all samples**. Defaults to **Send safe samples**.

## Device Guard device policy

September 9, 2021

Device Guard is a security feature available with Windows 10 and Windows 11. This feature enables virtualization-based security by using the Windows Hypervisor to support security services on the device. The Device Guard policy enables security features such as secure boot, UEFI lock, and virtualization.

### Prerequisites

- Windows 10 and Windows 11 Desktops and Tablets with an Enterprise or Education license
- Device Guard enabled in Windows

For more information on Device Guard, see <https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-manage>.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Windows Desktop and Tablet settings

The screenshot displays the 'Device Guard' configuration page. On the left, a sidebar lists 'Device Guard' as the selected policy, with sub-sections for '1 Policy Info', '2 Platforms' (with a 'Clear All' link), '3 Assignment', and '4 Deployment Rules'. The 'Windows Desktop/Tablet' platform is selected under '2 Platforms'. The main content area shows the 'Device Guard' configuration for this platform. It includes a description: 'This policy configures virtualization-based security settings on Windows 10 desktops and tablets. The policy applies to devices running Windows 10 Enterprise or Education, version 1709 (RS3) or later.' The settings are: 'Enable virtualization-based security' (disabled), 'Configure LSA protection' (set to 'Turns off Credential Guard'), and 'Specify platform security level' (set to 'Turns on VBS with Secure Boot').

- **Enable virtualization-based security:** Disable or enable virtualization-based security features. Virtualization-based security uses the Windows Hypervisor to support security services.
- **Configure LSA protection:** Lets you configure Credential Guard. This setting lets users turn on Credential Guard with virtualization-based security to help protect credentials on the next restart. Options are **Turns off Credential Guard**, **Turns on Credential Guard with UEFI lock**, and **Turns on Credential Guard without UEFI lock**. Default is **Turns off Credential Guard**.



- **Specify platform security level:** Lets you specify the platform security level on the next restart. Options are **Turns on VBS with Secure Boot** and **Turns on VBS with Secure Boot and direct memory access**. Default is **Turns on VBS with Secure Boot**.

Endpoint Management queries a device to determine whether the virtualization based security settings match the settings on the server. If the security settings match, Endpoint Management doesn't deploy this policy to the device. If the security settings don't match, Endpoint Management deploys the policy.

## Device Health Attestation device policy

September 8, 2021

In Endpoint Management, you can require Windows 10 and Windows 11 devices to report the state of their health. To report their health state, devices send specific data and runtime information to the Health Attestation Service (HAS) for analysis. The HAS creates and returns a Health Attestation Certificate that the device then sends to Endpoint Management. Endpoint Management uses the contents of the Health Attestation Certificate to deploy automatic actions that you have set up.

The data verified by the HAS are:

- AIK Present
- Bit Locker Status
- Boot Debugging Enabled
- Boot Manager Rev List Version
- Code Integrity Enabled
- Code Integrity Rev List Version
- Apple Deployment Program Policy
- ELAM Driver Loaded
- Issued At
- Kernel Debugging Enabled
- PCR
- Reset Count
- Restart Count
- Safe Mode Enabled
- SBCP Hash
- Secure Boot Enabled
- Test Signing Enabled
- VSM Enabled
- WinPE Enabled

For more information, refer to the Microsoft [Device HealthAttestation CSP](#) page.

You can configure DHA by using Microsoft Cloud or an on-premises Windows DHA server, as follows:

- To configure DHA by using Microsoft Cloud: Add a Device Health Attestation policy and configure it as described in this article.
- To configure DHA by using an on-premises Windows DHA server: Configure a DHA server. Then, add a Device Health Attestation policy and configure it as described in this article.

To configure a DHA server, you install the DHA server role on a machine running Windows Server 2016 Technical Preview 5 or later. For instructions, see [Configure an on-premises Device Health Attestation server](#).

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Windows Phone and Windows Desktop/Tablet settings

### If you configure DHA by using Microsoft Cloud

- **Enable Device Health Attestation:** Select whether to require Device Health Attestation. The default is **Off**.

### If you configure DHA by using an on-premises Windows DHA server

- **Enable Device Health Attestation:** Set to **On**.
- **Configure On-prem Health Attestation Service:** Set to **On**.
- **On-prem DHA Service FQDN:** Type the fully qualified domain name of the DHA server you set up.
- **On-prem DHA API version:** Select the version of the DHA service installed on the DHA server.

## Device name device policy

August 26, 2019

You can set the names on supervised iOS and macOS devices so that you can easily identify the devices. You can use macros, text, or a combination of both to define the device's name. For example, to set the device name as the serial number of the device, you would use `${device.serialnumber}`. To set the device name as a combination of the user's name and your domain, you would use `${user.username}@example.com`. For more information about macros, see [Macros in Endpoint Management](#).

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS and macOS settings

- **Device name:** Type the macro, a combination of macros, or a combination of macros and text to name each device uniquely. For example, use `${device.serialnumber}` to set the device names to each device's serial number, or use `${device.serialnumber} ${ user.username }` to include the user's name in the device name.

## Education Configuration device policy

April 16, 2020

The Education Configuration device policy defines:

- The Apple Classroom app settings for instructor devices.
- The certificates used to perform client authentication between instructor and student devices.

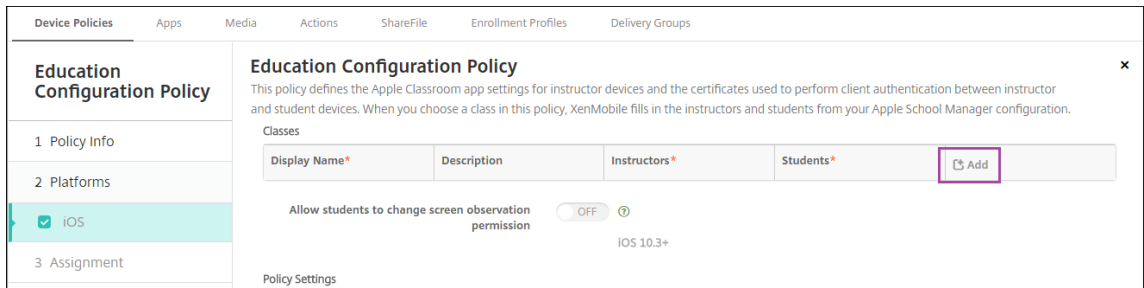
The Education Configuration device policy is supported for iOS (iPadOS) devices.

When you choose a class in this policy, the Endpoint Management console fills in the instructors and students from your Apple School Manager configuration. Create one policy if the Apple Classroom app settings in this policy are the same for all classes.

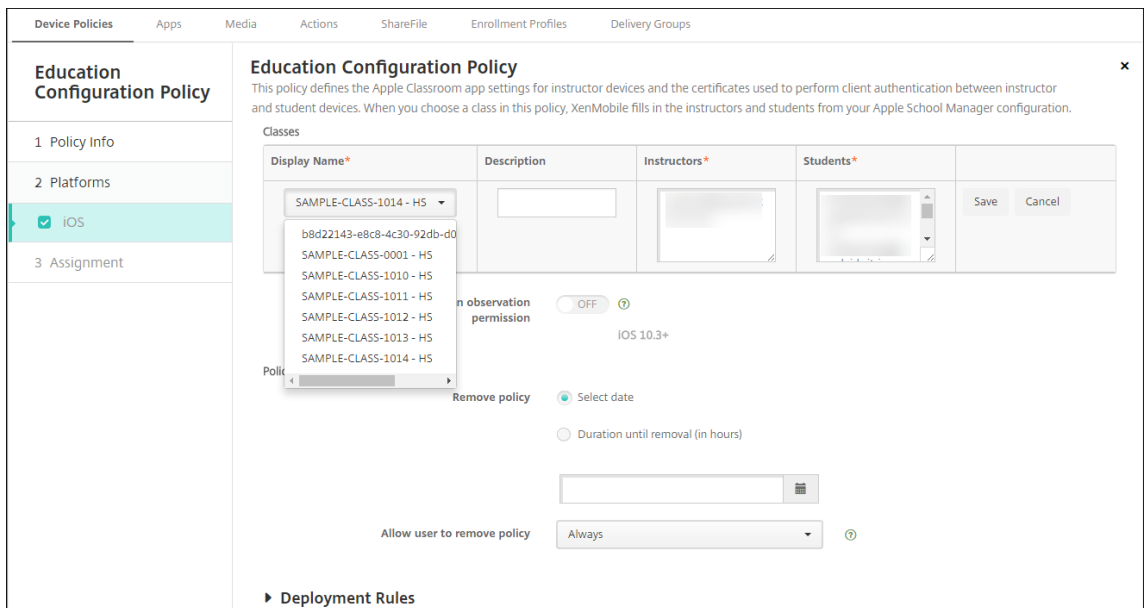
To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

- **Classes:** To add a class, click **Add**.



Then, Click the **Display Name** list. A list of classes obtained from your connected Apple School Manager account appears.



When you choose a class from **Display Name**, Endpoint Management fills in the instructors and students. Continue adding classes.

The screenshot displays the 'Education Configuration Policy' for iOS. The left sidebar shows a navigation menu with 'Policy Info', 'Platforms', 'iOS' (selected), and 'Assignment'. The main content area is titled 'Education Configuration Policy' and includes a description: 'This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.' Below this is a table of classes:

Display Name*	Description	Instructors*	Students*	Add
SAMPLE-CLASS-0001 - HS				
SAMPLE-CLASS-1010 - HS				
SAMPLE-CLASS-1011 - HS				
SAMPLE-CLASS-1012 - HS				

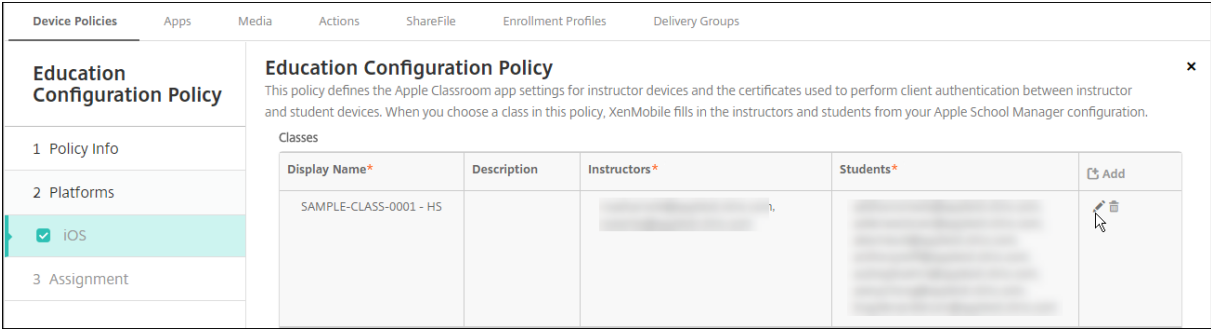
Below the table, there is a toggle for 'Allow students to change screen observation permission' which is currently 'ON'. At the bottom, there are 'Policy Settings' including 'Remove policy' with options for 'Select date' and 'Duration until removal (in hours)'.

- **Allow students to change screen observation permission:** If **On**, students enrolled in managed classes can choose whether to allow their teacher to observe their device screens. Default is **Off**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

### To edit class information in the policy

You can add a description to a class (the “Display name” in the Classroom app). You can also add or remove instructors and students. Endpoint Management doesn’t save such changes to your Apple School Manager account. For more information, see “Manage instructor, student, and class data” in [Integrate with Apple Education features](#).

Mouse over the **Add** column for the class you want to edit and then click the pencil icon.



The screenshot displays the 'Education Configuration Policy' configuration page in the Citrix Endpoint Management console. The page has a navigation menu on the left with the following items: '1 Policy Info', '2 Platforms', '3 Assignment', and 'iOS' (which is selected and highlighted in green). The main content area is titled 'Education Configuration Policy' and includes a description: 'This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.' Below the description is a table titled 'Classes' with the following columns: 'Display Name\*', 'Description', 'Instructors\*', 'Students\*', and 'Add'. The 'Add' column contains a trash icon for deleting a class. The table contains one row with the following data: 'SAMPLE-CLASS-0001 - HS' in the 'Display Name\*' column, an empty 'Description' column, a blurred 'Instructors\*' column, a blurred 'Students\*' column, and a trash icon in the 'Add' column.

To delete a class from the policy, mouse over the **Add** column for the class you want to delete and then click the trash icon.

## Endpoint Management options device policy

June 23, 2021

You add an Endpoint Management options policy to configure Secure Hub behavior when connecting to Endpoint Management from Android devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Android settings

### Endpoint Management Options Policy

This policy lets you configure parameters for connections to Endpoint Management.

#### Device agent configuration

Traybar notification - hide traybar icon  OFF

Connection time-out(s) \*

Keep-alive interval(s) \*

#### Remote support

Prompt the user before allowing remote control  OFF

Before a file transfer

► **Deployment Rules**

- **Tray bar notification - hide tray bar icon:** Select whether the tray bar icon is hidden or visible. The default is **Off**.
- **Connection: time-outs:** Type the length of time in seconds that a connection can be idle before the connection times out. The default is 20 seconds.
- **Keep-alive intervals:** Type the length of time in seconds to keep a connection open. The default is 120 seconds.
- **Prompt the user before allowing remote control:** Select whether to prompt the user before allowing remote support control. The default is **Off**.
- **Before a file transfer:** In the list, click whether to warn the user about a file transfer or whether to ask the user for permission. Available values: **Do not warn the user**, **Warn the user**, and **Ask for user permission**. The default is **Do not warn the user**.

## Android Enterprise settings

### Endpoint Management Options Policy

This policy lets you configure parameters for connections to Endpoint Management.

**Device agent configuration**

Traybar notification - hide traybar icon  OFF

**VPN always-on configuration**

Enable always-on VPN  ON ?

VPN package  ?

► **Deployment Rules**

Supported starting with Android version 7.

- **Tray bar notification - hide tray bar icon:** Select whether the tray bar icon is hidden or visible. The default is **Off**.
- **Enable always-on VPN:** Select whether the always-on VPN is enabled. When this setting is **On**, the VPN service starts when the device is powered on. The VPN service continues to run while the device is on. Default is **Off**.
- **VPN Package:** Type the package name of the VPN app the device uses. By default, the package name of the Citrix SSO app, **com.citrix.CitrixVPN**, is autopopulated in this field.

## Android for Workspace (Preview) settings

- **Enable always-on VPN:** Select whether the always-on VPN is enabled. When this setting is **On**, the VPN service starts when the device is powered on. The VPN service continues to run while the device is on. Default is **Off**.

## Endpoint Management uninstall device policy

August 21, 2018

You can add a device policy in Endpoint Management to uninstall Endpoint Management from Android devices. When deployed, this policy removes Endpoint Management from all devices in the deployment group.



To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Android settings

- **Uninstall Endpoint Management from devices:** Select whether to uninstall Endpoint Management from every device to which you deploy this policy. The default is **Off**.

## Enterprise Hub device policy

April 6, 2020

An Enterprise Hub device policy for Windows Phone lets you distribute apps through the Enterprise Hub Company store.

Before you can create the policy, you need the following:

- An AET (.aetx) signing certificate from DigiCert
- The Citrix Company Hub app signed by using the Microsoft app signing tool (XapSignTool.exe)

#### Note:

Endpoint Management supports only one Enterprise Hub policy for one mode of Windows Phone Secure Hub. For example, to upload Windows Phone Secure Hub for Endpoint Management, don't create multiple Enterprise Hub policies with different versions of Secure Hub. You can only deploy the initial Enterprise Hub policy during device enrollment.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Windows Phone settings

The screenshot shows the 'Enterprise Hub Policy' configuration page in the Citrix Endpoint Management console. The page is titled 'Enterprise Hub Policy' and includes a navigation menu on the left with the following items: '1 Policy Info', '2 Platforms', '3 Assignment', and 'Windows Phone' (which is selected). The main content area contains the following information:

- Enterprise Hub Policy**: To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe).
- Upload .aetx file**: A text input field followed by a green 'Browse' button.
- Upload signed Enterprise Hub app**: A text input field followed by a green 'Browse' button.
- Deployment Rules**: A section header with a right-pointing arrow.

At the bottom right of the page, there are 'Back' and 'Next >' buttons.

- **Upload .aetx file:** Select the .aetx file by clicking **Browse** and navigating to the file location.
- **Upload signed Enterprise Hub app:** Select the Enterprise Hub app by clicking **Browse** and navigating to the app location.

## Exchange device policy

January 6, 2021

You can use the Exchange ActiveSync device policy to configure an email client on user devices to let them access their corporate email hosted on Exchange. Each platform requires a different set of values, which are described in detail in the following sections.

To create this policy, you need the host name or IP address of the Exchange Server. For information about ActiveSync settings, see the Microsoft article, [ActiveSync CSP](#).

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

Exchange	Exchange
1 Policy Info	This policy configures Microsoft Exchange ActiveSync so user devices can access corporate email, calendar, contacts, and other synced services hosted on Exchange.
2 Platforms <span>Clear All</span>	Exchange ActiveSync account name *
<input checked="" type="checkbox"/> iOS	Exchange ActiveSync host name *
<input type="checkbox"/> macOS	Use SSL <span>ON</span>
<input type="checkbox"/> Android HTC	Domain
<input type="checkbox"/> Android Enterprise	User
<input type="checkbox"/> Samsung SAFE	Email address
<input type="checkbox"/> Samsung Knox	Use OAuth <span>OFF</span> iOS 12.0+
<input type="checkbox"/> Windows Phone	Password
<input type="checkbox"/> Windows Desktop/Tablet	Email sync interval <span>3 days</span>
3 Assignment	Identity credential (keystore or PKI credential) <span>None</span>

- **Exchange ActiveSync account name:** Type the description of the email account that is displayed on user devices.
- **Exchange ActiveSync host name:** Type the address of the email server.
- **Use SSL:** Select whether to secure connections between user devices and the Exchange Server. The default is **On**.
- **Domain:** Enter the domain in which the Exchange Server resides. You can use the system macro `$user.domainname` in this field to automatically look up user domain names.
- **User:** Specify the user name for the Exchange user account. You can use the system macro `$user.username` in this field to automatically look up user names.
- **Email address:** Specify the full email address. You can use the system macro `$user.mail` in this field to automatically look up user email accounts.
- **Use OAuth:** If set to **On**, the connection uses OAuth for authentication. The default is **Off**. This option applies to iOS 12.0 and later.
- **Password:** Enter an optional password for the Exchange user account. This setting doesn't appear when **Use OAuth** is **On**.
- **Email sync interval:** In the list, choose how often email is synced with the Exchange Server. The default is **3 days**.
- **Identity credential (keystore or PKI):** In the list, click an optional identity credential if you have configured an identity provider for Endpoint Management. This field is only required when Exchange requires a client certificate authentication. The default is **None**.

- **Authorize moving email between accounts:** Select whether to allow users to:

- move email out of this account into another account
- forward email from a different account
- reply from a different account.

The default is **Off**.

- **Send email only from the email app:** Select whether to restrict users to the iOS mail app for sending email. The default is **Off**.

- **Prevent users from syncing recent addresses:** Select whether to prevent users from syncing recent addresses. The default is **Off**.

- **Enable S/MIME signing:** Select whether this account supports S/MIME signing. The default is **On**. When set to **On**, the following fields appear.

- **Signing identity credential:** Choose the signing credential to use.
- **User can override S/MIME signing:** If set to **On**, users can turn S/MIME signing on and off in the settings of their devices. The default is **Off**. This option applies to iOS 12.0 and later.
- **User can override S/MIME signing certificate UUID:** If set to **On**, users can select, in the settings of their devices, the signing credential to use. The default is **Off**. This option applies to iOS 12.0 and later.

- **Enable S/MIME encryption:** Select whether this account supports S/MIME encryption. The default is **Off**. When set to **On**, the following fields appear.

- **Encryption identity credential:** Choose the encryption credential to use.
- **Enable per message S/MIME switch:** When set to **On**, shows users an option to switch S/MIME encryption on or off for each message they compose. The default is **Off**.
- **User can override S/MIME encryption:** If set to **On**, users can, in the settings of their devices, select whether S/MIME is on by default. The default is **Off**. This option applies to iOS 12.0 and later.
- **User can override S/MIME encryption certificate UUID:** If set to **On**, users can turn S/MIME encryption identity and encryption on and off in the settings of their devices. The default is **Off**. This option applies to iOS 12.0 and later.

- **Policy settings**

- **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
  - \* **Select date:** Click the calendar to select the specific date for removal.
  - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

## Synced Exchange Services

The synced Exchange Services settings allow you to choose whether to sync the following features:

- Calendars
- Contacts
- Mail
- Notes
- Reminders

## macOS settings

Exchange	Exchange
1 Policy Info	This policy configures Microsoft Exchange ActiveSync so user devices can access corporate email, calendar, contacts, and other synced services hosted on Exchange.
2 Platforms <span>Clear All</span>	<p><b>Exchange ActiveSync account name *</b> <input type="text"/></p> <p><b>User *</b> <input type="text"/></p> <p><b>Email address *</b> <input type="text"/></p> <p><b>Use OAuth</b> <input type="checkbox"/> OFF macOS 10.14+</p> <p><b>Password</b> <input type="text"/> macOS 10.14+</p> <p><b>Internal Exchange host</b> <input type="text"/></p> <p><b>Internal server port</b> <input type="text"/></p> <p><b>Internal server path</b> <input type="text"/></p> <p><b>Use SSL for internal Exchange host</b> <input checked="" type="checkbox"/> ON</p> <p><b>External Exchange host</b> <input type="text"/></p> <p><b>External server port</b> <input type="text"/></p>
<input type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input type="checkbox"/> Android HTC <input type="checkbox"/> Android Enterprise <input type="checkbox"/> Samsung SAFE <input type="checkbox"/> Samsung Knox <input type="checkbox"/> Windows Phone <input type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	

- **Exchange ActiveSync account name:** Type the description of the email account that is displayed on user devices.
- **User:** Specify the user name for the Exchange user account. You can use the system macro `$user.username` in this field to automatically look up user names.
- **Email address:** Specify the full email address. You can use the system macro `$user.mail` in this field to automatically look up user email accounts.
- **Use OAuth:** If set to **On**, the connection uses OAuth for authentication. The default is **Off**. This option applies to macOS 10.14 and later.
- **OAuth sign-in URL:** Specifies the URL to load into a webview to authenticate using OAuth when you don't use the AutoDiscovery service. This field appears when **Use OAuth** is set to **On**.
- **Password:** Enter an optional password for the Exchange user account. This setting doesn't appear when **Use OAuth** is **On**.

- **Internal Exchange host:** If you want your internal and external Exchange host names to be different, type an optional internal Exchange host name.
- **Internal server port:** If you want your internal and external Exchange server ports to be different, type an optional internal Exchange server port number.
- **Internal server path:** If you want your internal and external Exchange server paths to be different, type an optional internal Exchange server path.
- **Use SSL for internal Exchange host:** Select whether to secure connections between user devices and the internal Exchange host. The default is **On**.
- **External Exchange host:** If you want your internal and external Exchange host names to be different, type an optional external Exchange host name.
- **External server port:** If you want your internal and external Exchange server ports to be different, type an optional external Exchange server port number.
- **External server path:** If you want your internal and external Exchange server paths to be different, type an optional external Exchange server path.
- **Use SSL for external Exchange host:** Select whether to secure connections between user devices and the internal Exchange host. The default is **On**.
- **Allow Mail Drop:** Select whether to allow users to share files wirelessly between two Macs, without having to connect to an existing network. The default is **Off**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

## Android Enterprise

Exchange	Exchange
1 Policy Info	This policy configures Microsoft Exchange ActiveSync so user devices can access corporate email, calendar, contacts, and other synced services hosted on Exchange.
2 Platforms <span>Clear All</span>	<p><b>Server name or IP address *</b> <input type="text"/></p> <p><b>Domain</b> <input type="text"/></p> <p><b>User ID *</b> <input type="text"/></p> <p><b>Password</b> <input type="text"/></p> <p><b>Email address</b> <input type="text"/></p> <p><b>Identity credential (keystore or PKI)</b> <input type="text" value="None"/></p> <p>► <b>Deployment Rules</b></p>
<input type="checkbox"/> iOS	
<input type="checkbox"/> macOS	
<input type="checkbox"/> Android HTC	
<input checked="" type="checkbox"/> Android Enterprise	
<input type="checkbox"/> Samsung SAFE	
<input type="checkbox"/> Samsung Knox	
<input type="checkbox"/> Windows Phone	
<input type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	

- **Server name or IP address:** Type the Exchange Server host name or IP address.
- **Domain:** Type the domain in which the Exchange Server resides. You can use the system macro `$user.domainname` in this field to automatically look up user domain names.
- **User ID:** Specify the user name for the Exchange user account. You can use the system macro `$user.username` in this field to automatically look up user names.
- **Password:** Type an optional password for the Exchange user account.
- **Email address:** Specify the full email address. You can use the system macro `$user.mail` in this field to automatically look up user email accounts.
- **Identity credential (keystore or PKI):** In the list, click an optional identity credential if you have configured an identity provider for Endpoint Management. This field is only required when Exchange requires a client certificate authentication. The default is **None**.

## Samsung SAFE and Samsung Knox settings

Exchange	Exchange
1 Policy Info	This policy configures Microsoft Exchange ActiveSync so user devices can access corporate email, calendar, contacts, and other synced services hosted on Exchange.
2 Platforms <span>Clear All</span>	<p>Server name or IP address *</p> <input type="text"/>
<input type="checkbox"/> iOS	Domain
<input type="checkbox"/> macOS	User ID *
<input type="checkbox"/> Android HTC	Password
<input type="checkbox"/> Android Enterprise	Email address *
<input checked="" type="checkbox"/> Samsung SAFE	Identity credential (keystore or PKI)
<input checked="" type="checkbox"/> Samsung Knox	Use SSL connection <input checked="" type="checkbox"/>
<input type="checkbox"/> Windows Phone	Sync contacts <input checked="" type="checkbox"/>
<input type="checkbox"/> Windows Desktop/Tablet	Sync calendar <input checked="" type="checkbox"/>
3 Assignment	Default account <input checked="" type="checkbox"/>

- **Server name or IP address:** Type the Exchange Server host name or IP address.
- **Domain:** Type the domain in which the Exchange Server resides. You can use the system macro `$user.domainname` in this field to automatically look up user domain names.
- **User ID:** Specify the user name for the Exchange user account. You can use the system macro `$user.username` in this field to automatically look up user names.
- **Password:** Type an optional password for the Exchange user account.
- **Email address:** Specify the full email address. You can use the system macro `$user.mail` in this field to automatically look up user email accounts.
- **Identity credential (keystore or PKI):** In the list, click an optional identity credential if you have configured an identity provider for Endpoint Management. This field is only required when Exchange requires a client certificate authentication.
- **Use SSL connection:** Select whether to secure connections between user devices and the Exchange Server. The default is **On**.
- **Sync contacts:** Select whether to enable synchronization for user contacts between devices and the Exchange Server. The default is **On**.
- **Sync calendar:** Select whether to enable synchronization for user calendars between devices and the Exchange Server. The default is **On**.
- **Default account:** Select whether to make user Exchange accounts the default for sending email from their devices. The default is **On**.



## Windows Phone and Windows Desktop/Tablet settings

Exchange	Exchange
1 Policy Info	This policy configures Microsoft Exchange ActiveSync so user devices can access corporate email, calendar, contacts, and other synced services hosted on Exchange.
2 Platforms <span>Clear All</span>	<p><b>Account name or display name *</b> <input type="text"/></p> <p><b>Server name or IP address *</b> <input type="text"/></p> <p><b>Domain</b> <input type="text"/></p> <p><b>User ID or user name *</b> <input type="text"/></p> <p><b>Email address *</b> <input type="text"/></p> <p><b>Use SSL connection</b> <input type="checkbox"/> OFF</p> <p><b>Sync items</b></p> <p>Past days to sync <input type="text" value="All content"/></p> <p><b>Sync scheduling</b></p> <p>Frequency <input type="text" value="When item arrives"/></p> <p>Logging level <input type="text" value="Disabled"/></p>
<input type="checkbox"/> iOS	
<input type="checkbox"/> macOS	
<input type="checkbox"/> Android HTC	
<input type="checkbox"/> Android Enterprise	
<input type="checkbox"/> Samsung SAFE	
<input type="checkbox"/> Samsung Knox	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	

### Note:

This policy does not allow you to set the user password. Users must set that parameter from their devices after you push the policy.

- **Account name or display name:** Type the Exchange ActiveSync account name.
- **Server name or IP address:** Type the Exchange Server host name or IP address.
- **Domain:** Enter the domain in which the Exchange Server resides. You can use the system macro `$user.domainname` in this field to automatically look up user domain names.
- **User ID or user name:** Specify the user name for the Exchange user account. You can use the system macro `$user.username` in this field to automatically look up user names.
- **Email address:** Specify the full email address. You can use the system macro `$user.mail` in this field to automatically look up user email accounts.
- **Use SSL connection:** Select whether to secure connections between user devices and the Exchange Server. The default is **Off**.
- **Past days to sync:** In the list, click how many days into the past to sync all content on the device with the Exchange Server. The default is **All content**.
- **Frequency:** In the list, click the schedule to use when syncing data that is sent to the device from the Exchange Server. The default is **When item arrives**.
- **Logging level:** In the list, click **Disabled**, **Basic**, or **Advanced** to specify the level of detail when logging Exchange activity. The **default is Disabled**.

## Files device policy

April 19, 2021

You can add and deploy files for users to access on their Android and Android Enterprise devices. You specify the directory where you want to store the file on the device. For example, you want users to receive a company document or .pdf file. Deploy the file to devices and let users know where the file is located.

Android devices don't support running scripts natively. Users need third-party software to run scripts.

You can add the following file types with this policy:

- Text-based files (.xml, .html, .py, and so on)
- Other files, such as documents, pictures, spreadsheets, or presentations

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Android Enterprise settings

#### Files Policy

This policy lets you upload files and executable scripts to devices.

**File to be imported \***

**File type**  File  Script

**Replace macro expressions**  OFF

**Destination folder**

**Destination file name**

**If file exists**

**▶ Deployment Rules**

- **File to be imported:** To select the file to import, click **Browse** and navigate to the file location.
- **File type:** Select either **File** or **Script**.
- **Execute immediately:** When you select **Script**, the **Execute immediately** option appears. Nothing happens when you enable this setting. Users must run the script manually.
- **Replace macro expressions:** Select whether to replace macro token names in a script with a device or user property. For macro syntax, see [Macros](#). The default is **Off**.
- **Destination folder:** In the list, select the location where you want to store the uploaded file, or select **Add new** to specify a file location. Select the `%Flash Storage%` or the `%XenMobile Storage%` macro to indicate where to store the uploaded file. The macro expands to the applicable location on each device.
  - `%XenMobile Storage%` expands to `Android/data/com.zenprise/` in the internal storage directory.
  - For Android 9.0 and earlier, `%Flash Storage%` saves the file to the external storage directory.
  - For Android 10.0 and later, `%Flash Storage%` saves the file to the **Downloads** folder of the internal storage directory.
  - For Android 11.0 and later, `%XenMobile Storage%` no longer applies because of restrictions imposed by Google on access to the target location.
- **Destination file name:** Optional. If you must change a file name before deploying it to a device, type the file name.
- **If file exists:** In the list, select whether to copy an existing file. The default is **Copy file only if different**.

## Android settings

- **File to be imported:** To select the file to import, click **Browse** and navigate to the file location.
- **File type:** Select either **File** or **Script**.
- **Execute immediately:** When you select **Script**, the **Execute immediately** option appears. Nothing happens when you enable this setting. Users must run the script manually.
- **Replace macro expressions:** Select whether to replace macro token names in a script with a device or user property. For macro syntax, see [Macros](#). The default is **Off**.
- **Destination folder:** In the list, select the location where you want to store the uploaded file, or select **Add new** to specify a file location. Select the `%Flash Storage%` or the `%XenMobile Storage%` macro to indicate where to store the uploaded file. The macro expands to the applicable location on each device.
  - `%XenMobile Storage%` expands to `Android/data/com.zenprise/` in the internal storage directory.
  - For Android 9.0 and earlier, `%Flash Storage%` saves the file to the external storage directory.
  - For Android 10.0 and later, `%Flash Storage%` saves the file to the **Downloads** folder of

the internal storage directory.

- For Android 11.0 and later, %XenMobile Storage%\ no longer applies because of restrictions imposed by Google on access to the target location.
- **Destination file name:** Optional. If you must change a file name before deploying it to a device, type the file name.
- **If file exists:** In the list, select whether to copy an existing file. The default is **Copy file only if different**.

## FileVault device policy

July 12, 2021

The macOS FileVault full-disk encryption (FileVault 2) feature protects the system volume by encrypting its contents. A user logs in to a FileVault-enabled macOS device with their account password each time that the device starts. If the user loses their password, a recovery key enables them to unlock the disk and reset their password.

This device policy enables FileVault user setup screens and configures settings such as recovery keys. For more information about FileVault, see the Apple support site.

To add the FileVault policy, go to **Configure > Device Policies**.

### macOS settings

The screenshot displays the configuration page for a FileVault 2 Policy. On the left, a sidebar lists the policy name and navigation options: '1 Policy Info', '2 Platforms' (with a 'Clear All' link), '3 Assignment', and 'macOS' (which is selected and highlighted in teal). The main content area is titled 'FileVault 2 Policy' and includes a descriptive sentence: 'This policy lets you enable FileVault device encryption on enrolled macOS devices.' Below this, there are several settings:

- Enable FileVault 2:** A toggle switch is turned ON.
- FileVault 2 Settings:**
  - Prompt for FileVault setup during logout:** A toggle switch is turned OFF.
  - Maximum times to skip FileVault setup:** A dropdown menu is set to 0.
  - Recovery key type:** A dropdown menu is set to 'Personal & institutional recovery key'.
  - Show personal recovery key:** A toggle switch is turned OFF.
  - Institutional Recovery Key certificate \*:** A dropdown menu is set to 'None'.
  - Escrow Personal Recovery Key:** A toggle switch is turned OFF.
- Deployment Rules:** A link with a right-pointing arrow is located at the bottom of the settings list.

- **Enable FileVault:** If **On**, prompts the user to enable FileVault during the next N logouts, as specified by the option **Maximum times to skip FileVault setup**. If **Off**, users don't receive a prompt

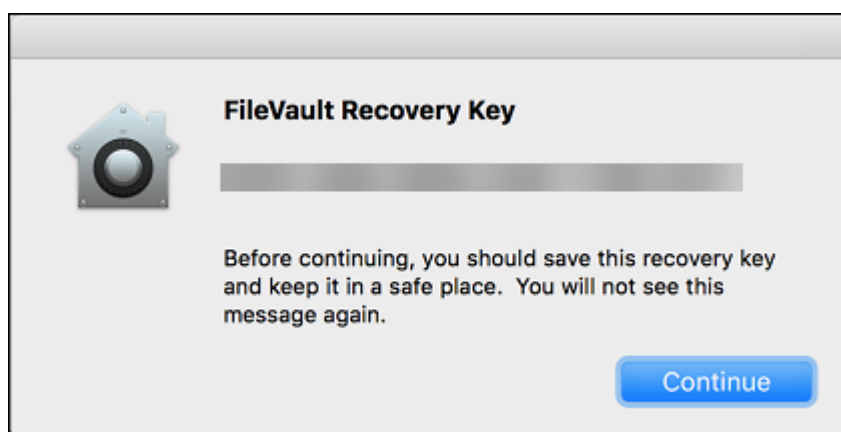
to enable FileVault, but they can still enable FileVault on their own.

- **Prompt for FileVault setup during logout:** If **On**, users see a prompt asking them to enable FileVault when they log out.
- **Maximum times to skip FileVault setup:** The maximum number of times that the user can skip FileVault setup. When the user reaches the maximum, the user must set up FileVault to log in. If **0**, the user must enable FileVault during the first login attempt. Default is **0**.
- **Recovery key type:** A user who forgets their password can type a recovery key to unlock the disk and reset their password. Recovery key options:
  - **Personal recovery key:** A personal recovery key is unique to a user. During FileVault setup, a user chooses whether to create a recovery key or to allow their iCloud account to unlock their disk. To show the recovery key to the user after FileVault setup completes, enable **Show personal recovery key**. Showing the key enables the user to record the key for future use. To allow users to look up their key if they lose it, enable **Escrow personal recovery key**.

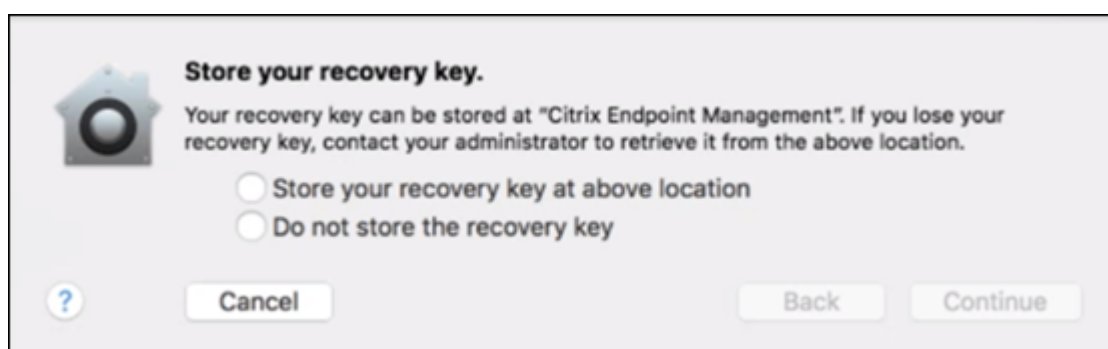
You can rotate personal recovery keys through security actions. For more information on rotating personal recovery keys, see [Security actions](#).

For information about recovery key management, see the Apple support site.

- **Institutional recovery key:** You can create an institutional (or main) recovery key and FileVault certificate, which you then use to unlock user devices. For information, see the Apple support site. Use Endpoint Management to deploy the FileVault certificate to devices. For information, see [Certificates and authentication](#).
- **Personal & institutional recovery key:** By enabling both types of recovery keys, you must unlock a user device only if the user loses their personal recovery key.
- **Institutional recovery key certificate:** If you select **Institutional recovery key** or **Personal & Institutional recovery key** as the **Recovery key type**, select the recovery key certificate for that key.
- **Show personal recovery key:** If **On**, the user device shows the personal recovery key to the user after setting up FileVault. Defaults to **Off**.

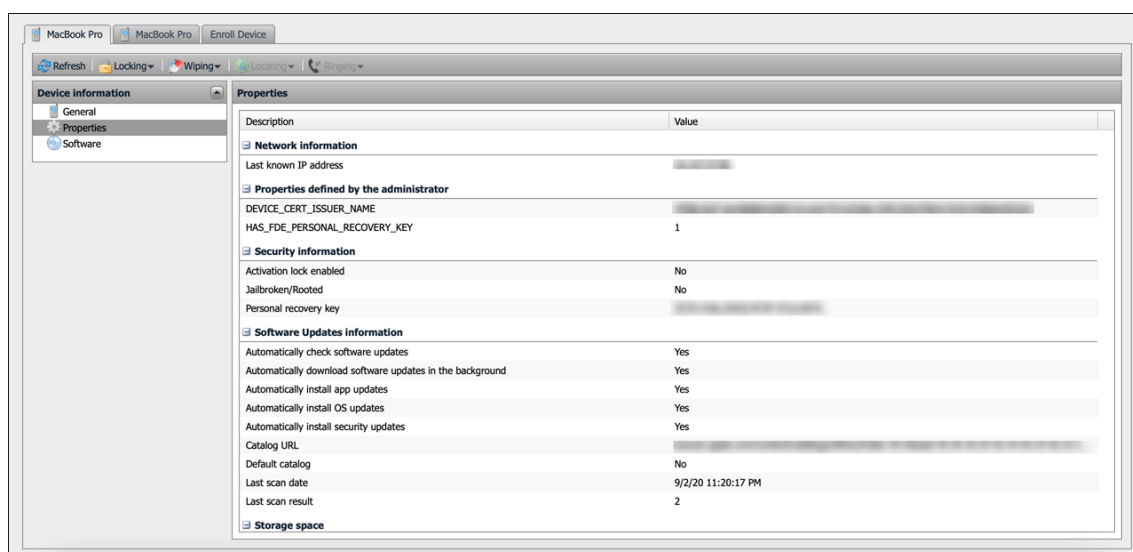


- **Escrow personal recovery key:** When enabled, users can store a copy of the personal recovery key for each device with Endpoint Management.



To access the key from Endpoint Management, go to **Manage > Devices**, select the macOS device and click **Edit**. Then, go to **Device details > General** and locate the **Personal recovery Key**.

To allow users to view their recovery key from the Self-Help Portal, enable **Escrow personal recovery key** and **Display personal recovery key to user**. The key appears in the Self-Help Portal on the **Properties** page under **Security information**. For more information about the Self-Help Portal, see [Self-Help Portal](#).



You can enable the **Escrow personal recovery key** setting even if you don't enable the **Enable FileVault** setting. If you disable the **Enable FileVault** setting, users can still enable FileVault on their own. In this situation, enable **Escrow personal recovery key** to allow users to store a copy of their key with Endpoint Management.

If a user enables FileVault before enrolling the device in Endpoint Management, Endpoint Management doesn't store their recovery key. The device shows up as FileVault-enabled in the console.

## Firewall device policy

September 8, 2021

This policy lets you configure firewall settings for Samsung, macOS, and Windows devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Samsung SAFE settings

- **Allow/Deny host:** For each host to which you want to allow or deny access, click **Add** and configure the following:
  - **Host name/IP range:** The host name or IP address range of the site you want to affect.
  - **Port/port range:** The port or port range.
  - **Allow/deny rule filter:** Click **Allow list** to allow access or click **Block list** to deny access to the site.

- **Reroute configuration:** For each proxy you want to configure, click **Add** and configure the following:
  - **Host name/IP range:** The host name or IP address range for the proxy reroute.
  - **Port/port range:** The port or port range for the proxy reroute.
  - **Proxy IP:** The proxy IP address for the proxy reroute.
  - **Proxy port:** The proxy port for the proxy reroute.
- **Proxy Configuration**
  - **Proxy IP:** The IP address of the proxy server.
  - **Port:** The proxy server port.

## macOS settings

Requires macOS 10.12 and later.

The screenshot shows the 'Firewall Policy' configuration page in the Citrix Endpoint Management console. The left sidebar has 'Firewall Policy' selected, with sub-sections for '1 Policy info', '2 Platforms' (where 'macOS' is checked), and '3 Assignment'. The main content area is titled 'Firewall Policy' and includes the following settings:

- Enable Firewall:** ON (toggle)
- Block all incoming connections:** OFF (toggle)
- Enable stealth mode:** ON (toggle)

Below these are 'App specific incoming connection settings' with a table:

Application *	Allowed	Add
test	True	
test2	True	

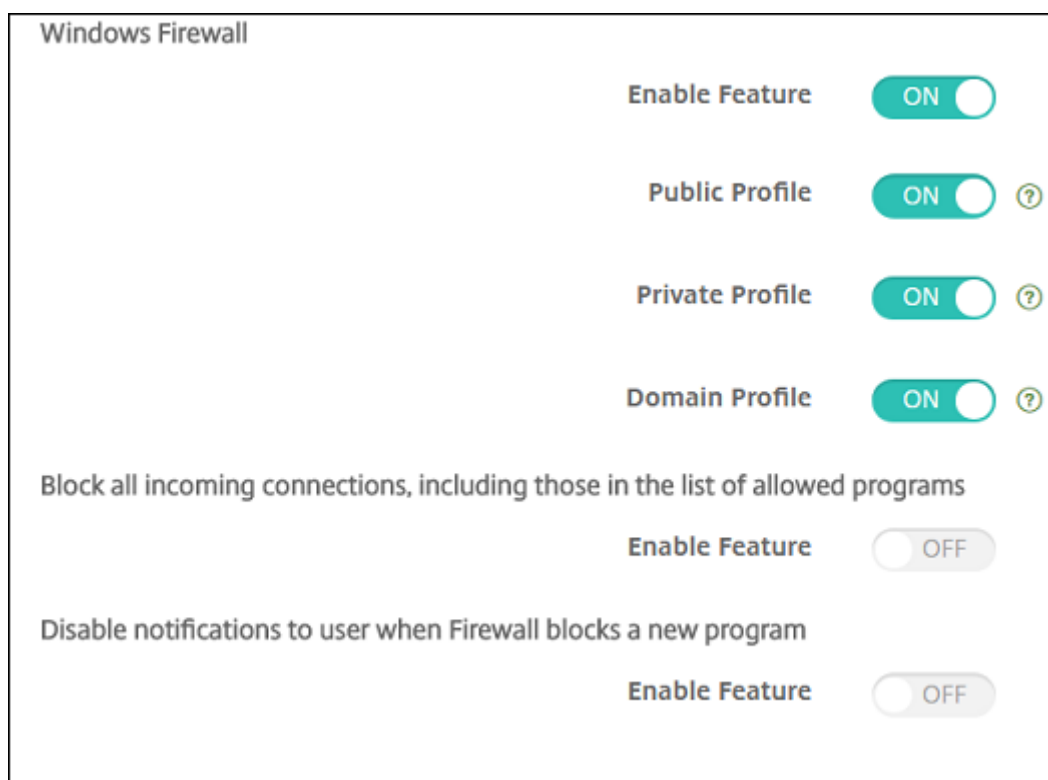
At the bottom, there are 'Policy Settings' including 'Remove policy' (radio buttons for 'Select date' and 'Duration until removal (in hours)'), a date picker, and 'Allow user to remove policy' (dropdown menu set to 'Always').

- **Enable Firewall.** To enable the firewall, set this option to **On**.
- **Block all incoming connections.** When this option is set to **On**, it blocks all incoming connections except the connections required for basic services.
- **Enable stealth mode.** In stealth mode, the device doesn't respond to or acknowledge attempts to access it from the network by test applications using ICMP, such as Ping. To enable stealth mode, set this option to **On**.
- **App specific incoming connection settings.** To allow specific apps to receive connections, add the apps and set **Allowed** to **True**.

## Windows Desktop and Tablet settings

Requires Windows Desktop and Tablet devices running Windows 10 (version 1709 or later) or Windows 11.





- **Enable Feature:** Controls incoming and outgoing traffic on computers to which this policy is deployed. Default is **On**.
- **Public Profile:** Controls Windows Firewall while computers are connected to untrusted networks at public places, such as at an airport or coffee shop. Default is **On**.
- **Private Profile:** Controls Windows Firewall while computers are connected to trusted networks, such as their home network. Default is **On**.
- **Domain Profile:** Controls Windows Firewall while the computers are connected to the domain networks, such as at their workplace. Default is **On**.
- **Block all incoming connections, including those in the list of allowed programs:** Default is **Off**.
- **Disable notifications to user when Firewall blocks a new program:** Default is **Off**.

## Font device policy

April 7, 2020

You can add a device policy in Endpoint Management to add more fonts to iOS and macOS devices. Fonts must be TrueType (.ttf) or OpenType (.oft) fonts. Font collections (.ttc or .otc) are not supported.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device](#)

policies.

## iOS settings

- **User-visible name:** Type the name that users see in their font lists.
- **Font file:** To select the font file to add to user devices, click **Browse** and then navigate to the file location.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

## macOS settings

- **User-visible name:** Type the name that users see in their font lists.
- **Font file:** To select the font file to add to user devices, click **Browse** and then navigate to the file location.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

## Home screen layout device policy

March 10, 2021

The Home screen layout device policy lets you specify the layout of apps and folders for the iOS Home screen of supervised iOS devices.

**Important:**

Deploying multiple Home Screen Layout policies to a device results in an iOS error on the device. This limitation applies whether you define the home screen through this Endpoint Management policy or through the Apple Configurator.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

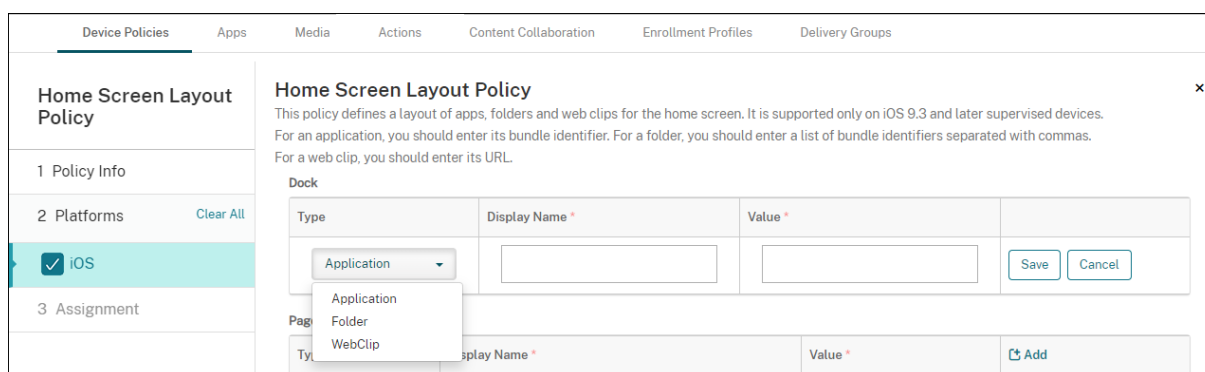
**iOS settings**

The screenshot shows the configuration page for a 'Home Screen Layout Policy'. The left sidebar has three sections: '1 Policy Info', '2 Platforms' (with a 'Clear All' link and 'iOS' selected), and '3 Assignment'. The main content area is titled 'Home Screen Layout Policy' and includes a description: 'This policy defines a layout of apps, folders and web clips for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application, you should enter its bundle identifier. For a folder, you should enter a list of bundle identifiers separated with commas. For a web clip, you should enter its URL.' Below this are sections for 'Dock', 'Page 1', 'Page 2', 'Page 3', 'Page 4', and 'Page 5'. Each section contains a table with columns for 'Type', 'Display Name', and 'Value', and an 'Add' button. At the bottom right, there are 'Back', 'Next >', and a refresh icon.

- For each of the screen areas you want to configure (such as **Dock** or **Page 1**), click **Add**.
- **Type:** Choose **Application**, **Folder**, or **Web Clip**.

The **Restricted app usage > Allow only some apps** setting in the [Restrictions device policy](#) can prevent web clips from appearing properly on the home screen. For web clips to appear properly, do either of the following:

- Set **Restricted app usage** to **Allow all apps** or **Do not allow some apps**.
- With **Restricted app usage** set to **Allow only some apps**, add an app with the bundle ID `com.apple.webapp` to allow web clips.



- **Display Name:** The name to appear on the home screen for the app or folder.
- **Value:** For apps, type the bundle identifier. For folders, type a list of bundle identifiers, separated by commas. For web clips, type the bundle ID `com.apple.webClip.managed` and configure the URL of the web clip in the web clip policy. If more than one Web Clip value exists with the same URL, the behavior is undefined on iOS 11.3 and later devices.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on iOS 9.3 and later.

## Import Device Configuration device policy

April 6, 2020

The Import Device Configuration device policy lets you deploy custom configurations to Citrix Ready workspace hub devices. The general steps are:

1. Manually configure your first Citrix Ready workspace hub device.
2. Download the configuration file from the device.
3. Configure the Import Device Configuration policy and deploy the policy to push the configuration to all other devices.

For more information, see [Workspace hub device management](#).

## Workspace Hub settings

- **URL:** The URL for the configuration file hosted on a file sharing web server.

## Import iOS & macOS Profile device policy

September 23, 2020

You can import device configuration XML files for iOS and macOS devices into Endpoint Management. The file contains device security policies and restrictions that you prepare with the Apple Configurator 2 or Profile Creator. The configuration XML file can contain macros. For more information, see [Macros](#).

### Use cases

Import the following configurations created outside of Endpoint Management for macOS devices using Profile Creator:

- **System Policy Control:** The policy identifies apps signed by the certified Apple developers and lets users download verified apps from the Mac App Store.

When configuring the policy:

- Select **Enable Gatekeeper** to ensure that users run only verified and trusted software.
- Select **Allow Identified Developers** to ensure that users install apps only signed by certified Apple developers.

- **Privacy Preferences Policy Control:** The policy lets you grant or restrict cross-application access to certain files or features, such as location services, camera, and screen capture.

Configure the settings you plan to deploy. For more information, see [Privacy Preferences Policy Control payload settings](#).

- **Kernel Extensions Policy:** The policy lets the users install app extensions that extend the native capabilities of the operating system. Kernel extensions run at the kernel level.

Configure the settings you plan to deploy. For more information, see [Kernel Extension Policy payload settings](#).

- **Ethernet Settings Policy:** The policy lets you manage the Ethernet network connection.

Configure the settings you plan to deploy. For more information, see [Ethernet settings](#).

Use either the Apple Configurator 2 or Profile Creator to configure the following policies for macOS and iOS devices:

- **Wi-Fi Policy:** The policy lets you manage how users connect their devices to a Wi-Fi network.

When configuring the policy:

- Add the target SSID to the top of the priority list.
- Choose the connection mode to use when the user joins a network. If you select **System**, the device uses the system credentials to authenticate the user. If you select **Login window**, the device uses the same credentials entered at the login window to authenticate the user.

For more information, see [Wi-Fi settings](#).

- **Restrictions Policy:** The policy allows or restricts the use of certain features on user devices.

Configure the settings you plan to deploy. For more information, see [Restrictions overview](#).

- **VPN Policy:** The policy provides a device-level encrypted connection to private networks.

Configure the settings you plan to deploy. For more information, see [VPN overview](#).

## Create a configuration profile using the Apple Configurator 2

1. Install the Apple Configurator 2 from Apple App Store.
2. Start the Apple Configurator 2 and go to **File > New Profile**. A new configuration window appears.
3. In the **General** settings pane, type a name and an identifier for your profile, then add any additional payload options.
4. On the left pane, select a payload, click **Configure**, and enter the settings. Don't sign your profile, as signed profiles are not supported.

To add multiple payloads within a single profile, select a payload and click the **Add Payload** button in the upper-right corner.

5. Go to **File > Save**, choose a name and location to save the XML file, and click **Save**.

## Create a configuration profile using Profile Creator

1. Install the Profile Creator from [GitHub](#).
2. Start the Profile Creator and go to **File > New**. A new configuration window appears.
3. In the **General** settings pane, type a name and description for your profile, then add any additional payload options.
  - Recommendation: Select **Prevent users from removing this profile**.
  - Set **Payload Scope** to **System** or **User**.

- On the left pane, choose the policy, configure the settings, and click **Add** in the upper-right corner.

To configure multiple policies within a single profile, select a policy and click the **Add** button.

- Go to **File > Export**, choose a name and location to save the XML file, and click **Save**.

To import a configuration file for the iOS and macOS Profile device policy in the Endpoint Management console, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS and macOS settings

- **iOS configuration profile** or **macOS configuration profile**: To select the configuration file to import, click **Browse** and then navigate to the file location.

## Keyguard Management device policy

June 23, 2021

Android keyguard manages the device and work challenge lock screens. This policy lets you manage features for Android Enterprise work profile keyguard and advanced device keyguard. You can control:

- Keyguard management on work profile devices. You can specify the features available to users before they unlock the device keyguard and the work challenge keyguard. For example, by default users can use fingerprint unlock and view unredacted notifications on the lock screen.
- Keyguard management on fully managed and dedicated devices. You can specify the features available, such as trust agents and secure camera, before they unlock the keyguard screen. Or, you can choose to disable all keyguard features.
- Keyguard management on fully managed devices with work profiles. These devices were formerly known as COPE (corporate owned personally enabled) devices. You can use one Keyguard Management policy to apply separate settings to the device and the work profile.

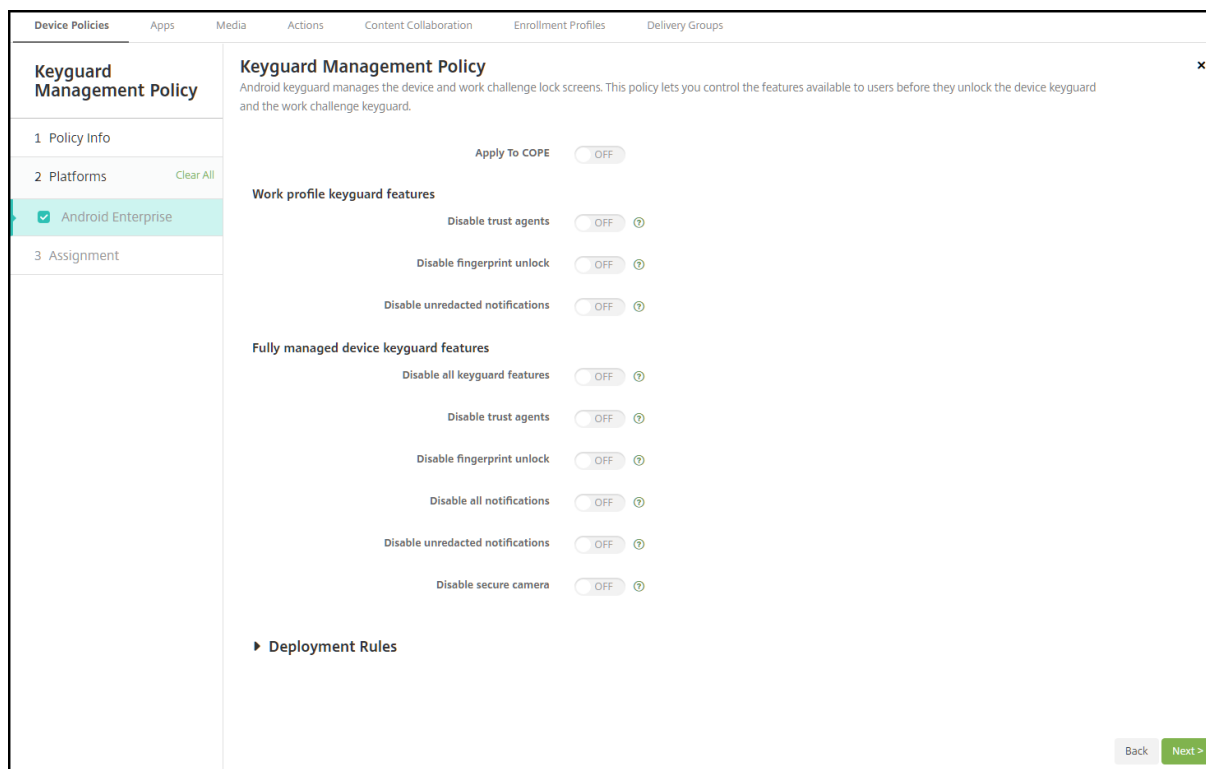
To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

Watch this video to learn more:





## Android Enterprise settings



- **Apply to COPE:** Allows you to configure Keyguard Management device policy settings for fully managed devices with work profiles.

When this setting is **On**, you can apply separate settings to the device and to the work profile on fully managed devices with work profiles.

When this setting is **Off**, you can apply settings to work profile devices or fully managed devices. Settings you configure for work profiles only apply to work profile devices. Settings you configure for fully managed devices apply only to fully managed devices.

Default is **Off**.

- **Work profile keyguard features:** Controls whether the following features are available before a user unlocks the work profile keyguard (lock screen).
  - **Disable trust agents:** If **Off**, trust agents can operate on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable all trust agents on the work profile. Default is **Off**.
  - **Disable biometric authentication:** If **Off**, biometric authentication is available on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable biometric authentication on the work profile. This setting disables fingerprint unlock, face authentication, and iris authentication. Default is **Off**. For Android 9.0 and later.
  - **Disable fingerprint unlock:** If **Off**, fingerprint unlock is available on secure keyguard

screens when a challenge is set on the work profile. Set to **On** to disable fingerprint unlock on the work profile. Default is **Off**.

- **Disable face authentication:** If **Off**, face authentication is available on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable face authentication on the work profile. Default is **Off**. For Android 9.0 and later.
  - **Disable iris authentication:** If **Off**, iris authentication is available on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable iris authentication on the work profile. Default is **Off**. For Android 9.0 and later.
  - **Disable unredacted notifications:** If **Off**, both redacted and unredacted notifications appear on secure keyguard screens. Set to **On** to disable unredacted notifications and only show redacted notifications. Default is **Off**.
- **Fully managed device keyguard features:** Controls whether the following features are available before a user unlocks the device keyguard (lock screen). These features apply to fully managed or dedicated devices.
    - **Disable all keyguard features:** If **Off**, all current and future keyguard customizations are available on the secure keyguard screens. Set to **On** to disable all keyguard customizations. Default is **Off**.
    - **Disable trust agents:** If **Off**, trust agents can operate on secure keyguard screens. Set to **On** to disable trust agents. Default is **Off**.
    - **Disable biometric authentication:** If **Off**, biometric authentication is available on secure keyguard screens when a challenge is set on the device. Set to **On** to disable biometric authentication on the device. The biometric authentication features disabled are fingerprint unlock, face authentication, and iris authentication. Default is **Off**. For Android 9.0 and later.
    - **Disable fingerprint unlock:** If **Off**, fingerprint unlock is available on secure keyguard screens when a challenge is set on the device. Set to **On** to disable fingerprint unlock on the device. Default is **Off**.
    - **Disable face authentication:** If **Off**, face authentication is available on secure keyguard screens when a challenge is set on the device. Set to **On** to disable face authentication on the device. Default is **Off**. For Android 9.0 and later.
    - **Disable iris authentication:** If **Off**, iris authentication is available on secure keyguard screens when a challenge is set on the device. Set to **On** to disable iris authentication on the device. Default is **Off**. For Android 9.0 and later.
    - **Disable all notifications:** If **Off**, all notifications appear on secure keyguard screens. Set to **On** to show all notifications. Default is **Off**.
    - **Disable unredacted notifications:** If **Off**, both redacted and unredacted notifications appear on secure keyguard screens. Set to **On** to disable unredacted notifications and only show redacted notifications. Default is **Off**.
    - **Disable secure camera:** If **Off**, secure camera is available on secure keyguard screens. Set

to **On** to disable the secure camera. Default is **Off**.

### Android for Workspace (Preview) settings

- **Disable trust agents:** If **Off**, trust agents can operate on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable all trust agents on the work profile. Default is **Off**.
- **Disable biometric authentication:** If **Off**, biometric authentication is available on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable biometric authentication on the work profile. This setting disables fingerprint unlock, face authentication, and iris authentication. Default is **Off**. For Android 9.0 and later.
- **Disable fingerprint unlock:** If **Off**, fingerprint unlock is available on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable fingerprint unlock on the work profile. Default is **Off**.
- **Disable face authentication:** If **Off**, face authentication is available on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable face authentication on the work profile. Default is **Off**. For Android 9.0 and later.
- **Disable iris authentication:** If **Off**, iris authentication is available on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable iris authentication on the work profile. Default is **Off**. For Android 9.0 and later.
- **Disable unredacted notifications:** If **Off**, both redacted and unredacted notifications appear on secure keyguard screens. Set to **On** to disable unredacted notifications and only show redacted notifications. Default is **Off**.

## Kiosk device policy

September 8, 2021

The Kiosk policy lets you restrict devices to Kiosk mode by limiting the apps that can run. Citrix Endpoint Management does not control which part of the device locks in Kiosk mode. The device manages the kiosk mode settings after you deploy the policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

To set up iPads to run in Kiosk mode, use the App lock device policy. For information about setting up iPads as kiosks, see [Configure an iPad as a kiosk](#). You can also configure an iPad to open only a single website. For information, see the [Webclip policy](#).

## Samsung SAFE settings

You can specify that only a specific app or apps can be used. This policy is useful for corporate devices that are designed to run only a specific type or class of apps. This policy also lets you choose custom images for the device home screen and lock screen wallpapers for when the device is in Kiosk mode.

### To put a Samsung SAFE device into Kiosk mode

1. Enable the Samsung SAFE API key on the mobile device, as described in [Samsung MDM license key device policies](#). This step lets you enable policies on Samsung SAFE devices.
2. Enable Firebase Cloud Messaging for Android devices, as described in [Firebase Cloud Messaging](#). This step enables Android devices connect back to Endpoint Management.
3. Add a Kiosk device policy, as described in the next section.
4. Assign those three device policies to the appropriate delivery groups. Consider whether you want to include other policies, such as App inventory, in those delivery groups.

To remove the devices from Kiosk mode, create a Kiosk device policy that has **Kiosk mode** set to **Disable**. Update the delivery groups to remove the Kiosk policy that enabled Kiosk mode and to add the Kiosk policy that disables Kiosk mode.

### To add a Kiosk device policy for Samsung SAFE

All apps that you specify for Kiosk mode must already be installed on the user devices.

Some options apply only to the Samsung Mobile Device Management (MDM) API 4.0 and later.

- **Kiosk mode:** Click **Enable** or **Disable**. The default is **Enable**. When you click **Disable**, all the following options disappear.
- **Launcher package:** Citrix recommends that you leave this field blank unless you have developed an in-house launcher to enable users to open the Kiosk app or apps. If you use an in-house launcher, enter the full name of the launcher application package.
- **Emergency phone number:** Enter an optional phone number. Anyone can use this number to contact your company to find a lost device. Applies only to MDM 4.0 and later.
- **Allow navigation bar:** Select whether to let users see and use the navigation bar while in Kiosk mode. Applies only to MDM 4.0 and later. The default is **On**.
- **Allow multi-window mode:** Select whether to let users use multiple windows while in Kiosk mode. Applies only to MDM 4.0 and later. The default is **On**.
- **Allow status bar:** Select whether to let users see the status bar while in Kiosk mode. Applies only to MDM 4.0 and later. The default is **On**.
- **Allow system bar:** Select whether to let users see the system bar while in Kiosk mode. The default is **On**.

- **Allow task manager:** Select whether to let users see and use the task manager while in Kiosk mode. The default is **On**.
- **Change Common SAFE passcode:** This setting helps protect against inadvertent changes to the Common SAFE passcode field. When this setting is **Off**, you can't change the Common SAFE passcode field. The default is **Off**.
- **Common SAFE passcode:** If you set a general passcode policy for all Samsung SAFE devices, enter that optional passcode in this field.
- **Wallpapers**
  - **Define a home wallpaper:** Select whether to use a custom image for the home screen while in Kiosk mode. The default is **Off**.
    - \* **Home image:** When you enable **Define a home wallpaper**, select the image file by clicking **Browse** and navigating to the file location.
  - **Define a lock wallpaper:** Select whether to use a custom image for the lock screen while in Kiosk mode. The default is **Off**. Applies only to MDM 4.0 and later.
    - \* **Lock image:** When you enable **Define a lock wallpaper**, select the image file by clicking **Browse** and navigating to the file location.
- **Apps:** For each app that you want to add to Kiosk mode, click **Add** and then do the following:
  - **New app to add:** Enter the full name of the app to add. For example, com.android.calendar lets users use the Android calendar app.
  - Click **Save** to add the app or click **Cancel** to cancel adding the app.

## Windows Desktop and Tablet settings

For Windows Desktop and Tablet devices, the Kiosk policy applies only to local users and users enrolled in Azure AD.

A single app or multiple apps can run in Kiosk mode on Windows Desktop and Tablet devices.

Prerequisites:

- To run *a single app* in Kiosk mode: Windows 10 (version 1709 or later) or Windows 11
- To run *multiple apps* in Kiosk mode: Windows 10 (version 1803 or later) or Windows 11

- **UWP app AUMID:** Click **Add**, select Universal Windows Platform (UWP) app, and enter the application user model ID (AUMID) for each UWP app. For example, enter the following AUMID:
  - `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`
- **Win32 app path** and **Win32 app AUMID:** Click **Add**, select Windows desktop (Win32) app, and enter the path and the AUMID for each Win32 app. For example, enter the following path and AUMID:
  - `%windir%\system32\mspaint.exe` or `C:\Windows\System32\mspaint.exe`
  - `{ 1AC14E77-02E7-4E5D-B744-2EB1AE5198B7 } \mspaint.exe`
- **Start layout:** Only the default start screen for apps is available.
- **Default XML:** Only the default XML script is available.
- **Select user type:** Specify the user type to receive the Kiosk policy. Your options:
  - **Local:** Endpoint Management creates a user for the target device or adds an existing user.
  - **Azure AD:** Endpoint Management adds users enrolled in Azure AD.
- **User name:** Enter the user name to receive the Kiosk policy.
  - To create a local user name on the target device, enter the name. Ensure that your local user name doesn't contain the domain. If you enter an existing name, Endpoint Management doesn't create a user or change the current password.
  - To add an Azure AD user, enter the name in the format `azuread\user`. The `user` portion can be either the **Name** entered when creating a user in Azure AD, or the **User name** entered when creating a user in Azure AD. The assigned user cannot be an Azure AD administrator.
- **Password:** There is no password configuration for the Azure AD users. Type the password only for the local user name.
- **Show task bar:** Enable the taskbar to provide users with an easy way to view and manage applications. The default is **Off**.

- Click **Next** and save the changes.

For a UWP app that you want to allow in Kiosk mode, you need to provide the AUMID. To get a list of the AUMIDs for all Microsoft Store apps installed for the current device user, run the following PowerShell command:

```
1 $installedapps = get-AppxPackage
2
3 $aumidList = @()
4 foreach ($app in $installedapps)
5 {
6
7     foreach ($id in (Get-AppxPackageManifest $app).package.applications
8         .application.id)
9     {
10         $aumidList += $app.packagefamilyname + "!" + $id
11     }
12
13 }
14
15
16 $aumidList
17
18 <!--NeedCopy-->
```

## Chrome OS settings

Assign the Kiosk policy to a specific delivery group rather than the **All Users** group. After successfully enrolling the device and signing out, Kiosk mode launches on the device.

To remove the device from Kiosk mode, select the device and delete it from the administrator console. This action removes all the policies pushed from the Endpoint Management console to the device.

The screenshot displays the Citrix Endpoint Management console interface. The top navigation bar includes tabs for Device Policies, Apps, Media, Actions, Sharefile, Enrollment Profiles, and Delivery Groups. The main content area is titled 'Kiosk Policy' and contains the following settings:

- Heartbeat setting:  ON
- Device log upload enabled:  ON
- Device status alert delivery:  EMAIL,  SMS

Below these settings is a section for 'Email addresses' with a text input field and 'Save' and 'Cancel' buttons. At the bottom, there is a section for 'Chrome kiosk apps' with 'Add' and 'Delete' icons.

- **Heartbeat setting:** Monitor the status of the device. The default is **On**.

- **Device log upload enabled:** Store the record of events from the Chrome device. You can locate the .log file in the Google Workspace domain. The default is **On**.
- **Device status alert delivery:** Send alert notifications via email or text messages. Only configured emails and mobile numbers get notifications.
  - **Email addresses:** If you select the **Email** box, specify the email addresses to receive the alerts. Save the changes.
  - **Mobile numbers:** If you select the **SMS** box, specify the phone numbers to receive the alerts. Save the changes.

### Configure multiple kiosk apps

The screenshot shows the 'Kiosk Policy' configuration interface. On the left, a sidebar contains sections: '1 Policy Info', '2 Platforms' (with a 'Select All' link), and '3 Assignment'. Under '2 Platforms', 'Chrome OS' is selected with a checkmark. The main area shows a list of apps with 'Add' and 'Delete' buttons. A modal form for adding a new app is open, with the following fields: 'App name \*' (Citrix Kiosk App), 'App ID \*' (a blurred ID), 'URL' (empty), and 'Extension policy' (empty text area).

To add multiple apps, click **Add**.

- **App name:** Enter the full name of the app to add.
- **App ID:** Specify the ID of the app that you want to allow in Kiosk mode.
- **URL:** Specify the URL to download the app. You can enter a specific URL or download the app from the App Store.
- **Extension policy:** Customize the browsing experience by adjusting Chrome functionality and behavior. Enter a configuration code that contains a valid JSON object.
- Click **Next** and save the changes. Users can start the apps in Kiosk mode after you deploy the policy.

### Auto launch apps in Kiosk mode

Prerequisite:

Before configuring auto launch, add the apps to the Kiosk policy.



- **Auto launch kiosk app:** Launches the Kiosk policy when users start the device.
  - **App name:** Enter the full name of the app to auto launch.
  - **App ID:** Specify the ID of the app that you want to allow in Kiosk mode.
  - **Enable auto login cancel:** When the device starts, provide users with the option to sign in using the regular sign-in screen. The default is **On**.
  - **Prompt for network when offline:** Let users select a network when the device enters Kiosk mode. The default is **On**.

## Android Enterprise settings

You can allow apps and set lock task mode for dedicated Android Enterprise devices, which are also known as corporate owned single use (COSU) devices.

To allow an app, click **Add**. You can add multiple apps to the allow list. For more information, see [Android Enterprise](#).

- **Apps to allow:** Enter the package name of the app you want to allow or select the app from the list.
  - Click **Add new** to enter the package name of the allowed app in the list.
  - Select the existing app from the list. The list shows apps that are uploaded in Endpoint Management. By default, Secure Hub and Google Play services are on the allow list.

Apps to allow *	Lock task mode
Make a selection Add new Citrix Secure Web Google Chrome: Fast & Secure	<input checked="" type="radio"/> Allow <input type="radio"/> Block

- **Lock task mode:** Choose **Allow** to set the app to be pinned to the device screen when the user starts the app. Choose **Block** to set the app not to be pinned. Default is **Allow**.

When an app is in lock task mode, the app is pinned to the device screen when the user opens it. No Home button appears and the **Back** button is disabled. The user exits the app using an action

programmed into the app, such as signing out.

## Knox Platform for Enterprise device policy

November 18, 2020

Samsung upgraded the Knox License (KLM) and renamed it to the Knox Platform for Enterprise (KPE) Premium license key. You can replace existing Enterprise Licenses (ELM) and KLM keys with a new KPE Premium license key or continue to use the legacy keys in Citrix Endpoint Management.

- You purchase a Samsung Knox Platform for Enterprise License and obtain the KPE Premium key from Samsung. For more information, see the Samsung Developer documentation.
- To use a KPE key, create a Knox Platform for Enterprise device policy. If you are replacing legacy keys with a KPE key, remove the old Samsung MDM license key device policy.
- For information about using existing ELM and KLM keys, see [Samsung MDM license key device policy](#).

### Samsung SAFE settings

The screenshot displays the configuration interface for a 'Knox Platform for Enterprise' device policy. The left-hand navigation pane includes sections for '1 Policy Info', '2 Platforms' (with a 'Clear All' link), and '3 Assignment'. Under '2 Platforms', 'Samsung SAFE' and 'Android Enterprise' are both checked. The main configuration area is titled 'Knox Platform for Enterprise' and includes a note: 'For the SAFE platform and Knox platform, you must purchase a Samsung Knox Platform for Enterprise (PKE) license.' Below this note are two input fields: 'Knox Platform for Enterprise Key' (marked with a red asterisk) and 'Backwards Compatible Key' (with a help icon). A 'Deployment Rules' section is visible below the input fields.

- **Knox Platform for Enterprise Key:** The KPE key that you received from Samsung.
- **Backward-compatible key:** If you support Samsung devices running Knox 2.7.1 or earlier, specify the backward-compatible key that is provided with your entitlement-based Samsung Knox License key.

## Android Enterprise settings

Device Policies Apps Media Actions ShareFile Enrollment Profiles Delivery Groups

### Knox Platform for Enterprise

You can push your Knox Platform for Enterprise (KPE) key to Android Enterprise enrolled device for Knox version 3.0+

Knox Platform for Enterprise Key \*

1 Policy Info

2 Platforms [Clear All](#)

Samsung SAFE

Android Enterprise

3 Assignment

► Deployment Rules

- **Knox Platform for Enterprise Key:** The KPE key that you received from Samsung for devices running Knox version 3.0 or later.

After you submit the changes, Endpoint Management then validates and registers the information.

## Launcher configuration device policy

February 11, 2021

Citrix Launcher lets you customize the user experience for Android Enterprise devices and legacy Android devices deployed by Endpoint Management.

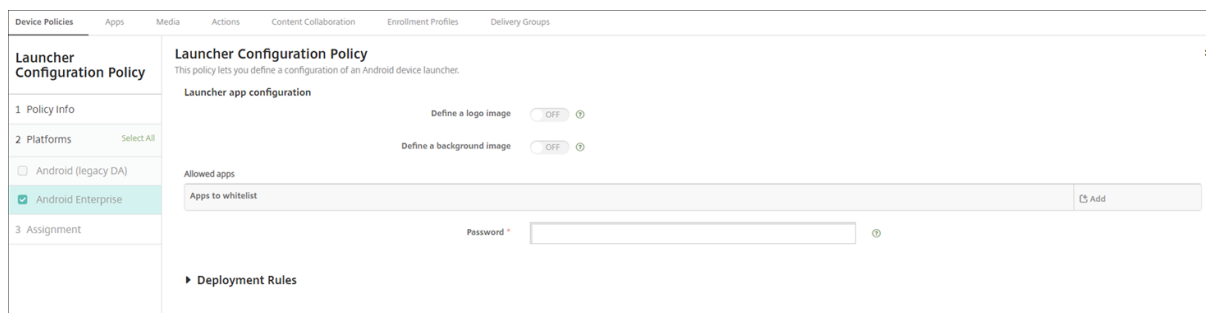
Use a Launcher configuration policy to control these Citrix Launcher features:

- Manage Android Enterprise devices and legacy Android devices so that users can access only the apps that you specify.
- Optionally specify a custom logo image for the Citrix Launcher icon and a custom background image for Citrix Launcher.
- Specify a password that users must type to exit the launcher.

Citrix Launcher isn't intended to be an extra layer of security over what the device platform already provides.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Android Enterprise and Android settings



- **Define a logo image:** Select whether to use a custom logo image for the Citrix Launcher icon. The default is **Off**.
- **Logo image:** When you enable **Define a logo image**, select the image file by clicking **Browse** and navigating to the file's location. Supported file types are PNG, JPG, JPEG, and GIF.
- **Define a background image:** Select whether to use a custom image for the Citrix Launcher background. The default is **Off**.
- **Background image:** When you enable **Define a background image**, select the image file by clicking **Browse** and navigating to the file's location. Supported file types are PNG, JPG, JPEG, and GIF.
- **Allowed apps:** For each app that you want to allow in Citrix Launcher, click **Add** and then do the following:
  - **New app to add:** Enter the full name of the app to add. For example, com.android.calendar for the Android calendar app.
  - Click **Save** to add the app or click **Cancel** to cancel adding the app.
- **Password:** The password a user must enter to exit Citrix Launcher.

## LDAP device policy

March 24, 2020

You create an LDAP policy for iOS devices in Endpoint Management to provide information about an LDAP server to use, including any necessary account information. The policy also provides a set of LDAP search policies to use when querying the LDAP server.

You need the LDAP host name before configuring this policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

- **Account description:** Enter an optional account description.
- **Account user name:** Enter an optional user name.
- **Account password:** Enter an optional password. Use this field only with encrypted profiles.
- **LDAP host name:** Enter the LDAP server host name. This field is required.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the LDAP server. The default is **On**.
- **Search Settings:** Add search settings to use when querying the LDAP server. You can enter as many search settings as you want, but you should add at least one search setting to make the account useful. Click **Add** and then do the following:
  - **Description:** Enter a description of the search setting. This field is required.
  - **Scope:** Choose **Base**, **One level**, or **Subtree** to define how deeply into the LDAP tree to search. The default is **Base**.
    - \* **Base** searches the node pointed to by Search base.
    - \* **One level** searches the Base node and one level below it.
    - \* **Subtree** searches the Base node, plus all its children, regardless of depth.
  - **Search base:** Enter the path to the node at which to start searching. For example, ou=people or o=example corp. This field is required.
  - Click **Save** to add the search setting or click **Cancel** to cancel adding the search setting.
  - Repeat these steps for each search setting that you want to add.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

## macOS settings

- **Account description:** Enter an optional account description.
- **Account user name:** Enter an optional user name.
- **Account password:** Enter an optional password. Use this field only with encrypted profiles.
- **LDAP host name:** Enter the LDAP server host name. This field is required.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the LDAP server. The default is **On**.
- **Search Settings:** Add search settings to use when querying the LDAP server. You can enter as many search settings as you want, but you should add at least one search setting to make the account useful. Click **Add** and then do the following:
  - **Description:** Enter a description of the search setting. This field is required.

- **Scope:** Choose **Base**, **One level**, or **Subtree** to define how deeply into the LDAP tree to search. The default is **Base**.
  - \* **Base** searches the node pointed to by Search base.
  - \* **One level** searches the Base node and one level below it.
  - \* **Subtree** searches the Base node, plus all its children, regardless of depth.
- **Search base:** Enter the path to the node at which to start searching. For example, `ou=people` or `o=example corp`. This field is required.
- Click **Save** to add the search setting or click **Cancel** to cancel adding the search setting.
- Repeat these steps for each search setting you want to add.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

## Location device policy

October 5, 2021

You create location device policies in Endpoint Management to enforce geographic boundaries. When users breach the defined boundary, also called a *geofence*, Endpoint Management can perform certain actions. For example, you can configure the policy to issue a warning message to users when they breach the defined perimeter. You can also configure the policy to wipe users' corporate data when they breach a perimeter, right away or after a delay. For information about security actions, such as enabling tracking and locating a device, see [Security actions](#).

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

Location Policy	Location Policy
1 Policy Info	This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.
2 Platforms	<b>Device agent configuration</b>
<input checked="" type="checkbox"/> iOS	Location Timeout: <input type="text" value="1"/> <input type="button" value="Minutes"/>
<input type="checkbox"/> Android	Tracking duration: <input type="text" value="6"/> <input type="button" value="Hours"/>
<input type="checkbox"/> Android Enterprise	Accuracy: <input type="text" value="328"/> <input type="button" value="Feet"/>
3 Assignment	Report if Location Services are disabled: <input type="button" value="OFF"/>
	Geofencing: <input type="button" value="OFF"/>

- **Location timeout:** Type a numeral and then click **Seconds** or **Minutes** to set how often Endpoint Management attempts to fix the device's location. Valid values are 60–900 seconds or 1–15 minutes. The default is **1 minute**.
- **Tracking duration:** Type a numeral and then click **Hours** or **Minutes** to set how long Endpoint Management tracks the device. Valid values are 1–10 hours or 10–600 minutes. The default is **6 hours**.
- **Accuracy:** Type a numeral and then click **Meters**, **Feet**, or **Yards** to set how close to a device Endpoint Management tracks the device. Valid values are 10–5000 yards, 30–15000 feet, or 10–5000 meters. The default is **328 feet (100 meters)**.
- **Report if Location Services are disabled:** Select whether the device sends a report to Endpoint Management when the user turns off GPS. The default is **Off**.
- **Geofencing**

Geofencing	<input checked="" type="checkbox"/>
Radius	<input type="text" value="16400"/> <input type="button" value="Feet"/>
Center point latitude*	<input type="text" value="0.000000"/>
Center point longitude*	<input type="text" value="0.000000"/>
Warn user on perimeter breach	<input type="button" value="OFF"/> ?
Wipe corporate data on perimeter breach	<input type="button" value="OFF"/>

When you enable Geofencing, configure these settings:

- **Radius:** Type a numeral and then click the units to be used to measure the radius. The default is **16400 feet (5000 meters)**. Valid values for radius are:
  - 164–16400 feet
  - 50–50000 meters

- 54–54680 yards
- 1–31 miles
- **Center point latitude:** Type a latitude, such as 37.787454, to define the geofence center point’s latitude.
- **Center point longitude:** Type a longitude, such as 122.402952, to define the geofence center point’s longitude.
- **Warn user on perimeter breach:** Select whether to issue a warning message when users breach the defined perimeter. The default is **Off**. No connection to Endpoint Management is required to display the warning message.
- **Wipe corporate data on perimeter breach:** Select whether to wipe users’ devices when they breach the perimeter. The default is **Off**. When you enable this option, the **Delay on local wipe** field appears.
  - Type a numeral and then click **Seconds** or **Minutes** to set the length of time to delay before wiping corporate data from user devices. The delay gives users an opportunity to return to the allowed location before Endpoint Management selectively wipes their devices. The default is **0 seconds**.

## Android (legacy DA) settings

Android location tracking requires Android 8.5 or later.

The screenshot displays the 'Location Policy' configuration page. On the left, a sidebar lists '1 Policy Info', '2 Platforms' (with 'Clear All' and 'Android' selected), and '3 Assignment'. The main content area is titled 'Location Policy' and includes a description: 'This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.' Below this, the 'Device agent configuration' section contains:
 

- 'Poll interval': A text input field with '15' and a dropdown menu set to 'Minutes'.
- 'Report if Location Services is disabled': A toggle switch set to 'OFF'.
- 'Geofencing': A toggle switch set to 'OFF'.
- 'Enable Tracking': A toggle switch set to 'OFF'.

 At the bottom, there is a 'Deployment Rules' section with a right-pointing arrow.

- **Poll interval:** Type a numeral and then click **Minutes** or **Hours**, or **Days** to set how often Endpoint Management attempts to fix the device’s location. Valid values are 15–1440 minutes, 1–24 hours, or any number of days. The default is **15 minutes**.
- **Report if Location Services are disabled:** Select whether the device sends a report to Endpoint Management when the user turns off GPS. The default is **Off**.
- **Geofencing**



Geofencing  ON

Radius

Center point latitude \*

Center point longitude \*

Warn user on perimeter breach  OFF ⓘ

Device connects to Endpoint Management for policy refresh

- Perform no action on perimeter breach
- Wipe corporate data on perimeter breach
- Lock device locally

When you enable Geofencing, configure these settings:

- **Radius:** Type a numeral and then click the units to be used to measure the radius. The default is **16400 feet (5000 meters)**. Valid values for radius are:
  - 164–164000 feet
  - 1–50 kilometers
  - 50–50000 meters
  - 54–54680 yards
  - 1–31 miles
- **Center point latitude:** Type a latitude, such as 37.787454, to define the geofence center point's latitude.
- **Center point longitude:** Type a longitude, such as 122.402952, to define the geofence center point's longitude.
- **Warn user on perimeter breach:** Select whether to issue a warning message when users breach the defined perimeter. The default is **Off**. No connection to Endpoint Management is required to display the warning message.
- **Device connects to Endpoint Management for policy refresh:** Select one of the following options for when users breach the perimeter:
  - **Perform no action on perimeter breach:** Do nothing. This is the default.
  - **Wipe corporate data on perimeter breach:** Wipe corporate data after a specified length of time. When you enable this option, the **Delay on local wipe** field appears.
    - \* Type a numeral and then click **Seconds** or **Minutes** to set the length of time to delay before wiping corporate data from user devices. The delay gives users an opportunity to return to the allowed location before Endpoint Management selectively wipes their devices. The default is **0 seconds**.
  - **Lock device locally:** Lock users' devices after a specified length of time. When you enable this option, the **Delay on lock** field appears.
    - \* Type a numeral and then click **Seconds** or **Minutes** to set the length of time to delay before locking user devices. The delay gives users an opportunity to return to the

allowed location before Endpoint Management locks their devices. The default is **0 seconds**.

- **Enable tracking:** Select whether the device tracks user location. The default is **Off**.

## Android Enterprise settings

For Android location tracking to work, ensure that the following requirements are met:

- Android 8.5 or later
- The Allow location sharing setting enabled in the Restrictions device policy for Android Enterprise
- Connection scheduling (Firebase Cloud Messaging recommended)

The screenshot displays the 'Location Policy' configuration page in the Citrix Endpoint Management console. The page is divided into a left-hand navigation pane and a main configuration area. The navigation pane includes sections for '1 Policy Info', '2 Platforms' (with a 'Select All' link), and '3 Assignment'. Under '2 Platforms', the 'Android Enterprise' option is selected with a checkmark. The main configuration area is titled 'Location Policy' and includes a descriptive paragraph: 'This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.' Below this, there are several settings: 'Apply To COPE' (toggle OFF), 'Managed device' section with 'Location Mode' set to 'Off' (dropdown menu), 'Managed profile' section with 'Report if Location Services is disabled' (toggle OFF) and 'Geofencing' (toggle OFF). A 'Deployment Rules' section is partially visible at the bottom.

## Apply to fully managed devices with a work profile

For fully managed devices with work profiles (formerly known as COPE devices), only the location mode setting is available.

- **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices:** Allows you to configure the location mode for fully managed devices with work profiles. When this setting is on, configure the settings for the work profile:
  - **Report if Location Services are disabled:** Select whether the device sends a report to Endpoint Management when the user turns off GPS. The default is **Off**.
  - **Geofencing:** See the settings in this article under Managed device.

When **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices** is off, settings apply to the managed device and work profile as shown in the following sections. Default is **Off**.

## Managed device

- **Location Mode:** Specify the degree of location detection to enable. You can use the Locate security action only when location mode is set to **High Accuracy** or **Battery Saving**. The default is **High Accuracy**.
  - **High Accuracy:** Enables all location detection methods, including GPS, networks, and other sensors.
  - **Sensors Only:** Enables only GPS and other sensors.
  - **Battery Saving:** Enables only the network location provider.
  - **Off:** Disables location detection.
- **Geofencing:**

Geofencing

Poll interval \*   
 

Radius \*   
 

Center point latitude \*

Center point longitude \*

Warn user on perimeter breach  

Device connects to Endpoint Management for policy refresh

Perform no action on perimeter breach

Wipe corporate data on perimeter breach

Lock device locally

When you enable **Geofencing**, configure these settings:

- **Poll interval:** Type a numeral and then click **Minutes** or **Hours**, or **Days** to set how often End-point Management attempts to fix the device's location. Valid values are 1–1440 minutes, 1–24 hours, or any number of days. The default is **10 minutes**. Setting this value to less than 10 minutes might adversely affect the device's battery life.
- **Radius:** Type a numeral and then click the units to be used to measure the radius. The default is **16400 feet (5000 meters)**. Valid values for radius are:
  - 164–164000 feet
  - 1–50 kilometers
  - 50–50000 meters
  - 54–54680 yards

- 1–31 miles
- **Center point latitude:** Type a latitude, such as 37.787454, to define the geofence center point's latitude. To look up the value, go to **Manage > Devices**, select the device, click **Secure**, and then click **Locate**. After locating the device, Endpoint Management reports the device location in the **Device Details > General** page under **Security**.
- **Center point longitude:** Type a longitude, such as 122.402952, to define the geofence center point's longitude.
- **Warn user on perimeter breach:** Select whether to issue a warning message when users breach the defined perimeter. The default is **Off**. No connection to Endpoint Management is required to display the warning message.
- **Device connects to Endpoint Management for policy refresh:** Select one of the following options for when users breach the perimeter:
  - **Perform no action on perimeter breach:** Do nothing. This setting is the default.
  - **Wipe corporate data on perimeter breach:** Wipe corporate data after a specified length of time. When you enable this option, the **Delay on local wipe** field appears.
    - \* Type a numeral and then click **Seconds** or **Minutes** to set the length of time to delay before wiping corporate data from user devices. The delay gives users an opportunity to return to the allowed location before Endpoint Management selectively wipes their devices. The default is **0 seconds**.
  - **Lock device locally:** Lock users' devices after a specified length of time. When you enable this option, the **Delay on lock field** appears.
    - \* Type a numeral and then click **Seconds** or **Minutes** to set the length of time to delay before locking user devices. The delay gives users an opportunity to return to the allowed location before Endpoint Management locks their devices. The default is **0 seconds**.

### Work profile

- **Report if Location Services are disabled:** Select whether the device sends a report to Endpoint Management when the user turns off GPS. The default is **Off**.
- **Geofencing:** See the settings in this article under Managed device.

## Lock screen message device policy

March 24, 2020

The Lock screen message policy lets you set messages to appear on the following iOS devices when they are lost:

- The login window of shared iPads
- The lock screen of supervised iOS devices

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

- **Asset tag information for the device:** The asset tag for the device. Apple devices truncate long strings, so be sure to test a string before deploying the policy to production. String length depends on the Apple device model and Apple settings, which can change.
- **Login window and lock screen footnote:** Information to help in returning the device, such as an address or other contact information. For example, your message might be in the form “If Lost, return to”. Apple devices truncate long strings, so be sure to test a string before deploying the policy to production. String length depends on the Apple device model and Apple settings, which can change.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

## Mail device policy

April 6, 2020

You can add a mail device policy in Endpoint Management to configure an email account on iOS or macOS devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS and macOS settings

Mail Policy	
1 Policy Info	
2 Platforms <span>Select All</span>	
<input checked="" type="checkbox"/> iOS	
<input type="checkbox"/> macOS	
3 Assignment	
	<p>Allow Mail Drop <input type="checkbox"/> OFF IOS 9.2+</p> <p>Enable S/MIME Signing <input checked="" type="checkbox"/> ON IOS 10.3+</p> <p>Signing identity credential <input type="text" value="None"/> IOS 5.0+</p> <p>S/MIME Signing User Overrideable <input type="checkbox"/> OFF IOS 12.0+</p> <p>S/MIME Signing Certificate UUID User Overrideable <input type="checkbox"/> OFF IOS 12.0+</p> <p>Enable S/MIME Encryption <input checked="" type="checkbox"/> ON IOS 10.3+</p> <p>Encryption identity credential <input type="text" value="None"/> IOS 5.0+</p> <p>Enable per message S/MIME switch <input type="checkbox"/> OFF</p> <p>S/MIME Encrypt By Default User Overrideable <input type="checkbox"/> OFF IOS 12.0+</p> <p>S/MIME Encryption Certificate UUID User Overrideable <input type="checkbox"/> OFF IOS 12.0+</p>

- **Account description:** Type an account description that appears in the Mail and Settings apps. This field is required.
- **Account type:** Choose either **IMAP** or **POP** to select the protocol to be used for user accounts. The default is **IMAP**. When you select **POP**, the following **Path** prefix option disappears.
- **Path prefix:** Type **INBOX** or your IMAP mail account path prefix. This field is required.
- **User display name:** Type the full user name to be used for messages and other purposes. This field is required.
- **Email address:** Type the full email address for the account. This field is required.
- **Incoming email settings**
  - **Email server host name:** Type the incoming mail server host name or IP address. This field is required.
  - **Email server port:** Type the incoming mail server port number. The default is **143**. This field is required.
  - **User name:** Type the user name for the email account. This name is generally the same as the email address up to the @ character. This field is required.
  - **Authentication type:** Choose the authentication type to be used. The default is **Password**. When **None** is selected, the following **Password** field disappears.
  - **Password:** Type an optional password for the incoming mail server.
  - **Use SSL:** Select whether the incoming mail server uses Secure Socket Layer authentication. The default is **Off**.
- **Outgoing email settings**
  - **Email server host name:** Type the outgoing mail server host name or IP address. This field is required.

- **Email server port:** Type the outgoing mail server port number. If no port, you do not enter a port number, the default port for the given protocol is used.
- **User name:** Type the user name for the email account. This name is generally the same as the email address up to the @ character. This field is required.
- **Authentication type:** Choose the authentication type to use. The default is **Password**.
- **Password:** Type an optional password for the outgoing mail server.
- **Outgoing password same as incoming:** Select whether the incoming and outgoing passwords are the same. The default is **Off**, which means the passwords are different.
- **Use SSL:** Select whether the outgoing mail server uses Secure Socket Layer authentication. The default is **Off**.

- **Policy**

- **Authorize email move between accounts:** Select whether to allow users to:
  - \* move email out of this account into another account
  - \* forward email from a different account
  - \* reply from a different account.The default is **Off**.
- **Sending email only from mail app:** Select whether to restrict users to the iOS mail app for sending email.
- **Disable mail recents syncing:** Select whether to prevent users from syncing recent addresses. The default is **Off**. This option applies only to iOS 6.0 and later.
- **Allow Mail Drop:** Select whether to allow use of Apple Mail Drop for devices running iOS 9.2 and later. The default is **Off**.
- **Enable S/MIME Signing:** Select whether this account supports S/MIME signing. The default is **On**. When set to **On**, the following fields appear.
  - \* **Signing identity credential:** Choose the signing credential to use.
  - \* **S/MIME Signing User Overridable:** If set to **On**, users can turn S/MIME signing on and off in the settings of their devices. The default is **Off**. This option applies to iOS 12.0 and later.
  - \* **S/MIME Signing Certificate UUID User Overridable:** If set to **On**, users can select, in the settings of their devices, the signing credential to use. The default is **Off**. This option applies to iOS 12.0 and later.
- **Enable S/MIME Encryption:** Select whether this account supports S/MIME encryption. The default is **Off**. When set to **On**, the following fields appear.
  - \* **Encryption identity credential:** Choose the encryption credential to use.
  - \* **Enable per message S/MIME switch:** When set to **On**, shows users an option to switch S/MIME encryption on or off for each message they compose. The default is **Off**.
  - \* **S/MIME Encrypt By Default User Overridable:** If set to **On**, users can, in the settings of their devices, select whether S/MIME is on by default. The default is **Off**. This option

applies to iOS 12.0 and later.

- \* **S/MIME Encryption Certificate UUID User Overridable:** If set to **On**, users can turn S/MIME encryption identity and encryption on and off in the settings of their devices. The default is **Off**. This option applies to iOS 12.0 and later.

- **Policy Settings**

- **Remove policy:** To remove the policy later, configure this setting to remove the policy on a **Select date** or for a **Duration until removal (in hours)**.
- **Allow user to remove policy:** Allow users to remove the mail policy **Always**, only with a **Passcode required**, or **Never**. Only available for macOS.
- **Profile scope:** For macOS only, choose whether the policy applies on a per **User** level or across the whole **System**.

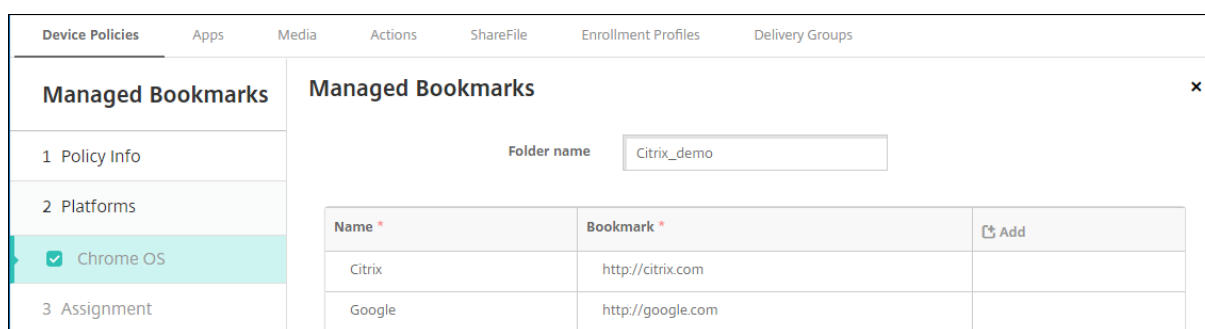
## Managed bookmarks device policy

August 26, 2019

With the Managed bookmarks device policy, you can deploy a folder of bookmarks to Chrome OS devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Chrome OS settings



- **Folder name:** The name of a bookmark folder to deploy to Chrome OS devices.
- **Name:** The name of a bookmark.
- **Bookmark:** The URL for the bookmark.



## Managed configurations policy

June 23, 2021

The Managed configurations device policy controls various app configuration options and app restrictions. You create this policy for each Android Enterprise app that you want to control.

This policy applies to Android for Workspace (Preview) devices as well.

The app developer defines the options and tooltips available for an app. If a tooltip mentions using a “templated value,” use the corresponding Endpoint Management macro instead. For more information, see [Remote configuration overview](#) (on the Android developer site) and [Macros](#).

The app configuration settings can include items such as:

- Email app settings
- Allow or block URLs for a web browser
- Option to control app content sync through a cellular connection or only by a Wi-Fi connection

For information about the settings that appear for your apps, contact the app developer.

### Prerequisites

- Complete Android Enterprise setup tasks on Google and connect Android Enterprise to managed Google Play. For more information, see [Android Enterprise](#).
- Add Android Enterprise apps to Endpoint Management. For more information, see [Adding Apps to Endpoint Management](#).

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Requirements for per-app VPNs

To create a per-app VPN for AE, you need to perform extra steps, in addition to configuring the Managed configurations device policy. Also, you must verify that the following prerequisites are met:

- On-premises Citrix Gateway
- The following applications are installed on the device:
  - Citrix SSO
  - Citrix Secure Hub

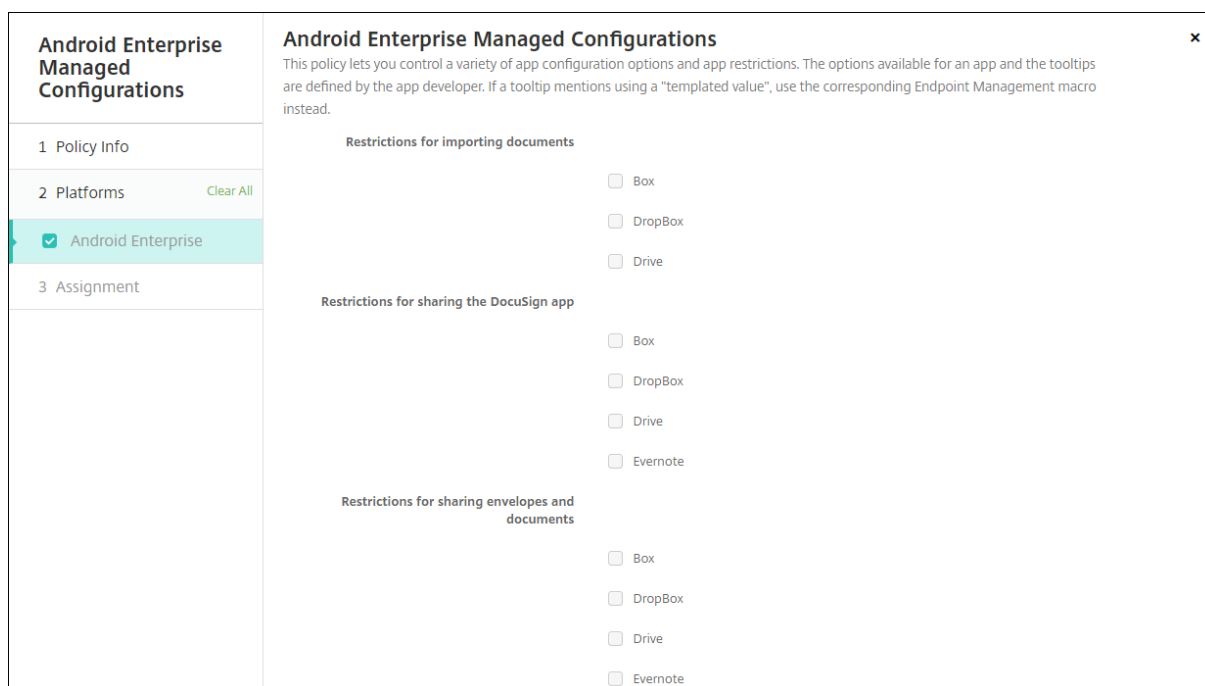
A general workflow to configure a per-app VPN for AE devices is as follows:

1. Configure a VPN profile as described in this article.
2. Configure Citrix ADC to accept traffic from the per-app VPN. For details, see [Full VPN setup on Citrix Gateway](#).

## Android Enterprise settings

After you choose to add a Managed configurations device policy, a prompt to select an app appears. If there are no Android Enterprise apps added to Endpoint Management, you cannot proceed.

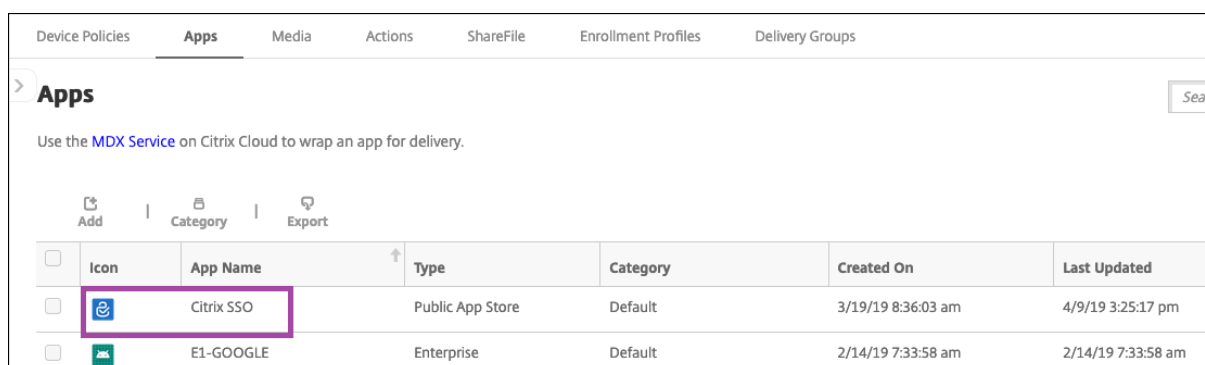
After you select an app, then configure the policy settings. The settings are specific to each app.



## Configure VPN profiles for Android Enterprise

Make VPN profiles available to Android Enterprise devices using the Citrix SSO app with the Android Enterprise managed configuration device policy.

Start by adding Citrix SSO to the Endpoint Management console as a Google Play store app. See [Add a public app store app](#).



Watch this video to learn more:



### **Create an Android Enterprise managed configuration for Citrix SSO**

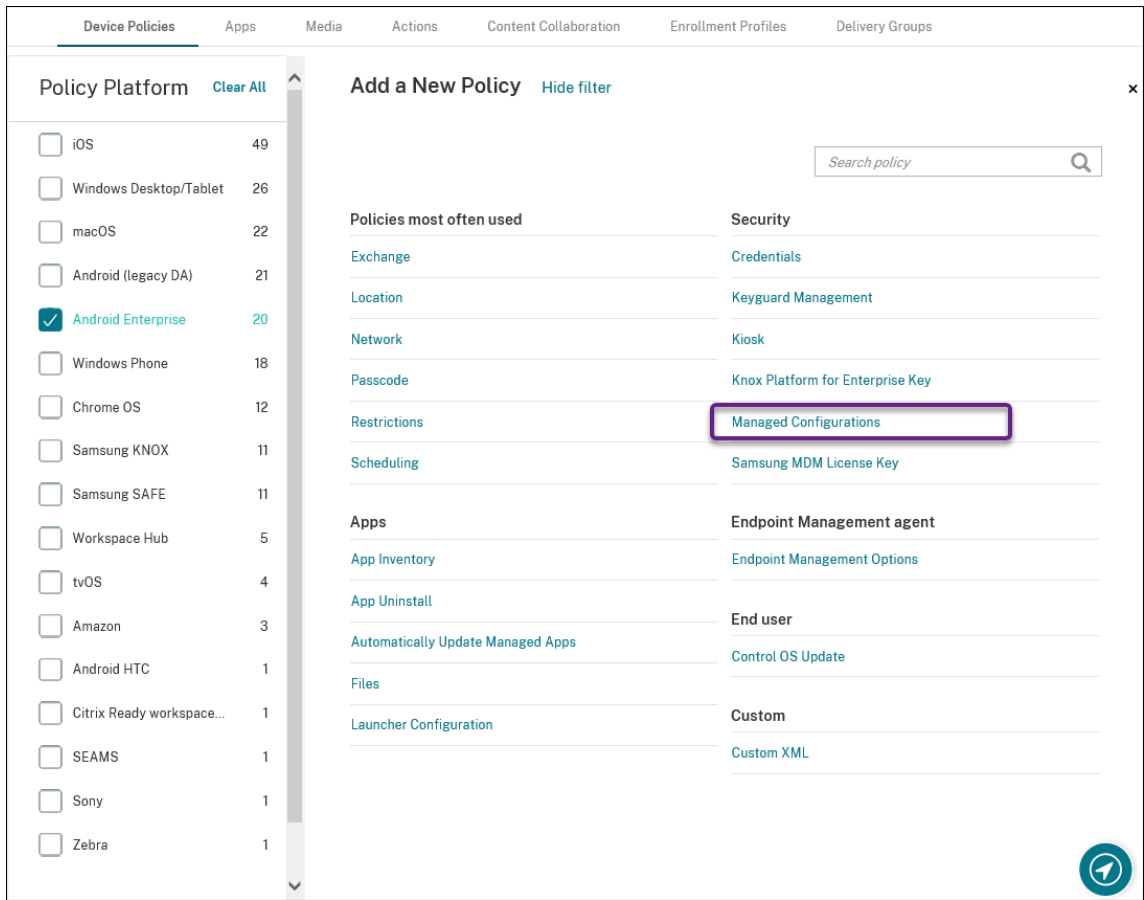
Configure the Managed configurations device policy for Citrix SSO to create VPN profiles. Devices that have the Citrix SSO app installed and the policy deployed can access the VPN profiles you create.

Endpoint Management uses the user certificate in the device keystore if:

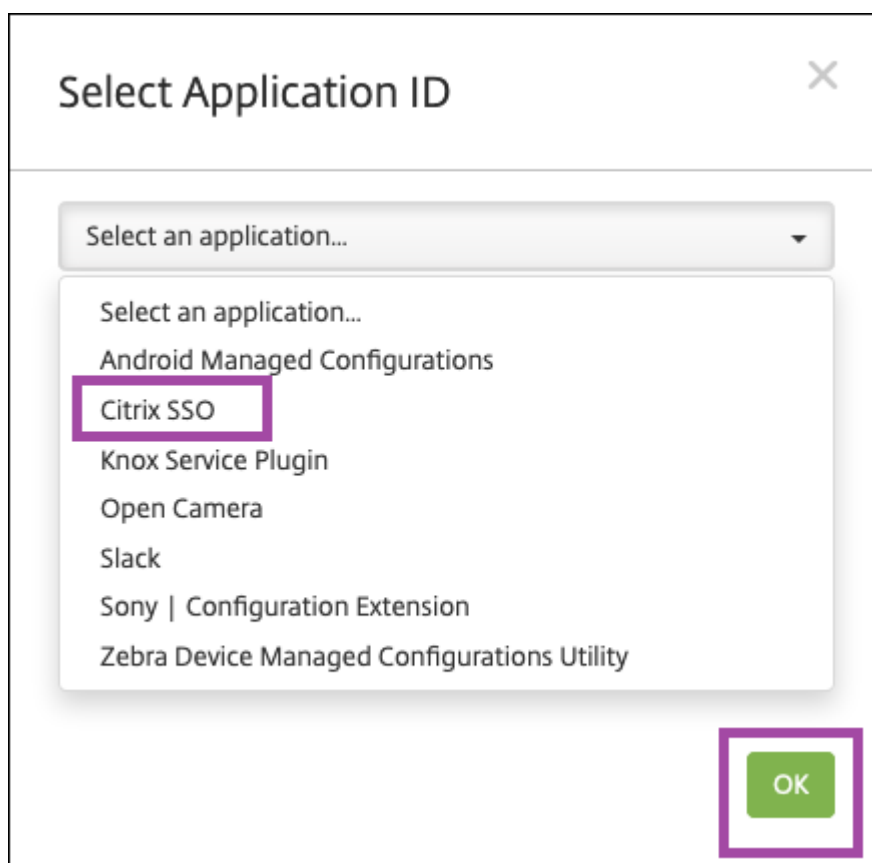
- Citrix Gateway is configured for certificate-based authentication.
- **Deliver user certificate for authentication** is enabled in the Endpoint Management page **Settings > Citrix Gateway**.

You need your Citrix Gateway FQDN and port.

1. In the Endpoint Management console, click **Configure > Device Policies**. Click **Add**.
2. Select **Android Enterprise**. Click **Managed configurations**.



3. When the **Select Application ID** window appears, choose **Citrix SSO** from the list and click **OK**.



4. Type a name and description for your Citrix SSO VPN configuration. Click **Next**.

Android Enterprise Managed Configurations	Policy Information
	com.citrix.CitrixVPN
1 Policy Info	<b>Policy Name *</b> <input type="text" value="Citrix SSO VPN Configuration"/>
2 Platforms <span>Clear All</span>	<b>Description</b> <input type="text" value="VPN Profile"/>
<input checked="" type="checkbox"/> Android Enterprise	
3 Assignment	

5. Configure VPN profile parameters.

- **VPN Profile Name:** Type a name for the VPN profile. If you are creating more than one VPN profile, use a unique name for each. If you don't provide a name, the address you put in the **Server Address** field is used as the VPN profile name.
- **Server Address(\*):** Type your Citrix Gateway FQDN. If your Citrix Gateway port is not 443, also type your port. Use URL format. For example, `https://gateway.mycompany.com:8443`.
- **Username (optional):** Provide the user name that end users use to authenticate to the

Citrix Gateway. You can use the Endpoint Management macro {user.username} for this field. (See [Macros](#).) If you don't provide a user name, users are prompted to provide a user name when they connect to Citrix Gateway.

- **Password (optional):** Provide the password that end users use to authenticate to the Citrix Gateway. If you don't provide a password, users are prompted to provide a password when they connect to Citrix Gateway.
- **Certificate Alias (optional):** Type a certificate alias. The certificate alias makes it easier for the app to access the certificate. When the same certificate alias is used with the Credentials device policy, the app retrieves the certificate and authenticates the VPN without any action by users.
- **Per-App VPN Type (optional):** If you are using per-app VPN to restrict which apps use this VPN, you can configure this setting. If you select **Allow**, network traffic for app package names listed in the **PerAppVPN app list** are routed through the VPN. The network traffic of all other apps is routed outside the VPN. If you select **Disallow**, network traffic for app package names listed in the **PerAppVPN app list** are routed outside the VPN. The network traffic of all other apps is routed through the VPN. Default is **Allow**.
- **PerAppVPN app list:** A list of apps whose traffic is allowed or blocked on the VPN, depending on the value of **Per-App VPN Type**. List the app package names separated by commas or semicolons. App package names are case sensitive and must appear on this list exactly as they appear in the Google Play store. This list is optional. Keep this list empty for provisioning device-wide VPN.
- **Default VPN profile:** Type the name of the VPN profile to use when users tap the connect switch in the Citrix SSO app instead of a specific profile. If this field is left empty, the main profile is used for connection. If only one profile is configured, it is marked as default profile. For always-on VPN, this field must be set to the name of the VPN profile to be used for establishing always-on VPN.
- **Disable User Profiles:** If this setting is On, users can't create their own VPNs on their devices. If this setting is Off, users can create their own VPNs on their devices. Default is Off.
- **Block Untrusted Servers:** This setting is Off in either of the following scenarios:
  - When you use a self-signed certificate for Citrix Gateway
  - When the root certificate for the CA issuing the Citrix Gateway certificate is not in the system CA list.

If this setting is On, the Android operating system validates the Citrix Gateway certificate. If the validation fails, the connection is not allowed. Default value is On.

6. Optionally, create custom parameters. The custom parameters **XenMobileDeviceId** and **User-Agent** are supported. Select the current VPN configuration and click **Add**.

a) Create a custom parameter:

- **Parameter name:** Type **XenMobileDeviceId**. This field is the device ID to use for Network Access Check based on device enrollment in Endpoint Management. If Endpoint Management enrolls and manages the device, the VPN connection is allowed. Otherwise, authentication is denied at the time of VPN establishment.
- **Parameter value:** For Endpoint Management to determine the enrollment and management state of the devices, the value of XenMobileDeviceId set to `DeviceID_${device.id}`.

a) To create another custom parameter, click **Add** again. Create this custom parameter.

- **Parameter name:** Type **UserAgent**. This text appended to the User-Agent HTTP header for performing an extra check on Citrix Gateway. Value of this text is appended to the User-Agent HTTP header by the Citrix SSO app while communicating with the Citrix Gateway.

- **Parameter value:** Type the text you want to append to the User-Agent HTTP header. This text must conform to the HTTP User-Agent specifications.
7. Optionally, create more VPN profile configurations. Click **Add** under the list of configurations. A new configuration appears in the list. Select the new configuration and repeat step 5 and, optionally, step 6.

The screenshot shows the 'Android Enterprise Managed Configurations' interface. On the left, there is a sidebar with navigation options: '1 Policy Info', '2 Platforms' (with a 'Clear All' link), '3 Assignment', and 'Android Enterprise' (which is selected and highlighted in green). The main area is titled 'List of additional VPN profiles' and contains an 'Add' button (highlighted with a purple box) and a 'Delete' button. Below these buttons is a list of configurations, with 'Configuration-0' selected. To the right of the list is a form for configuring a VPN profile. The form fields are: 'VPN Profile Name' (text input with 'Profile2'), 'Server Address(\*)' (text input with 'https://gw2.mycompany.com:8443'), 'Username (optional)' (text input), 'Password (optional)' (text input), 'Certificate Alias (optional)' (text input), 'Per-App VPN Type (optional)' (dropdown menu with 'Allow' selected), and 'PerAppVPN app list' (text input). Each field has a small circular icon to its right.

8. When you have created all the VPN profiles you want, click **Next**.
9. Configure deployment rules for this managed configuration for Citrix SSO.
10. Click **Save**.

This managed configuration for Citrix SSO now appears in your list of configured device policies.

To enable always-on for the VPN profiles you configured, set the [Endpoint Management options device policy](#).

**Note:**

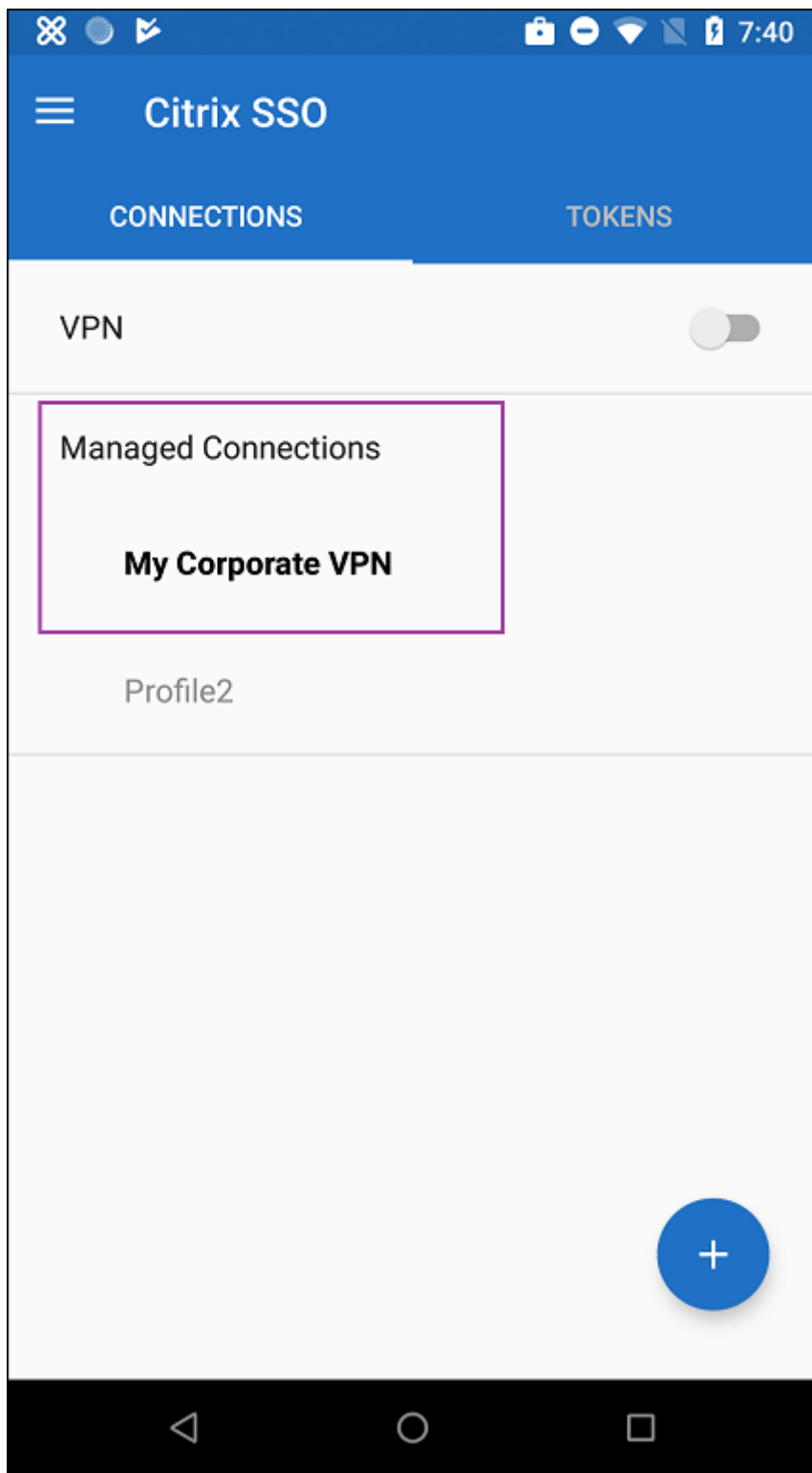
Citrix Secure Hub 19.5.5 or higher is required for always-on VPN for Android Enterprise.

### Accessing VPN profiles from the device

To access the VPN profiles you created, Android Enterprise users install Citrix SSO from the Google Play store.

The VPN profile or profiles you configured appear in the **Managed Connections** area of the app. Users tap the VPN profile to connect using that VPN profile.





After users have authenticated and connected, a check mark appears next to the VPN profile. The key icon indicates the VPN is connected.

## Manage Zebra Android devices using Zebra OEMConfig

Manage Zebra Android devices using the Zebra Technologies OEMConfig administrative tool. For information about the Zebra OEMConfig app, see the [Zebra Technologies website](#).

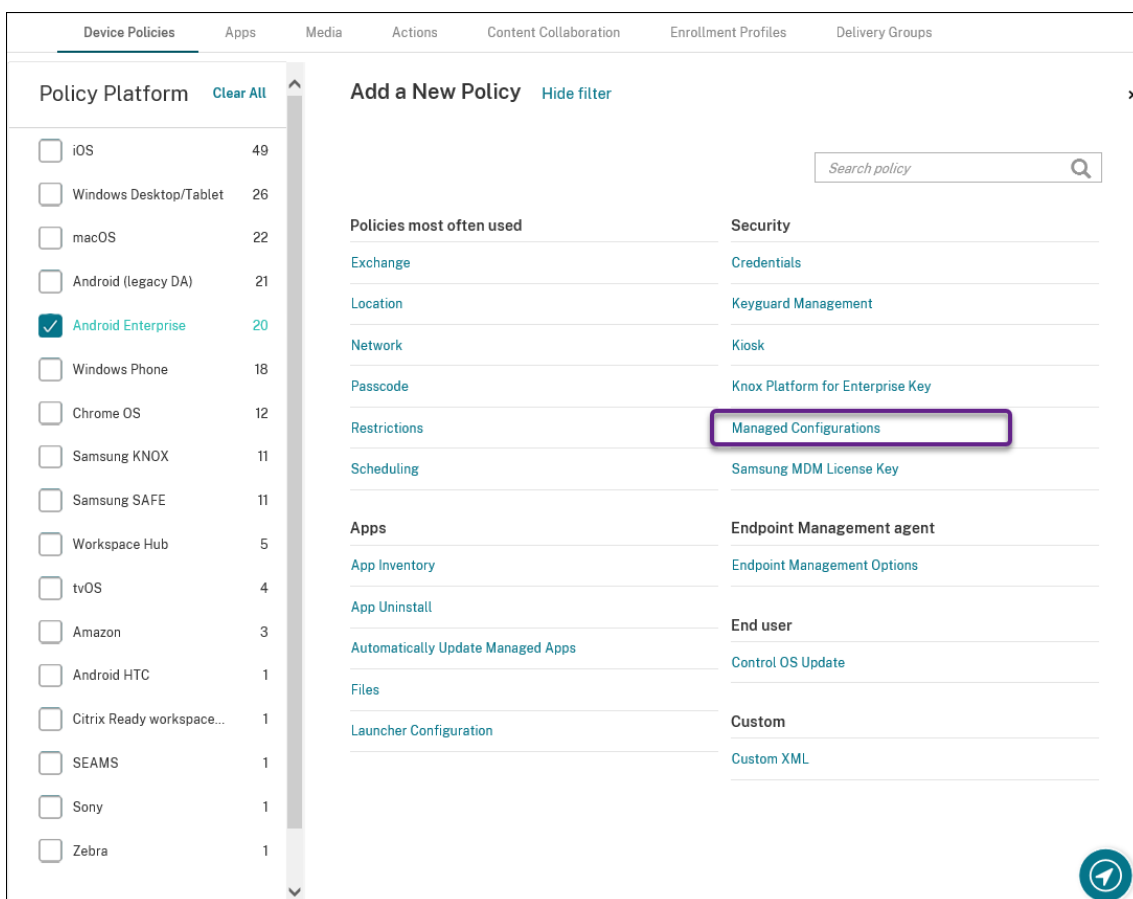
Endpoint Management supports Zebra OEMConfig version 9.2 and higher. For information about system requirements for installing Zebra OEMConfig on devices, see [OEMConfig Setup](#) on the Zebra Technologies website.

To start: In the Endpoint Management console, add the Zebra OEMConfig app as a Google Play store app. See [Add a public app store app](#).

## Create an Android Enterprise managed configuration for the Zebra OEMConfig app

Configure the Managed configurations device policy for the Zebra OEMConfig app. The policy applies to Zebra devices that have the Zebra OEMConfig app installed and the policy deployed.

1. In the Endpoint Management console, click **Configure > Device Policies**. Click **Add**.
2. Select **Android Enterprise**. Click **Managed configurations**.



3. When the **Select Application ID** window appears, choose **ZebraOEMConfig powered by MX** from the list and click **OK**.

4. Type a name and description for your Zebra OEMConfig configuration. Click **Next**.
5. Type a name for the Zebra OEMConfig configuration.
6. Configure the available parameters. For example:
  - To disable the camera on the front of the device, select **Camera Configuration** and set **Use of Front Camera** to **Off**.
  - To change the devices time format, select **Clock Configuration** and set **Time Format** to **12** (12-hour) or **24** (24-hour).

For a list and descriptions of all available configuration, see [Zebra Managed Configurations](#) on the Zebra Technologies website.

1. Optionally, create more Zebra OEMConfig configurations. Click **Add** under the list of configurations. A new configuration appears in the list. Select the new configuration and configure the parameters.
2. When you have created all the Zebra OEMConfig configurations you want, click **Next**.
3. Configure deployment rules for this managed configuration for Zebra OEMConfig.
4. Click **Save**.

## Managed domains device policy

September 2, 2021

You can define managed domains that apply to email and the Safari browser. Managed domains help you protect corporate data by controlling which apps can open documents downloaded from domains using Safari.

For iOS supervised devices, you specify:

- URLs or subdomains to control how users can open documents, attachments, and downloads from the browser.
- URLs from which users can save passwords in Safari.

For the steps on setting an iOS device to supervised mode, see [Deploy devices using Apple Configurator 2](#).

When a user sends email to a recipient whose domain is not on the managed email domains list, the message is flagged on the user's device to warn them that they are sending a message to someone outside your corporate domain.

For items such as documents, attachments, or downloads: When a user opens an item by using Safari from a web domain that is on the managed web domains list, the appropriate corporate app opens

the item. If the item is not from a web domain on the managed web domains list, the user cannot open the item with a corporate app. They must use a personal, unmanaged app.

For supervised devices, even if you do not specify Safari password autofill domains: If the device is configured as ephemeral multi-user, users can't save passwords. However, if the device isn't configured as ephemeral multi-user, users can save all passwords.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

To specify domains:

Format	Description
<code>example.com</code>	Treat any path under <code>example.com</code> as managed, but not <code>site.example.com/</code> .
<code>foo.example.com</code>	Treat any path under <code>foo.example.com</code> as managed, but not <code>example.com/</code> or <code>bar.example.com/</code> .
<code>\*.example.com</code>	Treat any path under <code>foo.example.com</code> or <code>bar.example.com</code> as managed, but not <code>example.com/</code> .
<code>example.com/sub</code>	Treat <code>example.com/sub</code> and any path under it as managed, but not <code>example.com/</code> .
<code>foo.example.com/sub</code>	Treat any path under <code>foo.example.com/sub</code> as managed, but not <code>example.com</code> , <code>example.com/sub</code> , <code>foo.example.com/</code> , or <code>bar.example.com/sub</code> .
<code>\*.example.com/sub</code>	Treat any path under <code>foo.example.com/sub</code> or <code>bar.example.com/sub</code> as managed, but not <code>example.com</code> or <code>foo.example.com/</code> .

Rules:

- Leading “www.” and trailing slashes in URLs are ignored when domains are compared.
- If an entry contains a port number, only addresses that specify that port number are considered managed. Otherwise, only the standard ports are considered managed (port 80 for http and port 443 for https). For example, the pattern `*.example.com:8080` matches `https://site`

.example.com:8080/page.html, but not <https://site.example.com/page.html>, whereas the pattern \*.example.com matches <https://site.example.com/page.html> and <https://site.example.com/page.html>, but not <https://site.example.com:8080/page.html>.

- Managed Safari web domain definitions are cumulative. Patterns defined by all managed Safari web domain payloads are used to match a URL request.

Settings:

- **Managed Domains**
  - **Unmarked Email Domains:** For each email domain you want to include in the list, click **Add** and then do the following:
    - \* **Managed Email Domain:** Type the email domain.
    - \* Click **Save** to save the email domain or click **Cancel** to not save the email domain.
  - **Managed Safari Web Domains:** For each web domain you want to include in the list, click **Add** and then do the following:
    - \* **Managed Web Domain:** Type the web domain.
    - \* Click **Save** to save the web domain or click **Cancel** to not save the web domain.
  - **Safari Password AutoFill Domains:** For each autofill domain you want to include in the list, click **Add** and then do the following:
    - \* **Safari Password AutoFill Domain:** Type the autofill domain.
    - \* Click **Save** to save the autofill domain or click **Cancel** to not save the autofill domain.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

## Maps device policy

June 28, 2019

Windows 10 phone devices support offline maps. Use the Maps device policy to specify which maps to download to devices. The Microsoft Maps configuration service provider (CSP) only supports maps of Germany, the United Kingdom, and the United States.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Windows Phone settings

To add a map, click **Add** and then select the **Country** and **State**. Repeat those steps to add more maps.

## Maximum resident users device policy

April 15, 2020

The Maximum resident users device policy is for shared devices running iOS (iPadOS). For more information about Shared iPads, see [Integrate with Apple Education features](#).

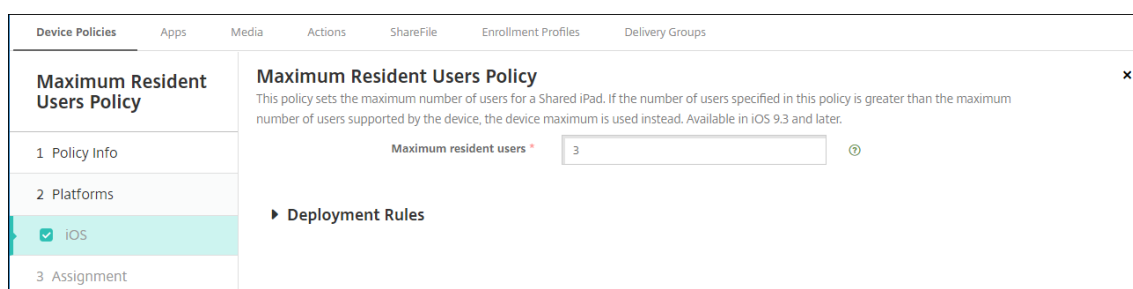
This policy must deploy when the iPad is in the “awaiting configuration” phase during the Setup Assistant. Apple doesn’t allow this policy to deploy after Shared iPads enroll.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### iOS settings

- **Maximum Resident Users:** The maximum number of users for a Shared iPad. If the number of users specified in this policy is greater than the maximum number of users supported by the device: Endpoint Management uses the device maximum instead. Default is **5** users.

Apple recommends that you keep the Maximum resident users value as low as possible. A low value maximizes the amount of iPad storage for each user. In addition, a low value minimizes communication with iCloud and provides a faster sign in experience. For information about how Apple handles shared storage on an iPad, see <https://developer.apple.com/education/shared-ipad/>.



## MDM options device policy

September 2, 2021

The MDM options device policy manages Find My Phone/iPad Activation Lock on supervised iOS devices. For the steps on setting an iOS device to supervised mode, see [Deploy devices using Apple Configurator 2](#).

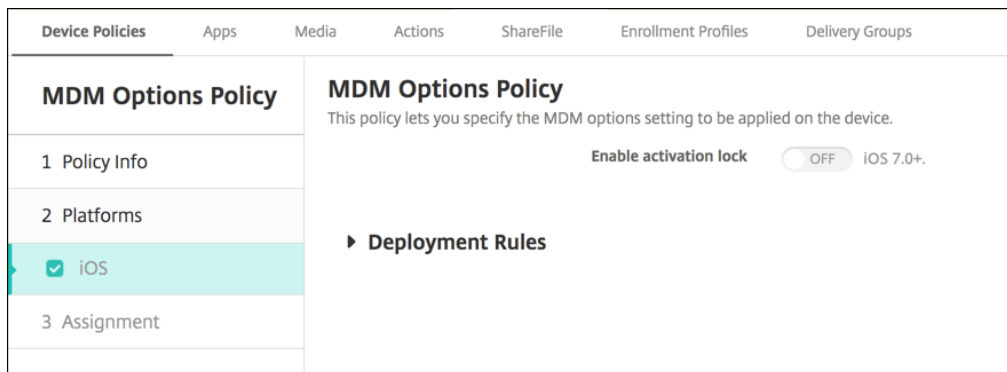
Activation Lock is a feature of Find My iPhone/iPad that prevents reactivation of a lost or stolen supervised device. Activation Lock requires the user Apple ID and password before anyone can turn off Find My iPhone/iPad, erase the device, or reactivate the device. For the devices that your organization owns, bypassing an Activation Lock is necessary to, for example, reset or reallocate devices.

To enable Activation Lock, you configure and deploy the Endpoint Management MDM Options device policy. You can then manage a device from the Endpoint Management console without the Apple credentials of the user. To bypass the Apple credential requirement of an Activation Lock, issue the Activation Lock Bypass security action from the Endpoint Management console.

For example, if the user returns a lost phone or to set up the device before or after a Full Wipe: When the phone prompts for the Apple App Store account credential, you can bypass that step by issuing the Activation Lock Bypass security action from the Endpoint Management console.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings



- **Enable Activation Lock:** Select whether to enable Activation Lock on the devices to which you deploy this policy. The default is **Off**.

After you enable Activation Lock by deploying the MDM options device policy: The Security action **Activation Lock Bypass** appears when you select those devices on the **Manage > Devices** page and click **Security**. An Activation Lock Bypass allows you to remove the Activation Lock from supervised devices prior to device activation without knowing the Apple ID and password of the device users. You can send an Activation Lock Bypass to a device before or after a Full Wipe. For more information, see [Bypass an iOS activation lock](#).

## Network device policy

October 5, 2021

The network device policy lets you manage how users connect their devices to Wi-Fi networks by defining the following items:

- Network names and types
- Authentication and security policies
- Proxy server use
- Other Wi-Fi related details

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Prerequisites

Before you create a policy, complete the following:

- Create any delivery groups that you plan to use.
- Know the network name and type.
- Know any authentication or security types that you plan to use.
- Know any proxy server information that you might need.
- Install any necessary CA certificates.
- Have any necessary shared keys.
- Create the PKI entity for certificate-based authentication.
- Configure credential providers.

For more information, see [Authentication](#) and its subarticles.



## iOS and tvOS settings

Media	Actions	Content Collaboration	Enrollment Profiles	Delivery Groups
<h3>Network</h3> <p>This policy lets you configure a network profile for devices.</p>				
	Network type	<input type="text" value="Standard"/>	<input type="button" value="ⓘ"/>	
	Network name *	<input type="text"/>	<input type="button" value="ⓘ"/>	
	Hide network	<input type="checkbox"/> <input type="button" value="x"/> iOS 5.0+		
	Automatically join this wireless network	<input checked="" type="checkbox"/> <input type="button" value="ⓘ"/>		
	Disable captive network detection	<input type="checkbox"/> <input type="button" value="x"/> <input type="button" value="ⓘ"/>		
	Use static MAC address	<input type="checkbox"/> <input type="button" value="x"/> <input type="button" value="ⓘ"/>		
	Security type	<input type="text" value="None"/>	<input type="button" value="ⓘ"/>	
<h4>Proxy server settings</h4>				
	Proxy configuration	<input type="text" value="None"/>	<input type="button" value="ⓘ"/>	
<h4>QoS settings</h4>				
	Fast Lane QoS marking	<input type="text" value="Do not restrict QoS marking"/>	<input type="button" value="ⓘ"/>	
<h4>Policy settings</h4>				
	Remove policy	<input checked="" type="radio"/> Select date <input type="radio"/> Duration until removal (in hours)		
		<input type="text"/>	<input type="button" value="📅"/>	
				<input type="button" value="Back"/> <input type="button" value="Next &gt;"/>

- **Network type:** In the list, choose **Standard**, **Legacy Hotspot**, or **Hotspot 2.0** to set the network type you plan to use.
- **Network name:** Type the SSID that is seen in the list of available networks for the device. Does not apply to **Hotspot 2.0**.
- **Hide network:** Choose whether the network is hidden.
- **Automatically join this wireless network:** Choose whether a device joins the network automatically. If a device is connected to another network, it doesn't join this network. The user must disconnect from the previous network before the device automatically connects. The default is **On**.

- **Disable captive network detection:** The captive network assistant helps users access subscription or Wi-Fi Hotspot networks. You typically find these networks in coffee shops, hotels, and other public locations. If **On**, devices can still connect to captive networks, but the user must open a browser and log in manually. The default is **Off**.
- **Use static MAC address:** MAC addresses are unique identifiers a device transmits within a network. To increase privacy, iOS and iPadOS devices can use a different MAC address each time they connect to a network. If **On**, the device always uses the same MAC address when connecting to this network. If **Off**, the device uses a different MAC address every time it connects to this network. The default is **Off**.
- **Security type:** In the list, choose the security type you plan to use. Does not apply to **Hotspot 2.0**.
  - None - Requires no further configuration.
  - WEP
  - WPA/WPA2/WPA3 Personal
  - Any (Personal)
  - WEP Enterprise
  - WPA/WPA2/WPA3 Enterprise: For the latest release of Windows 10, configure the Simple Certificate Enrollment Protocol (SCEP) to use WPA-2 Enterprise. Endpoint Management can then send the certificate to the devices to authenticate to the Wi-Fi server. To configure SCEP, go to the Distribution page of **Settings > Credential Providers**. For more information, see [Credential providers](#).
  - Any (Enterprise)

The following sections list the options you configure for each of the preceding connection types.

- **Proxy server settings**
  - **Proxy configuration:** In the list, choose **None**, **Manual**, or **Automatic** to set how the VPN connection routes through a proxy server and then configure any additional options. The default is **None**, which requires no further configuration.
  - If you choose **Manual**, configure these settings:
    - \* **Host name or IP address:** Type the host name or IP address of the proxy server.
    - \* **Port:** Type the proxy server port number.
    - \* **User name:** Type an optional user name to authenticate to the proxy server.
    - \* **Password:** Type an optional password to authenticate to the proxy server.
  - If you choose **Automatic**, configure these settings:
    - \* **Server URL:** Type the URL of the PAC file that defines the proxy configuration.
    - \* **Allow direct connection if PAC is unreachable:** Choose whether to allow users to connect directly to the destination if the PAC file is unreachable. The default is **On**.
- **Fast Lane QoS marking:** If you don't restrict QoS marking for a Wi-Fi network that supports

Cisco Fast Lane QoS, all apps are allowed to use L2 and L3 marking. If you restrict QoS marking, specify the apps that can use L2 and L3 marking.

- **Enable QoS marking:** If you restrict QoS marking, use this setting to disable it completely or only mark certain apps. If **Off**, you disable QoS marking entirely. If **On**, configure a list of apps that can use QoS marking. The default is **On**.
  - **Allow Apple audio/video calling:** Choose whether audio and video calling apps can use QoS marking. If **Off**, the quality of video and audio calls can suffer.
  - **Allow specific apps:** Add an app package ID to this list to allow the app to use QoS marking.
- **Hotspot 2.0 settings**
    - **Displayed operator name:** The friendly name broadcast by the Hotspot device. Users see this name in their list of available Wi-Fi networks.
    - **Domain name:** The domain name used for Hotspot 2.0 negotiation.
    - **Allow connecting to roaming partner networks:** If **On**, devices roaming off their home network can connect to partner networks.
    - **Roaming Consortium Organization Identifiers (OI):** Add a list of organization identifiers the device can access. A Roaming Consortium OI belongs to an organization with shared authentication methods. If the Hotspot you configure isn't available, the device connects to a Roaming Consortium OI listed here.
    - **Network Access Identifier (NAI) realm names:** Configure a list of realm names used to identify users to a roaming network. A NAI transmits in the form `user@realm`.
    - **Mobile Country Codes (MCCs) and Mobile Network Configurations (MNCs):** A Mobile Country Code consists of three digits that identify the country of a network. The Mobile Network Code consists of 2 or 3 unique digits. When used together, the MCC/MNC uniquely identifies a mobile network operator or carrier.
  - **Policy settings**
    - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
      - \* **Select date:** Click the calendar to select the specific date for removal.
      - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
    - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field. Not available for iOS.

**WPA, WPA Personal, Any (Personal) settings for iOS**

**Password:** Type an optional password. If you leave this field blank, users might be prompted for their passwords when they log on.

**WEP Enterprise, WPA Enterprise, WPA2 Enterprise, WPA3 Enterprise, Any (Enterprise) settings for iOS**

When you choose any of these security types, EAP settings appear after **QoS settings**.

**Important:**

If you select the **WPA2 Enterprise** security type, you must allow at least one EAP protocol.

- **Allowed EAP protocols:** Enable the EAP types you want to support and then configure the associated settings. The default is **Off** for each of the available EAP type.
- **Inner authentication (TTLS):** *Required only when you enable TTLS.* In the list, choose the inner authentication method to use. Options are: **PAP**, **CHAP**, **MSCHAP**, or **MSCHAPv2**. The default is **MSCHAPv2**.
- **EAP-FAST with PAC:** Choose whether to use protected access credentials (PACs).
  - If you choose **Use PAC**, choose whether to use a provisioning PAC.
    - \* If you choose **Provisioning PAC**, choose whether to allow an anonymous TLS handshake between the end-user client and Endpoint Management.
      - **Provisioning PAC anonymously**
- **Authentication:**
  - **User name:** Type a user name.
  - **Per-connection password:** Choose whether to require a password each time that users log on.
  - **Password:** Type an optional password. If you leave this field blank, users might be prompted for their passwords when they log on.
  - **Identity credential (keystore or PKI credential):** In the list, choose the type of identity credential. The default is **None**.
  - **Outer identity:** *Required only when you enable PEAP, TTLS, or EAP-FAST.* Type the externally visible user name. You can increase security by typing a generic term such as “anonymous” so that the user name isn’t visible.
  - **Require a TLS certificate:** Choose whether to require a TLS certificate.
- **Trust**
  - **Trusted certificates:** To add a trusted certificate, click **Add** and, for each certificate you want to add, do the following:
    - \* **Application:** In the list, choose the application you want to add.
    - \* Click **Save** to save the certificate or click **Cancel**.
  - **Trusted server certificate names:** To add trusted server certificate common names, click

**Add** and, for each name you want to add, do the following:

- \* **Certificate:** Type the name of the server certificate. You can use wildcards to specify the name, such as wpa.\*.example.com.
- \* Click **Save** to save the certificate name or click **Cancel**.
- **Allow trust exceptions:** Choose whether the certificate trust dialog appears on users devices when a certificate is untrusted. The default is **On**.

## macOS settings

The screenshot displays the 'Network' configuration page for macOS. The left-hand navigation pane shows 'Device Policies' with a sub-section 'Platforms' where 'macOS' is selected. The main content area is titled 'Network' and includes the following settings:

- Network:** Wi-Fi
- Network type:** Standard
- Network name:** (empty field)
- Hide network:** (toggle off)
- Automatically join this wireless network:** (toggle on)
- Security type:** None
- Priority:** 0
- Proxy server settings:** Proxy configuration: None
- Policy settings:**
  - Remove policy:** Select date (selected)
  - Duration until removal (in hours): (empty field)
  - Allow user to remove policy:** Always
  - Profile scope:** User

At the bottom right, there are 'Back' and 'Next >' buttons, and the text 'macOS 10.7+' is visible.

- **Network:** In the list, choose the network option you plan to use. The default is **Wi-Fi**.
  - Wi-Fi
  - Global Ethernet
  - First Active Ethernet
  - Second Active Ethernet
  - Third Active Ethernet
  - First Ethernet
  - Second Ethernet

- Third Ethernet
- **Network type:** In the list, choose **Standard**, **Legacy Hotspot**, or **Hotspot 2.0** to set the network type you plan to use.
- **Network name:** Type the SSID that is seen in the list of available networks for the device. Does not apply to **Hotspot 2.0**.
- **Hide network:** Choose whether the network is hidden.
- **Automatically join this wireless network:** Choose whether the network is joined automatically. If a device is already connected to another network, it doesn't join this network. The user must disconnect from the previous network before the device automatically connects. The default is **On**.
- **Security type:** In the list, choose the security type you plan to use. Does not apply to **Hotspot 2.0**.
  - None - Requires no further configuration.
  - WEP
  - WPA/WPA2 Personal
  - Any (Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Any (Enterprise)

The following sections list the options you configure for each of the preceding connection types.

- **Priority:** For multiple networks, type a number to define the priority of the network connection. The device connects to the network with the lowest priority number first. Negative numbers are acceptable. The default is **0**.
- **Proxy server settings**
  - **Proxy configuration:** In the list, choose **None**, **Manual**, or **Automatic** to set how the VPN connection routes through a proxy server and then configure any additional options. The default is **None**, which requires no further configuration.
  - If you choose **Manual**, configure these settings:
    - \* **Host name or IP address:** Type the host name or IP address of the proxy server.
    - \* **Port:** Type the proxy server port number.
    - \* **User name:** Type an optional user name to authenticate to the proxy server.
    - \* **Password:** Type an optional password to authenticate to the proxy server.
  - If you choose **Automatic**, configure these settings:
    - \* **Server URL:** Type the URL of the PAC file that defines the proxy configuration.
    - \* **Allow direct connection if PAC is unreachable:** Choose whether to allow users to connect directly to the destination if the PAC file is unreachable. The default is **On**.

- **Hotspot 2.0 settings**

- **Displayed operator name:** The friendly name broadcast by the Hotspot device. Users see this name in their list of available Wi-Fi networks.
- **Domain name:** The domain name used for Hotspot 2.0 negotiation.
- **Allow connecting to roaming partner networks:** If **On**, devices roaming off their home network can connect to partner networks.
- **Roaming Consortium Organization Identifiers (OI):** Add a list of organization identifiers the device can access. A Roaming Consortium OI belongs to an organization with shared authentication methods. If the Hotspot you configure isn't available, the device connects to a Roaming Consortium OI listed here.
- **Network Access Identifier (NAI) realm names:** Configure a list of realm names used to identify users to a roaming network. A NAI transmits in the form `user@realm`.
- **Mobile Country Codes (MCCs) and Mobile Network Configurations (MNCs):** A Mobile Country Code consists of three digits that identify the country of a network. The Mobile Network Code consists of 2 or 3 unique digits. When used together, the MCC/MNC uniquely identifies a mobile network operator or carrier.

- **Policy settings**

- **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
  - \* **Select date:** Click the calendar to select the specific date for removal.
  - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
- **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
- **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

### **WPA, WPA Personal, WPA 2 Personal, Any (Personal) settings for macOS**

- **Password:** Type an optional password. If you leave this field blank, users might be prompted for their passwords when they log on.

### **WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise) settings for macOS**

- **Connection mode:** If **On**, choose the connection mode to use when the user joins the network. The default is **Off**.
  - **System:** If marked, the device uses the system credentials to authenticate the user. The default is cleared.

- **Login window:** If marked, the device uses the same credentials entered at the login window to authenticate the user. The default is cleared.

When you choose any of these security types, EAP settings appear after **QoS settings**.

**Important:**

If you select the **WPA2 Enterprise** security type, you must allow at least one EAP protocol.

- **Allowed EAP protocols:** Enable the EAP types you want to support and then configure the associated settings. The default is **Off** for each of the available EAP type.
- **Inner authentication (TTLS):** *Required only when you enable TTLS.* In the list, choose the inner authentication method to use. Options are: **PAP**, **CHAP**, **MSCHAP**, or **MSCHAPv2**. The default is **MSCHAPv2**.
- **EAP-FAST with PAC:** Choose whether to use protected access credentials (PACs).
  - If you select **Use PAC**, choose whether to use a provisioning PAC.
    - \* If you choose **Provisioning PAC**, choose whether to allow an anonymous TLS handshake between the end-user client and Endpoint Management.
      - **Provisioning PAC anonymously**
- **Authentication:**
  - **Use Active Directory authentication:** Choose whether to enable Active Directory authentication. Available for macOS 10.7 and later. To make this option available, complete the following:
    - \* Set **PEAP** as the EAP protocol.
    - \* Set the profile scope to **System**. You can use this setting option only when you apply the policy to the entire system.
  - **User name:** Type a user name.
  - **Per-connection password:** Choose whether to require a password each time users log on.
  - **Password:** Type an optional password. If you leave this field blank, users might be prompted for their passwords when they log on.
  - **Identity credential (keystore or PKI credential):** In the list, choose the type of identity credential. The default is **None**.
  - **Outer identity:** *Required only when you enable PEAP, TTLS, or EAP-FAST.* Type the externally visible user name. You can increase security by typing a generic term like “anonymous” so that the user name isn’t visible.
  - **Require a TLS certificate:** Choose whether to require a TLS certificate.
- **Trust**
  - **Trusted certificates:** To add a trusted certificate, click **Add** and, for each certificate you want to add, do the following:
    - \* **Application:** In the list, choose the application you want to add.
    - \* Click **Save** to save the certificate or click **Cancel**.



- **Trusted server certificate names:** To add trusted server certificate common names, click **Add** and, for each name you want to add, do the following:
  - \* **Certificate:** Type the name of the server certificate you want to add. You can use wildcards to specify the name, such as wpa\*.example.com.
  - \* Click **Save** to save the certificate name or click **Cancel**.
- **Allow trust exceptions:** Choose whether the certificate trust dialog appears on user devices when a certificate is untrusted. The default is **On**.

## Android Enterprise and Android for Workspace (Preview) settings

The screenshot displays the 'Network' configuration page in the Citrix Endpoint Management console. The left-hand navigation pane shows a list of platforms: iOS, macOS, TV OS, Android (legacy DA), **Android Enterprise** (checked), and Windows Phone. The main content area is titled 'Network' and includes a sub-header 'This policy lets you configure a network profile for devices.' Below this, there are several configuration fields: 'Network name' (text input), 'Authentication' (dropdown menu set to 'Open'), 'Encryption' (dropdown menu set to 'WEP'), 'Password' (text input), and 'Hide network' (toggle switch, currently off). A 'Deployment Rules' section is partially visible below. At the bottom right, there are 'Back' and 'Next >' buttons.

- **Network name:** Type the SSID that is in the list of available networks on the user device.
- **Authentication:** In the list, choose the type of security to use with the Wi-Fi connection.
  - Open
  - Shared
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

The following sections list the options you configure for each of the preceding connection types. The default is **Open**.

### Open, Shared settings for Android Enterprise

- **Encryption:** In the list, choose either **Disabled** or **WEP**. The default is **WEP**.
- **Password:** Type an optional password.

- **Hide network:** Choose whether the network is hidden.

### WPA, WPA-PSK, WPA2, WPA2-PSK settings for Android

- **Encryption:** In the list, choose either **TKIP** or **AES**. The default is **TKIP**.
- **Password:** Type an optional password.
- **Hide network:** Choose whether the network is hidden.

### 802.1x settings for Android

- **EAP Type:** In the list, choose **PEAP**, **TLS**, or **TTLS**. The default is **PEAP**.
- **Password:** Type an optional password.
- **Authentication phase 2:** In the list, choose **None**, **PAP**, **MSCHAP**, **MSCHAPPv2**, or **GTC**. The default is **PAP**.
- **Identity:** Type the optional user name and domain.
- **Anonymous:** Type the optional, externally visible user name. You can increase security by typing a generic term like “anonymous” so that the user name isn’t visible.
- **CA certificate:** In the list, choose the certificate to use.
- **Identity credential:** In the list, choose the identity credential to use. The default is **None**.
- **Hide network:** Choose whether the network is hidden.

### Android (legacy DA) settings

The screenshot displays the 'Network' configuration interface. On the left, a sidebar lists various platform policies, with 'Android (legacy DA)' checked. The main area is titled 'Network' and contains the following fields:

- Network name:** A text input field with a help icon.
- Authentication:** A dropdown menu currently set to 'Open'.
- Encryption:** A dropdown menu currently set to 'WEP'.
- Password:** A text input field with a help icon.
- Hide network:** A toggle switch currently turned off.

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

- **Network name:** Type the SSID that is in the list of available networks on the user device.
- **Authentication:** In the list, choose the type of security to use with the Wi-Fi connection.
  - Open

- Shared (Android Enterprise only)
- WPA (Android Enterprise only)
- WPA-PSK (Android Enterprise only)
- WPA2
- WPA2-PSK
- 802.1x EAP

The following sections list the options you configure for each of the preceding connection types.

### **Open, Shared settings for Android**

- **Encryption:** In the list, choose either **Disabled** or **WEP**. The default is **WEP**.
- **Password:** Type an optional password.
- **Hide network:** Choose whether the network is hidden.

### **WPA, WPA-PSK, WPA2, WPA2-PSK settings for Android**

- **Encryption:** In the list, choose either **TKIP** or **AES**. The default is **TKIP**.
- **Password:** Type an optional password.
- **Hide network:** Choose whether the network is hidden.

### **802.1x settings for Android**

- **EAP type:** In the list, choose **PEAP**, **TLS**, or **TTLS**. The default is **PEAP**.
- **Password:** Type an optional password.
- **Authentication phase 2:** In the list, choose **None**, **PAP**, **MSCHAP**, **MSCHAPPv2**, or **GTC**. The default is **PAP**.
- **Identity:** Type the optional user name and domain.
- **Anonymous:** Type the optional, externally visible user name. You can increase security by typing a generic term like “anonymous” so that the user name isn’t visible.
- **CA certificate:** In the list, choose the certificate to use.
- **Identity credential:** In the list, choose the identity credential to use. The default is **None**.
- **Hide network:** Choose whether the network is hidden.

## Windows Phone settings

The screenshot displays the 'Network' configuration page in the Citrix Endpoint Management console. The left-hand navigation pane is titled 'Network' and lists various platforms: Policy Info, Platforms (with a 'Select All' link), iOS, macOS, TV OS, Android (legacy DA), Android Enterprise, and Windows Phone (which is currently selected and highlighted in blue). The main content area is also titled 'Network' and includes a sub-header: 'This policy lets you configure a network profile for devices.' Below this, there are several configuration options: 'Network name' (a text input field with a help icon), 'Authentication' (a dropdown menu currently set to 'Open'), 'Connect if hidden' (a toggle switch), and 'Connect automatically' (a toggle switch). Under the 'Proxy server settings' section, there are two more text input fields: 'Host name or IP address' and 'Port'. At the bottom right of the main area, there are 'Back' and 'Next >' buttons.

- **Network name:** Type the SSID that is in the list of available networks on the user device.
- **Authentication:** In the list, choose the type of security to use with the Wi-Fi connection.
  - Open
  - WPA Personal
  - WPA-2 Personal
  - WPA-2 Enterprise: For the latest release of Windows 10, configure SCEP to use WPA-2 Enterprise. SCEP configuration enables Endpoint Management to send the certificate to devices to authenticate to the Wi-Fi server. To configure SCEP, go to **Distribution** page of **Settings > Credential Providers**. For more information, see [Credential providers](#).

The following sections list the options you configure for each of the preceding connection types.

### Open settings for Windows Phone

- **Connect if hidden:** Choose whether to connect when the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.

### WPA Personal, WPA-2 Personal settings for Windows Phone

- **Encryption:** In the list, choose either **AES** or **TKIP** to set the type of encryption. The default is **AES**.
- **Shared key:** Provide the encryption key for the method you selected.
- **Connect if hidden:** Choose whether to connect when the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.

## WPA-2 Enterprise settings for Windows Phone

- **Encryption:** In the list, choose either **AES** or **TKIP** to set the type of encryption. The default is **AES**.
- **EAP Type:** in the list, choose either **PEAP-MSCHAPv2** or **TLS** to set the EAP type. The default is **PEAP-MSCHAPv2**.
- **Connect if hidden:** Choose whether to connect when the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.
- **Push certificate via SCEP:** Choose whether to push the certificate to user devices using the SCEP.
- **Credential provider for SCEP:** In the list, choose the SCEP credential provider. The default is **None**.

## Proxy server settings for Windows Phone

- **Host name or IP address:** Type the name or IP address of the proxy server.
- **Port:** Type the port number for the proxy server.

## Windows Desktop/Tablet settings

The screenshot displays the configuration interface for a Network policy. The left-hand navigation pane shows the 'Network' policy selected, with the 'Windows Desktop/Tablet' platform checked. The main configuration area includes the following settings:

- Network name:** A text input field with a help icon.
- Authentication:** A dropdown menu currently set to 'Open'.
- Hide network:** A toggle switch currently turned off.
- Connect automatically:** A toggle switch currently turned off.
- Proxy server settings:**
  - Host name or IP address:** A text input field.
  - Port:** A text input field.
- Deployment Rules:** A section header with a right-pointing arrow.

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

- **Network name:** The SSID seen in the list of available networks.
- **Authentication:** In the list, click the type of security to use with the Wi-Fi connection.

- Open
- WPA Personal
- WPA-2 Personal
- WPA Enterprise
- WPA-2 Enterprise: For the latest release of Windows 10, configure SCEP to use WPA-2 Enterprise. SCEP configuration enables Endpoint Management to send the certificate to devices to authenticate to the Wi-Fi server. To configure SCEP, go to **Distribution** page of **Settings > Credential Providers**. For more information, see [Credential providers](#).

The following sections list the options you configure for each of the preceding connection types.

### **Open settings for Windows 10 and Windows 11**

- **Hide network:** Choose whether the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.

### **WPA Personal, WPA-2 Personal settings for Windows 10 and Windows 11**

- **Encryption:** In the list, choose either **AES** or **TKIP** to set the type of encryption. The default is **AES**.
- **Shared key:** Provide the encryption key for the method you selected.
- **Hide network:** Choose whether the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.

### **WPA-2 Enterprise settings for Windows 10 and Windows 11**

- **Encryption:** In the list, choose either **AES** or **TKIP** to set the type of encryption. The default is **AES**.
- **EAP Type:** in the list, choose either **PEAP-MSCHAPv2** or **TLS** to set the EAP type. The default is **PEAP-MSCHAPv2**.
- **Hide network:** Choose whether the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.
- **Enable SCEP?:** Choose whether to push the certificate to user devices by using SCEP.
- **Credential provider for SCEP:** In the list, choose the SCEP credential provider. The default is **None**.

## Chrome OS settings

Device Policies	Apps	Media	Actions	Content Collaboration	Enrollment Profiles	Delivery Groups
<b>Network</b>						
1 Policy Info						
2 Platforms <a href="#">Select All</a>						
<input type="checkbox"/> iOS						
<input type="checkbox"/> macOS						
<input type="checkbox"/> TV OS						
<input type="checkbox"/> Android (legacy DA)						
<input type="checkbox"/> Android Enterprise						
<input type="checkbox"/> Windows Phone						
<input type="checkbox"/> Windows Desktop/Tablet						
<input checked="" type="checkbox"/> Chrome OS						
<input type="checkbox"/> Workspace Hub						
3 Assignment						
<p><b>Network</b></p> <p>Name * <input type="text"/> ⓘ</p> <p>Priority <input type="text"/> ⓘ</p> <p>Allow gateway ARP polling <input checked="" type="checkbox"/> ⓘ</p> <p>Automatically connect <input type="checkbox"/> ⓘ</p> <p>Hidden SSID <input type="checkbox"/> ⓘ</p> <p>SSID * <input type="text"/> ⓘ</p> <p>Roam threshold <input type="text"/> ⓘ</p> <p>Select the type of security <input type="text" value="None"/> ⓘ</p> <p><a href="#">Back</a> <a href="#">Next &gt;</a></p>						

- **Name:** Type a user-friendly description of this connection. This setting is required.
- **Priority:** For multiple networks, type a number to define the priority of the network connection. The device connects to the network with the lowest priority number first. Negative numbers are acceptable. The default is **0**.
- **Allow gateway ARP Polling:** If **On**, this setting allows ARP messages to be sent to the default gateway to monitor the status of the current connection. Default is **On**.
- **Automatically connect:** If **On**, devices connect to the network automatically when in range. Default is **Off**.
- **Hidden SSID:** When set to **On**, the SSID of the network isn't broadcast. Default is **Off**.
- **SSID:** The SSID seen in the list of available networks on a device.
- **Roam threshold:** Type the roam threshold for this network. This number represents the signal-to-noise value (in dB) below which a device attempts to roam to a new network.
- **Select type of security:** Choose the type of security used with this Wi-Fi connection. Options are **None** and **WPA-PSK**. Default is **None**.
- **Passphrase:** If you select **WPA-PSK** as the security, type the passphrase for the network.

## Citrix Ready workspace hub settings

The screenshot displays the 'Network' configuration page in the Citrix Ready workspace hub settings. The left-hand navigation pane includes sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', the 'Workspace Hub' option is checked and highlighted in teal. The main configuration area is titled 'Network' and includes the following fields:

- Network name \***: A text input field with a help icon.
- Authentication**: A dropdown menu set to 'WPA-2 Enterprise' with a help icon.
- EAP type**: A dropdown menu set to 'Automatic' with a help icon.
- Identity**: A text input field with a help icon.
- Password**: A text input field with a help icon.
- Anonymous**: A text input field with a help icon.
- CA certificate**: A dropdown menu set to 'Select certificate' with a help icon.

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

You can connect to 5 GHz Wi-Fi networks if your Citrix Ready workspace hub device is built on the Raspberry Pi 3 Model B+ platform or later. Configure your device to connect to the network:

- **Name:** Type a user-friendly description of this connection. This setting is required.
- **Authentication:** If **Open**, no authentication is required. If **WPA-2 Enterprise**, configure authentication settings for the device. Default is **Open**.
- **EAP Type:** Select an authentication protocol type. If **Automatic**, the workspace hub device automatically determines the authentication protocol. You can also select **PEAP-MSCHAPv2**. Default is **Automatic**.
- **Identity:** Type a user name for authentication.
- **Password:** Type a password for authentication.
- **Anonymous:** Type an optional, externally visible user name. You can increase security by typing a generic term like “anonymous” so that the user name isn’t visible.
- **CA certificate:** In the list, choose the certificate to use.

To push the network policy to the device, the device must connect using Ethernet. After the device restarts, it connects to the network automatically.



## Network usage device policy

May 8, 2020

You can set network usage rules to specify how iOS devices use networks, such as cellular data networks. The rules apply to managed apps and specified SIMs. Managed apps are apps that you deploy to users' devices through Endpoint Management. They don't include apps that users have downloaded directly to their devices without being deployed through Endpoint Management. They also don't include apps already installed on the devices when the devices were enrolled in Endpoint Management. This policy applies to SIMs for iOS 13 devices. You can configure app rules, SIM rules, or both. SIM rules apply to all managed apps on that device.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### iOS settings

- **Application Rules**
  - **Allow roaming cellular data:** Select whether the specified apps can use a cellular data connection while roaming. The default is **Off**.
  - **Allow cellular data:** Select whether the specified apps can use a cellular data connection. The default is **Off**.
  - **App Identifier Matches:** For each app you want to add to the list, click **Add**, and then configure the following:
    - \* **App Identifier:** Type an app identifier.
  - Click **Save** to save the app to the list or **Cancel** to not save the app to the list.
- **SIM Rules**
  - **SIM Wi-Fi assist policy:** Enabling **Switch from poor Wi-Fi** makes the Wi-Fi assist policy switch from poor Wi-Fi to cellular connections more aggressively. This setting can increase cellular data use and impact battery life.
  - **SIM ICCIDs:** For each SIM you want to add to the list, click **Add**, and then configure the following:
    - \* **ICCID:** Type the 19- or 20-digit number for the SIM card to add.

## Office device policy

September 8, 2021

Endpoint Management lets you deploy Microsoft Office 365 products using the Office configuration

service provider (CSP). By configuring the Office device policy, you can deploy Microsoft Office apps to any devices running Windows 10 (version 1709 or later) or Windows 11.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Windows Desktop/Tablet settings

The screenshot displays the configuration interface for an Office device policy. The left sidebar shows a navigation menu with 'Office' selected, and sub-items for 'Policy Info', 'Platforms', 'Windows Desktop/Tablet' (highlighted), and 'Assignment'. The main content area is titled 'Office' and includes the following settings:

- Product ID:** A dropdown menu set to 'O365ProPlusRetail'.
- Office 365 Apps:** A list of apps with checkboxes. All are checked by default: Access, Excel, OneDrive for Business (Groove), OneDrive for Business (Next Gen Sync Client), OneNote, Outlook, PowerPoint, Publisher, Skype For Business, Word, Project Online Desktop Client, and Visio Pro for Office 365.
- OS Version:** A dropdown menu set to '32-bit'.
- Update channel:** A dropdown menu set to 'Monthly'.
- Properties:** Two toggle switches: 'Automatically accept the app end user license agreement' (ON) and 'User shared computer activation' (OFF).

- **Product ID:** Select a product ID based on your Office 365 plan. Options are **O365ProPlusRetail**, **O365BusinessRetail**, or **O365SmallBusPremRetail**.
- **Office 365 Apps:** Select the Office 365 apps that you want deployed. All apps are selected by default.
- **Additional Office apps:** If you own licenses for **Project Online Desktop Client** or **Visio Pro for Office 365**, you can select these apps to have them installed.
- **Office Version:** Select whether to install the **32-bit** or **64-bit** version of Office.
- **Update channel:** Choose how often you want updates to occur. Options are **Monthly**, **Monthly (Targeted)**, **Semi-Annual**, or **Semi-Annual (Targeted)**.
- **Properties:**
  - **Automatically accept the app end user license agreement:** Select **On** or **Off**. Defaults to **On**.

- **User shared computer activation:** Select whether the computer is shared or not. Options are **On** or **Off**. Defaults to **Off**.
- **Office Language:** Office automatically installs in any languages that Windows already has installed. You can select extra languages to install.

## Organization information device policy

December 17, 2018

The Organization information device policy specifies your organization information for alert messages that are pushed from Endpoint Management to iOS devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### iOS settings

- **Name:** Type the name of the organization running Endpoint Management.
- **Address:** Type the organization's address.
- **Phone:** Type the organization's support phone number.
- **Email:** Type the support email address.
- **Magic:** Type a word or phrase that describes the services managed by the organization.

## OS Update device policy

September 13, 2021

The OS Update device policy lets you deploy:

- The latest OS updates to supervised iOS devices.

The OS Update device policy only works for supervised devices enrolled in Apple Deployment Program.

- The latest OS and app updates to Apple Deployment Program enrolled macOS devices running macOS 10.11.5 and later.
- The latest OS updates to supervised Samsung SAFE devices.

For Samsung SAFE devices, Endpoint Management sends the OS Update policy to Secure Hub, which then applies the policy to the device. The **Manage > Devices** page shows when Endpoint Management sends the policy and when the device receives the policy.

- The latest OS updates to supervised Desktop and Tablet devices running Windows 10 or Windows 11.

You can also use the OS Update policy to manage delivery optimization settings for desktops and tablets running Windows 10 (version 1607 or later) or Windows 11. Delivery optimization is a peer-to-peer client update service provided by Microsoft for Windows 10 and Windows 11 updates. The goal of delivery optimization is to reduce bandwidth issues during the update process. Bandwidth reduction is achieved by sharing the downloading task among multiple devices. For more information, see the Microsoft article, [Configure Delivery Optimization for Windows 10 updates](#).

- The latest OS updates to managed Android Enterprise devices (Android 7.0 and later).
- The latest OS updates to Chrome OS devices.
- The specified OS update file to Citrix Ready workspace hub devices.

### Important:

The OS update policy does not allow you to disable updates entirely. To delay updates up to 90 days, create a restriction policy. See [Restriction device policy](#).

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

**OS update**

This policy lets you deploy OS updates. The policy supports supervised devices. Available for: iOS 10.3+. For devices running a version prior to iOS 10.3, this policy supports devices that are both supervised and enrolled with automated device enrollment.

OS update options \*  Download only ⓘ  
 Download and/or install ⓘ

OS update frequency (1-365 days) \*  ⓘ

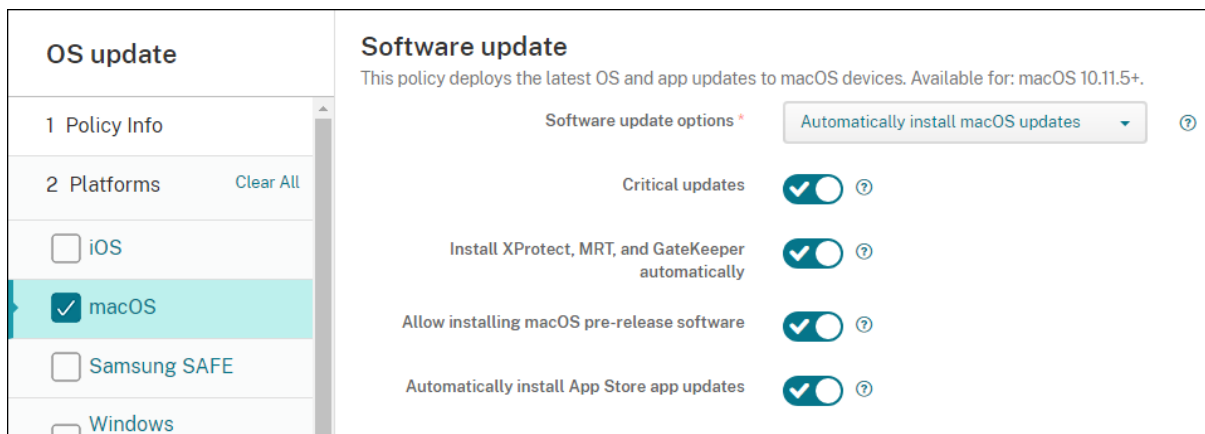
OS update version \*  Latest version ⓘ  
 Specified version only ⓘ  
 ⓘ iOS 11.3+

The following settings are for supervised iOS devices.

- **OS update options:** Both of the options download the latest OS updates to supervised devices according to the **OS update frequency**. The device prompts users to install updates. The prompt is visible after the user unlocks the device.
- **OS update frequency:** Determines how frequently Endpoint Management checks and updates the device OS. The default is **7** days.

- **OS updates version:** Specifies the version to use to update supervised iOS devices. The default is **Latest version**.
  - **Latest version:** Select to update to the latest OS version.
  - **Specific version only:** Select to update to a specific OS version and then type the version number.

## macOS settings



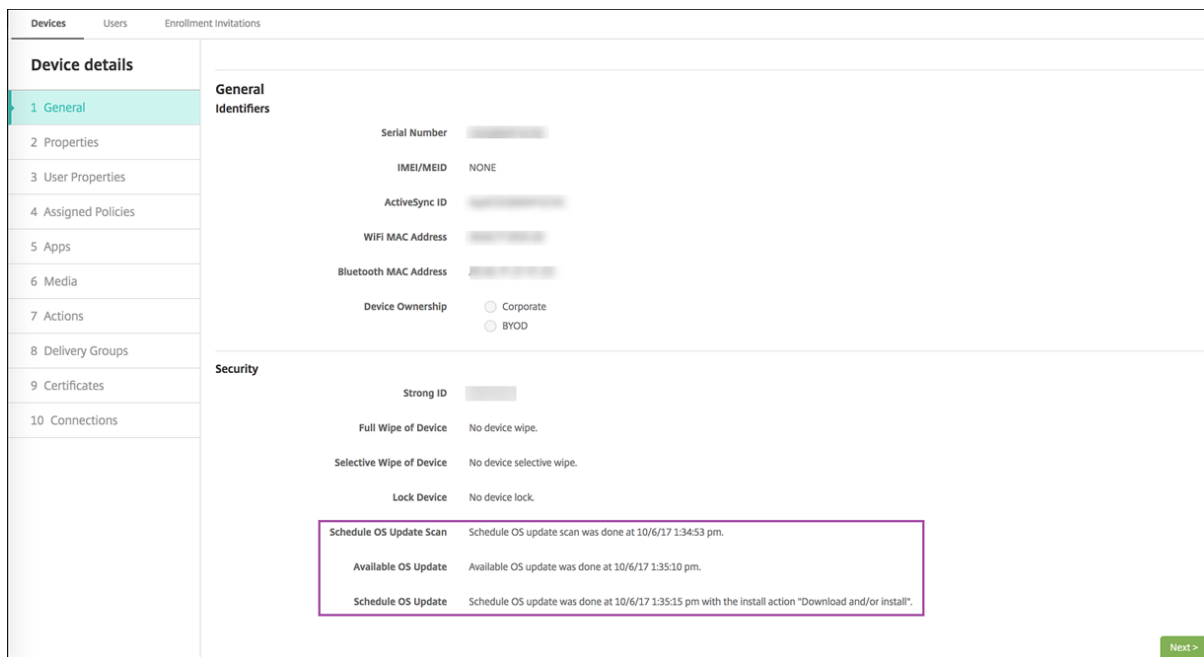
- **Software updates options:** Controls how macOS devices check for and install updates. Select from the following options:
  - **Automatically install macOS updates:** Updates download and install automatically.
  - **Download new updates when available:** Updates download but require manual installation.
  - **Check for updates:** Checks to see if updates exist but doesn't download or install the updates automatically.
  - **Don't check for updates:** Don't check for new updates, download the updates, or install the updates automatically. Users can still install updates manually.
- **Critical updates:** Allow automatic installation of critical macOS updates.
- **Install xProtect, MRT, and GateKeeper updates automatically:** Allow macOS devices to install updates for security software automatically.
- **Allow installation of macOS pre-release software:** Allow users to install pre-release versions of macOS software.
- **Automatically install App Store app updates:** Allow App Store apps to update automatically.

## Get status for iOS and macOS update actions

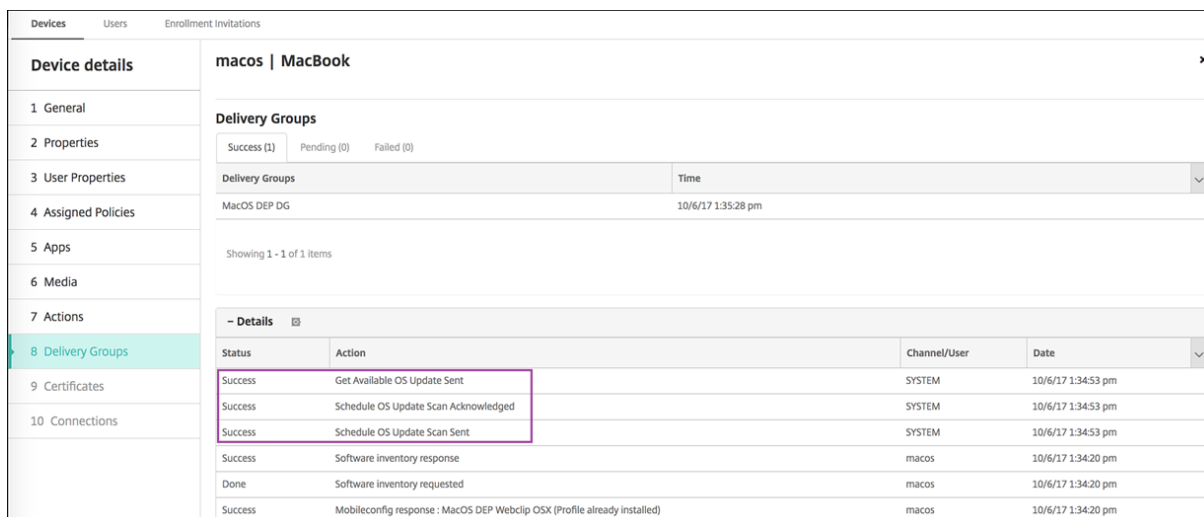
For iOS and macOS, Endpoint Management doesn't deploy the Control OS Update policy to devices. Instead, Endpoint Management uses the policy to send these MDM commands to devices:

- Schedule OS Update Scan: Requests that the device performs a background scan for OS updates. (Optional for iOS)
- Available OS Updates: Queries the device for a list of available OS updates.
- Schedule OS Update: Requests that the device performs macOS updates, app updates, or both. Thus, the device OS determines when it downloads or installs the OS and app updates.

The **Manage > Devices > Device details (General)** page shows the status of scheduled and available OS update scans, and scheduled macOS and app updates.



For more details about the status of update actions, go to the **Manage > Devices > Device details (Delivery Groups)** page.



For details such as available OS updates and the last installation attempt, go to the **Manage > Devices > Device details (Properties)** page.

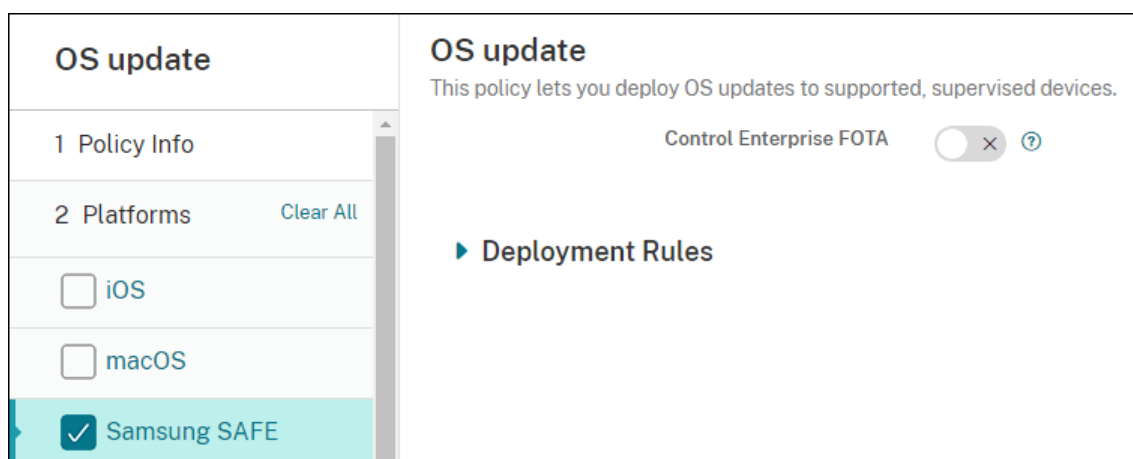
Devices		Users	Enrollment Invitations
<b>Device details</b>		DEP account name	DEP Account FR
1 General		DEP profile assigned	10/6/17 1:08:16 pm
2 Properties		DEP profile pushed	10/6/17 1:08:16 pm
3 User Properties		DEP registration by	[REDACTED]
4 Assigned Policies		DEP registration date	1/20/17 4:42:06 pm
5 Apps		Description	MB 12.0 SPACE GRAY/1.1GHZ/8GB/256GB-FRA
6 Media		Device model	MacBook
7 Actions		Device name	FranckD MacBook
8 Delivery Groups		Model ID	MacBook8,1
9 Certificates		OS Update Install Failure Message	
10 Connections		OS Update Install Status	Success <span>✕</span>
		OS Update Is Critical	No
		OS Update Last Install Attempt	10/6/17 1:35:15 pm
		OS Update Version	macOS Sierra Update, iTunes
		Operating system build	16B2657

Devices		Users	Enrollment Invitations
<b>Device details</b>		<b>Properties</b>	
1 General		-- Custom <span>Add</span>	
2 Properties		AutoCheckEnabled	true
3 User Properties		AutomaticAppInstallationEnabled	false
4 Assigned Policies		AutomaticOSInstallationEnabled	false
5 Apps		AutomaticSecurityUpdatesEnabled	true
6 Media		BackgroundDownloadEnabled	true
7 Actions		CatalogURL	<a href="https://swscan.apple.com/content/catalogs/others/index-10.12-10.11-10.10-10.9-mountainlion-snowleopard-leopard.merged-1.sucatalog.gz" target="">https://swscan.apple.com/content/catalogs/others/index-10.12-10.11-10.10-10.9-mountainlion-snowleopard-leopard.merged-1.sucatalog.gz</a>
8 Delivery Groups		IsDefaultCatalog	true
9 Certificates		PerformPeriodicCheck	true
10 Connections		PreviousScanDate	2017-10-06T11:28:41Z
		PreviousScanResult	0

## Samsung SAFE settings

Samsung Enterprise Firmware-Over-the-Air (E-FOTA), lets you determine when devices get updated and the firmware version to use. To use E-FOTA:

1. Create a Samsung MDM License Key device policy with the keys and license information you received from Samsung. For more information, see [Samsung MDM license key device policy](#).
2. Create a Control OS Updates device policy to enable Enterprise FOTA.



- **Control Enterprise FOTA:** If enabled, Samsung devices check for the latest update and install it automatically. When disabled, users can check for updates and install them manually. The default is disabled.
- **Enterprise FOTA License Key:** Select the License Key to use when checking for updates. You can configure this setting in the Samsung MDM License Key policy.



## Windows Desktop and Tablet settings

OS update	OS update																				
1 Policy Info	This policy lets you deploy OS updates to supported, supervised devices.																				
2 Platforms <span>Clear All</span>	<p><b>Active hours</b></p> <p>Select the active hours mode <span>Not configured</span> ⓘ</p> <p><b>Automatic update</b></p> <p>Automatic update behavior <span>Automatically install and restart</span> ⓘ</p> <p><b>Windows automatic update settings</b></p> <p>Scan for app updates from Microsoft update <span>Not configured</span> ⓘ</p> <p>Specify updates branch <span>Not configured</span> ⓘ</p> <p>Configure number of days to defer feature updates <input type="checkbox"/> ⓘ</p> <p>Configure number of days to defer quality updates <input type="checkbox"/> ⓘ</p> <p>Pause quality updates <span>Not configured</span> ⓘ</p> <p>Allow updates only in approval list <span>Not configured</span> ⓘ</p> <p><b>Internal update server</b></p> <p>Use internal update server <input type="checkbox"/> ⓘ</p> <p><b>Delivery optimization</b></p> <p>Configure delivery optimization * <input type="checkbox"/> ⓘ</p> <p><b>Windows updates</b></p> <p><b>Pending updates</b></p> <table border="1"> <thead> <tr> <th>Update ID</th> <th>Title</th> <th>Description</th> <th>Support information</th> <th>Approval status</th> <th><a href="#">Add</a></th> </tr> </thead> <tbody> <tr> <td colspan="6"> </td> </tr> </tbody> </table> <p><b>Approved updates</b></p> <table border="1"> <thead> <tr> <th>Title</th> <th>Description</th> <th>Support information</th> <th><a href="#">Add</a></th> </tr> </thead> <tbody> <tr> <td colspan="4"> </td> </tr> </tbody> </table>	Update ID	Title	Description	Support information	Approval status	<a href="#">Add</a>							Title	Description	Support information	<a href="#">Add</a>				
Update ID	Title	Description	Support information	Approval status	<a href="#">Add</a>																
Title	Description	Support information	<a href="#">Add</a>																		
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Samsung SAFE <input checked="" type="checkbox"/> Windows Desktop/Tablet <input type="checkbox"/> Android Enterprise <input type="checkbox"/> Chrome OS <input type="checkbox"/> Workspace Hub <input type="checkbox"/> Citrix Ready workspace hub																					
3 Assignment																					

- **Select active hours mode:** Select a mode to configure the active hours for performing OS updates. You can specify a range of hours or a start and end time. After you select a mode, more settings appear: **Specify max range for active hours** or **Active hours start** and **Active hours end**. **Not configured** allows Windows to perform OS updates at any time. Defaults to **Not configured**.
- **Auto update behavior:** Configures the download, install, and restart behavior of the Windows update service on user devices. Defaults to **Auto install and restart**.
  - **Notify user before downloading the update:** Windows notifies users when updates are available. Windows doesn't automatically download and install updates. Users must initiate the download and install actions.
  - **Auto install and notify to schedule device restart:** Windows downloads updates automatically on non-metered networks. Windows installs updates during Automatic Maintenance when the device isn't in use and isn't running on battery power. If Automatic Maintenance can't install updates for two days, Windows Update installs the updates immediately. If the installation requires a restart, Windows prompts the user to schedule the restart time. The user has up to seven days to schedule the restart. After seven days, Win-

dows forces the device to restart. Enabling the user to control the start time reduces the risk of accidental data loss caused by apps that don't shut down properly on restart.

- **Auto install and restart:** Default setting. Windows downloads updates automatically on non-metered networks. Windows installs updates during Automatic Maintenance when the device isn't in use and isn't running on battery power. If Automatic Maintenance can't install updates for two days, Windows Update installs the updates immediately. If the installation requires a restart, Windows automatically restarts the device when the device is inactive.
- **Auto install and restart at a specified time:** When you choose this option, more settings appear so you can specify the day and time. The default is 3 AM daily. Automatic installation happens at the specified time and device restart occurs after a 15-minute countdown. When Windows is ready to restart, a logged in user can interrupt the 15-minute countdown to delay the restart.
- **Auto install and restart without end-user control:** Windows downloads updates automatically on non-metered networks. Windows installs updates during Automatic Maintenance when the device isn't in use and isn't running on battery power. If Automatic Maintenance can't install updates for two days, Windows Update installs updates immediately. If the installation requires a restart, Windows automatically restarts the device when the device is inactive. This option also sets the user control panel to read-only.
- **Turn off automatic updates:** Disables Windows automatic updates on the device.
- **Scan for app updates from Microsoft update:** Specifies whether Windows accepts updates for other Microsoft apps from the Microsoft update service. Defaults to **Not configured**.
  - **Not configured:** Use this setting if you don't want to configure the behavior. Windows doesn't change the related UI on user devices. Users can accept or reject updates for other Microsoft apps.
  - **Yes:** Windows allows app updates to be installed from the Windows update service. The related setting on the user device is inactive, so the user can't modify the setting.
  - **No:** Windows doesn't allow app updates to be installed from the Windows update service. The related setting on the user device is inactive, so the user can't modify the setting.
- **Specify updates branch:** Specifies which Windows update service branch to use for updates. Defaults to **Not configured**.
  - **Not configured:** Use this setting if you don't want to configure the behavior. Windows doesn't change the related UI on user devices. Users can choose a Windows update service branch.
  - **Current Branch:** Windows receives updates from Current Branch. The related setting on the user device is inactive, so the user can't modify the setting.
  - **Current Branch for Business:** Windows receives updates from Current Branch for Business. The related setting on the user device is inactive, so the user can't modify the setting.

- **Configure number of days to defer feature updates:** If **On**, Windows defers feature updates by the specified number of days and the user can't change the setting. If **Off**, the user can change the number of days to defer feature updates. Defaults to **Off**.
- **Configure number of days to defer quality updates:** If **On**, Windows defers quality updates by the specified number of days and the user can't change the setting. If **Off**, the user can change the number of days to defer quality updates. Defaults to **Off**.
- **Pause quality updates:** Specifies whether to pause quality updates for 35 days. Defaults to **Not configured**.
  - **Not configured:** Use this setting if you don't want to configure the behavior. Windows doesn't change the related UI on user devices. Users can choose to pause quality updates for 35 days.
  - **Yes:** Windows pauses the installation of quality updates from the Windows Update Service for 35 days. The related setting on the user device is inactive, so the user can't modify the setting.
  - **No:** Windows doesn't pause the installation of quality updates from the Windows Update Service. The related setting on the user device is inactive, so the user can't modify the setting.
- **Allow updates only in approval list:** Specifies whether to install only the updates that an MDM server approves. Endpoint Management doesn't support configuring an approved list of updates. Defaults to **Not configured**.
  - **Not configured:** Use this setting if you don't want to configure the behavior. Windows doesn't change the related UI on user devices. Users can choose which updates to allow.
  - **Yes, install only approved updates:** Allows installation of approved updates only.
  - **No, install all applicable updates:** Allows installation of any applicable updates on the device.
- **Use internal update server:** Specifies whether to obtain updates from the Windows update service or an internal update server through Windows Server Update Services (WSUS). If **Off**, devices use the Windows update service. If **On**, devices connect to the specified WSUS server for updates. Defaults to **Off**.
  - **Accept updates signed by entities other than Microsoft:** Specifies whether to accept updates signed by third-party entities other than Microsoft. This feature requires that the device trusts the third-party vendor certificate. Defaults to **Off**.
  - **Allow connection to Microsoft update service:** Allows Windows update on the device to connect periodically to the Microsoft update service, even if the device is configured to get updates from a WSUS server. Defaults to **On**.
  - **WSUS server:** Specify the server URL for the WSUS server.
  - **Alternate intranet server to host updates:** Specify an alternate intranet server URL to host updates and receive reporting information.
- **Configure delivery optimization:** Whether to use delivery optimization for Windows 10 and

Windows 11 Updates. Default is **Off**.

- **Cache size:** The maximum size of the delivery optimization cache. A value of **0** means an unlimited cache. Default is **10** GB.
- **Allow VPN peer caching:** Whether to allow devices to participate in peer caching when connected to the domain network through VPN. When **On**, the device can download from or upload to other domain network devices, either on VPN or on the corporate domain network. Default is **Off**.
- **Download method:** The download method that delivery optimization can use for downloads of Windows Updates, app, and app updates. Default is **HTTP blended with peering behind the same NAT**. Options are:
  - **HTTP only, no peering:** Disables peer-to-peer caching but allows delivery optimization to download content from Windows Update servers or Windows Server Update Services (WSUS) servers.
  - **HTTP blended with peering behind the same NAT:** Enables peer sharing on the same network. The Delivery Optimization cloud service finds other clients that connect to the Internet using the same public IP as the target client. These clients then attempt to connect to other peers on the same network by using their private subnet IP.
  - **HTTP blended with peering across a private group:** Automatically selects a group based on the device Active Directory Domain Services (AD DS) site or the domain the device authenticates to. Peering occurs across internal subnets, between devices that belong to the same group, including devices in remote offices.
  - **HTTP blended with Internet peering:** Enable Internet peer sources for Delivery Optimization.
  - **Simple download mode with no peering:** Disable the use of Delivery Optimization cloud services. Delivery Optimization switches to this mode automatically during these conditions: When the Delivery Optimization cloud services are unavailable, unreachable, or when the content file size is less than 10 MB. In this mode, Delivery Optimization provides a reliable download experience, with no peer-to-peer caching.
  - **Do not use Delivery Optimization and use BITS instead:** Enables clients to use Branch-Cache. For more information, see the Microsoft article, [BranchCache](#).
- **Max download bandwidth:** The maximum download bandwidth in KBs/second. Default is **0**, which means dynamic bandwidth adjustment.
- **Percentage of maximum download bandwidth:** The maximum download bandwidth that delivery optimization can use across all concurrent download activities. The value is a percentage of the available download bandwidth. Default is **0**, which means dynamic adjustment.
- **Max upload bandwidth:** The maximum upload bandwidth in KBs/second. Default is **0**. A value of **0** means unlimited bandwidth.
- **Monthly upload data cap:** The maximum size in GBs that delivery optimization can upload to Internet peers in each calendar month. Default is 20 GB. A value of **0** means unlimited monthly

uploads.

### **How Endpoint Management handles approved updates to Windows Desktop and Tablet devices**

You can specify whether to install only approved updates. Endpoint Management handles the updates as follows:

- For a security update, such as for Windows Defender definitions, Endpoint Management automatically approves the update and sends an install command to the device during the next sync.
- For all other update types, Endpoint Management waits for your approval before sending the install command to the device.

### **Prerequisites**

- You must upload the Microsoft root certificate to the Endpoint Management server as a server certificate.
- For information about importing a server certificate, see “To import a certificate” in [Certificates and authentication](#).

### **To install only approved updates**

1. Go to **Configure > Device Policies** and open the OS Update device policy.
2. Change the **Allow updates only in approval list** setting to **Yes, install only approved updates**.

### **To approve an update**

1. In the OS Update device policy, scroll down to the **Pending updates** table. Endpoint Management obtains the updates listed in the table from the devices.
2. Search for updates with an **Approval status** of **Pending**.
3. Click the row for the update you want to approve and then click the edit icon for that row (in the **Add** column).

Update Id	Title	Description	Support Info	Approval status
b16fea38-0300-4991-84e8-7e001c1e0304	2017-10 Cumulative Update for Windows 10 Version 1703 for x64-based Systems (KB4014167)	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	<a href="http://support.microsoft.com/help/4041676">http://support.microsoft.com/help/4041676</a>	Pending
8727129e-3646-4c13-b3d7-79da36f6621	Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - October 2017 (KB890830)	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Jaxiter, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product; to help protect your computer, you should use an antivirus product.	<a href="http://support.microsoft.com/KB890830">http://support.microsoft.com/KB890830</a>	Pending
eefca5a7-c604-4e6d-a342-1012a96054f7	2017-10 Security Update for Adobe Flash Player for Windows 10 Version 1703 for x64-based Systems (KB4049179)	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	<a href="http://support.microsoft.com/help/4049179">http://support.microsoft.com/help/4049179</a>	Pending

4. To approve the update, click **Approved** and then click **Save**.

Update Id	Title	Description	Support Info	Approval status
b16fea38-	2017-10 Cumulative Update for Windows 10	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the	<a href="http://support.microsoft.com/help/4041676">http://support.microsoft.com/help/4041676</a>	<input type="radio"/> Pending <input type="radio"/> Approved <input type="button" value="Save"/> <input type="button" value="Cancel"/>

**Note:**

Although the Pending updates table includes add and delete commands, those commands don't result in any changes to the Endpoint Management database. Editing approval status is the only action available for pending updates.

To view the Windows update status for a device, go to **Manage > Devices > Properties**.

- Windows updates		Add
Update for Adobe Flash Player for Windows 10 Version 1703 for x64-based Systems (KB4051613)	Approved to install	✕
Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - October 2017 (KB890830)	Approved to install	

When an update publishes, the **Update ID** appears in the first column with a status (Success or Failure). You can create a report or an automated action for devices with failed updates. The date and time of the publication also appears.

**How updates work for first-time and subsequent deployments**

The effect of the OS Update device policy on devices differs for a first-time deployment versus a deployment after devices get updates.

- For Endpoint Management to query a device for updates, you must configure and assign to a delivery group at least one OS Update device policy.  
Endpoint Management queries a device for installable updates during a device MDM sync.
- After the first OS Update device policy deploys, the list of Windows updates is empty because no device has reported yet.
- When the devices in the assigned delivery group report updates, Endpoint Management saves those updates in its database. To approve any reported updates, edit the policy again.

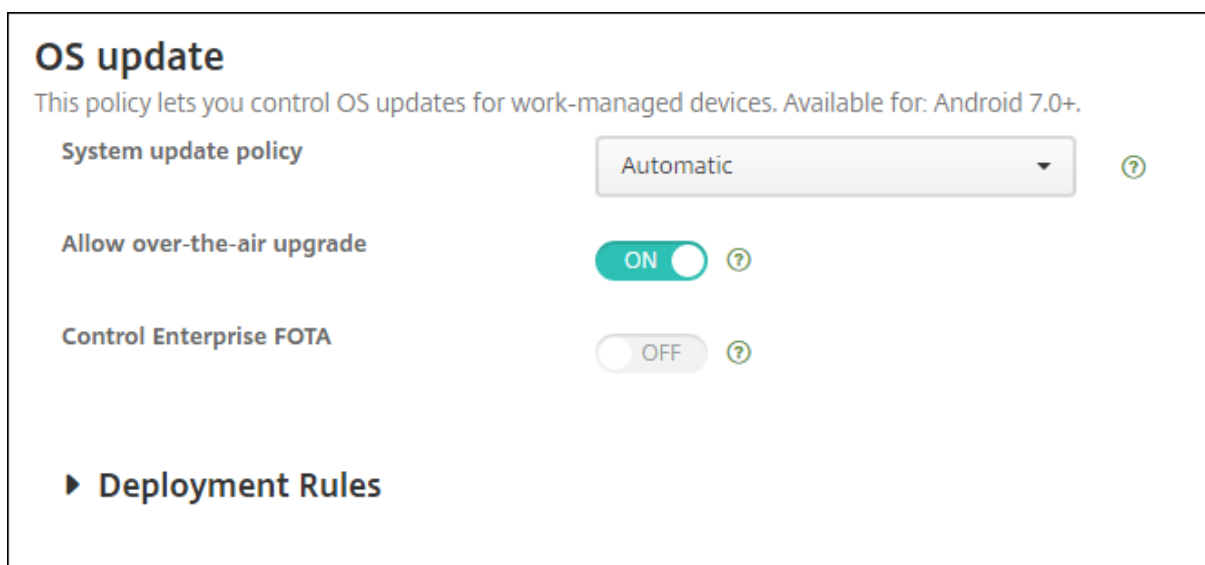
Update approval applies only to the policy you are editing. Updates approved in one policy don't show as approved in another policy. The next time that a device syncs, Endpoint Management sends a command to the device to indicate that the update is approved.

- For a second OS Update device policy, the update list contains the updates stored in the Endpoint Management database. Approve updates for each policy.

During each device sync, Endpoint Management queries the device for the approved update state until the device reports that an update installed. For updates that require a restart after an install, Endpoint Management queries the state of the update until the device reports that the update installed.

- Endpoint Management doesn't restrict the updates shown in the policy configuration page by delivery group or device. All updates reported by devices appear in the list.

## Android Enterprise settings



- **System update policy:** Determines when system updates occur. If you enable the **Control Enterprise FOTA** setting, updates occur automatically, regardless of the configuration for this setting.
  - **Automatic:** Installs an update when it is available.
  - **Windowed:** Installs an update automatically within the daily maintenance window specified in the **Start time** and **End time**.
    - \* **Start time:** The start of the maintenance window, measured as the number of minutes (**0 - 1440**) from midnight in the device local time. Default is **0**.
    - \* **End time:** The end of the maintenance window, measured as the number of minutes (**0 - 1440**) from midnight in the device local time. Default is **120**.
  - **Postpone:** Allows a user to postpone an update for up to 30 days.

- **Allow over-the-air upgrade:** If disabled, user devices can't receive software updates wirelessly. The default is **On**.
- **Control Enterprise FOTA:** If enabled, Samsung devices check for the latest update and install it automatically. When disabled, users can check for updates and install them manually. For Android Enterprise devices running Samsung Knox 3.0 or later. Default is **Off**.
  - **Enterprise FOTA License Key:** Select the License Key to use when checking for updates. You can configure this setting in the Samsung MDM License Key policy. For Android Enterprise devices running Samsung Knox 3.0 or later. Default is **None**. The key can be set using the **Samsung MDM license key** device policy. See [Samsung MDM license key device policy](#).

## Chrome OS settings

- **Update enabled:** Specifies whether to update Chrome OS devices automatically to a newly released version of Chrome OS. Default is **Off**.
- **Reboot after update:** Specifies whether to reboot a Chrome OS device the next time that the user signs out after a successful automatic update. Default is **Off**.
- **Target platform version prefix:** If a device is on an older version, this setting specifies the prefix of the target version to update to. If a device is already on a version with the given prefix, no update occurs. If the device is on a higher version, it remains on the higher version. Rollback isn't supported. Default is empty.

Use one of the following version formats:

- "" or unset: Update to latest version available.
- **10323.:** Update to any minor version of 10323 (for example, 10323.58.0).
- **10323.58.:** Update to any minor version of 10323.58 (for example, 10323.58.0).



- **10323.58.0:** Update to this specific version only.
- **Delay update period:** Specifies how long a device can wait before downloading an update. The delay is counted from the time the update first deploys to the server. The device might wait a portion of this time in terms of clock time and the remaining time based on the number of update checks. The maximum duration value is **14** days. Default is **0**.
- **Release channel:** Specifies the Google release channel used to deliver Chrome OS updates. Requires Google Workspace Chrome configuration.
  - **Delegated:** Means that users can choose the release channel on their devices.
  - **Stable:** The Stable channel is fully tested. By default, Chrome OS updates get distributed over the Stable channel.
  - **Beta:** The preview channel contains upcoming changes and improvements with low risks.
  - **Dev:** The Dev channel contains the latest features and might be unstable.

### Workspace Hub settings

You can use the OS Update device policy to specify an update file for Citrix Ready workspace hub devices. When a workspace hub device checks in with the Endpoint Management server, the device downloads the update file and installs it automatically.

OS update	OS update
1 Policy Info	OS update This policy lets you update the OS of your Citrix Ready workspace hub devices.
2 Platforms <span>Clear All</span>	URL * <input type="text"/> ?
<input type="checkbox"/> iOS	OS version * <input type="text"/> ?
<input type="checkbox"/> macOS	
<input type="checkbox"/> Samsung SAFE	
<input type="checkbox"/> Windows Desktop/Tablet	
<input type="checkbox"/> Android Enterprise	
<input type="checkbox"/> Chrome OS	
<input checked="" type="checkbox"/> Workspace Hub	

- **URL:** The URL where you uploaded the OS update file. First, download the OS update file from the OS vendor and upload it to a share accessible by HTTP or HTTPS. Do not protect the share with any credentials. The update file for a CLASS only applies to devices of the same CLASS.  
  
The URL also must end with the naming used in the OS update file in the format `VERSION-CLASS-KERNEL-ARCHITECTURE-BUILDNUM.lfi`.

When the Citrix Ready workspace hub device checks in with the Endpoint Management server, the device downloads the update file and installs it automatically. The installation happens whether the device has a lower or higher OS version than the one being installed.

The policy applies only on devices of the same CLASS as the update file configured in the policy. For example, if the policy has an update file for an NComputing device (NC class), then only the NComputing devices checking in receive the update. If a ViewSonic device (VS class) checks in, Endpoint Management doesn't apply the update.

- **OS Version:** The OS version in the format `VERSION-CLASS-KERNEL-ARCHITECTURE-BUILDNUM` or `VERSION-CLASS-KERNEL-BUILDNUM`.

## Passcode device policy

October 11, 2021

Create a passcode policy in Endpoint Management based on your organization's standards. You can require passcodes on users' devices and can set various formatting and passcode rules. Create policies for iOS, macOS, Android, Samsung Knox, Android Enterprise, Android for Workspace, Windows Phone, and Windows desktop/tablet. Each platform requires a different set of values, which are described in this article.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### iOS settings

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<h4>Passcode Policy</h4> <p>This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.</p>						
<b>1 Policy Info</b>		<b>Passcode Policy</b>				
<b>2 Platforms</b>		<b>Passcode requirements</b>				
<input checked="" type="checkbox"/> iOS		Passcode required <input checked="" type="checkbox"/> ON				
<input checked="" type="checkbox"/> macOS		Minimum length <input type="text" value="6"/>				
<input checked="" type="checkbox"/> Android		Allow simple passcodes <input checked="" type="checkbox"/> ON ⓘ				
<input checked="" type="checkbox"/> Samsung KNOX		Required characters <input type="checkbox"/> OFF ⓘ				
<input checked="" type="checkbox"/> Android for Work		Minimum number of symbols <input type="text" value="0"/>				
<input checked="" type="checkbox"/> Windows Phone		<b>Passcode security</b>				
<input checked="" type="checkbox"/> Windows Desktop/Tablet		Device lock grace period (minutes of inactivity) <input type="text" value="None"/> ⓘ				
<b>3 Assignment</b>		Lock device after (minutes of inactivity) (0-999) <input type="text" value="None"/>				
		Passcode expiration in days (1-730) <input type="text" value="0"/>				
		Previous passcodes saved (0-50) <input type="text" value="0"/> ⓘ				

- **Passcode required:** Select this option to require a passcode and to display the configuration options for an iOS passcode device policy. The page expands to let you configure settings for passcode requirements, passcode security, and policy settings.
- **Passcode requirements**
  - **Minimum length:** In the list, click the minimum passcode length. The default is **6**.
  - **Allow simple passcodes:** Select whether to allow simple passcodes. Simple passcodes are a repeated or sequential set of characters. The default is **On**.
  - **Required characters:** Select whether to require passcodes to have at least one letter. The default is **Off**.
  - **Minimum number of symbols:** In the list, click the number of symbols the passcode must contain. The default is **0**.
- **Passcode security**
  - **Device lock grace period (minutes of inactivity):** In the list, click the length of time before users must enter a passcode to unlock a locked device. The default is **None**.
  - **Lock device after inactivity:** In the box, enter the length of time a device can be inactive before it is locked. The value can be between 1 and 15 minutes. Set the value to **None** to disable the policy. The default is **None**.
  - **Passcode expiration in days (1-730):** Type the number of days after which the passcode expires. Valid values are 1–730. The default is **0**, which means the passcode never expires.
  - **Previous passwords saved (0-50):** Type the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is **0**, which means users can reuse passwords.
  - **Maximum failed sign-on attempts:** In the list, click the number of times a user can fail to sign in.
    - \* If you set this number higher than 6, after the sixth attempt, the device imposes a time delay between attempts. The time delay increases with each failed attempt. After the final attempt, all data and settings are securely erased.
    - \* If you set the number at 6 or lower, the device is erased without implementing a time delay.
    - \* If you select **Not defined**, after 6 attempts, the devices imposes an increasing time limit between attempts but is not wiped.The default is **Not defined**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

## macOS settings

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<h3>Passcode Policy</h3> <p>This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.</p>						
<p><b>Passcode required</b> <input type="checkbox"/> OFF</p>						
<p>Passcode security</p> <p><b>Delay after failed sign-on attempts, in minutes</b> <input type="text"/></p>						
<p>Policy Settings</p> <p><b>Profile scope</b> <input type="text" value="User"/> macOS 10.7+</p>						
<p>► <b>Deployment Rules</b></p>						
<p>1 Policy Info</p>						
<p>2 Platforms</p> <p><input type="checkbox"/> iOS</p> <p><input checked="" type="checkbox"/> macOS</p> <p><input checked="" type="checkbox"/> Android</p> <p><input checked="" type="checkbox"/> Samsung KNOX</p> <p><input checked="" type="checkbox"/> Android for Work</p> <p><input checked="" type="checkbox"/> Windows Phone</p> <p><input checked="" type="checkbox"/> Windows Desktop/Tablet</p>						
<p>3 Assignment</p>						

- **Passcode required:** Select this option to require a passcode and to display the configuration options for an iOS passcode device policy. The page expands to let you configure settings for passcode requirements, passcode security, and policy settings.
- If **Passcode required** is disabled, next to **Delay after failed sign-on attempts, in minutes**, type the number of minutes to delay before allowing users to reenter their passcodes.
- If you enable **Passcode required**, configure the following settings:
  - **Passcode requirements**
    - **Minimum length:** In the list, click the minimum passcode length. The default is **6**.
    - **Allow simple passcodes:** Select whether to allow simple passcodes. Simple passcodes are a repeated or sequential set of characters. The default is **On**.
    - **Required characters:** Select whether to require passcodes to have at least one letter. The default is **Off**.
    - **Minimum number of symbols:** In the list, click the number of symbols the passcode must contain. The default is **0**.
  - **Passcode security**
    - **Device lock grace period (minutes of inactivity):** In the list, click the length of time before users must enter a passcode to unlock a locked device. The default is **None**.
    - **Lock device after inactivity:** In the list, click the length of time a device can be inactive before it is locked. The value can be between 1 and 5 minutes. Set the value to **None** to disable the policy. The default is **None**.
    - **Passcode expiration in days (1-730):** Type the number of days after which the passcode expires. Valid values are 1–730. The default is **0**, which means the passcode never expires.
    - **Previous passwords saved (0-50):** Type the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is **0**,

which means users can reuse passwords.

- **Maximum failed sign-on attempts:** In the list, click the number of times a user can fail to sign in.
  - \* If you set this number higher than 6, after the sixth attempt, the device imposes a time delay between attempts. The time delay increases with each failed attempt. After the final attempt, the device locks.
  - \* If you set the number at 6 or lower, the device locks without implementing a time delay.
  - \* If you select **Not defined**, after 6 attempts, the device imposes an increasing time limit between attempts but does not lock.

The default is **Not defined**.

- **Delay after failed sign-on attempts, in minutes:** Type the number of minutes before the login window appears after a user reaches the maximum number of failed attempts.
- **Force passcode reset:** If **Off**, users don't need to reset their passcode the next time they authenticate after their device receives this policy. The default is **On**.

- **Policy settings**

- **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
  - \* **Select date:** Click the calendar to select the specific date for removal.
  - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
- **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
- **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

## Android (legacy DA) settings

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<h3>Passcode Policy</h3> <p>This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.</p>						
<p>1 Policy Info</p>						
<p>2 Platforms</p>						
<input type="checkbox"/> iOS						
<input type="checkbox"/> macOS						
<input checked="" type="checkbox"/> Android						
<input checked="" type="checkbox"/> Samsung KNOX						
<input checked="" type="checkbox"/> Android for Work						
<input checked="" type="checkbox"/> Windows Phone						
<input checked="" type="checkbox"/> Windows Desktop/Tablet						
<p>3 Assignment</p>						
<p><b>Passcode Required</b> <input type="radio"/> OFF</p>						
<p>Encryption</p> <p><b>Enable encryption</b> <input type="radio"/> OFF A 3.0+</p>						
<p>Samsung SAFE</p> <p><b>Use same passcode across all users</b> <input type="radio"/> OFF</p>						
<p>► <b>Deployment Rules</b></p>						

### Note:

The default setting for Android is **Off**.

- **Passcode required:** Select this option to require a passcode and to display the configuration options for an Android passcode device policy. The page expands to let you configure settings for passcode requirements, passcode security, encryption, and Samsung SAFE.
- **Passcode requirements**
  - **Minimum length:** In the list, click the minimum passcode length. The default is 6.
  - **Biometric recognition:** Select whether to enable biometric recognition. If you enable this option, the Required characters field is hidden. The default is **Off**.
  - **Required characters:** In the list, click **No Restriction**, **Both numbers and letters**, **Numbers only**, or **Letters only** to configure how passcodes are composed. The default is **No restriction**.
  - **Advanced rules:** Select whether to apply advanced passcode rules. The default is **Off**.
  - When you enable **Advanced rules**, from each of the following lists, click the minimum number of each character type that a passcode must contain:
    - \* **Symbols:** The minimum number of symbols.
    - \* **Letters:** The minimum number of letters.
    - \* **Lowercase letters:** The minimum number of lowercase letters.
    - \* **Uppercase letters:** The minimum number of uppercase letters.
    - \* **Numbers or symbols:** The minimum number of numbers or symbols.
    - \* **Numbers:** The minimum number of numbers.
- **Passcode security**

- **Lock device after inactivity:** In the list, click the length of time a device can be inactive before it is locked. The default is **None**
- **Passcode expiration in days (1-730):** Type the number of days after which the passcode expires. Valid values are 1–730. The default is **0**, which means the passcode never expires.
- **Previous passwords saved (0-50):** Type the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is **0**, which means users can reuse passwords.
- **Maximum failed sign-on attempts:** In the list, click the number of times a user can fail to sign in successfully after which the device is wiped. The default is **Not defined**.

- **Encryption**

- **Enable encryption:** Select whether to enable encryption. The option is available regardless of the **Passcode required** setting.

To encrypt their devices, users must start with a charged battery and keep the device plugged in until encryption completes. The process can take an hour or more. If they interrupt the encryption process, they can lose some or all data on their devices. After a device is encrypted, the process can't be reversed except by doing a factory reset, which erases all the data on the device.

- **Samsung SAFE**

**Note:**

As a workaround for disabling face or Iris recognition on Samsung SAFE devices: Create a Restrictions device policy for Samsung SAFE. In the Restrictions policy, turn on **Disable Applications** and add `com.samsung.android.bio.face.service` or `com.samsung.android.server.iris` to the table. Then, deploy the Restrictions policy.

- **Use same passcode across all users:** Select whether to use the same passcode for all users. The default is **Off**. This setting applies only to Samsung SAFE devices and is available regardless of the **Passcode required** setting.
- When you enable **Use same passcode across all users**, type the passcode to be used by all users in the **Passcode** field.
- When you enable **Passcode required**, configure the following Samsung SAFE settings:
  - \* **Changed characters:** Type the number of characters users must change from their previous passcode. The default is **0**.
  - \* **Times a character can occur:** Type the maximum number of times a character can occur in a passcode. The default is **0**.
  - \* **Alphabetic sequence length:** Type the maximum length of an alphabetic sequence in a passcode. The default is **0**.
  - \* **Numeric sequence length:** Type the maximum length of a numeric sequence in a passcode. The default is **0**.

- \* **Allow users to make password visible:** Select whether users can make their passcodes visible. The default is **On**.
- \* **Configure biometric authentication:** Select whether to enable biometric authentication. The default is **Off**. If you set it to **On**, you can set these options:
  - **Allow fingerprint:** Select to allow users to authenticate using a fingerprint.
  - **Allow iris:** Select to allow users to authenticate using an iris.
- \* **Forbidden strings:** You create forbidden strings to prevent users from using insecure strings that are easy to guess like “password”, “pwd”, “welcome”, “123456”, “111111”, and so on. For each string you want to deny, click **Add** and then do the following:
  - **Forbidden strings:** Type the string users can’t use.
  - Click **Save** to add the string or click **Cancel** to cancel adding the string.

## Samsung Knox settings

The screenshot shows the 'Passcode Policy' configuration page in the Citrix Endpoint Management console. The left-hand navigation pane includes sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', the following options are listed: iOS, macOS, Android, Samsung KNOX (checked), Android for Work (checked), Windows Phone (checked), and Windows Desktop/Tablet (checked). The main content area is titled 'Passcode Policy' and contains the following settings:

- Passcode requirements:** Minimum length is set to 6.
- Allow users to make password visible:** Set to OFF.
- Forbidden Strings:** A section with an 'Add' button.
- Minimum number of:**
  - Changed characters: 0
  - Symbols: 0
- Maximum number of:**
  - Number of times a character can occur: 0
  - Alphabetic sequence length: 0
  - Numeric sequence length: 0

- **Passcode requirements**
  - **Minimum length:** In the list, click the minimum passcode length. The default is **6**.
  - **Allow users to make password visible:** Select whether to let users make the password visible.
  - **Forbidden strings:** You create forbidden strings to prevent users from using insecure strings that are easy to guess like “password”, “pwd”, “welcome”, “123456”, “111111”, and so on. For each string you want to deny, click **Add** and then do the following:
    - \* **Forbidden strings:** Type the string users can’t use.
    - \* Click **Save** to add the string or click **Cancel** to cancel adding the string.
- **Minimum number of**
  - **Changed characters:** Type the number of characters users must change from their previ-



ous passcode. The default is **0**.

- **Symbols:** Type the minimum number of required symbols in a passcode. The default is **0**.

- **Maximum number of**

- **Times a character can occur:** Type the maximum number of times a character can occur in a passcode. The default is **0**.
- **Alphabetic sequence length:** Type the maximum length of an alphabetic sequence in a passcode. The default is **0**.
- **Numeric sequence length:** Type the maximum length of a numeric sequence in a passcode. The default is **0**.

- **Passcode security**

- **Lock device after inactivity:** In the list, click the number of seconds a device can be inactive before it is locked. The default is **None**.
- **Passcode expiration in days (1-730):** Type the number of days after which the passcode expires. Valid values are 1–730. The default is **0**, which means the passcode never expires.
- **Previous passwords saved (0-50):** Type the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is **0**, which means users can reuse passwords.
- **Lock the device after (failed sign-on attempts):** In the list, click the number of times a user can fail to sign on successfully after which the device is locked. The default is **Not defined**.
- **Wipe the device after (failed sign-on attempts):** In the list, click the number of times a user can fail to sign on successfully. After this number of attempts, the Knox container (along with the Knox data) is wiped from the device. Users must reinitialize the Knox container after the wiping occurs. The default is **Not defined**.

## Android Enterprise settings

The screenshot displays the 'Passcode Policy' configuration page in the Citrix Endpoint Management console. The page is divided into a left-hand navigation pane and a main configuration area.

**Navigation Pane:**

- Device Policies (selected)
- Apps
- Media
- Actions
- Content Collaboration
- Enrollment Profiles
- Delivery Groups

**Passcode Policy Configuration:**

**1 Policy Info**

**2 Platforms** Select All

- iOS
- macOS
- Android (legacy DA)
- Samsung KNOX
- Android Enterprise**
- Android Management Api
- Windows Phone
- Windows (Docktop/Tablet)

**Passcode Policy**

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock. Note: When devices running Samsung Knox 3.0 are enrolled in work profile mode, device passcode settings for Knox 3.0 and later do not apply to the device passcode, even if you configure them. The descriptions of these settings tell you which ones these are.

- Device passcode required:**  ON
- Show apps and shortcuts while passcode is not in compliance:**  OFF ⓘ
- Passcode requirements for device passcode:**
  - Minimum length:** 6
  - Allow users to make password visible (Knox 3.0+):**  OFF ⓘ
  - Biometric recognition:**  OFF
  - Required characters:** Numbers only
- Forbidden Strings (Knox 3.0+):** ⓘ

Buttons: Back, Next >

For Android Enterprise devices, you can require a passcode for the device or a security challenge for the Android Enterprise work profile or both.

For devices running Android 8.0 or later and Samsung Knox 3.0 and later, configure settings for Samsung Knox on the **Android Enterprise** page. For devices running earlier versions of Android or Samsung Knox, use the **Samsung Knox** page.

**Note:**

When devices running Samsung Knox 3.0 enroll as work profile devices, device passcode settings for Knox 3.0 and later don't apply, even if configured.

- **Device passcode required:** Requires a passcode on the device. When this setting is **On**, configure the settings under **Passcode requirements for device passcode** and **Passcode security for device passcode**. Default is **Off**.
- **Show apps and shortcuts while passcode is not in compliance:** When this setting is **On**, apps and shortcuts on the device are not hidden, even when the passcode is not compliant. When this setting is **Off**, apps and shortcuts are hidden when the passcode is not compliant. If you enable this setting, Citrix recommends you create an automated action to mark the device as out of compliance when the passcode is not in compliance. Default is **Off**.
- **Passcode requirements for device passcode:**
  - **Minimum length:** Specifies the minimum passcode length. The default is 6.
  - **Allow users to make password visible:** For devices running Samsung Knox 3.0 and later that have a valid Knox license key configured. For fully managed devices only. This setting does not apply to devices enrolled as work profile devices. Allows users to make the password visible. Default is **Off**.
  - **Biometric recognition:** Enables biometric recognition. If this setting is **On**, the **Required characters** field is hidden. The default is **Off**.
  - **Required characters:** Specifies the types of characters required for passcodes. In the list, choose **No Restriction**, **Both numbers and letters**, **Numbers only**, or **Letters only**. Use **No restrictions** only for devices running Android 7.0. Android 7.1 and later don't honor the **No restrictions** setting. The default is **Both numbers and letters**.
  - **Forbidden strings:** For devices running Samsung Knox 3.0 and later that have a valid Knox license key configured. For fully managed devices only. This setting does not apply to devices enrolled as work profile devices. Specifies strings users can't use as passcodes. You create forbidden strings to prevent users from using insecure strings that are easy to guess like "password", "pwd", "welcome", "123456", "111111", and so on. For each string you want to deny: click **Add**; type the string you don't want users to use; click **Save** to add the string or click **Cancel** to cancel adding the string.
  - **Advanced rules:** Applies advanced rules for the types of characters that can occur in passcodes. When this setting is **On**, configure the settings under **Minimum number of** and **Maximum number of**. This setting is not available for Android devices earlier than An-

droid 5.0. The default is **Off**.

- **Minimum number of:**
  - \* **Symbols:** Specifies the minimum number of symbols. Default is **0**.
  - \* **Letters:** Specifies the minimum number of letters. Default is **0**.
  - \* **Lowercase letters:** Specifies the minimum number of lowercase letters. Default is **0**.
  - \* **Uppercase letters:** Specifies the minimum number of uppercase letters. Default is **0**.
  - \* **Numbers or symbols:** Specifies the minimum number of numbers or symbols. Default is **0**.
  - \* **Numbers:** Specifies the minimum number of numbers. Default is **0**.
  - \* **Changed characters:** For devices running Samsung Knox 3.0 and later that have a valid Knox license key configured. For fully managed devices only. This setting does not apply to devices enrolled as work profile devices. Specifies the number of characters users must change from their previous passcode. The default is **0**.
- **Maximum number of:** For devices running Samsung Knox 3.0 and later that have a valid Knox license key configured. For fully managed devices only. This setting does not apply to devices enrolled as work profile devices.
  - \* **Times a character can occur:** Specifies the maximum number of times a character can occur in a passcode. The default is **0**, which means there is no maximum limit.
  - \* **Alphabetic sequence length:** Specifies the maximum length of an alphabetic sequence in a passcode. The default is **0**, which means there is no maximum limit.
  - \* **Numeric sequence length:** Specifies the maximum length of a numeric sequence in a passcode. The default is **0**, which means there is no maximum limit.
- **Passcode security for device passcode:**
  - **Wipe the device after (failed sign-on attempts):** Specifies the number of times a user can fail to sign on after which the device is fully wiped. Default is **Not defined**.
  - **Lock device after inactivity:** Specifies the number of minutes a device can be inactive before it is locked. Set the value to 0 to disable the policy.
  - **Passcode expiration in days (1-730):** Specifies the number of days after which the passcode expires. Valid values are 1-730. The default is **0**, which means the passcode never expires.
  - **Previous passwords saved (0-50):** Specifies the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0-50. Default is **0**, which means users can reuse passwords.
  - **Lock the device after (failed sign-on attempts)** For devices running Samsung Knox 3.0 and later that have a valid Knox license key configured. For fully managed devices only. This setting does not apply to devices enrolled as work profile devices. Specifies the number of times a user can fail to sign on, after which the device is locked. Default is **Not defined**.
- **Work profile security challenge:** Require users to complete a security challenge for access to

apps running in an Android Enterprise work profile. For devices running Android 7.0 and later. When this setting is **On**, configure the settings under **Passcode requirements for work profile security challenge** and **Passcode security for work profile security challenge**. Default is **Off**.

- **Passcode requirements for work profile security challenge:**
  - **Minimum length:** Specifies the minimum passcode length. Default is 6.
  - **Allow users to make password visible:** For devices running Knox 3.0 and later that have a valid Knox license key configured. Allows users to make the password visible. Default is **Off**.
  - **Biometric recognition:** Enables biometric recognition. If this setting is **On**, the **Required characters** field is hidden. The default is **Off**.
  - **Required characters:** Specifies the types of characters required for passcodes. In the list, choose **No Restriction**, **Both numbers and letters**, **Numbers only**, or **Letters only**. Use **No restrictions** only for devices running Android 7.0. Android 7.1 and later don't honor the **No restrictions** setting. The default is **Both numbers and letters**.
  - **Forbidden strings:** For device running Knox 3.0 and later that have a valid Knox license key configured. Specifies strings users can't use as passcodes. You create forbidden strings to prevent users from using insecure strings that are easy to guess like "password", "pwd", "welcome", "123456", "111111", and so on. For each string you want to deny: click **Add**; type the string you don't want users to use; click **Save** to add the string or click **Cancel** to cancel adding the string.
  - **Advanced rules:** Applies advanced rules for the types of characters that can occur in passcodes. When this setting is **On**, configure the settings under **Minimum number of** and **Maximum number of**. This setting is not available for Android devices earlier than Android 5.0. The default is **Off**.
  - **Minimum number of:**
    - \* **Symbols:** Specifies the minimum number of symbols. Default is **0**.
    - \* **Letters:** Specifies the minimum number of letters. Default is **0**.
    - \* **Lowercase letters:** Specifies the minimum number of lowercase letters. Default is **0**.
    - \* **Uppercase letters:** Specifies the minimum number of uppercase letters. Default is **0**.
    - \* **Numbers or symbols:** Specifies the minimum number of numbers or symbols. Default is **0**.
    - \* **Numbers:** Specifies the minimum number of numbers. Default is **0**.
    - \* **Changed characters:** For devices running Knox 3.0 and later that have a valid Knox license key configured. Specifies the number of characters users must change from their previous passcode. The default is **0**.
  - **Maximum number of:** For devices running Knox 3.0 and later that have a valid Knox license key configured.
    - \* **Times a character can occur:** Specifies the maximum number of times a character can occur in a passcode. The default is **0**, which means there is no maximum limit.

- \* **Alphabetic sequence length:** Specifies the maximum length of an alphabetic sequence in a passcode. The default is **0**, which means there is no maximum limit.
- \* **Numeric sequence length:** Specifies the maximum length of a numeric sequence in a passcode. The default is **0**, which means there is no maximum limit.
- **Passcode security for work profile security challenge**
  - **Wipe the container after (failed sign-on attempts):** Specifies the number of times a user can fail to sign on, after which the work profile and its data are wiped from the device. Users must reinitialize the work profile after the wiping occurs. Default is **Not defined**.
  - **Lock container after inactivity:** Specifies the number of minutes a device can be inactive before the work profile is locked. The value can be between 0 and 999 minutes. Set the value to 0 to disable the policy.
  - **Passcode expiration in days (1-730):** Specifies the number of days after which the passcode expires. Valid values are 1–730. The default is **0**, which means the passcode never expires.
  - **Previous passwords saved (0-50):** Specifies the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is **0**, which means users can reuse passwords.
  - **Lock the container after (failed sign-on attempts):** For devices running Knox 3.0 and later that have a valid Knox license key configured. Specifies the number of times a user can fail to sign on, after which the device is locked. Default is **Not defined**.

### Android for Workspace (Preview) settings

- **Password scope:** Select whether you want the passcode policy to apply to the **Device only**, **Work profile only**, or **Device and work profile**. The default is **Device and work profile**.
  - **Device and work profile:** Applies to the whole device for fully managed or dedicated devices. Also applies to the work profile and BYOD devices.
  - **Device only:** Applies to the whole device for fully managed or dedicated devices.
  - **Work profile only:** Applies to the work profile and BYOD devices.
- **Passcode requirements:**
  - **Minimum length:** Specifies the minimum passcode length. The default is 6.
  - **Biometric recognition:** Enables biometric recognition. If this setting is **On**, the **Required characters** field is hidden. The default is **Off**.
  - **Required characters:** Specifies the types of characters required for passcodes. In the list, choose **No Restriction**, **Both numbers and letters**, **Numbers only**, or **Letters only**. Use **No restrictions** only for devices running Android 7.0. Android 7.1 and later don't honor the **No restrictions** setting. The default is **Both numbers and letters**.
  - **Advanced rules:** Applies advanced rules for the types of characters that can occur in passcodes. When this setting is **On**, configure the settings under **Minimum number of** and **Maximum number of**. This setting is not available for Android devices earlier than An-

droid 5.0. The default is **Off**.

– **Minimum number of:**

- \* **Symbols:** Specifies the minimum number of symbols. Default is **0**.
- \* **Letters:** Specifies the minimum number of letters. Default is **0**.
- \* **Lowercase letters:** Specifies the minimum number of lowercase letters. Default is **0**.
- \* **Uppercase letters:** Specifies the minimum number of uppercase letters. Default is **0**.
- \* **Numbers or symbols:** Specifies the minimum number of numbers or symbols. Default is **0**.
- \* **Numbers:** Specifies the minimum number of numbers. Default is **0**.

• **Passcode security:**

- **Wipe the device after (failed sign-on attempts):** Specifies the number of times a user can fail to sign on after which the device is fully wiped. Default is **Not defined**.
- **Lock device after inactivity:** Specifies the number of minutes a device can be inactive before it is locked. Set the value to 0 to disable the policy.
- **Passcode expiration in days (1-730):** Specifies the number of days after which the passcode expires. Valid values are 1–730. The default is **0**, which means the passcode never expires.
- **Previous passwords saved (0-50):** Specifies the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. Default is **0**, which means users can reuse passwords.

## Windows Phone settings

The screenshot displays the 'Passcode Policy' configuration page. On the left, a navigation pane shows 'Windows Phone' selected under '2 Platforms'. The main content area is titled 'Passcode Policy' and includes a description: 'This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.' Below this, several settings are visible: 'Passcode required' is a toggle switch set to 'ON'; 'Allow simple passcodes' is a toggle switch set to 'OFF'; 'Passcode requirements' includes 'Minimum length' (6), 'Characters required' (Letters only), and 'Minimum number of symbols' (1); 'Passcode security' includes 'Lock device after (minutes of inactivity) (0-999)' (0), 'Passcode expiration in 0-730 days \*' (0), 'Previous passwords saved (0-50)' (0), and 'Maximum failed sign-on attempts before wipe (0-999) \*' (0).

- **Passcode required:** Select this option to not require a passcode for Windows Phone devices. The default setting is **On**, which requires a passcode. The page collapses and the following op-

tions disappear when you disable this setting.

- **Allow simple passcodes:** Select whether to allow simple passcodes. Simple passcodes are a repeated or sequential set of characters. The default is Off.
- **Passcode requirements**
  - **Minimum length:** In the list, click the minimum passcode length. The default is **6**.
  - **Characters required:** In the list, click **Numeric or alphanumeric**, **Letters only**, or **Numbers only** to configure how passcodes are composed. The default is **Letters only**.
  - **Minimum number of symbols:** In the list, click the number of symbols the passcode must contain. The default is **1**.
- **Passcode security**
  - **Lock device after inactivity:** Type the number of minutes a device can be inactive before it is locked. The default is **0**.
  - **Passcode expiration in days (1-730):** Type the number of days after which the passcode expires. Valid values are 0–730. The default is **0**, which means the passcode never expires.
  - **Previous passwords saved (0-50):** Type the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is **0**, which means users can reuse passwords.
  - **Wipe the device after (failed sign-on attempts):** Type the number of times a user can fail to sign on successfully after which corporate data is wiped from the device. The default is **0**.

## Windows Desktop/Tablet settings

The screenshot displays the configuration interface for a Passcode Policy. On the left, a navigation pane shows 'Windows Desktop/Tablet' selected under 'Platforms'. The main area is titled 'Passcode Policy' and contains the following settings:

- Passcode required:** A toggle switch is turned ON.
- Passcode security:**
  - Lock device after (minutes of inactivity) (0-999):** Input field with value 0.
  - Passcode expiration in 0-730 days \*:** Input field with value 0.
  - Previous passwords saved (0-24):** Input field with value 0.
- Passcode requirements:**
  - Minimum length:** Dropdown menu set to 6.
- Deployment Rules:** A section header with a right-pointing arrow.

- **Passcode required:** Select this option to not require a passcode for Windows Desktop/Tablet devices. The default setting is **On**, which requires a passcode. The page collapses and the following options disappear when you disable this setting.

- **Passcode security**

- **Lock device after inactivity:** Type the number of minutes a device can be inactive before it is locked. The default is **0**.
- **Passcode expiration in days (0-730):** Type the number of days after which the passcode expires. Valid values are 0–730. The default is **0**, which means the passcode never expires.
- **Previous passwords saved (0-24):** Type the number of used passcodes to save. Users are unable to use any passcode found in this list. Valid values are 1–24. Enter a number between 1 and 24 in this field. The default is **0**.

- **Passcode requirements**

- **Minimum length:** In the list, click the minimum passcode length. The default is **6**.

## Passcode lock grace period device policy

April 15, 2020

The Passcode lock grace period device policy is for shared devices running iOS (iPadOS). For more information about Shared iPads, see [Integrate with Apple Education features](#).

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### iOS settings

- **Passcode Lock Grace Period:** The number of minutes that a Shared iPad screen stays locked before the user must enter a passcode to unlock the screen. Changing this setting to a less restrictive value doesn't take effect until a user signs out. Default is **Immediately**.

By default, the Shared iPad locks itself automatically after two minutes of inactivity.

The screenshot shows the configuration page for the 'Passcode Lock Grace Period Policy'. The left sidebar contains a navigation menu with 'Policy Info', 'Platforms', 'iOS' (selected), and 'Assignment'. The main content area has a title 'Passcode Lock Grace Period Policy' and a description: 'This policy sets the number of minutes that a Shared iPad screen is locked before the user must enter a passcode to unlock the screen. Changing this setting to a less restrictive value doesn't take effect until a user signs out. Available in iOS 9.3.2 and later.' Below the description is a dropdown menu for 'Passcode lock grace period' set to '1 minute'. There is also a 'Deployment Rules' section with a right-pointing arrow.

## Personal hotspot device policy

March 17, 2021



You can allow users to connect to the Internet when they are not in range of a Wi-Fi network by using the cellular data connection through their iOS devices' personal hotspot functionality.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### **iOS settings**

- **Disable personal hotspot:** Select whether to disable the personal hotspot functionality on user devices. The default is **Off**, which switches off the personal hotspot on users devices. This policy does not disable the functionality. Users can still use the personal hotspot on their devices, but when the policy is deployed, the personal hotspot is turned off so that it doesn't remain on by default.

## **Power management device policy**

August 26, 2019

The Power management device policy lets you control how Chrome OS devices respond to idle periods when using AC or battery power.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Chrome OS settings

Category	Setting	Value	Unit
AC	Idle delay *	60000	ms
	Idle warning delay *	60000	ms
	Screen dim delay *	60000	ms
	Screen off delay *	60000	ms
	Idle action	Do Nothing	
Battery	Idle delay *	60000	ms
	Idle warning delay *	60000	ms
	Screen dim delay *	60000	ms
	Screen off delay *	60000	ms
	Idle action	Do Nothing	

The following settings appear for both **AC** and **Battery**.

- **Idle delay:** The length of time without user input before taking the idle action. Specify in minutes. Default for **AC** is **60** minutes. Default for **Battery** is **10** minutes.
- **Idle warning delay:** The length of time without user input before showing a warning dialog. Specify in minutes. Default for **AC** is **58** minutes. Default for **Battery** is **8** minutes. (2 minutes before the **Idle delay** action starts).
- **Screen dim delay:** The length of time without user input before dimming the screen. Specify in minutes. Default for **AC** is **3** minutes. Default for **Battery** is **1** minute.
- **Screen off delay:** The length of time without user input before turning off the screen. Specify in minutes. Default for **AC** is **10** minutes. Default for **Battery** is **3** minutes.
- **Idle action:** Action to take after reaching the idle delay. Options are **Suspend**, **Logout**, **Shutdown**, **Do Nothing**. Default is **Suspend**.

## Profile Removal device policy

March 26, 2020

You can create an app profile removal device policy in Endpoint Management. The policy, when deployed, removes the app profile from users' iOS or macOS devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## macOS settings

The screenshot displays the configuration page for a 'Profile Removal Policy'. The top navigation bar includes 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar shows the policy configuration steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS' is unselected and 'macOS' is selected. The main configuration area includes:

- Profile ID \***: A dropdown menu with the text 'This field is mandatory.'
- Deployment scope**: A dropdown menu with 'User' selected. A note 'macOS 10.7+' is visible to the right.
- Comment**: A text input field.
- Deployment Rules**: A section header with a right-pointing arrow.

- **Profile ID:** In the list, click the app profile ID. This field is required.
- **Deployment scope:** In the list, click either **User** or **System**. The default is **User**. This option is available only on macOS 10.7 and later.
- **Comment:** Type an optional comment.

## Provisioning profile device policy

April 6, 2020

When you develop and code sign an iOS enterprise app, you usually include an enterprise distribution provisioning profile, which Apple requires for the app to run on an iOS device. If a provisioning profile is missing or has expired, the app crashes when a user taps to open it.

The primary problem with provisioning profiles is that they expire one year after they are generated on the Apple Developer Portal and you must keep track of the expiration dates for all your provisioning profiles on all iOS devices enrolled by your users. Tracking the expiration dates not only involves keeping track of the actual expiration dates, but also which users are using which version of the app. Two solutions are to email provisioning profiles to users or to put them on a web portal for download and installation. These solutions work, but they are prone to error because they require users to react to instructions in an email or to go to the web portal and download the correct profile and then install it.

To make this process transparent to users, in Endpoint Management you can install and remove provisioning profiles with device policies. Missing or expired profiles are removed as necessary and the up-to-date profiles are installed on users' devices, so that tapping an app simply opens it for use.

Before you can create a provisioning profile policy, you must create a provisioning profile file. For more information, see the Apple article about how to create a development provisioning profile on the [Apple Developer site](#).

## iOS settings

- **iOS provisioning profile:** Select the provisioning profile file to import by clicking **Browse** and then navigating to the file location.

## Provisioning profile removal device policy

March 23, 2020

A provisioning profile lets you distribute iOS apps to user devices. Apple requires that you sign an app using a provisioning profile to authorize the app to run on iOS devices. For more information, see [Provisioning profile device policy](#).

To remove or replace an older provisioning profile, use the Provisioning profile removal device policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

The screenshot shows the configuration page for a Provisioning Profile Removal Policy. The page is divided into a left sidebar and a main content area. The sidebar contains a list of steps: 1 Policy Info, 2 Platforms (with a 'Clear All' link), 3 Assignment, and a selected 'iOS' option. The main content area has a title 'Provisioning Profile Removal Policy' and a description: 'This policy lets remove a provisioning profile from an iOS device.' Below the description, there is a dropdown menu for 'iOS provisioning profile' with the text 'Select an option' and a 'Comment' text input field. At the bottom of the main content area, there is a section for 'Deployment Rules'.

- **iOS provisioning profile:** In the list, click the provisioning profile you want to remove.
- **Comment:** Optionally, add a comment.

## Proxy device policy

September 2, 2021

The Proxy device policy specifies global HTTP proxy settings for supported iOS devices. You can deploy only one global HTTP proxy policy per device.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Prerequisites

Before deploying this policy, be sure to set all iOS devices for which you want to set a global HTTP proxy into Supervised mode. For details, see [Deploy devices using Apple Configurator 2](#) or [Deploy devices through the Apple Deployment Program](#).

Set deployment rules to enroll devices before sending the Proxy policy to the devices.

## iOS settings

- **Proxy configuration:** Click **Manual** or **Automatic** for how the proxy will be configured on users' devices.
  - If you click **Manual**, configure these settings:
    - \* **Hostname or IP address for the proxy server:** Type the host name or IP address of the proxy server. This field is required.
    - \* **Port for the proxy server:** Type the proxy server port number. This field is required.
    - \* **User name:** Type an optional user name to authenticate to the proxy server.
    - \* **Password:** Type an optional password to authenticate to the proxy server.
  - If you click **Automatic**, configure these settings:
    - \* **Proxy PAC URL:** Type URL of the PAC file that defines the proxy configuration.
    - \* **Allow direct connection if PAC is unreachable:** Select whether to allow users to connect directly to the destination if the PAC file is unreachable. The default is **On**.
- **Allow bypassing proxy to access captive networks:** Select whether to allow bypassing the proxy to access captive networks. The default is **Off**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

## Public session device policy

July 21, 2021

Configure Chrome OS devices to run in a public session that doesn't require a user to sign on. Instead, a public session prompt appears on the sign on screen.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Deploy a public session device

Assign the Public session policy to a specific delivery group rather than the **All Users** group. For information on configuring delivery groups, see [Deploy Resources](#). After successfully enrolling the device and signing out, "Public Session" and the configured display name appears on the sign-on screen.

To remove a device from public session mode:

1. Remove the policy from the delivery group.
2. On the **Manage > Devices** page, select the device and then click **Deploy**.

This action removes the Endpoint Management policies from the device. You can then delete the device from the console.

### Chrome OS settings

- **Public session**
  - **Public session enabled:** Select whether the public session is enabled or disabled. Requires Google Workspace Chrome configuration. Default is **On**.
  - **Display name:** Type a name to display on the sign-on screen of the device.
  - **Session duration in minutes:** Type the number of minutes for the session to last. The systems signs users out after this amount of time. Default is **60**.
- **Security**
  - **Disable Incognito mode:** Don't allow users to browse in Incognito mode. Default is **On**.
  - **Show home button:** Allow users to see the home button in their browser. Default is **Off**.
  - **Disable proceeding from the safe browsing warning page:** Don't allow users to proceed to sites that can be harmful. Default is **On**.
  - **Safe browsing mode:** Turn on a safe browsing mode that warns users when they're about to access a potentially harmful site. Default is **Off**.
  - **Disable saving browsing history:** Don't allow the browser to save browsing history or sync tabs from other Chrome OS devices. Default is **On**.

- **Disable deleting browsing and download history:** Don't allow the user to delete browsing and download history from their session. Users can edit or delete the history database files directly. Default is **On**.
- **Disable bookmarks bar edit:** Don't allow users to edit the bookmarks you've configured. Default is **On**.
- **External storage accessibility:** Select whether users can access external storage devices, such as USB drives. Choose between **DEFAULT**, **READ ONLY**, or **READ WRITE**. Default is **DISABLED**.
- **Allowed websites:** Configure a list of websites that users can access. Wildcard expressions are allowed, such as `http://*.citrix.com`.
- **Blocked websites:** Configure a list of websites that users can't access. Wildcard expressions are allowed.
- **Content**
  - **Home page settings:** Choose what content users see on the home page. Options are **New tab page** and **Home page URL**. Default is **New tab page**.
  - **Pop-up default settings:** Select whether pop-ups are allowed. Default is **Allow pop-ups**.
  - **Pop-ups allowed from these sites:** If you block pop-ups, you can configure specific sites from which to allow pop-ups.
  - **Pop-ups not allowed from these sites:** If you allow pop-ups, you can configure specific sites from which to block pop-ups.
  - **Pages to load on startup:** Configure a list of URLs to be loaded when the session begins.
- **Bookmarks**
  - **Enable bookmarks bar:** If **On**, the bookmarks bar is displayed. Default is **On**.
  - **Folder name:** Type a name for the bookmarks folder.
  - **Bookmark:** Configure a list of bookmarks to appear, including a **Name** and **Bookmark URL**.
- **Chrome apps**
  - **App install allowed:** Select whether users can install apps or not. Options are **Allowed**, **Not allowed**, or **Unspecified**. If you choose **Unspecified**, the device default occurs. Default is **Allowed**.
  - You can also configure a list of apps to allow or block.
    - \* **App name:** Type a name for the app.
    - \* **App ID:** Type the app ID for the app.
    - \* **App install allowed:** Select whether this app is **Allowed**, **Not allowed**, or **Unspecified**. Default is **Allowed**.
    - \* **Installed:** If **On**, the app installs on the device automatically. Default is **Off**.
    - \* **Pinned:** If **On**, the app is pinned to the task bar. Default is **Off**.
    - \* **URL:** Type the app URL.
    - \* **Extension policy:** Type JSON parameters or a URL specific to the app you're config-

uring.

## Restrictions device policy

October 21, 2021

### Note:

When an upgrade includes new Restrictions device policy settings, you must edit and save the policy. Endpoint Management doesn't deploy the upgraded Restrictions device policy until you save it.

The Restrictions device policy allows or restricts certain features or functionality on user devices, such as the camera. You can set security restrictions and restrictions on media content. You can also set restrictions on the types of apps users can and cannot install. Most of the restriction settings default to **On**, or *allows*. The main exceptions are the iOS Security - Force feature and all Windows Tablet features, which default to **Off**, or *restricts*.

Any option for which you select **On** means that the user can perform the operation or use the feature. For example:

- **Camera:** If **On**, the user can use the camera on their device. If **Off**, the user cannot use the camera on their device.
- **Screenshots:** If **On**, the user can take screenshots on their device. If **Off**, the user cannot take screenshots on their device.

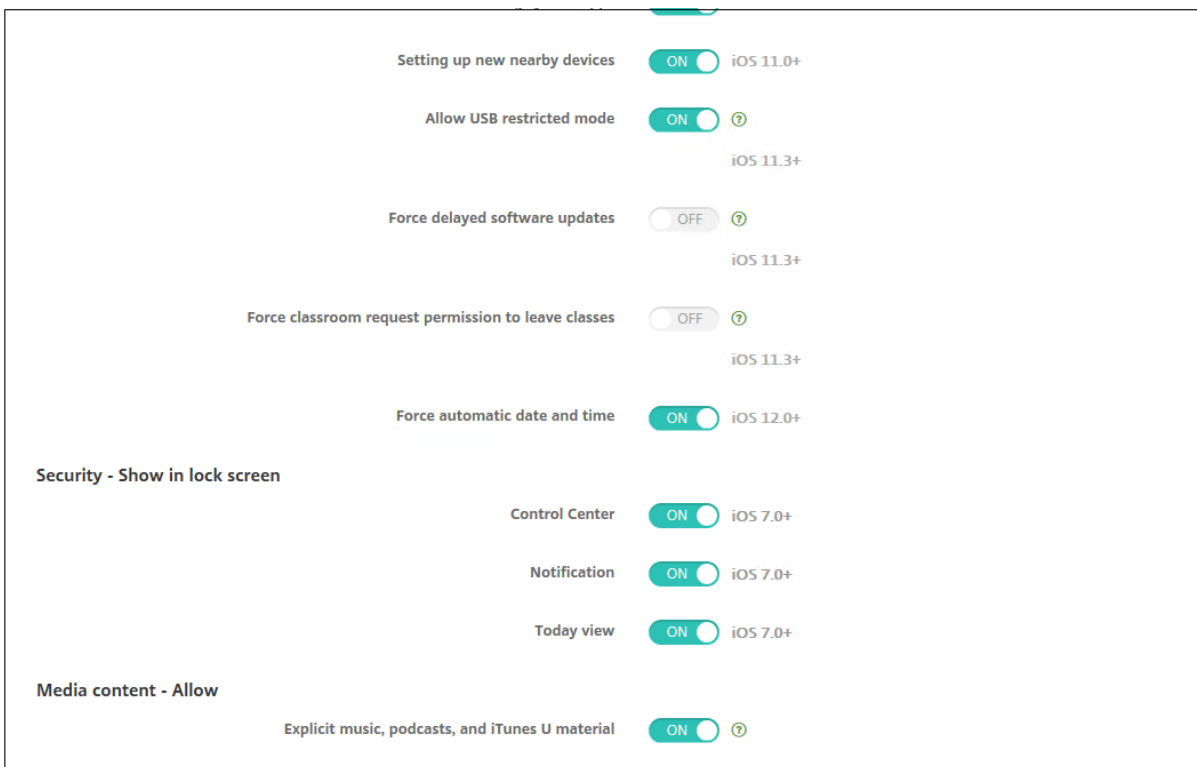
For Windows 10 RS2 Phone: After a Custom XML policy or Restrictions policy that disables Internet Explorer deploys to the phone, the browser remains enabled. To work around this issue, restart the phone. This issue is a third-party issue.

If you have both the restrictions device policy and the kiosk device policy configured, the restrictions device policy takes precedence.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).



## iOS settings



Some iOS restrictions policy settings apply only to specific versions of iOS, as noted here and in the Endpoint Management console Restrictions policy page.

These settings apply when the device is enrolled in user enrollment mode, unsupervised (full MDM) mode, or supervised mode. The following table shows the enrollment modes that are available for each setting for iOS 13 and later.

- **Automated Device Enrollment:** Supervised devices. These are devices enrolled through bulk enrollment.
- **Device Enrollment:** Unsupervised devices. These devices are individually enrolled and the entire device is fully MDM.
- **User Enrollment:** Devices on which only specific users are managed. For more information about User Enrollment, see the Apple documentation.

iOS restrictions policy settings might apply when the device is enrolled in user enrollment mode, unsupervised (full MDM) mode, or supervised mode. The following table shows the enrollment modes that are available for each restrictions policy setting for iOS 13 and later.

**Apple Enrollment Type**

Automated Device Enrollment

Device Enrollment

User Enrollment

As noted in the table, some settings that were previously available in unsupervised and supervised mode are available only in supervised mode starting with iOS 13. The following rules apply:

Some settings that were previously available in unsupervised and supervised mode are available only in supervised mode starting with iOS 13. The following rules apply:

- If a supervised iOS 13+ device enrolls in Endpoint Management, the settings apply to the device.
- If an unsupervised iOS 13+ device enrolls in Endpoint Management, the settings don't apply to the device.
- If an iOS 12 (or lower) device already enrolled in Endpoint Management and then upgrades to iOS 13, there are no changes. The settings apply to the device as they did before the upgrade.

For information on setting an iOS device to supervised mode, see [Deploy devices using Apple Configurator 2](#).

Setting	User Enrollment	Unsupervised	Supervised
<b>Allow hardware controls</b>			
Camera	No	Yes	Yes
FaceTime	No	No	Yes
Screen captures	Yes	No	Yes
Allow the Classroom app to remotely observe student screens	No	No	Yes
Allow the Classroom app to perform AirPlay and View Screen without prompting	No	No	Yes
Photo streams	No	Yes	Yes
Shared photo streams	No	Yes	Yes

Setting	User Enrollment	Unsupervised	Supervised
Allow shared iPad temporary session	No	No	Yes
Voice dialing	No	Yes	Yes
Siri	Yes	Yes	Yes
Allow while device is locked	Yes	Yes	Yes
Siri profanity filter	No	No	Yes
Installing apps	No	No	Yes
Allow global background fetch while roaming	No	Yes	Yes
<b>Allow apps</b>			
Apple App Store	No	No	Yes
In-app purchases	No	Yes	Yes
Require Apple App Store password for purchases	No	Yes	Yes
Safari	No	No	Yes
Autofill	No	No	Yes
Force fraud warning	Yes	Yes	Yes
Enable JavaScript	No	Yes	Yes
Block pop-ups	No	Yes	Yes
Accept cookies	No	Yes	Yes
<b>Network - Allow iCloud actions</b>			
iCloud documents and data	No	No	Yes
iCloud backup	No	Yes	Yes
iCloud photo keychain	No	Yes	Yes
iCloud photo library	No	Yes	Yes

Setting	User Enrollment	Unsupervised	Supervised
<b>Security - Force</b>			
Encrypted backups	Yes	Yes	Yes
Limited ad tracking	No	Yes	Yes
Passcode on first AirPlay pairing	Yes	Yes	Yes
Paired Apple Watch to use Wrist Detection	Yes	Yes	Yes
Sharing managed documents using AirDrop	Yes	Yes	Yes
<b>Security - Allow</b>			
Accepting untrusted SSL certificates	No	Yes	Yes
Automatic update to certificate trust settings	No	Yes	Yes
Require managed pasteboard	Yes	Yes	Yes
Documents from managed apps in unmanaged apps	Yes	Yes	Yes
Unmanaged apps read managed contacts	No	No	Yes
Managed apps write unmanaged contacts	No	No	Yes
Documents from unmanaged apps in managed apps	Yes	Yes	Yes
Diagnostic submission to Apple	Yes	Yes	Yes
Touch ID to unlock device	No	Yes	Yes

Setting	User Enrollment	Unsupervised	Supervised
Passbook notifications when locked	No	Yes	Yes
Handoff	No	Yes	Yes
iCloud sync for managed apps	Yes	Yes	Yes
Backup for enterprise books	Yes	Yes	Yes
Notes and highlights sync for enterprise books	Yes	Yes	Yes
Internet results in Spotlight	No	Yes	Yes
Enterprise app trust	No	Yes	Yes
<b>Supervised only settings - Allow</b>			
Allow eSIM modification	No	No	Yes
Erase all content and settings	No	No	Yes
Screen Time	No	No	Yes
Podcasts	No	No	Yes
Installing configuration profiles	No	No	Yes
Fingerprint modification	No	No	Yes
Installing apps from device	No	No	Yes
Keyboard shortcuts	No	No	Yes
Paired Apple watch	No	No	Yes
Passcode modification	No	No	Yes

Setting	User Enrollment	Unsupervised	Supervised
Device name modification	No	No	Yes
Wallpaper modification	No	No	Yes
Automatically downloading apps	No	No	Yes
AirDrop	No	No	Yes
iMessage	No	No	Yes
Siri user-generated content	No	No	Yes
iBooks	No	No	Yes
Removing apps	No	Yes	Yes
Game Center	No	No	Yes
Add friends	No	No	Yes
Multiplayer gaming	No	No	Yes
Modifying account settings	No	No	Yes
Modifying app cellular data settings	No	No	Yes
Modifying app cellular data settings	No	No	Yes
Allow network drive connections	No	No	Yes
Allow USB device connections	No	No	Yes
Allow Find My iPhone	No	No	Yes
Allow Find My Friends settings	No	No	Yes
Modifying Find My Friends settings	No	No	Yes
Pairing with non-Configurator hosts	No	No	Yes

Setting	User Enrollment	Unsupervised	Supervised
Predictive keyboards	No	No	Yes
Keyboard auto-corrections	No	No	Yes
Keyboard spell-check	No	No	Yes
Allow QuickPath Keyboard	No	No	Yes
Definition lookup	No	No	Yes
<b>Single App bundle ID</b>			
News	No	No	Yes
Apple Music service	No	No	Yes
Apple Music	No	No	Yes
Notifications modification	No	No	Yes
Restricted App usage	No	No	Yes
Diagnostic submission modification	No	No	Yes
Bluetooth modification	No	No	Yes
Allow dictation	No	No	Yes
Modify whether Wi-Fi is on or off	No	No	Yes
Join only Wi-Fi networks installed by a network policy	No	No	Yes
Allow the Classroom app to perform AirPlay and View Screen without prompting	No	No	Yes

Setting	User Enrollment	Unsupervised	Supervised
Allow the Classroom app to lock to an app and lock the device without prompting	No	No	Yes
Automatically join the Classroom app classes without prompting	No	No	Yes
Allow AirPrint	No	No	Yes
Allow storage of AirPrint credentials in Keychain	No	No	Yes
Allow discovery of AirPrint printers by using iBeacons	No	No	Yes
Allow AirPrint only to destinations with trusted certificates	No	No	Yes
Adding VPN configurations	No	No	Yes
Modifying cellular plan settings	No	No	Yes
Removing system apps	No	No	Yes
Setting up new nearby devices	No	No	Yes
Allow USB restricted mode	No	No	Yes
Force delayed software updates	No	No	Yes
Enforced software update delay	No	No	Yes



Setting	User Enrollment	Unsupervised	Supervised
Force classroom request permission to leave classes	No	No	Yes
Force authentication before autofill	No	No	Yes
Force automatic date and time	No	No	Yes
Password AutoFill	No	No	Yes
Password proximity requests	No	No	Yes
Password Sharing	No	No	Yes
Allow personal hotspot modification	No	No	Yes
<b>Security - Show in lock screen</b>			
Control Center	Yes	Yes	Yes
Notification	Yes	Yes	Yes
Today view	Yes	Yes	Yes
<b>Media content - Allow</b>			
Explicit music, podcasts, and iTunes U material	No	No	Yes
Explicit sexual content in iBooks	No	Yes	Yes
Ratings region	No	Yes	Yes
Movies	No	Yes	Yes
TV Shows	No	Yes	Yes
Apps	No	Yes	Yes

- **Allow hardware controls**

- **Camera:** Allow users to use the camera on their devices.

- \* **FaceTime:** Allow users to use FaceTime on their devices. For supervised iOS devices.

- **Screen captures:** Allow users to take screenshots on their devices.
    - \* **Allow the Classroom app to remotely observe student screens:** If this restriction is unselected, an instructor can't use the Classroom app to remotely observe student screens. The default setting is selected, an instructor can use the Classroom app to observe student screens. The setting for **Allow the Classroom app to perform AirPlay and View Screen without prompting** determines whether students receive a prompt to give the instructor permission. For supervised iOS devices.
    - \* **Allow the Classroom app to perform AirPlay and View Screen without prompting:** If this restriction is selected, the instructor can perform AirPlay and View Screen on a student device, without prompting for permission. The default setting is unselected. For supervised iOS devices.
  - **Photo streams:** Allow users to use MyPhotoStream to share photos through iCloud to all their iOS devices.
  - **Shared photo streams:** Allow users to use iCloud Photo Sharing to share photos with coworkers, friends, and family.
  - **Allow shared iPad temporary session:** Prevents access to temporary sessions on shared iPads.
  - **Voice dialing:** Enables voice dialing on user devices.
  - **Siri:** Allows users to use Siri.
    - \* **Allow while device is locked:** Allow users to use Siri while their devices are locked.
    - \* **Siri profanity filter:** Enable the Siri profanity filter. The default is to restrict this feature, which means no profanity filtering is done.  
For more information about Siri and security, see [Siri and dictation policies](#).
  - **Installing apps:** Allow users to install apps. For supervised iOS devices.
  - **Allow global background fetch while roaming:** Allow devices to automatically sync mail accounts to iCloud while the device is roaming. When **Off**, disables global background fetch activity when an iOS phone is roaming. Defaults to **On**.
- **Allow apps**
    - **Apple App Store:** Allow users to access the Apple App Store. For supervised iOS devices.
    - **In-app purchases:** Allow users to make in-app purchases.
      - \* **Require Apple App Store password for purchases:** Require a password for in-app purchases. The default is to restrict this feature, which means no password is required for in-app purchases.
    - **Safari:** Allow users to access Safari. For supervised iOS devices.
      - \* **Autofill:** Allow users to set up autofill for user names and passwords on Safari.
      - \* **Force fraud warning:** If this setting is enabled and users visit a suspected phishing website, Safari alerts users. The default is to restrict this feature, which means no warnings are issued.
      - \* **Enable JavaScript:** Allow JavaScript to run on Safari.

- \* **Block pop-ups:** Block pop-ups while viewing websites. The default is to restrict this feature, which means pop-ups are not blocked.
- **Accept cookies:** Set to what extent cookies are accepted. In the list, choose an option to allow or restrict cookies. The default option is **Always**, which allows all websites to save cookies in Safari. Other options are **Current website only**, **Never**, and **From visited sites only**.
- **Network - Allow iCloud actions**
  - **iCloud documents and data:** Allow users to sync documents and data to iCloud. For supervised iOS devices.
  - **iCloud backup:** Allow users to back up their devices to iCloud.
  - **iCloud keychain:** Allow users to store passwords, Wi-Fi network, credit card, and other information in the iCloud Keychain.
  - **Cloud photo library:** Allow users to access their iCloud photo library.
- **Security - Force**

The default is to restrict the following features, which means no security features are enabled.

  - **Encrypted backups:** Force backups to iCloud to be encrypted.
  - **Limited ad tracking:** Block targeted ad tracking.
  - **Passcode on first Airplay pairing:** Require that AirPlay-enabled devices are verified with a one-time onscreen code before they can use AirPlay.
  - **Paired Apple Watch to use Wrist Detection:** Require a paired Apple Watch to use **Wrist Detection**.
  - **Sharing managed documents using AirDrop:** Setting this option to **On** makes AirDrop appear as an unmanaged drop target.
- **Security - Allow**
  - **Accepting untrusted SSL certificates:** Allow users to accept websites' untrusted SSL certificates.
  - **Automatic update to certificate trust settings:** Allow trusted certificates to be updated automatically.
  - **Require managed pasteboard:** Allow copy and paste functionality to follow the same restrictions that you apply to **Documents from managed apps in unmanaged apps** and **Documents from unmanaged apps in managed apps**.

For example, you configure the following:

    - \* **Require managed pasteboard:** On
    - \* **Documents from managed apps in unmanaged apps:** Off
    - \* **Documents from unmanaged apps in managed apps:** OnAfter you deploy the policy to iOS devices, users can't copy and paste data from managed apps to unmanaged apps, but they can copy and paste data from unmanaged

apps to managed apps.

- **Documents from managed apps in unmanaged apps:** Allow users to move data from managed (corporate) apps to unmanaged (personal) apps.
- **Documents from unmanaged apps in managed apps:** Allow users to move data from unmanaged (personal) apps to managed (corporate) apps.
- **Diagnostic submission to Apple:** Allow anonymous diagnostic data about users' devices to be sent to Apple.
- **Touch ID to unlock device:** Allow users to use their fingerprints to unlock their devices.
- **Passbook notifications when locked:** Allow Passbook notifications to appear on the lock screen.
- **Handoff:** Allow users to transfer activities from one iOS device to another nearby iOS device.
- **iCloud sync for managed apps:** Allow users to sync managed apps to iCloud.
- **Backup for enterprise books:** Allow enterprise books to be backed up to iCloud.
- **Notes and highlights sync for enterprise books:** Allow notes and highlights users have added to enterprise books to be synced to iCloud.
- **Enterprise app trust:** Allow enterprise applications to be trusted. Enterprise apps are any apps that are custom made for your organization. These can be made internally or they can be developed and purchased from an external vendor. For additional information, see [Install custom enterprise apps on iOS](#).
- **Internet results in Spotlight:** Allow Spotlight to show search results from the Internet in addition to the device.
- **Unmanaged apps read managed contacts:** Optional. Only available if **Documents from managed apps in unmanaged apps** is disabled. If this policy is enabled, unmanaged apps can read data from managed accounts' contacts. Default is **Off**. Available as of iOS 12.
- **Managed apps write unmanaged contacts:** Optional. If enabled, allow managed apps to write contacts to unmanaged accounts' contacts. If **Documents from managed apps in unmanaged apps** is enabled, this restriction has no effect. Default is **Off**. Available as of iOS 12.

- **Supervised only settings - Allow**

These settings apply only to supervised devices. For the steps on setting an iOS device to supervised mode, see [Deploy devices using Apple Configurator 2](#).

- **Allow eSIM modification:** Allow users to change the eSIM settings on their device.
- **Erase all content and settings:** Allow users to erase all content and settings from their devices.
- **Screen Time:** Allow users to enable Screen Time.
- **Podcasts:** Allow users to download and sync podcasts.

- **Installing configuration profiles:** Allow users to install a configuration profile other than that the one deployed by you.
- **Fingerprint modification:** Allow users to change or delete their Touch ID fingerprint.
- **Installing apps from device:** Allow users to install apps. Disabling this setting stops end users from installing new apps. The App Store is disabled and its icon is removed from the Home Screen.
- **Keyboard shortcuts:** Allow users to create custom keyboard shortcuts for words or phrases that they use often.
- **Paired Apple watch:** Allow users to pair an Apple Watch to a supervised device.
- **Passcode modification:** Allow users to change the passcode on a supervised device.
- **Device name modification:** Allow users to change the name of their device.
- **Wallpaper modification:** Allow users to change the wallpaper on their devices.
- **Automatically downloading apps:** Allow apps to download.
- **AirDrop:** Allow users to share photos, videos, websites, locations, and more with nearby iOS devices.
- **iMessage:** Allow users to text over Wi-Fi with iMessage.
- **Siri user-generated content:** Allow Siri to query user-generated content from the web. Consumers, not traditional journalists; produce user-generated content. For example, content found on Twitter or Facebook is user-generated.
- **iBooks:** Allow users to use the iBooks app.
- **Removing apps:** Allow users to remove apps from their devices.
- **Game Center:** Allow users to play online games through Game Center on their devices.
  - \* **Add friends:** Allow users to send a notification to a friend to play a game.
  - \* **Multiplayer gaming:** Allow users to start multiplayer game play on their devices.
- **Modifying account settings:** Allow users to modify their device account settings.
- **Modifying app cellular data settings:** Allow users to modify how apps use cellular data.
- **Allow network drive connections:** Prevents connecting to network drives in the Files app.
- **Allow USB device connections:** Prevents connecting to any connected USB devices in the Files app.
- **Allow Find My iPhone:** Disables the **Find My iPhone** option in the Find My app.
- **Allow Find My Friends settings:** Disables the **Find My Friends** option in the Find My app.

- **Modifying Find My Friends settings:** Allow users to change their Find My Friends settings.
- **Pairing with non-Configurator hosts:** Allow the administrator to control to which devices a user device can pair. Disabling this setting prevents pairing except with the supervising host running the Apple Configurator. If no supervising host certificate is configured, all pairing is disabled.
- **Predictive keyboards:** Allow user devices to use the predictive keyboard for suggesting words as they type. Disable this option in situations such as administering standardized tests where you do not want users to have access to suggested words.
- **Keyboard auto-corrections:** Allow user devices to use keyboard autocorrect. Disable this option in situations such as administering standardized tests where you do not want users to have access to autocorrect.
- **Keyboard spell-check:** Allow user devices to use spell checking while typing. Disable this option in situations such as administering standardized tests where you do not want users to have access to the spell-checker.
- **Definition lookup:** Allow user devices to use definition look-up while typing. Disable this option in situations such as administering standardized tests where you do not want users to be able to look up definitions as they type.
- **Single App bundle ID:** Create a list of apps allowed to retain control over the device and prevent interaction with other apps or functions.  
To add an app, click **Add**, type an **App name**, and click **Save**. Repeat that process for each app you want to add.
- **News:** Allow users to use the News app.
- **Apple Music service:** Allow users to use the Apple Music service. If you don't allow Apple Music service, the Music app runs in classic mode.
- **Apple Music:** Allow users to use Apple Music.
- **Notifications modification:** Allow users to modify notification settings.
- **Restricted App usage:** Allow users to use all apps or to use or not use apps, based on the bundle IDs you provide. Applies only to supervised devices. If you select **Only allow some apps**, add an app with the bundle ID `com.apple.webapp` to allow web clips.

**Note:**

Beginning with iOS 11, Apple introduced changes to the policies that are available to app restrictions. Apple no longer lets you remove access to the Settings app and the Phone app by restricting the appropriate iOS application bundle.

After you configure the Restrictions device policy to block some apps and then deploy the policy: If you later want to allow some or all of those apps, changing and deploying the

Restrictions device policy doesn't change the restrictions. In this case, iOS doesn't apply the changes to the iOS profile. To proceed, use the Profile Removal policy to remove the iOS Profile and then deploy the updated Restrictions device policy.

If you change this setting to **Only allow some apps**: Before deploying this policy, advise users of devices enrolled using Apple Deployment Program to sign in to their Apple accounts from the Setup Assistant. Otherwise, users might have to disable two-factor authentication on their devices to sign in to their Apple accounts and access allowed apps.

- **Diagnostic submission modification**: Allow users to modify the diagnostic submission and app analytics settings in the **Settings > Diagnostics & Usage** pane.
- **Bluetooth modification**: Allow users to modify Bluetooth settings.
- **Allow dictation**: Supervised only. If this restriction is set to **Off**, dictation input is not allowed, including speech-to-text. The default setting is **On**.
- **Modify whether Wi-Fi is on or off**: Prevents Wi-Fi from being turned on or off in the Settings or Control Center. Entering airplane mode has no effect also. This restriction does not prevent selecting which Wi-Fi network to use.
- **Join only Wi-Fi networks installed by a network policy**: Optional. Supervised only. If this restriction is set to **On**, the device can join Wi-Fi networks only when they were set up through a configuration profile. The default setting is **Off**.
- **Allow the Classroom app to perform AirPlay and View Screen without prompting**: If this restriction is selected, the instructor can perform AirPlay and View Screen on a student device, without prompting for permission. The default setting is unselected. For supervised iOS devices.
- **Allow the Classroom app to lock to an app and lock the device without prompting**: If this restriction is set to **On**, the Classroom app automatically locks user devices to an app and locks the device, without prompting the users. The default setting is **Off**. For supervised devices running iOS 11 (minimum version).
- **Automatically join the Classroom app classes without prompting**: If this restriction is set to **On**, the Classroom app automatically joins users to classes, without prompting the users. The default setting is **Off**. For supervised devices running iOS 11 (minimum version).
- **Allow AirPrint**: If this restriction is set to **Off**, users can't print with AirPrint. The default setting is **On**. When this restriction is **On**, these extra restrictions appear. For supervised devices running iOS 11 (minimum version).
  - \* **Allow storage of AirPrint credentials in Keychain**: If this restriction is unselected, the AirPrint user name and password aren't stored in the Keychain. The default setting is selected. For supervised devices running iOS 11 (minimum version).

- \* **Allow discovery of AirPrint printers by using iBeacons:** If this restriction is unselected, iBeacon discovery of AirPrint printers is disabled. This setting prevents spurious AirPrint Bluetooth beacons from phishing for network traffic. The default setting is selected. For supervised devices running iOS 11 (minimum version).
- \* **Allow AirPrint only to destinations with trusted certificates:** If this restriction is selected, users can use AirPrint to print only to destinations with trusted certificates. The default setting is unselected. For supervised devices running iOS 11 (minimum version).
- **Adding VPN configurations:** If this restriction is set to **Off**, users can't create VPN configurations. The default setting is **On**. For supervised devices running iOS 11 (minimum version).
- **Modifying cellular plan settings:** If this restriction is set to **Off**, users can't modify cellular plan settings. The default setting is **On**. For supervised devices running iOS 11 (minimum version).
- **Removing system apps:** If this restriction is set to **Off**, users can't remove system apps from their device. The default setting is **On**. For supervised devices running iOS 11 (minimum version).
- **Setting up new nearby devices:** If this restriction is set to **Off**, users can't set up new nearby devices. The default setting is **On**. For supervised devices running iOS 11 (minimum version).
- **Allow USB restricted mode:** If **Off**, the device can always connect to USB accessories while locked. Default is **On**. Available only for supervised iOS 11.3 and later devices.
- **Force delayed software updates:** If **On**, delays user visibility of software updates. With this restriction in place, the user doesn't see a software update until the specified number of days after the software update release date. Default is **Off**. Available only for supervised iOS 11.3 and later devices. The OS update policy contains more settings for controlling how often devices receive updates. See [OS Update device policy](#).
- **Enforced software update delay (days):** Allows you to specify a number of days to delay a software update on the device. The maximum delay is **90** days. Default is **30** days. Available only for supervised iOS 11.3 and later devices.
- **Force classroom request permission to leave classes:** If **On**, a student enrolled in an unmanaged course with Classroom must request permission from the teacher when attempting to leave the course. Default is **Off**. Available only for supervised iOS 11.3 and later devices.
- **Force authentication before autofill:** Forces the user to authenticate before they can use the autofill feature.



- **Force automatic date and time:** Allows you to automatically set the date and time on supervised devices. If **On**, device users can't clear **Set Automatically** under **General > Date & Time**. The time zone on the device updates only when the device can determine its location. That is, when a device has a cellular connection or a Wi-Fi connection with location services enabled. Default is **Off**. Available only for supervised iOS 12 and later devices.
- **Password AutoFill:** Optional. If disabled, users cannot use the AutoFill Passwords or Automatic Strong Passwords features. Default is **On**. Available as of iOS 12.
- **Password proximity requests:** Optional. If disabled, users' devices don't request passwords from nearby devices. Default is **On**. Available as of iOS 12.
- **Password Sharing:** Optional. If disabled, users can't share their passwords using the Air-Drop Passwords feature. Default is **On**. Available as of iOS 12.
- **Allow personal hotspot modification:** Prevents users from changing the personal hotspot settings.
- **Security - Show in lock screen**
  - **Control Center:** Allow access to Control Center on the lock screen. Control Center lets users easily modify Airplane Mode, Wi-Fi, Bluetooth, Do Not Disturb Mode, and Lock Rotation settings.
  - **Notification:** Allow notifications on the lock screen.
  - **Today view:** Allow Today View, which aggregates information such as the weather and the current day's calendar items, on the lock screen.
- **Media content - Allow**
  - **Explicit music, podcasts, and iTunes U material:** Allow explicit material on users' devices.
  - **Explicit sexual content in iBooks:** Allow explicit material to be downloaded from iBooks.
  - **Ratings region:** Set the region from which parental control ratings are obtained. In the list, click a country to set the ratings region. The default is **United States**.
  - **Movies:** Set whether movies are allowed on users' devices. If movies are allowed, optionally set the ratings level for movies. In the list, click an option to allow or restrict movies on the device. The default is Allow all movies.
  - **TV Shows:** Set whether TV shows are allowed on users' devices. If TV shows are allowed, optionally set the ratings level for TV shows. In the list, click an option to allow or restrict TV shows on the device. The default is Allow all TV Shows.
  - **Apps:** Set whether apps are allowed on users' devices. If apps are allowed, optionally set the ratings level for apps. In the list, click an option to allow or restrict apps on the device. The default is Allow all apps.
- **Policy settings**

- **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
  - \* **Select date:** Click the calendar to select the specific date for removal.
  - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.
- **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on iOS 9.3 and later.

## macOS settings

### Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Preferences**

Restrict items in System Preferences  OFF

**Apps**

Allow use of Game Center  ON macOS 10.11+

Allow adding Game Center friends  ON

Allow multiplayer gaming  ON

Allow Game Center account modification  ON

Allow App Store adoption  ON

Allow Safari AutoFill  ON

Require admin password to install or update apps  OFF

Restrict App Store to software update only  OFF

Restrict which apps are allowed to open  OFF

**Widgets**

Allow only the following Dashboard widgets to run  OFF

**Media**

Setting	Unsupervised	Supervised
<b>Apps</b>		
Allow use of Game Center	No	Yes
Allow adding Game Center friends	No	Yes
Allow multiplayer gaming	No	Yes

<b>Setting</b>	<b>Unsupervised</b>	<b>Supervised</b>
Allow Game Center account modification	Yes	Yes
Allow App Store adoption	Yes	Yes
Allow Safari Autofill	No	Yes
Require admin password to install or update apps	Yes	Yes
Restrict App Store to software update only	Yes	Yes
Restrict which apps are allowed to open	Yes	Yes
<b>Media</b>		
Allow AirDrop	No	Yes
<b>Functionality</b>		
Lock desktop picture	No	Yes
Allow use of camera	No	Yes
Allow Apple Music	No	Yes
Allow Spotlight Suggestions	Yes	Yes
Allow Look Up	Yes	Yes
Allow use of iCloud password for local accounts	Yes	Yes
Allow iCloud documents & data	Yes	Yes
Allow iCloud Desktop and Documents	No	Yes
Allow iCloud Keychain Sync	No	Yes
Allow iCloud Mail	Yes	Yes
Allow iCloud Contacts	Yes	Yes
Allow iCloud Calendars	Yes	Yes
Allow iCloud Reminders	Yes	Yes
Allow iCloud Bookmarks	Yes	Yes
Allow iCloud Notes	Yes	Yes

Setting	Unsupervised	Supervised
Allow iCloud Photos	Yes	Yes
Allow Auto Unlock	Yes	Yes
Allow Touch ID To Unlock Mac	Yes	Yes
Force delayed software updates	No	Yes
Password AutoFill	No	Yes
Password proximity requests	No	Yes
Password Sharing	Yes	Yes

- **Preferences**

- **Restrict items in System Preferences:** Allow or restrict user access to System Preferences. The default is **Off**, which allows users full access to System Preferences. If enabled, configure the following settings.

- \* **System Preference Pane:** Select whether the settings you select are enabled or disabled. The default is to enable all settings, which are **On** by default.

- Users & Groups
      - General
      - Accessibility
      - App Store
      - Software Update
      - Bluetooth
      - CDs & DVDs
      - Date & Time
      - Desktop & Screen Saver
      - Displays
      - Dock
      - Energy Saver
      - Extensions
      - FibreChannel
      - iCloud
      - Ink
      - Internet Accounts
      - Keyboard
      - Language & Text
      - Mission Control

- Mouse
- Network
- Notifications
- Parental Controls
- Printers & Scanners
- Profiles
- Security & Privacy
- Sharing
- Sound
- Dictation & Speech
- Spotlight
- Startup Disk
- Time Machine
- Trackpad
- Xsan

- **Apps**

- **Allow use of Game Center:** Allow users to play online games through Game Center. The default is **On**.
- **Allow adding Game Center friends:** Allow users to send a notification to a friend to play a game. The default is **On**.
- **Allow multiplayer gaming:** Allow users to initiate multiplayer game play. The default is **On**.
- **Allow Game Center account modification:** Allow users to modify their Game Center account settings. The default is **On**.
- **Allow App Store adoption:** Allow or restrict the App Store to adopt apps that preexist in OS X. The default is **On**.
- **Allow Safari Autofill:** Allow Safari to automatically populate fields on websites with passwords, addresses, and other basic information that it has stored. The default is **On**.
- **Require admin password to install or update apps:** Require an administrator password to install or update apps. The default is **Off**, which means no administrator password is required.
- **Restrict App Store to software update only:** Restrict the App Store to updates only, which disables all tabs in the App Store except Updates. The default is **Off**, which allows full App Store access.
- **Restrict which apps are allowed to open:** Restrict or allow apps users can use. The default is **Off**, which allows all apps to be used. If enabled, configure the following settings:
  - \* **Allowed Apps:** Click **Add**, enter the name and bundle ID for an app allowed to launch, and then click **Save**. For Citrix mobile productivity apps, use the ID from the **Package ID** field when adding the app. Repeat this step for each app allowed to launch.

- \* **Disallowed Folders:** Click **Add**, type the file path to a folder you want to restrict user access (for example, /Applications/Utilities), and then click **Save**. Repeat this step for all folders you do not want users to be able to access.
- \* **Allowed folders:** Click **Add**, type the file path to a folder to which you want to grant user access, and then click **Save**. Repeat this step for all folders you want users to be able to access.
- **Widgets**
  - **Allow only the following Dashboard widgets to run:** If **On**, users can only run the Dashboard widgets configured in this setting. The default is **Off**, which allows users to run all widgets. If enabled, configure the following setting:
    - \* **Allowed Widgets:** Click **Add**, type the name and ID of a widget that is allowed to run, and then click **Save**. Repeat this step for each widget you want to run on the Dashboard.
- **Media**
  - **Allow AirDrop:** Allow users to share photos, videos, websites, locations, and more with nearby iOS devices.
- **Sharing**
  - **Automatically enable new sharing services:** Select whether to automatically enable sharing services.
  - **Mail:** Select whether to allow a shared mailbox.
  - **Facebook:** Select whether to allow a shared Facebook account.
  - **Video Services - Flickr, Vimeo, Tudou, and Youku:** Select whether to allow shared video services.
  - **Add to Aperture:** Select whether to allow shared ability to add to Aperture.
  - **Sina Weibo:** Select whether to allow a shared Sina Weibo account.
  - **Twitter:** Select whether to allow a shared Twitter account.
  - **Messages:** Select whether to allow shared access to messages.
  - **Add to iPhoto:** Select whether to allow shared ability to add to iPhoto.
  - **Add to Reading List:** Select whether to allow shared ability to add to Reading List.
  - **AirDrop:** Select whether to allow a shared AirDrop account.
- **Functionality**
  - **Lock desktop picture:** Select whether users can change the desktop picture. The default is **Off**, which means users can change the desktop picture.
  - **Allow use of camera:** Select whether users can use the camera on their Macs. The default is **Off**, which means users cannot use the camera.
  - **Allow Apple Music:** Allow users to use the Apple Music service (macOS 10.12 and later). If you don't allow Apple Music service, the Music app runs in classic mode. Applies only to supervised devices. Defaults to **On**.
  - **Allow Spotlight Suggestions:** Select whether users can use Spotlight Suggestions to

search their Mac and to provide Spotlight Suggestions from the Internet and the App Store. The default is **Off**, which prevents users from using Spotlight Suggestions.

- **Allow Look Up:** Select whether users can look up the definitions of words with the context menu or the Spotlight search menu. The default is **Off**, which prevents users from using Look Up on their Macs.
- **Allow use of iCloud password for local accounts:** Select whether users can use their Apple ID and iCloud password to sign on to their Macs. Enabling this policy means that users use only one ID and password for *all* login screens on their Macs. The default is **On**, which allows users to use their Apple ID and iCloud password to access their Macs.
- **Allow iCloud documents & data:** Select whether to allow users to access documents and data stored on iCloud on their Macs. The default is **On**, which prevents users from using iCloud documents and data on their Macs.
  - \* **Allow iCloud Desktop and Documents:** (macOS 10.12.4 and later) The default is selected.
- **Allow iCloud Keychain Sync:** Allow iCloud Keychain sync (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Mail:** Allow users to use iCloud Mail (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Contacts:** Allow users to use iCloud Contacts (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Calendars:** Allow users to use iCloud Calendars (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Reminders:** Allow users to use iCloud Reminders (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Bookmarks:** Allow users to sync with iCloud Bookmarks (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Notes:** Allow users to use Cloud Notes (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Photos:** If you change this setting to **Off**, any photos not fully downloaded from the iCloud Photo Library are removed from local device storage (macOS 10.12 and later). The default is **On**.
- **Allow Auto Unlock:** For information about this option and Apple Watch, see <https://www.imore.com/auto-unlock> (macOS 10.12 and later). The default is **On**.
- **Allow Touch ID To Unlock Mac:** (macOS 10.12.4 and later). The default is **On**.
- **Force delayed software updates:** If **On**, this setting delays user visibility of software updates. Users don't see a software update until the specified number of days after the software update release date. Default is **Off**. Available only for supervised devices running macOS 10.13.4 and later. The OS update policy contains more settings for controlling how often devices receive updates. See [OS Update device policy](#).

- **Enforced software update delay (days):** Specifies how many days to delay a software update on the device. The maximum is 90 days. Default is **30**. Available only for supervised devices running macOS 10.13.4 and later.
- **Password AutoFill:** Optional. If disabled, users cannot use the AutoFill Passwords or Automatic Strong Passwords features. Default is **On**. (macOS 10.14 and later)
- **Password proximity requests:** Optional. If disabled, users' devices don't request passwords from nearby devices. Default is **On**. (macOS 10.14 and later)
- **Password Sharing:** Optional. If disabled, users can't share their passwords using the AirDrop Passwords feature. Default is **On**. (macOS 10.14 and later)

## tvOS settings

- **Security and Media Settings - Allow**

- **Passcode on first AirPlay pairing:** Require that AirPlay-enabled devices are verified with a one-time onscreen code before they can use AirPlay.
- **Explicit sexual content in iBooks:** Allow explicit material to be downloaded from iBooks.
- **Explicit music, podcasts, and iTunes U material:** Allow explicit material on user devices.
- **In-app purchases:** Allow users to make in-app purchases.
  - \* **Require Apple App Store password for purchases:** Require a password for in-app purchases. The default is to restrict this feature, which means no password is required for in-app purchases.

- **Supervised only settings - Allow**

- **Device name modification:** Allow users to change the name of their device.
- **Allow pairing with Apple TV Remote app:** Allow users to pair their device with the Apple TV Remote app.
- **Siri profanity filter:** Siri profanity filter: Enable the Siri profanity filter. The default is to restrict this feature, which means no profanity filtering is done.
- **Enable AirPlay:** Allow users to stream content or mirror their iOS device screen on this device.
- **Restricted App usage:** Allow users to use all apps or to use or not use apps, based on the bundle IDs you provide. Applies only to supervised devices.

After you configure the Restrictions device policy to block some apps and then deploy the policy: If you later want to allow some or all of those apps, changing and deploying the Restrictions device policy doesn't change the restrictions. In this case, iOS doesn't apply the changes to the iOS profile.

If you change this setting to **Only allow some apps:** Before deploying this policy, advise users of devices enrolled using Apple Deployment Program to sign in to their Apple accounts from the Setup Assistant. Otherwise, users might have to disable two-factor authentication on their devices to sign in to their Apple accounts and access allowed apps.



- **Policy settings**

- **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
  - \* **Select date:** Click the calendar to select the specific date for removal.
  - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
- **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field. Not available for iOS.

### **Android settings**

- **Camera:** Allow users to use the camera on their devices. If **Off**, the camera is disabled. Defaults to **On**.

## Android Enterprise settings

Apply to fully managed devices with a work profile  ON

For fully managed devices with a work profile, apply the policy to:

Work profile

Managed device

### Security

Allow account management  OFF ?

Allow cross profile copy and paste  OFF ?

Allow screen capture  OFF ?

Allow use of camera  OFF ?

Allow configuring location provider  ON ?

Allow location sharing  OFF ?

Allow user to configure user credentials  ON

Allow printing  OFF ?

When a new or factory reset Android device enrolls in work profile mode, devices running Android 8.0-10.x enroll as fully-managed devices with a work profile. Devices running Android 11+ enroll as work profile on corporate-owned devices. The restriction policy can apply to either the work profile on the device or the managed device.

On devices enrolled in the work profile on corporate-owned devices mode, the following restrictions don't work:

- Allow backup service
- Enable system apps
- Keep the keyguard from locking the device

- Allow use of the status bar
- Keep the device screen on
- Allow user control of application settings
- Allow user to configure user credentials
- Allow VPN configuration
- Allow USB mass storage
- Allow factory reset
- Allow app uninstall
- Allow non-Google Play apps
- Allow cross profile copy and paste
- Enable app verification
- Allow account management
- Allow printing
- Allow NFC
- Allow adding users

By default, the **USB Debugging and Unknown Sources** settings are disabled on a device when it is enrolled in Android Enterprise in work profile mode.

For devices running Android 8.0-10.x and Samsung Knox 3.0 and later, configure settings for Samsung Knox and Samsung SAFE on the **Android Enterprise** page. For devices running earlier versions of Android or Samsung Knox, use the **Samsung Knox** and **Samsung SAFE** pages.

Samsung restrictions don't apply to devices enrolled in the work profile on corporate-owned devices mode. Use the Knox Service Plugin (KSP) to apply Samsung restrictions to these devices. For more information, see the [Samsung documentation](#).

We recommend that you use Samsung Knox 3.4 or higher for the latest Samsung Knox management features.

Watch this video to learn more:



- **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices:** Allows restrictions policy settings to be configured for fully managed devices with work profiles. These devices are also known as COPE (corporate owned personally enabled) devices. When this setting is **On**, select one of these settings:
  - **Work profile:** The restrictions settings you configure apply only to the work profile on the device.
  - **Managed device:** The restrictions settings you configure apply only to the device.

When this setting is **Off**, the credentials settings you configure apply to the device, except for settings that explicitly apply to the work profile. Default is **Off**.

When **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices** is off, configure the following settings:

- **Security**
  - **Allow account management:** Allows account to be added to in work profile and managed devices. Default is **Off**.
  - **Allow cross profile copy and paste:** If **On**, users can copy and paste between apps in the Android Enterprise profile and apps in the personal area. Default is **Off**.
  - **Allow screen capture:** Allows users to record or take a screen capture of the device screen. Default is **Off**.
  - **Allow use of camera:** Allows users to take pictures and make videos with the device camera. Default is **Off**.

- **Allow VPN configuration:** Allows users to create VPN configurations. For work profile devices running Android 6 and later and for fully managed devices. Default is **On**.
- **Allow backup service:** Allows users to back up application and system data on their devices. Default is **On**.
- **Allow NFC:** Allow users to send webpages, photos, videos, or other content from their devices to another device using Near Field Communication (NFC). For MDM 4.0 and later. Default is **On**.
- **Allow configuring location provider:** Allows users to turn on GPS on their devices. For Android API 28 and later. Default is **On**.
- **Allow location sharing:** For managed profiles, the device owner can override this setting. Default is **Off**.

**Tip:**

You can create Location device policies in Endpoint Management to enforce geographic boundaries. See [Location device policy](#).

- **Allow user to configure user credentials:** Specify whether users can configure credentials in the managed keystore. Default is **On**.
- **Allow printing:** If **On**, the setting allows users to print to any printer accessible from the user device. The default is **Off**. Available for: Android 9 and later.
- **Allow USB debugging:** Default is **Off**.

**• Apps**

- **Enable system apps:** Allows users to run pre-installed device apps. Default is **Off**. To enable specific apps, click **Add** in the **System apps list** table.
  - \* **System apps list:** A list of the system apps you want to enable on the device. Set **Enable system apps** to **On** and add the app package name. To look up the package name for a system app, you can use the Android Debug Bridge (`adb`) to call the Android package manager (`pm`) command. For example, `adb shell "pm list packages -f name"`, where "name" is part of the package name. For more information, see <https://developer.android.com/studio/command-line/adb>. For Android Enterprise devices, you can restrict app permissions using the [Android Enterprise app permissions](#) policy.
- **Disable applications:** Blocks a specified list of apps from running on devices. Default is **Off**. To disable an installed app, change the setting to **On** and then click **Add** in the **Application list** table.
  - \* **Application list:** A list of the apps you want to block. Set **Disable applications** to **On** and add the app. Type the app package name. Changing and deploying an app list overwrites the prior app list. For example: If you disable `com.example1` and

com.example2, and then later change the list to com.example1 and com.example3, Endpoint Management enables com.example.2.

- **Enable app verification:** Enables the OS to scan apps to detect malicious behavior. Default is **On**.
- **Enable Google apps:** Allows users to download apps from Google Mobile Services onto the device. Default is **On**.
- **Allow non-Google Play apps:** Allows the installation of apps from stores other than Google Play. Default is **Off**.
- **Allow user control of application settings:** Allows users to uninstall apps, disable apps, clear cache and data, force stop any app, and clear defaults. Users perform these actions from the Settings app. Default is **Off**.
- **Allow app uninstall:** Allows users to uninstall apps from within the Managed Google Play Store. Default is **Off**.

- **BYOD work profile**

- **Allow work profile app widgets on home screen:** If this setting is **On**, users can place work profile app widgets on the device home screen. If this setting is **Off**, users cannot place work profile app widgets on the device home screen. Default is **Off**.
  - \* **Apps with allowed widgets:** A list of the apps you want to allow on the home screen. Set **Allow work profile app widgets on home screen** to **On** and add the app. Click **Add** and select an app whose widgets you want to allow on the home screen from the list. Click **Save**. Repeat that process to allow more app widgets.
- **Allow work profile contacts in device contacts:** Shows contacts from the managed Android Enterprise profile in the parent profile, for incoming calls (Android 7.0 and later). Default is **Off**.

- **Fully managed device only**

- **Allow adding users:** Allows users to add new users on a device. Default is **On**.
- **Allow data roaming:** Allows users to use cellular data while roaming. The default is Off, which disables roaming on users' devices. Default is **Off**.
- **Allow SMS:** Allows users to send and receive SMS messages. Default is **Off**.
- **Allow use of the status bar:** If **On**, this setting enables the status bar on managed devices and dedicated devices (also known as COSU devices). This setting disables notifications, quick settings, and other screen overlays that allow escape from full-screen mode. Users can go to system settings and see notifications. For Android 6.0 and later. Default is **Off**.
- **Allow Bluetooth:** Allows users to use Bluetooth. Default is **On**.
  - \* **Allow Bluetooth sharing:** If unselected, users can't establish outgoing Bluetooth sharing on their device. The default is selected.
- **Allow configuring date and time:** Allows users to change the date and time on their devices. Default is **On**.

- **Allow factory reset:** Allows users to do a factory reset on their devices. Default is **On**.
  - **Keep the device screen on:** If this setting is set to **On**, the device screen remains on when the device is plugged in. Default is **Off**.
  - **Allow USB mass storage:** Allows transfer of large data files between users' devices and a computer over a USB connection. Default is **On**.
  - **Allow microphone:** Allows users to use the microphone on their devices. Default is **On**.
  - **Allow tethering:** Allows users to configure portable hotspots and tether data. Default is **Off**.
  - **Keep the keyguard from locking the device:** If **On**, this setting disables the keyguard on the lock screen on managed devices and dedicated devices (also known as COSU devices). Default is **Off**.
  - **Allow Wi-Fi changes:** If **On**, users can turn Wi-Fi on or off and connect to Wi-Fi networks. Default is **On**.
  - **Allow file transfer:** Allows file transfers over USB. Default is **Off**.
- **Samsung**
    - **Enable TIMA Keystore:** The TIMA Keystore provides TrustZone-based secure key storage for the symmetric keys. RSA key pairs and certificates are routed to the default key store provider for storage. Default is **Off**.
    - **Allow share list:** Allows users to share content between apps in the Share Via list. Default is **On**.
    - **Enable audit log:** Enables creation of event audit logs for forensic analysis of a device. Default is **Off**.
  - **Samsung: Fully managed device only**
    - **Enable ODE Trusted Boot verification:** Use ODE trusted boot verification to establish a chain of trust from the bootloader to the system image. Default is **On**.
    - **Allow emergency calls only:** Allows users to enable Emergency Call Only mode on their devices. Default is **Off**.
    - **Allow firmware recovery:** Allows users to recover the firmware on their devices. Default is **On**.
    - **Allow fast encryption:** Allows encryption of only used memory space. This encryption contrasts full disk encryption, which encrypts all data. That data includes settings, application data, downloaded files and applications, media, and other files. Default is **On**.
    - **Enable Common Criteria mode:** Places device into Common Criteria Mode. The Common Criteria configuration enforces stringent security processes. Default is **On**.
    - **Enable reboot banner:** Displays a DoD approved system use notification message or banner when users' devices are restarted. Default is **Off**.
    - **Allow settings changes:** Allows users to change settings on their fully managed devices. Default is **On**.

- **Enable background data usage:** Allows apps to sync data in the background. for fully managed devices. Default is **On**.
- **Allow clipboard:** Allow users to copy data to the clipboard on their devices.
  - \* **Allow clipboard share:** Allow users to share clipboard content between their devices and a computer (MDM 4.0 and later).
- **Allow home key:** Allows users to use the **Home** key on their fully managed devices. Default is **On**.
- **Allow mock location:** Allows users to fake their GPS location. For fully managed devices. Default is **Off**.
- **NFC:** Allows users to use NFC on their fully managed devices (MDM 3.0 and later). Default is **On**.
- **Allow power off:** Allows users to power off their fully managed devices (MDM 3.0 and later). Default is **On**.
- **Allow Wi-Fi direct:** Allows users to connect directly to another device through their Wi-Fi connection. Default is **On**. If **On**, you must enable the **Allow Wi-Fi changes** setting.
- **Allow SD card:** Allows users to use an SD card, if available, with their devices. Default is **On**.
- **Allow USB host storage:** Allows users' devices to act as the USB host when a USB device connects to their devices. Users' devices then supply power to the USB device. Default is **On**.
- **Allow voice dialer:** Allows users to use the voice dialer on their devices (MDM 4.0 and later). Default is **On**.
- **Allow S beam:** Allows users to share content with others using NFC and Wi-Fi Direct (MDM 4.0 and later). Default is **On**.
- **Allow S voice:** Allows users to use the intelligent personal assistant and knowledge navigator on their devices (MDM 4.0 and later). Default is **On**.
- **Allow USB tethering:** Allows users to share a mobile data connection with another device using their USB connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
- **Allow Bluetooth tethering:** Allows users to share a mobile data connection with another device using their Bluetooth connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
  - \* **Allow Bluetooth sharing:** If unselected, users can't establish outgoing Bluetooth sharing on their device. The default is selected.
- **Allow Wi-Fi tethering:** Allows users to share a mobile data connection with another device using their Wi-Fi connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
- **Allow incoming MMS:** Allows users to receive MMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.



- **Allow outgoing MMS:** Allows users to send MMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Allow incoming SMS:** Allows users to receive SMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Allow outgoing SMS:** Allows users to send SMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Configure mobile networks:** Allows users to use their cellular data connection. Default is **Off**.
- **Limit by day (MB):** Enter the number of MB of mobile data users can use each day. The default is 0, which disables this feature (MDM 4.0 and later).
- **Limit by week (MB):** Enter the number of MB of mobile data users can use each week. The default is 0, which disables this feature (MDM 4.0 and later).
- **Limit by month (MB):** Enter the number of MB of mobile data users can use each month. The default is 0, which disables this feature (MDM 4.0 and later).
- **Allow only secure VPN connections:** Allows users to only use secure connections (MDM 4.0 and later). Default is **On**.
- **Allow audio recording:** Allows users to record audio with their devices (MDM 4.0 and later). Default is **On**. If **On** you must turn on the **Allow microphone** setting.
- **Allow video recording:** Allows users to record video with their devices (MDM 4.0 and later). Default is **Off**. If **On** you must turn on the **Allow use of camera** setting.
- **Allow push messages when roaming:** Allow users to use cellular data for pushing. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.
- **Allow automatic synchronization when roaming:** Allow users to use cellular data for syncing. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.
- **Allow voice calls when roaming:** Allow users to use cellular data for voice calls. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.
- **Samsung: Knox container/Fully managed device**
  - **Enable revocation check:** Enables checking for revoked certificates. Default is **Off**.
- **Samsung: Knox container only**
  - **Move apps to container:** Allows users to move apps between the Knox container and the personal area on their devices. Default is **On**.
  - **Enforce multi-factor authentication:** Users must use a fingerprint and one other authentication method, such as password or PIN, to open their devices. Default is **On**.
  - **Enforce authentication for container:** Use a different authentication method from the method used to unlock the device to open the KNOX container. Default is **On**.
  - **Enable secure keypad:** Forces users to use a secure keyboard inside the Knox container. Default is **On**.
- **Samsung: DeX**

- **Enable Samsung DeX:** Enables supported Knox-enabled devices to run in Samsung DeX mode. Requires Samsung Knox 3.1 (minimum version). Default is **On**. For information about Samsung DeX device requirements and setting up Samsung DeX, see the Samsung Developers documentation.
  - \* **Allow Ethernet in DeX mode only:** Enables use of Ethernet in Samsung DeX mode. Cellular data, Wi-Fi, and tethering (Wi-Fi, Bluetooth, and USB) are restricted in DeX mode. Default is unselected.
  - \* **Upload DeX logo image:** Select this setting to specify a .png image to use as an icon for Samsung DeX.
  - \* **DeX screen timeout (seconds):** Specify the amount of idle time, in seconds, after which the DeX screen turns off. To disable the timeout, type **0**. Default is **1200** seconds (20 minutes).
  - \* **Add app shortcut in Samsung DeX:** Specify an app package name to add a shortcut for the app to DeX. To look up an app package name, go to Google Play and select the app. The URL includes the package name: <https://play.google.com/store/apps/details?id=<package.name><!--NeedCopy-->>.
  - \* **Remove app shortcut in Samsung DeX:** Specify an app package name to remove a shortcut from DeX. Go to Google Play to look up app package names.
  - \* **App packages to disable in Samsung DeX:** Specify a comma-separated list of the app packages that you want to block from Samsung DeX mode. For example: `"com.android.chrome", "com.google.android.gm"<!--NeedCopy-->`.

When **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices** is on and **For fully managed devices with a work profile, apply the policy to** is set to **Work profile**, configure these settings:

- **Security**

- **Allow account management:** Allows account to be added to in work profile and managed devices. Default is **Off**.
- **Allow cross profile copy and paste:** If **On**, users can copy and paste between apps in the Android Enterprise profile and apps in the personal area. Default is **Off**.
- **Allow screen capture:** Allows users to record or take a screen capture of the device screen. Default is **Off**.
- **Allow use of camera:** Allows users to take pictures and make videos with the device camera. Default is **Off**.
- **Allow configuring location provider:** Allows users to turn on GPS on their devices. For Android API 28 and later. Default is **On**.
- **Allow location sharing:** For managed profiles, the device owner can override this setting. Default is **Off**.

**Tip:**

You can create Location device policies in Endpoint Management to enforce geographic boundaries. See [Location device policy](#).

- **Allow user to configure user credentials:** Specify whether users can configure credentials in the managed keystore. Default is **On**.
- **Allow printing:** If **On**, the setting allows users to print to any printer accessible from the user device. The default is **Off**. Available for: Android 9 and later.

**• Apps**

- **Enable system apps:** Allows users to run pre-installed device apps. Default is **Off**. To enable specific apps, click **Add** in the **System apps list** table.
  - \* **System apps list:** A list of the system apps you want to enable on the device. Set **Enable system apps** to **On** and add the app package name. To look up the package name for a system app, you can use the Android Debug Bridge (`adb`) to call the Android package manager (`pm`) command. For example, `adb shell "pm list packages -f name"`, where “name” is part of the package name. For more information, see <https://developer.android.com/studio/command-line/adb>. For Android Enterprise devices, you can restrict app permissions using the [Android Enterprise app permissions](#) policy.
- **Disable applications:** Blocks a specified list of apps from running on devices. Default is **Off**. To disable an installed app, change the setting to **On** and then click **Add** in the **Application list** table.
  - \* **Application list:** A list of the apps you want to block. Set **Disable applications** to **On** and add the app. Type the app package name. Changing and deploying an app list overwrites the prior app list. For example: If you disable `com.example1` and `com.example2`, and then later change the list to `com.example1` and `com.example3`, Endpoint Management enables `com.example.2`.
- **Enable app verification:** Enables the OS to scan apps to detect malicious behavior. Default is **On**.
- **Enable Google apps:** Allows users to download apps from Google Mobile Services onto the device. Default is **On**.
- **Allow non-Google Play apps:** Allows the installation of apps from stores other than Google Play. Default is **Off**.
- **Allow user control of application settings:** Allows users to uninstall apps, disable apps, clear cache and data, force stop any app, and clear defaults. Users perform these actions from the Settings app. Default is **Off**.
- **Allow app uninstall:** Allows users to uninstall apps from within the Managed Google Play Store. Default is **Off**.

- **BYOD work profile**

- **Allow work profile app widgets on home screen:** If this setting is **On**, users can place work profile app widgets on the device home screen. If this setting is **Off**, users cannot place work profile app widgets on the device home screen. Default is **Off**.
  - \* **Apps with allowed widgets:** A list of the apps you want to allow on the home screen. Set **Allow work profile app widgets on home screen** to **On** and add the app. Click **Add** and select an app whose widgets you want to allow on the home screen from the list. Click **Save**. Repeat that process to allow more app widgets.
- **Allow work profile contacts in device contacts:** Shows contacts from the managed Android Enterprise profile in the parent profile, for incoming calls (Android 7.0 and later). Default is **Off**.

- **Samsung**

- **Enable TIMA Keystore:** The TIMA Keystore provides TrustZone-based secure key storage for the symmetric keys. RSA key pairs and certificates are routed to the default key store provider for storage. Default is **Off**.
- **Allow share list:** Allows users to share content between apps in the Share Via list. Default is **On**.
- **Enable audit log:** Enables creation of event audit logs for forensic analysis of a device. Default is **Off**.

- **Samsung: Knox container/Fully managed device**

- **Enable revocation check:** Enables checking for revoked certificates. Default is **Off**.

- **Samsung: Knox container only**

- **Move apps to container:** Allows users to move apps between the Knox container and the personal area on their devices. Default is **On**.
- **Enforce multi-factor authentication:** Users must use a fingerprint and one other authentication method, such as password or PIN, to open their devices. Default is **On**.
- **Enforce authentication for container:** Use a different authentication method from the method used to unlock the device to open the KNOX container. Default is **On**.
- **Enable secure keypad:** Forces users to use a secure keyboard inside the Knox container. Default is **On**.

When **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices** is on and **For fully managed devices with a work profile, apply the policy to** is set to **Managed device**, configure these settings:

- **Security**

- **Allow account management:** Allows account to be added to in work profile and managed devices. Default is **Off**.

- **Allow cross profile copy and paste:** If **On**, users can copy and paste between apps in the Android Enterprise profile and apps in the personal area. Default is **Off**.
- **Allow screen capture:** Allows users to record or take a screen capture of the device screen. Default is **Off**.
- **Allow use of camera:** Allows users to take pictures and make videos with the device camera. Default is **Off**.
- **Allow VPN configuration:** Allows users to create VPN configurations. For work profile devices running Android 6 and later and for fully managed devices. Default is **On**.
- **Allow backup service:** Allows users to back up application and system data on their devices. Default is **On**.
- **Allow NFC:** Allow users to send webpages, photos, videos, or other content from their devices to another device using Near Field Communication (NFC). For MDM 4.0 and later. Default is **On**.
- **Allow configuring location provider:** Allows users to turn on GPS on their devices. For Android API 28 and later. Default is **On**.
- **Allow location sharing:** For managed profiles, the device owner can override this setting. Default is **Off**.

**Tip:**

You can create Location device policies in Endpoint Management to enforce geographic boundaries. See [Location device policy](#).

- **Allow user to configure user credentials:** Specify whether users can configure credentials in the managed keystore. Default is **On**.
- **Allow printing:** If **On**, the setting allows users to print to any printer accessible from the user device. The default is **Off**. Available for: Android 9 and later.
- **Allow USB debugging:** Default is **Off**.

**• Apps**

- **Enable system apps:** Allows users to run pre-installed device apps. Default is **Off**. To enable specific apps, click **Add** in the **System apps list** table.
  - \* **System apps list:** A list of the system apps you want to enable on the device. Set **Enable system apps** to **On** and add the app package name. To look up the package name for a system app, you can use the Android Debug Bridge (`adb`) to call the Android package manager (`pm`) command. For example, `adb shell "pm list packages -f name"`, where "name" is part of the package name. For more information, see <https://developer.android.com/studio/command-line/adb>. For Android Enterprise

devices, you can restrict app permissions using the [Android Enterprise app permissions](#) policy.

- **Disable applications:** Blocks a specified list of apps from running on devices. Default is **Off**. To disable an installed app, change the setting to **On** and then click **Add** in the **Application list** table.
    - \* **Application list:** A list of the apps you want to block. Set **Disable applications** to **On** and add the app. Type the app package name. Changing and deploying an app list overwrites the prior app list. For example: If you disable com.example1 and com.example2, and then later change the list to com.example1 and com.example3, Endpoint Management enables com.example2.
  - **Enable app verification:** Enables the OS to scan apps to detect malicious behavior. Default is **On**.
  - **Enable Google apps:** Allows users to download apps from Google Mobile Services onto the device. Default is **On**.
  - **Allow non-Google Play apps:** Allows the installation of apps from stores other than Google Play. Default is **Off**.
  - **Allow user control of application settings:** Allows users to uninstall apps, disable apps, clear cache and data, force stop any app, and clear defaults. Users perform these actions from the Settings app. Default is **Off**.
  - **Allow app uninstall:** Allows users to uninstall apps from within the Managed Google Play Store. Default is **Off**.
- **Fully managed device only**
    - **Allow adding users:** Allows users to add new users on a device. Default is **On**.
    - **Allow data roaming:** Allows users to use cellular data while roaming. The default is Off, which disables roaming on users' devices. Default is **Off**.
    - **Allow SMS:** Allows users to send and receive SMS messages. Default is **Off**.
    - **Allow use of the status bar:** If **On**, this setting enables the status bar on managed devices and dedicated devices (also known as COSU devices). This setting disables notifications, quick settings, and other screen overlays that allow escape from full-screen mode. Users can go to system settings and see notifications. For Android 6.0 and later. Default is **Off**.
    - **Allow Bluetooth:** Allows users to use Bluetooth. Default is **On**.
      - \* **Allow Bluetooth sharing:** If unselected, users can't establish outgoing Bluetooth sharing on their device. The default is selected.
    - **Allow configuring date and time:** Allows users to change the date and time on their devices. Default is **On**.
    - **Allow factory reset:** Allows users to do a factory reset on their devices. Default is **On**.
    - **Keep the device screen on:** If this setting is set to **On**, the device screen remains on when the device is plugged in. Default is **Off**.
    - **Allow USB mass storage:** Allows transfer of large data files between users' devices and a

computer over a USB connection. Default is **On**.

- **Allow microphone:** Allows users to use the microphone on their devices. Default is **On**.
- **Allow tethering:** Allows users to configure portable hotspots and tether data. Default is **Off**. When this setting is on, these settings are available for Samsung devices:
- **Keep the keyguard from locking the device:** If **On**, this setting disables the keyguard on the lock screen on managed devices and dedicated devices (also known as COSU devices). Default is **Off**.
- **Allow Wi-Fi changes:** If **On**, users can turn Wi-Fi on or off and connect to Wi-Fi networks. Default is **On**.
- **Allow file transfer:** Allows file transfers over USB. Default is **Off**.

- **Samsung**

- **Enable TIMA Keystore:** The TIMA Keystore provides TrustZone-based secure key storage for the symmetric keys. RSA key pairs and certificates are routed to the default key store provider for storage. Default is **Off**.
- **Allow share list:** Allows users to share content between apps in the Share Via list. Default is **On**.
- **Enable audit log:** Enables creation of event audit logs for forensic analysis of a device. Default is **Off**.

- **Samsung: Fully managed device only**

- **Enable ODE Trusted Boot verification:** Use ODE trusted boot verification to establish a chain of trust from the bootloader to the system image. Default is **On**.
- **Allow emergency calls only:** Allows users to enable Emergency Call Only mode on their devices. Default is **Off**.
- **Allow firmware recovery:** Allows users to recover the firmware on their devices. Default is **On**.
- **Allow fast encryption:** Allows encryption of only used memory space. This encryption contrasts full disk encryption, which encrypts all data. That data includes settings, application data, downloaded files and applications, media, and other files. Default is **On**.
- **Enable Common Criteria mode:** Places device into Common Criteria Mode. The Common Criteria configuration enforces stringent security processes. Default is **On**.
- **Enable reboot banner:** Displays a DoD approved system use notification message or banner when users' devices are restarted. Default is **Off**.
- **Allow settings changes:** Allows users to change settings on their fully managed devices. Default is **On**.
- **Enable background data usage:** Allows apps to sync data in the background. for fully managed devices. Default is **On**.
- **Allow clipboard:** Allow users to copy data to the clipboard on their devices. Default is **On**.
  - \* **Allow clipboard share:** Allow users to share clipboard content between their devices

and a computer (MDM 4.0 and later).

- **Allow home key:** Allows users to use the **Home** key on their fully managed devices. Default is **On**.
- **Allow mock location:** Allows users to fake their GPS location. For fully managed devices. Default is **Off**.
- **NFC:** Allows users to use NFC on their fully managed devices (MDM 3.0 and later). Default is **On**.
- **Allow power off:** Allows users to power off their fully managed devices (MDM 3.0 and later). Default is **On**.
- **Allow Wi-Fi direct:** Allows users to connect directly to another device through their Wi-Fi connection. Default is **On**. If **On**, you must enable the **Allow Wi-Fi changes** setting.
- **Allow SD card:** Allows users to use an SD card, if available, with their devices. Default is **On**.
- **Allow USB host storage:** Allows users' devices to act as the USB host when a USB device connects to their devices. Users' devices then supply power to the USB device. Default is **On**.
- **Allow voice dialer:** Allows users to use the voice dialer on their devices (MDM 4.0 and later). Default is **On**.
- **Allow S beam:** Allows users to share content with others using NFC and Wi-Fi Direct (MDM 4.0 and later). Default is **On**.
- **Allow S voice:** Allows users to use the intelligent personal assistant and knowledge navigator on their devices (MDM 4.0 and later). Default is **On**.
- **Allow USB tethering:** Allows users to share a mobile data connection with another device using their USB connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
- **Allow Bluetooth tethering:** Allows users to share a mobile data connection with another device using their Bluetooth connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
- **Allow Wi-Fi tethering:** Allows users to share a mobile data connection with another device using their Wi-Fi connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
- **Allow incoming MMS:** Allows users to receive MMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Allow outgoing MMS:** Allows users to send MMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Allow incoming SMS:** Allows users to receive SMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Allow outgoing SMS:** Allows users to send SMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.



- **Configure mobile networks:** Allows users to use their cellular data connection. Default is **Off**.
- **Limit by day (MB):** Enter the number of MB of mobile data users can use each day. The default is 0, which disables this feature (MDM 4.0 and later).
- **Limit by week (MB):** Enter the number of MB of mobile data users can use each week. The default is 0, which disables this feature (MDM 4.0 and later).
- **Limit by month (MB):** Enter the number of MB of mobile data users can use each month. The default is 0, which disables this feature (MDM 4.0 and later).
- **Allow only secure VPN connections:** Allows users to only use secure connections (MDM 4.0 and later). Default is **On**.
- **Allow audio recording:** Allows users to record audio with their devices (MDM 4.0 and later). Default is **On**. If **On** you must turn on the **Allow microphone** setting.
- **Allow video recording:** Allows users to record video with their devices (MDM 4.0 and later). Default is **Off**. If **On** you must turn on the **Allow use of camera** setting.
- **Allow push messages when roaming:** Allow users to use cellular data for pushing. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.
- **Allow automatic synchronization when roaming:** Allow users to use cellular data for syncing. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.
- **Allow voice calls when roaming:** Allow users to use cellular data for voice calls. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.
- **Samsung: Knox container/Fully managed device**
  - **Enable revocation check:** Enables checking for revoked certificates. Default is **Off**.
- **Samsung: Knox container only**
  - **Move apps to container:** Allows users to move apps between the Knox container and the personal area on their devices. Default is **On**.
  - **Enforce multi-factor authentication:** Users must use a fingerprint and one other authentication method, such as password or PIN, to open their devices. Default is **On**.
  - **Enforce authentication for container:** Use a different authentication method from the method used to unlock the device to open the KNOX container. Default is **On**.
  - **Enable secure keypad:** Forces users to use a secure keyboard inside the Knox container. Default is **On**.

## Android for Workspace (Preview) settings

- **Security**
  - **Allow account management:** Allows account to be added to in work profile and managed devices. Default is **Off**.

- **Allow screen capture:** Allows users to record or take a screen capture of the device screen. Default is **Off**.
- **Allow use of camera:** Allows users to take pictures and make videos with the device camera. Default is **Off**.
- **Allow VPN configuration:** Allows users to create VPN configurations. For work profile devices running Android 6 and later and for fully managed devices. Default is **On**.
- **Allow location sharing:** Allows location sharing. For managed profiles, the device owner can override this setting. Default is **Off**.
- **Allow user to configure user credentials:** Specify whether users can configure credentials in the managed keystore. Default is **On**.
- **Allow USB debugging:** Default is **Off**.

- **Apps**

- **Allow non-Google Play apps:** Allows the installation of apps from stores other than Google Play. Default is **Off**.
- **Disable applications:** Blocks a specified list of apps from running on devices. Default is **Off**. To disable an installed app, change the setting to **On** and then click **Add** in the **Application list** table.
  - \* **Application list:** A list of the apps you want to block. Set **Disable applications** to **On** and add the app. Type the app package name. Changing and deploying an app list overwrites the prior app list. For example: If you disable com.example1 and com.example2, and then later change the list to com.example1 and com.example3, Endpoint Management enables com.example.2.
- **Enable app verification:** Enables the OS to scan apps to detect malicious behavior. Default is **On**.

- **BYOD work profile**

- **Allow work profile contacts in device contacts:** Shows contacts from the managed Android Enterprise profile in the parent profile, for incoming calls (Android 7.0 and later). Default is **Off**.

## Samsung SAFE settings

### Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Allow hardware controls

- Enable ODE Trusted Boot Verification
- Allow Development Mode
- Allow Emergency Calls Only
- Allow Firmware Recovery
- Allow Fast Encryption
- Common Criteria Mode
- Factory reset
- Date Time Change
- DOD boot banner
- Settings changes

If you use Android Enterprise with Samsung SAFE, configure the restrictions on the Android Enterprise platform page. Some options are available only under specific Samsung Mobile Device Management APIs. Those options are marked with the relevant version information.

- **Allow hardware controls**

- **Enable ODE Trusted Boot verification:** Use ODE trusted boot verification to establish a chain of trust from the bootloader to the system image.
- **Allow Development Mode:** Allow users to enable the developer settings on their devices.
- **Allow emergency call only:** Allow users to enable Emergency Call Only mode on their devices.
- **Allow firmware recovery:** Allow users to recover the firmware on their devices.
- **Allow fast encryption:** Allow encryption of only used memory space. This setting contrasts with full disk encryption, which encrypts all data. That data includes settings, application data, downloaded files and applications, media, and other files.
- **Enable Common Criteria Mode:** Places the device into Common Criteria Mode. The Common Criteria configuration enforces stringent security processes.
- **Allow factory reset:** Allow users to do a factory reset on their devices.
- **Allow configuring date and time:** Allow users to change the date and time on their devices.
- **Enable reboot banner:** Display a DoD approved system use notification message or banner when users' devices are restarted.
- **Allow settings changes:** Allow users to change settings on their devices.

- **Allow backup service:** Allow users to back up application and system data on their devices.
- **Over-the-air upgrade:** Allow users' devices to receive software updates wirelessly (MDM 3.0 and later).
- **Allow background data usage:** Allow apps to sync data in the background.
- **Camera:** Allow users to use the camera on their devices.
- **Allow clipboard:** Allow users to copy data to the clipboard on their devices.
  - \* **Allow clipboard share:** Allow users to share clipboard content between their devices and a computer (MDM 4.0 and later).
- **Allow home key:** Allow users to use the **Home** key on their devices.
- **Allow microphone:** Allow users to use the microphone on their devices.
- **Allow mock location:** Allow users to fake their GPS location.
- **NFC:** Allow users to use NFC on their devices (MDM 3.0 and later).
- **Allow power off:** Allow users to power off their devices (MDM 3.0 and later).
- **Screen captures:** Allow users to take screenshots on their devices.
- **Allow SD card:** Allow users to use an SD card, if available, with their devices.
- **Allow voice dialer:** Allow users to use the voice dialer on their devices (MDM 4.0 and later).
- **Allow S Beam:** Allow users to share content with others using NFC and Wi-Fi Direct (MDM 4.0 and later).
- **Allow S Voice:** Allow users to use the intelligent personal assistant and knowledge navigator on their devices (MDM 4.0 and later).
- **Allow adding users:** Allows users to add new users on a device. Default is **On**.
- **Allow apps**
  - **Face recognition:** Allows users to use the face recognition app. Default is **On**.
  - **Browser:** Allow users to use the web browser.
  - **YouTube:** Allow users to access YouTube.
  - **Google Play/Marketplace:** Allow users to access Google Play and the Google Apps Marketplace.
  - **Allow Non-Google Play apps:** Allow users to download apps from sites other than Google Play and the Google Apps Marketplace. If **On**, a user can use the security settings on their device to trust apps from unknown sources.
  - **Force stop of system app:** Allow users to disable pre-installed system apps (MDM 4.0 and later).
  - **Disable applications:** If **On**, blocks a specified list of apps from running on Samsung SAFE devices. To disable an installed app, change the setting to **On** and then click **Add** in the **Application list** table.
    - \* **Application list:** A list of the apps you want to block. Set **Disable applications** to **On** and add the app. Type the app package name. Changing and deploying an app list overwrites the prior app list. For example: If you disable com.example1 and

com.example2, and then later change the list to com.example1 and com.example3, Endpoint Management enables com.example.2.

- **Network**

- **Allow incoming MMS:** Allow users to receive MMS messages.
- **Allow incoming SMS:** Allow users to receive SMS messages.
- **Allow outgoing MMS:** Allow users to send MMS messages.
- **Allow outgoing SMS:** Allow users send SMS messages.
- **Allow VPN configuration:** Allows users to create VPN configurations. For work profile devices running Android 6 and later and for fully managed devices. Default is **On**.
- **Allow bluetooth:** Allow users to use Bluetooth.
  - \* **Bluetooth tethering:** Allow users to share a mobile data connection with another device using their Bluetooth connection.
- **Wi-Fi:** Allow users to connect to Wi-Fi networks.
  - \* **Wi-Fi tethering:** Allow users to share a mobile data connection with another device using their Wi-Fi connection.
  - \* **Direct:** Allow users to connect directly to another device through their Wi-Fi connection (MDM 4.0 and later).
  - \* **State change:** Allow apps to change Wi-Fi connectivity state.
- **Allow tethering:** Allow users to share a mobile data connection with another device.
- **Allow configure mobile networks:** Allow users to use their cellular data connection.
- **Allow roaming:** Allow users to use cellular data while roaming. The default is Off, which disables roaming on users' devices.
- **Allow only secure VPN connections:** Allow users to only use secure connections (MDM 4.0 and later).
- **Allow NFC:** Allow users to send webpages, photos, videos, or other content from their devices to another device using NFC (MDM 4.0 and later).
- **Allow audio recording:** Allow users to record audio with their devices (MDM 4.0 and later).
- **Allow video recording:** Allow users to record video with their devices (MDM 4.0 and later).
- **Location services:** Allow users to turn on GPS on their devices.
- **Limit by day (MB):** Enter the number of MB of mobile data users can use each day. The default is 0, which disables this feature (MDM 4.0 and later).
- **Limit by week (MB):** Enter the number of MB of mobile data users can use each week. The default is 0, which disables this feature (MDM 4.0 and later).
- **Limit by month (MB):** Enter the number of MB of mobile data users can use each month. The default is 0, which disables this feature (MDM 4.0 and later).
- **Allow USB actions** Allow USB connection between users' devices and a computer.
  - **Allow USB debugging:** Allow debugging over USB.
  - **Allow USB host storage:** Allow users' devices to act as the USB host when a USB device connects to their devices. Users' devices then supply power to the USB device.

- **Allow USB mass storage:** Allow transfer of large data files between users' devices and a computer over a USB connection.
- **Allow file transfer:** Allows file transfers over USB. Default is **Off**.
- **USB:** Allow debugging over USB.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

## Samsung Knox settings

**Restrictions Policy**

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

- Allow use of camera
- Enable Revocation Check
- Move Apps To Container
- Enforce Multifactor Authentication
- Enable TIMA Key store
- Enforce Auth For Container
- Share List
- Enable Audit Log
- Use Secure Keypad
- Enable Google Apps

Enable Google Apps  ON

Authentication Smart Card Browser  ON

Enable Samsung DeX  ON ?

Allow Ethernet in DeX mode only ?

Upload DeX logo image ?

DeX screen timeout (seconds) \*  ?

Add App shortcut in Samsung DeX

Remove App shortcut in Samsung DeX

App packages to disable in Samsung DeX

If you use Android Enterprise with Samsung Knox, configure the restrictions on the Android Enterprise platform page. These options are available only under Samsung Knox Premium (minimum version is Knox 2.0).

- **Allow use of camera:** Allow users to use the camera on their devices.
- **Enable revocation check:** Enable checking for revoked certificates.
- **Move apps to container:** Allow users to move apps between the Knox container and the personal area on their devices.
- **Enforce multi-factor authentication:** Users must use a fingerprint and one other authentication method, such as password or PIN, to open their devices.
- **Enable TIMA Keystore:** The TIMA Keystore provides TrustZone-based secure key storage for the symmetric keys. RSA key pairs and certificates are routed to the default key store provider for storage.
- **Enforce authentication for container:** Use a different authentication method from the method used to unlock the device to open the KNOX container.
- **Allow share list:** Allow users to share content between apps in the Share Via list.
- **Enable audit log:** Enable creation of event audit logs for forensic analysis of a device.
- **Enable secure keypad:** Force users to use a secure keyboard inside the Knox container.
- **Enable Google apps:** Allow users to download apps from Google Mobile Services into the Knox container.
- **Authentication Smart Card Browser:** Enable browser authentication on devices equipped with a smart card reader.
- **Enable Samsung DeX:** Enables supported Knox-enabled devices to run in Samsung DeX mode. Requires Samsung Knox 3.1 (minimum version). Default is **On**. For information about Samsung DeX device requirements and setting up Samsung DeX, see [How Samsung DeX works](#).
  - **Allow Ethernet in DeX mode only:** Enable use of Ethernet in Samsung DeX mode. Cellular data, Wi-Fi, and tethering (Wi-Fi, Bluetooth, and USB) are restricted in DeX mode.

- **Upload DeX logo image:** Select this setting to specify a .png image to use as an icon for Samsung DeX.
- **DeX screen timeout (seconds):** Specify the amount of idle time, in seconds, after which the DeX screen turns off. To disable the timeout, type **0**. Default is **1200** seconds (20 minutes).
- **Add app shortcut in Samsung DeX:** Specify an app package name to add a shortcut for the app to DeX. To look up an app package name, go to Google Play and select the app. The URL includes the package name: `https://play.google.com/store/apps/details?id=<package.name>`.
- **Remove app shortcut in Samsung DeX:** Specify an app package name to remove a shortcut from DeX. Go to Google Play to look up app package names.
- **App packages to disable in Samsung DeX:** Specify a comma-separated list of the app packages that you want to block from Samsung DeX mode. For example: `"com.android.chrome", "com.google.android.gm"`.

## Windows Phone and Windows Desktop/Tablet settings

### Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

WiFi Settings

- Allow WiFi
- Allow Internet sharing
- Allow auto-connect to WiFi Sense hotspots
- Allow manual configuration

Connectivity

- Allow NFC
- Allow bluetooth
- Allow VPN over cellular
- Allow VPN over cellular while roaming
- Allow USB connection

- **Wi-Fi Settings**
  - **Allow Wi-Fi:** Allow a device to connect to a Wi-Fi network. Windows Phone only.
  - **Allow Internet sharing:** Allow a device to share its internet connection with other devices by turning it into a Wi-Fi hotspot.
  - **Allow manual configuration:** Allow users to manually configure Wi-Fi connections. Windows Phone only.
- **Connectivity**



- **Allow NFC:** Allow device to communicate with an NFC tag or another NFC-enabled transmitting device. Windows Phone only.
- **Allow bluetooth:** Allow device to connect through Bluetooth.
- **Allow VPN over cellular:** Allow the device to connect over VPN to a cellular network.
- **Allow VPN over cellular while roaming:** Allow the device to connect over VPN when the device roams over cellular networks.
- **Allow USB connection:** Allow a desktop to access a device's storage through a USB connection. Windows Phone only.
- **Allow cellular data roaming:** Allow users to use cellular data while roaming.
- **Accounts**
  - **Allow Microsoft account connection:** Allow the device to use a Microsoft account for non-email related connection authentication and services.
  - **Allow non-Microsoft email:** Allow user to add non-Microsoft email accounts.
- **Search:** Windows Phone only.
  - **Allow search to use location:** Allow searches to use the device's location service.
  - **Filter adult content:** Allow adult content. The default is **Off**, which means adult content is not filtered.
  - **Allow Bing Vision to store images:** Allow Bing Vision to store images captured when performing Bing Vision searches.
- **System**
  - **Allow storage card:** Allow the device to use a storage card.
  - **Telemetry:** In the list, click an option to allow or restrict the device from sending telemetry information. The default is **Allowed**. Other options are **Not allowed** and **Allowed, except for secondary data request**.
  - **Allow location services:** Allow location services.
  - **Allow preview of internal builds:** Allow users to preview Microsoft internal builds.
- **Camera:** Windows Desktop/Tablet only
  - **Allow use of camera:** Allow users to use their device camera.
- **Bluetooth:** Windows Desktop/Tablet only
  - **Allow discoverable mode:** Allow Bluetooth devices to find the local device.
  - **Local device name:** A name for the local device.
- **Security:** Windows Phone only
  - **Allow manual root certificate installation:** Allow users to manually install a root certificate.
  - **Require device encryption:** Require device encryption. After encryption is enabled on a device, it cannot be disabled. The default is **Off**.
  - **Allow copy and paste:** Allow users to copy and paste data on their devices.
  - **Allow screen capture:** Allow users to create screen captures on their devices.
  - **Allow voice recording:** Allow users to use voice recording on their devices.

- **Allow Save As of Office files:** Allow users to save Office files with Save As.
- **Allow action center notifications:** Allow Action Center notifications on the device lock screen.
- **Allow Cortana:** Allow users access to Cortana, the intelligent personal assistant and knowledge navigator.
- **Allow sync of device settings:** Allow users to sync settings between Windows Phone 8.1 devices when roaming.
- **Experience:** Windows Desktop/Tablet only
  - **Allow Cortana:** Allow users access to Cortana, the intelligent personal assistant and knowledge navigator.
  - **Allow device discovery:** Allow network discovery of the device.
  - **Allow manual MDM unenrollment:** Allow users to manually unenroll their device from Endpoint Management MDM.
  - **Allow sync of device settings:** Allow users to sync settings between Windows 10 and Windows 11 devices when roaming.
- **Above Lock:** Windows Desktop/Tablet only
  - **Allow toasts:** Allow toast notifications on the lock screen. Windows Desktop/Tablet only
- **Apps**
  - **Allow store access:** Allow users to access the Microsoft Store. Windows Phone only.
  - **Allow developer unlock:** Allow users to register their devices with Microsoft and develop or install apps that are not in the Windows Phone app store. Windows Phone only.
  - **Allow web browser access:** Allow Internet Explorer on the device. Windows Phone only.
  - **Allow automatic updates from app store:** Allow apps from the app store to automatically update. Windows Desktop/Tablet only.
- **Privacy:** Windows Desktop/Tablet only
  - **Allow input personalization:** Allows the input personalization service to run. The input personalization service improves predictive inputs such as pen and touch keyboard based on what a user types.
- **Settings:** Windows Desktop/Tablet only.
  - **Allow auto play:** Allows users to change Auto Play settings.
  - **Allow data sense:** Allows users to change Data Sense settings.
  - **Allow date time:** Allows users to change date and time settings.
  - **Allow language:** Allows users to change language settings.
  - **Allow power sleep:** Allows users to change power and sleep settings.
  - **Allow region:** Allows users to change region settings.
  - **Allow sign-in options:** Allows users to change sign-in settings.
  - **Allow workplace:** Allows users to change workplace settings.
  - **Allow your account:** Allows users to change account settings.

## Amazon settings

### Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Allow hardware controls

- Factory reset
- Profiles

Allow apps

- Non-Amazon Appstore apps
- Social networks

Network

- Bluetooth
- WiFi switch
- WiFi settings
- Cellular data
- Roaming data

- **Allow hardware controls**
  - **Factory reset:** Allow users to do a factory reset on their devices
  - **Profiles:** Allow users to change the hardware profile on their devices.
- **Allow apps**
  - **Non-Amazon Appstore apps:** Allow users to install non-Amazon app store apps on their devices.
  - **Social networks:** Allow users to access social networks from their devices.
- **Network**
  - **Bluetooth:** Allow users to use Bluetooth.
  - **Wi-Fi switch:** Allow apps to change Wi-Fi connectivity state.
  - **Wi-Fi settings:** Allow users to change Wi-Fi settings.
  - **Configure mobile networks:** Allow users to use their cellular data connection.
  - **Roaming data:** Allow users to use cellular data while roaming.
  - **Location services:** Allow users to use GPS.
- **USB actions:**
  - **Debugging:** Allow users' devices to connect through USB to a computer for debugging.

## Chrome OS settings

### User policy

#### Restrictions Policy x

User policy

- Disable form autofill  ON ?
- Disable password saving  ON ?
- Disable page translation  ON ?
- Block images  ON ?
- Disable Incognito mode  ON ?
- Disable saving browsing history  OFF ?
- Disable deleting browsing and download history  OFF ?
- Disable printing  OFF ?
- Disable proceeding from the safe browsing warning page  ON ?
- Safe browsing mode  ON ?
- Enable bookmarks bar  ON ?
- Disable bookmarks bar edit  ON ?
- Disable task manager end process  ON ?
- Show home button  ON ?
- External storage accessibility  ?
- Websites  Allow list  Block list

Allowed websites \* Add

- **Disable form autofill:** Select whether to allow the autofill function of the Chrome browser. If this policy is set to **On**, the autofill function is not allowed. Default is **On**.
- **Disable password saving:** Select whether to allow the save password function in the Chrome browser. If this policy is set to **On**, the save password function not allowed. Default is **On**.
- **Disable page translation:** Select whether to allow translation of webpages that are in other languages in the Chrome browser. If this policy is set to **On**, translation of webpages is not allowed. Default is **On**.

- **Block images:** Select whether to allow display of images in webpages in the Chrome browser. If this policy is set to **On**, images in webpages in the Chrome browser are not displayed. Default is **Off**.
- **Disable Incognito mode:** If **On**, Chrome OS device users can't open an Incognito window in Chrome. Requires Google Workspace Chrome configuration. Default is **On**.
- **Disable saving browsing history:** If **On**, users can't save browsing history, override this setting, or sync tabs from Chrome OS devices. Requires Google Workspace Chrome configuration. Default is **Off**.
- **Disable deleting browsing and download history:** If **On**, users can't delete browsing or download history from Chrome OS devices. However, even if you prevent users from deleting history from Chrome, users might be able to edit or delete the history database files directly. The browser itself can expire or archive any or all history items at any time. Requires Google Workspace Chrome configuration. Default is **Off**.
- **Disable printing:** If **On**, users can't print from Google Chrome. Printing is disabled in locations such as the wrench menu, extensions, and Javascript apps. Printing is possible from plug-ins that bypass Google Chrome to print, such as Flash apps with a Print command in their context menu. Requires Google Workspace Chrome configuration. Default is **Off**.
- **Disable proceeding from the safe browsing warning page:** If **Off**, users can continue from the warning page to visit the potentially malicious site from Chrome OS devices. Requires Google Workspace Chrome configuration. Default is **On**.
- **Safe browsing mode:** If **Off**, Google Safe Browsing mode is never active. Users can't change or override the "Protect you and your device from dangerous sites" setting in Chrome. Requires Google Workspace Chrome configuration. Default is **On**.
- **Enable bookmarks bar:** If **On**, Chrome displays the bookmarks bar. Requires Google Workspace Chrome configuration. Default is **On**.
- **Disable bookmarks bar edit:** If **On**, users can't add, update, or delete bookmarks. Requires Google Workspace Chrome configuration. Default is **On**.
- **Disable task manager end process:** If **On**, disables the **End Process** button in **Task Manager**. Requires Google Workspace Chrome configuration. Default is **On**.
- **Show home button:** If **On**, Chrome displays the browser home button. Requires Google Workspace Chrome configuration. Default is **On**.
- **External storage accessibility:** Controls how users access external storage devices through the file browser. Requires Google Workspace Chrome configuration. Options:
  - **Disabled:** No access to external storage.
  - **Read only:** Users can have read access external storage only.

- **Write only:** Users can have write access external storage only.

Default is **Disabled**.

- **Websites:** Select whether to control access to websites in the Chrome browser using an allow or block list. If you choose **Allow list**, specify a list of allowed URLs. If you choose **Block list**, specify a list of URL exceptions to the block list in Chrome policies in the Google admin console. The most specific filter determines if a URL is blocked or allowed. The allow list takes precedence over the block list. Default is **Block list**. After you make a selection, click **Add** to add a list of websites.
- **Extension sources:** Specify the list of URLs that allow users to install extensions, apps, and themes.

## Device policy

Restrictions Policy	Device Policy
1 Policy Info	Disable Guest user mode <input type="checkbox"/> OFF ⓘ
2 Platforms <span>Clear All</span>	Single sign-on IDP redirection <input checked="" type="checkbox"/> ON ⓘ
<input checked="" type="checkbox"/> iOS	Enable device state reporting <input checked="" type="checkbox"/> ON ⓘ
<input checked="" type="checkbox"/> macOS	Enable recent users reporting <input checked="" type="checkbox"/> ON ⓘ
<input checked="" type="checkbox"/> TV OS	Single sign-on cookie behavior <input checked="" type="checkbox"/> ON ⓘ
<input checked="" type="checkbox"/> Android	Enable App Runtime for Chrome (ARC) <input checked="" type="checkbox"/> ON ⓘ
<input checked="" type="checkbox"/> Android Enterprise	Force re-enrollment <input checked="" type="checkbox"/> ON ⓘ
<input checked="" type="checkbox"/> Samsung SAFE	Device Disabled Message <input type="text"/> ⓘ
<input checked="" type="checkbox"/> Samsung KNOX	Sign-in auto complete domain name <input type="text"/> ⓘ
<input checked="" type="checkbox"/> Windows Phone	Device time zone settings <input checked="" type="radio"/> System time zone
<input checked="" type="checkbox"/> Windows Desktop/Tablet	<input type="radio"/> Time zone detection
<input checked="" type="checkbox"/> Amazon	System time zone (UTC-7:00) Pacific Daylight Time (Los Ange... ⓘ
<input checked="" type="checkbox"/> Windows Mobile/CE	<input type="text"/> ⓘ
<input checked="" type="checkbox"/> Chrome OS	<input type="text"/> ⓘ
3 Assignment	Users allowed to sign on ⓘ <input type="button" value="Add"/>

- **Disable Guest user mode:** If **On**, guest users can't sign on to Chrome OS devices. Requires Google Workspace Chrome configuration. The default is **Off**.
- **Single sign-on IDP redirection:** If **On**, enables SAML-based single sign-on. Requires Google Workspace Chrome configuration. The default is **On**.
- **Enable device state reporting:** If **On**, a device reports its current device state, including firmware, Chrome and platform version, and boot mode. Requires Google Workspace Chrome configuration. Default is **On**.
- **Enable recent users reporting:** If **On**, the device reports a list of users that recently logged on to the device. Users aren't reported if the device is configured to erase all local user data.

Requires Google Workspace Chrome configuration. Default is **On**.

- **Single sign-on cookie behavior:** If **On**, transfers cookies set by a SAML IdP to user profiles each time a user signs on with SAML credentials. If **Off**, cookies transfer during the first sign-on only. Requires Google Workspace Chrome configuration. The default is **On**.
- **Enable App Runtime for Chrome (ARC):** If **On**, allows enrolled Chrome OS device users to run Android apps. Specify ARC apps in the App Restrictions device policy. Requires Google Workspace Chrome configuration. ARC isn't available if either Ephemeral mode or multiple sign-on is enabled in the current user session. If **Off**, enterprise Chrome OS device users can't run Android apps. The default is **On**.
- **Forced re-enrollment:** If **On**, forces devices to re-enroll into their previous Google Workspace domain after a device wipe. Requires Google Workspace Chrome configuration. Default is **On**.
- **Device Disabled Message:** If the device is disabled for any reason, the user sees the message entered into this text box.
- **Sign-in autocomplete domain name:** If set to a domain name, such as `students.school.edu`, Chrome shows the domain name as an autocomplete option when users sign in. If left blank, Chrome doesn't show an autocomplete option for the domain name. Requires Google Workspace Chrome configuration.
- **Device time zone settings:**
  - **System time zone:** Selects the time zone for the Chrome device.
  - **Time zone detection:** Specifies the settings used to detect the time zone. Requires Google Workspace Chrome configuration.
    - \* **Users decide:** Allows users to configure the policy through the standard Date and Time settings on the Chrome OS device.
    - \* **Disabled:** Denies access to the time zone information.
    - \* **IP only:** Sets the time zone based on the device IP address.
    - \* **WiFi access points:** Sets the time zone based on the user's Wi-Fi connection.
    - \* **Use Location info:** Sets the time zone by detecting the user's present location.
- **Users allowed to sign on:** Limits the users who can sign on to Chrome OS devices, based on an email suffix, such as `*@example.com`.

## Roaming device policy

December 17, 2018

You can add a device policy in Endpoint Management to configure whether to allow voice and data roaming on supported iOS devices. When voice roaming is disabled, data roaming is automatically disabled.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device](#)

[policies.](#)

## iOS settings

- **Disable voice roaming:** Select whether to disable voice roaming. When this option is enabled, data roaming is automatically disabled. The default is **Off**, which allows voice roaming.
- **Disable data roaming:** Select whether to disable data roaming. This option is available only when voice roaming is enabled. The default is **Off**, which allows data roaming.

## Samsung MDM license key device policy

August 31, 2021

Use the Samsung MDM license key device policy if you have legacy Enterprise Licenses (ELM) and Knox Licenses (KLM). If you have a Knox Platform for Enterprise (KPE) premium license key, use the [Knox Platform for Enterprise device policy](#) instead. A premium license key is required to create a Knox container.

For the SAFE platform, use the macro to generate the ELM key. Deploy the Samsung Enterprise License Management (ELM) key to a device before you can deploy SAFE policies and restrictions. Endpoint Management also supports the Samsung Enterprise Firmware-Over-The-Air (E-FOTA) service. Endpoint Management supports and extends both Samsung for Enterprise (SAFE) and Samsung Knox policies.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Samsung SAFE settings

Device Policies	Apps	Actions	ShareFile	Delivery Groups
<b>Samsung MDM License Key Policy</b> For the SAFE platform, use the macro to generate the ELM key. For the KNOX platform, as a prerequisite, you need to purchase a Samsung KNOX Workspace license. You then provide the license key in order to enable the KNOX APIs and deploy KNOX policies and restrictions to devices.				
1 Policy Info	<b>ELM license key *</b> <input type="text" value="\${elm.license.key}"/>			
2 Platforms	Enterprise FOTA			
<input checked="" type="checkbox"/> Samsung SAFE <input checked="" type="checkbox"/> Samsung KNOX	<b>Enterprise FOTA Customer ID</b> <input type="text"/> ⓘ			
	<b>Enterprise FOTA license</b> <input type="text"/> ⓘ			
	<b>Client ID</b> <input type="text"/> ⓘ			
3 Assignment	<b>Client Secret</b> <input type="text"/> ⓘ			

- **ELM License key:** Endpoint Management pre-fills this field with the macro that generates the ELM license key. If the field is blank, type this macro: `${elm.license.key}`



## Configure Samsung E-FOTA settings

Samsung Enterprise FOTA (E-FOTA) lets you determine when devices get updated and the firmware version to use. E-FOTA enables you to test updates before deploying them, to ensure that the updates are compatible with your apps. You can force devices to update with the latest firmware version available, without requiring user interaction.

Samsung supports E-FOTA for Samsung Knox 2.7.1 devices (minimum version) that are running authorized firmware.

Citrix Endpoint Management supports adding devices from the Endpoint Management console to Knox E-FOTA One. For more information about exporting a device list from Endpoint Management, see [Export the Devices table](#). For more information about adding a device to Knox E-FOTA One, see the [Samsung documentation](#).

Citrix Endpoint Management does not support the Knox E-FOTA on MDM solution.

To configure an E-FOTA policy:

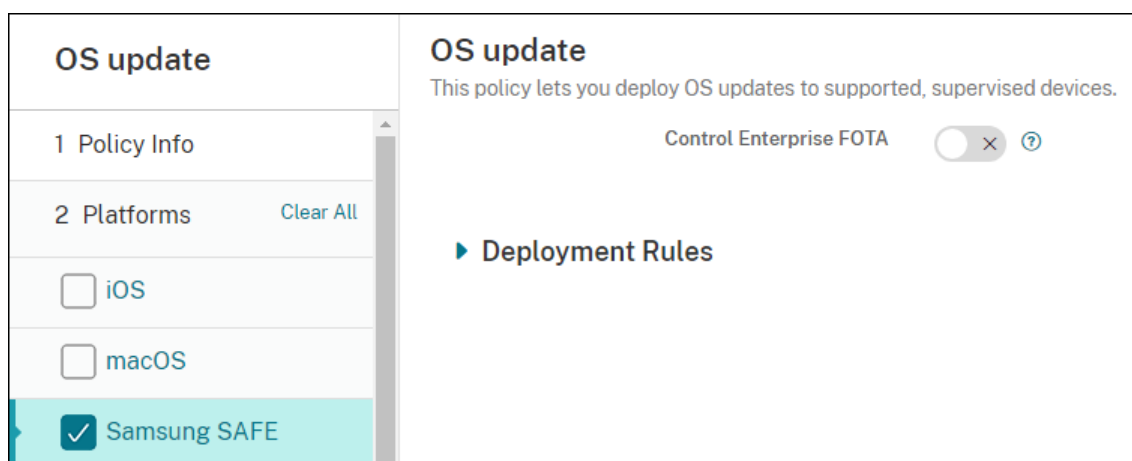
1. Create a Samsung MDM License Key device policy with the keys and license information you received from Samsung. Endpoint Management then validates and registers the information. If Endpoint Management detects an E-FOTA issue, an error message appears to indicate the problem. Use the code provided to troubleshoot the issue. For more information, see [Error codes](#) in Samsung documentation.

Type the **ELM License key**: Endpoint Management pre-fills this field with the macro that generates the ELM license key. If the field is blank, type this macro: `#{elm.license.key}`

Type the following information provided by Samsung when you purchased an E-FOTA package:

- **Enterprise FOTA Customer ID**
- **Enterprise FOTA license**
- **Client ID**
- **Client Secret**

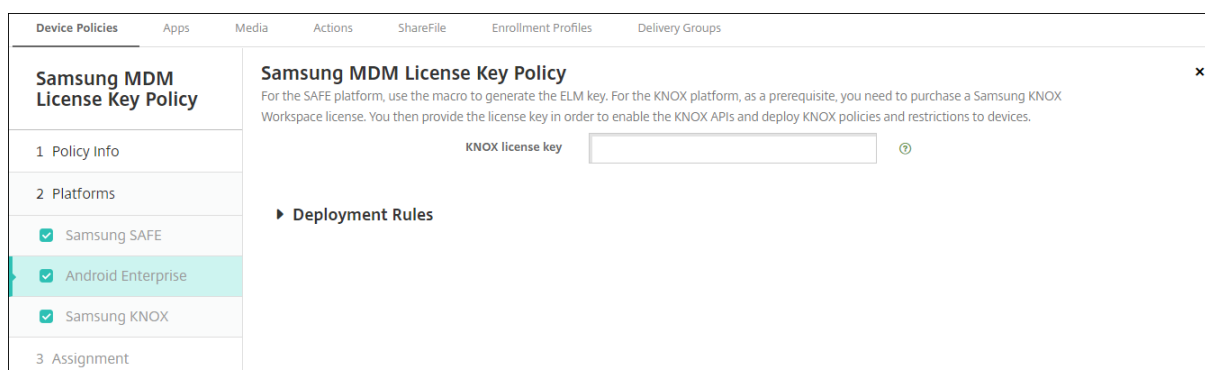
2. Create a Control OS Update device policy.



- **Enable Enterprise FOTA:** Set to **On**.
- **Enterprise FOTA License Key:** Select the Samsung MDM License Key policy name that you created in Step 1.

3. Deploy the Control OS Update policy to Secure Hub.

## Android Enterprise and Samsung Knox settings



- **Knox license key:** Type the Knox license key that you obtained from Samsung.

## SCEP device policy

June 9, 2021

This policy lets you configure iOS and macOS devices to retrieve a certificate from an external SCEP server over the Simple Certificate Enrollment Protocol (SCEP). To deliver a certificate to devices using SCEP from a PKI that is connected to Endpoint Management, create a PKI entity and a PKI provider in distributed mode. For details, see [PKI Entities](#).

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<b>SCEP Policy</b>						
This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.						
<b>SCEP Policy</b>		<b>URL base *</b> <input type="text"/>				
1 Policy Info		<b>Instance name *</b> <input type="text"/>				
2 Platforms		<b>Subject X.500 name (RFC 2253)</b> <input type="text"/>				
<input checked="" type="checkbox"/> iOS		<b>Subject alternative names type</b> <input type="text" value="None"/>				
<input checked="" type="checkbox"/> macOS		<b>Maximum retries</b> <input type="text" value="3"/>				
3 Assignment		<b>Retry delay</b> <input type="text" value="10"/>				
		<b>Challenge password</b> <input type="text"/>				
		<b>Key size (bits)</b> <input type="text" value="1024"/>				
		<b>Use as digital signature</b> <input type="checkbox" value="OFF"/>				
		<b>Use for key encipherment</b> <input type="checkbox" value="OFF"/>				

- **URL base:** Type the address of the SCEP server to define where SCEP requests are sent, over HTTP or HTTPS. The private key isn't sent with the Certificate Signing Request (CSR), so it might be safe to send the request unencrypted. If the one-time password is configured for reuse, use HTTPS to protect the password. This step is required.
- **Instance name:** Type any string that the SCEP server recognizes. For example, it could be a domain name like example.org. If a CA has multiple CA certificates, you can use this field to distinguish the required domain. This step is required.
- **Subject X.500 name (RFC 2253):** Type the representation of an X.500 name as an array of Object Identifier (OID) and value. For example, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, which translates to: [ [ [ "C", "US" ] ], [ [ "O", "Apple Inc." ] ], ..., [ [ "1.2.5.3", "bar" ] ] ]. You can represent OIDs as dotted numbers with shortcuts for country (C), locality (L), state (ST), organization (O), organizational unit (OU), and common name (CN).
- **Subject alternative names type:** Select an alternative name type. An optional alternative name type can provide the values required by the CA for issuing a certificate. You can specify **None**, **RFC 822 name**, **DNS name**, or **URI**.
- **Maximum retries:** Type the number of times a device should retry when the SCEP server sends a PENDING response. The default is **3**.
- **Retry delay:** Type the number of seconds to wait between subsequent retries. The first retry is attempted without delay. The default is **10**.

- **Challenge password:** Enter a pre-shared secret.
- **Key size (bits):** Select **2048** or higher as the key size in bits.
- **Use as digital signature:** Choose whether to use the certificate as a digital signature. The SCEP server verifies the certificate use as a digital signature before using the public key to decrypt the hash.
- **Use for key encipherment:** Choose whether to use the certificate for key encipherment. A server first checks whether the certificate provided by a client is allowed for key encipherment. Then the server uses the public key in a certificate to verify that a piece of data was encrypted using the private key. If not, the operation fails.
- **SHA-256 fingerprint (hexadecimal string):** If your CA uses HTTP, use this field to provide the fingerprint of the CA certificate. The device uses the fingerprint to confirm the authenticity of the CA response during enrollment. You can provide a SHA-256 fingerprint, or you can select a certificate to import its signature.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

## macOS settings

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<b>SCEP Policy</b>						
This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.						
<b>SCEP Policy</b>		<p><b>URL base *</b> <input type="text"/></p> <p><b>Instance name *</b> <input type="text"/></p> <p><b>Subject X.509 name (RFC 2253)</b> <input type="text"/></p> <p><b>Subject alternative names type</b> <input type="text" value="None"/></p> <p><b>Maximum retries</b> <input type="text" value="3"/></p> <p><b>Retry delay</b> <input type="text" value="10"/></p> <p><b>Challenge password</b> <input type="text"/></p> <p><b>Key size (bits)</b> <input type="text" value="1024"/></p> <p><b>Use as digital signature</b> <input type="checkbox" value="OFF"/></p> <p><b>Use for key encipherment</b> <input type="checkbox" value="OFF"/></p>				
1 Policy Info						
2 Platforms		<p><input type="checkbox"/> iOS</p> <p><input checked="" type="checkbox"/> macOS</p>				
3 Assignment						

- **URL base:** Type the address of the SCEP server to define where SCEP requests are sent, over HTTP or HTTPS. The private key isn't sent with the Certificate Signing Request (CSR), so it might

be safe to send the request unencrypted. If the one-time password is configured for reuse, use HTTPS to protect the password. This step is required.

- **Instance name:** Type any string that the SCEP server recognizes. For example, it could be a domain name like example.org. If a CA has multiple CA certificates, you can use this field to distinguish the required domain. This step is required.
- **Subject X.500 name (RFC 2253):** Type the representation of an X.500 name as an array of Object Identifier (OID) and value. For example, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, which translates to: [ [ [ "C" , "US" ] ], [ [ "O" , "Apple Inc." ] ], ..., [ [ "1.2.5.3" , "bar" ] ] ]. You can represent OIDs as dotted numbers with shortcuts for country (C), locality (L), state (ST), organization (O), organizational unit (OU), and common name (CN).
- **Subject alternative names type:** Select an alternative name type. An optional alternative name type can provide the values required by the CA for issuing a certificate. You can specify **None, RFC 822 name, DNS name, or URI.**
- **Maximum retries:** Type the number of times a device should retry when the SCEP server sends a PENDING response. The default is **3**.
- **Retry delay:** Type the number of seconds to wait between subsequent retries. The first retry is attempted without delay. The default is **10**.
- **Challenge password:** Type a pre-shared secret.
- **Key size (bits):** Select **2048** or higher as the key size in bits.
- **Use as digital signature:** Choose whether to use the certificate as a digital signature. The SCEP server verifies the certificate use as a digital signature before using the public key to decrypt the hash.
- **Use for key encipherment:** Choose whether to use the certificate for key encipherment. A server first checks whether the certificate provided by a client is allowed for key encipherment. Then the server uses the public key in a certificate to verify that a piece of data was encrypted using the private key. If not, the operation fails.
- **SHA-256 fingerprint (hexadecimal string):** If your CA uses HTTP, use this field to provide the fingerprint of the CA certificate. The device uses the fingerprint to confirm the authenticity of the CA response during enrollment. You can provide a SHA-256 fingerprint, or you can select a certificate to import its signature.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.

- \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
- **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
- **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

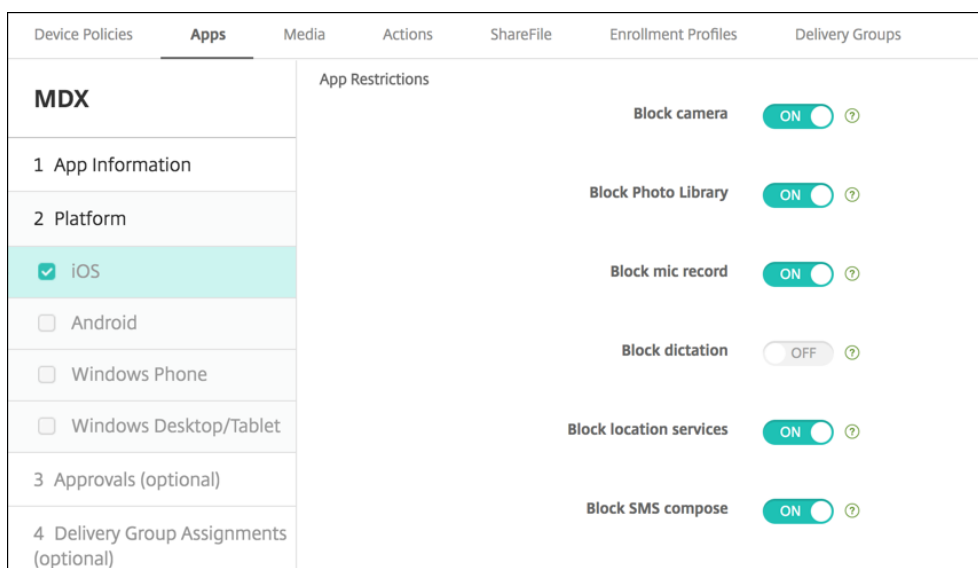
## Siri and dictation policies

April 16, 2020

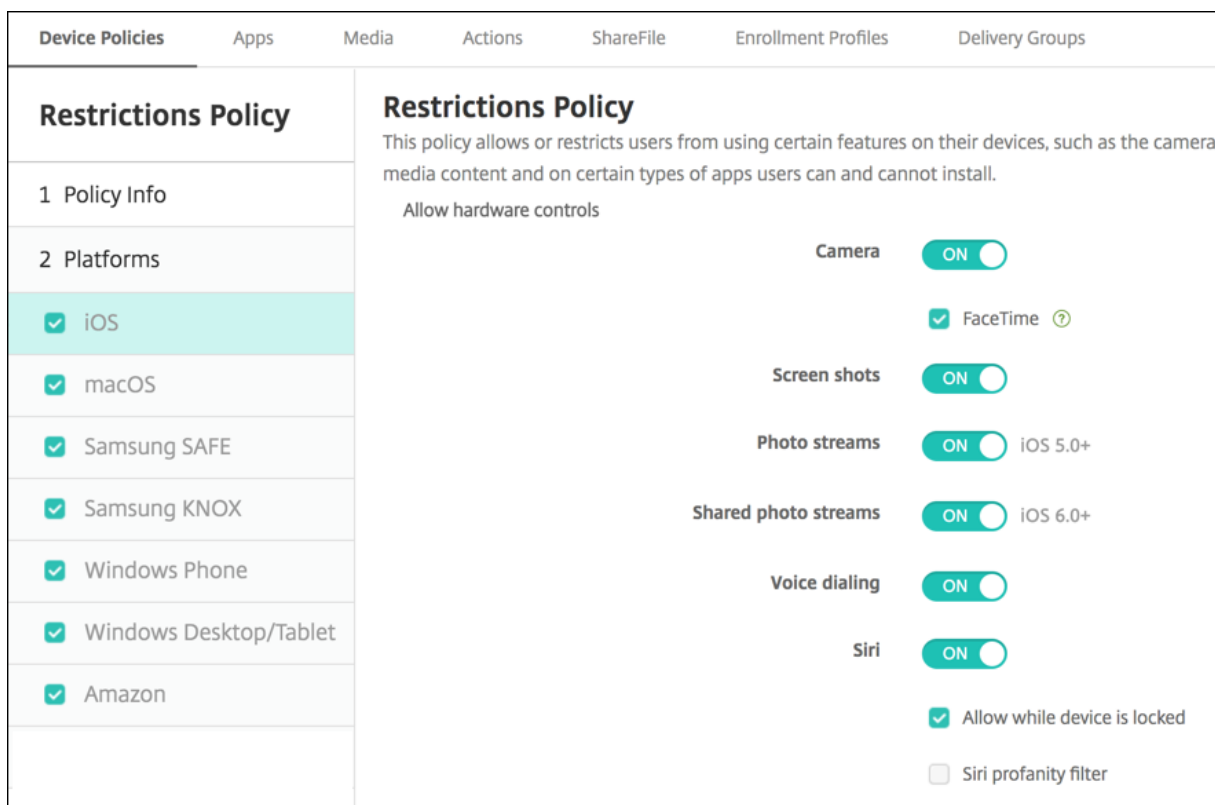
When users ask Siri something or dictate text on managed iOS devices, Apple collects the voice data for purposes of improving Siri. The voice data passes through Apple’s cloud-based services, and therefore exists outside the secure Endpoint Management container. The text that results from dictation, however, remains within the container.

Endpoint Management allows you to block Siri and dictation services, as your security needs require.

In MAM deployments, the **Block dictation** policy for each app is **On** by default, which disables the device’s microphone. Set it to **Off** if you want to allow dictation. You can find the policy in the Endpoint Management console at **Configure > Apps**. Select the app, click **Edit**, then click **iOS**.



In MDM deployments, you can also disable Siri with the Siri policy at **Configure > Device Policies**. The use of Siri is allowed by default.



A few points to keep in mind when deciding whether to allow Siri and dictation:

- According to information that Apple has made public, Apple keeps Siri and dictation voice clip data for up to two years. The data is assigned a random number to represent the user, and voice files are associated with this random number.
- You can review the Apple privacy policy by going to **Settings > General > Keyboards** on any iOS device and tapping the link under **Enable Dictation**.

## SSO account device policy

March 24, 2020

The SSO account device policy device policy lets ou create single sign-on (SSO) accounts in Endpoint Management. Those accounts let users sign on one-time only to access Endpoint Management and your internal company resources from various apps. Users do not need to store any credentials on the device. The SSO account enterprise user credentials are used across apps, including apps from the App Store. This policy is designed to work with a Kerberos authentication backend.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

- **Account name:** Enter the Kerberos SSO account name that appears on users' devices. This field is required.
- **Kerberos principal name:** Enter the Kerberos principal name. This field is required.
- **Identity credential (Keystore or PKI credential):** In the list, click an optional identity credential that can be used to renew the Kerberos credential without user interaction.
- **Kerberos realm:** Enter the Kerberos realm for this policy. This is typically your domain name in all capital letters (for example, EXAMPLE.COM). This field is required.
- **Permitted URLs:** For each URL for which you want to require SSO, click **Add** and then do the following:
  - **Permitted URL:** Enter a URL that you want to require SSO when a user visits the URL from the iOS device.  
For example, when a user tries to browse to a site and the web site initiates a Kerberos challenge: If that site is not in the URL list, the iOS device does not attempt SSO by providing the Kerberos token that Kerberos might have cached on the device from a previous Kerberos logon. The match has to be exact on the host part of the URL. For example, <https://shopping.apple.com> is valid, but [https://\\*.apple.com](https://*.apple.com) is not.  
Also, if Kerberos is not activated based on host matching, the URL still falls back to a standard HTTP call. This could mean almost anything including a standard password challenge or an HTTP error if the URL is only configured for SSO using Kerberos.
  - Click **Add** to add the URL or click **Cancel** to cancel adding the URL.
- **App Identifiers:** For each app that is allowed to use this login, click **Add** and then do the following:
  - **App Identifier:** Enter an app identifier for an app that is allowed to use this login. If you do not add any app identifiers, this login matches **all** app identifiers.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

## Storage encryption device policy

January 6, 2021

You create storage encryption device policies in Endpoint Management to encrypt internal and external storage, and, depending on the device, to prevent users from using a storage card on their devices.



You can create policies for Samsung SAFE and Windows Phone. Each platform requires a different set of values, which are described in detail in this article.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Prerequisites

For Samsung SAFE devices, make sure the following requirements are met before you configure this policy:

- Set the Screen Lock option on user devices.
- Plug in users devices and charge them to at least 80%.
- Make sure that the devices require a password containing both numbers and letters or symbols.

## Samsung SAFE settings

- **Encrypt internal storage:** Select whether to encrypt internal storage on users' devices. Internal storage includes device memory and internal storage. The default is **On**.
- **Encrypt external storage:** Select whether to encrypt external storage on users' devices. The default is **On**.

## Windows Phone settings

- **Require device encryption:** Select whether to encrypt users' devices. The default is **Off**.
- **Disable storage card:** Select whether to prevent users from using a storage card on their devices. The default is **Off**.

## Store device policy

April 6, 2020

You can create a policy in Endpoint Management to specify whether devices display an app store web clip on the home screen.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS, Android, and Windows Desktop/Tablet settings

For each platform that you configure, select whether an app store web clip appears on user devices. The default is **On**.

## Subscribed calendars device policy

March 24, 2020

You can add a device policy in Endpoint Management to add a subscribed calendar to the calendars list on iOS devices. The list of public calendars to which you can subscribe is available on the Apple Support site in Downloads.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Prerequisite

You must have subscribed to a calendar before you can add it to the subscribed calendars list on user devices.

### iOS settings

- **Description:** Enter a description of the calendar. This field is required.
- **URL:** Enter the calendar URL. You can enter a `webcal://` URL or an `https://` link to an iCalendar file (.ics). This field is required.
- **User name:** Enter the user's logon name. This field is required.
- **Password:** Enter an optional user password.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the calendar. The default is **Off**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

## Terms and conditions device policy

August 21, 2018

You create terms and conditions device policies in Endpoint Management when you want users to accept your company's specific policies governing connections to the corporate network. When users enroll their devices with Endpoint Management, they are presented with the terms and conditions and must accept them to enroll their devices. Declining the terms and conditions cancels the enrollment process.

You can create different policies for terms and conditions in different languages if your company has international users and you want them to accept terms and conditions in their native languages. You must provide a file for each platform and language combination you plan to deploy. For Android and iOS devices, you must supply PDF files. For Windows devices, you must supply text (.txt) files and accompanying image files.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### iOS and Android settings

- **File to be imported:** Select the terms and conditions file to import by clicking **Browse** and then navigating to the file's location.
- **Default Terms & Conditions:** Select whether this file is the default document for users who are members of multiple groups with different terms and conditions. The default is **Off**.

### Windows Phone and Windows Tablet settings

- **File to be imported:** Select the terms and conditions file to import by clicking **Browse** and then navigating to the file's location.
- **Image:** Select the image file to import by clicking **Browse** and then navigating to the file's location.
- **Default Terms & Conditions:** Select whether this file is the default document for users who are members of multiple groups with different terms and conditions. The default is **Off**.

## Tunnel device policy

October 13, 2021

Application tunnels (app tunnels) are designed to increase service continuity and data transfer reliability for your mobile apps. App tunnels define proxy parameters between the client component of any mobile device app and the app server component. You can configure the Tunnel policy for Android devices.

Any app traffic sent through a tunnel that you define in this policy goes through Endpoint Management before being redirected to the server running the app.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Android settings

### Tunnel Policy

This policy lets you configure an app tunnel. While doing so, you can choose if the tunnel will be used for the remote support app.

**Use this tunnel for remote support**  OFF

**Connection configuration**

**Connection initiated by**  ?

**Maximum connections per device \***  ?

**Define connection time out**  OFF ?

**Block cellular connections passing by this tunnel**  OFF ?

**App device parameters**

**Client port \***  ?

**App server parameters**

**IP address or server name \***

**Server port \***

- **Connection initiated by:** Click **Device** or **Server** to specify the source initiating the connection.
- **Maximum connections per device:** Type a number to specify how many concurrent TCP connections the app can establish. This field applies only to device-initiated connections.
- **Define connection time out:** Select whether to set a length of time an app can be idle before the tunnel is closed.
  - **Connection time out:** If you set **Define connection time out** to **On**, type the length of time in seconds that an app can be idle before the tunnel is closed.
- **Block cellular connections passing by this tunnel:** Select whether this tunnel is blocked while roaming. WiFi and USB connections aren't blocked.

- **Client port:** Type the client port number. In most cases, this value is the same as for the server port.
- **IP address or server name:** Type the IP address or name of the app server. This field applies only to device-initiated connections.
- **Server port:** Type the server port number.

## VPN device policy

October 6, 2021

The VPN device policy configures virtual private network (VPN) settings that enable user devices to connect securely to corporate resources. You can configure the VPN device policy for the following platforms. Each platform requires a different set of values, which are described in detail in this article.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Requirements for per-app VPNs

You configure the per-app VPN feature for the following platforms through VPN policies:

- iOS
- macOS
- Android (legacy DA)
- Samsung SAFE
- Samsung Knox

For Android Enterprise, use the [Managed configurations device policy](#) to configure VPN profiles.

Per-app VPN options are available for certain connection types. The following table indicates when per-app VPN options are available.

Platform	Connection type	Remark
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO, or Custom SSL.	

Platform	Connection type	Remark
macOS	Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, or Custom SSL.	
Android (legacy DA)	Citrix SSO	
Samsung SAFE	IPSEC, SSL	VPN type set to <b>Generic</b>
Samsung Knox	IPSEC, SSL	VPN type set to <b>Generic</b>

To create a per-app VPN for iOS and Android (legacy DA) devices using the Citrix SSO app, you need to perform extra steps, in addition to the VPN policy configuration. Also, you must verify that the following prerequisites are met:

- On-premises Citrix Gateway
- The following applications are installed on the device:
  - Citrix SSO
  - Citrix Secure Hub

A general workflow to configure a per-app VPN for iOS and Android devices using the Citrix SSO app is as follows:

1. Configure a VPN device policy as described in this article.
  - For iOS, see [Configure Citrix SSO protocol for iOS](#). After you configure the Citrix SSO protocol for iOS through a VPN device policy, you also need to create an App Attributes policy to associate an app to the per-app VPN policy. For more information, see [Configure a per-app VPN](#).
    - For the **Authentication type for the connection** field, if you select **Certificate**, you must first configure certificate-based authentication for Endpoint Management. See [Client certificate or certificate plus domain authentication](#).
  - For Android (legacy DA), see [Configure the Citrix SSO protocol for Android](#).
    - For the **Authentication type for the connection** field, if you select **Certificate** or **Password and Certificate**, you must first configure certificate-based authentication for Endpoint Management. See [Client certificate or certificate plus domain authentication](#).
2. Configure Citrix ADC to accept traffic from the per-app VPN. For details, see [Full VPN setup on Citrix Gateway](#).

## iOS settings

The Citrix VPN connection type in the VPN device policy for iOS doesn't support iOS 12. Perform these steps to delete your existing VPN device policy and create a VPN device policy with the Citrix SSO connection type:

1. Delete your VPN device policy for iOS.
2. Add a VPN device policy for iOS with the following settings:
  - **Connection type: Citrix SSO**
  - **Enable per-app VPN: On**
  - **Provider type: Packet tunnel**
3. Add an App Attributes device policy for iOS. For **Per-app VPN identifier**, choose **iOS\_VPN**.

The screenshot displays the 'VPN Policy' configuration page in the Citrix Endpoint Management console. The left-hand navigation pane shows 'VPN Policy' selected under 'Device Policies', with 'iOS' checked under 'Platforms'. The main configuration area is titled 'VPN Policy' and includes a descriptive note: 'This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.' The configuration fields are as follows:

- Connection name:** Text input field.
- Connection type:** Dropdown menu set to 'L2TP'.
- Server name or IP address:** Text input field with an asterisk.
- User account:** Text input field.
- Authentication:** Radio buttons for 'Password authentication' (selected) and 'RSA SecureID authentication'.
- Shared secret:** Text input field.
- Send all traffic:** Toggle switch set to 'OFF'.
- Proxy configuration:** Dropdown menu set to 'None'.

- **Connection name:** Type a name for the connection.
- **Connection type:** In the list, select the protocol to be used for this connection. The default is **L2TP**.
  - **L2TP:** Layer 2 Tunneling Protocol with pre-shared key authentication.
  - **PPTP:** Point-to-Point Tunneling.
  - **IPSec:** Your corporate VPN connection.
  - **Cisco Legacy AnyConnect:** This connection type requires that the Cisco Legacy AnyConnect VPN client is installed on the user device. Cisco is phasing out the Cisco Legacy AnyConnect client that was based on a now deprecated VPN framework. To use the current Cisco AnyConnect client, use a **Connection type** of **Custom SSL**. For required settings, see “Configure Custom SSL protocol” in this section.
  - **Juniper SSL:** Juniper Networks SSL VPN client.
  - **F5 SSL:** F5 Networks SSL VPN client.
  - **SonicWALL Mobile Connect:** Dell unified VPN client for iOS.

- **Ariba VIA:** Ariba Networks Virtual Internet Access client.
- **IKEv2 (iOS only):** Internet Key Exchange version 2 for iOS only.
- **AlwaysOn IKEv2:** Always-on access using IKEv2.
- **AlwaysOn IKEv2 Dual Configuration:** Always-on access using IKEv2 dual configuration.
- **Citrix SSO:** Citrix SSO client for iOS 12 and later.
- **Custom SSL:** Custom Secure Socket Layer. This connection type is required for the Cisco AnyConnect client that has a bundle ID of **com.cisco.anyconnect**. Specify a **Connection name** of **Cisco AnyConnect**. You can also deploy the VPN policy and enable a Network Access Control (NAC) filter for iOS devices. The filter blocks a VPN connection for devices that have non-compliant apps installed. The configuration requires specific settings for the iOS VPN policy as described in the following iOS section. For more information about other settings required to enable the NAC filter, see [Network Access Control](#).

The following sections list the configuration options for each of the preceding connection types.

### Configure L2TP Protocol for iOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- Select either **Password authentication** or **RSA SecurID authentication**.
- **Shared secret:** Type the IPsec shared secret key.
- **Send all traffic:** Select whether to send all traffic over the VPN. The default is **Off**.

### Configure PPTP Protocol for iOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- Select either **Password authentication** or **RSA SecurID authentication**.
- **Encryption level:** In the list, select an encryption level. The default is **None**.
  - **None:** Use no encryption.
  - **Automatic:** Use the strongest encryption level supported by the server.
  - **Maximum (128-bit):** Always use 128-bit encryption.
- **Send all traffic:** Select whether to send all traffic over the VPN. The default is **Off**.

### Configure IPsec Protocol for iOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Shared Secret** or **Certificate** for the type of authentication for this connection. The default is **Shared Secret**.
- If you enable **Shared Secret**, configure these settings:



- **Group name:** Type an optional group name.
- **Shared secret:** Type an optional shared secret key.
- **Use hybrid authentication:** Select whether to use hybrid authentication. With hybrid authentication, the server first authenticates itself to the client, and then the client authenticates itself to the server. The default is **Off**.
- **Prompt for password:** Select whether to prompt users for their passwords when they connect to the network. The default is **Off**.
- If you enable **Certificate**, configure these settings:
  - **Identity credential:** In the list, select the identity credential to use. The default is **None**.
  - **Prompt for PIN when connecting:** Select whether to require users to enter their PIN when connecting to the network. The default is **Off**.
  - **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see [Configure Enable VPN on demand settings for iOS](#).
- **Enable per-app VPN:** Select whether to enable per-app VPN. The default is **Off**.
- **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
- **Safari domains:** Click **Add** to add a Safari domain name.

### Configure Cisco legacy AnyConnect Protocol for iOS

To transition from the Cisco legacy AnyConnect client to the new Cisco AnyConnect client, use the Custom SSL protocol.

- **Provider bundle identifier:** For the Legacy AnyConnect client, the bundle ID is `com.cisco.anyconnect.gui`.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Group:** Type an optional group name.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when

users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.

- **Include All Networks:** Select whether to allow all networks to use this connection. The default is **Off**.
- **Exclude Local Networks:** Select whether to exclude local networks from using the connection or to allow the networks. The default is **Off**.
- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
  - **Provider type:** Select whether the per-app VPN is provided as an **App proxy** or as a **Packet tunnel**. Default is **App proxy**.
  - **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - \* **Domain:** Type the domain to be added.
    - \* Click **Save** to save the domain or click **Cancel** to not save the domain.

### Configure Juniper SSL Protocol for iOS

- **Provider bundle identifier:** If your per-app VPN profile contains the bundle identifier of an app with multiple VPN providers of the same type, specify the provider to use here.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Realm:** Type an optional realm name.
- **Role:** Type an optional role name.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.

- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
  - **Provider type:** Select whether the per-app VPN is provided as an **App proxy** or as a **Packet tunnel**. Default is **App proxy**.
  - **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - \* **Domain:** Type the domain to be added.
    - \* Click **Save** to save the domain or click **Cancel** to not save the domain.

### Configure F5 SSL Protocol for iOS

- **Provider bundle identifier:** If your per-app VPN profile contains the bundle identifier of an app with multiple VPN providers of the same type, specify the provider to use here.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.
- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.
  - **Provider type:** Select whether the per-app VPN is provided as an **App proxy** or as a **Packet tunnel**. Default is **App proxy**.
  - **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - \* **Domain:** Type the domain to be added.

- \* Click **Save** to save the domain or click **Cancel** to not save the domain.

### Configure SonicWALL Protocol for iOS

- **Provider bundle identifier:** If your per-app VPN profile contains the bundle identifier of an app with multiple VPN providers of the same type, specify the provider to use here.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Logon group or domain:** Type an optional logon group or domain.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.
- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you set this option to **On**, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.
  - **Provider type:** Select whether the per-app VPN is provided as an **App proxy** or as a **Packet tunnel**. Default is **App proxy**.
  - **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - \* **Domain:** Type the domain to be added.
    - \* Click **Save** to save the domain or click **Cancel** to not save the domain.

### Configure Ariba VIA protocol for iOS

- **Provider bundle identifier:** If your per-app VPN profile contains the bundle identifier of an app with multiple VPN providers of the same type, specify the provider to use here.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.

- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.
- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.
  - **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - \* **Domain:** Type the domain to be added.
    - \* Click **Save** to save the domain or click **Cancel** to not save the domain.

### Configure IKEv2 protocols for iOS

This section includes settings used for the IKEv2, Always On IKEv2, and Always On IKEv2 Dual Configuration protocols. For the Always On IKEv2 Dual Configuration protocol, configure all these settings for both Cellular and Wi-Fi networks.

- **Allow user to disable automatic connection:** For the Always On protocols. Select whether to allow users to disable automatic connection to the network on their devices. The default is **Off**.
- **Host name or IP address for server:** Type the server name or IP address for the VPN server.
- **Local Identifier:** The FQDN or IP address for the IKEv2 client. This field is required.
- **Remote Identifier:** The FQDN or IP address for the VPN server. This field is required.
- **Device Authentication:** Choose **Shared Secret**, **Certificate**, or **Device Certificate Based on Device Identifier** for the type of authentication for this connection. The default is **Shared Secret**.
  - If you choose **Shared Secret**, type an optional shared secret key.
  - If you choose **Certificate**, choose an **Identity credential** to use. The default is **None**.

- If you choose **Device Certificate Based on Device Identifier**, choose the **Device identity type** to use. The default is **IMEI**. To use this option, bulk import certificates using the REST API. See [Upload certificates in bulk using the REST API](#). Only available when you select **Always On IKEv2**.
- **Extended Authentication Enabled:** Select whether to enable Extended Authentication Protocol (EAP). If **On**, type the **User account** and **Authentication password**.
- **Dead Peer Detection Interval:** Choose how often a peer device is contacted to ensure that the peer device remains reachable. The default is **None**. Options are:
  - **None:** Disable dead peer detection.
  - **Low:** Contacts peer every 30 minutes.
  - **Medium:** Contacts peer every 10 minutes.
  - **High:** Contacts peer every 1 minute.
- **Disable Mobility and Multihoming:** Choose whether to disable this feature.
- **Use IPv4/IPv6 internal subnet attributes:** Choose whether to enable this feature.
- **Disable redirects:** Choose whether to disable redirects.
- **Enable Fallback:** If enabled, this setting allows a tunnel over cellular data to carry traffic that is eligible for Wi-Fi Assist and requires a VPN. Default is **Off**.
- **Enable NAT keepalive while the device is asleep:** For the Always On protocols. Keepalive packets maintain NAT mappings for IKEv2 connections. The chip sends these packets at regular intervals when the device is awake. If this setting is on, the chip sends keepalive packets even while the device is asleep. The default interval is 20 seconds over Wi-Fi and 110 seconds over cellular. You can change the interval by using the NAT keepalive interval parameter.
- **NAT keepalive Interval (seconds):** Defaults to 20 seconds.
- **Enable Perfect Forward Secrecy:** Choose whether to enable this feature.
- **DNS server IP addresses:** Optional. A list of DNS server IP address strings. These IP addresses can include a mixture of IPv4 and IPv6 addresses. Click **Add** to type an address.
- **Domain name:** Optional. The primary domain of the tunnel.
- **Search domains:** Optional. A list of domain strings used to qualify single-label host names fully.
- **Append supplemental match domains to resolver's list:** Optional. Determines whether to add the supplemental match domains list to the resolver's list of search domains. Default is **On**.
- **Supplemental match domains:** Optional. A list of domain strings used to determine which DNS queries are to use the DNS resolver settings contained in the DNS server addresses. This

key creates a split DNS configuration where only hosts in certain domains get resolved by using the DNS resolver of the tunnel. Hosts not in one of the domains in this list get resolved by using the default resolver of the system.

If this parameter contains an empty string, then that string is the default domain. As a result, a split tunnel configuration can direct all DNS queries to the VPN DNS servers before the primary DNS servers. If the VPN tunnel is the default route of the network, the listed DNS servers become the default resolver. In that case, the supplemental match domains list is ignored.

- **IKE SA Parameters** and **Child SA Parameters**: Configure these settings for each Security Association (SA) parameters option:
  - **Encryption Algorithm**: In the list, select the IKE encryption algorithm to use. The default is **3DES**.
  - **Integrity Algorithm**: In the list, select the integrity algorithm to use. The default is **SHA-256**.
  - **Diffie Hellman Group**: In the list, select the Diffie Hellman group number. The default is **2**.
  - **ike LifeTime in Minutes**: Type an integer between 10 and 1440 representing the SA lifetime (rekey interval). The default is **1440** minutes.
- **Service Exceptions**: For the Always On protocols. Service exceptions are system services that are exempt from Always On VPN. Configure these service exceptions settings:
  - **Voice Mail**: In the list, select how to handle the voice mail exception. The default is **Allow traffic via tunnel**.
  - **AirPrint**: In the list, select how to handle the AirPrint exception. The default is **Allow traffic via tunnel**.
  - **Allow traffic from captive web sheet outside the VPN tunnel**: Select whether to allow users to connect to public hotspots outside the VPN tunnel. The default is **Off**.
  - **Allow traffic from all captive networking apps outside the VPN tunnel**: Select whether to allow all hotspot networking apps outside the VPN tunnel. The default is **Off**.
  - **Captive networking app bundle identifiers**: For each hotspot networking app bundle identifier that users are allowed to access, click **Add** and type the hotspot networking app **Bundle Identifier**. Click **Save** to save the app bundle identifier.
- **Per-app VPN**: Configure these settings for IKEv2 connection types.
  - **Enable per-app VPN**: Select whether to enable per-app VPN. The default is **Off**.
  - **On-demand match app enabled**: Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.

- **Safari domains:** Click **Add** to add a Safari domain name.
- **Proxy configuration:** Choose how the VPN connection routes through a proxy server. Default is **None**.

### Configure Citrix SSO protocol for iOS

The Citrix SSO client is available in the Apple Store.

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.
- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you set this option to **On**, configure the following settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.
  - **Provider type:** Select whether the per-app VPN is provided as an **App proxy** or as a **Packet tunnel**. Default is **App proxy**.
  - **Provider type:** Set to **Packet tunnel**.
  - **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - \* **Domain:** Type the domain to be added.
    - \* Click **Save** to save the domain or click **Cancel** to not save the domain.
- **Custom XML:** For each custom XML parameter you want to add, click **Add** and specify the key/-value pairs. Available parameters are:
  - **disableL3:** Disables system level VPN. Allows only per app VPN. No **Value** is needed.
  - **user agent:** Associates with this device policy any Citrix Gateway policies that are targeted to VPN plug-in clients. For requests initiated by the plug-in, the **Value** for this key is automatically added to the VPN plug-in.



## Configure Custom SSL protocol for iOS

To transition from the Cisco Legacy AnyConnect client to the Cisco AnyConnect client:

1. Configure the VPN device policy with the Custom SSL protocol. Deploy the policy to iOS devices.
2. Upload the Cisco AnyConnect client from <https://apps.apple.com/us/app/cisco-anyconnect/id1135064690>, add the app to Endpoint Management, and then deploy the app to iOS devices.
3. Remove the old VPN device policy from iOS devices.

Settings:

- **Custom SSL identifier (reverse DNS format):** Set to the bundle identifier. For the Cisco AnyConnect client, use **com.cisco.anyconnect**.
- **Provider Bundle Identifier:** If the app specified in **Custom SSL identifier** has multiple VPN providers of the same type (App proxy or Packet tunnel), then specify this bundle identifier. For the Cisco AnyConnect client, use **com.cisco.anyconnect**.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.
- **Include All Networks:** Select whether to allow all networks to use this connection. The default is **Off**.
- **Exclude Local Networks:** Select whether to exclude local networks from using the connection or to allow the networks. The default is **Off**.
- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you set this option to **On**, configure the following settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.
  - **Provider Type:** A provider type indicates whether the provider is a VPN service or proxy service. For VPN service, choose **Packet tunnel**. For proxy service, choose **App proxy**. For the Cisco AnyConnect client, choose **Packet tunnel**.

- **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
  - \* **Domain:** Type the domain to be added.
  - \* Click **Save** to save the domain or click **Cancel** to not save the domain.
- **Custom XML:** For each custom XML parameter you want to add, click **Add** and do the following:
  - **Parameter name:** Type the name of the parameter to be added.
  - **Value:** Type the value associated with the **Parameter name**.
  - Click **Save** to save the parameter or click **Cancel** to not save the parameter.

### Configure the VPN device policy to support NAC

1. The **Connection type** of **Custom SSL** is required for configuring the NAC filter.
2. Specify a **Connection name** of **VPN**.
3. For **Custom SSL identifier**, type **com.citrix.NetScalerGateway.ios.app**
4. For **Provider bundle identifier**, type **com.citrix.NetScalerGateway.ios.app.vpnplugin**

The values in step 3 and 4 come from the required Citrix SSO installation for NAC filtering. You do not configure an authentication password. For more information on using the NAC function, see [Network Access Control](#).

### Configure enable VPN on demand options for iOS

- **On Demand Domain:** For each domain and associated action to take when users connect, click **Add** and do the following:
  - **Domain:** Type the domain to be added.
  - **Action:** In the list select one of the possible actions:
    - **Always establish:** The domain always triggers a VPN connection.
    - **Never establish:** The domain never triggers a VPN connection.
    - **Establish if necessary:** The domain triggers a VPN connection attempt if domain name resolution fails. Failure happens when the DNS server cannot resolve the domain, redirects to a different server, or times out.
    - Click **Save** to save the domain or click **Cancel** to not save the domain.
- **On demand rules**
  - **Action:** In the list, select the action to be taken. The default is **EvaluateConnection**. Possible actions are:
    - \* **Allow:** Allow VPN on demand to connect when triggered.
    - \* **Connect:** Unconditionally initiate a VPN connection.
    - \* **Disconnect:** Remove the VPN connection and do not reconnect on demand as long as the rule matches.
    - \* **EvaluateConnection:** Evaluate the ActionParameters array for each connection.

- \* **Ignore:** Leave any existing VPN connection up, but do not reconnect on demand as long as the rule matches.
- **DNSDomainMatch:** For each domain against which a device's search domain list can match that you want to add, click **Add** and do the following:
  - \* **DNS Domain:** Type the domain name. You can use the wildcard "\*" prefix for matching multiple domains. For example, \*.example.com matches mydomain.example.com, yourdomain.example.com, and herdomain.example.com.
  - \* Click **Save** to save the domain or click **Cancel** to not save the domain.
- **DNSServerAddressMatch:** For each IP address to which any of the network's specified DNS servers can match that you want to add, click **Add** and do the following:
  - \* **DNS Server Address:** Type the DNS server address you want to add. You can use the wildcard "\*" suffix for matching DNS servers. For example, 17.\* matches any DNS server in the class A subnet.
  - \* Click **Save** to save the DNS server address or click **Cancel** to not save the DNS server address.
- **InterfaceTypeMatch:** In the list, select the type of primary network interface hardware in use. The default is **Unspecified**. Possible values are:
  - \* **Unspecified:** Matches any network interface hardware. This option is the default.
  - \* **Ethernet:** Matches only Ethernet network interface hardware.
  - \* **WiFi:** Matches only Wi-Fi network interface hardware.
  - \* **Cellular:** Matches only Cellular network interface hardware.
- **SSIDMatch:** For each SSID to match against the current network that you want to add, click **Add** and do the following:
  - \* **SSID:** Type the SSID to add. If the network is not a Wi-Fi network, or if the SSID does not appear, the match fails. Leave this list empty to match any SSID.
  - \* Click **Save** to save the SSID or click **Cancel** to not save the SSID.
- **URLStringProbe:** Type a URL to fetch. If this URL is successfully fetched without redirection, this rule matches.
- **ActionParameters : Domains:** For each domain that EvaluateConnection checks that you want to add, click **Add** and do the following:
  - \* **Domain:** Type the domain to be added.
  - \* Click **Save** to save the domain or click **Cancel** to not save the domain.
- **ActionParameters : DomainAction:** In the list, select the **VPN behavior** for the specified **ActionParameters : Domains** domains. The default is **ConnectIfNeeded**. Possible actions are:
  - \* **ConnectIfNeeded:** The domain triggers a VPN connection attempt if domain name resolution fails. Failure happens when the DNS server cannot resolve the domain, redirects to a different server, or times out.
  - \* **NeverConnect:** The domain never triggers a VPN connection.

- **Action Parameters: RequiredDNSServers:** For each DNS server to use for resolving the specified domains, click **Add** and do the following:
  - \* **DNS Server:** Valid only when **ActionParameters : DomainAction = ConnectIfNeeded**. Type the DNS server IP address. This server can reside outside of the device's current network configuration. If the DNS server is not reachable, a VPN connection is established in response. Ensure that the DNS server is either an internal DNS server or a trusted external DNS server.
  - \* Click **Save** to save the DNS server or click **Cancel** to not save the DNS server.
- **ActionParameters: RequiredURLStringProbe:** Optionally, type an HTTP or HTTPS (preferred) URL to probe, using a GET request. If the URL's host name can't be resolved, the server is unreachable, or the server doesn't respond, a VPN connection is established. Valid only when **ActionParameters: DomainAction = ConnectIfNeeded**.
- **OnDemandRules: XML content:** Type, or copy and paste, XML configuration-on-demand rules.
  - \* Click **Check Dictionary** to validate the XML code. **Valid XML** appears below the **XML content** text box if the XML is valid. If it isn't valid, an error message describes the error.
- **Proxy**
  - **Proxy configuration:** In the list, select how the VPN connection routes through a proxy server. The default is **None**.
    - \* If you enable **Manual**, configure these settings:
      - **Host name or IP address for the proxy server:** Type the host name or IP address for the proxy server. This field is required.
      - **Port for the proxy server:** Type the proxy server port number. This field is required.
      - **User name:** Type an optional proxy server user name.
      - **Password:** Type an optional proxy server password.
    - \* If you configure **Automatic**, configure this setting:
      - **Proxy server URL:** Type the URL for the proxy server. This field is required.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

### Configure a per-app VPN

Per-app VPN options for iOS are available for these connection types: Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, Citrix SSO, and Custom SSL.

To configure a per-app VPN:

1. In **Configure > Device Policies**, create a VPN policy. For example:

**VPN Policy**

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

1 Policy Info

2 Platforms

- iOS
- macOS
- Android
- Samsung SAFE
- Samsung KNOX
- Windows Phone
- Windows Desktop/Tablet
- Amazon

3 Assignment

Connection name: XenMobile

Connection type: Custom SSL

Custom SSL identifier (reverse DNS format): com.example.custom.identifier

Provider bundle identifier: com.example.bundle.identifier

Server name or IP address: app-domain.example.com

User account: administrator

Authentication type for the connection: Password

Auth Password: .....

Per-app VPN

Enable per-app VPN:  ON  IOS 7.0+

On-demand match app enabled:  ON  ⓘ

Provider type: App proxy

Safari domains ⓘ

Back Next >

**VPN Policy**

Enable per-app VPN:  ON  IOS 7.0+

On-demand match app enabled:  ON  ⓘ

Provider type: App proxy

Safari domains ⓘ

Domain: Add

Custom XML

Custom parameters ⓘ

Parameter name: Value Add

Proxy

Proxy configuration: None

Policy Settings

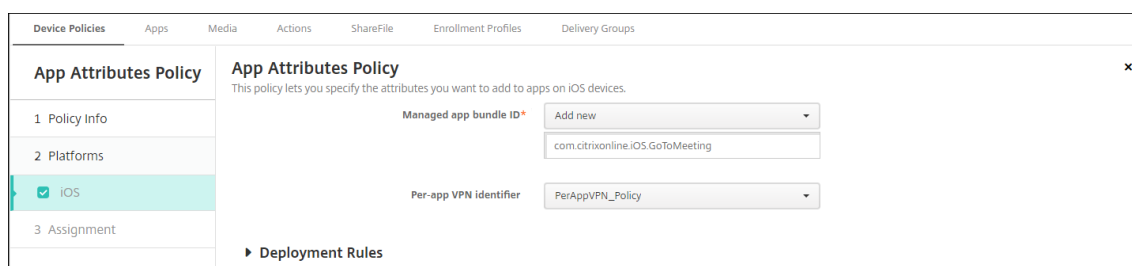
Remove policy:  Select date  Duration until removal (in hours)

Allow user to remove policy: Always

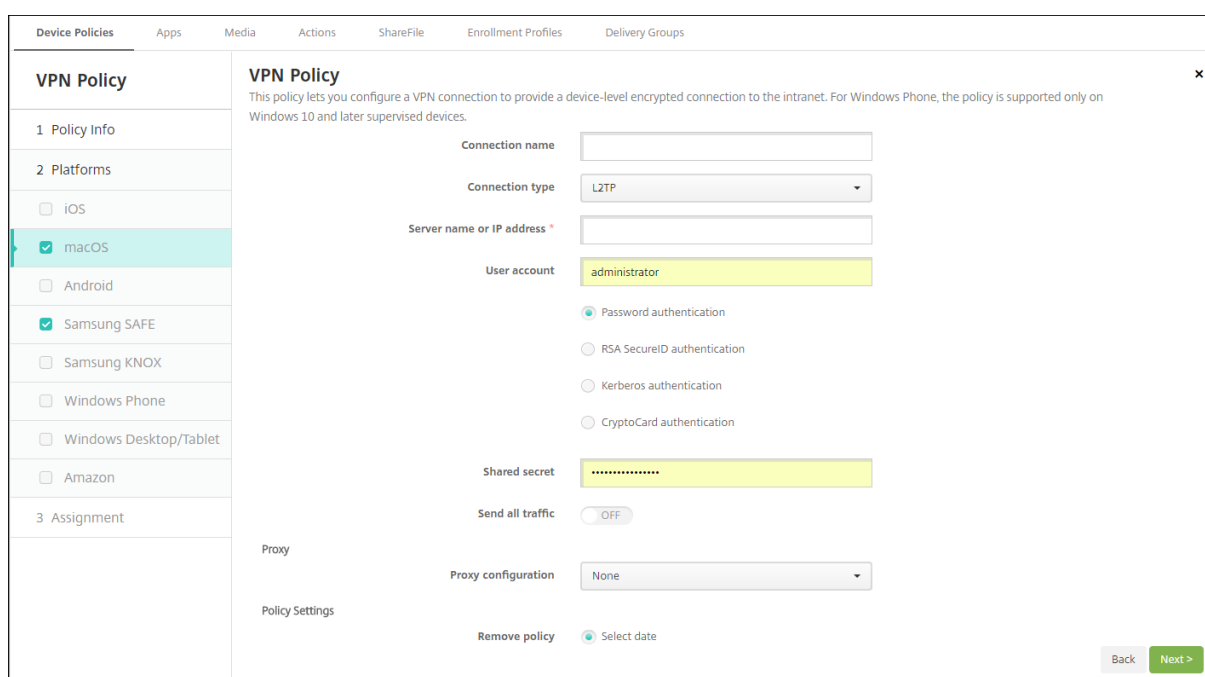
Deployment Rules

Back Next >

2. In **Configure > Device Policies**, create an App Attributes policy to associate an app to the per-app VPN policy. For **Per-app VPN identifier**, choose the name of the VPN policy created in Step 1. For **Managed app bundle ID**, choose from the app list or type the app bundle ID. (If you deploy an iOS App Inventory policy, the app list contains apps.)



## macOS settings



- **Connection name:** Type a name for the connection.
- **Connection type:** In the list, select the protocol to be used for this connection. The default is L2TP.
  - **L2TP:** Layer 2 Tunneling Protocol with pre-shared key authentication.
  - **PPTP:** Point-to-Point Tunneling.
  - **IPSec:** Your corporate VPN connection.
  - **Cisco AnyConnect:** Cisco AnyConnect VPN client.
  - **Juniper SSL:** Juniper Networks SSL VPN client.
  - **F5 SSL:** F5 Networks SSL VPN client.
  - **SonicWALL Mobile Connect:** Dell unified VPN client for iOS.
  - **Ariba VIA:** Ariba Networks Virtual Internet Access client.
  - **Citrix VPN:** Citrix VPN client.
  - **Custom SSL:** Custom Secure Socket Layer.

The following sections list the configuration options for each of the preceding connection types.

### Configure L2TP Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- Select **Password authentication, RSA SecurID authentication, Kerberos authentication, or CryptoCard authentication.** The default is **Password authentication.**
- **Shared secret:** Type the IPsec shared secret key.
- **Send all traffic:** Select whether to send all traffic over the VPN. The default is **Off.**

### Configure PPTP Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- Select **Password authentication, RSA SecurID authentication, Kerberos authentication, or CryptoCard authentication.** The default is **Password authentication.**
- **Encryption level:** Select the desired encryption level. The default is **None.**
  - **None:** Use no encryption.
  - **Automatic:** Use the strongest encryption level supported by the server.
  - **Maximum (128-bit):** Always use 128-bit encryption.
- **Send all traffic:** Select whether to send all traffic over the VPN. The default is **Off.**

### Configure IPsec Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Shared Secret** or **Certificate** for the type of authentication for this connection. The default is **Shared Secret.**
  - If you enable **Shared Secret** authentication, configure these settings:
    - \* **Group name:** Type an optional group name.
    - \* **Shared secret:** Type an optional shared secret key.
    - \* **Use hybrid authentication:** Select whether to use hybrid authentication. With hybrid authentication, the server first authenticates itself to the client, and then the client authenticates itself to the server. The default is **Off.**
    - \* **Prompt for password:** Select whether to prompt users for their passwords when they connect to the network. The default is **Off.**
  - If you enable **Certificate** authentication, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None.**
    - \* **Prompt for PIN when connecting:** Select whether to require users to enter their PIN when connecting to the network. The default is **Off.**

- \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand options.

### Configure Cisco AnyConnect Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Group:** Type an optional group name.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand options.
  - **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
    - \* **On-demand match app enabled:** Select whether a per-app VPN connection triggers automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
    - \* **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
      - **Domain:** Type the domain to be added.
      - Click **Save** to save the domain or click **Cancel** to not save the domain.

### Configure Juniper SSL Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Realm:** Type an optional realm name.
- **Role:** Type an optional role name.



- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings.
- **Enable per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure the following settings:
  - **On-demand match app enabled:** Select whether a per-app VPN connection triggers automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
  - **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - \* **Domain:** Type the domain to be added.
    - \* Click **Save** to save the domain or click **Cancel** to not save the domain.

### Configure F5 SSL Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings.

- **Enable per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connection triggers automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
  - **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - \* **Domain:** Type the domain to be added.
    - \* Click **Save** to save the domain or click **Cancel** to not save the domain.

### Configure SonicWALL Mobile Connect Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Logon group or domain:** Type an optional logon group or domain.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings.
- **Enable per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connection triggers automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
  - **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - \* **Domain:** Type the domain to be added.
    - \* Click **Save** to save the domain or click **Cancel** to not save the domain.

**Configure Ariba VIA protocol for macOS**

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings.
- **Enable per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connection triggers automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
  - **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - \* **Domain:** Type the domain to be added.
    - \* Click **Save** to save the domain or click **Cancel** to not save the domain.

**Configure Custom SSL protocol for macOS**

- **Custom SSL identifier (reverse DNS format):** Type the SSL identifier in reverse DNS format. This field is required.
- **Server name or IP address:** Type the server name or IP address for the VPN server. This field is required.
- **User account:** Type an optional user account.
  - **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - \* **Identity credential:** In the list, select the identity credential to use. The default is

**None.**

- \* **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
- \* **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings.
- **Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - \* **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.
  - \* **Safari domains:** For each Safari domains that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - **Domain:** Type the domain to be added.
    - Click **Save** to save the domain or click **Cancel** to not save the domain.
- **Custom XML:** For each custom XML parameter you want to add, click **Add** and do the following:
  - **Parameter name:** Type the name of the parameter to be added.
  - **Value:** Type the value associated with **Parameter name**.
  - Click **Save** to save the domain or click **Cancel** to not save the domain.

**Configure enable VPN on demand options**

- **On Demand Domain:** For each domain and associated action to be taken when users connect to them that you want to add, click **Add** to and do the following:
  - **Domain:** Type the domain to be added.
  - **Action:** In the list select one of the possible actions:
    - \* **Always establish:** The domain always triggers a VPN connection.
    - \* **Never establish:** The domain never triggers a VPN connection.
    - \* **Establish if necessary:** The domain triggers a VPN connection attempt if domain name resolution fails. Failure happens when the DNS server cannot resolve the domain, redirects to a different server, or times out.
  - Click **Save** to save the domain or click **Cancel** to not save the domain.
- **On demand rules**
  - **Action:** In the list, select the action to be taken. The default is **EvaluateConnection**. Possible actions are:
    - \* **Allow:** Allow VPN on demand to connect when triggered.
    - \* **Connect:** Unconditionally initiate a VPN connection.
    - \* **Disconnect:** Remove the VPN connection and do not reconnect on demand as long as the rule matches.

- \* **EvaluateConnection:** Evaluate the **ActionParameters** array for each connection.
- \* **Ignore:** Leave any existing VPN connection up, but do not reconnect on demand as long as the rule matches.
- **DNSDomainMatch:** For the domains against which a device's search domain list can match, click **Add** to and do the following:
  - \* **DNS Domain:** Type the domain name. You can use the wildcard "\*" prefix for matching multiple domains. For example, \*.example.com matches mydomain.example.com, yourdomain.example.com, and herdomain.example.com.
  - \* Click **Save** to save the domain or click **Cancel** to not save the domain.
- **DNSServerAddressMatch:** For each IP address to which any of the network's specified DNS servers can match that you want to add, click **Add** and do the following:
  - \* **DNS Server Address:** Type the DNS server address you want to add. You can use the wildcard "\*" suffix for matching DNS servers. For example, 17.\* matches any DNS server in the class A subnet.
  - \* Click **Save** to save the DNS server address or click **Cancel** to not save the DNS server address.
- **InterfaceTypeMatch:** In the list, click the type of primary network interface hardware in use. The default is **Unspecified**. Possible values are:
  - \* **Unspecified:** Matches any network interface hardware. This option is the default.
  - \* **Ethernet:** Matches only Ethernet network interface hardware.
  - \* **WiFi:** Matches only Wi-Fi network interface hardware.
  - \* **Cellular:** Matches only Cellular network interface hardware.
- **SSIDMatch:** For each SSID to match against the current network that you want to add, click **Add** and so the following.
  - \* **SSID:** Type the SSID to add. If the network is not a Wi-Fi network, or if the SSID does not appear, the match fails. Leave this list empty to match any SSID.
  - \* Click **Save** to save the SSID or click **Cancel** to not save the SSID.
- **URLStringProbe:** Type a URL to fetch. If this URL is successfully fetched without redirection, this rule matches.
- **ActionParameters : Domains:** For each domain that EvaluateConnection checks that you want to add, click **Add** and do the following:
  - \* **Domain:** Type the domain to be added.
  - \* Click **Save** to save the domain or click **Cancel** to not save the domain.
- **ActionParameters : DomainAction:** In the list, select the **VPN behavior** for the specified **ActionParameters : Domains** domains. The default is **ConnectIfNeeded**. Possible actions are:
  - \* **ConnectIfNeeded:** The domain triggers a VPN connection attempt if domain name resolution fails. Failure happens when the DNS server cannot resolve the domain, redirects to a different server, or times out.

- \* **NeverConnect:** The domain never triggers a VPN connection.
- **Action Parameters: RequiredDNSServers:** For each DNS server to use for resolving the specified domains, click **Add** and do the following:
  - \* **DNS Server:** Valid only when **ActionParameters : DomainAction = ConnectIfNeeded**. Type the DNS server IP address to add. This server can reside outside of the device's current network configuration. If the DNS server is not reachable, a VPN connection is established in response. This DNS server must be either an internal DNS server or a trusted external DNS server.
  - \* Click **Save** to save the DNS server or click **Cancel** to not save the DNS server.
- **ActionParameters: RequiredURLStringProbe:** Optionally, type an HTTP or HTTPS (preferred) URL to probe, using a GET request. If the URL's host name cannot be resolved, the server is unreachable, or the server does not respond, a VPN connection is established. Valid only when **ActionParameters: DomainAction = ConnectIfNeeded**.
- **OnDemandRules: XML content:** Type, or copy and paste, XML configure-on-demand rules.
  - \* Click **Check Dictionary** to validate the XML code. **Valid XML** appears below the **XML content** text box if the XML is valid. If it isn't valid, an error message describes the error.
- **Proxy**
  - **Proxy configuration:** In the list, select how the VPN connection routes through a proxy server. The default is **None**.
    - \* If you enable **Manual**, configure these settings:
      - **Host name or IP address for the proxy server:** Type the host name or IP address for the proxy server. This field is required.
      - **Port for the proxy server:** Type the proxy server port number. This field is required.
      - **User name:** Type an optional proxy server user name.
      - **Password:** Type an optional proxy server password.
    - \* If you configure **Automatic**, configure this setting:
      - **Proxy server URL:** Type the URL for the proxy server. This field is required.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.

- **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

## Android (legacy DA) settings

The screenshot displays the 'VPN Policy' configuration window in the Citrix Endpoint Management console. The left sidebar shows the navigation menu with 'Android' selected under the 'Platforms' section. The main content area is titled 'VPN Policy' and includes a description: 'This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.' The configuration fields are as follows:

- Connection name \***: Text input field.
- Server name or IP address \***: Text input field.
- Connection type**: Dropdown menu set to 'Cisco AnyConnect'.
- Identity credential**: Dropdown menu set to 'None'.
- Backup VPN server**: Text input field.
- User group**: Text input field.
- Automatic VPN policy**: Toggle switch set to 'OFF'.

Below these fields, there is a section for 'Trusted Networks' and a 'Deployment Rules' section.

### Configure Cisco AnyConnect VPN protocol for Android

- **Connection name:** Type a name for the Cisco AnyConnect VPN connection. This field is required.
- **Server name or IP address:** Type the name or IP address of the VPN server. This field is required.
- **Identity credential:** In the list, select an identity credential.
- **Backup VPN server:** Type the backup VPN server information.
- **User group:** Type the user group information.
- **Trusted Networks**
  - **Automatic VPN policy:** Enable or disable this option to set how the VPN reacts to trusted and untrusted networks. If enabled, configure these settings:
    - \* **Trusted network policy:** In the list, select the desired policy. The default is **Disconnect**. Possible options are:
      - **Disconnect:** The client terminates the VPN connection in the trusted network. This setting is the default.
      - **Connect:** The client initiates a VPN connection in the trusted network.
      - **Do Nothing:** The client takes no action.
      - **Pause:** When a user establishes a VPN session outside the trusted network then enters a network configured as trusted, the VPN session gets suspended. When the user leaves the trusted network again, the session resumes. This setting eliminates the need to establish a new VPN session after leaving a trusted network.

- \* **Untrusted network policy:** In the list, select the desired policy. The default is **Connect**. Possible options are:
  - **Connect:** The client initiates a VPN connection in the untrusted network.
  - **Do Nothing:** The client starts a VPN connection in the untrusted network. This option disables always-on VPN.
- **Trusted domains:** For each domain suffix that the network interface has when the client is in the trusted network, click **Add** to do the following:
  - \* **Domain:** Type the domain to be added.
  - \* Click **Save** to save the domain or click **Cancel** to not save the domain.
- **Trusted servers:** For each server address that a network interface has when the client is in the trusted network, click **Add** and do the following:
  - \* **Servers:** Type the server to be added.
  - \* Click **Save** to save the server or click **Cancel** to not save the server.

### Configure the Citrix SSO protocol for Android

- **Connection name:** Type a name for the VPN connection. This field is required.
- **Server name or IP address:** Type the FQDN or IP address of the Citrix Gateway.
- **Authentication type for the connection:** Choose an authentication type and complete any of these fields that appear for the type:
  - **User name and Password:** Type your VPN credentials for the **Authentication types** of **Password** or **Password and Certificate**. Optional. If you don't provide the VPN credentials, the Citrix VPN app prompts for a user name and password.
  - **Identity credential:** Appears for the **Authentication types** of **Certificate** or **Password and Certificate**. In the list, select an identity credential.
- **Enable per-app VPN:** Select whether to enable per-app VPN. If you don't enable per-app VPN, all traffic goes through the Citrix VPN tunnel. If you enable per-app VPN, specify the following settings. The default is **Off**.
  - **Allow list or Block list:** If **Allow list**, all apps in the allow list tunnel through this VPN. If **Block list**, all apps except those apps on the block list tunnel through this VPN.
  - **Application List:** The apps on an allow list or block list. Click **Add** and then type a comma-separated list of app package names.
- **Custom XML:** Click **Add** and then type custom parameters. Endpoint Management supports these parameters for Citrix VPN:
  - **DisableUserProfiles:** Optional. To enable this parameter, type **Yes** for the **Value**. If enabled, Endpoint Management doesn't display user-added VPN connections and the user cannot add a connection. This setting is a global restriction and applies to all VPN profiles.



- **userAgent:** A string value. You can specify a custom User Agent string to send in each HTTP request. The specified user agent string gets appended to the existing Citrix VPN user agent.

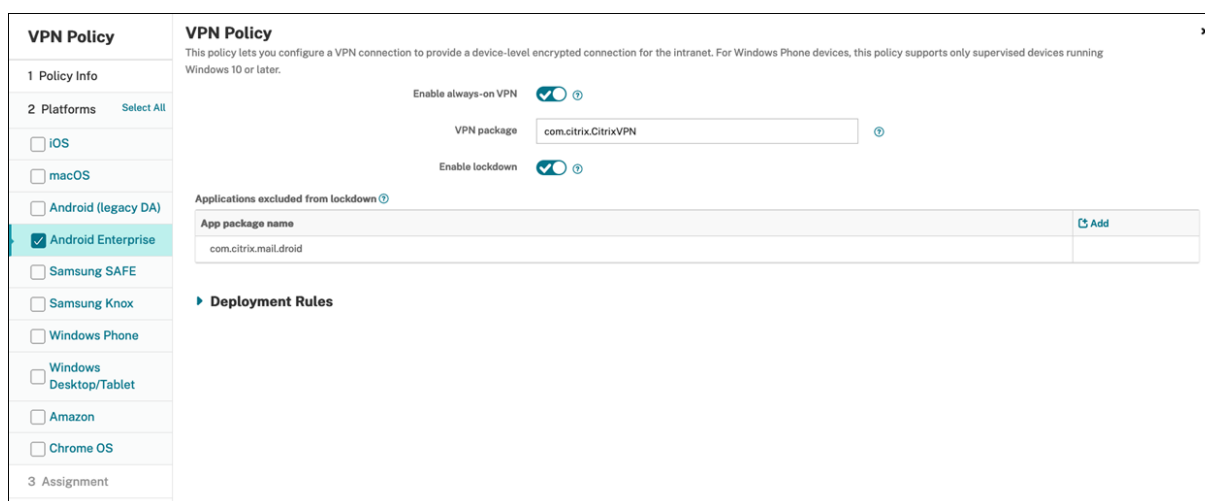
### Configure VPNs to support NAC

1. Use the **Connection type** of **Custom SSL** to configure the NAC filter.
2. Specify a **Connection name** of **VPN**.
3. For **Custom XML**, click **Add** and do the following:
  - **Parameter name:** Type **XenMobileDeviceId**. This field is the device ID to use for the NAC check based on device enrollment in Endpoint Management. If Endpoint Management enrolls and manages the device, the VPN connection is allowed. Otherwise, authentication is denied at the time of VPN establishment.
  - **Value:** Type **DeviceID\_\${device.id}**, which is the value for the parameter **XenMobileDeviceId**.
  - Click **Save** to save the parameter.

### Configure VPNs for Android Enterprise

To configure VPNs for Android Enterprise devices, create an Android Enterprise managed configuration device policy for the Citrix SSO app. See [Configure VPN profiles for Android Enterprise](#).

### Android Enterprise settings



- **Enable always-on VPN:** Select whether the VPN is always on. The default is **Off**. When enabled, the VPN connection remains on until the user manually disconnects.
- **VPN package** Type the package name for the VPN app devices use.

- **Enable lockdown:** If disabled, no app can access the network if a VPN connection doesn't exist. If enabled, the apps you configure in the following setting can access the network, even if a VPN connection doesn't exist. Available for Android 10 and later devices.
- **Applications excluded from lockdown:** Click **Add** to type the package names of apps you want to bypass the lockdown setting.

## Samsung SAFE settings

The screenshot displays the 'VPN Policy' configuration interface. On the left, a sidebar lists various device policies, with 'VPN Policy' selected. The main content area shows the configuration for a PPTP connection. The fields are as follows:

- Connection name:** K--PPTP
- Vpn Type:** PPTP
- Host name:** [Redacted]
- User name:** testuser
- Password:** [Redacted]
- Enable encryption:** OFF

Below the configuration fields, there is a section for 'Deployment Rules'.

- **Connection name:** Type a name for the connection.
- **VPN type:** In the list, select the protocol to be used for this connection. The default is **L2TP with pre-shared key**. Possible options are:
  - **L2TP with pre-shared key:** Layer 2 Tunneling Protocol with pre-shared key authentication. This setting is the default.
  - **L2TP with certificate:** Layer 2 Tunneling Protocol with certificate.
  - **PPTP:** Point-to-Point Tunneling.
  - **Enterprise:** Your corporate VPN connection. Applicable to SAFE versions earlier than 2.0.
  - **Generic:** A generic VPN connection. Applicable to SAFE versions 2.0 or higher.

### Configure L2TP with pre-shared key protocol for Samsung SAFE

- **Host name:** Type the name of the VPN host. This option is required.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **Pre-shared key:** Type the pre-shared key. This option is required.

### Configure L2TP with certificate protocol for Samsung SAFE

- **Host name:** Type the name of the VPN host. This option is required.

- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **Identity credential:** In the list, select the identity credential to be used. The default is **None**.

#### Configure PPTP protocol for Samsung SAFE

- **Host name:** Type the name of the VPN host. This option is required.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **Enable encryption:** Select whether to enable encryption on the VPN connection.

#### Configure Enterprise protocol for Samsung SAFE

- **Host name:** Type the name of the VPN host. This option is required.
- **Enable backup server:** If you enable a backup VPN server, type the FQDN or IP address of the backup VPN server.
- **Enable user authentication:** Select whether to require user authentication. If enabled, configure the following settings:
  - **User name:** Type a user name.
  - **Password:** Type the user password.
- **Group name:** Type an optional group name.
- **Authentication method:** In the list, select the authentication method to be used. Possible options are:
  - **Certificate:** Use certificate authentication. This setting is the default. If selected, in the **Identity credential** list, select the credential to use. The default is **None**.
  - **Pre-shared key:** Use a pre-shared key. If selected, in the **Pre-shared key** field, type the shared secret key.
  - **Hybrid RSA:** Use hybrid authentication using RSA certificates.
  - **EAP MD5:** Authenticate the EAP peer to the EAP server, but does no mutual authentication.
  - **EAP MSCHAPv2:** Use the Microsoft Challenge-Handshake Authentication Protocol for mutual authentication.
- **CA certificate:** In the list, select the certificate to be used. The default is **None**.
- **Enable default route:** Select whether to enable a default route to the VPN server. The default is **Off**.
- **Enable smartcard authentication:** Select whether to allow users to authenticate by using smart cards. The default is **Off**.
- **Enable mobile option:** The default is **Off**.
- **Diffie-Hellman group value (key strength):** In the list, select the key strength to be used. The default is 0.

- **Split tunnel type:** In the list, select the type of split tunnel to use. The default is **Auto**. Possible options are:
  - **Auto:** Split tunneling is used automatically.
  - **Manual:** Split tunneling is used over the IP address and port specified on the VPN server.
  - **Disabled:** Split tunneling is not used.
- **SuiteB type:** In the list, select the level of NSA Suite B encryption to use. The default is **GCM-128**. Possible options are:
  - **GCM-128:** Use 128-bit AES-GCM encryption.
  - **GCM-256:** Use 256-bit AES-GCM encryption.
  - **GMAC-128:** Use 128-bit AES-GMAC encryption.
  - **GMAC-256:** Use 256-bit AES-GMAC encryption.
  - **None:** Use no encryption.
- **Forward routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.

### Configure generic protocol for Samsung SAFE

- **Host name:** Type the name of the VPN host. This option is required.
- **Enable user authentication:** Select whether to require user authentication. If enabled, in **Password**, type the user password.
- **User name:** Type a user name.
- **Package Name Agent VPN:** The package name, or ID, of the VPN installed on the device; for example, Mocana or Pulse Secure.
- **VPN Connection type:** In the list, select either **IPSEC** or **SSL** for the connection type to be used. The default is **IPSEC**. The following sections describe the configuration settings for each connection type.

### Configure IPSEC connection type settings for Samsung SAFE

- **Identity:** Type an optional identifier for this configuration.
- **IPsec group ID type:** In the list, select the IPsec group ID type to use. The default is **Default**. Possible options are:
  - **Default**
  - **IPv4 address**
  - **Fully qualified domain name (FQDN)**
  - **User FQDN**
  - **IKE key ID**
- **IKE version:** In the list, select the Internet Key Exchange version to use. The default is **IKEv1**.

- **Authentication method:** In the list, select the authentication method to be used. The default is **Certificate**. Possible options are:
  - **Certificate:** Use certificate authentication. If selected, in the **Identity credential** list, select the credential to use. The default is **None**.
  - **Pre-shared key:** Use a pre-shared key. If selected, in the **Pre-shared key** field, type the shared secret key.
  - **Hybrid RSA:** Use hybrid authentication using RSA certificates.
  - **EAP MD5:** Authenticate the EAP peer to the EAP server, but does no mutual authentication.
  - **EAP MSCHAPv2:** Use the Microsoft Challenge-Handshake Authentication Protocol for mutual authentication.
  - **CAC based Authentication:** Use a Common Access Card (CAC) for authentication.
- **Identity credential:** In the list select the identity credential to use. The default is **None**.
- **CA certificate:** In the list, select the certificate to be used.
- **Enable dead peer detection:** Select whether to contact a peer to ensure that it remains alive. The default is **Off**.
- **Enable default route:** Select whether to enable a default route to the VPN server.
- **Enable mobile option:** The default is **Off**.
- **ike LifeTime in Minutes:** Type the number of minutes before the VPN connection must be reestablished. The default is 1440 minutes (24 hours).
- **ipsec LifeTime in Minutes:** Type the number of minutes before the VPN connection must be reestablished. The default is 1440 minutes (24 hours).
- **Diffie-Hellman group value (key strength):** In the list, select the key strength to be used. The default is **0**.
- **IKE Phase 1 key exchange mode:** Select either **Main** or **Aggressive** for the IKE Phase 1 negotiation mode. The default is **Main**.
  - **Main:** No information is exposed to potential attackers during negotiation, but is slower than **Aggressive** mode.
  - **Aggressive:** Some information (for example, the identity of the negotiating peers) is exposed to potential attackers during negotiation, but is faster than **Main** mode.
- **Perfect forward secrecy (PFS) value:** Select whether to use PFS to require a new key exchange renegotiating a connection.
- **Split tunnel type:** In the list, select the type of split tunnel to use. Possible options are:
  - **Auto:** Split tunneling is automatically used.
  - **Manual:** Split tunneling is used over the IP address and port specified on the VPN server.
  - **Disabled:** Split tunneling is not used.
- **IPSEC Encryption algorithm:** A VPN configuration that the IPsec protocol uses.
- **IKE Encryption Algorithm:** A VPN configuration that the IPsec protocol uses.
- **IKE Integrity Algorithm:** A VPN configuration that the IPsec protocol uses.
- **Vendor:** A personal profile for generic agents that communicate with the Knox API.

- **Forward routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.
- **Per App VPN:** For each per-app VPN you want to add, click **Add** and do the following:
  - **Per App VPN:** The VPN configuration that the app uses to communicate.
  - Click **Save** to save the per-app VPN or click **Cancel** to not save the per-app VPN.

### Configure SSL connection type settings for Samsung SAFE

- **Authentication method:** In the list, select the authentication method to be used. The default is **Not Applicable**. Possible options are:
  - **Not Applicable**
  - **Certificate:** Use certificate authentication. If selected, in the **Identity credential** list, select the credential to use. The default is **None**.
  - **CAC based Authentication:** Use a Common Access Card (CAC) for authentication.
- **CA certificate:** In the list, select the certificate to be used.
- **Enable default route:** Select whether to enable a default route to the VPN server.
- **Enable mobile option:** The default is **Off**.
- **Split tunnel type:** In the list, select the type of split tunnel to use. Possible options are:
  - **Auto:** Split tunneling is automatically used.
  - **Manual:** Split tunneling is used over the IP address and port specified on the VPN server.
  - **Disabled:** Split tunneling is not used.
- **SSL Algorithm:** Type the SSL algorithm to use for client-server negotiation.
- **Vendor:** A personal profile for generic agents that communicate with the Knox API.
- **Forward routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.
- **Per App VPN:** For each per-app VPN you want to add, click **Add** and do the following:
  - **Per App VPN:** The VPN configuration that the app uses to communicate.
  - Click **Save** to save the per-app VPN or click **Cancel** to not save the per-app VPN.

## Samsung Knox settings

The screenshot displays the 'VPN Policy' configuration interface. The left-hand navigation pane is titled 'VPN Policy' and includes sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', the 'Samsung KNOX' option is selected. The main configuration area is titled 'VPN Policy' and contains a descriptive note: 'This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.' The configuration options include:

- Vpn Type:** Enterprise (selected)
- Connection name \***: [Text input field]
- Host name \***: [Text input field]
- Enable backup server:** OFF
- Enable user authentication:** OFF
- Group name:** [Text input field]
- Authentication method:** Certificate
- Identity credential:** None
- CA certificate:** Select certificate
- Enable default route:** OFF
- Enable smartcard authentication:** OFF
- Enable mobile option:** OFF

At the bottom right, there are 'Back' and 'Next >' buttons.

When you configure any policy for Samsung Knox, it applies only inside the Samsung Knox container.

- **VPN Type:** In the list, select the type of VPN connection to configure. The connection can be either **Enterprise** (applicable to Knox versions earlier than 2.0) or **Generic** (applicable to Knox versions 2.0 or higher). The default is **Enterprise**.

The following sections list the configuration options for each of the preceding connection types.

### Configure Enterprise protocol for Samsung Knox

- **Connection name:** Type a name for the connection. This field is required.
- **Host name:** Type the name of the VPN host. This option is required.
- **Enable backup server:** Select whether to enable a backup VPN server. If enabled, in **Backup VPN server**, type the FQDN or IP address of the backup VPN server.
- **Enable user authentication:** Select whether to require user authentication. If enabled, configure the following settings:
  - **User name:** Type a user name.
  - **Password:** Type the user password.
- **Group name:** Type an optional group name.
- **Authentication method:** In the list, select the authentication method to be used. Possible options are:
  - **Certificate:** Use certificate authentication. For certificate authentication, also select the credential to use from the **Identity credential** list.

- **Pre-shared key:** Use a pre-shared key. If selected, in the **Pre-shared key** field, type the shared secret key.
- **Hybrid RSA:** Use hybrid authentication using RSA certificates.
- **EAP MD5:** Authenticate the EAP peer to the EAP server, but does no mutual authentication.
- **EAP MSCHAPv2:** Use the Microsoft Challenge-Handshake Authentication Protocol for mutual authentication.
- **CA certificate:** In the list, select the certificate to be used.
- **Enable default route:** Select whether to enable a default route to the VPN server.
- **Enable smartcard authentication:** Select whether to allow users to authenticate by using smart cards. The default is **Off**.
- **Enable mobile option:** The default is **Off**.
- **Diffie-Hellman group value (key strength):** In the list, select the key strength to be used. The default is **0**.
- **Split tunnel type:** In the list, select the type of split tunnel to use. Possible options are:
  - **Auto:** Split tunneling is automatically used.
  - **Manual:** Split tunneling is used over the IP address and port specified on the VPN server.
  - **Disabled:** No split tunneling is used.
- **SuiteB type:** In the list, select the level of NSA Suite B encryption to use. Possible options are:
  - **GCM-128:** Use 128-bit AES-GCM encryption: This setting is the default.
  - **GCM-256:** Use 256-bit AES-GCM encryption.
  - **GMAC-128:** Use 128-bit AES-GMAC encryption.
  - **GMAC-256:** Use 256-bit AES-GMAC encryption.
  - **None:** Use no encryption.
- **Forward routes:** Click **Add** to add any optional forwarding routes if your corporate VPN server supports multiple route tables.

### Configure generic protocol for Samsung Knox

- **Connection name:** Type a name for the connection. This field is required.
- **Package Name Agent VPN:** The package name, or ID, of the VPN installed on the device; for example, Mocana or Pulse Secure.
- **Host name:** Type the name of the VPN host. This option is required.
- **Enable user authentication:** Select whether to require user authentication. If enabled, configure the following settings:
  - **User name:** Type a user name.
  - **Password:** Type the user password.
- **Identity:** Type an optional identifier for this configuration. Only applies when **Vpn Connection type = IPSEC**.
- **VPN Connection type:** In the list, select either **IPSEC** or **SSL** for the connection type to be used. The default is **IPSEC**. The following sections describe the configuration settings for each connec-



tion type.

- **Configure IPSEC connection settings**

- **IPsec group ID type:** In the list, select the IPsec group ID type to use. The default is **Default**. Possible options are:
  - \* **Default**
  - \* **IPv4 address**
  - \* **Fully qualified domain name (FQDN)**
  - \* **User FQDN**
  - \* **IKE key ID**
- **IKE version:** In the list, select the Internet Key Exchange version to use. The default is **IKEv1**.
- **Authentication method:** In the list, select the authentication method to be used. The default is **Certificate**. Possible options are:
  - \* **Certificate:** Use certificate authentication. If selected, in the **Identity credential** list, select the credential to use. The default is **None**.
  - \* **Pre-shared key:** Use a pre-shared key. If selected, in the **Pre-shared key** field, type the shared secret key.
  - \* **Hybrid RSA:** Use hybrid authentication using RSA certificates.
  - \* **EAP MD5:** Authenticate the EAP peer to the EAP server, but does no mutual authentication.
  - \* **EAP MSCHAPv2:** Use the Microsoft Challenge-Handshake Authentication Protocol for mutual authentication.
  - \* **CAC based Authentication:** Use a Common Access Card (CAC) for authentication.
- **CA certificate:** In the list, select the certificate to be used.
- **Enable dead peer detection:** Select whether to contact a peer to ensure that it remains alive. The default is **Off**.
- **Enable default route:** Select whether to enable a default route to the VPN server.
- **Enable mobile option:** The default is **Off**.
- **ike LifeTime in Minutes:** Type the number of minutes before the VPN connection must be reestablished. The default is 1440 minutes (24 hours).
- **ipsec LifeTime in Minutes:** Type the number of minutes before the VPN connection must be reestablished. The default is 1440 minutes (24 hours).
- **Diffie-Hellman group value (key strength):** In the list, select the key strength to be used. The default is **0**.
- **IKE Phase 1 key exchange mode:** Select either **Main** or **Aggressive** for the IKE Phase 1 negotiation mode. The default is **Main**.
  - \* **Main:** No information is exposed to potential attackers during negotiation, but is slower than **Aggressive** mode.
  - \* **Aggressive:** Some information (for example, the identity of the negotiating peers) is

- exposed to potential attackers during negotiation, but is faster than **Main** mode.
- **Perfect forward secrecy (PFS) value:** Select whether to use PFS to require a new key exchange renegotiating a connection.
  - **Split tunnel type:** In the list, select the type of split tunnel to use. Possible options are:
    - \* **Auto:** Split tunneling is automatically used.
    - \* **Manual:** Split tunneling is used over the IP address and port specified on the VPN server.
    - \* **Disabled:** Split tunneling is not used.
  - **SuiteB Type:** In the list, select the level of NSA Suite B encryption to use. The default is **GCM-128**. Possible options are:
    - \* **GCM-128:** Use 128-bit AES-GCM encryption.
    - \* **GCM-256:** Use 256-bit AES-GCM encryption.
    - \* **GMAC-128:** Use 128-bit AES-GMAC encryption.
    - \* **GMAC-256:** Use 256-bit AES-GMAC encryption.
    - \* **None:** Use no encryption.
  - **IPSEC Encryption algorithm:** VPN configuration that the IPsec protocol uses.
  - **IKE Encryption Algorithm:** VPN configuration that the IPsec protocol uses.
  - **IKE Integrity Algorithm:** VPN configuration that the IPsec protocol uses.
  - **Knox:** Configurations for Samsung Knox only.
  - **Vendor:** A personal profile for generic agents that communicate with the Knox API.
  - **Forward routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
    - \* **Forward route:** Type the IP address for the forwarding route.
    - \* Click **Save** to save the route or click **Cancel** to not save the route.
  - **Per App VPN:** For each per-app VPN you want to add, click **Add** and do the following:
    - \* **Per App VPN:** The VPN configuration the app uses to communicate.
    - \* Click **Save** to save the per-app VPN or click **Cancel** to not save the per-app VPN.
- **Configure SSL connection settings**
    - **Authentication method:** In the list, click the authentication method to use. Possible options are:
      - \* **Not Applicable:** No authentication method applies. This setting is the default.
      - \* **Certificate:** Use certificate authentication. This setting is the default. If selected, in the Identity credential list, select the credential to use. The default is None.
      - \* **CAC based Authentication:** Use a Common Access Card (CAC) for authentication.
    - **CA certificate:** In the list, select the certificate to be used.
    - **Enable default route:** Select whether to enable a default route to the VPN server.
    - **Enable mobile option:** The default is **Off**.
    - **Split tunnel type:** In the list, select the type of split tunnel to use. Possible options are:
      - \* **Auto:** Split tunneling is automatically used.

- \* **Manual:** Split tunneling is used over the IP address and port specified.
- \* **Disabled:** No split tunneling is used.
- **SuiteB Type:** In the list, select the level of NSA Suite B encryption to use. The default is GCM-128. Possible options are:
  - \* **GCM-128:** Use 128-bit AES-GCM encryption.
  - \* **GCM-256:** Use 256-bit AES-GCM encryption.
  - \* **GMAC-128:** Use 128-bit AES-GMAC encryption.
  - \* **GMAC-256:** Use 256-bit AES-GMAC encryption.
  - \* **None: Use no encryption:** Type the SSL algorithm to use for client-server negotiation.
- **SSL Algorithm:** Type the SSL algorithm to use for client-server negotiation.
- **Knox:** Configurations for Samsung Knox only.
- **Vendor:** A personal profile for generic agents that communicate with the Knox API.
- **Forward routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - \* **Forward route:** Type the IP address for the forwarding route.
  - \* Click **Save** to save the route or click **Cancel** to not save the route.
- **Per App VPN:** For each per-app VPN you want to add, click **Add** and do the following:
  - \* **Per App VPN:** The VPN configuration the app uses to communicate.
  - \* Click **Save** to save the per-app VPN or click **Cancel** to not save the per-app VPN.

## Windows Phone settings

The screenshot displays the 'VPN Policy' configuration interface. On the left, a navigation pane shows 'Windows Phone' selected under the 'Platforms' section. The main area contains the following configuration options:

- Connection name:** Text input field.
- Profile type:** Dropdown menu set to 'Native'.
- VPN server name:** Text input field.
- Tunneling protocol:** Dropdown menu set to 'L2TP'.
- Authentication method:** Dropdown menu set to 'EAP'.
- EAP method:** Dropdown menu set to 'TLS'.
- DNS suffix:** Text input field.
- Trusted networks:** Text input field.
- Require smart card certificate:** Toggle switch set to 'OFF'.
- Automatically select client certificate:** Toggle switch set to 'OFF'.
- Remember credential:** Toggle switch set to 'OFF'.
- Always-on VPN:** Toggle switch set to 'OFF'.

At the bottom right, there are 'Back' and 'Next >' buttons.

These settings are supported only on Window 10 and later supervised phones.

- **Connection name:** Enter a name for the connection. This field is required.
- **Profile type:** In the list, select either **Native** or **Plugin**. The default is **Native**. The following sections describe the settings for each of these options.
- **Configure Native profile type settings:** These settings apply to the VPN built into users' Windows phones.
  - **VPN server name:** Type the FQDN or IP address for the VPN server. This field is required.
  - **Tunneling protocol:** In the list, select the type of VPN tunnel to use. The default is **L2TP**. Possible options are:
    - \* **L2TP:** Layer 2 Tunneling Protocol with pre-shared key authentication.
    - \* **PPTP:** Point-to-Point Tunneling.
    - \* **IKEv2:** Internet Key Exchange version 2.
  - **Authentication method:** In the list, select the authentication method to use. The default is **EAP**. Possible options are:
    - \* **EAP:** Extended Authentication Protocol.
    - \* **MSChapV2:** Use the Microsoft Challenge-Handshake Authentication Protocol for mutual authentication. This option is not available when you select IKEv2 for the tunnel type. When you choose MSChapV2, an **Automatically use Windows credentials** option appears. The default is **Off**.
  - **EAP method:** In the list, select the EAP method to be used. The default is **TLS**. This field is not available when MSChapV2 authentication is enabled. Possible options are:
    - \* **TLS:** Transport Layer Security
    - \* **PEAP:** Protected Extensible Authentication Protocol
  - **DNS Suffix:** Type the DNS suffix.
  - **Trusted networks:** Type a list of networks separated by commas that do not require a VPN connection for access. For example, when users are on your company wireless network, they can access protected resources directly.
  - **Require smart card certificate:** Select whether to require a smart card certificate. The default is Off.
  - **Automatically select client certificate:** Select whether to automatically choose the client certificate to use for authentication. The default is Off. This option is unavailable when **Require smart card certificate** is enabled.
  - **Remember credential:** Select whether to cache the credential. The default is Off. When enabled, credentials are cached whenever possible.
  - **Always on VPN:** Select whether the VPN is always on. The default is Off. When enabled, the VPN connection remains on until the user manually disconnects.
  - **Bypass For Local:** Type the address and port number to allow local resources to bypass the proxy server.
- **Configure Plugin protocol type:** These settings apply to VPN plug-ins obtained from the Windows Store and installed on users' devices.

- **Server address:** Type the URL, host name, or IP address for the VPN server.
- **Client app ID:** Type the package family name for the VPN plug-in.
- **Plugin Profile XML:** Select the custom VPN plug-in profile to be used by clicking **Browse** and navigating to the file's location. Contact the plug-in provider for format and details.
- **DNS Suffix:** Type the DNS suffix.
- **Trusted networks:** Type a list of networks separated by commas that do not require a VPN connection for access. For example, when users are on your company wireless network, they can access protected resources directly.
- **Remember credential:** Select whether to cache the credential. The default is Off. When enabled, credentials are cached whenever possible.
- **Always on VPN:** Select whether the VPN is always on. The default is Off. When enabled, the VPN connection remains on until the user manually disconnects.
- **Bypass For Local:** Type the address and port number to allow local resources to bypass the proxy server.

## Windows Desktop/Tablet settings

The screenshot displays the 'VPN Policy' configuration page in the Citrix Endpoint Management console. The left-hand navigation pane shows 'VPN Policy' selected, with sub-sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Windows Desktop/Tablet' is selected. The main configuration area contains the following settings:

- Connection name \***: Text input field.
- Profile type**: Dropdown menu set to 'Native'.
- Server address \***: Text input field.
- Remember credential**: Toggle switch set to 'OFF'.
- DNS suffix**: Text input field.
- Tunnel type \***: Dropdown menu set to 'L2TP'.
- Authentication method \***: Dropdown menu set to 'EAP'.
- EAP method \***: Dropdown menu set to 'TLS'.
- Trusted networks**: Text input field.
- Require smart card certificate**: Toggle switch set to 'OFF'.
- Automatically select client certificate**: Toggle switch set to 'OFF'.
- Always-on VPN**: Toggle switch set to 'OFF'.
- Bypass For Local**: Toggle switch (partially visible).

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

- **Connection name:** Enter a name for the connection. This field is required.
- **Profile type:** In the list, select either **Native** or **Plugin**. The default is **Native**.
- **Configure Native profile type:** These settings apply to the VPN built into users' Windows devices.
  - **Server address:** Type the FQDN or IP address for the VPN server. This field is required.
  - **Remember credential:** Select whether to cache the credential. The default is **Off**. When enabled, credentials are cached whenever possible.

- **DNS Suffix:** Type the DNS suffix.
- **Tunnel type:** In the list, select the type of VPN tunnel to use. The default is **L2TP**. Possible options are:
  - \* **L2TP:** Layer 2 Tunneling Protocol with pre-shared key authentication.
  - \* **PPTP:** Point-to-Point Tunneling.
  - \* **IKEv2:** Internet Key Exchange version 2.
- **Authentication method:** In the list, select the authentication method to use. The default is **EAP**. Possible options are:
  - \* **EAP:** Extended Authentication Protocol.
  - \* **MSChapV2:** Use the Microsoft Challenge-Handshake Authentication Protocol for mutual authentication. This option is not available when you select **IKEv2** for the tunnel type.
- **EAP method:** In the list, select the EAP method to be used. The default is **TLS**. This field is not available when MSChapV2 authentication is enabled. Possible options are:
  - \* **TLS:** Transport Layer Security
  - \* **PEAP:** Protected Extensible Authentication Protocol
- **Trusted networks:** Type a list of networks separated by commas that do not require a VPN connection for access. For example, when users are on your company wireless network, they can access protected resources directly.
- **Require smart card certificate:** Select whether to require a smart card certificate. The default is **Off**.
- **Automatically select client certificate:** Select whether to automatically choose the client certificate to use for authentication. The default is **Off**. This option is unavailable when you enable **Require smart card certificate**.
- **Always on VPN:** Select whether the VPN is always on. The default is **Off**. When enabled, the VPN connection remains on until the user manually disconnects.
- **Bypass For Local:** Type the address and port number to allow local resources to bypass the proxy server.
- **Configure Plugin profile type:** These settings apply to VPN plug-ins obtained from the Windows Store and installed on users' devices.
  - **Server address:** Type the FQDN or IP address for the VPN server. This field is required.
  - **Remember credential:** Select whether to cache the credential. The default is **Off**. When enabled, credentials are cached whenever possible.
  - **DNS Suffix:** Type the DNS suffix.
  - **Client app ID:** Type the package family name for the VPN plug-in.
  - **Plugin Profile XML:** Select the custom VPN plug-in profile to be used by clicking **Browse** and navigating to the file's location. Contact the plug-in provider for format and details.
  - **Trusted networks:** Type a list of networks separated by commas that do not require a VPN connection for access. For example, when users are on your company wireless network,

they can access protected resources directly.

- **Always on VPN:** Select whether the VPN is always on. The default is **Off**. When enabled, the VPN connection remains on until the user manually disconnects.
- **Bypass For Local:** Type the address and port number to allow local resources to bypass the proxy server.

## Amazon settings

The screenshot shows the 'VPN Policy' configuration page in the Citrix Endpoint Management console. The left sidebar has sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, macOS, Android, Samsung SAFE, Samsung KNOX, Windows Phone, Windows Desktop/Tablet, and Amazon (which is highlighted in light blue). The main content area is titled 'VPN Policy' and includes a description: 'This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.' Below this are several input fields: 'Connection name \*', 'Vpn Type' (a dropdown menu currently showing 'L2TP PSK'), 'Server address \*', 'User name' (with 'administrator' entered), 'Password' (masked with dots), 'L2TP Secret', 'IPsec Identifier', 'IPsec pre-shared key', 'DNS search domains', 'DNS servers', and 'Forwarding routes'. At the bottom right, there are 'Back' and 'Next >' buttons. A 'Deployment Rules' section is partially visible at the bottom left of the main area.

- **Connection name:** Enter a name for the connection.
- **VPN type:** Select the connection type. Possible options are:
  - **L2TP PSK:** Layer 2 Tunneling Protocol with pre-shared key authentication. This setting is the default.
  - **L2TP RSA:** Layer 2 Tunneling Protocol with RSA authentication.
  - **IPSEC XAUTH PSK:** Internet Protocol Security with pre-shared key and extended authentication.
  - **IPSEC HYBRID RSA:** Internet Protocol Security with hybrid RSA authentication.
  - **PPTP:** Point-to-Point Tunneling.

The following sections list the configuration options for each of the preceding connection types.

### Configure L2TP PSK settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.

- **Password:** Type an optional password.
- **L2TP Secret:** Type the shared secret key.
- **IPSec Identifier:** Type the name of the VPN connection that users see on their devices when connecting.
- **IPSec pre-shared key:** Type the secret key.
- **DNS search domains:** Type the domains against which a user device's search domain list can match.
- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.

#### Configure L2TP RSA settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **L2TP Secret:** Type the shared secret key.
- **DNS search domains:** Type the domains against which a user device's search domain list can match.
- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **Server certificate:** In the list, select the server certificate to be used.
- **CA certificate:** In the list, select the CA certificate to be used.
- **Identity credential:** In the list, select the identity credential to be used.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.

#### Configure IPSEC XAUTH PSK settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **IPSec Identifier:** Type the name of the VPN connection that users see on their devices when connecting.
- **IPSec pre-shared key:** Type the shared secret key.



- **DNS search domains:** Type the domains against which a user device's search domain list can match.
- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.

### Configure IPSEC AUTH RSA settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **DNS search domains:** Type the domains against which a user device's search domain list can match.
- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **Server certificate:** In the list, select the server certificate to be used.
- **CA certificate:** In the list, select the CA certificate to be used.
- **Identity credential:** In the list, select the identity credential to be used.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.

### Configure IPSEC HYBRID RSA settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **DNS search domains:** Type the domains against which a user device's search domain list can match.
- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **Server certificate:** In the list, select the server certificate to be used.
- **CA certificate:** In the list, select the CA certificate to be used.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.

- Click **Save** to save the route or click **Cancel** to not save the route.

### Configure PPTP settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **DNS search domains:** Type the domains against which a user device’s search domain list can match.
- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **PPP encryption (MPPE):** Select whether to enable data encryption with Microsoft Point-to-Point Encryption (MPPE). The default is **Off**.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.

### Chrome OS settings

The screenshot shows the Citrix Endpoint Management console interface. At the top, there are navigation tabs: Device Policies, Apps, Media, Actions, ShareFile, Enrollment Profiles, and Delivery Groups. The 'Device Policies' tab is active. On the left, a sidebar shows a list of policies under 'VPN Policy'. The 'Chrome OS' policy is selected and highlighted in light blue. The main area displays the configuration for this policy. A description states: 'This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.' The configuration fields include:
 

- VPN connection name \***: Text input field.
- Priority of this network**: Text input field.
- Connection type**: Dropdown menu set to 'L2TP-IPsec'.
- Host \***: Text input field.
- Auto connect**: Toggle switch set to 'OFF'.
- User name**: Text input field.
- Save credentials**: Toggle switch set to 'OFF'.
- Enable LCP echo**: Toggle switch set to 'OFF'.
- Authentication type**: Dropdown menu set to 'Pre-shared key'.
- Pre-Shared key**: Text input field.
- Save Pre-Shared key**: Toggle switch set to 'OFF'.
- IKE protocol version**: Dropdown menu set to 'v2'.

- **VPN connection name:** Type a user-friendly description of this connection. This setting is required.
- **Priority of this network:** Type a suggested priority value for this network. Use an integer value.
- **Connection type:** In the list, select **Open VPN** as the connection type.

Selecting **Open VPN** reveals more settings that are specific to OpenVPN connections. Scroll to see all settings.

VPN Policy	VPN Policy
1 Policy Info	This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms <span>Select All</span>	<p><b>VPN connection name *</b> <input type="text"/> ⓘ</p> <p><b>Priority of this network</b> <input type="text"/> ⓘ</p> <p><b>Connection type</b> <span>Open VPN</span> ⓘ</p> <div style="border: 2px solid purple; padding: 5px;"> <p><b>Host *</b> <input type="text"/> ⓘ</p> <p><b>Auto connect</b> <span>OFF</span> ⓘ</p> <p><b>Port</b> <input type="text"/></p> <p><b>Protocol</b> <span>udp</span></p> <p><b>User authentication type</b> <span>None</span> ⓘ</p> <p><b>User name</b> <input type="text"/> ⓘ</p> <p><b>Password</b> <input type="text"/></p> <p><b>OTP</b> <input type="text"/> ⓘ</p> <p><b>Save credentials</b> <span>OFF</span> ⓘ</p> <p><b>Cache credentials in memory</b> <span>OFF</span> ⓘ</p> <p><b>Auth</b> <span>SHA1</span> ⓘ</p> <p><b>Authentication retry type</b> <span>Ask again for authentication each time</span> ⓘ</p> <p><b>Cipher</b> <span>BF-CBC</span> ⓘ</p> <p><b>LZO compression</b> <span>adaptive</span> ⓘ</p> </div>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android <input type="checkbox"/> Samsung SAFE <input type="checkbox"/> Samsung KNOX <input type="checkbox"/> Windows Phone <input type="checkbox"/> Windows Desktop/Tablet <input type="checkbox"/> Amazon <input checked="" type="checkbox"/> Chrome OS	
3 Assignment	

- **Host:** Type the host name or IP address of the server the VPN connects to. Required for OpenVPN. The value you type here is the primary host. Optionally, you can configure extra hosts to connect to if the primary host fails to connect.
- **Auto connect:** Select whether the VPN connects to the host automatically. If this setting is set to **On**, the VPN connects to the host automatically. Default is **Off**.
- **Port:** Type the host server port number. Default is **1194**.
- **Protocol:** Type the protocol used when communicating with the host server. Default is **UDP**.

- **User authentication type:** In the list, choose the required form of user authentication:
  - **None:** No password or one-time PIN required.
  - **Password:** Password only. You can configure this value or let the user provide it at the time of connection.
  - **Password and OTP:** Password and one-time PIN. You can configure these values or let the user provide it at the time of connection.
  - **OTP:** One-time PIN. You can configure this value or let the user provide it at the time of connection.
- **User name:** Type the user name that is used to connect to the VPN. If not specified, the user is prompted for a user name when connecting to the VPN. This value is subject to text string expansions:
  - `${LOGIN_ID}` expands to the email address of the user before the @ symbol.
  - `${LOGIN_EMAIL}` - expands to the email address of the user.
- **Password:** Type the password text string that is used connection to the VPN. If not specified, the user is prompted for a password when connecting.
- **OTP:** Type the one-time PIN text string that is used to connect to the VPN. A password text string. If not specified, the user is prompted for a one-time PIN when connecting.
- **Save credentials:** Select whether user credentials are saved after a connection. If this setting is set to **Off**, users must enter their credentials each time they connect.
- **Cache credentials in memory:** Select whether user passwords and one-time PINs entered by users are cached in memory on the device. If this setting is set to **On**, caching is enabled. Default is **Off**.
- **Authentication:** Type the authentication algorithm used to secure the connection. Defaults to **SHA-256**.
- **Authentication retry type:** In the list, select the way the VPN responds when user credentials are not verified. Options are **Fail with error on retry**, **Retry without asking for authentication**, and **Ask again for authentication each time**. Default is **Fail with error on retry**.
- **Cipher:** Type the cipher algorithm used to secure connection. Default is **BF-CBC**.
- **LZO compression:** Select whether to use LZO compression for the VPN. If this setting is set to **On**, the VPN uses LZO compression. Default is **Off**.
- **Adaptive compression:** Select whether to use adaptive compression for the VPN. If this setting is set to **On**, the VPN uses adaptive compression. Default is **Off**.

VPN Policy	
1 Policy Info	Cipher: BF-CBC ⓘ
2 Platforms <span>Select All</span>	LZO compression: adaptive ⓘ
<input type="checkbox"/> iOS	Adaptive compression: OFF ⓘ
<input type="checkbox"/> macOS	<b>Extra hosts ⓘ</b>
<input type="checkbox"/> Android	Host name: <input type="text"/> ⓘ Add
<input type="checkbox"/> Samsung SAFE	Server poll time-out in seconds: <input type="text"/> ⓘ
<input type="checkbox"/> Samsung KNOX	Ignore default route: OFF ⓘ
<input type="checkbox"/> Windows Phone	Key direction: <input type="text"/> ⓘ
<input type="checkbox"/> Windows Desktop/Tablet	Peer certificate type: <input type="text"/> ⓘ
<input type="checkbox"/> Amazon	Push peer information: OFF
<input checked="" type="checkbox"/> Chrome OS	Peer certificate extended key usage: <input type="text"/> ⓘ
3 Assignment	Peer certificate key usage ⓘ
	Key usage numbers: <input type="text"/> ⓘ Add
	Peer certificate TLS: None ⓘ
	Data channel key renegotiation delay in seconds: <input type="text"/> ⓘ
	Bandwidth limit: <input type="text"/> ⓘ

- **Extra hosts:** Configure a list of hosts to try, in order, if the device cannot connect to the primary host. Configuring these extra hosts is optional.

1. Click **Add** to the right of **Host name**.
2. Type the server host name or IP address.
3. Click **Save**.

Repeat these steps to add more extra hosts.

- **Server poll time-out in seconds:** Type the maximum number of seconds to try to connect to this server before moving on to the next server in the list.
- **Ignore default route:** Select whether the host ignores the VPN gateway. By default, the device creates a default route to the gateway address advertised by the VPN server. If this setting is set to On, split tunneling is allowed. Default is Off. If the server pushes a redirect-configuration flag to the client, this setting is ignored.
- **Key direction:** Type the key direction text string. The key direction is passed in as `--key-direction`.
- **Peer certificate type:** Type **server** to check the peer certificate type. If this setting is not set, the peer certificate type is not checked.
- **Push peer information:** Select whether peer certificate information is pushed to this host. If this setting is set to **On**, peer information is pushed. Default is **Off**.

- **Peer certificate extended key usage:** Type the explicit extended key usage text string, in OID notation. Sign the peer certificate with that text string. Optional.
- **Peer certificate key usage:** Add key usage numbers required. These strings are hex encoded numbers.
- **Peer certificate TLS:** Require peer certificate signing based on RFC3280TLS rules. Default is **None**.
- **Data channel key renegotiation delay in seconds:** Type an integer to indicate the number of seconds to wait before renegotiating a channel key.
- **Bandwidth limit:** Type an integer to indicate the outgoing tunnel bandwidth limit, in the number of bytes per second.
- **Static challenge:** Type a string used in static challenge responses.
- **TLS authentication key contents:** Type the TLS key contents here. If this field is empty, TLS authentication can't be used.
- **TLS remote connections:** Type an X.509 name or common name to allow connections to only server hosts that share that name.
- **TLS minimum version:** Type the minimum TLS protocol version used by OpenVPN.
- **Verbosity level:** Type an integer for the verbosity level for TLS. If not specified, the verbosity level defaults to OpenVPN's default.
- **Verbosity hash:** If set, this value is passed as the `--verify-hash` argument to OpenVPN. The hash specifies the SHA-256 fingerprint for the level-1 certificate.
- **Verify host's X509 name:** Type the host's X.509 name used for comparison in verifying the name.
- **Verify host's X509 name type:** Select a type of X.509 name to be verified. Options: **name**, **name-prefix**, and **subject**.

## Wallpaper device policy

July 13, 2021

The Wallpaper device policy lets you add a .png or .jpg file to set wallpaper on an iOS device lock screen, home screen, or both. This policy is available for supervised devices only. To use different wallpaper on iPads and iPhones, you need to create different wallpaper policies and deploy them to the appropriate users.

The following table lists the Apple recommended image dimensions for iOS devices.

## iPhone

---

Device	Image dimensions in pixels
iPhone 12 Pro Max	2778 x 1284
iPhone 12 & iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 2nd Gen	1334 x 750
iPhone 7 Plus, 8 Plus	2208 x 1242
iPhone 7, 8	1334 x 750
iPhone 8 Plus	1334 x 750
iPhone 8	1334 x 750

---

## iPad

---

Device	Image dimensions in pixels
iPad Pro (1st, 2nd and 3rd gen 12.9")	2732 x 2048
iPad Pro 10.5-inch	2224 x 1668
iPad Pro (9.7-inch)	1536 x 2048
iPad Air 2	2048 x 1536

---

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

- **Apply to:** In the list, select **Lock screen**, **Home (icon list) screen**, or **Lock and home screens** to set where the wallpaper is to appear.
- **Wallpaper file:** To select the wallpaper file, click **Browse** and then navigate to the file location.

## Web content filter device policy

September 2, 2021

You can filter web content on iOS devices by using the Apple auto-filter function with specific sites that you add to allow or block lists. Web content filter device policy is available only on iOS devices in Supervised mode. For information about placing an iOS device into Supervised mode, see [Deploy devices using Apple Configurator 2](#).

### Note:

Android devices don't support web content filtering.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## iOS settings

- **Filter type:** In the list, click either **Built-in** or **Plug-in**, and then follow the procedures that follow for the option you choose. The default is **Built-in**.

### Built-in filter type

- **Web Content Filter**
  - **Auto filter enabled:** Whether to use the Apple auto-filter function to analyze websites for inappropriate content. The default is **Off**.
  - **Permitted URLs:** This list is ignored when **Auto filter enabled** is set to **Off**. When **Auto filter enabled** is set to **On**, the items in this list are always accessible whether or not the auto filter allows access. For each URL you want to add to the allow list, click **Add** and do the following:
    - \* Type the URL of the permitted website. You must add `https://` or `http://` before the web address.
    - \* Click **Save** to save the website to the allow list or click **Cancel** not to save it.
  - **Blocked URLs:** Items in this list are always blocked. For each URL you want to add to the block list, click **Add** and do the following:



- \* Enter the URL of the website to be blocked. You must add <https://> or <http://> before the web address.
- \* Click **Save** to save the website to the block list or click **Cancel** not to save it.
- **Bookmark allow list**
  - **Bookmark allow list:** Specifies the sites that users can access. To enable access to web sites, add their URL.
    - \* **URL:** The URL of each web site that users can access. For example, to enable access to the Secure Hub store, add the Endpoint Management server URL to the **URL** list. You must add <https://> or <http://> before the web address. This field is required.
    - \* **Bookmark folder:** Enter an optional bookmark folder name. If this field is left blank, the bookmark is added to the default bookmarks directory.
    - \* **Title:** Enter a descriptive title for the web site. For example, type “Google” for the URL <https://google.com>.
    - \* Click **Save** to save the website to the allow list or click **Cancel** not to save it.

### Plug-in filter type

- **Filter name:** Enter a unique name for the filter.
- **Identifier:** Enter the bundle ID of the plugin that provides the filtering service.
- **Service address:** Enter an optional server address. Valid formats are IP address, host name, or URL.
- **User name:** Enter an optional user name for the service.
- **Password:** Enter an optional password for the service.
- **Certificate:** In the list, click an optional identity certificate to be used to authenticate the user to the service. The default is **None**.
- **Filter WebKit traffic:** Select whether to filter WebKit traffic.
- **Filter Socket traffic:** Select whether to filter socket traffic.
- **Custom Data:** For each custom key you want to add to the web filter, click **Add** and then do the following:
  - **Key:** Type the custom key.
  - **Value:** Type a value for the custom key.
  - Click **Save** to save the custom key or click **Cancel** not to save it.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

## Web clip device policy

January 28, 2021

You can place shortcuts, or web clips, to websites to appear alongside apps on user devices. You can specify your own icons to represent the web clips for iOS, iPadOS, macOS, and Android devices. Windows tablet requires just a label and a URL. For iOS and iPadOS devices, configure the home screen layout device policy to organize the web clips you create. If you restrict access to apps on iOS, ensure that you configure the restriction device policy to allow web clips. For information on configuring these policies, see [Home screen layout device policy](#) and [Restrictions device policy](#).

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### iOS settings

- **Label:** Type the label that is to appear with the web clip.
- **URL:** Type the URL associated with the web clip. The URL must begin with a protocol, for example, <https://server>.
- **Removable:** Select whether users can remove the web clip. The default is **Off**.
- **Icon to be updated:** Select the icon to be used for the web clip by clicking **Browse** and navigating to the file location.
- **Precomposed icon:** Select whether the icon has effects (rounded corners, drop shadow, and reflective shine) applied to it. The default is **Off**, which adds the effects.
- **Full screen:** Select whether the linked webpage opens in full-screen mode. This setting also enables an iPad to only open a single website. Alternatively, to set up iPads to run in Kiosk mode, use the App lock device policy. For more information, see [Configure an iPad as a kiosk](#). The default is **Off**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

### macOS settings

- **Label:** Type the label that is to appear with the web clip.

- **URL:** Type the URL associated with the web clip. The URL must begin with a protocol, for example, <https://server>.
- **Icon to be updated:** Select the icon to be used for the web clip by clicking Browse and navigating to the file location.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - \* **Select date:** Click the calendar to select the specific date for removal.
    - \* **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.

### Android settings

- **Rule:** Select whether this policy adds or removes a web clip. The default is **Add**.
- **Label:** Type the label that is to appear with the web clip.
- **URL:** Type the URL associated with the web clip.
- **Define an icon:** Select whether to use an icon file. The default is **Off**.
- **Icon file:** If **Define an icon** is **On**, select the icon file to use by clicking **Browse** and navigating to the file location.

### Windows Desktop/Tablet settings

- **Name:** Type the label that is to appear with the web clip.
- **URL:** Type the URL associated with the web clip.

### Windows Agent device policy

August 31, 2021

Use the Windows Agent device policy to run PowerShell scripts on managed Windows desktops and tablets. You can point to script files uploaded to Endpoint Management as an enterprise app and to other servers that host scripts. For information about adding enterprise apps, see [Add apps](#).

All scripts execute under privileged status, you don't need to run scripts as an administrator.

After deploying and running the script, you can configure automated actions based on the results of the script. For instance, you run a script that monitors a registry key and returns a result. Based on the returned result, an automated action runs. The action grants or denies access to an app, marks the device as out of compliance, or has other effects.

You can also use this policy to deploy customized MSI installers by configuring a PowerShell script that points to a .msi file and a .mst file.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Windows Desktop and Tablet settings

The screenshot displays the 'Windows Agent policy' configuration interface. The left sidebar shows a navigation menu with 'Windows Desktop/Tablet' selected. The main area shows the policy details and configuration options.

**Windows Agent policy**  
This policy lets you configure, schedule, and run PowerShell scripts on MDM-managed devices.

**1 Policy Info**

**2 Platforms** [Clear All](#)

- Windows Desktop/Tablet

**3 Assignment**

**example**

**Config name \*** example

**Task type \*** PowerShell

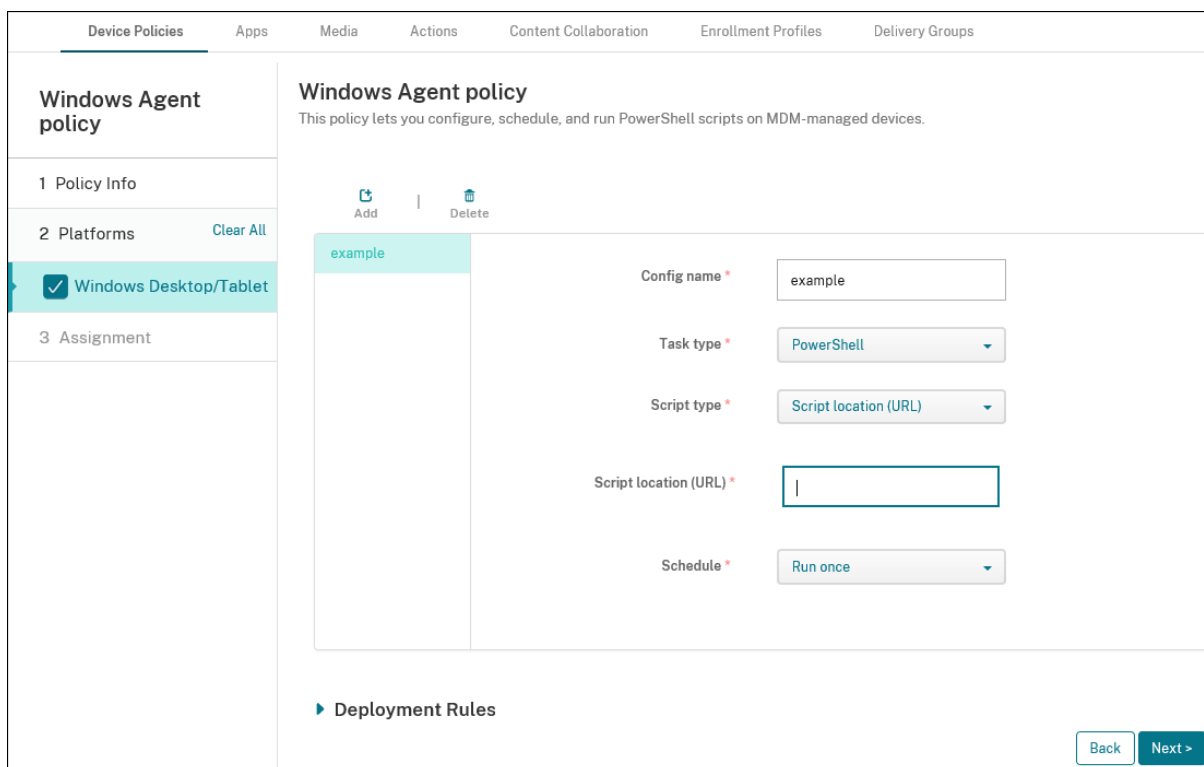
**Script type \*** Uploaded script

**Script \*** Select an option

**Schedule \*** Run once

**Deployment Rules**

[Back](#) [Next >](#)



- **Config name:** Type a descriptive name for your configuration.
- **Task type:** Select **PowerShell**.
- **Script type:** Select **Uploaded script** for scripts that you have uploaded to Endpoint Management or select **Script location (URL)** for scripts hosted externally. For more information on how to upload a script to Endpoint Management, see [Add Win32 apps as Enterprise apps](#).
  - **Select script:** If you chose **Uploaded script**, select the script to run.
  - **Script location (URL):** If you chose **Script location (URL)**, enter the location of the script to run. This URL must deliver the script as a payload. Endpoint Management doesn't support URLs that deliver scripts as a JavaScript download. The script must also be publicly available.
- **Schedule:** Select **Run once** to run the selected script one time or select **Run on a recurring basis** to run the script regularly.
  - **Run every (hours):** Type the number of hours between script runs.

To check on the status of a script, navigate to **Manage > Devices** in your console. Select the device on which you want to check the script status and click **Edit**. Under **Properties**, you can check the status of your scripts by clicking **Download** under the **Windows Agent** heading.

## Deploy a PowerShell script to trigger an automated action

1. Create a PowerShell script to monitor a registry key. The following PowerShell script checks to see if the firewall is enabled.

```
1 $body = @{
2   }
3
4 $firewallEnabled = Get-ItemPropertyValue HKLM:\SYSTEM\
   CurrentControlSet\Services\SharedAccess\Parameters\
   FirewallPolicy\StandardProfile -Name EnableFirewall
5 if($firewallEnabled -eq 1){
6
7   $body["firewallEnabled"]="true"
8 }
9   else {
10
11   $body["firewallEnabled"]="false"
12 }
13
14 $body | ConvertTo-Json -Depth 10
15 <!--NeedCopy-->
```

This script returns a value of either

```
1 {
2
3   "firewallEnabled": "true"
4 }
5
6 <!--NeedCopy-->
```

or

```
1 {
2
3   "firewallEnabled": "false"
4 }
5
6 <!--NeedCopy-->
```

2. Upload the script to the Endpoint Management console as an enterprise app or host the script at an accessible URL.
3. Configure the Windows Agent device policy described in this article. Ensure that the script is scheduled to run immediately.

4. After the script runs, determine the script status.
  - a) Navigate to **Manage > Devices** in your console.
  - b) Select the device to check its script status and then click **Edit**.
  - c) Click **Download** under the **Windows Agent** heading.
5. Configure an automated action based on the status received. For more information on configuring automated actions, see [Create an automated action based on a Windows Agent device policy result](#). That section shows the specific automated actions created for the example script and Windows Agent device policy.

## Windows GPO Configuration device policy

September 8, 2021

The Windows GPO Configuration device policy allows you to:

- Use the Endpoint Management console to import Group Policy Objects (GPOs) and deploy them to Windows 10 and Windows 11 devices.
- Configure GPOs for any Windows device supported by Citrix Workspace Environment Management.
- Configure GPOs at a device and user level.

### Import GPOs for deployment to Windows 10 and Windows 11 devices

Rather than relying on an AD administrator to use the Group Policy Management console to manage GPOs, you can import and deploy GPOs through the Endpoint Management console.

To create a backup of your GPOs in Endpoint Management:

1. Request that your AD administrator export GPOs from the Group Policy Management console and provide the files to you.
2. In the Endpoint Management console, go to **Configure > Device Policies** and create a **Windows GPO Configuration** policy.
3. Click **Upload**, locate the file, and then click **Open** to import the file.

The screenshot displays the 'Windows GPO Configuration Policy' configuration interface. The top navigation bar includes 'Device Policies', 'Apps', 'Media', 'Actions', 'Content Collaboration', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar shows a tree view with '1 Policy Info' selected, followed by '2 Platforms' and '3 Assignment'. The 'Windows Desktop/Tablet' platform is checked. The main area, titled 'Policy Information', explains that the policy is used for configuring OS-level settings via Group Policy Administrative Templates. It features a 'Policy Name' input field, a 'Description' text area, and an 'Auto save' toggle set to 'ON' with a note that contents are saved every 2 minutes. At the bottom, the 'Upload GPO policy' section provides instructions and an 'Upload' button for uploading GPO files.

For information about configuring GPOs, see in this article, [Windows desktop and tablet settings](#).

## Configure GPOs for deployment to Citrix Workspace Environment Management

The Windows GPO Configuration device policy allows you to configure GPOs for any Windows device supported by Citrix Workspace Environment Management (WEM). Endpoint Management pushes the policies to the Citrix WEM service. The WEM service then applies the GPOs to devices and their apps by using the WEM agent installed on devices.

For information about installing the Workspace Environment Management agent, see [Install and configure](#).

This policy uses all Windows OS ADMX files. If you want to upload a third-party ADMX file, use the App Configuration device policy. For more information on uploading third-party ADMX files, see [Application Configuration device policy](#).

- You can push GPO configurations to any device that WEM supports, even if Endpoint Management doesn't support the device natively. For a list of the devices supported, see [Operating System requirements](#).
- This policy requires that a device has the WEM agent installed and configured. There is no need to MDM or MAM enroll the devices.
- Endpoint Management pushes GPO settings through the WEM channel. (Microsoft doesn't support pushing device-level settings through the MDM channel.) Devices which receive the Windows GPO Configuration device policy run in the Endpoint Management mode called WEM. In the **Manage > Devices** list of enrolled devices, the **Mode** column for WEM-managed devices lists **WEM**.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).



## Windows desktop and tablet settings

This policy allows you to configure GPOs at a device and user level.

Select and configure the Windows GPO to deploy to your Windows devices. You can modify **Device Configuration** and **User Configuration**. Policies are listed in a tree structure. Click **All Settings** to display every setting. For information about the settings, download a GPO reference sheet from [Microsoft](#).

To configure a setting, you first enable it. During configuration, Endpoint Management auto-saves the changes so that those settings persist. If you try to leave the page before a setting has been saved, a pop-up message indicates that there are unsaved changes.

If a setting has two options, a radio button selection appears. With more than two options, a menu appears.

### Note:

If you need to check which settings you configured, you can do the following.

1. In the Endpoint Management console, open the **Windows GPO Configuration** policy you want to edit.
2. Under **Devices** or **Users**, select **All Settings**.
3. Sort the table by **Status**, ascending. All unconfigured policies have the status **Not Configured**. The policies you configure are listed at the top.

## Windows Hello for Business device policy

February 23, 2021

Windows Hello for Business allows users to sign on to Windows devices by using their Active Directory or Azure Active Directory account. You use the Windows Hello for Business device policy to enable the feature so users can provision Windows Hello for Business on their device. The policy also lets you configure passcode limitations and other security features.

Go to **Configure > Device Policies** to add the Windows Hello for Business policy. Configure these settings:

### Windows Phone and Windows Desktop/Tablet settings

The screenshot displays the configuration page for the 'Windows Hello for Business policy'. The left sidebar shows the 'Platforms' section with 'Windows Phone' and 'Windows Desktop/Tablet' selected. The main configuration area includes the following settings:

- Windows Hello for Business:**
  - Use Windows Hello for Business:
  - Require security device:
- PIN complexity:**
  - Minimum PIN length: 4
  - Maximum PIN length: 127
  - Uppercase letters: Do not allow
  - Lowercase letters: Do not allow
  - Special characters: Do not allow
  - Digits: Require
  - History: 0
  - Expiration: 0
- Biometrics:**
  - Use biometrics:

At the bottom right, there are 'Back' and 'Next >' buttons.

- **Use Windows Hello for Business:** Enable the feature to allow users to provision Windows Hello for Business on their device.
- **Require security device:** Require that users have a Trusted Platform Module (TPM) to sign on.

- **Minimum/Maximum PIN length:** Minimum and maximum length for user PINs. **Minimum PIN Length** defaults to **4**. **Maximum PIN Length** defaults to **127**.
- **Uppercase letters, Lowercase letters, Special characters:** Select whether to **Allow, Require,** or **Do not allow** each type of character. Defaults to **Do not allow**.
- **Digits:** Whether to **Allow, Require,** or **Do not allow** digits. Defaults to **Require**.
- **History:** The number of past PINs that users can't reuse. Defaults to **0**, meaning users can reuse all PINs.
- **Expiration:** The number of days before a user must change their PIN. Defaults to **0**, which means that PINs don't expire.
- **Use biometrics:** Allow the use of biometrics instead of PINs for user sign-on.

## Windows Information Protection device policy

October 27, 2021

Windows Information Protection (WIP), previously known as enterprise data protection (EDP), is a Windows technology that protects against the potential leakage of enterprise data. Data leakage can occur through sharing of enterprise data to non-enterprise protected apps, between apps, or outside of the organization network. For more information, see [Protect your enterprise data using Windows Information Protection \(WIP\)](#).

You can create a device policy in Endpoint Management to specify the apps that require Windows Information Protection at the enforcement level you set. The Windows Information Protection policy is for supervised Phone, Tablet, and Desktop running Windows 10 (version 1607 or later) or Windows 11.

Endpoint Management includes some common apps and you can add others. You specify for the policy an enforcement level that affects the user experience. For example, you can:

- Block any inappropriate data sharing.
- Warn about inappropriate data sharing and allow users to override the policy.
- Run WIP silently while logging and permitting inappropriate data sharing.

To exclude apps from Windows Information Protection, define the apps in Microsoft AppLocker XML files and then import those files into Endpoint Management.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

## Windows Phone and Windows Desktop/Tablet settings

The screenshot shows the 'Windows Information Protection policy' configuration page. On the left, there is a navigation pane with sections: '1 Policy Info', '2 Platforms' (with a 'Clear All' link), and '3 Assignment'. Under '2 Platforms', 'Windows Phone' and 'Windows Desktop/Tablet' are both checked. The main content area shows the policy details and a 'Store App' table.

Publisher *	Product name *	Version *	Allowed	Actions
CN=O=IL=FC=I	Microsoft.MicrosoftEdge	*	Allowed	+ Add
CN=O=IL=FC=I	Microsoft.Office.Word	*	Allowed	Edit Remove

- **Desktop App** (Windows 10 and Windows 11 Desktops), **Store App** (Windows 10 Phones, Windows 10 and Windows 11 Tablets): Endpoint Management includes some common apps, as shown in the sample above. You can edit or remove those apps as needed.

To add other apps: In the **Desktop App** or **Store App** table, click **Add** and provide the app information.

**Allowed** apps can read, create, and update enterprise data. **Denied** apps can't access enterprise data. **Exempt** apps can read enterprise data but can't create or modify the data.

### Note:

Starting from Windows 11, Microsoft provides Notepad as a Store app instead of the traditional Desktop app. To enable this policy to take effect on Notepad running on Windows 11 devices, remove Notepad from the Desktop App table, and then add it to the Store App table.

- **AppLocker XML file:** Microsoft provides a list of Microsoft apps that have known compatibility issues with WIP. To exclude those apps from WIP, click **Browse** to upload the list. Endpoint Management combines the uploaded AppLocker XML file and the configured desktop and store apps in the policy sent to the device. For more information, see [Recommended block list for Windows Information Protection](#).
- **Enforcement level:** Select an option to specify how you want Windows Information Protection to protect and manage data sharing. Defaults to **Off**.
  - \* **0-Off:** WIP is off and doesn't protect or audit your data.
  - \* **1-Silent:** WIP runs silently, logs inappropriate data sharing, and doesn't block anything. You can access logs through [Reporting CSP](#).
  - \* **2-Override:** WIP warns users about potentially unsafe data sharing. Users can override warnings and share the data. This mode logs actions, including user overrides, to your audit log.

- \* **3-Block:** WIP prevents users from completing potentially unsafe data sharing.
- **Protected domain names:** The domains that your enterprise uses for its user identities. This list of managed identity domains, along with the primary domain, make up the identity of your managing enterprise. The first domain in the list is the primary corporate identity used in the Windows UI. Use pipes (|) to separate list items. For example: `domain1.com|domain2.com`
- **Data recovery certificate:** Click **Browse** and then select a recovery certificate to use for data recovery of encrypted files. This certificate is the same as the data recovery agent (DRA) certificate for the encrypting file system (EFS), only delivered through MDM instead of Group Policy. If a recovery certificate isn't available, create it. For information, see "Create a data recovery certificate" in this section.
- **Network domain names:** A list of domains that comprise the boundaries of the enterprise. WIP protects all traffic to the fully qualified domains in this list. This setting, with the **IP range** setting, detects whether a network endpoint is enterprise or personal on private networks. Use commas to separate list items. For example: `corp.example.com,region.example.com`
- **IP range:** A list of the enterprise IPv4 and IPv6 ranges that define the computers in the enterprise network. WIP considers these locations as a safe destination for enterprise data sharing. Use commas to separate list items. For example:  
`10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff`
- **Automatically detect IP ranges:** If **On**, prevents Windows from detecting IP ranges automatically. Defaults to **Off**.
- **Proxy servers:** A list of the proxy servers that the enterprise can use for corporate resources. This setting is required if you use a proxy in your network. Without a proxy server, enterprise resources might be unavailable when a client is behind a proxy. For example, resources might be unavailable from certain Wi-Fi hotspots at hotels and restaurants. Use semicolons (;) to separate list items. For example:  
`proxy.example.com:80;157.54.11.118:443`
- **Internal proxy servers:** A list of the proxy servers that your devices go through to reach your cloud resources. Using this server type indicates that the cloud resources you're connecting to are enterprise resources. Don't include in this list any of the servers in the **Proxy servers** setting, which are used for non-WIP-protected traffic. Use semicolons (;) to separate list items. For example:  
`example.internalproxy1.com;10.147.80.50`

- **Cloud resources:** A list of cloud resources protected by WIP. For each cloud resource, you can also optionally specify a proxy server in the **Proxy servers** list to route traffic for this cloud resource. All traffic routed through the **Proxy servers** is treated as enterprise traffic. Use pipes (|) to separate list items. For example:

```
domain1.com:InternalProxy.domain1.com|domain2.com:InternalProxy.  
domain2.com
```

- **Enable protection under lock:** Windows 10 Phone only. If **On**, the Passcode device policy is also required. Otherwise, the Windows Information Protection policy deployment fails. Also, if this policy is **On**, the setting **Protection under lock** appears. Default is **Off**.
- **Protection under lock:** Windows 10 Phone only. Specifies whether to encrypt enterprise data using a key that's protected by an employee PIN on a locked device. Apps can't read corporate data on a locked device. Defaults to **On**.
- **Revoke WIP certificate on unenroll:** Specifies whether to revoke local encryption keys from a user device when it's unenrolled from Windows Information Protection. After the encryption keys are revoked, a user can't access encrypted corporate data. If **Off**, the keys aren't revoked and the user continues to have access to protected files after unenrollment. Defaults to **On**.
- **Show overlay icons:** Specifies whether to include the Windows Information Protection icon overlay on corporate files in Explorer and enterprise only app tiles in the Start menu. Defaults to **Off**.

## Create a data recovery certificate

A data recover certificate is required to enable the **Windows Information Protection** policy.

1. On the machine where the Endpoint Management console is running, open a command prompt and navigate to a folder (other than Windows\System32) where you want to create a certificate.

2. Run this command:

```
cipher /r:ESFDRA
```

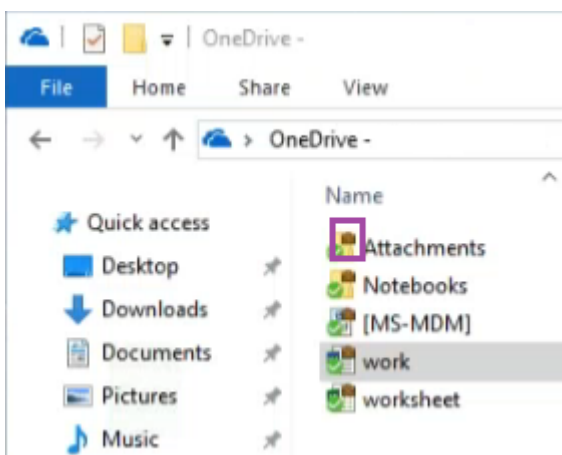
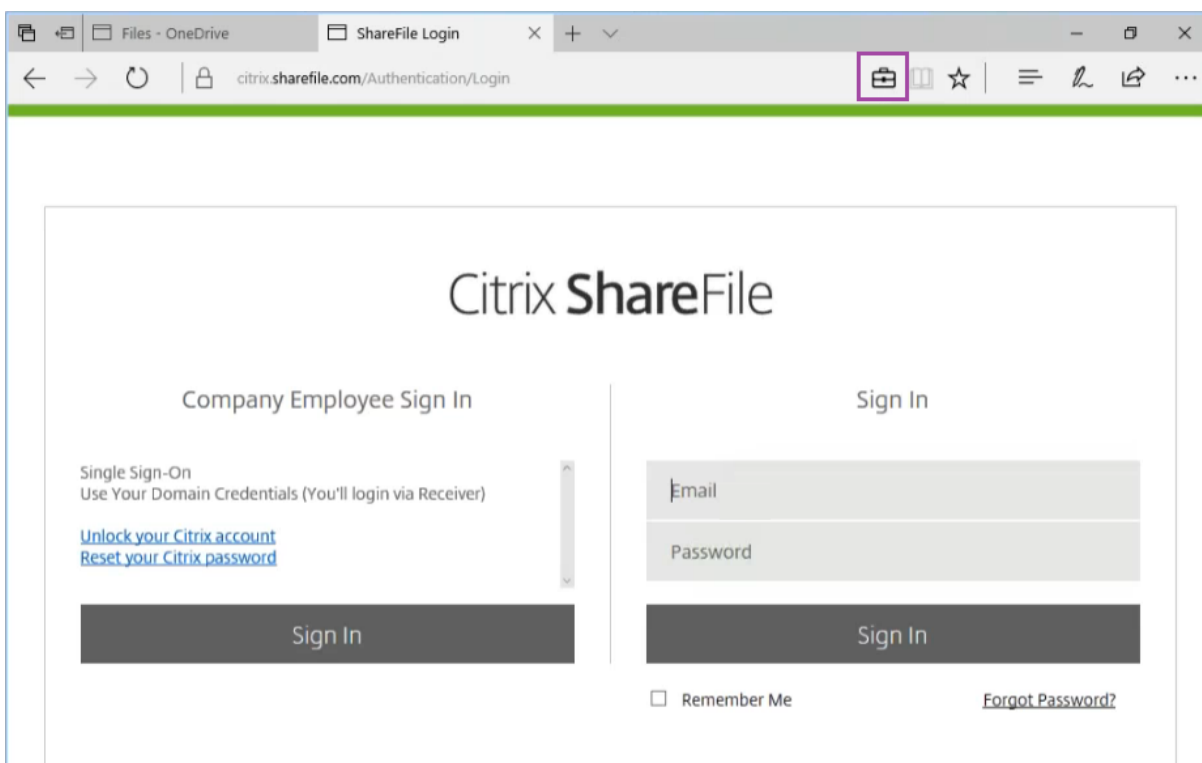
3. When prompted, enter a password to protect the private key file.

The cipher command creates a .cer and a .pfx file.

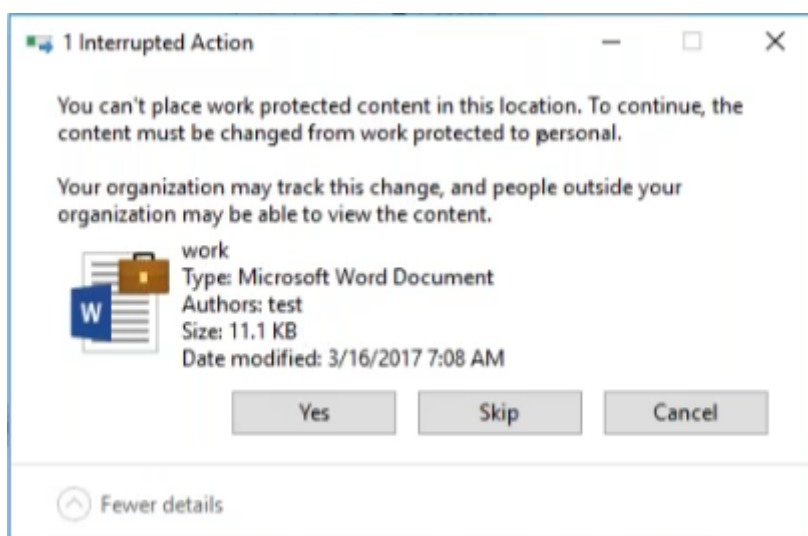
4. In the Endpoint Management console, go to **Settings > Certificates** and import the .cer file, which applies to both Windows 10 and Windows 11 tablets and Windows 10 phones.

## User experience

When Windows Information Protection is in effect, apps and files include an icon:



If a user copies or saves a protected file to a non-protected location, the following notification appears, depending on the enforcement level configured.



## Add apps

October 7, 2021

Adding apps to Endpoint Management provides mobile application management (MAM) capabilities. Endpoint Management assists with application delivery, software licensing, configuration, and application life cycle management.

MDX-enabling apps is an important part of preparing some types of apps for distribution to user devices. For an introduction to MDX, see [Endpoint Management components](#) and [MAM SDK overview](#).

- Citrix recommends use of the MAM SDK to MDX-enable apps. Or, you can continue to MDX-wrap apps until the MDX Toolkit is deprecated. See [Deprecation](#).
- You cannot use the MDX Toolkit to wrap Citrix mobile productivity apps. Get the mobile productivity app MDX files from Citrix downloads.

When you add apps to the Endpoint Management console, you:

- Configure app settings
- Optionally arrange apps into categories to organize them in Secure Hub
- Optionally define workflows to require approval before allowing users to access an app
- Deploy apps to users

This article covers the general workflows for adding apps. See the following articles for platform specifics:

- [Distribute Android Enterprise and Android for Workspace apps](#)
- [Distribute Apple apps](#)



## App types and features

The following table summarizes the types of apps you can deploy with Endpoint Management.

App type	Sources	Notes	See
MDX	iOS and Android apps you develop for your users. Citrix mobile productivity apps.	Develop iOS or Android apps with the MAM SDK or wrap them with the MDX Toolkit. For the mobile productivity apps, download the public-store MDX files from Citrix downloads. Then, add the apps to Endpoint Management.	Add an MDX app
Public app store	Free or paid apps from public app stores such as Google Play or the Apple App Store.	Upload the apps, MDX-enable the apps, then add the apps to Endpoint Management.	Add a public app store app
Web and SaaS	Your internal network (web apps) or a public network (SaaS).	Citrix Workspace provides mobile single sign-on to native SaaS apps from iOS and Android devices enrolled in MDM. Or, use Security Assertion Markup Language (SAML) application connectors	Add a Web or SaaS app

App type	Sources	Notes	See
Enterprise	Private apps, including Win32 apps, that aren't MDX-enabled. Private Android Enterprise or Android for Workspace apps that are MDX-enabled. Enterprise apps reside in Content Delivery Network locations or Endpoint Management servers.	Add the apps to Endpoint Management.	Add an enterprise app
Web link	Internet web addresses, intranet web addresses, or web apps that don't require single sign-on.	Configure web links in Endpoint Management.	Add a Web link

When planning app distribution, consider these features:

- About silent installations
- About required and optional apps
- About app categories
- Deliver enterprise apps from the Citrix CDN
- Enable Microsoft 365 apps
- Apply workflows
- App store and Citrix Secure Hub branding
- Citrix Virtual Apps and Desktops through the app store

### About silent installations

Citrix supports the silent installation and upgrade of iOS, Android Enterprise, Android for Workspace, and Samsung apps. Silent installation means that users are not prompted to install apps that you deploy to the device. The apps install automatically in the background.

Prerequisites to implement silent installation:

- For iOS, put the managed iOS device in supervised mode. For details, see [Import iOS & macOS Profile device policy](#).
- For Android Enterprise and Android for Workspace, the apps install in the Android work profile on the device. For details, see [Android Enterprise](#) and [Android for Workspace](#).
- For Samsung devices, enable Samsung Knox on the device.

To do so, you set the Samsung MDM license key device policy to generate Samsung ELM and Knox license keys. For details, see [Samsung MDM license key device policies](#).

### About required and optional apps

When you add apps to a delivery group, you choose whether they are optional or required. Citrix recommends deploying apps as **Required**.

- Required apps install silently on user devices, minimizing interaction. Having this feature enabled also allows apps to update automatically.
- Optional apps allow users to choose what apps to install, but users must initiate the installation manually through Secure Hub.

For apps marked as required, users can promptly receive updates in situations such as:

- You upload a new app and mark it as required.
- You mark an existing app as required.
- A user deletes a required app.
- A Secure Hub update is available.

### Requirements for forced deployment of required apps

- Secure Hub 10.5.15 for iOS and 10.5.20 for Android (minimum versions)
- MAM SDK or MDX Toolkit 10.6 (minimum version)
- After you upgrade Endpoint Management and Secure Hub: Users with enrolled devices must sign off and then sign on to Secure Hub to obtain the required app deployment updates.

### Examples

The following examples show the sequence of adding an app named Secure Tasks to a delivery group and then deploying the delivery group.

# Citrix Endpoint Management

Device Policies | Apps | Actions | ShareFile | Enrollment Profiles | **Delivery Groups**

### Delivery Group

- 1 Delivery Group Info
- 2 User
- 3 Resource (optional)
- Policies**
- Apps**
- Actions
- ShareFile
- Enrollment Profile
- 4 Summary

### Apps

Drag the apps that you want to include in the delivery group.

Enter app name  Search

Apps

- Angry Bird
- Box
- Fit
- SecureNotes

Required Apps

- SecureWeb
- Enterprise-01
- GTM
- SecureTask**

Optional Apps

- Jira
- Office365\_SAML

Device Policies | Apps | Actions | ShareFile | Enrollment Profiles | **Delivery Groups**

### Delivery Groups

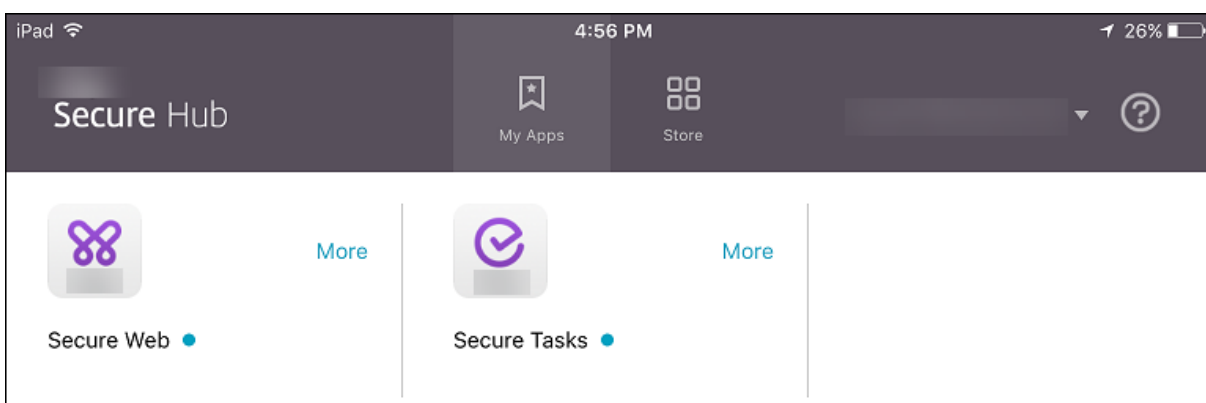
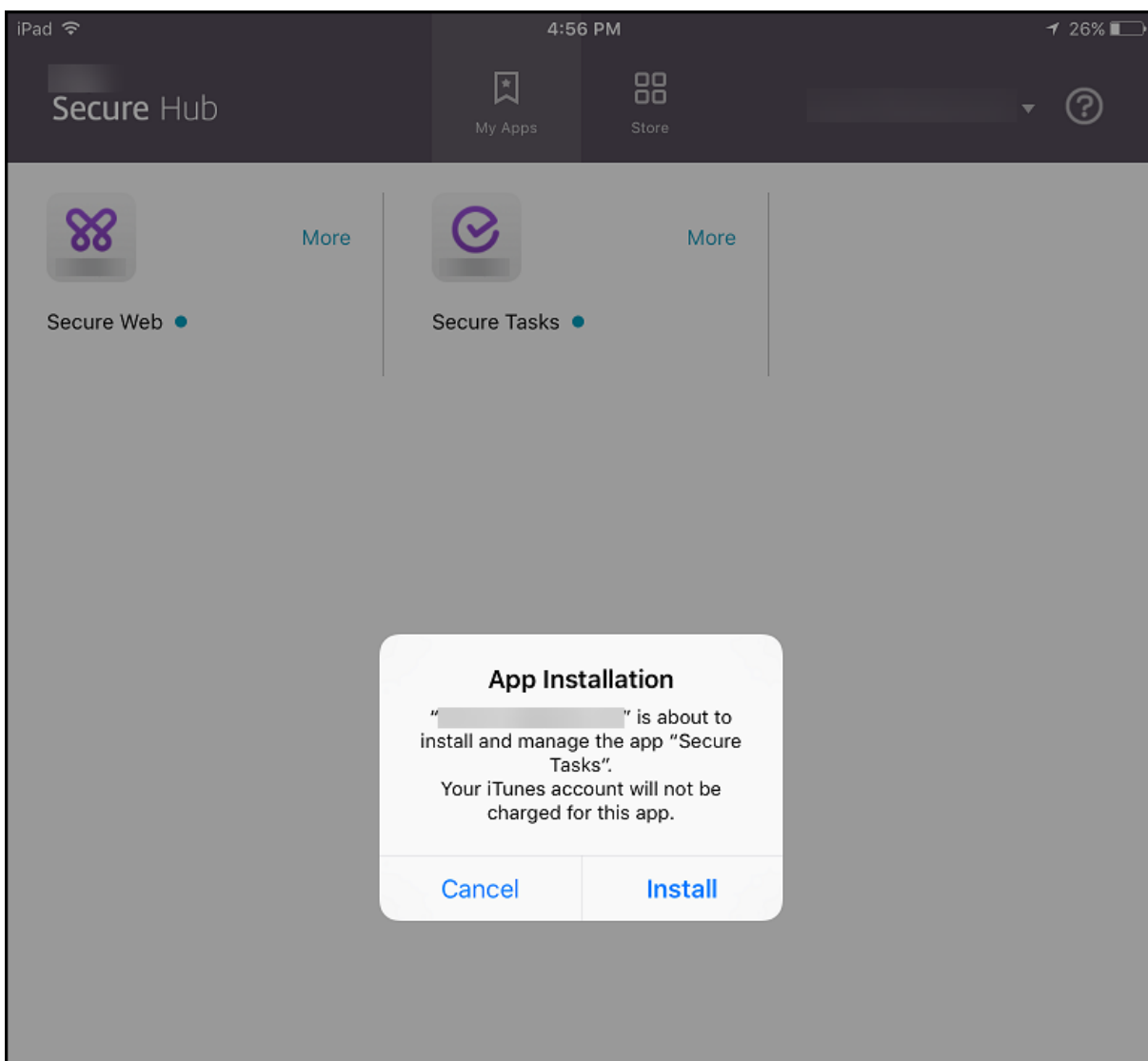
Show filter  Search

Add | Edit | **Deploy** | Delete | Export

Status	Name	Last Updated	Disabled
<input type="checkbox"/>	AllUsers	Apr 18 2017 2:43 AM	
<input checked="" type="checkbox"/>	<b>DeliveryGroup-01</b>	<b>Apr 19 2017 8:47 AM</b>	

Showing 1 - 2 of 2 items Items per page: 10

After the sample app, Secure Tasks, deploys to the user device, Secure Hub prompts the user to install the app.



**Important:**

MDX-enabled required apps, including enterprise apps and public app store apps, upgrade immediately. This upgrade occurs even if you configure an MDX policy for an app update grace

period and the user chooses to upgrade the app later.

### **iOS required app workflow for enterprise and public store apps**

1. Deploy the mobile productivity app during initial enrollment. The required app is installed on the device.
2. Update the app on the Endpoint Management console.
3. Use the Endpoint Management console to deploy required apps.
4. The app on the home screen is updated. And, for public store apps, the upgrade starts automatically. Users are not prompted to update.
5. Users open the app from the home screen. Apps upgrade immediately even if you set an App update grace period and the user taps to upgrade the app later.

### **Android required app workflow for enterprise apps**

1. Deploy the mobile productivity app during initial enrollment. The required app is installed on the device.
2. Use the Endpoint Management console to deploy required apps.
3. The app is upgraded. (Nexus devices prompt for install updates, but Samsung devices do a silent install.)
4. Users open the app from the home screen. Apps upgrade immediately even if you set an App update grace period and the user taps to upgrade the app later. (Samsung devices do a silent install.)

### **Android required app workflow for public store apps**

1. Deploy the mobile productivity app during initial enrollment. The required app is installed on the device.
2. Update the app on the Endpoint Management console.
3. Use the Endpoint Management console to deploy required apps. Or, open the Secure Hub Store on the device. The update icon appears in the store.
4. App upgrade starts automatically. (Nexus devices prompt users to install the update.)
5. Open the app on the home screen. The app is upgraded. Users are not prompted for a grace period. (Samsung devices do a silent install.)

### **Uninstall an app when the app is configured as required**

You can allow users to uninstall an app that is configured as required. Go to **Configure > Delivery Groups** and move the app from **Required Apps** to **Optional Apps**.

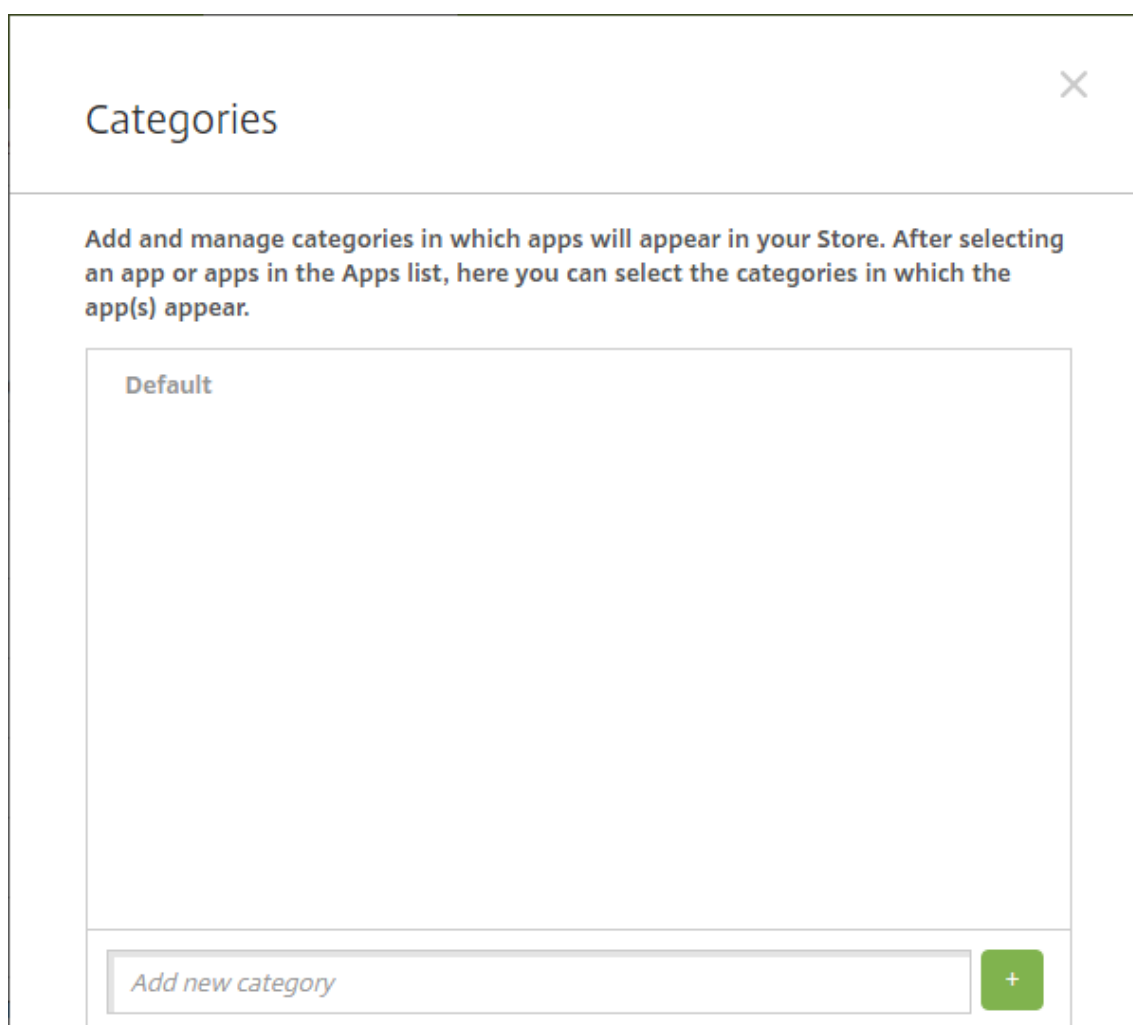
**Recommended:** Use a special delivery group to temporarily change an app to optional, so that specific users can uninstall the app. You can then change an existing required app to optional, deploy the app to that delivery group, and then uninstall the app from those devices. After that, if you want future enrollments for that delivery group to require the app, you can set the app back to required.

### About app categories

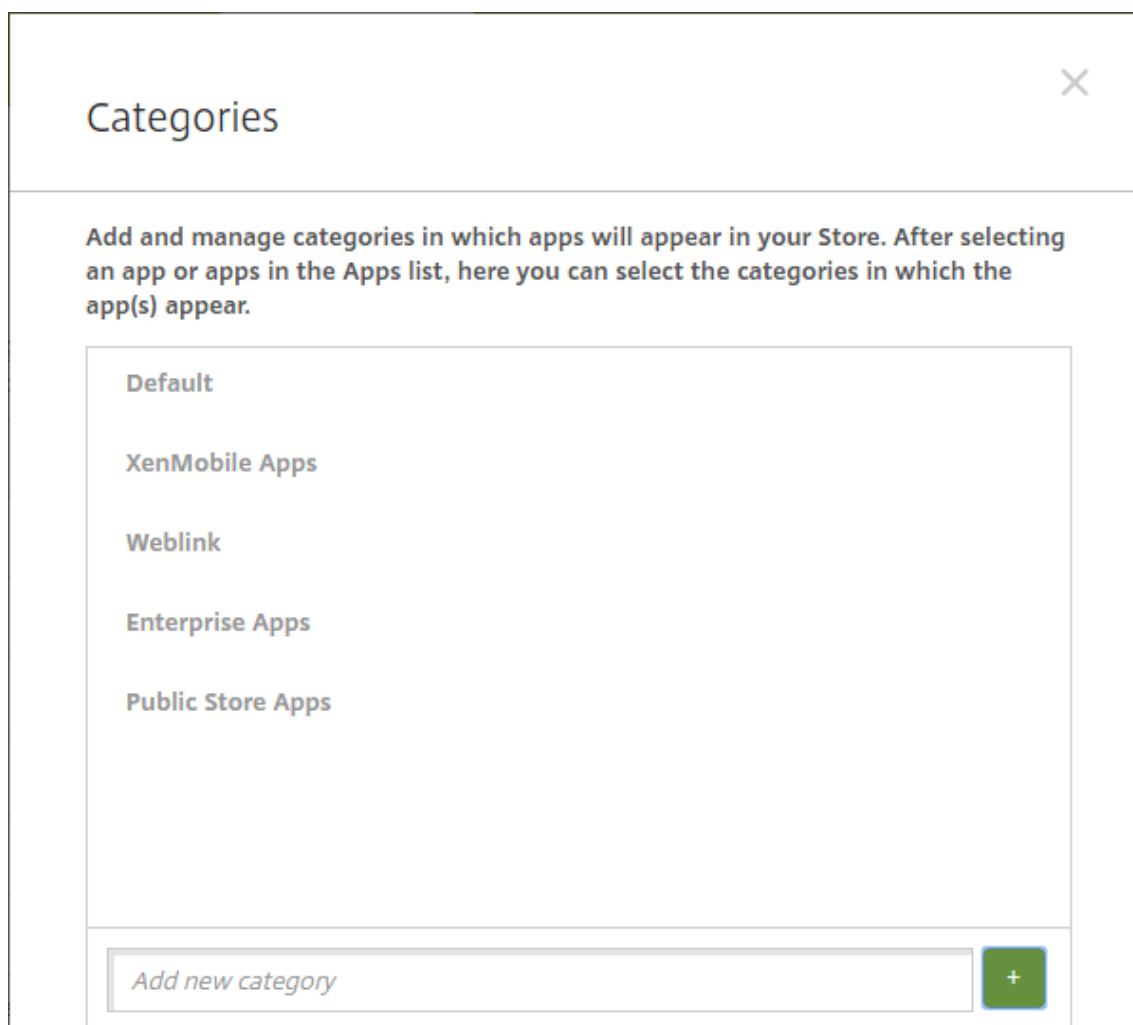
When users log on to Secure Hub, they receive a list of the apps, web links, and stores that you set up in Endpoint Management. You can use app categories to let users access only certain apps, stores, or web links. For example, you can create a Finance category and then add apps to the category that only pertain to finance. Or, you can configure a Sales category to which you assign sales apps.

When you add or edit an app, web link, or store, you can add the app to one or more of the configured categories.

1. In the Endpoint Management console, click **Configure > Apps > Category**. The **Categories** dialog box appears.



2. For each category you want to add, do the following:
  - Type the name of the category you want to add in the **Add a new category** field at the bottom of the dialog box. For example, you might type Enterprise Apps to create a category for enterprise apps.
  - Click the plus sign (+) to add the category. The newly created category is added and appears in the **Categories** dialog box.



3. When you're done adding categories, close the **Categories** dialog box.
4. On the **Apps** page, you can place an existing app into a new category.
  - Select the app you want to categorize.
  - Click **Edit**. The **App Information** page appears.
  - In the **App category** list, apply the new category by selecting the category check box. Clear the check boxes for any existing categories that you don't want to apply to the app.
  - Click the **Delivery Groups Assignments** tab or click **Next** on each of the following pages to step through the remaining app set-up pages.



- Click **Save** on the **Delivery Groups Assignments** page to apply the new category. The new category is applied to the app and appears in the **Apps** table.

## Add an MDX app

When you receive an MDX file for an iOS or Android app, you can upload the app to Endpoint Management. After you upload the app, you can configure app details and policy settings. For information about the app policies that are available for each device platform type, see:

- [MAM SDK overview](#)
- [MDX Policies at a Glance](#)

1. For Citrix mobile productivity apps, download the public-store MDX files: Go to <https://www.citrix.com/downloads>. Navigate to **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.
2. For other types of MDX apps, obtain the MDX file.
3. In the Endpoint Management console, click **Configure > Apps > Add**. The **Add App** dialog box appears.

**Add App** [Close]

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

<b>MDX</b> Apps wrapped with the <a href="#">MDX Service</a> to include app policies. You can deploy MDX apps obtained from internal and public stores. Example: Secure Mail	<b>Public App Store</b> Free or paid apps available in a public app store, such as iTunes or Google Play, for download. Example: GoToMeeting
<b>Web &amp; SaaS</b> Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps. Example: GoogleApps_SAML	<b>Enterprise</b> Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps. Example: Quick-iLaunch
<b>Web Link</b> A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.	

4. Click **MDX**. The **MDX App Information** page appears.
5. On the **App Information** pane, type the following information:
  - **Name:** Type a descriptive name for the app. The name appears under **App Name** on the **Apps** table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see [About app categories](#).

6. Click **Next**. The **App Platforms** page appears.
7. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.
8. To select an MDX file to upload, click **Upload** and navigate to the file location.
9. In the **App details** page, configure these settings:
  - **File name:** Type the file name associated with the app.
  - **App Description:** Type a description for the app.
  - **App version:** Optionally, type the app version number.
  - **Package ID:** Type the package ID for the app, obtained from the managed Google Play Store.
  - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
  - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
  - **Excluded devices:** Optionally, type the manufacturer or models of devices that cannot run the app.
  - **Remove app if MDM profile is removed:** Select whether to remove the app from an iOS device when the MDM profile is removed. The default is **On**.
  - **Prevent app data backup:** Select whether to prevent users from backing up app data on iOS devices. The default is **On**.
  - **Product track:** Specify which product track you want to push to iOS devices. If you have a track designed for testing, you can select and assign it to your users. The default is **Production**.
  - **Force app to be managed:** For an app that installs as unmanaged, select whether to prompt users to allow the app to be managed on unsupervised iOS devices. The default is **On**.
  - **App deployed via volume purchase:** Select whether to deploy the app by using Apple volume purchase. If **On**, and you deploy an MDX version of the app and use volume purchase to deploy the app, Secure Hub shows only the volume purchase instance. Default is **Off**.
10. Configure the **MDX Policies**. MDX policies vary by platform and include options for policy areas, including authentication, device security, and app restrictions. In the console, each of the policies has a tooltip that describes the policy.
11. Configure the deployment rules. For information, see [Configure deployment rules](#).
12. Expand **Store Configuration**.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Choose File

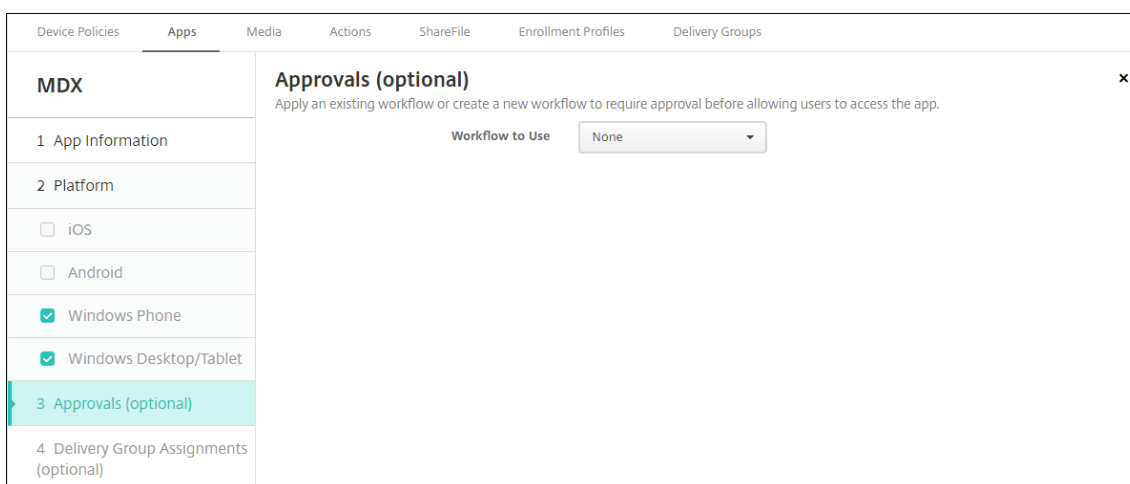
Allow app ratings

Allow app comments

Optionally, you can configure the following:

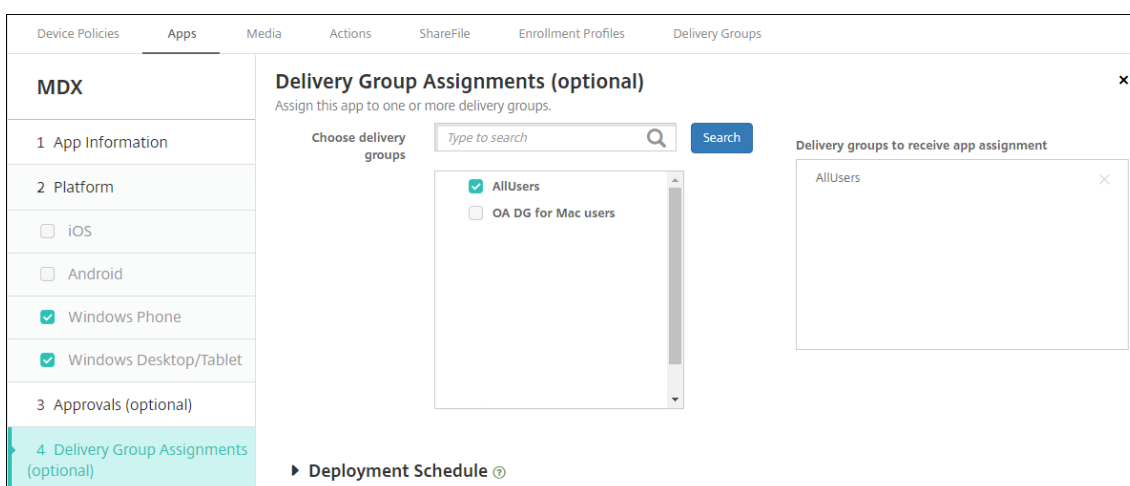
- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

13. Click **Next**. The **Approvals** page appears.



To use workflows to require approval before allowing users to access the app, see [Apply workflows](#). If you don't want to set up approval workflows, continue with the next step.

14. Click **Next**. The **Delivery Group Assignment** page appears.



15. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.

16. Expand **Deployment Schedule** and then configure the following settings:

- **Deploy:** Choose whether to deploy the app to devices. The default is **On**.
- **Deployment schedule:** Choose whether to deploy the app **Now** or **Later**. If you select **Later**, configure a date and time to deploy the app. The default is **Now**.
- **Deployment condition:** Choose **On every connection** to deploy the app every time the device connects. Choose **Only when previous deployment has failed** to deploy the app when the device failed to receive the app previously. The default is **On every connection**.

The **Deploy for always-on connection** option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.

The always-on option:

- Is not available for iOS devices
- Is not available for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management with version 10.18.19 or later
- Is not recommended for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management before version 10.18.19

The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

17. Click **Save**.

### **Add a public app store app**

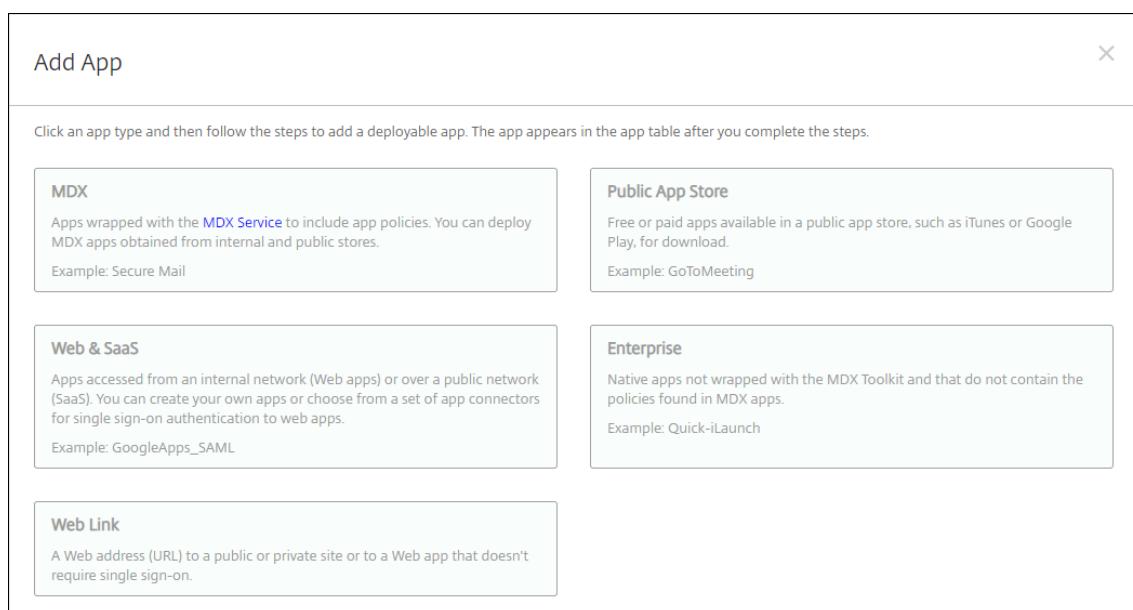
You can add free or paid apps to Endpoint Management that are available in a public app store, such as the Apple App Store or Google Play.

You can configure settings to retrieve app names and descriptions from the Apple App Store. When you retrieve the app information from the store, Endpoint Management overwrites the existing name and description. Manually configure Google Play store app information.

When you add a paid public app store app for Android Enterprise, you can review the Bulk Purchase licensing status. That status is the total number of licenses available, the number currently in use, and the email address of each user consuming the licenses. The Bulk Purchase plan for Android Enterprise simplifies the process of finding, buying, and distributing apps and other data in bulk.

Configure app information and choose platforms to deliver the app to:

1. In the Endpoint Management console, click **Configure > Apps > Add**. The **Add App** dialog box appears.



2. Click **Public App Store**. The **App Information** page appears.
3. On the **App Information** pane, type the following information:
  - **Name:** Type a descriptive name for the app. This name appears under **App Name** on the **Apps** table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see About app categories.
4. Click **Next**. The **App Platforms** page appears.
5. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.

Next you configure the app settings for each platform. See:

- Configure app settings for Google Play apps
- [Managed app store apps](#)
- Configure app settings for iOS apps

When you finish configuring the settings for a platform, set the platform deployment rules and app store configuration.

1. Configure the deployment rules. For information, see [Configure deployment rules](#).
2. Expand **Store Configuration**.

The screenshot shows the 'Store Configuration' interface for an app. It features a dropdown menu for 'App FAQ' with a button to 'Add a new FAQ question and answer'. Below this is the 'App screenshots' section, which contains five dashed boxes for uploading screenshots, each with a 'Choose File' button. At the bottom, there are two toggle switches: 'Allow app ratings' and 'Allow app comments', both of which are currently turned 'ON'.

Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

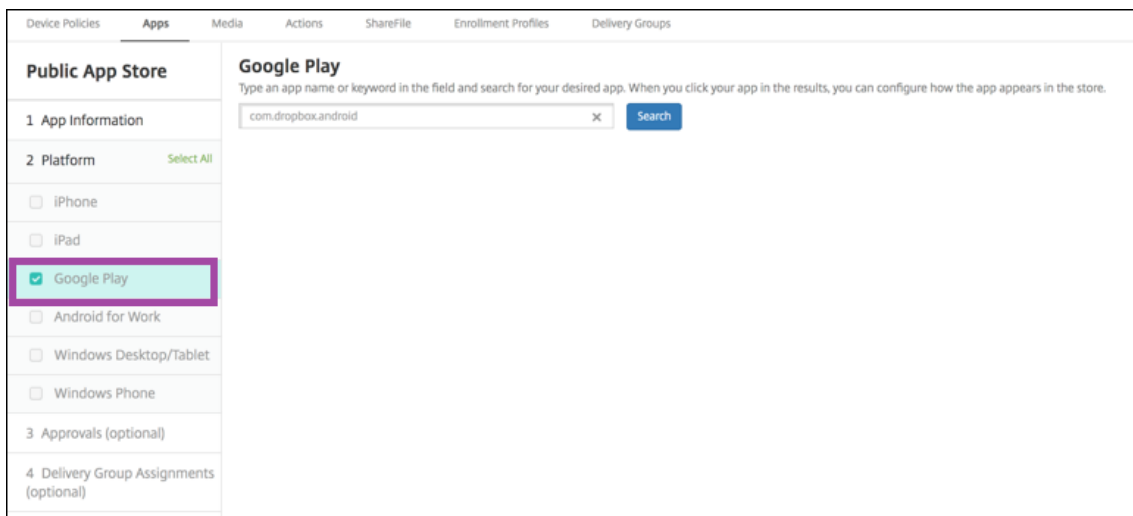
### Configure app settings for Google Play apps

#### Note:

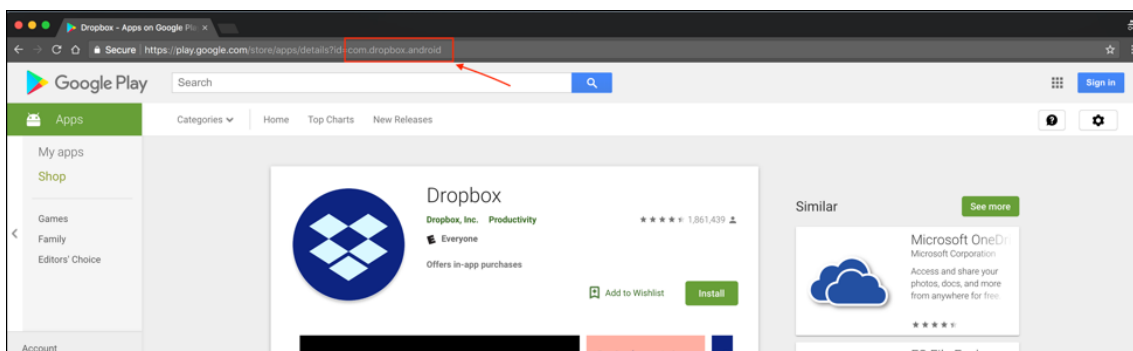
To make all apps in the Google Play store accessible from managed Google Play, use the **Access all apps in the managed Google Play store** server property. (See [Server properties](#).) Setting this property to **true** allows all Android Enterprise and Android for Workspace users to access public Google Play store apps. You can then use the [Restrictions device policy](#) to control access to these apps.

Configuring settings for Google Play store apps requires different steps than apps for other platforms. Manually configure Google Play store app information.

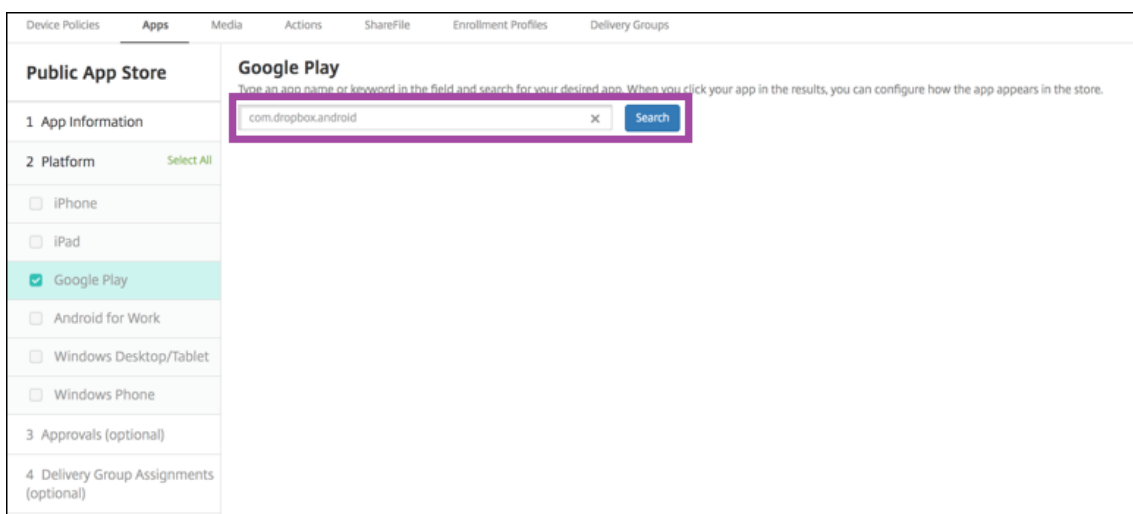
1. Ensure that **Google Play** is selected under **Platforms**.



2. Go to the Google Play store. From the Google Play store, copy the package ID. The ID can be found in the URL of the app.

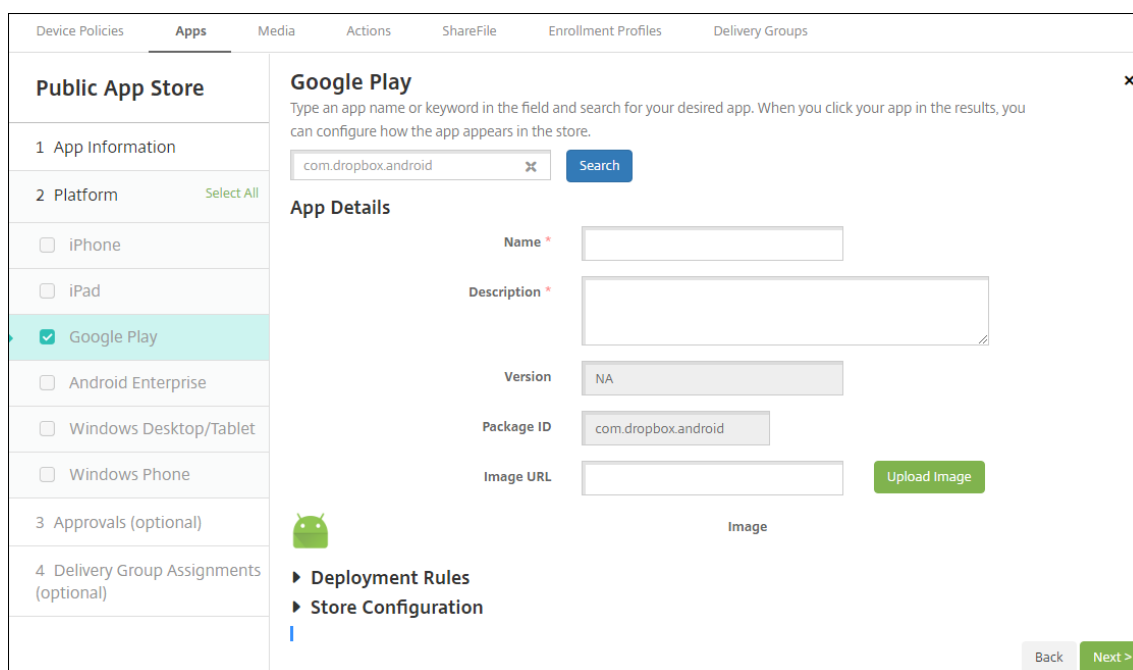


3. When adding a Public Store app in the Citrix Endpoint Management console, paste the package ID in the search bar. Click **Search**.



4. If the package ID is valid, a UI appears allowing you to enter app details.





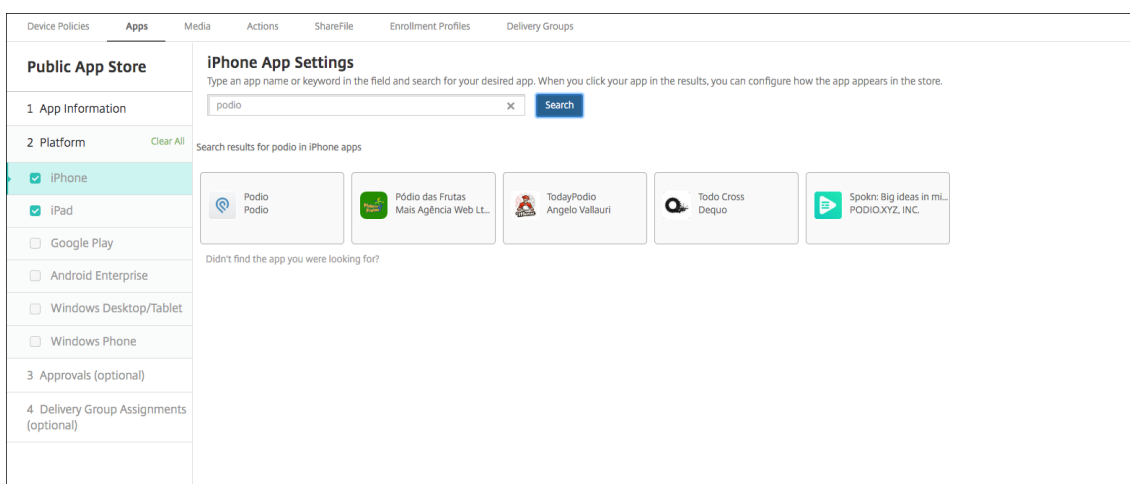
5. You can configure the URL for the image to appear with the app in the store. To use the image from the Google Play store:
  - a) Go the Google Play store. Right-click the app image and copy the image address.
  - b) Paste the image address into the **Image URL** field.
  - c) Click **Upload image**. The image appears beside **Image**.

If you don't configure an image, the generic Android image appears with the app.

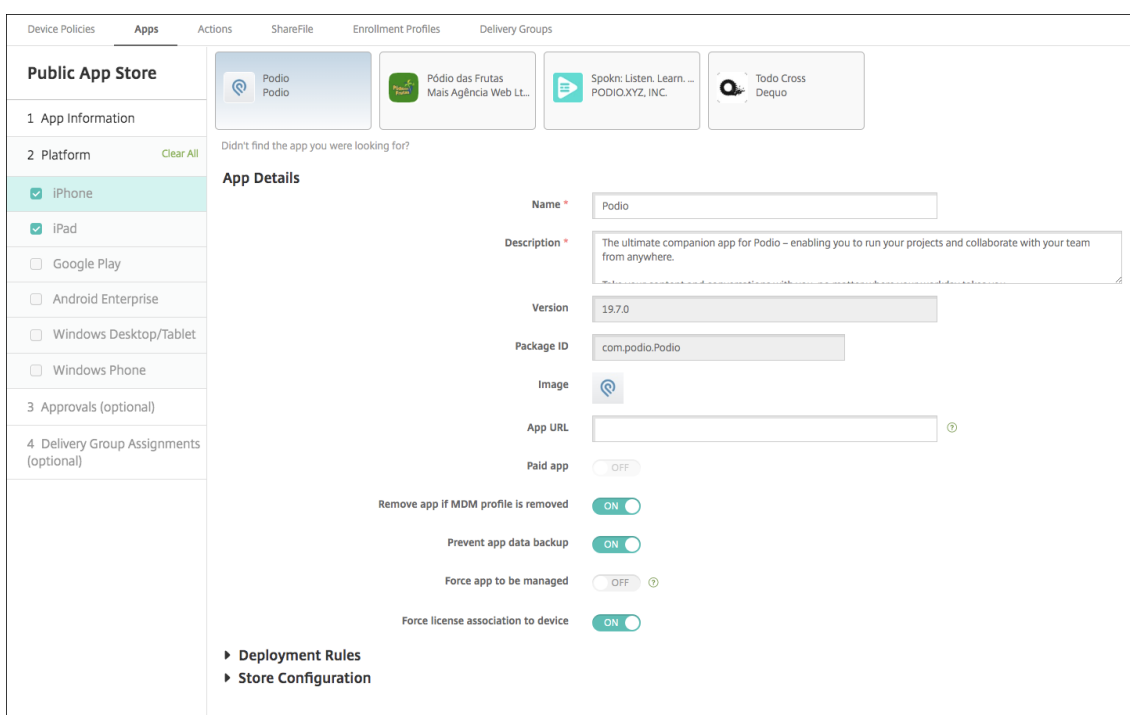
### Configure app settings for iOS apps

1. Type the app name in the search box and click **Search**. Apps matching the search criteria appear. Apps matching the search criteria appear.

The following figure shows the result of searching for **podio** in apps on an iPhone.



2. Click the app you want to add.
3. The **App Details** fields pre-populate with information related to the chosen app (including the name, description, version number, and associated image).



4. Configure the settings:
  - If necessary, change the name and description for the app.
  - **App URL:** Enter a comma-separated list of URLs to launch your apps from the Workspace app. This field is only available for iPhone and iPad devices.
  - **Paid app:** This field is preconfigured and cannot be changed.
  - **Remove app if MDM profile is removed:** Select whether to remove the app if the MDM profile is removed. The default is **On**.

- **Prevent app data backup:** Select whether to prevent the app from backing up data. The default is **On**.
  - **Product track:** Specify which product track you want to push to user devices. If you have a track designed for testing, you can select and assign it to your users. The default is **Production**.
  - **Force app to be managed:** For an app that installs as unmanaged, select whether to prompt users to allow the app to be managed on unsupervised iOS devices. The default is **Off**. For iOS devices enrolled through user enrollment, Endpoint Management doesn't enforce this setting and doesn't prompt users to allow app management.
  - **Force license to association to device:** Select whether to associate an app (developed with device association enabled) to a device rather than to a user. If the app you chose does not support assignment to a device, you can't change this setting.
5. Configure the deployment rules. For information, see [Configure deployment rules](#).
  6. Expand **Store Configuration**.

The screenshot shows the 'Store Configuration' section of the Citrix Endpoint Management console. It features a dropdown arrow next to the title. Below the title, there is an 'App FAQ' section with a button to 'Add a new FAQ question and answer'. The 'App screenshots' section contains five placeholder boxes, each with a 'Choose File' button. At the bottom, there are two toggle switches: 'Allow app ratings' and 'Allow app comments', both of which are currently turned 'ON'.

Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.

- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

7. For iPhone or iPad, expand **Volume Purchase**.

a) To enable Endpoint Management to apply a volume purchase license for the app: In the **Volume purchase license** list, click **Upload a volume purchase license**.

b) In the dialog box that appears, import the license.

The License Assignment table shows the number of licenses in use for the app, out of the total licenses available.

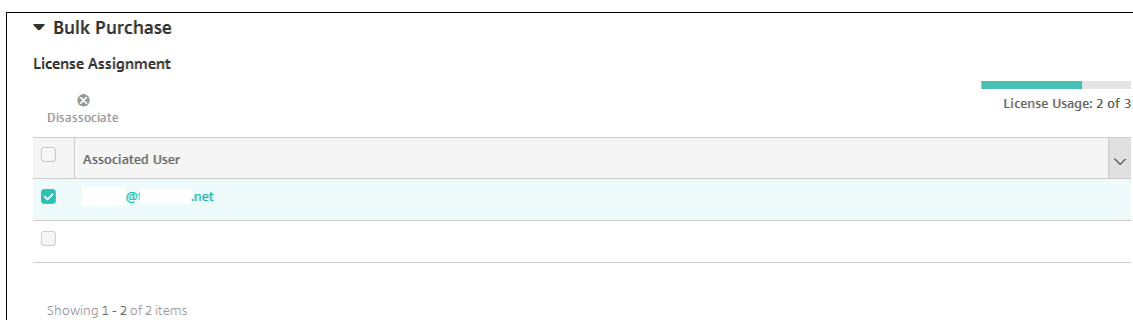
You can disassociate Volume Purchase licenses for an individual user. Doing so ends the license assignments and frees licenses.

c) When you add your volume purchase account, enable **App Auto Update**. This setting ensures that apps on user devices automatically update when an update appears in the Apple store. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens regardless of whether the app is required or optional.

8. For Android Enterprise, expand the **Bulk Purchase** section.

The License Assignment table shows the number of licenses in use for the app, out of the total licenses available.

You can select a user and then click **Disassociate** to end their license assignment and free a license for another user. You can only disassociate the license, however, if the user is not part of a delivery group that contains the specific app.



9. After you complete the **Volume Purchase** or **Bulk Purchase** settings, click **Next**. The **Approvals** page appears.

To use workflows to require approval before allowing users to access the app, see Apply workflows. If you don't need approval workflows, continue with the next step.

10. Click **Next**. The **Delivery Group Assignment** page appears.

11. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.
12. Expand **Deployment Schedule** and then configure the following settings:

- **Deploy:** Choose whether to deploy the app to devices. The default is **On**.
- **Deployment schedule:** Choose whether to deploy the app **Now** or **Later**. If you select **Later**, configure a date and time to deploy the app. The default is **Now**.
- **Deployment condition:** Choose **On every connection** to deploy the app every time the device connects. Choose **Only when previous deployment has failed** to deploy the app when the device failed to receive the app previously. The default is **On every connection**.

The **Deploy for always-on connection** option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.

The always-on option:

- Is not available for iOS devices
- Is not available for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management with version 10.18.19 or later
- Is not recommended for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management before version 10.18.19

The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

13. Click **Save**.

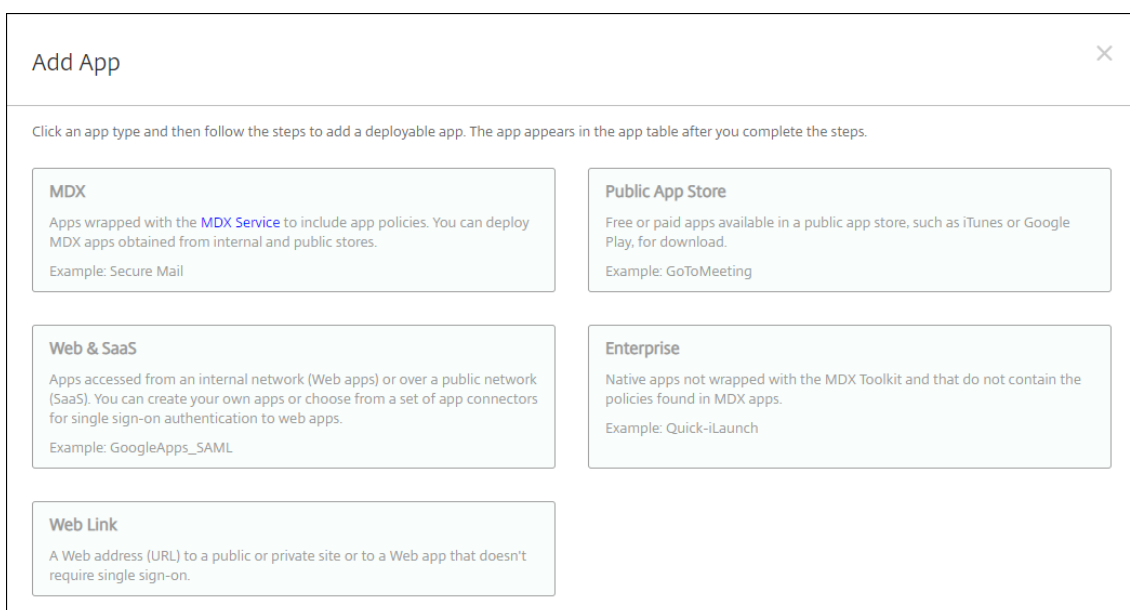
## Add a Web or SaaS app

Using the Endpoint Management console, you can give users single sign-on (SSO) authorization to your mobile, enterprise, web, and SaaS apps. If Endpoint Management is Workspace-enabled, see [Configure mobile SSO \(preview\)](#), in this article. If Endpoint Management isn't Workspace-enabled, you can enable apps for SSO by using application connector templates.

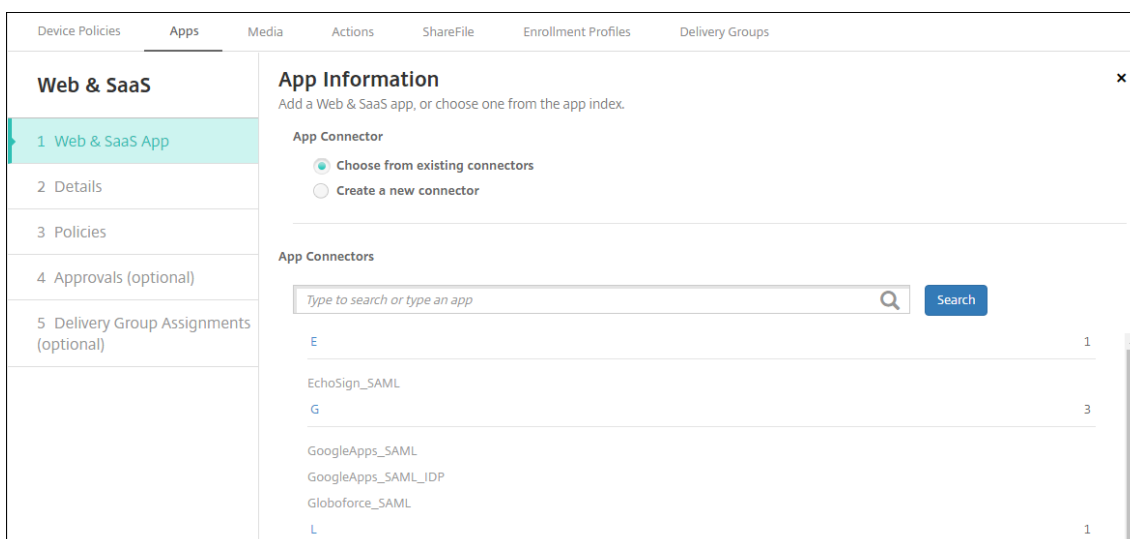
For a list of connector types available in Endpoint Management, see [Application connector types](#). You can also you build your own connector in Endpoint Management when you add a Web or SaaS app.

If an app is available for SSO only: After you save the settings, the app appears on the **Apps** tab in the Endpoint Management console.

1. In the Endpoint Management console, click **Configure > Apps > Add**. The **Add App** dialog box appears.



2. Click **Web & SaaS**. The **App Information** page appears.



3. Configure an existing or new app connector, as follows.

### To configure an existing app connector

1. In the **App Information** page, **Choose from existing connectors** is already selected, as shown previously. Click the connector you want to use in the **App Connectors** list. The app connector information appears.
2. Configure these settings:
  - **App name:** Accept the pre-filled name or type a new name.
  - **App description:** Accept the pre-filled description or type one of your own.

- **URL:** Accept the pre-filled URL or type the web address for the app. Depending on the connector you choose, this field can contain a placeholder that you must replace before you can move to the next page.
- **Domain name:** If applicable, type the domain name of the app. This field is required.
- **App is hosted in internal network:** Select whether the app is running on a server in your internal network. If users connect from a remote location to the internal app, they must connect through Citrix Gateway. Setting this option to **On** adds the VPN keyword to the app and allows users to connect through Citrix Gateway. The default is **Off**.
- **App category:** In the list, click an optional category to apply to the app.
- **User account provisioning:** Select whether to create user accounts for the app. If you use the Globoforce\_SAML connector, you must enable this option to ensure seamless SSO integration.
- If you enable **User account provisioning**, configure these settings:
  - **Service Account**
    - \* **User name:** Type the name of the app administrator. This field is required.
    - \* **Password:** Type the app administrator password. This field is required.
  - **User Account**
    - \* **When user entitlement ends:** In the list, click the action to take when users are no longer allowed access to the app. The default is **Disable account**.
  - **User Name Rule**
    - \* For each user name rule you want to add, do the following:
      - **User attributes:** In the list, click the user attribute to add to the rule.
      - **Length (characters):** In the list, click the number of characters from the user attribute to use in the user name rule. The default is **All**.
      - **Rule:** Each user attribute you add is automatically appended to the user name rule.
- **Password Requirement**
  - **Length:** Type the minimum user password length. The default is **8**.
- **Password Expiration**
  - **Validity (days):** Type the number of days the password is valid. Valid values are **0–90**. The default is 90.
  - **Automatically reset password after it expires:** Select whether to reset the password automatically when it expires. The default is **Off**. If you don't enable this field, users can't open the app after their passwords expire.

### To configure a new app connector

1. In the **App Information** page, select **Create a new connector**. The app connector fields appear.

The screenshot shows the 'App Information' form in the Citrix Endpoint Management console. The form is titled 'App Information' and includes a sub-header 'Add a Web & SaaS app, or choose one from the app index.' The form is divided into two main sections: a left-hand navigation pane and a main configuration area. The navigation pane is titled 'Web & SaaS' and contains five items: '1 Web & SaaS App' (selected), '2 Details', '3 Policies', '4 Approvals (optional)', and '5 Delivery Group Assignments (optional)'. The main configuration area contains the following fields and options:

- App Connector:** Radio buttons for 'Choose from existing connectors' and 'Create a new connector' (selected).
- Name\*:** A required text input field.
- Description\*:** A required text input field.
- Logon URL\*:** A required text input field.
- SAML version:** Radio buttons for '1.1' (selected) and '2.0'.
- Entity ID\*:** A required text input field.
- Relay state URL:** A text input field.
- Name ID format:** Radio buttons for 'Email Address' (selected) and 'Unspecified'.
- ACS URL\*:** A required text input field.
- Image:** Radio buttons for 'Use default' (selected) and 'Upload your own app image'.

An 'Add' button is located at the bottom of the form.

2. Configure these settings:

- **Name:** Type a name for the connector. This field is required.
- **Description:** Type a description for the connector. This field is required.
- **Logon URL:** Type, or copy and paste, the URL where users log on to the site. For example, if the app you want to add has a logon page, open a web browser and go to the logon page for the app. For example, it might be <https://www.example.com/logon>. This field is required.
- **SAML version:** Select either **1.1** or **2.0**. The default is **1.1**.
- **Entity ID:** Type the identity for the SAML app.
- **Relay state URL:** Type the web address for the SAML application. The relay state URL is the response URL from the app.
- **Name ID format:** Select either **Email Address** or **Unspecified**. The default is **Email Address**.
- **ACS URL:** Type the Assertion Consumer Service URL of the identity provider or service provider. The ACS URL gives users SSO capability.
- **Image:** Select whether to use the default Citrix image or to upload your own app image. The default is Use default.
  - To upload your own image, click **Browse** and navigate to the file location. The file must be a .PNG file. You can't upload a JPEG or GIF file. When you add a custom graphic, you can't change it later.

3. When you're finished, click **Add**. The **Details** page appears.



4. Click **Next**. The **App Policy** page appears.

The screenshot shows the 'App Policy' configuration page. On the left is a navigation pane with a sidebar titled 'Web & SaaS' containing five items: '1 Web & SaaS App', '2 Details', '3 Policies' (highlighted in teal), '4 Approvals (optional)', and '5 Delivery Group Assignments (optional)'. The main content area is titled 'App Policy' with a subtitle 'Fill in app information'. It features three sections: 'Device Security' with a toggle for 'Block jailbroken or rooted' set to 'ON'; 'Network Requirements' with toggles for 'WiFi required' and 'Internal network required' both set to 'OFF', and an empty text input field for 'Internal WiFi networks'. At the bottom, there is a section for 'Store Configuration' and two buttons: 'Back' and 'Next >'.

5. Configure these settings:

- **Device Security**
- **Block jailbroken or rooted:** Select whether to block jailbroken or rooted devices from accessing the app. The default is **On**.
- **Network Requirements**
- **WiFi required:** Select whether a Wi-Fi connection is required to run the app. The default is **Off**.
- **Internal network required:** Select whether an internal network is required to run the app. The default is **Off**.
- **Internal WiFi networks:** If you enabled **Wi-Fi required**, type the internal Wi-Fi networks to use.

6. Expand **Store Configuration**.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Choose File

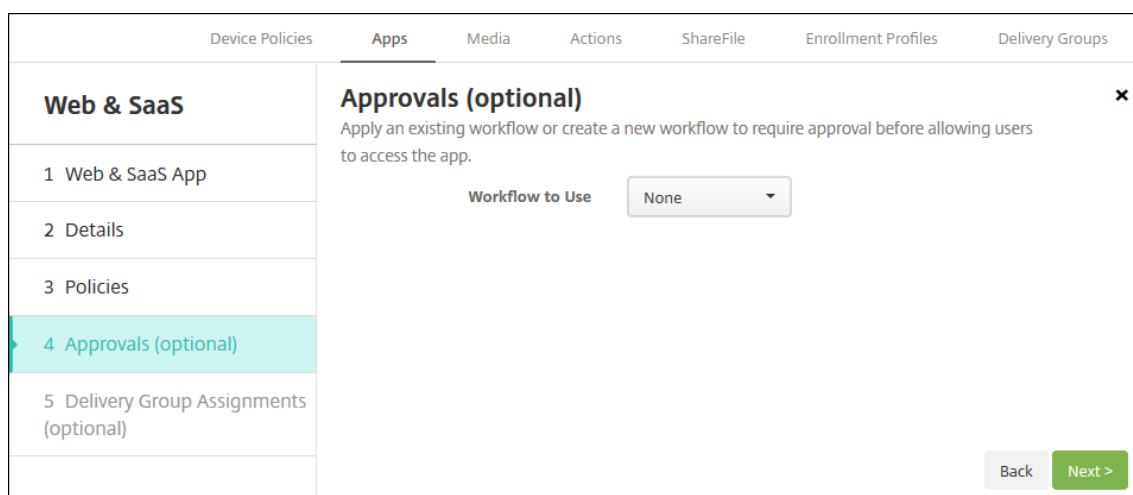
Allow app ratings

Allow app comments

Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

7. Click **Next**. The **Approvals** page appears.



To use workflows to require approval before allowing users to access the app, see [Apply workflows](#). If you don't need approval workflows, continue with the next step.

8. Click **Next**. The **Delivery Group Assignment** page appears.
9. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups. The groups you select appear in the **Delivery groups to receive app assignment** list.
10. Expand **Deployment Schedule** and then configure the following settings:
  - **Deploy:** Choose whether to deploy the app to devices. The default is **On**.
  - **Deployment schedule:** Choose whether to deploy the app **Now** or **Later**. If you select **Later**, configure a date and time to deploy the app. The default is **Now**.
  - **Deployment condition:** Choose **On every connection** to deploy the app every time the device connects. Choose **Only when previous deployment has failed** to deploy the app when the device failed to receive the app previously. The default is **On every connection**.

The **Deploy for always-on connection** option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.

The always-on option:

- Is not available for iOS devices
- Is not available for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management with version 10.18.19 or later
- Is not recommended for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management before version 10.18.19

The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

11. Click **Save**.

## Configure mobile SSO (preview)

Endpoint Management integration with Citrix Workspace supports mobile SSO to native SaaS apps from iOS and Android devices enrolled in MDM.

This section describes how to configure Endpoint Management and Citrix Gateway to deliver native SaaS apps. With that configuration, the Citrix Workspace app provides single sign-on across apps.

Prerequisites:

- Citrix Workspace Premium license
- Your identity provider configured in Citrix Cloud
- The following services configured:
  - Workspace service with Endpoint Management enabled. For information about enabling service integration, see [Workspace configuration](#).
  - Citrix Endpoint Management service
  - Citrix Gateway service
- Citrix Workspace app for iOS
- Citrix Workspace app for Android
- Single sign-on requires that your users manually turn on VPN on Android devices.

The general setup steps described in this section are:

1. Add a native SaaS app.
2. Add device policies.
3. Use Citrix Gateway to configure and publish a native SaaS app.

### Add a native SaaS app

To add a native SaaS app to Endpoint Management:

1. In the Endpoint Management console, click **Configure > Add > Public App Store**.
2. Provide the **App Information** and then click **Next**.
3. Complete the **Platform** pages for the iOS and Android devices you want to support. For help, see the sections under Add a public store app. You also need the package IDs that you copy during this setup when you configure the App attributes device policy for iOS, as described later in this section.
4. Click **Next**.
5. On the **Delivery Group Assignment** page, choose delivery groups and then click **Save**.

### Add device policies for iOS

The following device policies are required to support single sign-on to native SSO apps. Be sure to assign each policy to at least one delivery group.

- **App Inventory device policy for iOS:** For help, see [App inventory device policy](#).
- **VPN device policy for iOS:** For help, see the VPN device policy section, [iOS settings](#).

Configure the VPN device policy as follows:

- **Connection name:** Name for the connection.
  - **Connection type:** Select **Citrix SSO**.
  - **Server name or IP address:** Type **vpn.netscalergateway.net**.
  - **User account:** No value required.
  - **Authentication type for the connection:** No value required.
  - **Authentication password:** No value required.
  - **Enable per-app VPN:** Set to **On**.
  - **On-demand match app enabled:** Set to **On**.
  - **Provider type:** Select **Packet tunnel**.
  - **Safari domains:** Domains to trigger a per-app VPN connection. Some apps open in Web-View and therefore the traffic isn't tunneled. To enable the traffic to pass through the VPN, you must provide a Safari domain. Type **app.netscalergateway.net**.
  - **Custom parameters:** Set the **PerAppSplitTunnel** parameter to **1**.
- **App attributes device policy for iOS:** Configuring an App attributes device policy for iOS associates an added native SaaS app with the VPN. For help, see [App attributes device policy](#).

Configure the App attributes device policy as follows:

- On the **App Attributes Policy** page, select **Add new**. A blank field appears. Provide the package ID that you noted when adding the app to Endpoint Management.
- Select the newly created VPN from the **Per-app VPN identifier** menu. You provide the package ID and associate it with a VPN so that Endpoint Management uses the associated VPN for requests for that app.

### Add a VPN device policy for Android

Configure a VPN device policy with the following settings. Be sure to assign the policy to at least one delivery group.

- **Connection name:** Name for the connection.
- **Server name or IP address:** Type **vpn.netscalergateway.net**.
- **Connection type:** Select **Citrix SSO**.
- **Authentication type for the connection:** Default is **Password**. If you don't provide the VPN credentials, the Citrix VPN app prompts device users for a user name and password.
- **Enable per-app VPN:** Set to **On**.

- **On-demand match app enabled:** Set to **On**. Then, select **Allow list** or **Block list** depending on whether you want to list package names to allow or block.
- **App Package Name:** Click **Add** and then type a comma-separated list of app package names.

**Important:**

For applications that open a Chrome browser for accessing an identity provider URL, add `com.android.chrome` as an allowed application package. Otherwise, the application launch fails. You can also add other browser package names configured as the default browser for the system.

### Use Citrix Gateway to configure and publish a native SaaS app

After you complete the Endpoint Management setup, you then configure and publish the app with Citrix Gateway. For steps to configure and publish a SaaS app using Citrix Gateway, see [Support for Software as a Service apps](#).

When configuring and publishing a SaaS app in Citrix Gateway:

- Under the **Enhanced security** section, disable the **Enforce policy on mobile device** option.
- Use the same user assignment to publish a SaaS app that you assigned to the VPN device policy in Endpoint Management.

### Add an enterprise app

Enterprise apps in Endpoint Management are private apps you develop or obtain from another source. Except for private Android Enterprise and Android for Workspace apps delivered as MDX-enabled apps, enterprise apps aren't prepared with the MAM SDK or MDX Toolkit. You can upload an enterprise app on the **Apps** tab in the Endpoint Management console. Enterprise apps support the following platforms (and corresponding file types):

- iOS (.ipa file)
- macOS (.pkg file)

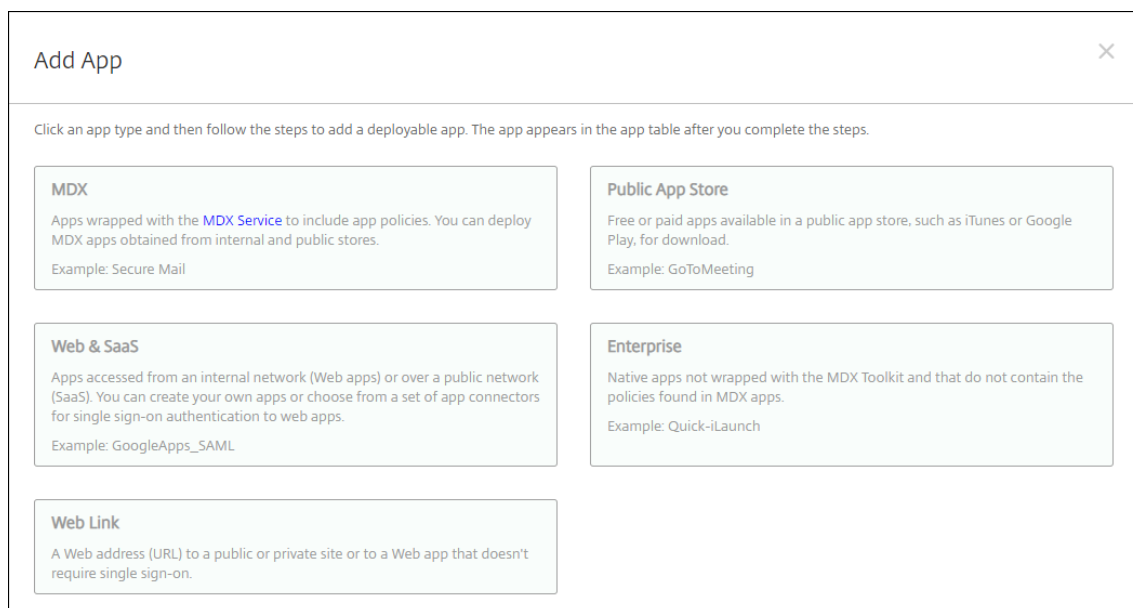
Endpoint Management does not limit the size of PKG files you upload but limits file upload times. By default, you must complete your upload within 100 s. For more information, see [Server properties](#).

- Android (.apk file)
- Samsung Knox (.apk file)
- Android Enterprise (.apk file)
- Android for Workspace (.apk file)

- See also: Add Win32 apps as Enterprise apps
- See also: [MDX-enabled private apps](#)

Adding apps downloaded from the Google Play store as enterprise apps is not supported. Add apps from the Google Play store as public app store apps instead. See Add a public app store app.

1. In the Endpoint Management console, click **Configure > Apps > Add**. The **Add App** dialog box appears.



2. Click **Enterprise**. The **App Information** page appears.
3. On the **App Information** pane, type the following information:
  - **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see About app categories.
4. Click **Next**. The **App Platforms** page appears.
5. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.
6. For each platform you chose, select the file to upload by clicking **Upload** and navigating to the file location.
7. Click **Next**. The app information page for the platform appears.
8. Configure the settings for the platform type, such as:
  - **File name:** Optionally, type a new name for the app.

- **App description:** Optionally, type a new description for the app.
  - **App version:** You can't change this field.
  - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
  - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
  - **Excluded devices:** Optionally, type the manufacturer or models of devices that cannot run the app.
  - **Package ID:** Unique identifier of your app.
  - **Remove app if MDM profile is removed:** Select whether to remove the app from a device when the MDM profile is removed. The default is **On**. This setting doesn't apply to macOS.
  - **Prevent app data backup:** Select whether to prevent the app from backing up data. The default is **On**. This setting doesn't apply to macOS.
  - **Force app to be managed:** Select whether to install an app as a managed app on unsupervised devices. The device type determines how Endpoint Management processes this setting when enabled. If you enable this setting, the app updates without prompting the user. The update happens regardless of whether the app is required or optional. The default is **Off**.
    - For iOS devices, if the app was installed already, users receive a prompt to allow the app to be managed. If you deploy an app to devices where the app doesn't exist, the app installs as a managed app regardless of the state of this setting. Available on iOS 9.0 and later. For iOS devices enrolled through user enrollment, Endpoint Management doesn't enforce this setting and doesn't prompt users to allow app management.
    - For macOS devices, enable the setting, and then deploy the app to the devices. The app automatically installs as a managed app. Users don't receive any prompts. If you deploy an app to devices where the app doesn't exist, the app installs as a managed app regardless of the state of this setting. Available on macOS 11.0 and later.
9. Configure the deployment rules. For information, see [Configure deployment rules](#).
10. Expand **Store Configuration**.



▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

Allow app comments

Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

11. Click **Next**. The **Approvals** page appears.

To use workflows to require approval before allowing users to access the app, see Apply workflows. If you don't need an approval workflow, continue to the next step.

12. Click **Next**. The **Delivery Group Assignment** page appears.

13. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.

14. Expand **Deployment Schedule** and then configure the following settings:

- **Deploy:** Choose whether to deploy the app to devices. The default is **On**.
- **Deployment schedule:** Choose whether to deploy the app **Now** or **Later**. If you select **Later**, configure a date and time to deploy the app. The default is **Now**.

- **Deployment condition:** Choose **On every connection** to deploy the app every time the device connects. Choose **Only when previous deployment has failed** to deploy the app when the device failed to receive the app previously. The default is **On every connection**.

The **Deploy for always-on connection** option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.

The always-on option:

- Is not available for iOS devices
- Is not available for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management with version 10.18.19 or later
- Is not recommended for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management before version 10.18.19

The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

15. Click **Save**.

### **Add Win32 apps as Enterprise apps**

You can upload MSI, APPX, AppxBundle, PS1, or EXE files for Win32 apps to Endpoint Management for deployment to managed Windows 10 and Windows 11 Desktop and Tablet devices. After you use Endpoint Management to deploy the files, the Windows device then installs the app as follows:

- If the upgraded app removes the old version during installation, then the device includes only the upgraded app.
- If the upgraded app can't remove the old version, but the new version can install, then the device includes both versions of the app. Endpoint Management no longer contains the information for the old version.
- If the upgraded app can't install when an old version exists, the new app doesn't install. In that case, first deploy the App Uninstall device policy to remove the old version. Then, deploy the new version.

### **Requirements**

- Windows 10 (version 1607 or later) or Windows 11
- Windows 10 Professional or Windows 11 Professional
- Windows 10 Enterprise or Windows 11 Enterprise
- Standalone Win 32 MSI apps installed with the /quiet option. For this deployment use case, Microsoft doesn't support MSIs containing multiple apps, nested MSIs, or interactive installation.

## Look up metadata

When you add a Win32 app to Endpoint Management, specify the metadata for the app. To look up the metadata, use the Orca application on a Windows computer and make note of the following information:

- Product code
- Product name
- Product version
- Package install type, either per user or per machine

## Add a Win32 app to Endpoint Management

1. Go to **Configure > Apps**, click **Enterprise**, and type a name for the app in the **App Information** page.
2. Clear all Platform check boxes except for **Windows Desktop/Tablet**.
3. On the **Windows Desktop/Tablet Enterprise App** page, click **Upload** and navigate to the file.
4. Configure these settings:

The screenshot shows the 'Windows Desktop/Tablet Enterprise App' configuration page. At the top, there are navigation tabs: 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main heading is 'Windows Desktop/Tablet Enterprise App' with a close button (X). Below the heading is a note: 'Use an MSI viewing tool, such as Orca, to obtain information such as product code and version. You must assign MSI apps to delivery groups as required apps.' There is an 'Upload' button and a text input field for 'Upload an .appx or .appxbundle or .msi file'. The form contains the following fields:

- App name \***: NetScaler Gateway Plug-in
- Description \***: Vpn
- App version \***: 12.0.51.24
- Minimum OS version**: (empty)
- Maximum OS version**: (empty)
- Excluded devices**: example: manufacturer or model, ...
- Product Code \***: (blurred) ⓘ

At the bottom, there is an 'Installation Context' section with a radio button selected for 'Device' and a help icon (i).

- **App name:** The name of the app, from the app metadata.
- **Description:** A description for the app.
- **App version:** The app version number, from the app metadata.
- **Minimum OS version:** Optional. The oldest operating system version that the device can run to use the app.

- **Maximum OS version:** Optional. The most recent operating system that the device must run to use the app.
  - **Excluded devices:** Optional. The manufacturer or models of devices that cannot run the app.
  - **Product Code:** The MSI app product code, in UUID format, from the app metadata.
  - **Installation Context:** Based on the app metadata, select whether the app is to install for the device or user. This setting isn't available for EXE files.
  - **Command Line:** The command-line options to use when calling MSIEXEC.exe
  - **Install Command Line:** Add command line arguments for installing EXE files silently.
  - **Uninstall Command Line:** Add command line arguments for uninstalling EXE files silently.
  - **Retry Count:** The number of times you can retry a download and installation operation before marking the installation as failed.
  - **Time Out:** The number of minutes that the installation process runs before the installer interprets the installation as failed and no longer monitors the process.
  - **Retry Interval:** The number of minutes between retry operations.
5. Configure the deployment rules. For information, see [Configure deployment rules](#).
  6. Expand **Store Configuration**.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

Allow app comments

Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

7. Click **Next** until you get to the **Summary** page and then click **Save**.
8. Go to **Configure > Delivery Groups** and add the Win32 app as a required app.
9. After you deploy the app, let your users know that the app is available.

### Upgrade a Win32 app

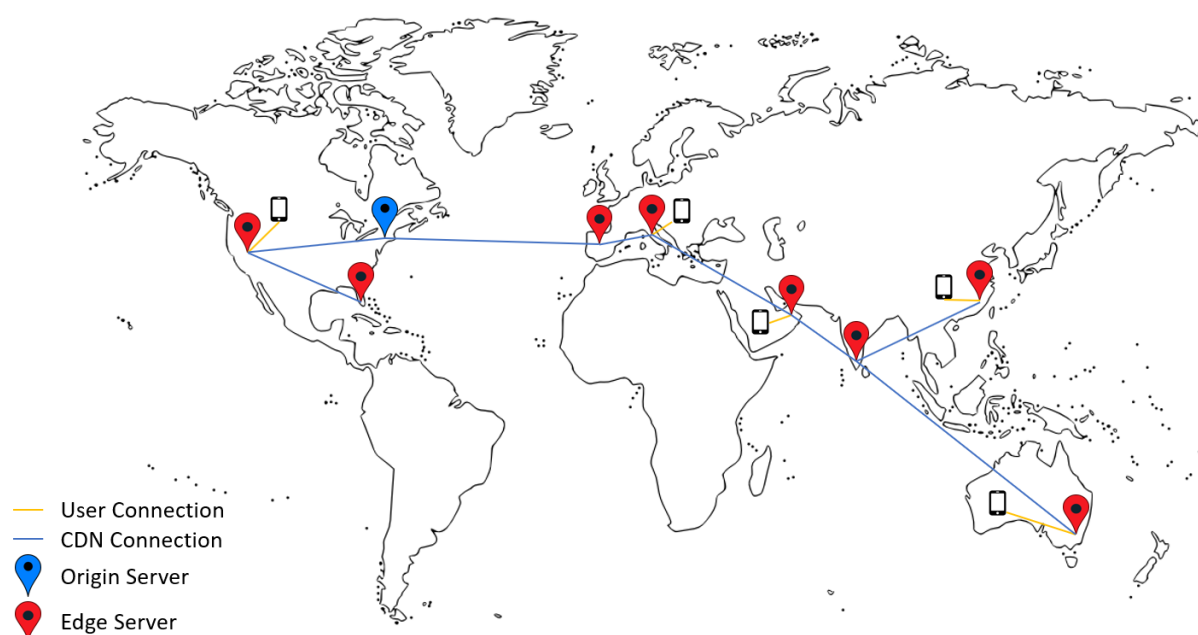
1. Look up the metadata for the app, as described earlier in “Look up metadata.”
2. Go to **Configure > Apps** to upload the new version of the app. Update the **App version**. If the new version of the app has a different **Product Code**, update that setting.
3. Submit the changes and deploy the app.

## Deliver enterprise and MDX apps from the Citrix CDN

You can deliver enterprise and MDX apps from the Citrix Content Delivery Network (CDN). A CDN refers to a geographically distributed group of servers that work together to securely provide fast delivery of application content. A local server delivers the apps to mobile devices.

A CDN improves app download times by distributing content geographically closer to the mobile devices through a nearby CDN distribution point. CDN delivers apps from the closest Point of Presence (POP) location to a user.

The following diagram shows an example of how CDN distributes apps to the Edge Server closest to mobile device users. An Edge Server caches content from the originating server when mobile devices request apps.



Users can connect to apps by using Secure Hub. When you add an app, Endpoint Management creates the app connector for it.

The Citrix CDN support for enterprise apps is available for the following platforms:

- iOS (MDM or MAM enrollment)
- Android (MDM or MAM enrollment)
- Windows desktop or tablet (MDM enrollment)
- macOS (MDM enrollment)

The Citrix CDN support for MDX apps is available for the following platforms:

- iOS (MDM or MAM enrollment)
- Android (MDM or MAM enrollment)

### How CDN works

At the core of the CDN service, servers are linked together with the goal of delivering apps faster. That goal is achieved by placing the apps securely on different distribution points worldwide. The mobile devices' DNS server used during the initial connection to the Endpoint Management server is what determines the distribution point.

For example: Suppose that the DNS server IP of the mobile device originates in Fort Lauderdale, Florida. The CDN uses a local distribution point closest to that location to deliver the app to the mobile device. That use of the CDN results in improved app download time.

When a mobile device first requests or pushes an enterprise app, Endpoint Management copies the app to the local distribution point and retains the app there for 24 hours for other local device downloads.

### Deliver enterprise apps from the Citrix CDN

As of Endpoint Management release 19.4.1, enterprise app delivery defaults to CDN delivery for all new multitenancy customers. For existing customers before this release, follow the instructions in this section.

For enterprise apps already on the Endpoint Management server, Endpoint Management continues to deliver those apps from the server until those apps get reuploaded after you complete the following steps.

#### Important:

Only Citrix Cloud administrators can enable CDN for an account. The server property `app.delivery.cdn` is visible in Endpoint Management only when you log on as a Citrix Cloud administrator. For information about Citrix Cloud administrators, see [Manage Citrix Cloud administrators](#).

1. Enable CDN for your account: In the Endpoint Management console: Go to **Settings > Server Properties**.
2. Search for `app.delivery.cdn` and then click **Edit**.
3. Change the value to **true**.

Key	app.delivery.cdn
Value *	true
Display name *	Application Delivery to enable CDN
Description	Application Delivery to enable CDN

4. In the Endpoint Management console, upload your enterprise apps again:
  - a) Go to **Configure > Apps** and filter the app list by **Type (Enterprise)** and **Platform**.
  - b) Select an app, click **Edit**, click **Next**, and click **Upload**.
  - c) Repeat the prior step for each enterprise app.

### Deliver MDX apps from the Citrix CDN

As of Endpoint Management release 20.12.0, MDX app delivery defaults to CDN delivery for all new multitenancy customers. For existing customers before this release, follow the instructions in this section.

For MDX apps already on the Endpoint Management server, Endpoint Management continues to deliver those apps from the server until those apps get reuploaded after you complete the following steps.

#### Important:

Only Citrix Cloud administrators can enable CDN for an account. The server property `app.delivery.cdn` is visible in Endpoint Management only when you log on as a Citrix Cloud administrator. For information about Citrix Cloud administrators, see [Manage Citrix Cloud administrators](#).

1. Enable CDN for your account: In the Endpoint Management console: Go to **Settings > Server Properties**.
2. Search for `app.delivery.cdn` and then click **Edit**.
3. Change the value to **true**.



<b>Key</b>	app.delivery.cdn
<b>Value *</b>	true
<b>Display name *</b>	Application Delivery to enable CDN
<b>Description</b>	Application Delivery to enable CDN

4. In the Endpoint Management console, upload your MDX apps again:
  - a) Go to **Configure > Apps** and filter the app list by **Type (MDX)** and **Platform**.
  - b) Select an app, click **Edit**, click **Next**, and click **Upload**.
  - c) Repeat the prior step for each MDX app.

### Add a Web link

A web link is a web address to an internet or intranet site. A web link can also point to a web application that doesn't require SSO. After you finish configuring a web link, the link appears as an icon in the app store. When users log on with Secure Hub, the link appears with the list of available apps and desktops.

You can configure web links from the **Apps** tab in the Endpoint Management console. When you finish configuring the web link, the link appears as a link icon in the list in the **Apps** table. When users log on with Secure Hub, the link appears with the list of available apps and desktops.

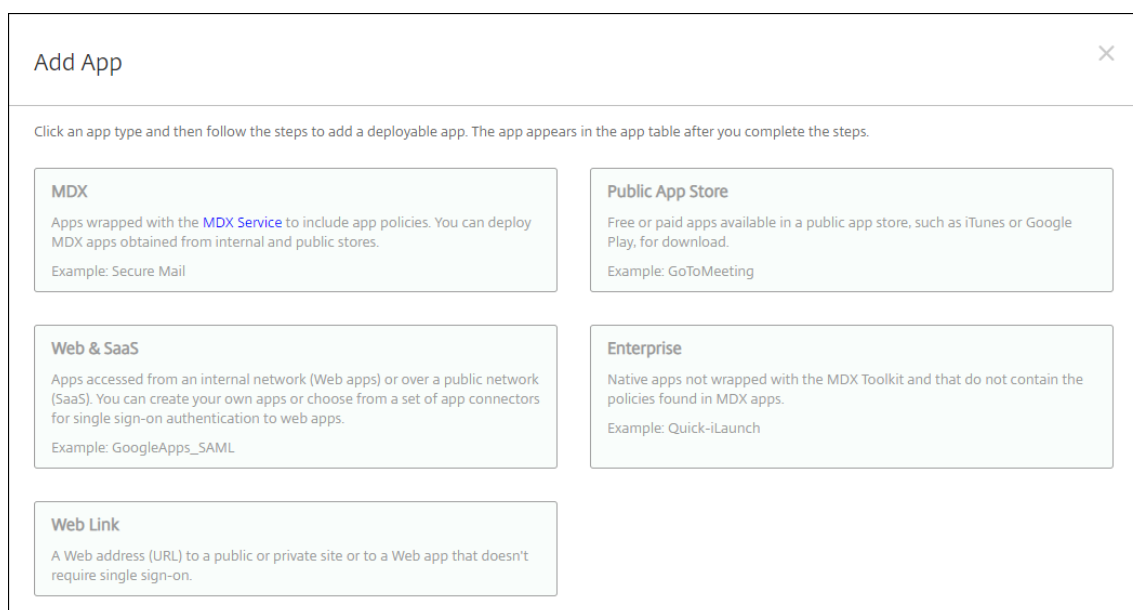
Watch this video to learn more:



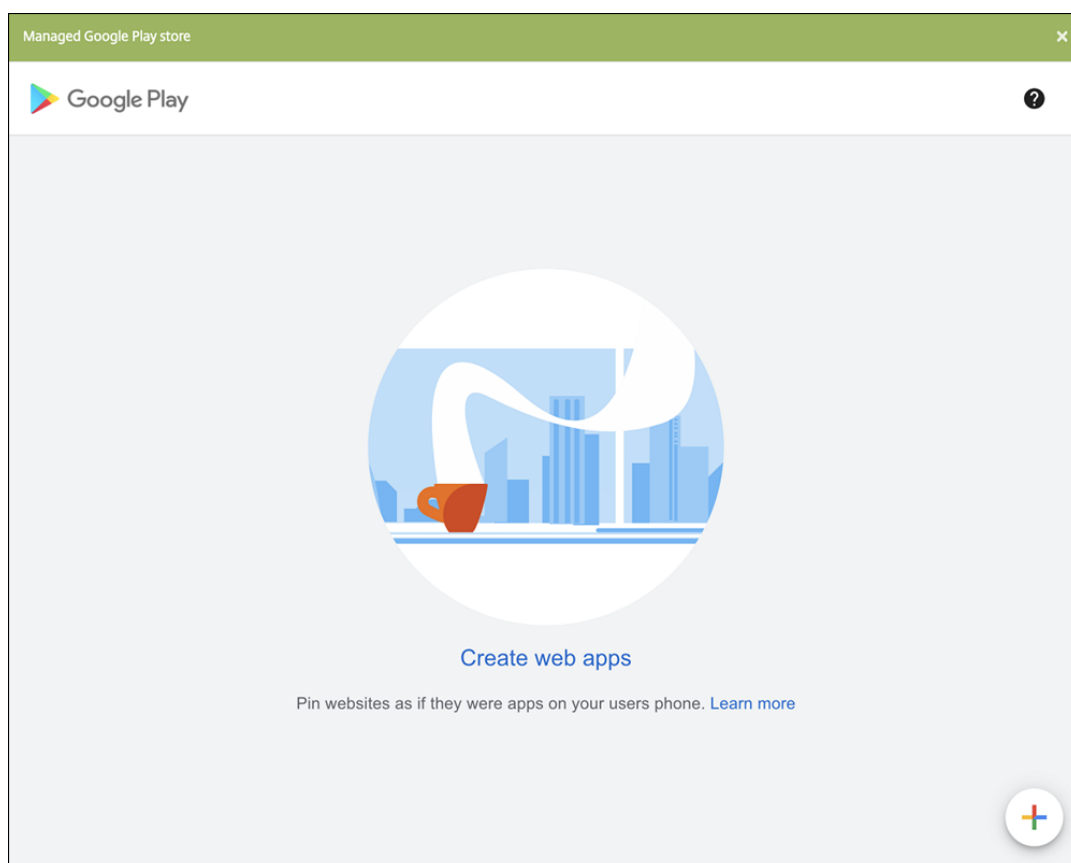
To add the link, you provide the following information:

- Name for the link
- Description of the link
- Web address (URL)
- Category
- Role
- Image in .png format (optional)

1. In the Endpoint Management console, click **Configure > Apps > Add**. The **Add App** dialog box appears.

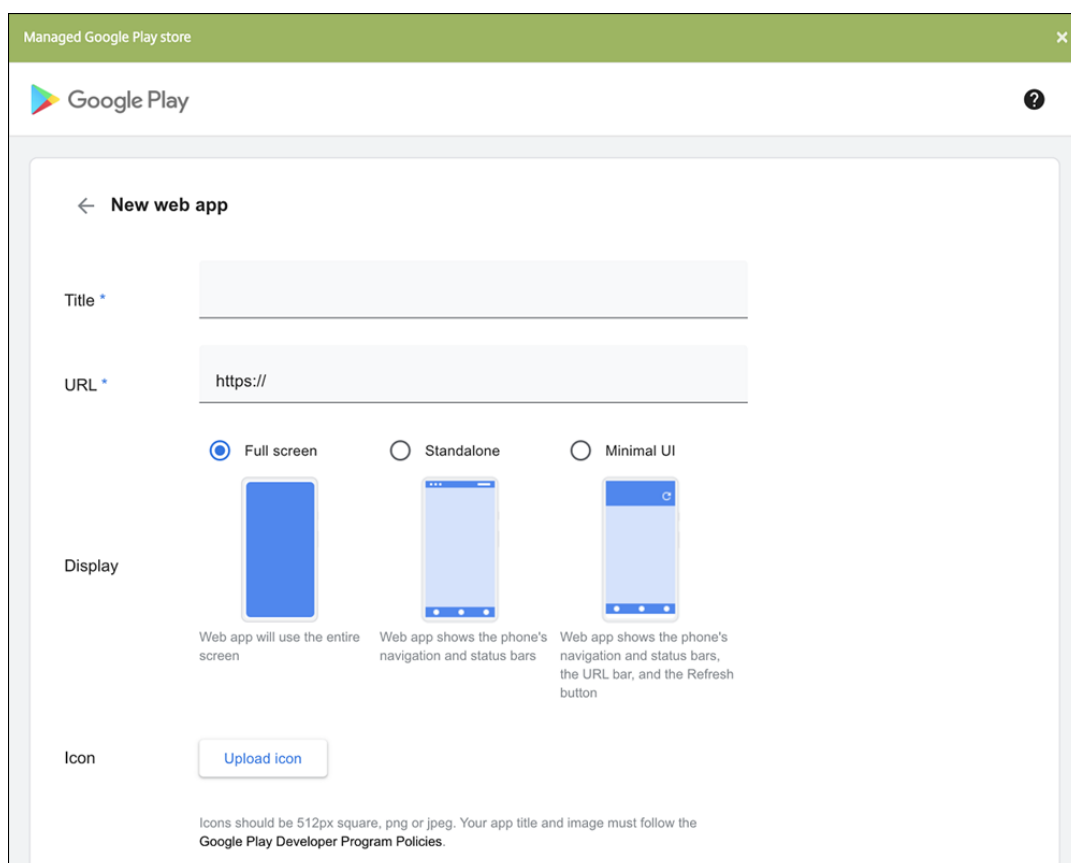


2. Click **Web Link**. The **App Information** page appears.
3. On the **App Information** pane, type the following information:
  - **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
  - **Description:** Type an optional description of the app.
  - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see About app categories.
4. Click **Next**. The **App Platforms** page appears.
5. Under **Platforms**, select **Other platforms** to add a web app for iOS, Android (legacy DA), Windows 8, and Windows Phone or select **Android Enterprise** or **Android for Workspace**. Clear the check box for any platforms you don't want to include.
  - If you select **Other platforms**, continue to the next step to configure the settings.
  - If you select **Android Enterprise** or **Android for Workspace**, click the **Upload** button to open the managed Google Play store. You do not need to register for a developer account to publish a web app. Click the **Plus** icon in the lower right corner to continue.



Configure these settings:

- **Title:** Type the name for the web app.
- **URL:** Type the web address for the app.
- **Display:** Choose how to display the web app on the user devices. The available options are **Full screen**, **Standalone**, and **Minimal UI**.
- **Icon:** Upload your own image to represent the web app.



When finished, click **Create**. It might take up to 10 minutes for your web app to publish.

6. For platforms other than Android Enterprise and Android for Workspace, configure these settings:

- **App name:** Accept the pre-filled name or type a new name.
- **App description:** Accept the pre-filled description or type one of your own.
- **URL:** Accept the pre-filled URL or type the web address for the app. Depending on the connector you choose, this field can contain a placeholder that you must replace before you can move to the next page.
- **App is hosted in internal network:** Select whether the app is running on a server in your internal network. If users connect from a remote location to the internal app, they must connect through Citrix Gateway. Setting this option to **On** adds the VPN keyword to the app and allows users to connect through Citrix Gateway. The default is **Off**.
- **App category:** In the list, click an optional category to apply to the app.
- **Image:** Select whether to use the default Citrix image or to upload your own app image. The default is Use default.
  - To upload your own image, click **Browse** and navigate to the file location. The file must be a .PNG file. You can't upload a JPEG or GIF file. When you add a custom graphic, you can't change it later.

7. Configure the deployment rules. For information, see [Configure deployment rules](#).
8. Expand **Store Configuration**.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings  ON

Allow app comments  ON

Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
  - **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
  - **Allow app ratings:** Allow users to rate the app in the app store.
  - **Allow app comments:** Allow users to leave comments on the app in the app store.
9. Click **Next**. The **Delivery Group Assignment** page appears.
  10. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.
  11. Expand **Deployment Schedule** and then configure the following settings:
    - **Deploy:** Choose whether to deploy the app to devices. The default is **On**.
    - **Deployment schedule:** Choose whether to deploy the app **Now** or **Later**. If you select **Later**, configure a date and time to deploy the app. The default is **Now**.

- **Deployment condition:** Choose **On every connection** to deploy the app every time the device connects. Choose **Only when previous deployment has failed** to deploy the app when the device failed to receive the app previously. The default is **On every connection**.

The **Deploy for always-on connection** option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.

The always-on option:

- Is not available for iOS devices
- Is not available for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management with version 10.18.19 or later
- Is not recommended for Android, Android Enterprise, Android for Workspace, and Chrome OS customers who began using Endpoint Management before version 10.18.19

The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

12. Click **Save**.

## Enable Microsoft 365 apps

You can open the MDX container to allow Secure Mail, Secure Web, and Citrix Files to transfer documents and data to Microsoft Office 365 apps. For details, see [Allowing Secure Interaction with Office 365 Apps](#).

## Apply workflows

Configure these settings to assign or create a workflow:

- **Workflow to Use:** In the list, click an existing workflow or click **Create a new workflow**. The default is **None**.

If you select **Create a new workflow**, configure these settings.

- **Name:** Type a unique name for the workflow.
- **Description:** Optionally, type a description for the workflow.
- **Email Approval Templates:** In the list, select the email approval template to be assigned. When you click the eye icon to the right of this field, a dialog box appears where you can preview the template.
- **Levels of manager approval:** In the list, select the number of levels of manager approval required for this workflow. The default is 1 level. Possible options are:
  - \* Not Needed

- \* 1 level
  - \* 2 levels
  - \* 3 levels
- **Select Active Directory domain:** In the list, select the appropriate Active Directory domain to be used for the workflow.
  - **Find additional required approvers:** Type the name of the additional required person in the search field and then click **Search**. Names originate in Active Directory.
  - When the name appears in the field, select the check box next to the name. The name and email address appear in the **Selected additional required approvers** list.

To remove a person from the **Selected additional required approvers** list, do one of the following:

- \* Click **Search** to see a list of all the persons in the selected domain.
- \* Type a full or partial name in the search box, and then click **Search** to limit the search results.
- \* Persons in the **Selected additional required approvers** list have check marks next to their name in the search results list. Scroll through the list and clear the check box next to each name you want to remove.

## App store and Citrix Secure Hub branding

You can set how apps appear in the store and add your logo to Secure Hub and the app store. These branding features are available for iOS and Android devices.

Before you begin, make sure you have your custom image ready and accessible.

The custom image must meet these requirements:

- The file must be in .png format
  - Use a pure white logo or text with a transparent background at 72 dpi.
  - The company logo cannot exceed this height or width: 170 px x 25 px (1x) and 340 px x 50 px (2x).
  - Name the files as Header.png and Header@2x.png.
  - Create a .zip file from the files, not a folder with the files inside it.
1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
  2. Under **Client**, click **Client Branding**. The **Client Branding** page appears.



Settings > Client Branding

### Client Branding

You can set the way apps appear in the store and add a logo to brand Secure Hub on mobile devices.

Store name\*  ⓘ

Default store view

Category

A-Z

Device

Phone

Tablet

Branding file

Note:

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.

A .zip file should be created from the files, not a folder with the files inside of it.

Configure the following settings:

- **Store name:** The store name appears in the user’s account information. Changing the name also changes the URL used to access store services. You typically do not need to change the default name.

**Important:**

The Store name can only contain alphanumeric characters.

- **Default store view:** Select either **Category** or **A-Z**. The default is **A-Z**
- **Device option:** Select either **Phone** or **Tablet**. The default is **Phone**.
- **Branding file:** To select a branding image or .zip file of images, click **Browse** and navigate to the file location.

3. Click **Save**.

To deploy this package to user devices, create a deployment package and then deploy the package.

## Citrix Virtual Apps and Desktops through the app store

**Important:**

If Endpoint Management is Workspace-enabled, Citrix Workspace provides access to Virtual Apps and Desktops. The setup in this section doesn’t apply to your site.

Endpoint Management can collect apps from Citrix Virtual Apps and Desktops and make the apps available to mobile device users in the app store. Users subscribe to the apps directly inside the app store and launch them from Citrix Workspace. The Citrix Workspace app must be installed on user devices to launch the apps.

To configure this setting, you need the fully qualified domain name (FQDN) or IP address and port number for an on-premises StoreFront.

1. In the Endpoint Management web console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **Virtual Apps and Desktops**. The **Virtual Apps and Desktops** page appears.

Settings > Virtual Apps and Desktops

### Virtual Apps and Desktops

Allows users to add Virtual Apps and Desktops through Secure Hub.

**Host \***

**Port \***

**Relative Path \***

**Use HTTPS**

**Use Cloud Connector**  [?](#)

**Resource Location \***  [?](#)

**Allowed Relative Paths \***  [?](#)

3. Configure these settings:

- **Host:** Type the fully qualified domain name (FQDN) or IP address for StoreFront.
- **Port:** Type the port number for StoreFront. The default is 80.
- **Relative Path:** Type the path. For example, /Citrix/PNAgent/config.xml
- **Use HTTPS:** Select whether to enable secure authentication between StoreFront and the client device. The default is **Off**.
- **Use Cloud Connector:** Choose **On** to use Cloud Connector for connections to the StoreFront server. Then, specify a **Resource Location** and **Allowed Relative Paths** for the connection.
  - **Resource Location:** Choose from the resource locations defined in [Citrix Cloud Connector](#).

- **Allowed Relative Paths:** The relative paths allowed for the specified resource location. Specify one path per line. You can use the asterisk (\*) wildcard.

Suppose that the resource location is <https://storefront.company.com> and you want to provide access to the following URLs:

- <https://storefront.company.com/Citrix/PNAgent/Config.xml>
- <https://storefront.company.com/Citrix/PNAgent/enum.aspx>
- <https://storefront.company.com/Citrix/PNAgent/launch.aspx>

To allow all requests with the URL <https://storefront.company.com/Citrix/PNAgent/>, enter this path: `/Citrix/PNAgent/*`

Endpoint Management blocks all other paths.

4. Click **Test Connection** to verify that Endpoint Management can connect to the specified StoreFront server.
5. Click **Save**.

## App connector types

July 1, 2019

The following table lists the connectors and the types of connectors that are available in Endpoint Management when you add a Web or SaaS app. You can also add a new connector to Endpoint Management when you add a Web or SaaS app.

The table indicates whether the connector supports user account management, which lets you create new accounts automatically or by using a workflow.

Connector name	SSO SAML	Supports user account management
EchoSign_SAML	Y	Y
Globoforce_SAML		<b>Note:</b> When using this connector, you must enable User Management for Provisioning to ensure seamless SSO integration.
GoogleApps_SAML	Y	Y
GoogleApps_SAML_IDP	Y	Y
Lynda_SAML	Y	Y

Connector name	SSO SAML	Supports user account management
Office365_SAML	Y	Y
Salesforce_SAML	Y	Y
Salesforce_SAML_SP	Y	Y
SandBox_SAML	Y	
SuccessFactors_SAML	Y	
ShareFile_SAML*	Y	
ShareFile_SAML_SP*	Y	
WebEx_SAML_SP	Y	Y

\* Not needed if your site is Workspace-enabled.

## Citrix Launcher

April 16, 2021

Citrix Launcher lets you customize the user experience for Android Enterprise devices and legacy Android devices deployed by Endpoint Management. With Citrix Launcher, you can prevent users from accessing certain device settings and restrict devices to one app or a small set of apps.

The minimum Android version supported for Secure Hub management of Citrix Launcher is Android 6.0.

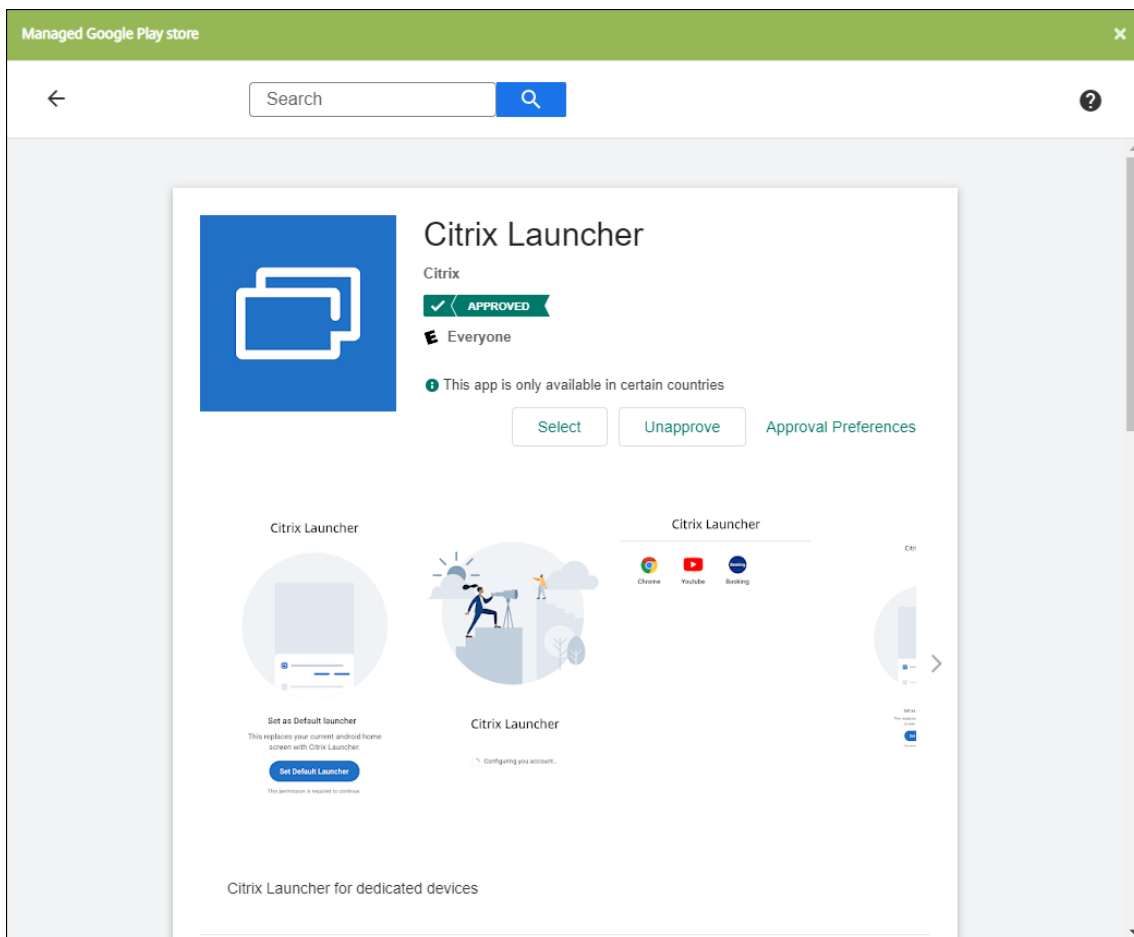
Use a **Launcher Configuration Policy** to control these Citrix Launcher features:

- Manage Android Enterprise devices and legacy Android devices so that users can access only the apps that you specify.
- Optionally specify a custom logo image for the Citrix Launcher icon and a custom background image for Citrix Launcher.
- Specify a password that users must type to exit the launcher.

Citrix Launcher isn't intended to be an extra layer of security over what the device platform already provides.

## Set up Citrix Launcher for Android Enterprise devices

1. Add the Citrix Launcher app (com.citrix.launcher.droid) to Endpoint Management as a public store app. In **Configure > Apps**, click **Add**, and then click **Public App Store**. For more information, see [Add a public app store app](#).



2. In the Kiosk device policy, specify which apps must be available on company-owned devices for dedicated use (also known as Android corporate owned single use (COSU) devices). Go to **Configure > Device Policies**, click **Add**, and select **Kiosk**. Then select the Citrix Launcher app and any additional apps in the allow list. If you previously added apps to the list, you don't need to upload the apps again. For more information, see [Android Enterprise settings](#).
3. Add the Launcher Configuration device policy. Go to **Configure > Device Policies**, click **Add**, and select **Launcher Configuration**. In the Launcher Configuration policy, add any of the apps that you specified in the Kiosk policy. You don't need to add all of the apps you specified in the Kiosk policy. You must add the Citrix Launcher app only in the Kiosk policy. For more information, see [Launcher Configuration Policy](#).
4. Create a delivery group and deploy resources. For more information, see the [Add a delivery group and deploy resources](#) section in this article.

After you deploy Citrix Launcher on company-owned Android Enterprise devices for dedicated use, Endpoint Management installs the app and replaces the default Secure Hub launcher. If you exit the Citrix Launcher app, Secure Hub becomes the default launcher again.

## Set up Citrix Launcher for legacy Android devices

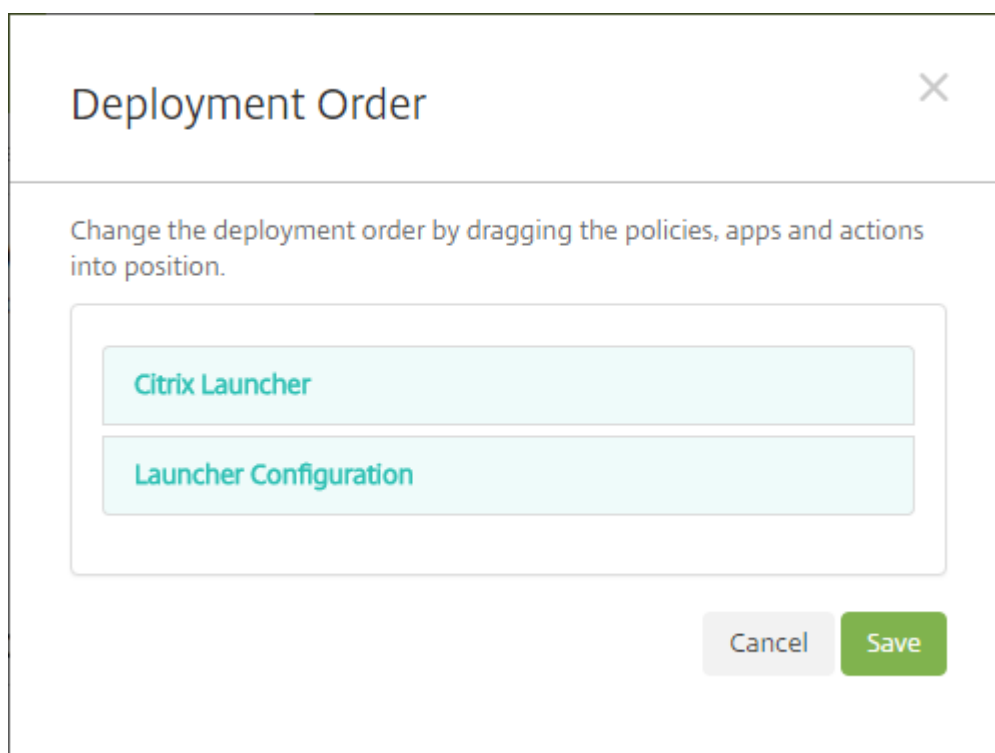
### Note:

In August 2020, Citrix deprecated support for the CitrixLauncher.apk for legacy Android devices. You can continue using the legacy Citrix Launcher app (com.citrix.launcher) for Android devices without receiving the new feature updates.

1. To locate the Citrix Launcher app, go to the [Citrix Endpoint Management download page](#) and search for **Citrix Launcher**. Download the latest file. The file is ready for upload into Endpoint Management and doesn't require wrapping.
2. Add the Launcher Configuration device policy. Go to **Configure > Device Policies**, click **Add**, and select **Launcher Configuration**. For more information, see [Launcher Configuration Policy](#).
3. Add the Citrix Launcher app to Endpoint Management as an enterprise app. In **Configure > Apps**, click **Add** and then click **Enterprise**. For more information, see [Add an enterprise app](#).
4. Create a delivery group and deploy resources. For more information, see the [Add a delivery group and deploy resources](#) section in this article.

## Add a delivery group and deploy resources

1. Create a delivery group for Citrix Launcher with the following configuration in **Configure > Delivery groups**.
  - On the **Policies** page, add a **Launcher Configuration Policy**.
  - On the **Apps** page, drag **Citrix Launcher** to **Required Apps**.
  - On the **Summary** page, click **Deployment Order** and ensure that the **Citrix Launcher** app precedes the **Launcher Configuration** policy.



2. Deploy resources to a delivery group by sending a push notification to all users in the delivery group. For more information about adding resources to a delivery group, see [Deploy resources](#).

### Manage devices without Citrix Launcher

Instead of using Citrix Launcher, you can use features that are already available.

To provision dedicated devices:

1. Create an enrollment profile by setting the **Device owner mode** to **Dedicated device**. See [Provisioning dedicated Android Enterprise devices](#) and [Enrollment profiles](#).
2. Create a Kiosk device policy to add apps to the allow list and set lock task mode. If you previously added apps to the list, you don't need to upload the apps again. For more information, see [Android Enterprise settings](#).
3. Enroll each device in the enrollment profile you created.

### Add apps using Apple volume purchase

October 20, 2021

Apple Business Manager (ABM) and Apple School Manager (ASM) let you buy licenses for apps and books in volume and synchronize the volume purchase information with Endpoint Management. You

can then use Endpoint Management to deploy these apps and books to iOS and macOS devices. Buying contents in volume simplifies the process of finding, buying, and distributing apps and books for an organization.

For more information about buying contents using ABM or ASM, see the [Apple Business Manager User Guide](#) or [Apple School Manager User Guide](#). This article describes how to synchronize volume-purchased licenses from ABM and ASM to Endpoint Management and how to manage the licenses.

**Note:**

Apple Volume Purchase Program (VPP) is no longer available as of January 14, 2021. The volume purchase function was integrated in ABM and ASM. If you currently use the Device Enrollment Program (DEP) or VPP, you can upgrade to ABM or ASM. For more information, see the Apple documentation [Upgrade from Apple Deployment Programs](#).

## About Apple volume purchase

When you buy contents in volume using ABM or ASM, note the following:

- You can buy licenses for the following content:
  - Public apps and books
  - Custom apps that are developed specifically for your organization
- You can deploy volume-purchased apps and books to organization-owned devices and BYO devices. Organization-owned devices enrolled through ABM or ASM support MDM or MDM+MAM enrollment but not MAM enrollment.
- For more information about distributing apps, see [Distribute Apple apps](#).
- For a list of known issues, see Knowledge Center article [CTX222633](#).

## Add a volume purchase account

After you buy content in the ABM or ASM portal, download the content token associated with Endpoint Management from the portal. Next, in Endpoint Management, create a volume purchase account based on this content code. This code lets Endpoint Management synchronize the content licenses from ABM or ASM.

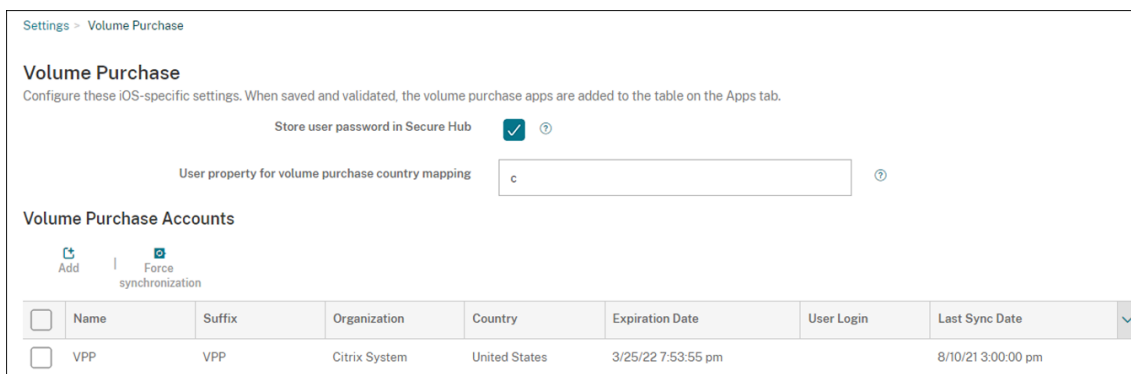
With the volume purchase, you can buy content and deploy it to devices by using managed licenses. If you currently use redemption codes and want to change to managed licenses, see the [Apple support document](#).

To add a volume purchase account in Endpoint Management

1. In the ABM or ASM portal, buy the content as needed and then download the content code file to a secure location.



2. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
3. Click **Volume purchase**. The **Volume purchase** configuration page appears.



4. Configure the following settings:
  - **Store user password in Secure Hub:** Select whether to store a user name and password in Secure Hub for Endpoint Management authentication. The default is **On**.
  - **User property for Volume purchase country mapping:** Type a country mapping code to allow users to download apps from the country-specific app store. Contact your content manager for this code.

Endpoint Management uses the country mapping code to choose the property pool of the volume purchase. For example, if the user property is United States, the user can't download apps if the mapping code is for the United Kingdom.
5. Click **Add**. The **Add a volume purchase account** dialog box appears.

### Add a volume purchase account ×

Define Business to Business (B2B) credentials will make this volume purchase account available as a B2B account.

**Name \***

**Suffix \***

**Company Token \***  ?

**User Login**  ?

**User Password**  ?

**App Auto Update**  × ?

6. Configure the following account settings:

**Note:**

If you use Apple Configurator 1, upload a license file as follows: Click **Configure > Apps**, go to a platform page of an app, and then expand **Volume purchase**.

- **Name:** Type a descriptive name for the account.
- **Suffix:** Type the suffix to appear with the app names inherited from the Apple stores. For example, if you enter **VP**, the **Secure Mail** app appears in the apps list as **Secure Mail - VP**.
- **Company Token:** Copy and paste the content token you downloaded in Step 1.
- **User Login:** (Optional) Type a user name for the administrator of this volume purchase account. If configured, the user name and password are required for synchronizing volume-purchased custom apps into Endpoint Management.
- **User Password:** (Optional) Type a password for the user name you typed.
- **App Auto Update:** If turned **On**, volume-purchased apps and optional apps in the Endpoint Management console update automatically when a new version is available. You still must update enterprise apps and public app store apps in the Endpoint Management console manually. If this setting is **Off**, you can still update volume-purchased apps in the Endpoint Management console manually. Once an app updates in the console, devices with the app installed receive that update as well. The default is **Off**.

After the volume account is added successfully, a message appears, notifying you of the follow-

ing:

- On the **Configure > Apps** page, the volume-purchased apps appear in the App list. The app names appear with the suffix you configured.
- On the **Configure > Media** page, the volume-purchased books appear in the Media list. The book names appear with the suffix you configured.

## Configure volume-purchased apps

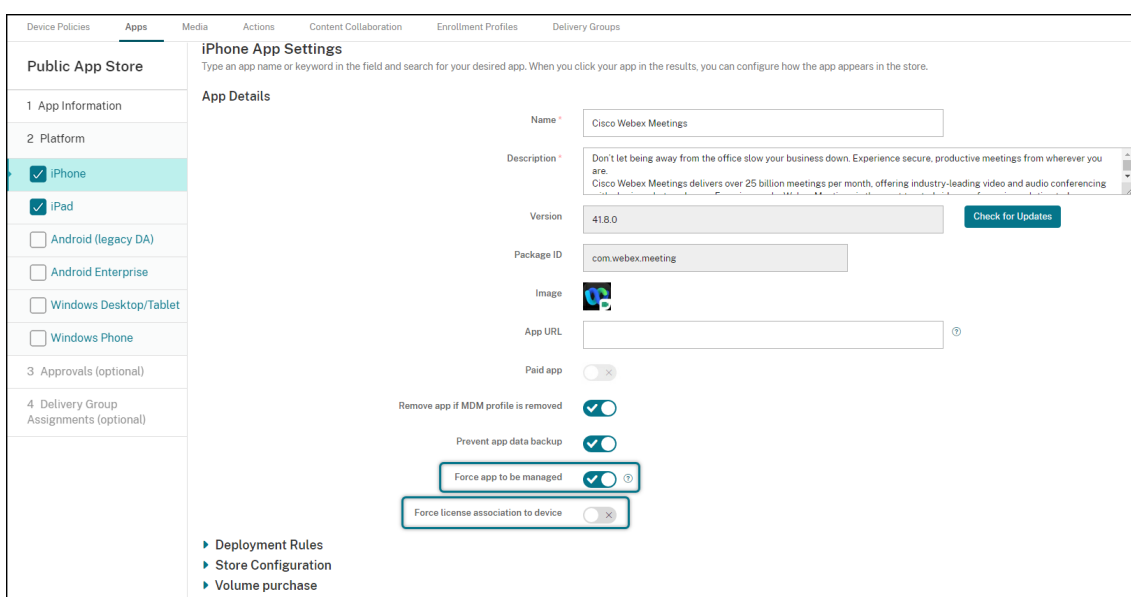
After you add a volume purchase account, the app information is synchronized to Endpoint Management and appears on the **Configure > Apps** page. You can now configure these apps, tune your delivery group, and adjust device policy settings for iOS and macOS devices. After you complete the configuration, users can enroll their devices.

When configuring a volume-purchased app, note the following settings:

- On the **Configure > Apps** page:
  - To let Endpoint Management deploy an app to a device rather than to a user, turn on **Force license association to device**. When this setting is on, users don't have to use their Apple ID and can download the apps without signing into their App Store account.
  - We recommend you turn on **Force app to be managed** for an app so that it automatically installs as a managed app.

### Note:

To enable the **Force app to be managed** setting to take effect, you must configure the `apple.app.force.managed` server property to **True** on the **Settings > Server Properties** page. For more information, see [Server properties](#)



- On the **Configure > Delivery Group** page:

To have the app install silently on user devices with minimal user interaction, go to the **Apps** page and then drag the app to the **Required Apps** list. By default, apps except Secure Hub are **Optional Apps**, which means users must start the app installation manually through Secure Hub.

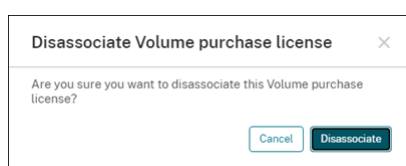
## Track and manage the use of app licenses

You can track the license usage for an app. If needed, you can take back a used license, making it available to another user or device.

1. Click **Configure > Apps**.
2. Select an app and click **Edit**.
3. Go to the **Platform** page and then expand **Volume purchase**.  
In the **Volume purchase ID Assignment** table, you can track how many licenses are used and by which user or device.

License ID	Usage Status	Associated User	Associated Device	Device Serial Number	Device Phone Number
8447476795	Used				
8447476794	Used				

4. To take back a license, select the license and then click **Disassociate**.



5. Click **Disassociate** to confirm the action.

## Retire a user from the volume purchase account

If you associate app licenses to users, you can retire users from the volume purchase accounts to take back all licenses that are assigned to those users. A use case includes when a user leaves your organization.

1. Click **Manage > Devices**
2. Select the device belonging to the target user and then click **Edit**.

3. Go to the **User Properties** page and select the volume purchase accounts as needed.
4. Click **Retire**.

The screenshot shows the 'User Properties' page in Citrix Endpoint Management. The 'Users' tab is selected. The left sidebar shows 'Device details' with '3 User Properties' highlighted. The main content area has the following fields:

- User name: user123
- Password: Enter new password
- Role: USER
- Membership: local\MSP (with a 'Manage Groups' button)
- Volume Purchase Accounts: Volume Purchase (with a 'Retire' button)

At the bottom right, there are 'Back' and 'Next >' buttons.

Endpoint Management revokes app licenses in the selected volume purchase accounts from the user.

## Synchronize the app information

Endpoint Management periodically synchronizes the app information with ABM or ASM. If needed, you can manually synchronize the app information. Synchronization makes sure that the app licenses and other app information reflect all changes. Such changes include when you manually delete an app from the volume purchase account.

## Change the default synchronization interval

By default, Endpoint Management refreshes the volume purchase license baseline at least every 1440 minutes (24 hours). A Citrix Cloud administrator can change the default interval through the server property, `vpp.baseline`. For more information, see [Server properties](#).

## Manually synchronize the app information

You can force a synchronization with ABM or ASM to get the latest app information immediately.

1. Click **Settings > Volume Purchase**

2. Select a volume purchase account and then click **Force synchronization**. Or click **Force synchronization** without selecting a volume purchase account to synchronize all accounts.

Settings > Volume Purchase

### Volume Purchase

Configure these iOS-specific settings. When saved and validated, the volume purchase apps are added to the table on the Apps tab.

Store user password in Secure Hub

User property for volume purchase country mapping

#### Volume Purchase Accounts

[Add](#) | [Force synchronization](#)

<input type="checkbox"/>	Name	Suffix	Organization	Country	Expiration Date	User Login	Last Sync Date
<input type="checkbox"/>	VPP	VPP	Citrix System	United States	3/25/22 7:53:55 pm		8/10/21 3:00:00 pm

3. Confirm the synchronization action. The synchronization starts.

The synchronization might take several minutes depending on the number of volume purchase licenses. After the synchronization completes, Endpoint Management refreshes the **Volume Purchase** page and updates the sync date and time in the new **Last Sync Date** column.

## Check for the app updates

If you turn on the **App Auto Update** setting when adding a volume purchase account, Endpoint Management periodically checks for the new versions for volume-purchased apps and optional apps and makes updates. If needed, you can manually check for the new version for any app and apply the app updates to Endpoint Management.

Once Endpoint Management receives a new version of a required app, it pushes the new version to the devices for silent installation without prompting users.

To check and apply the new version for an app

1. Click **Configure > Apps**. The **Apps** page appears.
2. Select an app and click **Edit**.
3. Go to the **Platform** page, and then click **Check for Updates** next to **Version**.
4. Go to the **Platform** page, and then click **Check for Updates** next to **Version**.
5. In the **Update** dialog box that appears, apply the update if a new version is available.

## Renew the content token for your volume purchase account

A content token expires annually. When the token is nearing expiration, Endpoint Management displays a license expiration warning. Renew the content token in time to prevent interruption for your users.

1. From the ABM or ASM portal, download an updated token.

2. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
3. Click **Volume Purchase**. The Volume Purchase configuration page appears.
4. Edit your volume purchase account with the updated token info.

## Deploy Microsoft Store for Business apps from Endpoint Management

September 8, 2021

Microsoft Store for Business is a location where you can find and distribute free and paid apps in volume for your organization. When you connect Citrix Endpoint Management to Microsoft Store for Business:

- The Endpoint Management **Configure > Apps** page lists the Store for Business apps.
- You can then deploy those apps to Windows 10 and Windows 11 devices.

Endpoint Management supports only online license app management, which is the default licensing model supported by Microsoft Store for Business. This model requires users and devices to connect to Microsoft Store services to acquire an app and its license.

To learn more about Microsoft Store for Business, see the Microsoft documentation at <https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview>.

### Prerequisites to access Microsoft Store for Business apps

- Azure Active Directory

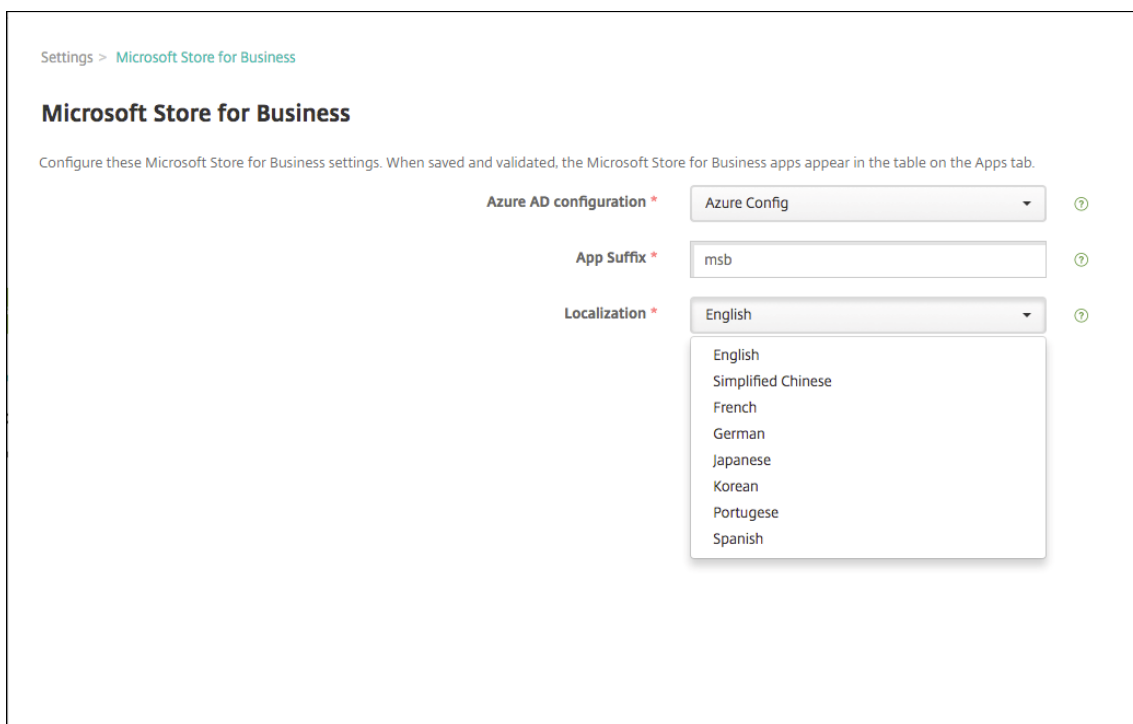
To access Microsoft Store for Business apps, you must first configure Azure Active Directory as an Identity Provider. For information on performing this configuration, see [Authentication with Azure Active Directory through Citrix Cloud](#).

- Microsoft Store for Business

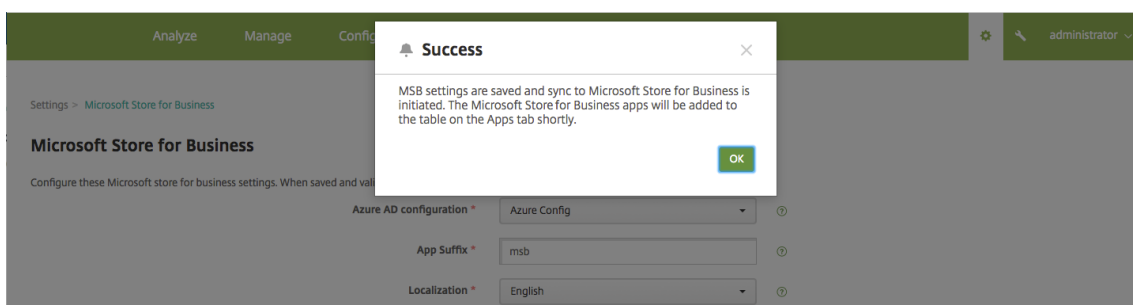
### Connect Endpoint Management to Microsoft Store for Business

1. In the Endpoint Management console **Settings** page, search for and click the link for **Microsoft Store for Business**.
2. Configure these settings:
  - **Azure AD configuration:** Select the Azure Active Directory instance you configured as part of the prerequisites.

- **App Suffix:** Enter a suffix added to all Microsoft Store for Business apps for easy identification.
- **Localization:** Select the language to use for the app details downloaded from Store for Business to Endpoint Management.

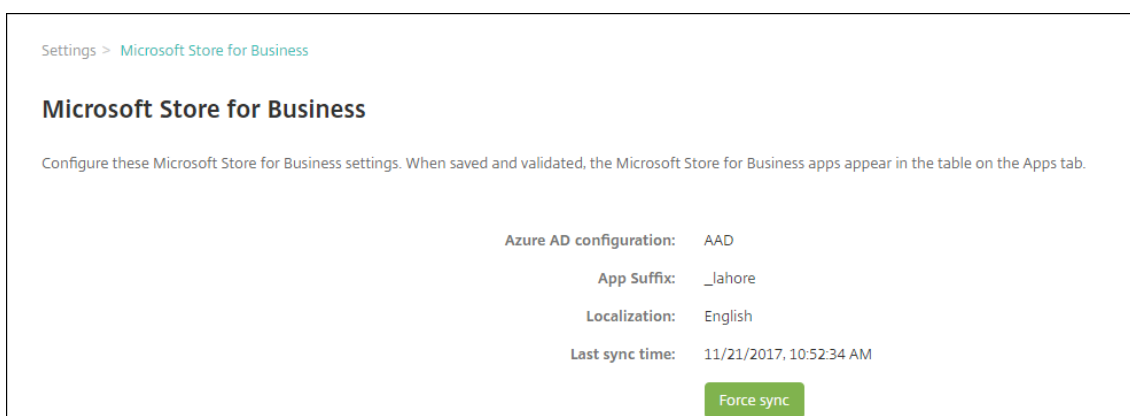


3. Click **Save**. Endpoint Management adds the Microsoft Store for Business apps to the **Configure > Apps** page.



4. To resync the apps later, return to the Microsoft Store for Business settings page and click the **Force Sync** button.



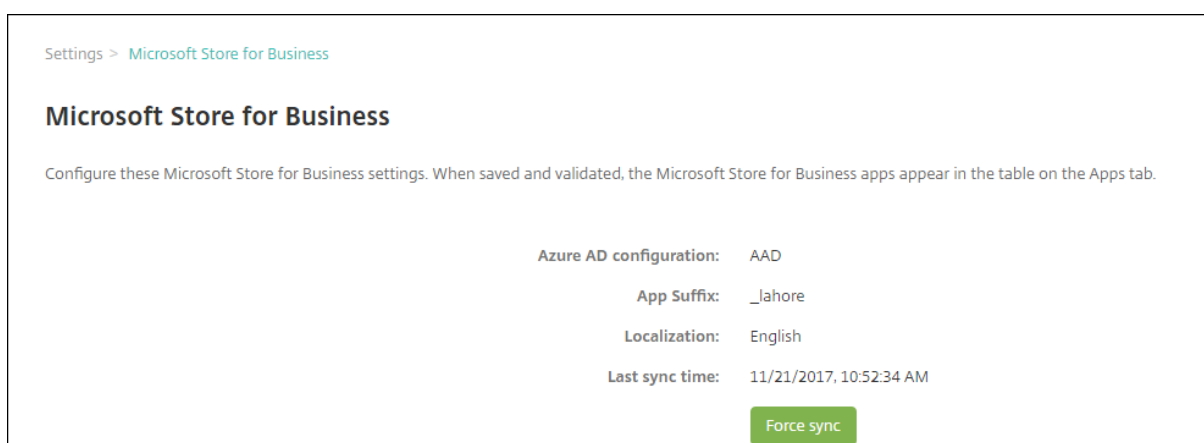


## Associate your Microsoft Store for Business account with Endpoint Management

1. Log in to the Microsoft Business Store using the same tenant account that you use to sign in to Azure Active Directory.
2. In the Business Store, choose **Settings > Management tools**.
3. On the **Management tools** page, choose **Add a management tool**.
4. Next, choose the name you specified for the MDM solution (such as Endpoint Management or XenMobile) when configuring Azure Active Directory in the Azure portal.

## Sync apps with the Store for Business

By default, Endpoint Management syncs with Microsoft Store for Business every 24 hours. To force a sync, go to **Settings > Microsoft Store for Business** and click **Force sync**.



## Assign Store for Business apps to delivery groups

Apps synced from Microsoft Store for Business have the suffix you configured on the **Settings > Microsoft Store for Business** page.

Icon	App Name	Type	Category	Created On	Last Updated	Disable
	Slackmsb	Public App Store	Default	11/2/17 2:47 AM	11/2/17 2:47 AM	<input type="checkbox"/>
	PDF Reader - View, Edit, Sharemsb	Public App Store	Default	11/2/17 2:47 AM	11/2/17 2:47 AM	<input type="checkbox"/>
	Lyftmsb	Public App Store	Default	11/2/17 2:47 AM	11/2/17 2:47 AM	<input type="checkbox"/>
	ShareFilemsb	Public App Store	Default	11/2/17 2:47 AM	11/2/17 2:47 AM	<input type="checkbox"/>
	WinDbg Previewmsb	Public App Store	Default	11/2/17 2:47 AM	11/2/17 2:47 AM	<input type="checkbox"/>
	LastPass: Free Password Managemersb	Public App Store	Default	11/2/17 2:47 AM	11/2/17 2:47 AM	<input type="checkbox"/>
	Athena DICOM Viewersmsb	Public App Store	Default	11/2/17 2:47 AM	11/2/17 2:47 AM	<input type="checkbox"/>
	Citrix Receivermsb	Public App Store	Default	11/2/17 2:47 AM	11/2/17 2:47 AM	<input type="checkbox"/>
	Windows App Studio UWP Samplesmsb	Public App Store	Default	11/2/17 2:47 AM	11/2/17 2:47 AM	<input type="checkbox"/>
	Duolingo - Learn Languages for Freemsb	Public App Store	Default	11/2/17 2:47 AM	11/2/17 2:47 AM	<input type="checkbox"/>

1. To add those apps to delivery groups: Go to **Configure > Delivery Groups**, select a group, click **Edit**, and then click **Apps**. Move the apps to the **Required Apps** list.
2. Go to **Configure > Apps**. Select one or more apps, click **Edit**, and then click **Delivery Group Assignments**.

## Revoke a user license for an app

1. Go to **Configure > Apps**, select the Store for Business app, and then click **Edit**.
2. Under **Platform**, click **Windows Desktop/Tablet**.
3. Scroll down and expand **Microsoft Store for Business**.

**Windows Phone App Settings**

Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

**App Details**

Name \* BusMap\_lehore

Description \* Quickly look up buses' information in Ho Chi Minh City with BusMap.

Package ID 21441QuanCoder4713827D103C\_c85Nk1ty52file

Image

Paid app OFF

**Deployment Rules**

**Store Configuration**

**Microsoft Store for Business**

**License Assignment**

Disassociate

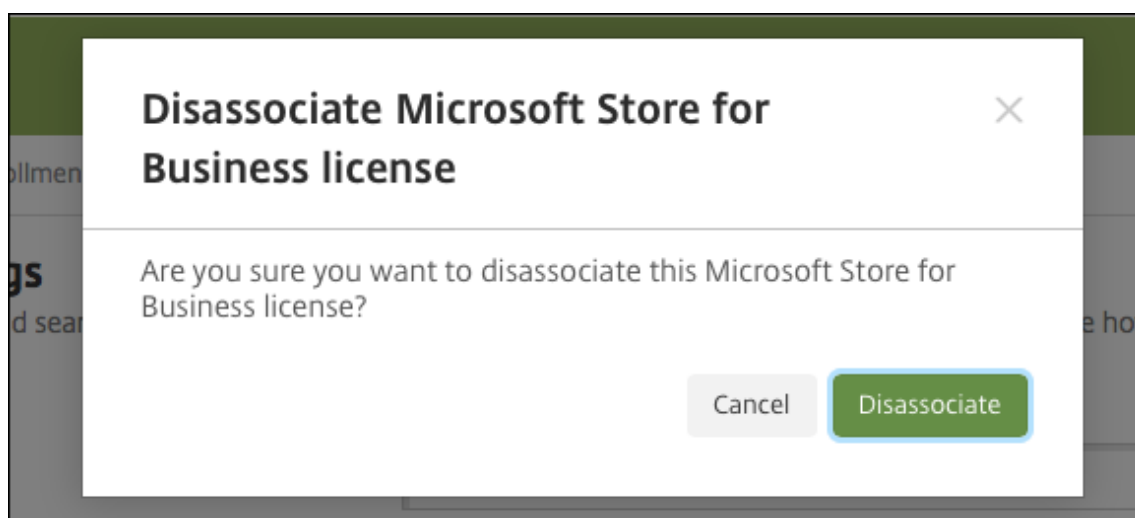
Associated User	Date Assigned	Status
	11/13/2017	active

Showing 1 - 1 of 1 items

License Usage: 1 of Unlimited

Back Next

4. Select the user and click **Disassociate**.



## Use Citrix Content Collaboration with Endpoint Management

September 7, 2021

Integration of Citrix Content Collaboration with Endpoint Management differs depending on whether your site is Workspace-enabled.

- When using Citrix Workspace and Citrix Workspace app with Citrix Content Collaboration, you deploy Content Collaboration from Citrix Workspace. Your users access Citrix Files from Citrix Workspace. For information, see [Deploy](#) and [Create or link a Content Collaboration \(ShareFile\) account to Citrix Cloud](#).
- If Endpoint Management isn't Workspace-enabled, Endpoint Management has two options for integrating with Citrix Content Collaboration: Citrix Files and storage zone connectors.

### Citrix Files

You can configure Endpoint Management to provide access to your Content Collaboration account. That configuration:

- Gives mobile users access to the full Content Collaboration feature set, such as file sharing, file sync, and storage zone connectors.
- Can provide Citrix Files with single sign-on authentication of mobile productivity app users and comprehensive access control policies.
- Provides Content Collaboration configuration, service level monitoring, and license usage monitoring through the Endpoint Management console.

For more information about configuring Endpoint Management for Enterprise accounts, see [SAML for single sign-on with Citrix Files](#).

### **Storage zone connectors**

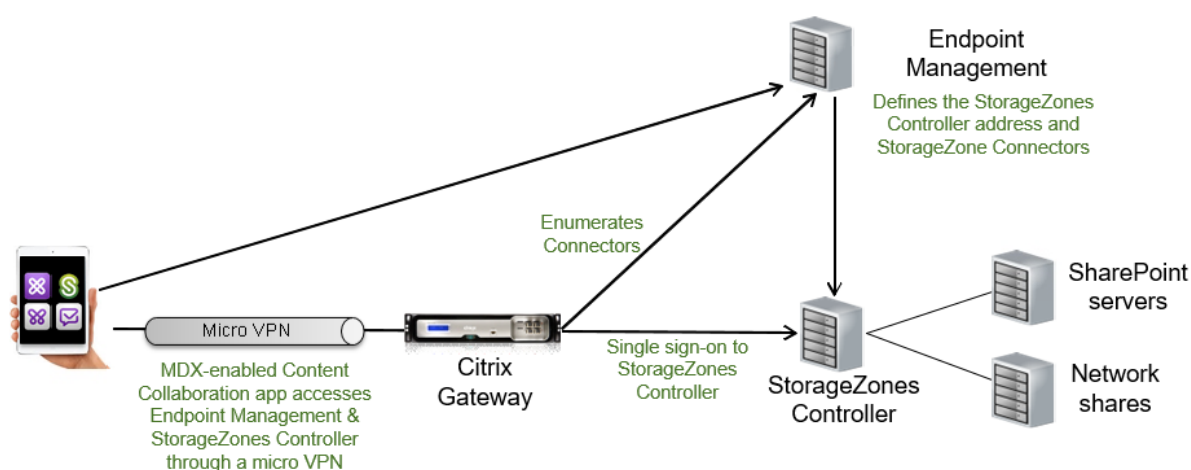
You can configure Endpoint Management to provide access only to storage zone connectors that you create through the Endpoint Management console. That configuration:

- Provides secure mobile access to existing on-premises storage repositories, such as SharePoint sites and network file shares.
- Doesn't require that you set up a Citrix Content Collaboration subdomain or host Citrix Files data.
- Provides users with mobile access to data through the Citrix mobile productivity apps for Citrix Files for iOS and Android. Users can edit Microsoft Office documents. Users can also preview and annotate Adobe PDF files from mobile devices.
- Complies with security restrictions against leaking user information outside of the corporate network.
- Provides simple setup of storage zone connectors through the Endpoint Management console. If you later decide to use the full Citrix Files functionality with Endpoint Management, you can change the configuration in the Endpoint Management console.

For an Endpoint Management integration with storage zone connectors only:

- Citrix Content Collaboration uses your single sign-on configuration to Citrix Gateway to authenticate with storage zones controller.
- Endpoint Management doesn't authenticate through SAML because the Citrix Files control plane isn't used.

The following diagram shows the high-level architecture for Endpoint Management use with storage zone connectors.



## Requirements

- Minimum component versions:
  - ShareFile for iOS (MDX) 5.3
  - ShareFile for Android (MDX) 5.3
  - Storage zones controller 5.11.20

This article contains instructions for how to configure storage zones controller 5.0
- Ensure that the server to run storage zones controller meets the system requirements. For requirements, see [System requirements](#).

The requirements for storage zones for Citrix Files Data and for Restricted storage zones don't apply to an Endpoint Management integration with storage zone connectors only.

Endpoint Management doesn't support Documentum connectors.

- To run PowerShell scripts:
  - Run the scripts in the 32-bit (x86) version of PowerShell.

## Installation tasks

Complete the following tasks, in the order presented, to install and set up storage zones controller. These steps are specific to Endpoint Management integration with storage zone connectors only. Some of these articles are in the storage zones controller documentation.

1. [Configure NetScaler for storage zones controller](#)

You can use Citrix Gateway as a DMZ proxy for storage zones controller.

2. [Install an SSL certificate](#)

A storage zones controller that hosts standard zones requires an SSL certificate. A storage zones controller that hosts restricted zones and uses an internal address doesn't require an SSL certificate.

3. [Prepare your server](#)

IIS and ASP.NET setup is required for storage zone connectors.

4. Install storage zones controller

5. Prepare storage zones controller for use with storage zone connectors-only

6. [Specify a proxy server for storage zones](#)

The storage zones controller console enables you to specify a proxy server for storage zones controller. You can also specify a proxy server using other methods.

7. [Configure the domain controller to trust the storage zones controller for delegation](#)

Configure the domain controller to support NTLM or Kerberos authentication on network shares or SharePoint sites.

8. Join a secondary storage zones controller to a storage zone

To configure a storage zone for high availability, connect at least two storage zones controllers to it.

### Install storage zones controller

1. Download and install the storage zones controller software:

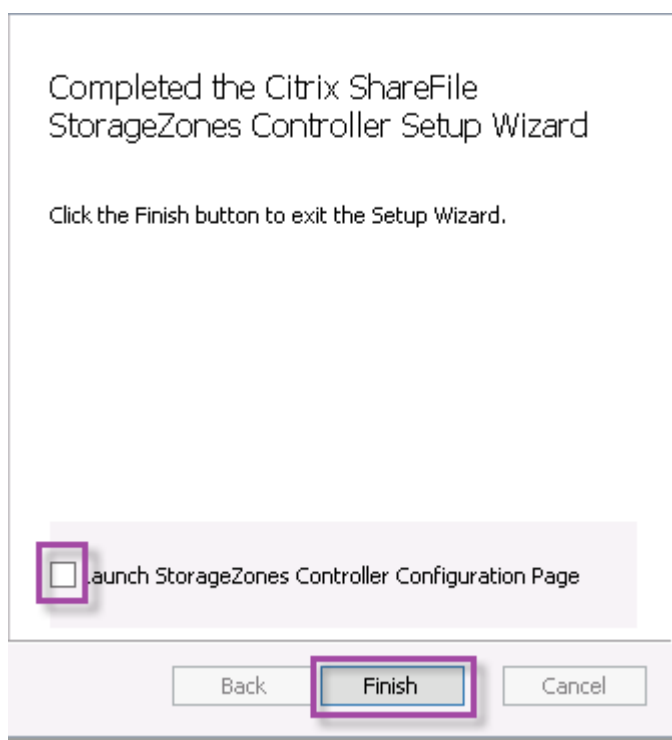
- a) From the Citrix Files download page at <https://www.citrix.com/downloads/sharefile.html>, log on and download the latest storage zones controller installer.
- b) Installing storage zones controller changes the default website on the server to the installation path of the controller. Enable **Anonymous Authentication** on the default website.

2. On the server where you want to install storage zones controller, run StorageCenter.msi.

The storage zones controller setup wizard starts.

3. Respond to the prompts:

- In the **Destination Folder** page, if Internet Information Services (IIS) is installed in the default location, leave the defaults. If not, browse to the IIS installation location.
- When installation is complete, clear the check box for **Launch Storage Zones Controller Configuration Page** and then click **Finish**.



4. When prompted, restart the storage zones controller.
5. To test that the installation was successful, navigate to <https://localhost/>. (If you get a certificate error, consider connecting with HTTP instead.) If the installation is successful, the Citrix Files logo appears.

If the Citrix Files logo does not appear, clear the browser cache and try again.

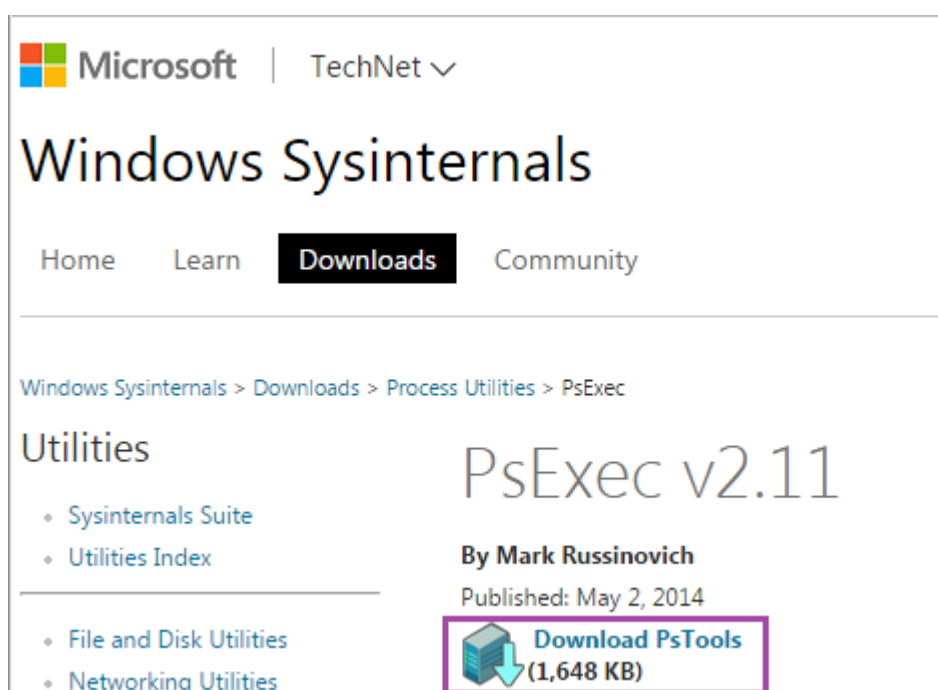
**Important:**

If you plan to clone the storage zones controller, capture the disk image before you proceed with configuring the storage zones controller.

### Prepare storage zones controller for use with storage zone connectors-only

For an integration only with storage zone connectors, you don't use the storage zones controller administrative console. That interface requires a Citrix Files administrator account, which isn't necessary for this solution. As a result, you run a PowerShell script to prepare the storage zones controller for use without the Citrix Files control plane. The script does the following:

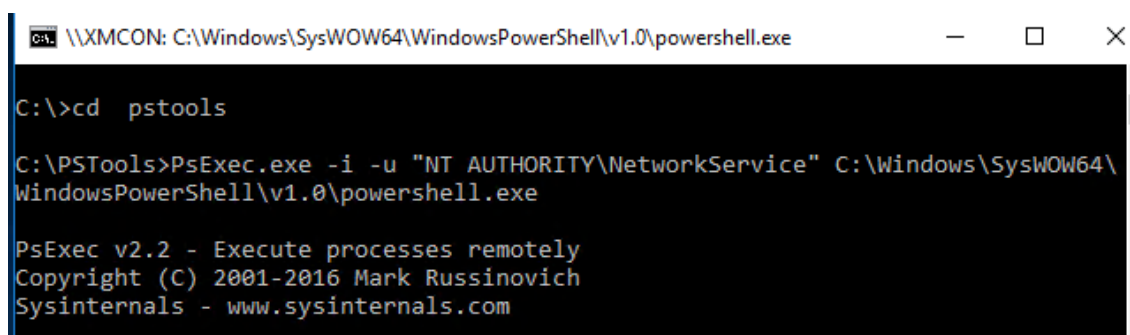
- Registers the current storage zones controller as a primary storage zones controller. You can later join secondary storage zones controller to the primary controller.
  - Creates a zone and sets the passphrase for it.
1. From your storage zones controller server, download the PsExec tool: Navigate to Microsoft [Windows Sysinternals](#) and then click **Download PsTools**. Extract the tool to the root of the C drive.



The screenshot shows the Microsoft TechNet website for Windows Sysinternals. The main navigation includes Home, Learn, Downloads (highlighted), and Community. The breadcrumb trail is Windows Sysinternals > Downloads > Process Utilities > PsExec. The page title is 'Windows Sysinternals'. Under 'Utilities', there are links for Sysinternals Suite, Utilities Index, File and Disk Utilities, and Networking Utilities. The main content area features 'PsExec v2.11' by Mark Russinovich, published on May 2, 2014. A 'Download PsTools (1,648 KB)' button is highlighted with a purple box.

2. Run the PsExec tool: Open the Command Prompt as the Administrator User and then type the following:

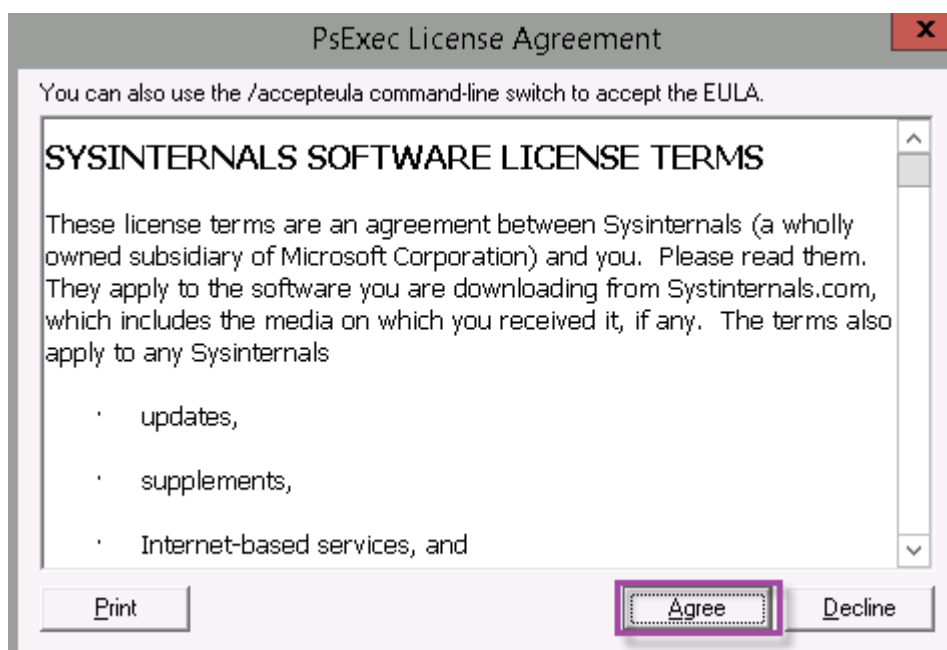
```
1  ````
2  cd c:\pstools
3  PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
   \WindowsPowerShell\v1.0\powershell.exe
4  <!--NeedCopy-->  ````
```



The screenshot shows a Windows Command Prompt window titled 'C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe'. The user has navigated to the 'pstools' directory and executed the command: `PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe`. The output shows the PsExec v2.2 help text: 'PsExec v2.2 - Execute processes remotely. Copyright (C) 2001-2016 Mark Russinovich. Sysinternals - www.sysinternals.com'.

3. When prompted, click **Agree** to run the Sysinternals tool.





A PowerShell window opens.

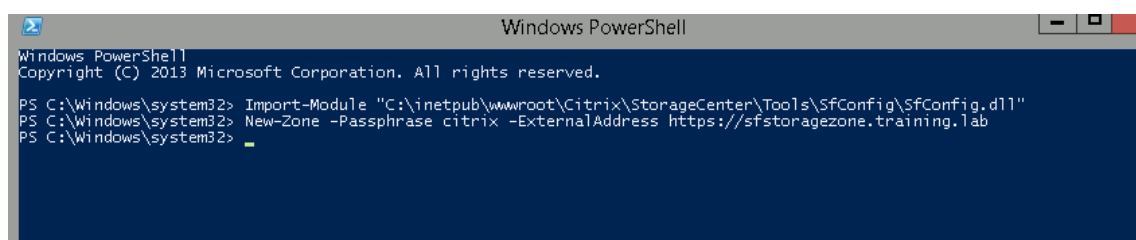
4. In the PowerShell window, type the following:

```
1  `` `
2  Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
   SfConfig\SfConfig.dll"
3  New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
   com
4  <!--NeedCopy--> `` `
```

Where:

**Passphrase:** Is the passphrase you want to assign to the site. Make a note of it. You cannot recover the passphrase from the controller. If you lose the passphrase, you cannot reinstall storage zones, join more storage zones controllers to the storage zone, or recover the storage zone if the server fails.

**ExternalAddress:** Is the external fully qualified domain name of the storage zones controller server.



Your primary storage zones controller is now ready.

Before you log in to Endpoint Management to create storage zone connectors: Complete the following configuration, if applicable:

[Specify a proxy server for storage zones](#)

[Configure the domain controller to trust the storage zones controller for delegation](#)

[Join a secondary storage zones controller to a storage zone](#)

To create storage zone connectors, see Define storage zones controller connections in Endpoint Management.

### **Join a secondary storage zones controller to a storage zone**

To configure a storage zone for high availability, connect at least two storage zones controllers to it. To join a secondary storage zones controller to a zone, install storage zones controller on a second server. Then join that controller to the zone of the primary controller.

1. Open a PowerShell window on the storage zones controller server that you want to join to the primary server.
2. In the PowerShell window, type the following:

```
Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
```

For example:

```
Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
```

### **Define storage zones controller connections in Endpoint Management**

Before you add storage zone connectors, you configure connection information for each storage zones controller enabled for storage zone connectors. You can define storage zones controllers as described in this section, or when you add a connector.

On your first visit to the **Configure > Content Collaboration** page, the page summarizes the differences between using Endpoint Management for Enterprise accounts and storage zone connectors.

Device Policies   Apps   Media   Actions   **Content Collaboration**   Enrollment Profiles   Delivery Groups

Choose a method for integrating Content Collaboration with Endpoint Management. Or, learn more about which mode to select.

	Content Collaboration	Storage Zone Connectors Only
Access network shares and SharePoint data from mobile devices	✓	✓
Edit Microsoft Office documents from mobile devices	✓	✓
Preview and annotate Adobe PDF files from mobile devices	✓	✓
Store data in Citrix-managed or customer-managed storage zones or both	✓	
Securely share files with people inside and outside the enterprise	✓	
Sync files and data across multiple devices	✓	
Access files through the Citrix Files website	✓	
Access Office 365 content and Personal Cloud connectors from mobile devices	✓	
Use auditing and reporting capabilities	✓	

Configure Content Collaboration
Configure Connectors

Click **Configure Connectors** to continue with the configuration steps in this article.

Device Policies   Apps   Media   Actions   **Content Collaboration**   Enrollment Profiles   Delivery Groups

**Storage Zone Connectors** Search

Storage zone connectors provide access to documents and folders in SharePoint sites and network file shares.

Add | Manage Storage Zones

Connector Name	Type	Storage Zone	Location	Delivery Groups
▼				

1. In **Configure > Content Collaboration**, click **Manage Storage Zones**.

Device Policies   Apps   Media   Actions   **ShareFile**   Enrollment Profiles   Delivery Groups

**StorageZone Connectors** Show filter Search

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

Add | Manage Storage Zones

Connector Name	Type	StorageZone	Location	Delivery Groups
▼				

2. In **Manage Storage Zones**, add the connection information.

**Manage Storage Zones**

*Add New*

**Name \*** ContentCollaborationTest

**FQDN \***

**Port \*** 443

**Secure Connection** ON

**Administrator user na...**

**Administrator passwo...**

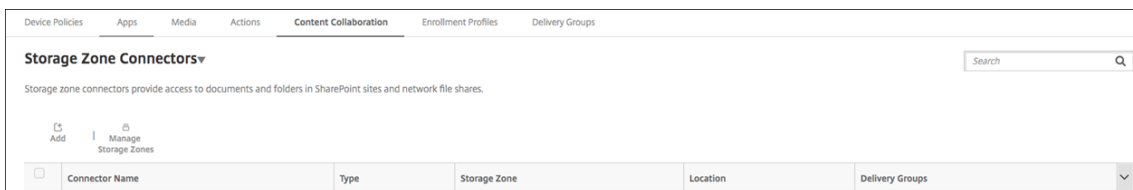
Add Cancel Save

- **Name:** A descriptive name for the storage zone, used to identify the storage zone in Endpoint Management. Don't include a space or special characters in the name.
  - **FQDN and Port:** The fully qualified domain name and port number for a storage zones controller that is reachable from the Endpoint Management server.
  - **Secure Connection:** If you use SSL for connections to storage zones controller, use the default setting, On. If you don't use SSL for connections, change this setting to Off.
  - **Administrator user name** and **Administrator password:** An administrator service account user name (in the form domain\admin) and password. Alternatively, a user account with read and write permissions on the storage zones controllers.
3. Click **Save**.
  4. To test the connection, verify that the Endpoint Management server can reach the fully qualified domain name of the storage zones controller on port 443.
  5. To define another storage zones controller connection, click the **Add** button in **Manage Storage Zones**.

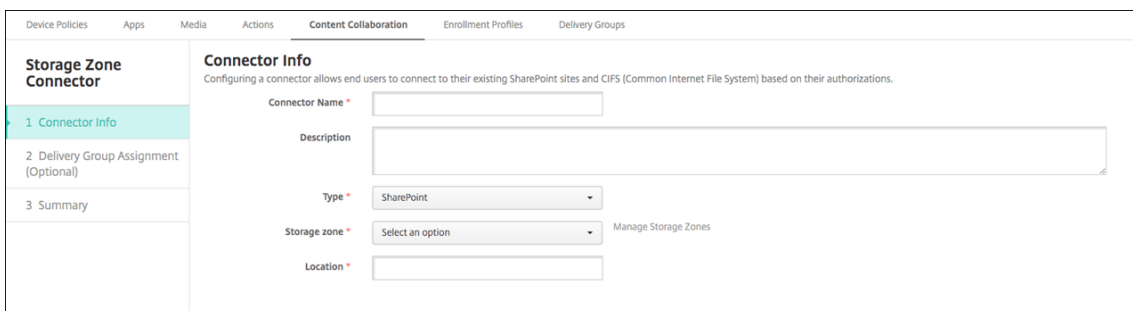
To edit or delete the information for a storage zones controller connection, select the connection name in **Manage Storage Zones**. Then, click **Edit** or **Delete**.

## Add a storage zone connector in Endpoint Management

1. Go to **Configure > Content Collaboration** and then click **Add**.

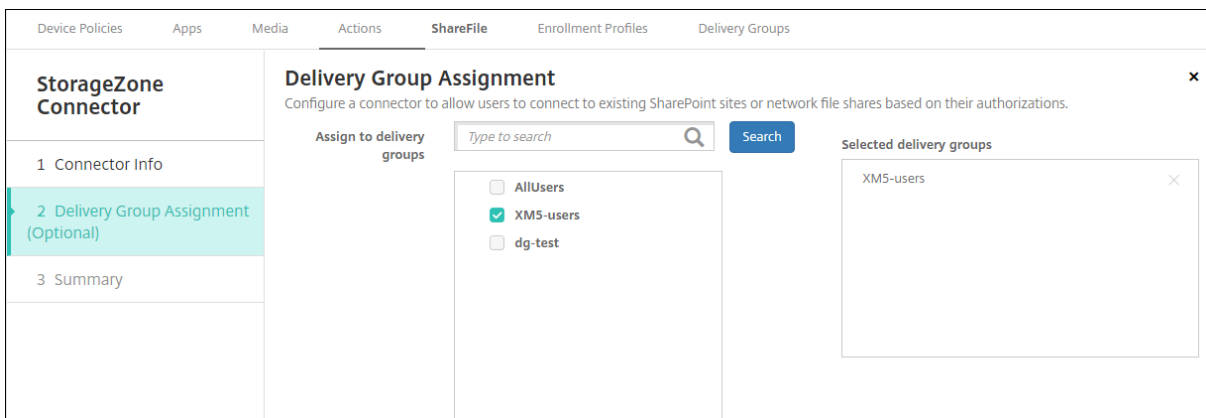


2. On the **Connector Info** page, configure these settings:



- **Connector Name:** A name that identifies the storage zone connector in Endpoint Management.
- **Description:** Optional notes about this Connector.
- **Type:** Choose either **SharePoint** or **Network**.
- **Storage zone:** Choose the storage zone associated with the connector. If the storage zone isn't listed, click **Manage Storage Zones** to define the storage zones controller.
- **Location:** For SharePoint, specify the URL of the SharePoint root-level site, site collection, or document library, in the form <https://sharepoint.company.com>. For a network share, specify the fully qualified domain name of the Uniform Naming Convention (UNC) path, in the form `\\server\share`.

3. On the **Delivery Group Assignment** page, optionally assign the Connector to delivery groups. Alternatively, you can associate connectors to delivery groups using **Configure > Delivery Groups**.



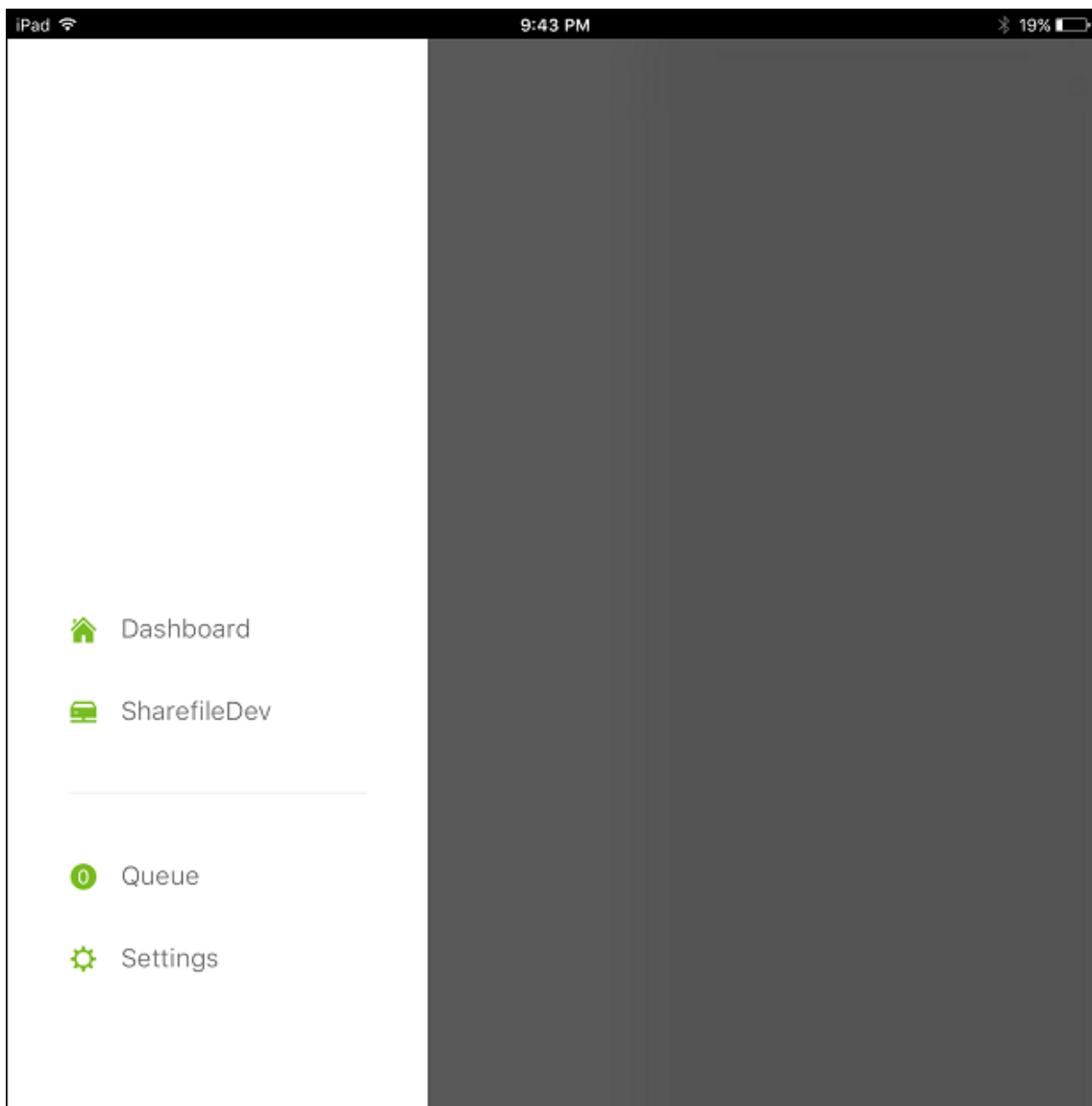
1. On the **Summary** page, you can review the options you configured. To adjust the configuration, click **Back**.
2. Click **Save** to save the connector.
3. Test the connector:

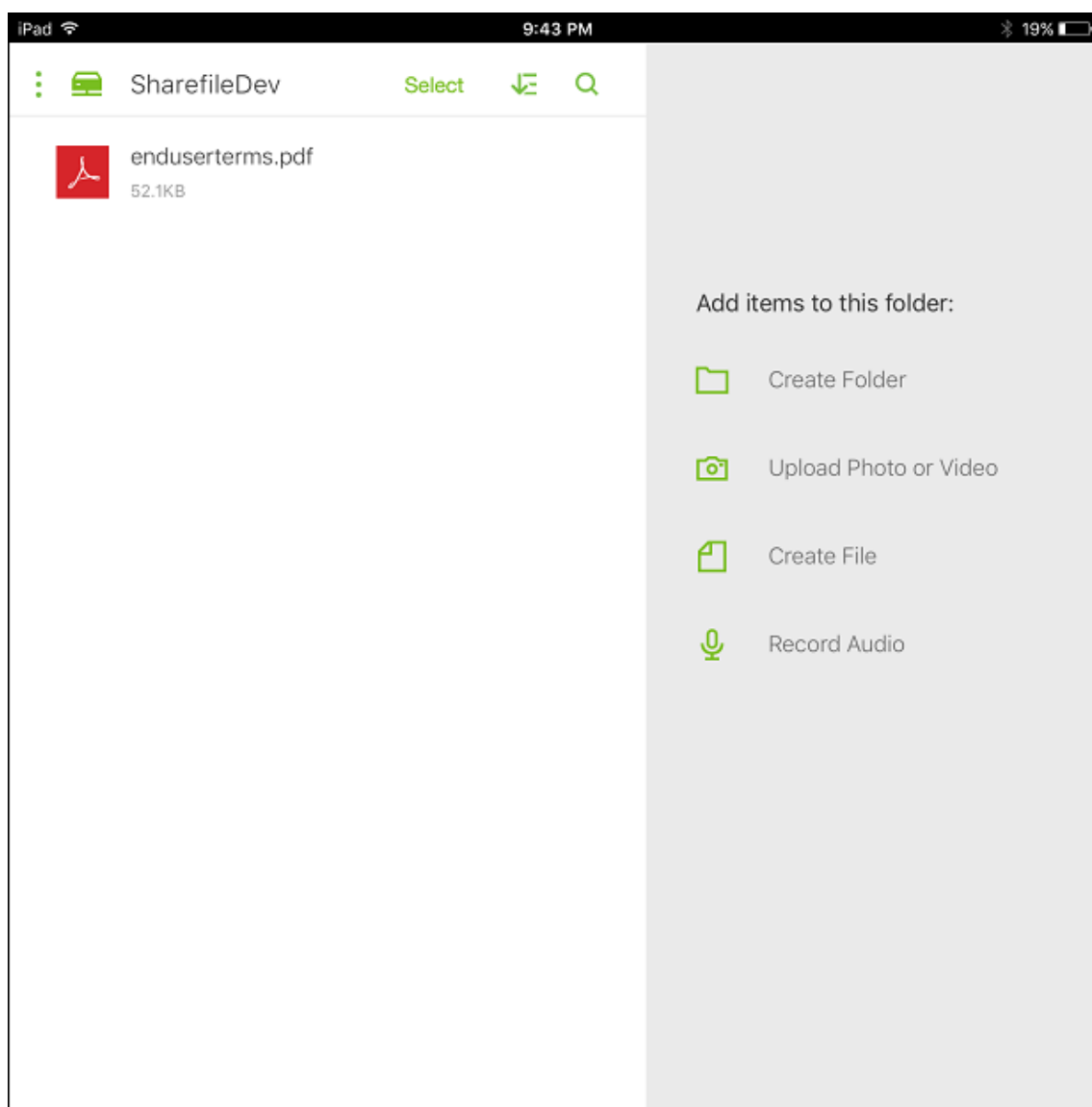
- a) When you wrap the Citrix Files clients, set the Network access policy to **Tunneled - Web SSO**.

In this mode of tunneling, the MDX framework terminates SSL/HTTP traffic from an MDX app. MDX then initiates new connections to internal connections on behalf of the user. This policy setting enables the MDX framework to detect and respond to authentication challenges issued by web servers.

- b) Add the Citrix Files clients to Endpoint Management. For details, see [To add Citrix Files clients to Endpoint Management](#).
- c) From a supported device, verify single sign-on to Citrix Files and connectors.

In the following samples, SharefileDev is the name of a connector.



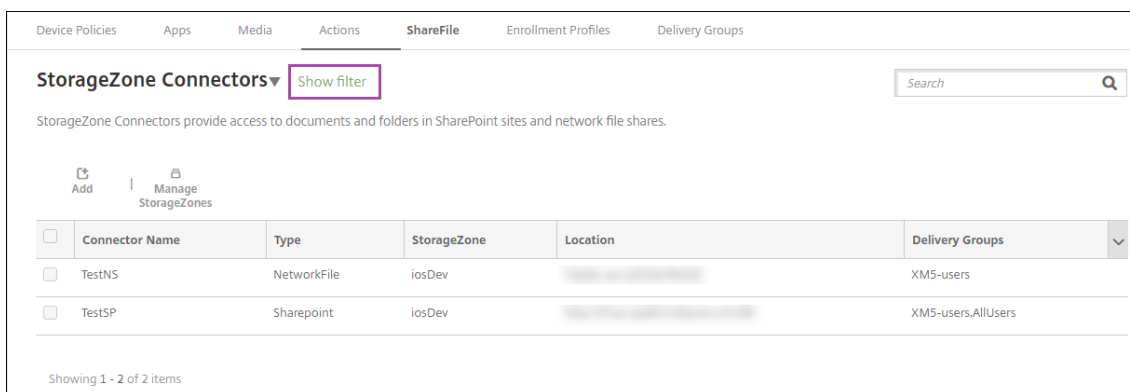


### **Filter the storage zone connectors list**

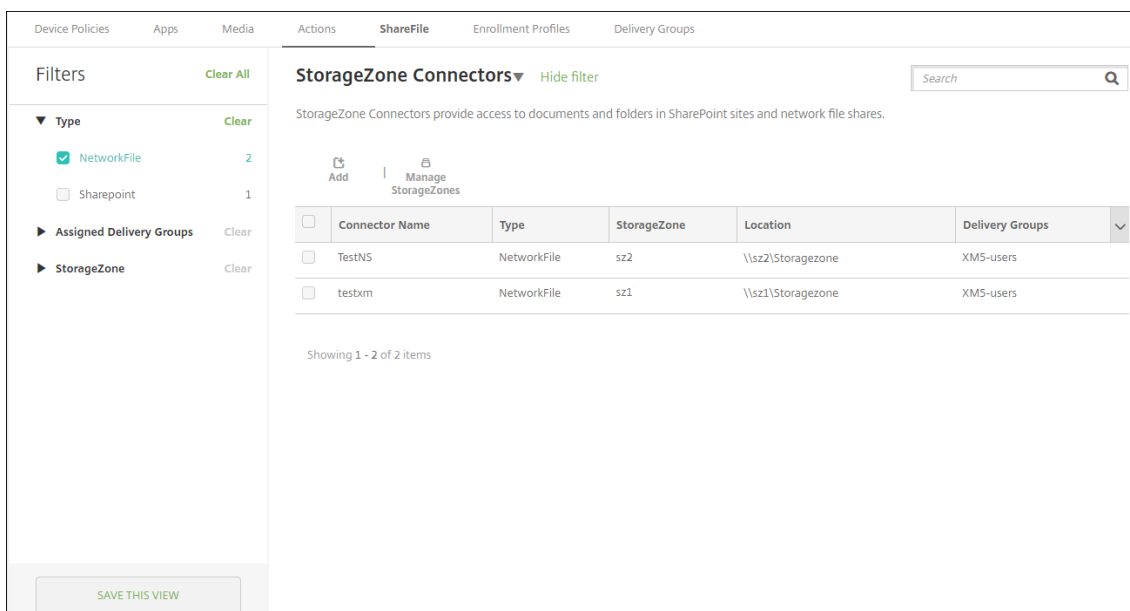
You can filter the list of storage zone connectors by connector type, assigned delivery groups, and storage zone.

1. Go to **Configure > Content Collaboration** and then click **Show filter**.

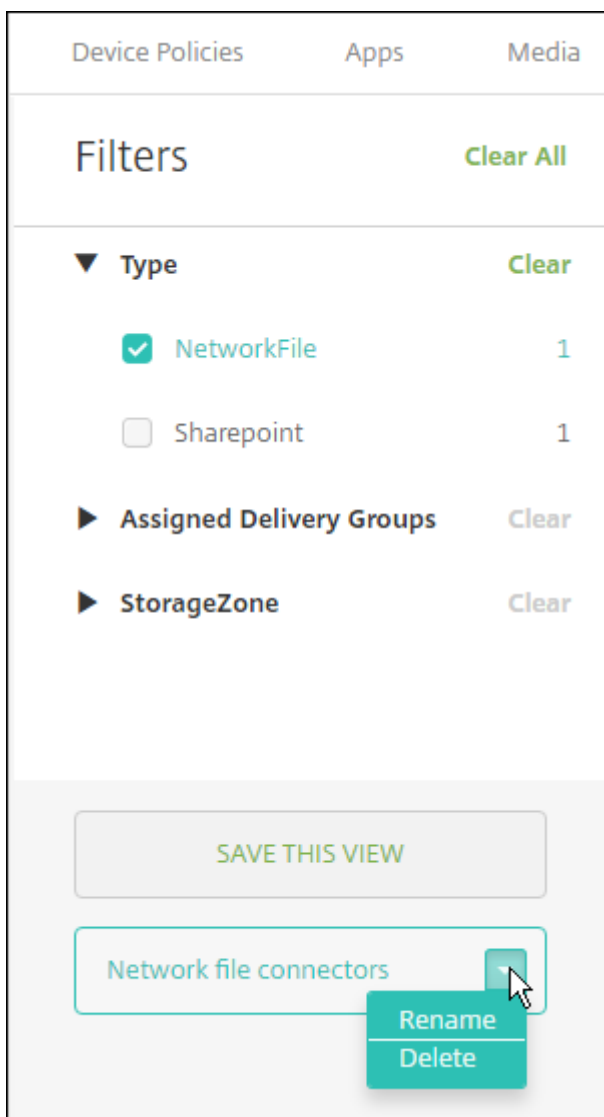




- Expand the filter headings to make selections. To save a filter, click **Save This View**, type the filter name, and click **Save**.



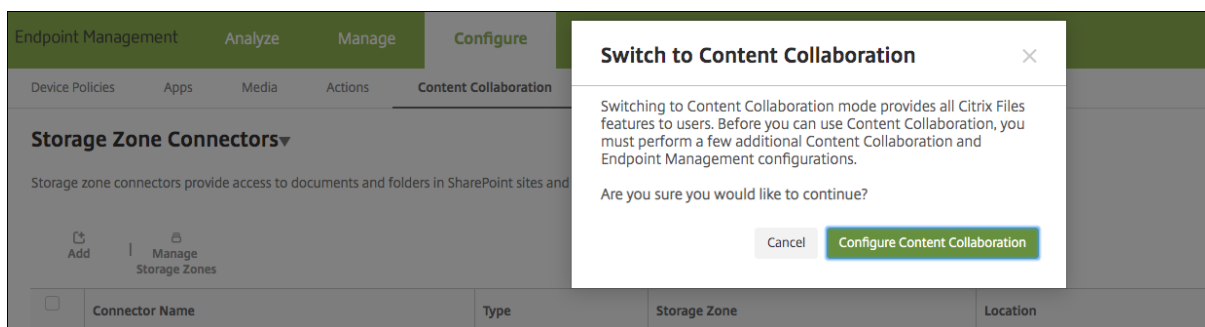
- To rename or delete a filter, click the arrow icon beside the filter name.



### Switch to Enterprise account

After integrating storage zone connectors with Endpoint Management, you can later switch to the full Enterprise feature set. Endpoint Management retains your existing storage zone connector integration settings.

Go to **Configure > Content Collaboration**, click the **Storage Zone Connectors** drop-down menu, and then click **Configure Content Collaboration**.



For information about configuring Enterprise accounts, see [SAML for single sign-on with Citrix Files](#).

## SmartAccess for HDX apps

March 25, 2021

This feature allows you to control access to HDX apps based on device properties, user properties of a device, or applications installed on a device. You use this feature by setting automated actions to mark the device as out of compliance to deny that device access. HDX apps used with this feature are configured in Citrix Virtual Apps and Desktops by using a SmartAccess policy that denies access to out-of-compliance devices. Endpoint Management communicates the status of the device to StoreFront using a signed, encrypted tag. StoreFront then allows or denies access based on the access control policy of the app.

To use this feature, your deployment requires:

- Citrix Virtual Apps and Desktops
- Citrix Endpoint Management
- Endpoint Management configured with a SAML certificate to be used for signing and encrypting tags. The same certificate without private key is uploaded on the StoreFront server.

To start using this feature:

- Configure the Endpoint Management server certificate to the StoreFront store
- Configure at least one Citrix Virtual Apps and Desktops delivery group with the required SmartAccess policy
- Set the automated action in Endpoint Management

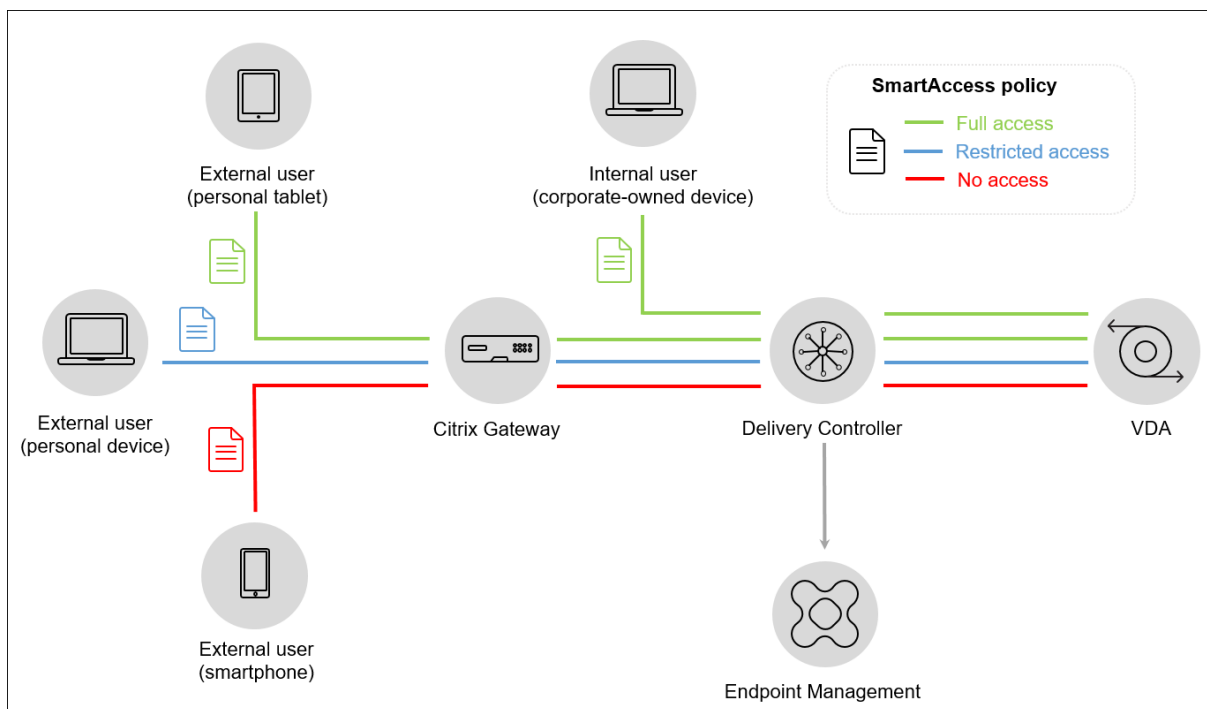
## SmartAccess to HDX apps for endpoints

With this feature, you can apply policy-based access control to restrict device access to HDX apps. You can apply these access levels to HDX apps:

- **Full access.** A device can access all HDX apps that the Secure Hub store provides.

- **Restricted access.** A device can access one or more but not all HDX apps.
- **No access.** A device cannot access any HDX apps.

The following graphic illustrates how access control works. An attempt to launch an HDX app in Secure Hub triggers a request to a Delivery Controller. The Delivery Controller then forwards the request to the Endpoint Management server for validation. The result of the validation determines the level of access the device has. For example, access to an HDX app is denied if the device is jailbroken.



## Export and configure the Endpoint Management server certificate and upload it to the StoreFront store

SmartAccess uses signed and encrypted tags to communicate between the Endpoint Management and StoreFront servers. To enable that communication, you add the Endpoint Management server certificate to the StoreFront store.

For more information about integrating StoreFront and Endpoint Management when Endpoint Management is enabled with domain and certificate-based authentication, see the [Support Knowledge Center](#).

## Export the SAML certificate from Endpoint Management

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears. Click **Certificates**.
2. Locate the SAML certificate for the Endpoint Management server.

Settings > Certificates

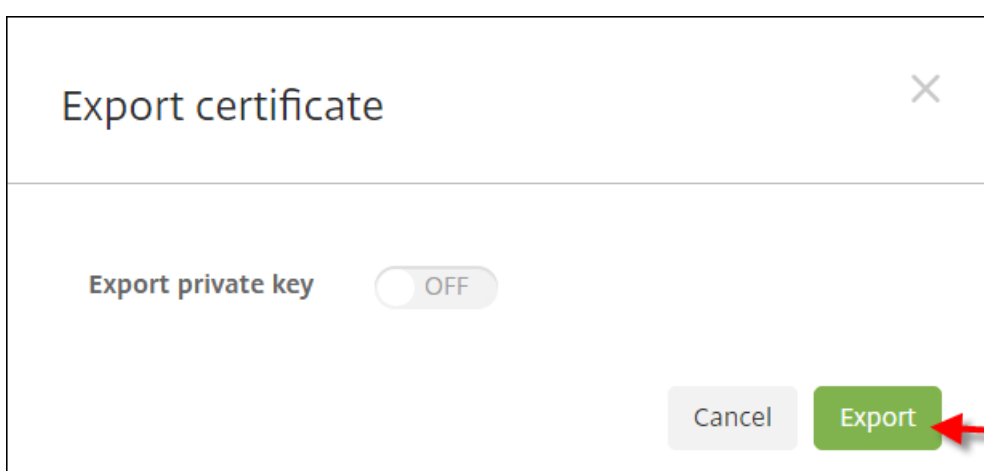
### Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

Import | Add | Detail | Export

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key
<input checked="" type="checkbox"/>	XMS.example.com	Self Signed/Generated	Up to date	2016-05-23	2026-05-21	SAML	✓
<input type="checkbox"/>	*.mpg.citrix.com		Up to date	2016-04-20	2017-05-27	SSL Listener	✓
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2016-05-23	2036-05-21	Devices CA	
<input type="checkbox"/>	Verizon Public SureServer CA G14-SHA2		Up to date	2014-04-09	2021-04-09	Root or intermediate	
<input type="checkbox"/>	Baltimore CyberTrust Root		Up to date	2000-05-12	2025-05-12	Root or intermediate	

3. Ensure that **Export private key** is set to **Off**. Click **Export** to export the certificate to your download directory.

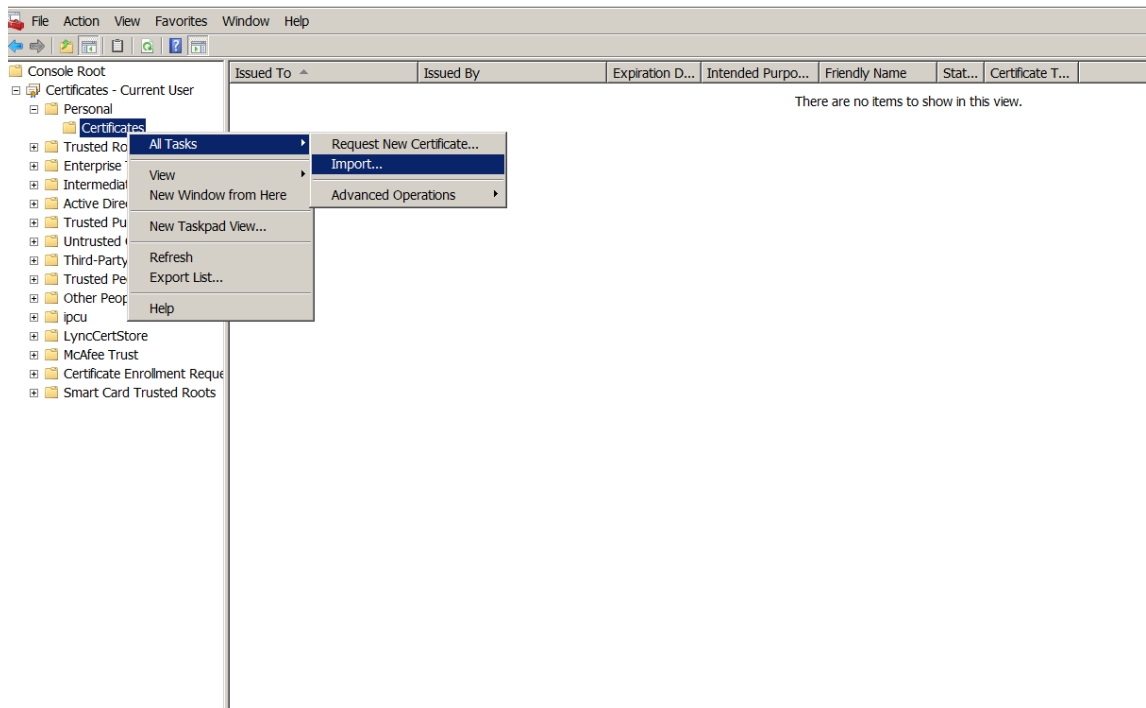


4. Locate the certificate in your download directory. The certificate is in PEM format.



### Convert the certificate from PEM to CER

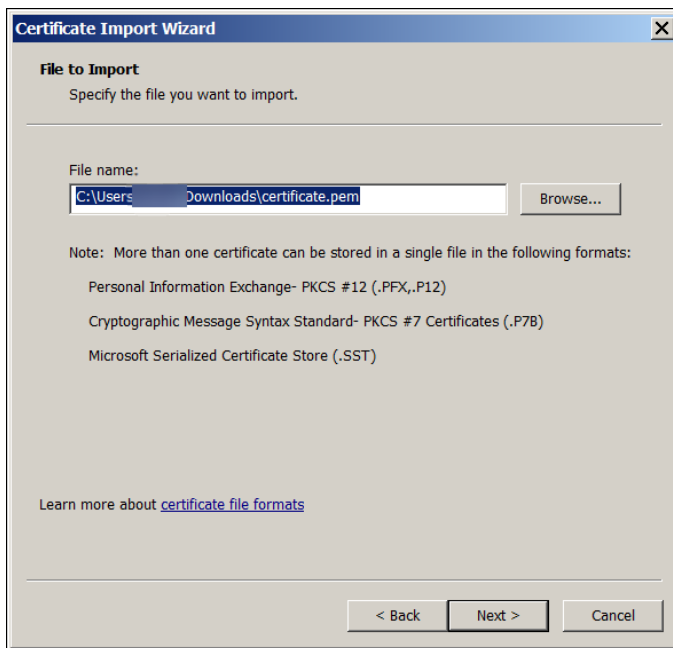
1. Open the Microsoft Management Console (MMC) and right-click **Certificates > All Tasks > Import**.



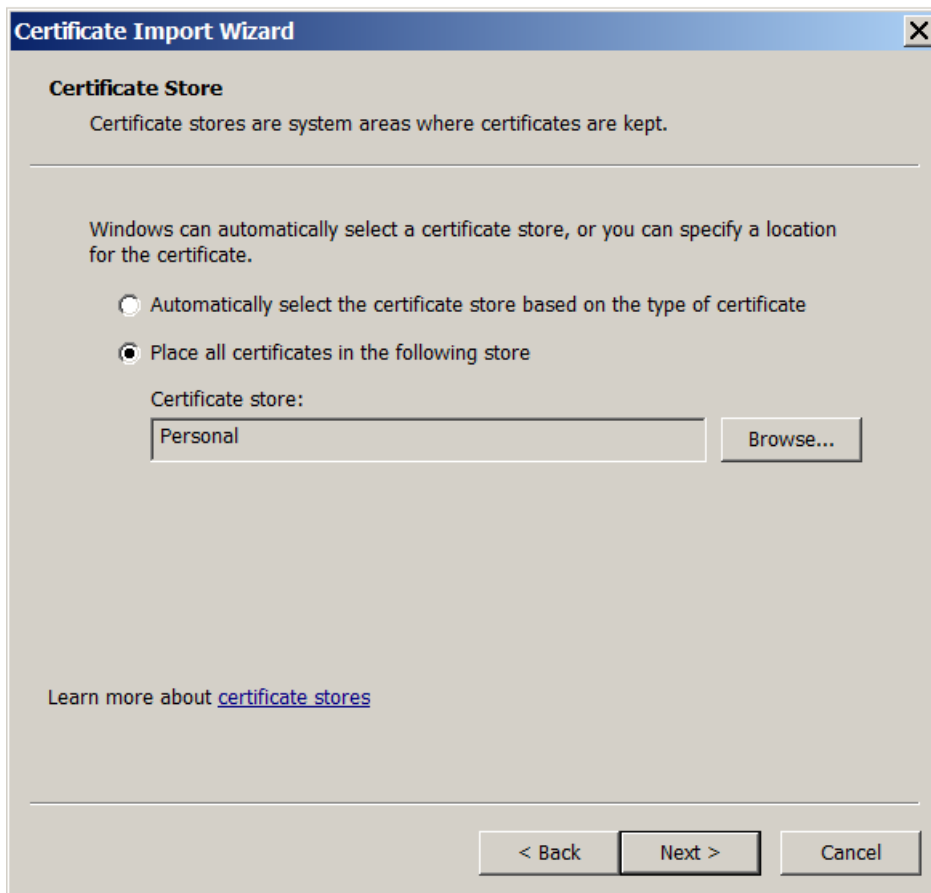
2. When the certificate import wizard appears, click **Next**.



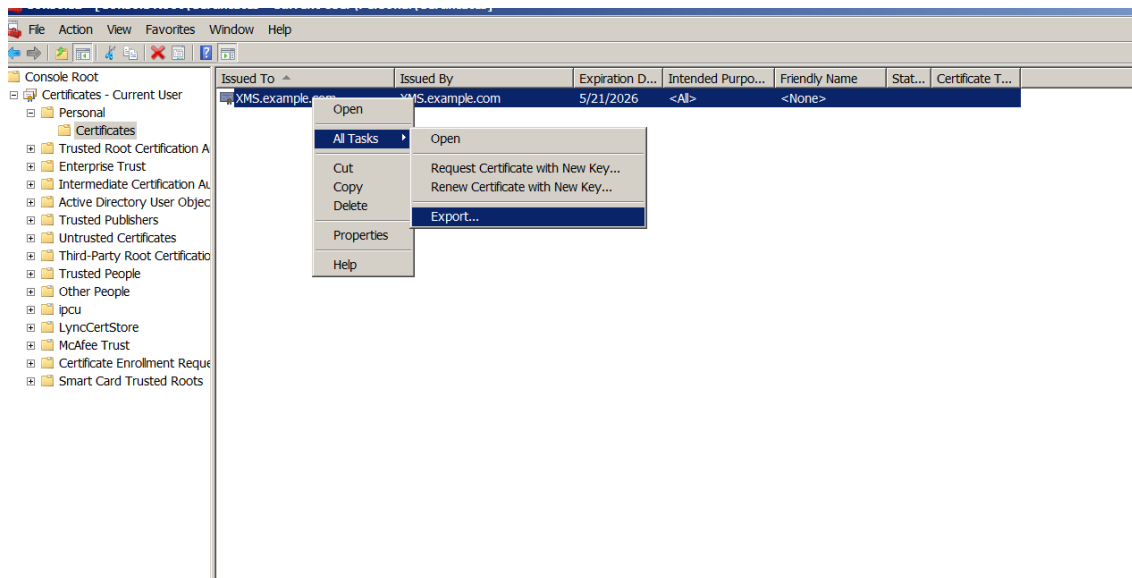
3. Browse to the certificate in the download directory.



4. Select **Place all certificates in the following store** and select **Personal** as the certificate store. Click **Next**.



5. Review your selections and click **Finish**. Click **OK** to dismiss the confirmation window.
6. In the MMC, right-click the certificate and then choose **All Tasks > Export**.

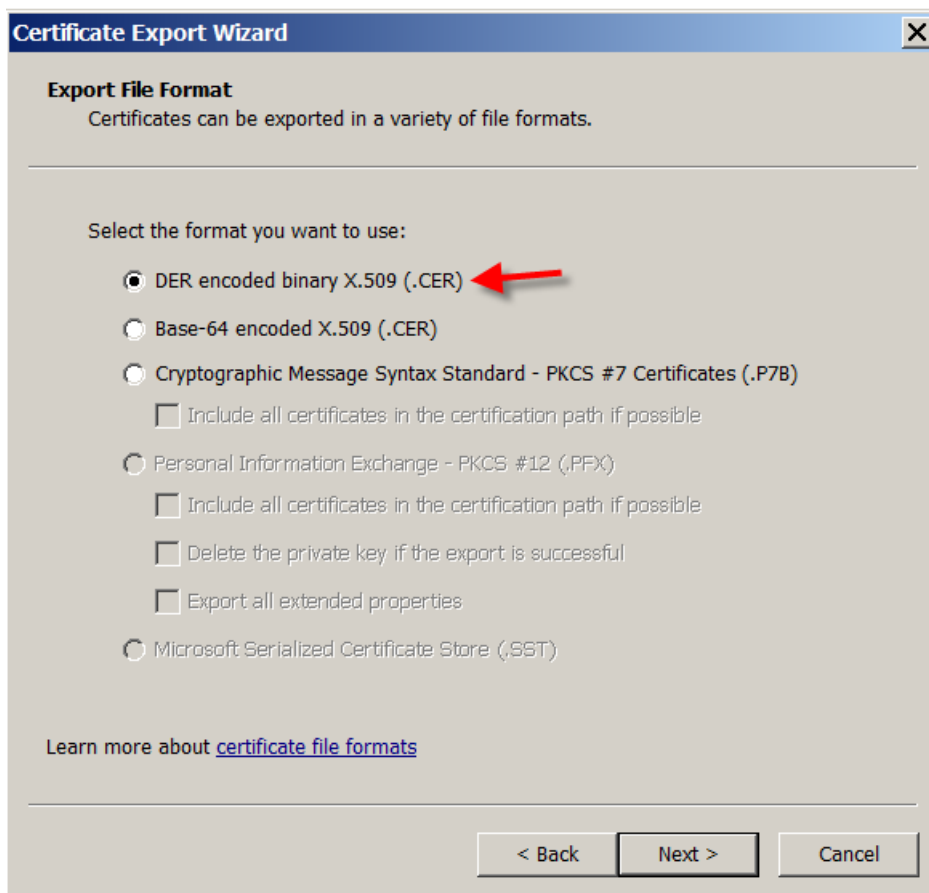


7. When the certificate export wizard appears, click **Next**.

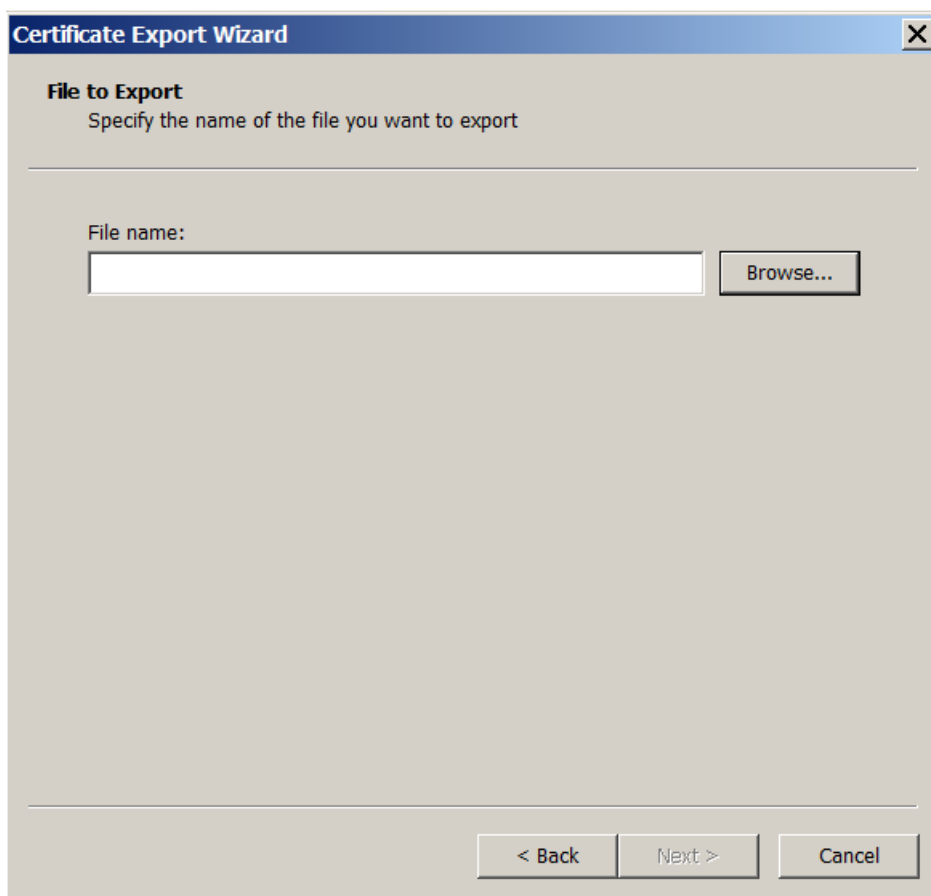




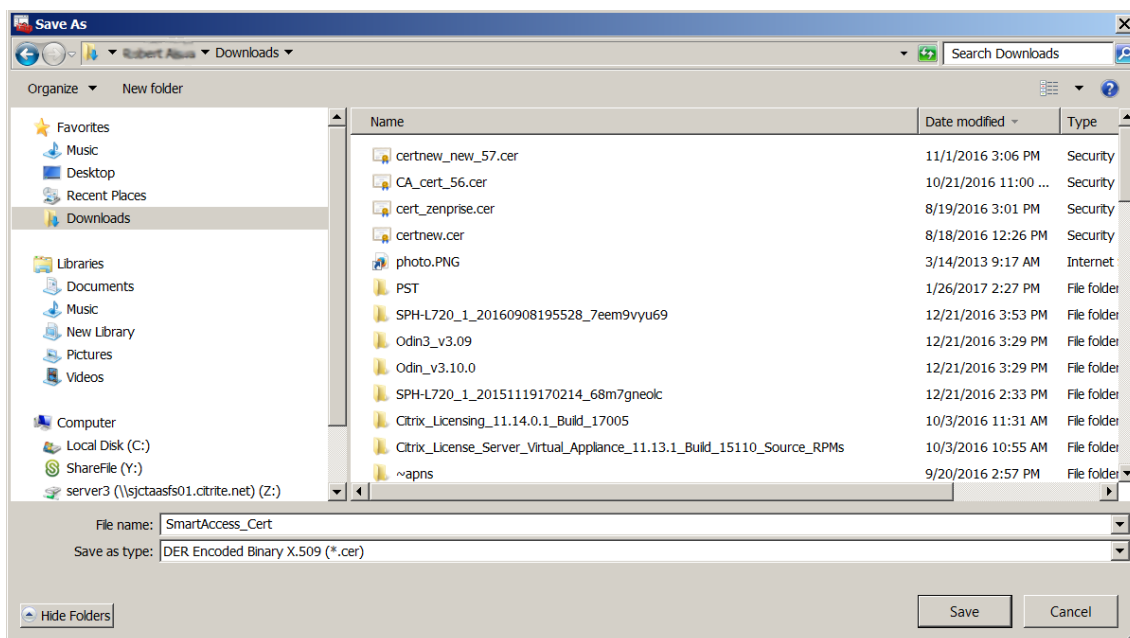
8. Choose the format **DER encoded binary X.509 (.CER)**. Click **Next**.



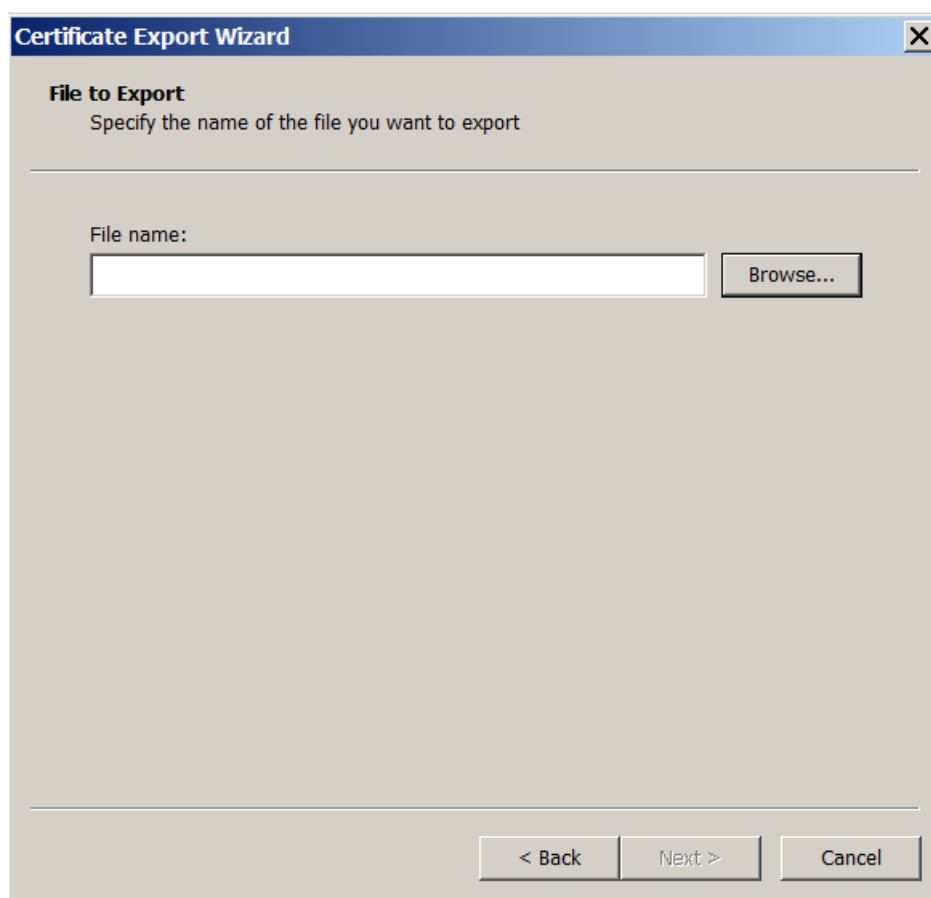
9. Browse to the certificate. Type a name for the certificate and then click **Next**.



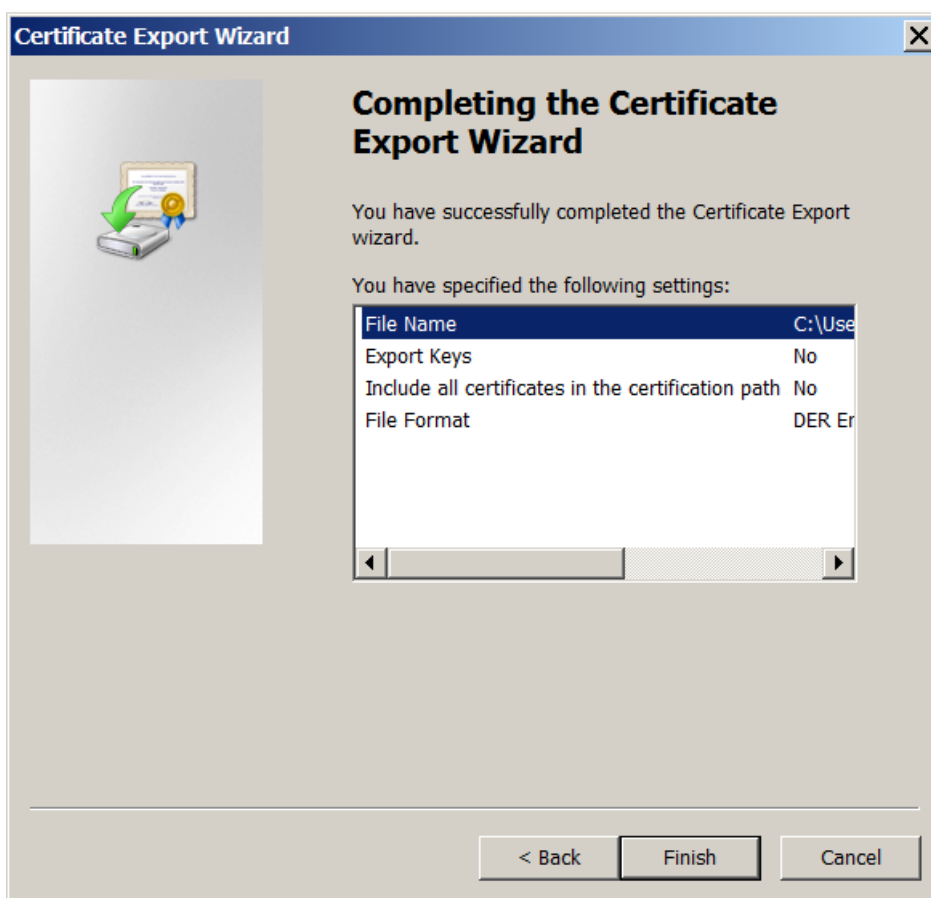
10. Save the certificate.



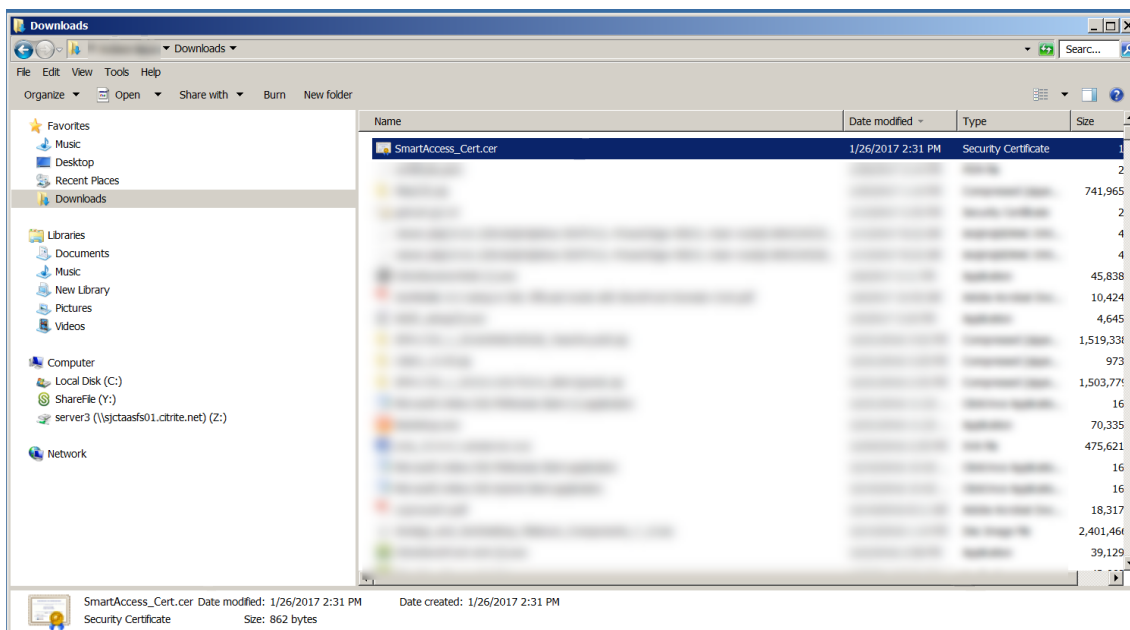
11. Browse to the certificate and click **Next**.



12. Review your selections and click **Finish**. Click **OK** to dismiss the confirmation window.

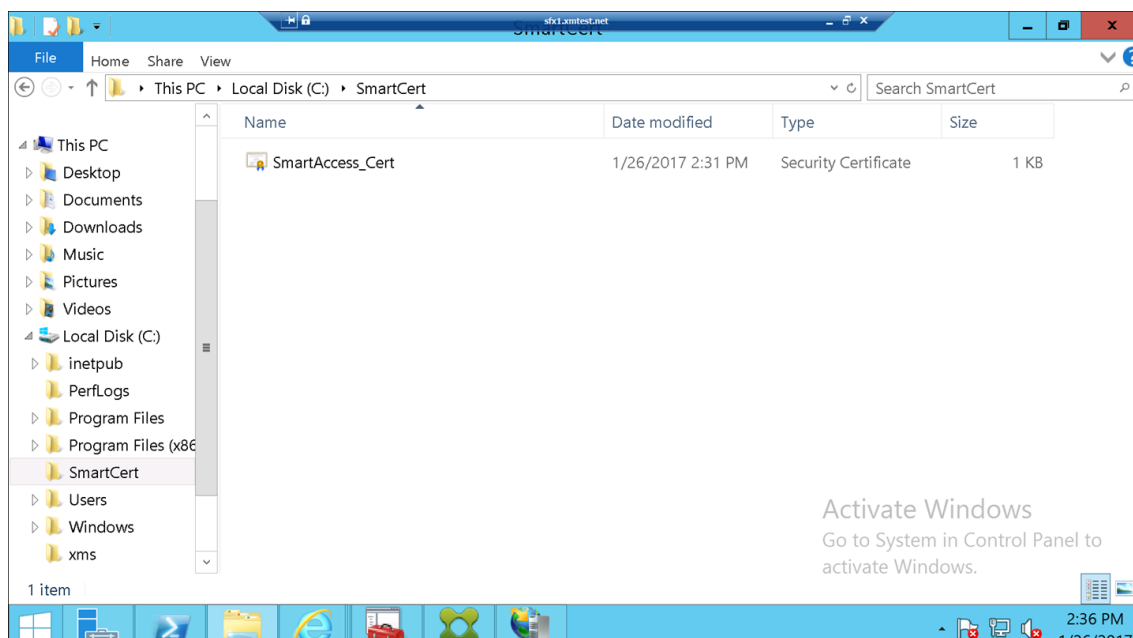


13. Locate the certificate in your download directory. Note that the certificate is in CER format.



## Copy the certificate to the StoreFront Server

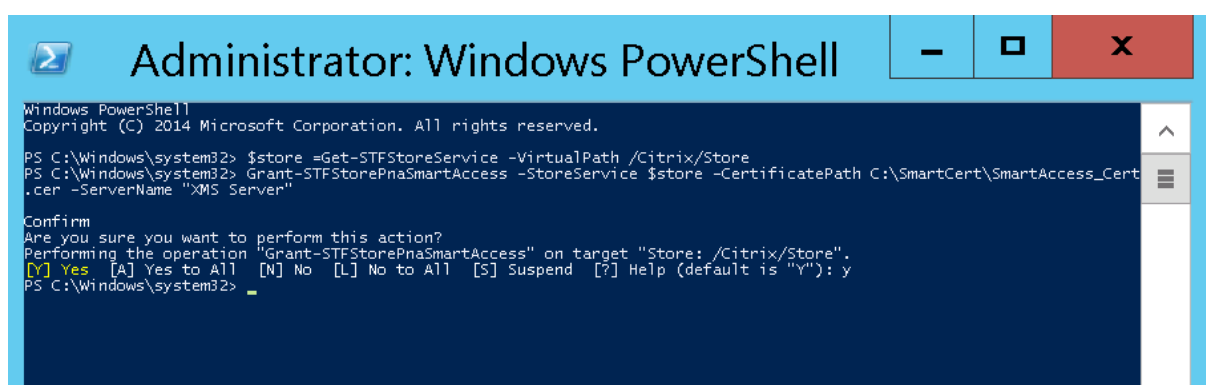
1. On the StoreFront server, create a folder called **SmartCert**.
2. Copy the certificate to the **SmartCert** folder.



## Configure the certificate on the StoreFront store

On the StoreFront server, run this PowerShell command to configure the converted Endpoint Management server certificate on the store:

```
1 Grant-STFStorePnaSmartAccess - StoreService $store -
   CertificatePath "C:\xms\xms.cer" - ServerName "XMS server"
2 <!--NeedCopy-->
```



If there are any existing certificates on the StoreFront store, run this PowerShell command to revoke them:

```
1 Revoke-STFStorePnaSmartAccess - StoreService $store - All
2 <!--NeedCopy-->
```

Alternatively, you can run any of these PowerShell commands on the StoreFront server to revoke existing certificates on the StoreFront store:

- Revoke by name:

```
1 $store = Get-STFStoreService - VirtualPath /Citrix/Store
2
3 Revoke-STFStorePnaSmartAccess - StoreService $store - ServerName "
  My XM Server"
4 <!--NeedCopy-->
```

- Revoke by thumbprint:

```
1 $store = Get-STFStoreService - VirtualPath /Citrix/Store
2
3 Revoke-STFStorePnaSmartAccess - StoreService $store -
  CertificateThumbprint "[Thumbprint]"
4 <!--NeedCopy-->
```

- Revoke by server object:

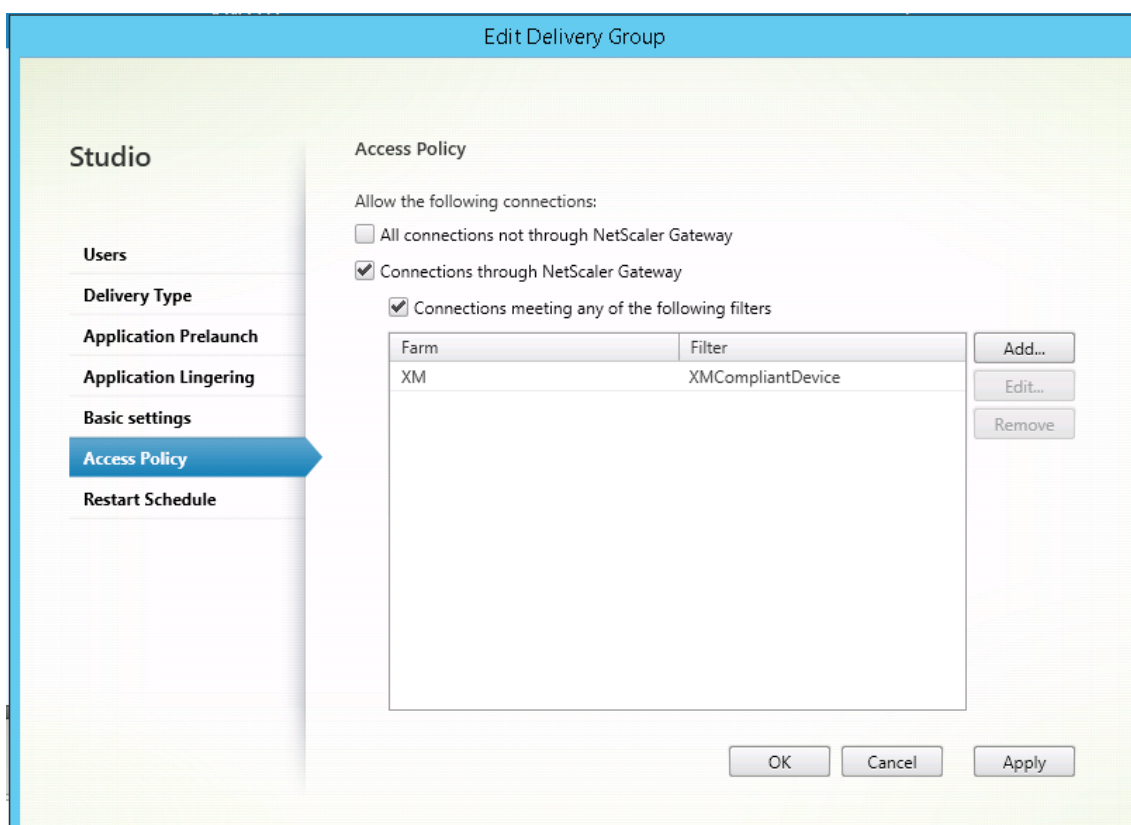
```
1 $store = Get-STFStoreService - VirtualPath /Citrix/Store
2
3 $access = Get-STFStorePnaSmartAccess - StoreService $store
4
5 Revoke-STFStorePnaSmartAccess - StoreService $store - SmartAccess
  $access.AccessConditionsTrusts[0]
6 <!--NeedCopy-->
```

## Configure the SmartAccess policy for Citrix Virtual Apps and Desktops

To add the required SmartAccess policy to the delivery group delivering the HDX app:

1. Open Citrix Studio from the Citrix Cloud console.
2. Select **Delivery Groups** in the Studio navigation pane.

3. Select a group delivering the app or apps you want to control access to. Then select **Edit Delivery Group** in the **Actions** pane.
4. On the **Access Policy** page, select **Connections through Citrix Gateway** and **Connection meeting any of the following**.
5. Click **Add**.
6. Add an access policy where **Farm** is **XM** and **Filter** is **XMCompliantDevice**.



7. Click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

## Set automated actions in Endpoint Management

The SmartAccess policy that you set in the delivery group for an HDX app denies access to a device when the device is out of compliance. Use automated actions to mark the device as out of compliance.

Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	Out of Compliance
<input type="checkbox"/>	MDM   MAM	[Redacted]	iOS	8.1	iPad	06/29/2016 10:37:56 am	212 days	
<input type="checkbox"/>	MDM   MAM	[Redacted]	iOS	10.2	iPhone	01/27/2017 10:10:59 am	0 day	True

1. From the Endpoint Management console, click **Configure > Actions**. The **Actions** page appears.
2. Click **Add** to add an action. The **Action Information** page appears.
3. On the **Action Information** page, type a name and description for the action.
4. Click **Next**. The **Action details** page appears. In the following example, a trigger is created that immediately marks devices as out of compliance if they have the user property name **eng5** or **eng6**.

**Action details**

Choose a trigger event and the associated action for that event.

**Trigger\***

User property

Name

Is

eng5 eng6

**Action\***

Mark the device as out of compliance

Is

True

0

Hours

5. In the **Trigger** list, choose **Device property**, **User property**, or **Installed app name**. SmartAccess doesn't support event triggers.
6. In the **Action** list:
  - Choose **Mark the device as out of compliance**.
  - Choose **Is**.
  - Choose **True**.
  - To set the action to mark the device as out of compliance immediately when the trigger condition is met, set the time frame to **0**.
7. Choose the Endpoint Management delivery group or groups to apply this action to.

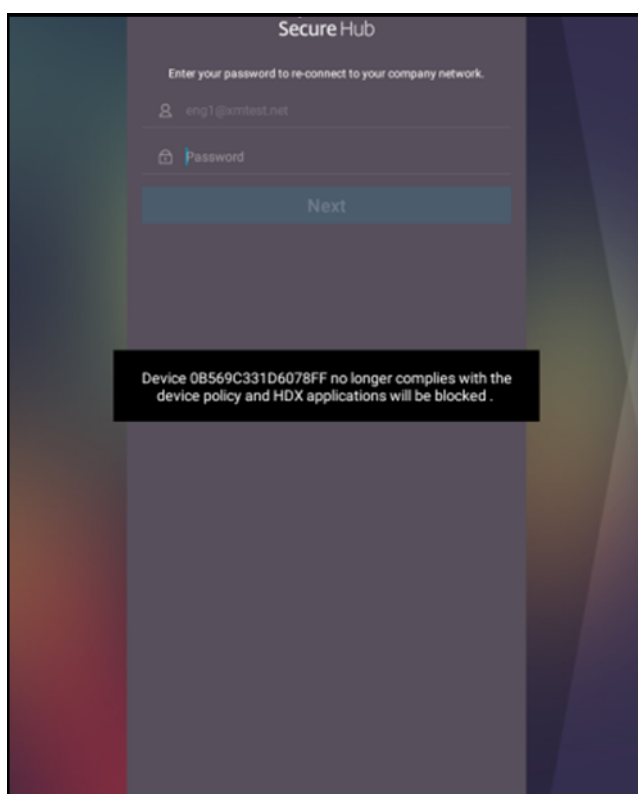


8. Review the summary of the action.
9. Click **Next** and then click **Save**.

When device is marked out of compliance, the HDX apps no longer appear in the Secure Hub store. The user is no longer subscribed to the apps. No notification is sent to the device and nothing in the Secure Hub store indicates that the HDX apps were previously available.

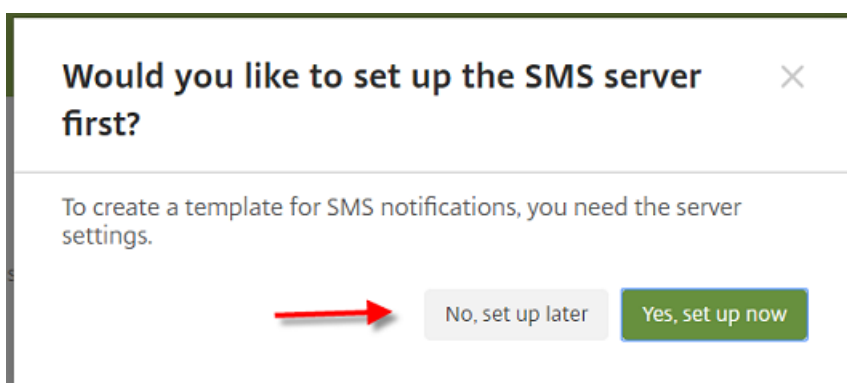
If you want users to be notified when a device is marked out of compliance, create a notification and then create an automated action to send that notification.

This example creates and sends this notification when a device is marked out of compliance: “Device serial number or telephone number no longer complies with the device policy and HDX applications will be blocked.”



### Create the notification users see when a device is marked as out of compliance

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Click **Notification Templates**. The **Notification Templates** page appears.
3. Click **Add** to add on the **Notification Templates** page.
4. When prompted to set up the SMS server first, click **No, set up later**.



5. Configure these settings:

- **Name:** HDX Application Block
- **Description:** Agent notification when device is out of compliance
- **Type:** Ad Hoc Notification
- **Secure Hub:** Activated
- **Message:** Device `${ firstnotnull(device.TEL_NUMBER,device.serialNumber) }` no longer complies with the device policy and HDX applications will be blocked.

6. Click **Save**.

## Create the action that sends the notification when a device is marked out of compliance

1. From the Endpoint Management console, click **Configure > Actions**. The **Actions** page appears.

2. Click **Add** to add an action. The **Action Information** page appears.
3. On the **Action Information** page, enter a name and description for the action:
  - Name: HDX blocked notification
  - **Description:** HDX blocked notification because device is out of compliance
4. Click **Next**. The **Action details** page appears.
5. In the **Trigger** list:
  - Choose **Device property**.
  - Choose **Out of compliance**.
  - Choose **Is**.
  - Choose **True**.

The screenshot shows the 'Action Information' page in Citrix Endpoint Management. The page is titled 'Action Information' and has a navigation menu on the left with options: 1 Action Info, 2 Details (selected), 3 Assignment (optional), and 4 Summary. The main content area is divided into two sections: 'Trigger' and 'Action'. The 'Trigger' section has four dropdown menus: 'Device property', 'Out of compliance', 'Is', and 'True'. The 'Action' section has a dropdown menu for 'Send notification', a dropdown menu for 'HDX Application Block', a text input field for 'Preview notification message' containing '0', a dropdown menu for 'Minutes', a text input field for 'Specify an action repeat interval', and a dropdown menu for 'Days'. At the bottom right, there are 'Back' and 'Next >' buttons.

6. In the **Action** list, specify the actions that occur when the trigger is met:
  - Choose **Send notification**
  - Choose **HDX Application Block, the notification you created**.
  - Choose **0**. Setting this value to 0 causes the notification to be sent as soon as the trigger condition is met.
7. Select the Endpoint Management delivery group or groups to apply this action to. In this example, choose **AllUsers**.
8. Review the summary of the action.
9. Click **Next** and then click **Save**.

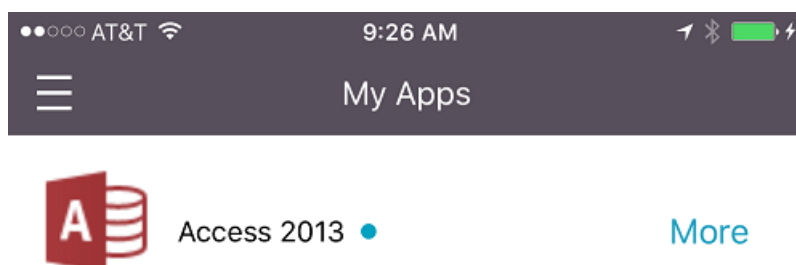
For more information on setting automated actions, see [Automated actions](#).

## How users regain access to HDX apps

Users can gain access to HDX apps again after the device is brought back into compliance:

1. On the device, go to the Secure Hub store to refresh the apps in the store.
2. Go to the app and tap **Add** to the app.

After the app is added, it appears in My Apps with a blue dot next to it, because it is a newly installed app.



## Upgrade MDX or enterprise apps

April 27, 2021

To upgrade an MDX or Enterprise app in Endpoint Management, disable the app in the Endpoint Management console, and then upload the new version of the app.

1. In the Endpoint Management console, click **Configure > Apps**. The **Apps** page appears.
2. For managed devices (devices enrolled in Endpoint Management for mobile device management), skip to Step 3. For unmanaged devices (devices enrolled in Endpoint Management for enterprise app management purposes only), do the following:
  - a) In the **Apps** table, select the check box next to the app or click the line containing the app you want to update.

- b) Click **Disable** in the menu that appears.

The screenshot shows the 'Apps' management interface. A table lists several applications, with 'Secure Web' highlighted. A context menu is open over the 'Secure Web' row, showing options: Edit, Disable, Category, and Delete. Below the menu, a 'Deployment' summary is displayed with three status boxes: 'Installed' (0), 'Pending' (0), and 'Failed' (0). A 'Show more >' link is at the bottom of the summary.

Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input checked="" type="checkbox"/>	Secure Web	MDX	Default	4/3/20 9:42:58 am	4/3/20 9:43:04 am	
<input type="checkbox"/>	Secure Mail	MDX	Default			
<input type="checkbox"/>	Citrix Files	MDX	Default			
<input type="checkbox"/>	AE App add	Public App Store	Default			
<input type="checkbox"/>	AE google chrome	Public App Store	Default			
<input type="checkbox"/>	Podio	Public App Store	Default			
<input type="checkbox"/>	AE App	Public App Store	Default			

- c) Click **Disable** in the confirmation dialog box. *Disabled* appears in the **Disable** column for the app.

Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>	Secure Web	MDX	Default	4/3/20 9:42:58 am	4/3/20 9:43:04 am	Disabled
<input type="checkbox"/>	Secure Mail	MDX	Default	4/3/20 9:43:09 am	4/3/20 9:43:16 am	

**Note:**

While the app is disabled, users can't reconnect to the app after they log off. Disabling an app is optional, but we recommend disabling the app to avoid app functionality issues. For example, users requesting to download the app at the same time you upload the new version might result in an issue.

- In the **Apps** table, click the check box next to the app or click the line containing the app you want to update.
- Click **Edit** in the menu that appears. The **App Information** page appears with the platforms you originally chose for the app selected.
- Configure these settings:
  - **Name:** Optionally, change the app name.
  - **Description:** Optionally, change the app description.
  - **App category:** Optionally, change the app category.
- Click **Next**. The first selected platform page appears. Do the following for each selected platform:
  - Choose the replacement file you want to upload by clicking **Upload** and navigating to the file location. The app uploads to Endpoint Management.

If you're uploading an app for Android Enterprise, a managed Google Play window appears. Upload the new version of the app here. For more details, see [Distribute Android Enterprise and Android for Workspace apps](#).

- b) Optionally, change the app details and policy settings for the platform.
  - c) Optionally, configure deployment rules and the app store. For information, see [Add an MDX app](#).
7. Click **Save**. The **Apps** page appears.
  8. If you disabled the app in Step 2, do the following:
    - a) In the **Apps** table, click to select the app you updated and then in the menu that appears, click **Enable**.
    - b) In the confirmation dialog box that appears, click **Enable**. Users can now access the app and receive a notification prompting them to upgrade the app.

## Add media

April 3, 2020

You add media to Endpoint Management so you can deploy the media to user devices. You can use Endpoint Management to deploy Apple Books that you obtain through Apple volume purchase.

After you configure a volume purchase account in Endpoint Management, your purchased and free books appear in **Configure > Media**. From the **Media** pages, you configure books for deployment to iOS devices by choosing delivery groups and specifying deployment rules.







The first time that a user receives a book and accepts the volume purchase license, deployed books install on the device. The books appear in the Apple Book app. You can't disassociate the book license from the user or remove the book from the device. Endpoint Management installs books as required media. If a user deletes an installed book from their device, the book remains in the Apple Book app, ready for download.

### Prerequisites

- iOS devices
- Configure Apple volume purchase in Endpoint Management, as described in [Apple Volume Purchase](#).

## Configure books

Apple Books obtained through volume purchase appear on the **Configure > Media** page.

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<b>Media</b> <a href="#">Show filter</a> <input type="text" value="Search"/>						
<input type="checkbox"/>	Icon	Media Name	Type	Created On	Last Updated	Vpp Account
<input type="checkbox"/>		The Wonderful Wizard of Oz - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:41 PM	test
<input type="checkbox"/>		Cool Werewolf Jokes For Kids - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:28 PM	test
<input type="checkbox"/>		Science Fiction Stories - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:32 PM	test
<input type="checkbox"/>		Coming Out - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:45 AM	test
<input type="checkbox"/>		Short Stories - VPP	Apple iBooks	6/15/17 1:29 PM	6/15/17 1:29 PM	test
<input type="checkbox"/>		A Diamond in My Pocket - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:39 AM	test
Showing 1 - 6 of 6 items    Items per page: <input type="text" value="10"/>						

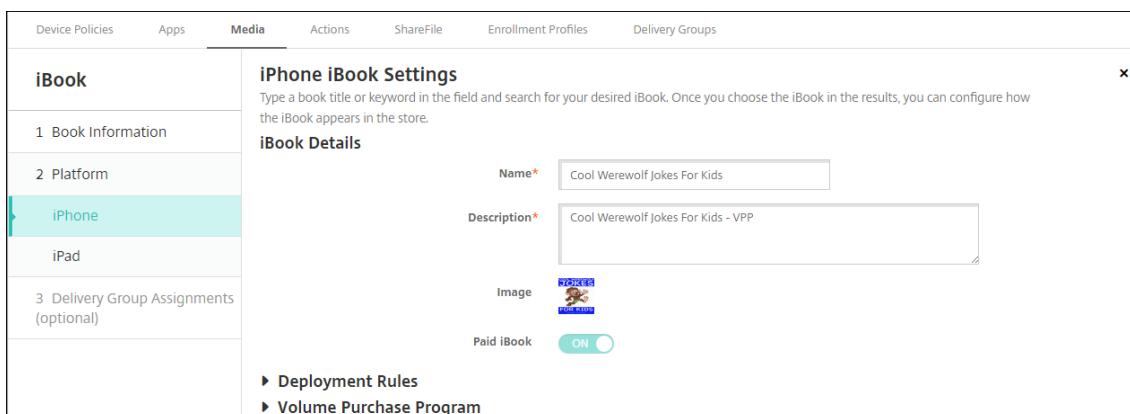
## To configure an Apple Book for deployment

1. In **Configure > Media**, select a book and click **Edit**. The **Book Information** page appears.

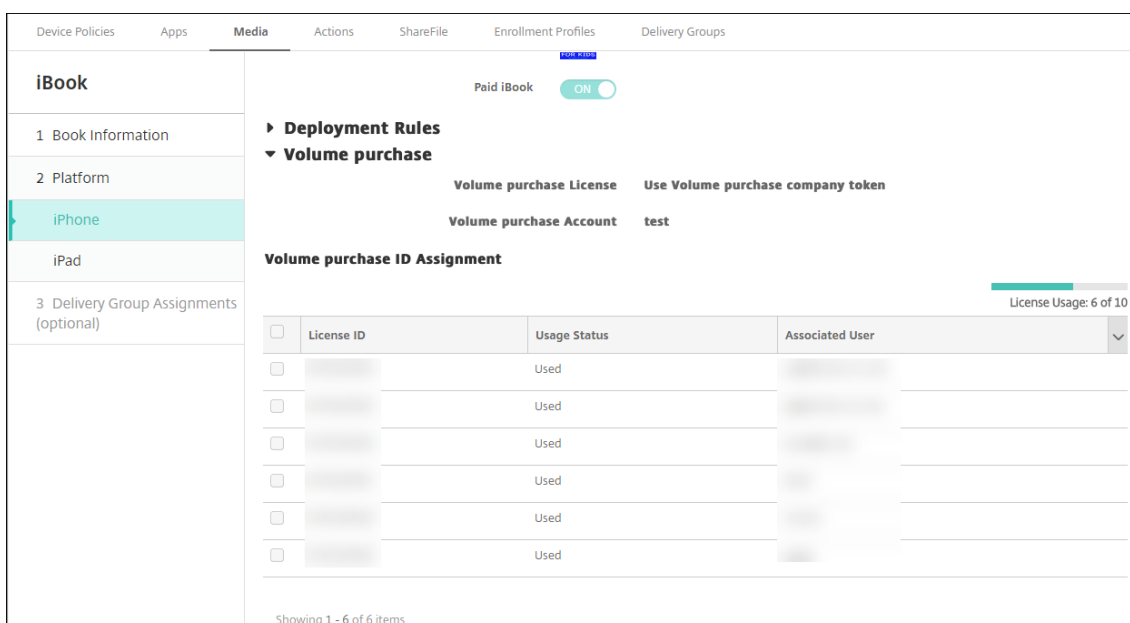
Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<b>iBook</b> <b>Book Information</b> <span>✕</span>						
<div style="display: flex;"> <div style="width: 20%; border-right: 1px solid #ccc; padding-right: 5px;"> <ul style="list-style-type: none"> <li style="background-color: #e0f2f1; padding: 5px;">1 Book Information</li> <li style="padding: 5px;">2 Platform</li> <li style="padding: 5px;">iPhone</li> <li style="padding: 5px;">iPad</li> <li style="padding: 5px;">3 Delivery Group Assignments (optional)</li> </ul> </div> <div style="width: 80%; padding-left: 10px;"> <p><b>Name*</b> <input type="text" value="Cool Werewolf Jokes For Kids - VPP"/> ⓘ</p> <p><b>Description</b> <input type="text" value="Cool Werewolf Jokes For Kids - VPP"/> ⓘ</p> </div> </div>						

The **Name** and **Description** appear only in the Endpoint Management console and logs.

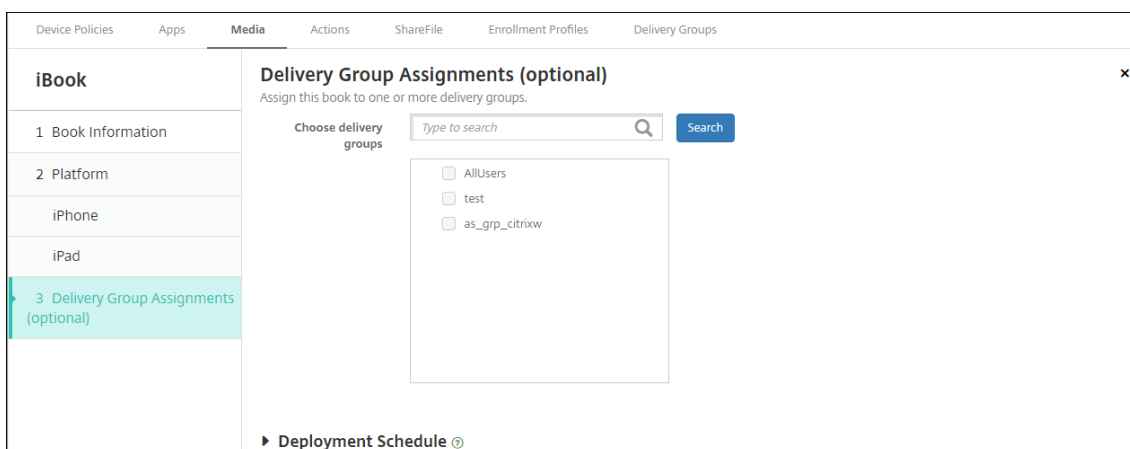
2. In the **iPhone iBook Settings** and **iPad iBook Settings** pages: While you can optionally change the book name and description, Citrix recommends that you don't change these settings. The image is for your information and isn't editable. **Paid iBook** indicates that a book is purchased through Apple volume purchase.



You can also specify deployment rules or view volume purchase information.



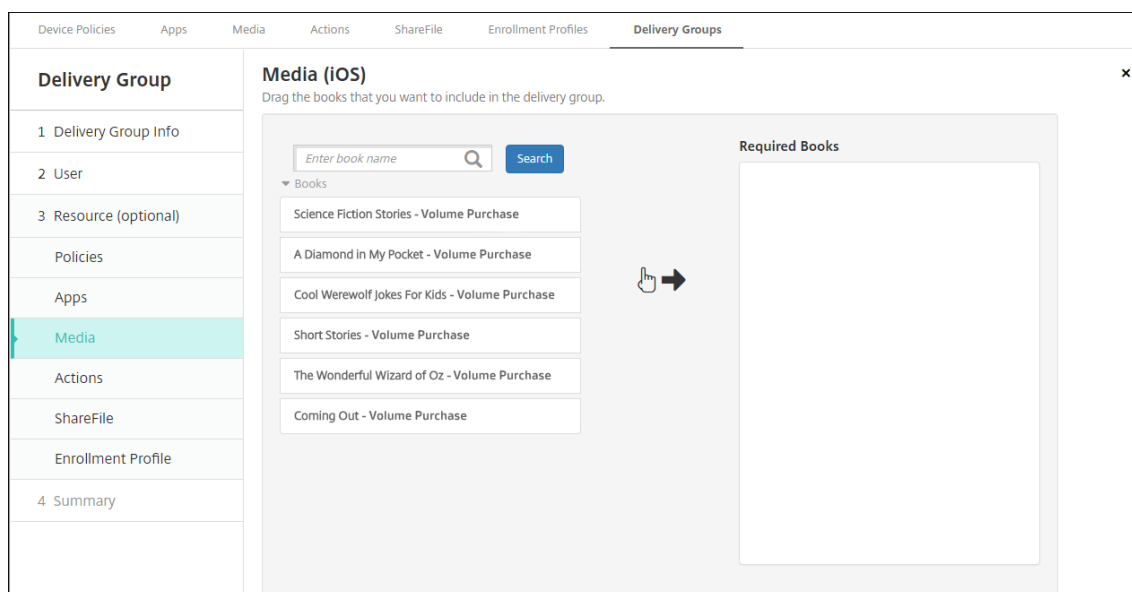
3. Optionally, assign the book to delivery groups and set a deployment schedule.



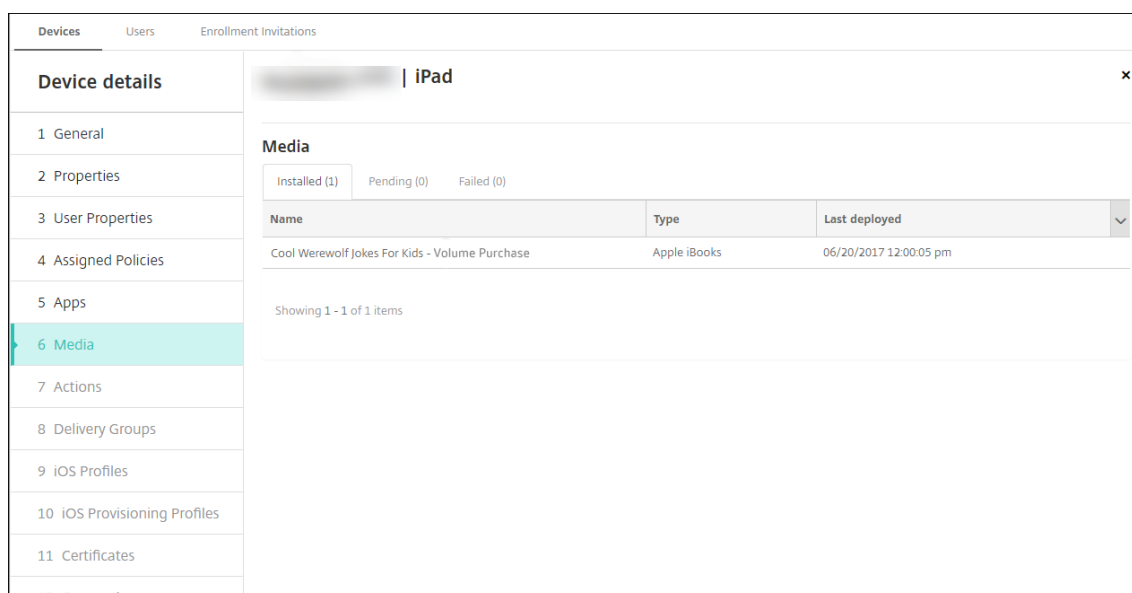
You can also assign books to delivery groups from the **Media** tab for **Configure > Delivery**



**Groups.** Endpoint Management supports required book deployment only.



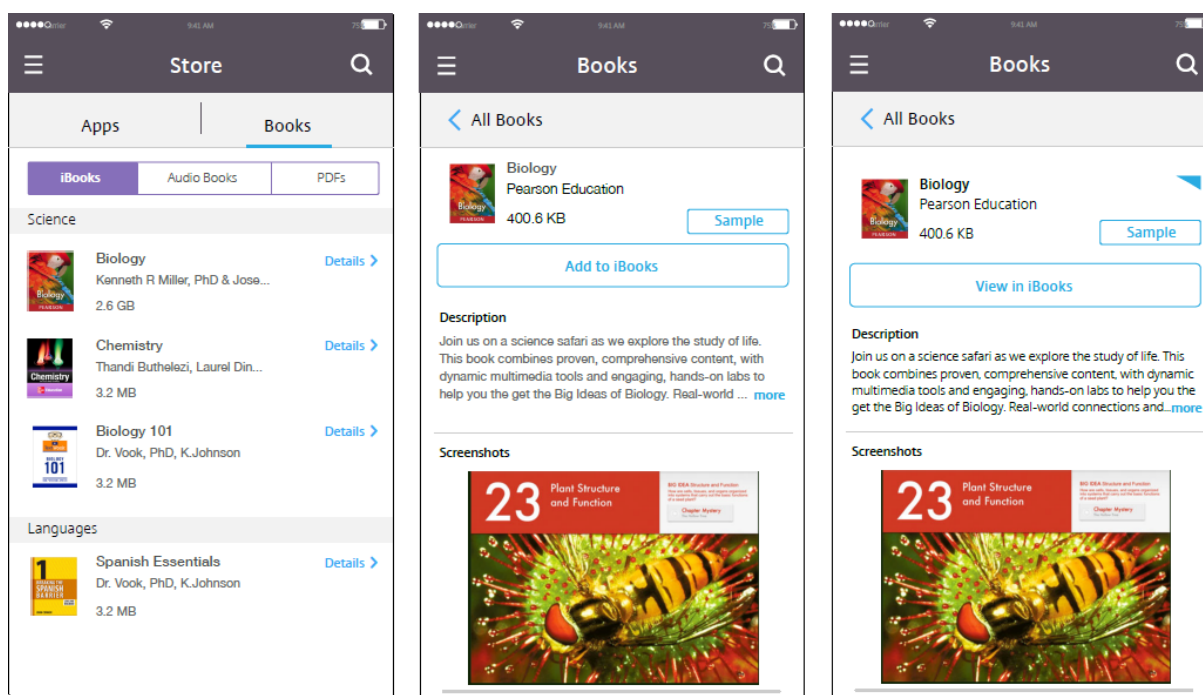
4. Use the **Media** tab for **Manage > Devices** to view deployment status.



**Note:**

On the **Configure > Media** page, if you select a book and click **Delete**, Endpoint Management removes the book from the list. However, the next time Endpoint Management syncs with Apple volume purchase, the book reappears on the list unless it has been removed from Apple volume purchase. Deleting a book from the list doesn't remove the book from devices.

Books appear on user devices as shown in the following example.



## Deploy resources

July 27, 2021

Device configuration and management typically involve creating resources (policies, apps, and media) and actions in the Endpoint Management console and then packaging them using delivery groups. Delivery groups define categories of users so you can deploy specified policies, apps, media, and actions to their devices. Using the Endpoint Management console, you can:

- Add, manage, and deploy delivery groups.
- Change the order in which Endpoint Management pushes resources and actions in a delivery group to devices. This order is called the *deployment order*.

You can specify deployment order in the Endpoint Management console. However, when a user is in multiple delivery groups that have duplicate or conflicting policies, Endpoint Management determines deployment order. See Calculation steps.

## About delivery groups

Inclusion in a delivery group is typically based on user characteristics, such as company, country, department, office address, and title. Delivery groups give you greater control over who gets which resources and when they get them. You can deploy a delivery group to all users or to a defined group of users.

Installing and configuring Endpoint Management creates the default delivery group, AllUsers. This group contains all local and Active Directory users. You can't delete the AllUsers group, but you can disable it when you don't want to push resources to all users. For details, see [Enable and disable the AllUsers delivery group](#).

When you deploy a resource to a delivery group, you send a push notification to all users in the delivery group. For Apple devices, use Apple Push Notification service (APNs) to send notifications. For more information see [APNs certificates](#)). For Android devices, use Firebase Cloud Messaging (FCM). For more information, see [Firebase Cloud Messaging](#). For Windows devices, use Windows Push Notification Service (WNS).

## About deploying resources

When you work on pushing resources to devices, consider:

- **Deployment order:** Deployment order is the sequence in which Endpoint Management pushes resources (policies, apps, and media) and actions to a device. Deployment order applies to devices in a delivery group with an enrollment profile configured for device management (MDM) or for a combination of application management (MAM) and MDM.
- **Deployment rules:** Endpoint Management uses deployment rules that you specify for user and device properties to filter policies, apps, media, actions, and delivery groups. For example, a deployment rule might specify to push the deployment package when a domain name matches a particular value.

Within a delivery group, you can specify a subset of users and devices that receive the resources based on their user and device properties. User and device property filtering within a delivery group takes precedence over deployment rules set on the resource.

- **Deployment schedule:** Endpoint Management uses the deployment schedule that you specify for policies, apps, media, and actions to control deployment of those items. You can specify that a deployment occurs now, on a set date and time, or when deployment conditions are met. You specify the schedule when you create the rule. See [Configure deployment rules](#).

Before adding delivery groups, consider how deployment order, rules, and schedule relate to your deployment goals.

## Deployment order

Deployment order is the sequence in which Endpoint Management pushes resources to devices. Deployment order is important when there are prerequisites for resources and dependencies between resources. Resources include policies, apps, actions, and delivery groups.

For example, if you're pushing out a Wi-Fi policy that has certificate-based authentication, you must push the certification policy out before the Wi-Fi policy. Otherwise, errors occur. Conversely, for some

policies (such as Terms and Conditions, software inventory, and actions), deployment order doesn't matter.

When you add a delivery group, you can specify the order in which resources are deployed to devices. However, Endpoint Management always identifies each situation in which a user is in multiple delivery groups that have duplicate or conflicting policies. In these cases, Endpoint Management calculates a deployment order both for objects that it delivers to a device and for actions it performs.

When determining deployment order, Endpoint Management applies filters and control criteria, such as deployment rules and deployment schedule, to resources. The following table shows which of these criteria you can apply to each type of resource.

Resource	Device platform	Deployment rules	Deployment schedule	User/groups
Device policy	Y	Y	Y	-
App	Y	Y	Y	-
Media	Y	Y	Y	-
Action	-	Y	Y	-
Delivery group	-	Y	-	Y

### Calculation steps

When Endpoint Management needs to calculate deployment order, it performs these steps.

**Note:**

The device platform doesn't affect the calculation steps.

1. Determine all the delivery groups for a specific user, based on the filters of users, groups, and deployment rules.
2. Create an ordered list of all resources (policies, apps, media, and actions) in the selected delivery groups. The list is based on the filters of device platform, deployment rules, and deployment schedule. The ordering algorithm is as follows:
  - a) Place resources from delivery groups that have an admin-defined deployment order ahead of resources from delivery groups without one. For details, see Example of calculation with user-defined order.
  - b) As a tie-breaker among delivery groups, order resources from delivery groups in reverse alphabetical order by delivery group name. For example, Endpoint Management places resources from delivery group B ahead of resources from delivery group A.

- c) While sorting, if an admin-defined deployment order is specified for the resources of a delivery group, maintain that order. Otherwise, sort the resources within that delivery group alphabetically by resource name.
- d) If the same resource appears more than once, remove the duplicate resource. Deliver only the first of these resources.

Resources associated with an admin-defined order deploy before resources without an admin-defined order.

### **Example of calculation with admin-defined order**

Suppose that you have two delivery groups:

- Delivery group Account Managers 1: With *unspecified* order for resources. Contains the policies **Network** and **Passcode**.
- Delivery group Account Managers 2: With *specified* order for resources. Contains the policies **Connection scheduling**, **Restrictions**, **Passcode**, and **Network**, in order.

If the calculation algorithm ordered deployment groups only by name, Endpoint Management would deploy in this order, starting with the delivery group Account Managers 1: **Network**, **Passcode**, **Connection scheduling**, and **Restrictions**. Endpoint Management would ignore **Passcode** and **Network**, both duplicates, from the Account Managers 2 delivery group.

However, the Account Managers 2 group has an admin-specified deployment order. So the calculation algorithm places resources from the Account Managers 2 delivery group higher in the list than the resources from the Account Managers 1 delivery group. As a result, Endpoint Management deploys the policies in this order: **Connection scheduling**, **Restrictions**, **Passcode**, and **Network**. Endpoint Management ignores the policies **Network** and **Passcode** from the Account Managers 1 delivery group, because they're duplicates. The algorithm respects the order specified by the Endpoint Management administrator.

### **Configure deployment rules**

Configure deployment rules to deliver resources when specific conditions are met. You can configure base or advanced deployment rules.

▼ Deployment Rules

Base Advanced

Deploy when All conditions are met. New Rule

Deploy this resource rega... only shareable

Installed app name is equal to Secure Hub

Passcode compliant True

Manage cellular roaming domestic

When adding a deployment rule using the base editor, first select when to deploy the resource.

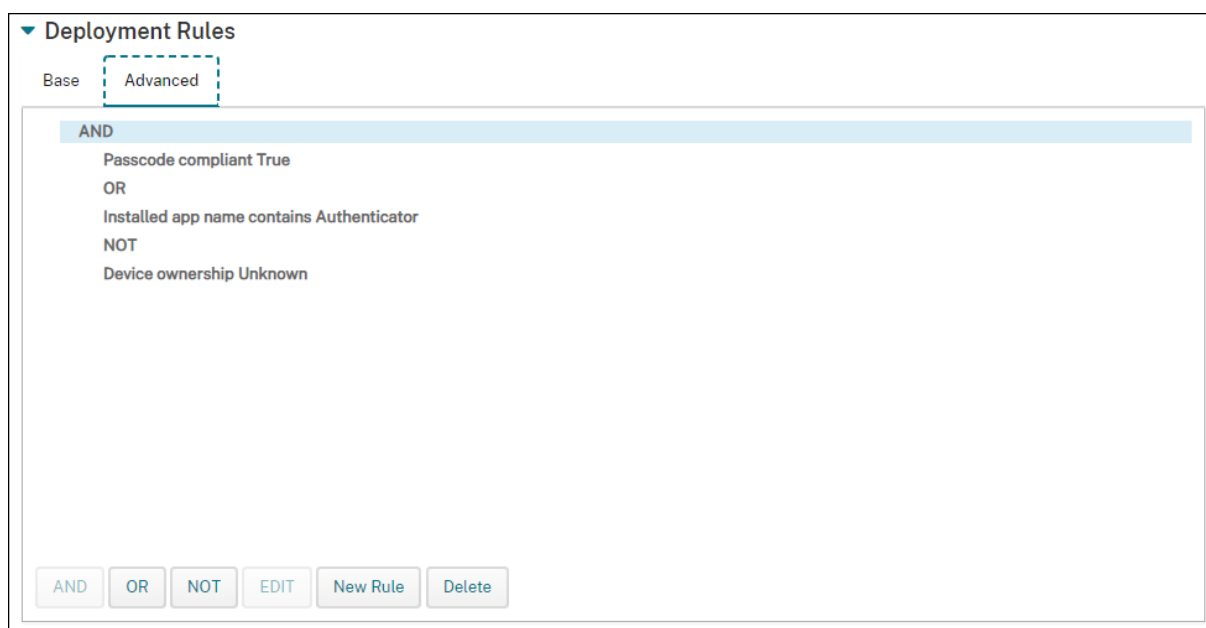
- **All:** Deliver the resource when the user or device meets all the conditions you configure.
- **Any:** Deliver the resource when the user or device meets at least one of the conditions you configure.

Click **New Rule** to choose a rule from a list of available rules to add. The available rules vary based on the resource being deployed and the platform for which you configure the resource. Within each rule are conditions.

You can specify to deploy the resource:

- Only when the selected property exists or except when the selected property exists.
- When the property matches the text you type exactly, the property contains the text you type, or the property doesn't match the text you type.
- When the device or user is compliant with the property you select or isn't compliant with the property you select.
- When the device or user properties match a condition you select from a predefined list.

Use the advanced editor to create more complex deployment rules. You can choose from more rules and you can combine different Boolean logic operators when creating an advanced rule.



### Work with delivery groups

You can work with delivery groups in the following ways:

- Add a delivery group
- Deploy to delivery groups
- Delete a delivery group
- Edit a delivery group
- Enable and disable the AllUsers delivery group.

#### Add a delivery group

When you create a delivery group, you specify whether the user assignments are managed in Endpoint Management or in Citrix Cloud. You can't change this specification after you create the delivery group.

If you plan to use the delivery group to deliver other Citrix Cloud services, specify to manage the user assignments in Citrix Cloud. Other Citrix Cloud services include Citrix Virtual Apps and Desktops, Citrix Content Collaboration, or Secure Browser Service. You can add Active Directory users only to delivery groups managed in Citrix Cloud.

If you need only mobility management for a delivery group of users and apps, set **Manage user assignments** to **In Endpoint Management**. You can't see delivery groups with users managed in Endpoint Management in Citrix Cloud. So you can't use delivery groups managed in Endpoint Management to deliver other services.

**Note:**

We recommend adding delivery groups before creating device policies and enrollment profiles. For information on creating them, see [Device policies](#) and [Enrollment profiles](#).

1. In the Endpoint Management console, click **Configure > Delivery Groups**.
2. From the **Delivery Groups** page, click **Add**.
3. In the **Delivery Group Information** page, type a name and description for the delivery group and then click **Next**.
4. On the **Assignments** page, specify how to manage the delivery group assignments.

The screenshot displays the 'Assignments' configuration page for a delivery group. On the left, a navigation pane lists various settings: Delivery Group, 1 Delivery Group Info, 2 Assignments (highlighted), 3 Resource (optional), Policies, Apps, Media, Actions, ShareFile, Enrollment Profile, and 4 Summary. The main content area is titled 'Assignments' and includes a 'Manage user assignments \*' section. Two radio buttons are present: 'In Endpoint Management' (selected) and 'In Citrix Cloud'. The 'In Endpoint Management' option includes a mobile phone icon and text stating it is for mobility management only. The 'In Citrix Cloud' option includes icons for a server, phone, and folder, and text indicating it is for additional services like Virtual Apps and ShareFile. Below these options are a 'Select domain' dropdown, an 'Include user groups' search field with a 'Search' button, and a list of user groups. At the bottom, there are radio buttons for 'Or' (selected) and 'And', a 'Deploy to anonymous user' toggle, and expandable filter sections for 'Filter by User Properties' and 'Filter by Device Properties'.

- **Manage user assignments:**

- **In Endpoint Management:** Select this option if you plan to create a delivery group for users and apps that need only mobility management. You can't see delivery groups whose user assignments are managed in Endpoint Management in Citrix Cloud and you can't use them to deliver other services.
- **In Citrix Cloud:** Select this option if you plan to use the delivery group to deliver other services. Those services might include Citrix Virtual Apps and Desktops or Citrix Content Collaboration.



## 5. Add users to the delivery group.

**Important:**

You can't change the **Manage user assignments** setting after creating the delivery group.

- **Select domain:** From the list, select the domain from which to choose users.
- **Include user groups:** Do one of the following:
  - In the list of user groups, click the groups you want to add. The selected groups appear in the **Selected user groups** list.
  - Click **Search** to see a list of all user groups in the selected domain. You can also type a full or partial group name in the search box and then click **Search** to narrow your search.

To remove a user group from the **Selected user groups** list, do one of the following:

- In the **Selected user groups** list, click the **X** next to each group you want to remove.
  - Click **Search** to see a list of all user groups in the selected domain. Or, type a full or partial group name before you click **Search** to narrow your search. Clear the check box of each group you want to remove.
  - **Or/And:** Select whether users are in any group (Or) or whether they must be in all groups (And) for the resource to be deployed to them.
  - **Deploy to anonymous user:** Select whether to deploy to unauthenticated users in the delivery group. Unauthenticated users are users that you can't authenticate but you allowed their devices to connect to Endpoint Management anyway.
6. Expand **Filter by User Properties** or **Filter by Device Properties** to specify how the delivery group manages resources.
- If you choose **Filter by Device Properties**, expand the device platform to configure the deployment rules:
    - **Device Properties - Android** (see Create a rule to deploy resources to Android devices)
    - **Device Properties - iOS**
    - **Device Properties - Windows Desktop/Tablet only**
  - The **Base** tab appears by default. Under the **Base** tab, specify when to deploy the policy. You can choose to deploy the policy when **All** conditions are met or when **Any** conditions are met. The default option is **All**.
    - Click **New Rule** to define the conditions.
    - In the lists, choose the conditions. For example, select Device ownership and BYOD.
    - Click **New Rule** for each condition you want to add.
  - Click the **Advanced** tab to combine the rules with Boolean options. The conditions you chose on the **Base** tab appear.

- Click **AND**, **OR**, or **NOT**, and then click **New Rule**.
  - In the lists, choose the conditions to add to the rule and then click the plus sign (+) on the right side.  
At any time, you can click to select a condition and then click **Edit** to change the condition or **Delete** to remove the condition.
7. Click **Next** to go to the **Policies** page. You optionally add policies, apps, media, or actions for the delivery group here. For details, see:
    - Add policies to a delivery group
    - Add apps to a delivery group
    - Add media to a delivery group
    - Add actions to a delivery group
  8. When you're satisfied with your delivery group, click **Summary** to see a summary of the configuration.
  9. Click **Save**. The new delivery group appears on the **Delivery Groups** page.

#### **Add policies to a delivery group**

1. From the **Resources (optional)** list, click **Policies**.
2. For each policy you want to add, do the following:
  - Scroll through the list of available policies to find the policy you want to add. Or, type a full or partial policy name in the search box, and then click **Search**.
  - Drag the policy you want to add into the box on the right.To remove a policy from the box, click the **X** next to the policy name.
3. Click **Next** to go to the **Apps** page.

#### **Add apps to a delivery group**

1. For each app you want to add, do the following:
  - Scroll through the list of available apps to find the app you want to add. Or, type a full or partial app name in the search box, and then click **Search**.
  - Drag the app into either the **Required Apps** box or the **Optional Apps** box.

For apps marked as required, users can promptly receive updates in situations such as when:

- You upload a new app and mark it required.
- You mark an existing app required.
- A user deletes a required app.
- A Secure Hub update is available.

For information about forced deployment of required apps, including how to enable the feature, see [About required and optional apps](#).

To remove an app from the box, click the **X** next to the app name.

2. Click **Next** to go to the **Media** page.

### Add media to a delivery group

1. For each book you want to add, do the following:
  - Scroll through the list of available books to find the book you want to add. Or, type a full or partial book name in the search box, and then click **Search**.
  - Drag the book you want to add into the **Required Books** box.

For books marked as required, users promptly receive updates in situations such as when:

- You upload a new book and mark it required.
- You mark an existing book required.
- A user deletes a required book.
- A Secure Hub update is available.

To remove a book from the box, click the **X** next to the book name.

2. Click **Next** to go to the **Actions** page.

### Add actions to a delivery group

1. For each action you want to add, do the following:
  - Scroll through the list of available actions to find the action you want to add. Or, type a full or partial action name in the search box, and then click **Search**.
  - Drag the action you want to add into the box on the right.

To remove an action from the box, click the **X** next to the action name.

2. Click **Next** to go to the **Content Collaboration** (formerly **ShareFile**) page.

### Apply the Content Collaboration configuration

The Content Collaboration page (formerly ShareFile) differs depending on whether you configured Endpoint Management (**Configure > Content Collaboration**) for Enterprise accounts or for storage zone connectors.

- If you configured Enterprise accounts for use with Endpoint Management, set **Enable Content Collaboration** to **On**. This setting provides the delivery group single sign-on access to Content Collaboration content and data.

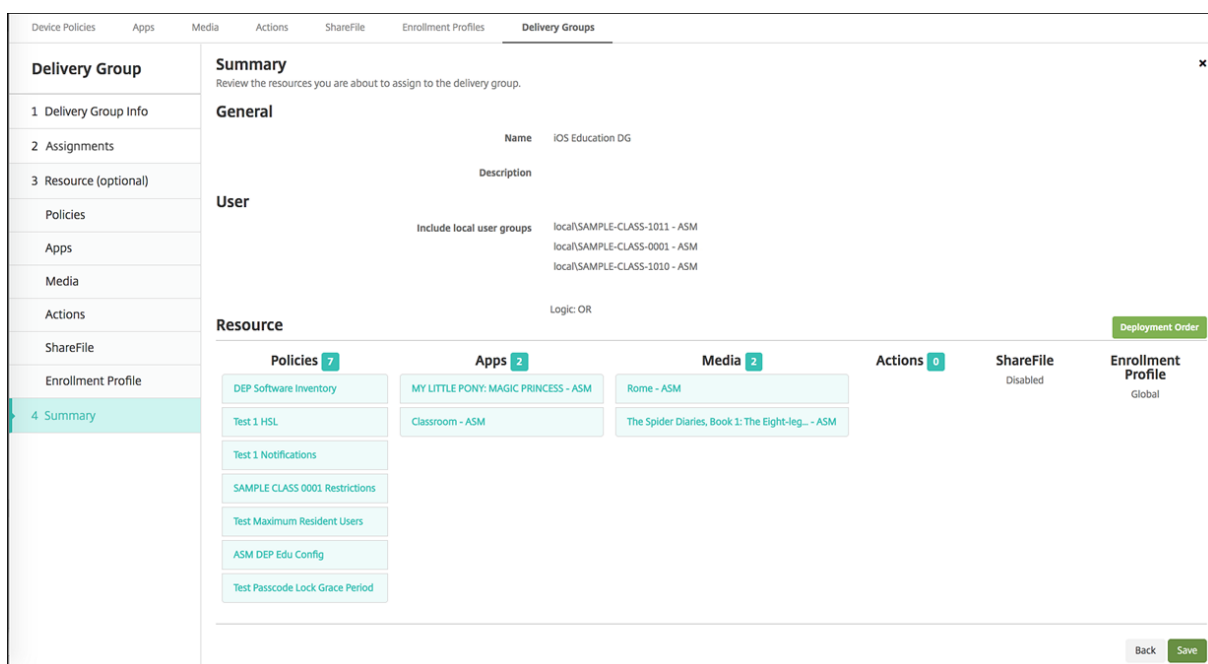
- If you configured storage zone connectors for use with Endpoint Management, drag the storage zone connectors to include in the delivery group to the box on the right.

### Review configured options and change deployment order

On the Summary page, you can review the options you’ve configured for the delivery group and change the deployment order of resources. The Summary page shows your resources by category. The Summary page doesn’t show the deployment order.

**Note:**

Click **Back** to return to previous pages change the configuration.



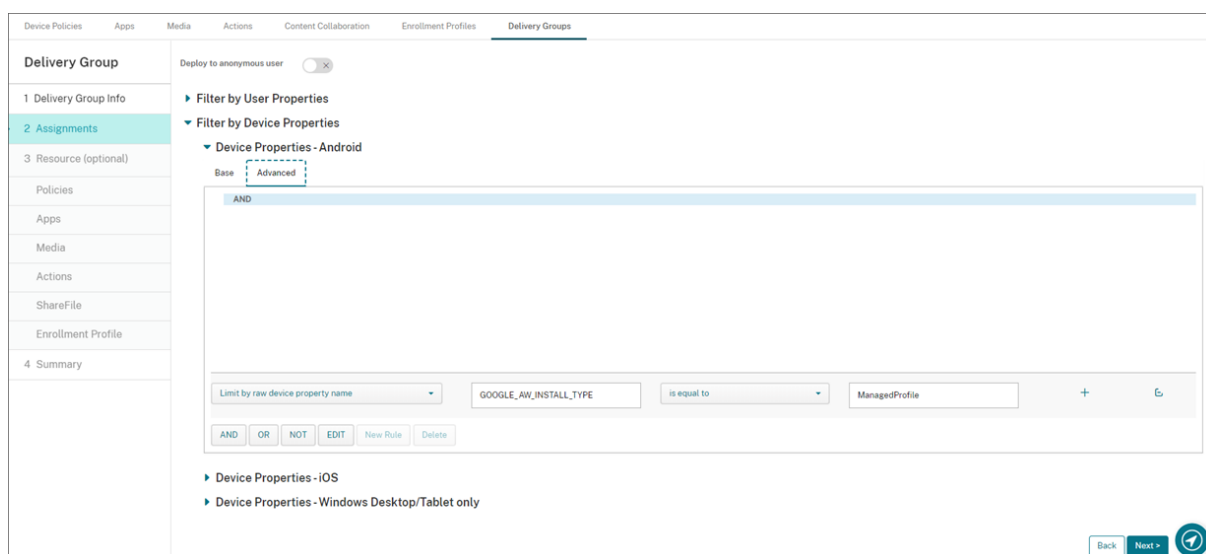
To view or change deployment order:

1. Click **Deployment Order**.
2. In the Deployment Order dialog box, drag a resource to the place in the order where you want to deploy it. The resources deploy in top-to-bottom order.
3. Click **Save** to save the deployment order.

When you have finished configuring the delivery group, on the Summary page, click **Save**.

### Create a rule to deploy resources to Android Enterprise

You can manage the deployment of a delivery group to Android Enterprise devices by using the Android device property rules. If you enroll multiple devices to the same user, you can create advanced filters for Android Enterprise based on device enrollment mode or the device application package ID.



To deploy a delivery group to Android Enterprise devices by using device enrollment mode:

1. Create a delivery group.
2. On the **Assignments** page, expand **Filter by Device Properties**.
3. In **Device Properties – Android**, open the **Advanced tab** and click **New rule**.
4. In the list, choose the condition to add to the rule:
  - For new Android Enterprise devices, choose **Limit by raw device property name** and type **GOOGLE\_AW\_INSTALL\_TYPE** in the first value field. Then you must set the condition to equal one of the enrollment modes.
  - For existing Android Enterprise devices, choose **Limit by known device property name** and select **Android Enterprise install type** in the first value field. Then you must set the condition to equal one of the enrollment modes.
5. In the second field, type an enrollment mode for your Android Enterprise devices:
  - **DeviceAdministrator:** Specifies company-owned devices intended only for work use (also known as device owner mode)
  - **ManagedProfile:** Specifies BYOD—personal devices enrolled with work Profile Management (also known as profile-owner mode)
  - **CorporateOwnedSingleUse:** Specifies dedicated devices (formerly known as corporate-owned, single-use devices)
  - **CorporateOwnedPersonallyEnabled:** Specifies fully managed devices with a work profile (formerly known as corporate-owned, personally enabled devices)
6. Finish configuring the delivery group as described Add a delivery group.

For more information, see [Device deployment scenarios and profiles](#).

To deploy a delivery group to Android Enterprise devices by using the device application package ID:

1. In **Device Properties – Android**, open the **Advanced tab** and click **New rule**.
2. In the list, choose **Installed app name** and enter the application package ID.

### **Edit a delivery group**

You can't change the name of an existing delivery group. To update other settings, go to **Configure > Delivery Groups**, select the group you want to edit, and then click **Edit**.

### **Enable and disable the AllUsers delivery group**

AllUsers is the only delivery group that you can enable or disable. You cannot delete AllUsers as you can other delivery groups.

From the **Delivery Groups** page, choose the AllUsers delivery group by selecting the check box next to **AllUsers** or by clicking in the line containing **AllUsers**. Then do one of the following:

- Click **Disable** to disable the AllUsers delivery group. This command is available only if the AllUsers group is enabled (the default). **Disabled** appears under the **Disabled** heading in the delivery group table.
- Click **Enable** to enable the AllUsers delivery group. This command is available only if the AllUsers group is disabled. **Disabled** no longer appears under the **Disabled** heading in the delivery group table.

### **Deploy to delivery groups**

Deploying to a delivery group means sending a push notification to all users with Apple, Android, and Windows tablet devices.

For users with other platform devices, if those devices are already connected to Endpoint Management, they receive the resources immediately. Otherwise, based on their scheduling policy, they receive the resources the next time that they connect.

For updated apps to appear in the Updated Available list in the app store on Android devices, first deploy an App Inventory policy to the user devices.

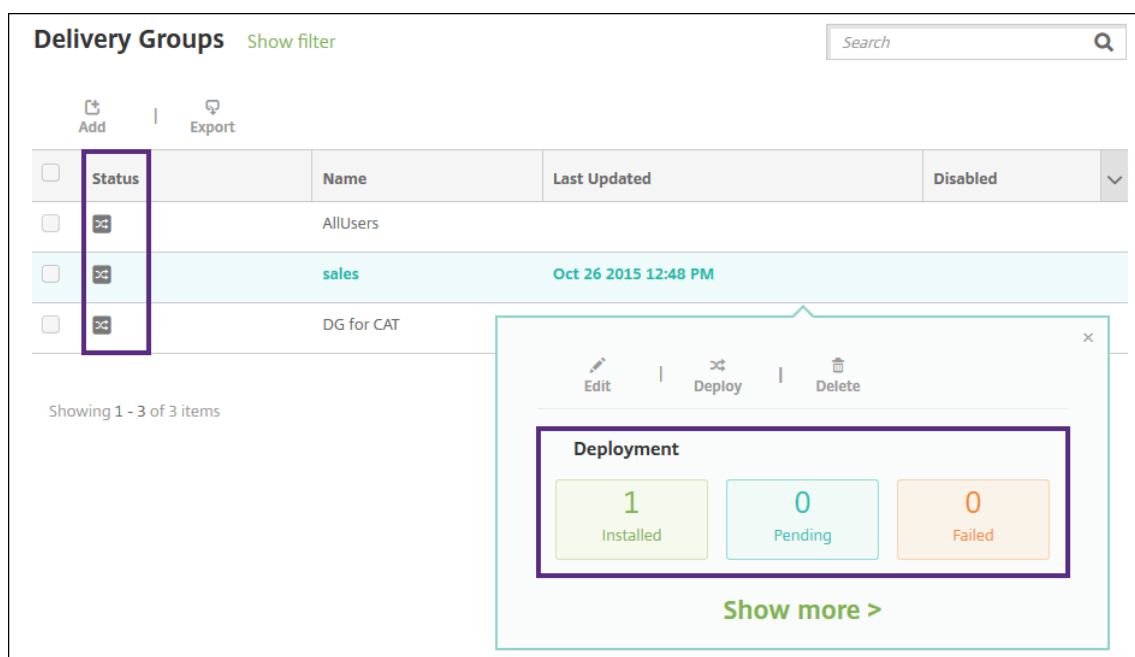
1. On the **Delivery Groups** page, do one of the following:
  - To deploy to more than one delivery group at a time, select the check boxes next to the groups you want to deploy.
  - To deploy to a single delivery group, either select the check box next to its name or click the line containing its name.
2. Click **Deploy**.

Depending on how you select a single delivery group, the **Deploy** command appears above or to the right of the delivery group.

Verify that the groups you want to deploy apps, policies, and actions to are listed. Then click **Deploy**. The apps, policies, and actions are deployed to the selected groups based on device platform and scheduling policy.

You can check deployment status on the **Delivery Groups** page in one of these ways:

- Look at the deployment icon under the **Status** heading for the delivery group, which indicates any deployment failure.
- Click the line containing the delivery group to display an overlay that shows **Installed**, **Pending**, and **Failed** deployments.



The screenshot displays the 'Delivery Groups' page in the Citrix Endpoint Management console. At the top, there is a search bar and a 'Show filter' link. Below the search bar are 'Add' and 'Export' buttons. The main content is a table with columns for 'Status', 'Name', 'Last Updated', and 'Disabled'. The 'Status' column is highlighted with a purple box. The table lists three delivery groups: 'AllUsers', 'sales', and 'DG for CAT'. The 'sales' group is highlighted in light blue and has a deployment icon (a square with a checkmark and an 'x') in the 'Status' column. An overlay window is open for the 'sales' group, showing a 'Deployment' summary with three boxes: '1 Installed' (green), '0 Pending' (blue), and '0 Failed' (orange). Below the summary is a 'Show more >' link. The overlay also has 'Edit', 'Deploy', and 'Delete' buttons at the top.

Status	Name	Last Updated	Disabled
<input type="checkbox"/>	AllUsers		<input type="checkbox"/>
<input type="checkbox"/>	sales	Oct 26 2015 12:48 PM	<input type="checkbox"/>
<input type="checkbox"/>	DG for CAT		<input type="checkbox"/>

### Clone a delivery group

Clone a delivery group when you want to create a delivery group that is similar to an existing one. Use the clone as the starting point for your new delivery group. Then make your changes to the clone, such as adding enrollment profiles or new sets of AD users.

1. In the Endpoint Management console, click **Configure** and then select the **Delivery Groups** tab.
2. From the list of delivery groups, select the one you want to use as the basis for the new group.
3. Select **Clone**.
4. In the Clone a Delivery Group dialog box, enter the name of the new group and, optionally, a description.
5. Select **Clone**.

## Delete delivery groups

You can't delete the AllUsers delivery group, but you can disable it when you don't want to push resources to all users. See [Enable and disable the AllUsers delivery group](#).

### Important:

You cannot undo a delete.

1. On the **Delivery Groups** page, do one of the following:
  - To delete more than one delivery group at a time, select the check boxes next to the groups you want to delete.
  - To delete a single delivery group, either select the check box next to its name or click the line containing its name.

2. Click **Delete**.

Depending on how you select a single delivery group, the **Delete** command appears above or to the right of the delivery group.

3. In the **Delete** dialog box, click **Delete**.

## Export the Delivery Groups table

1. Click **Export** above the **Delivery Groups** table. Endpoint Management extracts the information in the **Delivery Groups** table and converts it to a .csv file.
2. Open or save the .csv file by following the usual steps for your browser.

## Macros

March 30, 2021

Endpoint Management provides macros as a way to populate user or device property data within the text field of the following items:

- Policies
- Notifications
- Enrollment templates
- Device configuration XML file
- Automated actions
- Credential provider Certificate Signing Requests



Endpoint Management replaces a macro with the corresponding user or system values. For example, you can prepopulate the mailbox value for a user in a single Exchange profile across thousands of users.

## Macro syntax

A macro can take the following form:

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME [ 'DEFAULT VALUE' ] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)] ] }`

Enclose all syntax following the dollar sign (\$) in curly brackets ({}).

- Qualified property names reference either a user property, a device property, or a custom property.
- Qualified property names consist of a prefix, followed by the actual property name.
- User properties take the form `${ user.[PROPERTYNAME] (prefix="user.")}`.
- Device properties take the form `${ device.[PROPERTYNAME] (prefix="device.")}`.
- Property names are case-sensitive.
- A function can be a limited list or a link to a third-party reference that defines functions. This macro for a notification message includes the function `firstnotnull`:

Device `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` has been blocked...

- For custom macros (properties that you define), the prefix is `${ custom }`. You can omit the prefix.

Here's an example of a commonly used macro, `${ user.username }`, that populates the user name value in the text field of a policy. This macro is useful for configuring Exchange ActiveSync profiles and other profiles used by multiple users. The following example shows how to use macros in an Exchange policy. The macro for **User** is `${ user.username }`. The macro for **Email address** is `${ user.mail }`.

The following example shows how to use macros for a certificate signing request. The macro for **Subject name** is **CN=\$user.username**. The macro for the **Value** of a **Subject alternative name** is **\$user.userprincipalname**.

Type	Value*	Add
User Principal name	\$user.userprincipalname	

The following example shows how to use macros in a notification template. The example template defines the message sent to a user when HDX applications are blocked because of a non-compliant device. The macro for the **Message** is:

Device \${ firstnotnull(device.TEL\_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked.

Settings > Notification Templates > Add Notification Template

### Add Notification Template

Based on the types of templates you choose, you can notify users through supported channels, such as SMTP, SMS and Secure Hub.

**Name\***

**Description**

**Type**   
Manual sending supported

**Channels**

**Secure Hub**

**Message**

For more examples of macros used in notifications, go to **Settings > Notification Templates**, select a pre-defined template, and click **Edit**.

The following example shows a macro in the Device Name device policy. You can type a macro, a combination of macros, or a combination of macros and text to name each device uniquely. For example, use `${ device.serialnumber }` to set the device names to the serial number of each device. Use `${ device.serialnumber } ${ user.username }` to include the user name in the device name. The Device Name device policy works on supervised iOS and macOS devices.

Device Policies   Apps   Actions   ShareFile   Enrollment Profiles   Delivery Groups

### Device Name Policy

This policy lets you apply a name on a supervised device on iOS and Mac OS X devices. Available in iOS 8 and later.

**Device name\***

► **Deployment Rules**

- iOS
- Mac OS X

## Macros for default notification templates

You can use the following macros in the default notification templates:

- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`
- `${ enrollment.andriod.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`
- `${ enrollment.pin }`
- `${ enrollment.url }`
- `${ enrollment.urls }`

- `${ enrollment.ios.url }`
- `${ enrollment.macos.url }`
- `${ enrollment.android.url }`
- `${ enrollment.ios.platform }`
- `${ enrollment.macos.platform }`
- `${ enrollment.android.platform }`
- `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}`
- `${ firstnotnull(device.TEL_NUMBER,user.mobile)}`
- `${ outofcompliance.reason(smg_block)}`
- `${ outofcompliance.reason(whitelist_blacklist_apps_name)}`
- `${ vpp.account }`
- `${ vpp.appname }`
- `${ vpp.url }`
- `${ zdmserver.hostPath } /enroll`

**Note:**

The Endpoint Management console includes the terms “blacklist” and “whitelist”. We are changing those terms in an upcoming release to “block list” and “allow list”.

This example shows how to create a notification that includes enrollment URLs for multiple device platforms. The macro for the **Message** is:

```
${enrollment.urls}
```

Settings > Notification Templates > Add Notification Template

### Add Notification Template

Based on the types of templates you choose, you can notify users through supported channels, such as SMTP, SMS and Secure Hub.

**Name\***

**Description**

**Type**   
Manual sending not supported

**Channels**

**SMTP** ⚠ Channel cannot be activated until you define the SMTP server in the [Notification Server](#) section in Settings.

**Sender**

**Recipient**

**Subject**

**Message**

**SMS** ⚠ Channel cannot be activated until you define the SMS server in the [Notification Server](#) section in Settings.

**Recipient**

**Message**

These examples show how to create messages for notifications that prompt the users to click the enrollment URL for their device platforms:

#### Example 1:

```

1 To enroll, click the link below that applies to your device platform:
2
3 ${
4   enrollment.ios.platform }
5   - ${
6     enrollment.ios.url }
7
8
9 ${
10  enrollment.macos.platform }
11   - ${
12    enrollment.macos.url }
13
14
15 ${
16  enrollment.android.platform }
17   - ${

```

```
18 enrollment.android.url }
19
20
21 <!--NeedCopy-->
```

#### Example 2:

```
1 To enroll an iOS device, click the link ${
2 enrollment.ios.url }
3 .
4
5 To enroll a macOS device, click the link ${
6 enrollment.macos.url }
7 .
8
9 To enroll an Android device, click the link ${
10 enrollment.android.url }
11 .
12
13 <!--NeedCopy-->
```

### Macros for specific policies

For the Device Name device policy (for iOS and macOS), you can use these macros for the **Device name**:

- `${ device.serialnumber }`
- `${ user.username } @example.com`
- `${ device.serialnumber }`
- `${ device.serialnumber }`
- `${ user.username }`
- `${ enrollment.pin }`
- `${ user.dnsroot }`

For the Cellular device policy (for iOS), you can use macros for the values of non-string fields, such as Proxy server port. For example, you can now use a macro such as `${ device.xyz }` or `${ setting .xyz }`, which expands into an integer.

For a device configuration XML file that you import into Endpoint Management by using the Import iOS & macOS Profile device policy, you can use macros for the values of non-string fields.

For the Samsung MDM License Key device policy, you can use this macro for the **ELM license key**:

- `${ elm.license.key }`

For the Web clip device policy, you can use this macro for the **URL**:

- `${ webeas-url }`

### Macros to obtain built-in device properties

Display name	Macros
Device ID	<code>\$device.id</code>
Device GUID	<code>\$device.uniqueid</code>
Device IMEI	<code>\$device.imei</code>
OS Family	<code>\$device.OSFamily</code>
Serial Number	<code>\$device.serialNumber</code>

### Macros for all device properties

**Display name:** Account Suspended?

- **Web element:** `GOOGLE_AW_DIRECTORY_SUSPENDED`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_SUSPENDED }`

**Display name:** Activation lock bypass code

- **Web element:** `ACTIVATION_LOCK_BYPASS_CODE`
- **Macros:** `${ device.ACTIVATION_LOCK_BYPASS_CODE }`

**Display name:** Activation lock enabled

- **Web element:** `ACTIVATION_LOCK_ENABLED`
- **Macros:** `${ device.ACTIVATION_LOCK_ENABLED }`

**Display name:** Active Apple App Store account

- **Web element:** `ACTIVE_ITUNES`
- **Macros:** `${ device.ACTIVE_ITUNES }`

---

<b>Display name:</b>	ActiveSync device known by MSP
----------------------	--------------------------------

---

- **Web element:** `AS_DEVICE_KNOWN_BY_ZMSP`
- **Macros:** `${ device.AS_DEVICE_KNOWN_BY_ZMSP }`

**Display name:** Administrator disabled

- **Web element:** ADMIN\_DISABLED
- **Macros:** \${ device.ADMIN\_DISABLED }

**Display name:** AIK Present?

- **Web element:** WINDOWS\_HAS\_AIK\_PRESENT
- **Macros:** \${ device.WINDOWS\_HAS\_AIK\_PRESENT }

**Display name:** Amazon MDM API available

- **Web element:** AMAZON\_MDM
- **Macros:** \${ device.AMAZON\_MDM }

**Display name:** Android Enterprise Device ID

- **Web element:** GOOGLE\_AW\_DEVICE\_ID
- **Macros:** \${ device.GOOGLE\_AW\_DEVICE\_ID }

**Display name:** Android Enterprise Enabled Device?

- **Web element:** GOOGLE\_AW\_ENABLED\_DEVICE
- **Macros:** \${ device.GOOGLE\_AW\_ENABLED\_DEVICE }

**Display name:** Android Enterprise Install Type

- **Web element:** GOOGLE\_AW\_INSTALL\_TYPE
- **Macros:** \${ device.GOOGLE\_AW\_INSTALL\_TYPE }

**Display name:** Antispyware Signature status

- **Web element:** ANTI\_SPYWARE\_SIGNATURE\_STATUS
- **Macros:** \${ device.ANTI\_SPYWARE\_SIGNATURE\_STATUS }

**Display name:** Antispyware Status

- **Web element:** ANTI\_SPYWARE\_STATUS
- **Macros:** \${ device.ANTI\_SPYWARE\_STATUS }

**Display name:** Antivirus Signature Status

- **Web element:** ANTI\_VIRUS\_SIGNATURE\_STATUS
- **Macros:** \${ device.ANTI\_VIRUS\_SIGNATURE\_STATUS }

**Display name:** Antivirus Status

- **Web element:** ANTI\_VIRUS\_STATUS
- **Macros:** \${ device.ANTI\_VIRUS\_STATUS }



**Display name:** ASM Deployment Program activation lock bypass code

- **Web element:** `DEP_ACTIVATION_LOCK_BYPASS_CODE`
- **Macros:** `${ device.DEP_ACTIVATION_LOCK_BYPASS_CODE }`

**Display name:** ASM Deployment Program escrow key

- **Web element:** `DEP_ESCROW_KEY`
- **Macros:** `${ device.DEP_ESCROW_KEY }`

**Display name:** Asset tag

- **Web element:** `ASSET_TAG`
- **Macros:** `${ device.ASSET_TAG }`

**Display name:** Automatically check software updates

- **Web element:** `AutoCheckEnabled`
- **Macros:** `${ device.AutoCheckEnabled }`

**Display name:** Automatically download software updates in the background

- **Web element:** `BackgroundDownloadEnabled`
- **Macros:** `${ device.BackgroundDownloadEnabled }`

**Display name:** Automatically install app updates

- **Web element:** `AutomaticAppInstallationEnabled`
- **Macros:** `${ device.AutomaticAppInstallationEnabled }`

**Display name:** Automatically install OS updates

- **Web element:** `AutomaticOSInstallationEnabled`
- **Macros:** `${ device.AutomaticOSInstallationEnabled }`

**Display name:** Automatically install security updates

- **Web element:** `AutomaticSecurityUpdatesEnabled`
- **Macros:** `${ device.AutomaticSecurityUpdatesEnabled }`

**Display name:** Autoupdate Status

- **Web element:** `AUTOUPDATE_STATUS`
- **Macros:** `${ device.AUTOUPDATE_STATUS }`

**Display name:** Available RAM

- **Web element:** `MEMORY_AVAILABLE`

- **Macros:** `${ device.MEMORY_AVAILABLE }`

**Display name:** Available software updates

- **Web element:** `AVAILABLE_OS_UPDATE_HUMAN_READABLE`
- **Macros:** `${ device.AVAILABLE_OS_UPDATE_HUMAN_READABLE }`

**Display name:** Available storage space

- **Web element:** `FREEDISK`
- **Macros:** `${ device.FREEDISK }`

**Display name:** Backup battery

- **Web element:** `BACKUP_BATTERY_PERCENT`
- **Macros:** `${ device.BACKUP_BATTERY_PERCENT }`

**Display name:** Baseband firmware version

- **Web element:** `MODEM_FIRMWARE_VERSION`
- **Macros:** `'${device.MODEM_FIRMWARE_VERSION}'`

**Display name:** Battery Charging

- **Web element:** `BATTERY_CHARGING_STATUS`
- **Macros:** `${ device.BATTERY_CHARGING_STATUS }`

**Display name:** Battery charging

- **Web element:** `BATTERY_CHARGING`
- **Macros:** `${ device.BATTERY_CHARGING }`

**Display name:** Battery Remaining

- **Web element:** `BATTERY_ESTIMATED_CHARGE_REMAINING`
- **Macros:** `${ device.BATTERY_ESTIMATED_CHARGE_REMAINING }`

**Display name:** Battery Runtime

- **Web element:** `BATTERY_RUNTIME`
- **Macros:** `${ device.BATTERY_RUNTIME }`

**Display name:** Battery Status

- **Web element:** `BATTERY_STATUS`
- **Macros:** `${ device.BATTERY_STATUS }`

**Display name:** BES device known by MSP

- **Web element:** BES\_DEVICE\_KNOWN\_BY\_ZMSP
- **Macros:** \${ device.BES\_DEVICE\_KNOWN\_BY\_ZMSP }

**Display name:** BES PIN

- **Web element:** BES\_PIN
- **Macros:** \${ device.BES\_PIN }

**Display name:** BES server agent ID

- **Web element:** AGENT\_ID
- **Macros:** \${ device.AGENT\_ID }

**Display name:** BES server name

- **Web element:** BES\_SERVER
- **Macros:** \${ device.BES\_SERVER }

**Display name:** BES server version

- **Web element:** BES\_VERSION
- **Macros:** \${ device.BES\_VERSION }

**Display name:** BIOS Info

- **Web element:** BIOS\_INFO
- **Macros:** \${ device.BIOS\_INFO }

**Display name:** BitLocker Status

- **Web element:** WINDOWS\_HAS\_BIT\_LOCKER\_STATUS
- **Macros:** \${ device.WINDOWS\_HAS\_BIT\_LOCKER\_STATUS }

**Display name:** Bluetooth MAC address

- **Web element:** BLUETOOTH\_MAC
- **Macros:** \${ device.BLUETOOTH\_MAC }

**Display name:** Boot Debugging Enabled?

- **Web element:** WINDOWS\_HAS\_BOOT\_DEBUGGING\_ENABLED
- **Macros:** \${ device.WINDOWS\_HAS\_BOOT\_DEBUGGING\_ENABLED }

**Display name:** Boot Manager Rev List Version

- **Web element:** WINDOWS\_HAS\_BOOT\_MGR\_REV\_LIST\_VERSION
- **Macros:** \${ device.WINDOWS\_HAS\_BOOT\_MGR\_REV\_LIST\_VERSION }

**Display name:** Carrier Code

- **Web element:** CARRIER\_CODE
- **Macros:** \${ device.CARRIER\_CODE }

**Display name:** Carrier settings version

- **Web element:** CARRIER\_SETTINGS\_VERSION
- **Macros:** \${ device.CARRIER\_SETTINGS\_VERSION }

**Display name:** Catalog URL

- **Web element:** CatalogURL
- **Macros:** \${ device.CatalogURL }

**Display name:** Cellular altitude

- **Web element:** GPS\_ALTITUDE\_FROM\_CELLULAR
- **Macros:** \${ device.GPS\_ALTITUDE\_FROM\_CELLULAR }

**Display name:** Cellular course

- **Web element:** GPS\_COURSE\_FROM\_CELLULAR
- **Macros:** \${ device.GPS\_COURSE\_FROM\_CELLULAR }

**Display name:** Cellular horizontal accuracy

- **Web element:** GPS\_HORIZONTAL\_ACCURACY\_FROM\_CELLULAR
- **Macros:** \${ device.GPS\_HORIZONTAL\_ACCURACY\_FROM\_CELLULAR }

**Display name:** Cellular latitude

- **Web element:** GPS\_LATITUDE\_FROM\_CELLULAR
- **Macros:** \${ device.GPS\_LATITUDE\_FROM\_CELLULAR }

**Display name:** Cellular longitude

- **Web element:** GPS\_LONGITUDE\_FROM\_CELLULAR
- **Macros:** \${ device.GPS\_LONGITUDE\_FROM\_CELLULAR }

**Display name:** Cellular speed

- **Web element:** GPS\_SPEED\_FROM\_CELLULAR
- **Macros:** \${ device.GPS\_SPEED\_FROM\_CELLULAR }

**Display name:** Cellular technology

- **Web element:** CELLULAR\_TECHNOLOGY

- **Macros:** `${ device.CELLULAR_TECHNOLOGY }`

**Display name:** Cellular timestamp

- **Web element:** `GPS_TIMESTAMP_FROM_CELLULAR`
- **Macros:** `${ device.GPS_TIMESTAMP_FROM_CELLULAR }`

**Display name:** Cellular vertical accuracy

- **Web element:** `GPS_VERTICAL_ACCURACY_FROM_CELLULAR`
- **Macros:** `${ device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR }`

**Display name:** Change Password at Next Login?

- **Web element:** `GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`
- **Macros:** `'${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}`

**Display name:** Client device ID

- **Web element:** `CLIENT_DEVICE_ID`
- **Macros:** `${ device.CLIENT_DEVICE_ID }`

**Display name:** Cloud backup enabled

- **Web element:** `CLOUD_BACKUP_ENABLED`
- **Macros:** `${ device.CLOUD_BACKUP_ENABLED }`

**Display name:** Code Integrity Enabled?

- **Web element:** `WINDOWS_HAS_CODE_INTEGRITY_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED }`

**Display name:** Code Integrity Rev List Version

- **Web element:** `WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION`
- **Macros:** `${ device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION }`

**Display name:** Color

- **Web element:** `COLOR`
- **Macros:** `${ device.COLOR }`

**Display name:** CPU clock speed

- **Web element:** `CPU_CLOCK_SPEED`
- **Macros:** `${ device.CPU_CLOCK_SPEED }`

**Display name:** CPU type

- **Web element:** CPU\_TYPE
- **Macros:** \${ device.CPU\_TYPE }

**Display name:** Creation Time

- **Web element:** GOOGLE\_AW\_DIRECTORY\_CREATION\_TIME
- **Macros:** \${ device.GOOGLE\_AW\_DIRECTORY\_CREATION\_TIME }

**Display name:** Critical software updates

- **Web element:** AVAILABLE\_OS\_UPDATE\_IS\_CRITICAL
- **Macros:** \${ device.AVAILABLE\_OS\_UPDATE\_IS\_CRITICAL }

**Display name:** Current carrier network

- **Web element:** CARRIER
- **Macros:** \${ device.CARRIER }

**Display name:** Current mobile country code

- **Web element:** CURRENT\_MCC
- **Macros:** \${ device.CURRENT\_MCC }

**Display name:** Current mobile network code

- **Web element:** CURRENT\_MNC
- **Macros:** \${ device.CURRENT\_MNC }

**Display name:** Data roaming allowed

- **Web element:** DATA\_ROAMING\_ENABLED
- **Macros:** \${ device.DATA\_ROAMING\_ENABLED }

**Display name:** Date of the last iCloud backup

- **Web element:** LAST\_CLOUD\_BACKUP\_DATE
- **Macros:** \${ device.LAST\_CLOUD\_BACKUP\_DATE }

**Display name:** Default catalog

- **Web element:** IsDefaultCatalog
- **Macros:** \${ device.IsDefaultCatalog }

**Display name:** Apple Deployment Program account name

- **Web element:** BULK\_ENROLLMENT\_DEP\_ACCOUNT\_NAME
- **Macros:** \${ device.BULK\_ENROLLMENT\_DEP\_ACCOUNT\_NAME }

**Display name:** Apple Deployment Program Policy

- **Web element:** WINDOWS\_HAS\_DEP\_POLICY
- **Macros:** \${ device.WINDOWS\_HAS\_DEP\_POLICY }

**Display name:** Apple Deployment Program profile assigned

- **Web element:** PROFILE\_ASSIGN\_TIME
- **Macros:** \${ device.PROFILE\_ASSIGN\_TIME }

**Display name:** Apple Deployment Program profile pushed

- **Web element:** PROFILE\_PUSH\_TIME
- **Macros:** \${ device.PROFILE\_PUSH\_TIME }

**Display name:** Apple Deployment Program profile removed

- **Web element:** PROFILE\_REMOVE\_TIME
- **Macros:** \${ device.PROFILE\_REMOVE\_TIME }

**Display name:** Apple Deployment Program registration by

- **Web element:** DEVICE\_ASSIGNED\_BY
- **Macros:** \${ device.DEVICE\_ASSIGNED\_BY }

**Display name:** Apple Deployment Program registration date

- **Web element:** DEVICE\_ASSIGNED\_DATE
- **Macros:** \${ device.DEVICE\_ASSIGNED\_DATE }

**Display name:** Description

- **Web element:** DESCRIPTION
- **Macros:** \${ device.DESCRPTION }

**Display name:** Device model

- **Web element:** SYSTEM\_OEM
- **Macros:** \${ device.SYSTEM\_OEM }

**Display name:** Device name

- **Web element:** DEVICE\_NAME
- **Macros:** \${ device.DEVICE\_NAME }

**Display name:** Device Type

- **Web element:** DEVICE\_TYPE

- **Macros:** `${ device.DEVICE_TYPE }`

**Display name:** Do Not Disturb activated

- **Web element:** `DO_NOT_DISTURB`
- **Macros:** `${ device.DO_NOT_DISTURB }`

**Display name:** ELAM Driver Loaded?

- **Web element:** `WINDOWS_HAS_ELAM_DRIVER_LOADED`
- **Macros:** `${ device.WINDOWS_HAS_ELAM_DRIVER_LOADED }`

**Display name:** Encryption Compliance

- **Web element:** `ENCRYPTION_COMPLIANCE`
- **Macros:** `${ device.ENCRYPTION_COMPLIANCE }`

**Display name:** ENROLLMENT\_KEY\_GENERATION\_DATE

- **Web element:** `ENROLLMENT_KEY_GENERATION_DATE`
- **Macros:** `${ device.ENROLLMENT_KEY_GENERATION_DATE }`

**Display name:** Enterprise ID

- **Web element:** `ENTERPRISEID`
- **Macros:** `${ device.ENTERPRISEID }`

**Display name:** External storage 1: available space

- **Web element:** `EXTERNAL_STORAGE1_FREE_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE1_FREE_SPACE }`

**Display name:** External storage 1: available space

- **Web element:** `EXTERNAL_STORAGE1_FREE_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE1_FREE_SPACE }`

**Display name:** External storage 1: name

- **Web element:** `EXTERNAL_STORAGE1_NAME`
- **Macros:** `${ device.EXTERNAL_STORAGE1_NAME }`

**Display name:** External storage 1: total space

- **Web element:** `EXTERNAL_STORAGE1_TOTAL_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE1_TOTAL_SPACE }`

**Display name:** External storage 2: available space



- **Web element:** EXTERNAL\_STORAGE2\_FREE\_SPACE
- **Macros:** \${ device.EXTERNAL\_STORAGE2\_FREE\_SPACE }

**Display name:** External storage 2: name

- **Web element:** EXTERNAL\_STORAGE2\_NAME
- **Macros:** \${ device.EXTERNAL\_STORAGE2\_NAME }

**Display name:** External storage 2: total space

- **Web element:** EXTERNAL\_STORAGE2\_TOTAL\_SPACE
- **Macros:** \${ device.EXTERNAL\_STORAGE2\_TOTAL\_SPACE }

**Display name:** External storage encrypted

- **Web element:** EXTERNAL\_ENCRYPTION
- **Macros:** \${ device.EXTERNAL\_ENCRYPTION }

**Display name:** FileVault Enabled

- **Web element:** IS\_FILEVAULT\_ENABLED
- **Macros:** \${ device.IS\_FILEVAULT\_ENABLED }

**Display name:** Firewall Status

- **Web element:** DEVICE\_FIREWALL\_STATUS
- **Macros:** \${ device.DEVICE\_FIREWALL\_STATUS }

**Display name:** Firewall Status

- **Web element:** DEVICE\_FIREWALL\_STATUS
- **Macros:** \${ device.DEVICE\_FIREWALL\_STATUS }

**Display name:** Firewall Status

- **Web element:** FIREWALL\_STATUS
- **Macros:** \${ device.FIREWALL\_STATUS }

**Display name:** Firmware version

- **Web element:** FIRMWARE\_VERSION
- **Macros:** \${ device.FIRMWARE\_VERSION }

**Display name:** First synchronization

- **Web element:** ZMSP\_FIRST\_SYNC
- **Macros:** \${ device.ZMSP\_FIRST\_SYNC }

**Display name:** Google Directory Alias

- **Web element:** GOOGLE\_AW\_DIRECTORY\_GOOGLE\_ALIAS
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS }`

**Display name:** Google Directory Family Name

- **Web element:** GOOGLE\_AW\_DIRECTORY\_FAMILY\_NAME
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_FAMILY_NAME }`

**Display name:** Google Directory Name

- **Web element:** GOOGLE\_AW\_DIRECTORY\_NAME
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_NAME }`

**Display name:** Google Directory Primary Email

- **Web element:** GOOGLE\_AW\_DIRECTORY\_PRIMARY
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_PRIMARY }`

**Display name:** Google Directory User ID

- **Web element:** GOOGLE\_AW\_DIRECTORY\_USER\_ID
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_USER_ID }`

**Display name:** GPS altitude

- **Web element:** GPS\_ALTITUDE\_FROM\_GPS
- **Macros:** `${ device.GPS_ALTITUDE_FROM_GPS }`

**Display name:** GPS course

- **Web element:** GPS\_COURSE\_FROM\_GPS
- **Macros:** `${ device.GPS_COURSE_FROM_GPS }`

**Display name:** GPS horizontal accuracy

- **Web element:** GPS\_HORIZONTAL\_ACCURACY\_FROM\_GPS
- **Macros:** `${ device.GPS_HORIZONTAL_ACCURACY_FROM_GPS }`

**Display name:** GPS latitude

- **Web element:** GPS\_LATITUDE\_FROM\_GPS
- **Macros:** `${ device.GPS_LATITUDE_FROM_GPS }`

**Display name:** GPS longitude

- **Web element:** GPS\_LONGITUDE\_FROM\_GPS

- **Macros:** `${ device.GPS_LONGITUDE_FROM_GPS }`

**Display name:** GPS speed

- **Web element:** `GPS_SPEED_FROM_GPS`
- **Macros:** `${ device.GPS_SPEED_FROM_GPS }`

**Display name:** GPS timestamp

- **Web element:** `GPS_TIMESTAMP_FROM_GPS`
- **Macros:** `${ device.GPS_TIMESTAMP_FROM_GPS }`

**Display name:** GPS vertical accuracy

- **Web element:** `GPS_VERTICAL_ACCURACY_FROM_GPS`
- **Macros:** `${ device.GPS_VERTICAL_ACCURACY_FROM_GPS }`

**Display name:** Hardware Device ID

- **Web element:** `HW_DEVICE_ID`
- **Macros:** `${ device.HW_DEVICE_ID }`

**Display name:** Hardware encryption capabilities

- **Web element:** `HARDWARE_ENCRYPTION_CAPS`
- **Macros:** `${ device.HARDWARE_ENCRYPTION_CAPS }`

**Display name:** HAS\_CONTAINER

- **Web element:** `HAS_CONTAINER`
- **Macros:** `${ device.HAS_CONTAINER }`

**Display name:** Hash of the Apple App Store account currently logged on

- **Web element:** `ITUNES_STORE_ACCOUNT_HASH`
- **Macros:** `${ device.ITUNES_STORE_ACCOUNT_HASH }`

**Display name:** Home carrier network

- **Web element:** `SIM_CARRIER_NETWORK`
- **Macros:** `${ device.SIM_CARRIER_NETWORK }`

**Display name:** Home mobile country code

- **Web element:** `SIM_MCC`
- **Macros:** `${ device.SIM_MCC }`

**Display name:** Home mobile network code

- **Web element:** SIM\_MNC
- **Macros:** `${ device.SIM_MNC }`

**Display name:** ICCID

- **Web element:** ICCID
- **Macros:** `${ device.ICCID }`

**Display name:** Identity

- **Web element:** AS\_DEVICE\_IDENTITY
- **Macros:** `${ device.AS_DEVICE_IDENTITY }`

**Display name:** IMEI/MEID number

- **Web element:** IMEI
- **Macros:** `${ device.IMEI }`

**Display name:** IMSI

- **Web element:** SIM\_ID
- **Macros:** `${ device.SIM_ID }`

**Display name:** Internal storage encrypted

- **Web element:** LOCAL\_ENCRYPTION
- **Macros:** `${ device.LOCAL_ENCRYPTION }`

**Display name:** IP location

- **Web element:** IP\_LOCATION
- **Macros:** `${ device.IP_LOCATION }`

**Display name:** IPV4 Address

- **Web element:** IP\_ADDRESSV4
- **Macros:** `${ device.IP_ADDRESSV4 }`

**Display name:** IPV6 Address

- **Web element:** IP\_ADDRESSV6
- **Macros:** `${ device.IP_ADDRESSV6 }`

**Display name:** Issued At

- **Web element:** WINDOWS\_HAS\_ISSUED\_AT
- **Macros:** `${ device.WINDOWS_HAS_ISSUED_AT }`

**Display name:** Jailbroken/Rooted

- **Web element:** ROOT\_ACCESS
- **Macros:** \${ device.ROOT\_ACCESS }

**Display name:** Kernel Debugging Enabled?

- **Web element:** WINDOWS\_HAS\_OS\_KERNEL\_DEBUGGING\_ENABLED
- **Macros:** \${ device.WINDOWS\_HAS\_OS\_KERNEL\_DEBUGGING\_ENABLED }

**Display name:** Kiosk mode

- **Web element:** IS\_KIOSK
- **Macros:** \${ device.IS\_KIOSK }

**Display name:** Last known IP address

- **Web element:** LAST\_IP\_ADDR
- **Macros:** \${ device.LAST\_IP\_ADDR }

**Display name:** Last policy update time

- **Web element:** LAST\_POLICY\_UPDATE\_TIME
- **Macros:** \${ device.LAST\_POLICY\_UPDATE\_TIME }

**Display name:** Last scan date

- **Web element:** PreviousScanDate
- **Macros:** \${ device.PreviousScanDate }

**Display name:** Last scan result

- **Web element:** PreviousScanResult
- **Macros:** \${ device.PreviousScanResult }

**Display name:** Last scheduled software updates

- **Web element:** AVAILABLE\_OS\_UPDATE\_INSTALL\_LAST\_ATTEMPT\_TIME
- **Macros:** \${ device.AVAILABLE\_OS\_UPDATE\_INSTALL\_LAST\_ATTEMPT\_TIME }

**Display name:** Last scheduled software updates failure message

- **Web element:** AVAILABLE\_OS\_UPDATE\_INSTALL\_FAIL\_MSG
- **Macros:** \${ device.AVAILABLE\_OS\_UPDATE\_INSTALL\_FAIL\_MSG }

**Display name:** Last scheduled software updates status

- **Web element:** AVAILABLE\_OS\_UPDATE\_INSTALL\_STATUS

- **Macros:** `${ device.AVAILABLE_OS_UPDATE_INSTALL_STATUS }`

**Display name:** Last synchronization

- **Web element:** `ZMSP_LAST_SYNC`
- **Macros:** `${ device.ZMSP_LAST_SYNC }`

**Display name:** Locator service enabled

- **Web element:** `DEVICE_LOCATOR`
- **Macros:** `${ device.DEVICE_LOCATOR }`

**Display name:** MAC Address

- **Web element:** `MAC_ADDRESS`
- **Macros:** `${ device.MAC_ADDRESS }`

**Display name:** MAC Address Network Connection

- **Web element:** `MAC_NETWORK_CONNECTION`
- **Macros:** `${ device.MAC_NETWORK_CONNECTION }`

**Display name:** MAC Address Type

- **Web element:** `MAC_ADDRESS_TYPE`
- **Macros:** `${ device.MAC_ADDRESS_TYPE }`

**Display name:** Mailbox Setup

- **Web element:** `GOOGLE_AW_DIRECTORY_MAILBOX_SETUP`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP }`

**Display name:** Main battery

- **Web element:** `MAIN_BATTERY_PERCENT`
- **Macros:** `${ device.MAIN_BATTERY_PERCENT }`

**Display name:** MDM lost mode enabled

- **Web element:** `IS_MDM_LOST_MODE_ENABLED`
- **Macros:** `${ device.IS_MDM_LOST_MODE_ENABLED }`

**Display name:** MDX\_SHARED\_ENCRYPTION\_KEY

- **Web element:** `MDX_SHARED_ENCRYPTION_KEY`
- **Macros:** `${ device.MDX_SHARED_ENCRYPTION_KEY }`

**Display name:** MEID

- **Web element:** MEID
- **Macros:** `${ device.MEID }`

**Display name:** Mobile phone number

- **Web element:** TEL\_NUMBER
- **Macros:** `${ device.TEL_NUMBER }`

**Display name:** Model ID

- **Web element:** MODEL\_ID
- **Macros:** `${ device.MODEL_ID }`

**Display name:** Model Number

- **Web element:** MODEL\_NUMBER
- **Macros:** `${ device.MODEL_NUMBER }`

**Display name:** Network Adapter Type

- **Web element:** NETWORK\_ADAPTER\_TYPE
- **Macros:** `${ device.NETWORK_ADAPTER_TYPE }`

**Display name:** Operating system build

- **Web element:** SYSTEM\_OS\_BUILD
- **Macros:** `${ device.SYSTEM_OS_BUILD }`

**Display name:** Operating System Edition

- **Web element:** OS\_EDITION
- **Macros:** `${ device.OS_EDITION }`

**Display name:** Operating system language (locale)

- **Web element:** SYSTEM\_LANGUAGE
- **Macros:** `${ device.SYSTEM_LANGUAGE }`

**Display name:** Operating system version

- **Web element:** SYSTEM\_OS\_VERSION
- **Macros:** `${ device.SYSTEM_OS_VERSION }`

**Display name:** Organization address

- **Web element:** ORGANIZATION\_ADDRESS
- **Macros:** `${ device.ORGANIZATION_ADDRESS }`

**Display name:** Organization email

- **Web element:** ORGANIZATION\_EMAIL
- **Macros:** \${ device.ORGANIZATION\_EMAIL }

**Display name:** Organization magic

- **Web element:** ORGANIZATION\_MAGIC
- **Macros:** \${ device.ORGANIZATION\_MAGIC }

**Display name:** Organization name

- **Web element:** ORGANIZATION\_NAME
- **Macros:** \${ device.ORGANIZATION\_NAME }

**Display name:** Organization phone number

- **Web element:** ORGANIZATION\_PHONE
- **Macros:** \${ device.ORGANIZATION\_PHONE }

**Display name:** Out of Compliance

- **Web element:** OUT\_OF\_COMPLIANCE
- **Macros:** \${ device.OUT\_OF\_COMPLIANCE }

**Display name:** Owned by

- **Web element:** CORPORATE\_OWNED
- **Macros:** \${ device.CORPORATE\_OWNED }

**Display name:** Passcode compliant

- **Web element:** PASSCODE\_IS\_COMPLIANT
- **Macros:** \${ device.PASSCODE\_IS\_COMPLIANT }

**Display name:** Passcode compliant with configuration

- **Web element:** PASSCODE\_IS\_COMPLIANT\_WITH\_CFG
- **Macros:** \${ device.PASSCODE\_IS\_COMPLIANT\_WITH\_CFG }

**Display name:** Passcode present

- **Web element:** PASSCODE\_PRESENT
- **Macros:** \${ device.PASSCODE\_PRESENT }

**Display name:** PCRO

- **Web element:** WINDOWS\_HAS\_PCRO



- **Macros:** `${ device.WINDOWS_HAS_PCR0 }`

**Display name:** Perimeter breach

- **Web element:** `GPS_PERIMETER_BREACH`
- **Macros:** `${ device.GPS_PERIMETER_BREACH }`

**Display name:** Periodic check

- **Web element:** `PerformPeriodicCheck`
- **Macros:** `${ device.PerformPeriodicCheck }`

**Display name:** Personal Hotspot activated

- **Web element:** `PERSONAL_HOTSPOT_ENABLED`
- **Macros:** `${ device.PERSONAL_HOTSPOT_ENABLED }`

**Display name:** PIN code for geofence

- **Web element:** `PIN_CODE_FOR_GEO_FENCE`
- **Macros:** `${ device.PIN_CODE_FOR_GEO_FENCE }`

**Display name:** Platform

- **Web element:** `SYSTEM_PLATFORM`
- **Macros:** `${ device.SYSTEM_PLATFORM }`

**Display name:** Platform API level

- **Web element:** `API_LEVEL`
- **Macros:** `${ device.API_LEVEL }`

**Display name:** Policy name

- **Web element:** `POLICY_NAME`
- **Macros:** `${ device.POLICY_NAME }`

**Display name:** Primary Phone Number

- **Web element:** `IDENTITY1_PHONENUMBER`
- **Macros:** `${ device.IDENTITY1_PHONENUMBER }`

**Display name:** Primary SIM Carrier Operator

- **Web element:** `IDENTITY1_CARRIER_NETWORK_OPERATOR`
- **Macros:** `${ device.IDENTITY1_CARRIER_NETWORK_OPERATOR }`

**Display name:** Primary SIM ICCID

- **Web element:** IDENTITY1\_ICCID
- **Macros:** `${ device.IDENTITY1_ICCID }`

**Display name:** Primary SIM IMEI

- **Web element:** IDENTITY1\_IMEI
- **Macros:** `${ device.IDENTITY1_IMEI }`

**Display name:** Primary SIM IMSI

- **Web element:** IDENTITY1\_IMSI
- **Macros:** `${ device.IDENTITY1_IMSI }`

**Display name:** Primary SIM Roaming

- **Web element:** IDENTITY1\_ROAMING
- **Macros:** `${ device.IDENTITY1_ROAMING }`

**Display name:** Primary SIM Roaming

- **Web element:** IDENTITY1\_ROAMING\_COMPLIANCE
- **Macros:** `${ device.IDENTITY1_ROAMING_COMPLIANCE }`

**Display name:** Product name

- **Web element:** PRODUCT\_NAME
- **Macros:** `${ device.PRODUCT_NAME }`

**Display name:** Publisher Device ID

- **Web element:** PUBLISHER\_DEVICE\_ID
- **Macros:** `${ device.PUBLISHER_DEVICE_ID }`

**Display name:** Reset Count

- **Web element:** WINDOWS\_HAS\_RESET\_COUNT
- **Macros:** `${ device.WINDOWS_HAS_RESET_COUNT }`

**Display name:** Restart Count

- **Web element:** WINDOWS\_HAS\_RESTART\_COUNT
- **Macros:** `${ device.WINDOWS_HAS_RESTART_COUNT }`

**Display name:** Safe Mode Enabled?

- **Web element:** WINDOWS\_HAS\_SAFE\_MODE
- **Macros:** `${ device.WINDOWS_HAS_SAFE_MODE }`

**Display name:** Samsung Knox API available

- **Web element:** SAMSUNG\_KNOX
- **Macros:** `${ device.SAMSUNG_KNOX }`

**Display name:** Samsung Knox API version

- **Web element:** SAMSUNG\_KNOX\_VERSION
- **Macros:** `${ device.SAMSUNG_KNOX_VERSION }`

**Display name:** Samsung Knox attestation

- **Web element:** SAMSUNG\_KNOX\_ATTESTED
- **Macros:** `${ device.SAMSUNG_KNOX_ATTESTED }`

**Display name:** Samsung Knox attestation updated date

- **Web element:** SAMSUNG\_KNOX\_ATT\_UPDATED\_TIME
- **Macros:** `${ device.SAMSUNG_KNOX_ATT_UPDATED_TIME }`

**Display name:** Samsung SAFE API available

- **Web element:** SAMSUNG\_MDM
- **Macros:** `${ device.SAMSUNG_MDM }`

**Display name:** Samsung SAFE API version

- **Web element:** SAMSUNG\_MDM\_VERSION
- **Macros:** `${ device.SAMSUNG_MDM_VERSION }`

**Display name:** SBCP Hash

- **Web element:** WINDOWS\_HAS\_SBCP\_HASH
- **Macros:** `${ device.WINDOWS_HAS_SBCP_HASH }`

**Display name:** Screen: height

- **Web element:** SCREEN\_HEIGHT
- **Macros:** `${ device.SCREEN_HEIGHT }`

**Display name:** Screen: number of colors

- **Web element:** SCREEN\_NB\_COLORS
- **Macros:** `${ device.SCREEN_NB_COLORS }`

**Display name:** Screen: size

- **Web element:** SCREEN\_SIZE

- **Macros:** `${ device.SCREEN_SIZE }`

**Display name:** Screen: width

- **Web element:** `SCREEN_WIDTH`
- **Macros:** `${ device.SCREEN_WIDTH }`

**Display name:** Screen: X-axis resolution

- **Web element:** `SCREEN_XDPI`
- **Macros:** `${ device.SCREEN_XDPI }`

**Display name:** Screen: Y-axis resolution

- **Web element:** `SCREEN_YDPI`
- **Macros:** `${ device.SCREEN_YDPI }`

**Display name:** Secondary Phone Number

- **Web element:** `IDENTITY2_PHONENUMBER`
- **Macros:** `${ device.IDENTITY2_PHONENUMBER }`

**Display name:** Secondary SIM Carrier Operator

- **Web element:** `IDENTITY2_CARRIER_NETWORK_OPERATOR`
- **Macros:** `${ device.IDENTITY2_CARRIER_NETWORK_OPERATOR }`

**Display name:** Secondary SIM ICCID

- **Web element:** `IDENTITY2_ICCID`
- **Macros:** `${ device.IDENTITY2_ICCID }`

**Display name:** Secondary SIM IMEI

- **Web element:** `IDENTITY2_IMEI`
- **Macros:** `${ device.IDENTITY2_IMEI }`

**Display name:** Secondary SIM IMSI

- **Web element:** `IDENTITY2_IMSI`
- **Macros:** `${ device.IDENTITY2_IMSI }`

**Display name:** Secondary SIM Roaming

- **Web element:** `IDENTITY2_ROAMING`
- **Macros:** `${ device.IDENTITY2_ROAMING }`

**Display name:** Secondary SIM Roaming Compliance

- **Web element:** IDENTITY2\_ROAMING\_COMPLIANCE
- **Macros:** `${ device.IDENTITY2_ROAMING_COMPLIANCE }`

**Display name:** Secure Boot Enabled?

- **Web element:** WINDOWS\_HAS\_SECURE\_BOOT\_ENABLED
- **Macros:** `${ device.WINDOWS_HAS_SECURE_BOOT_ENABLED }`

**Display name:** Secure Boot Status

- **Web element:** SECURE\_BOOT\_STATE
- **Macros:** `${ device.SECURE_BOOT_STATE }`

**Display name:** SecureContainer Enabled

- **Web element:** DLP\_ACTIVE
- **Macros:** `${ device.DLP_ACTIVE }`

**Display name:** Security patch level

- **Web element:** SYSTEM\_SECURITY\_PATCH\_LEVEL
- **Macros:** `${ device.SYSTEM_SECURITY_PATCH_LEVEL }`

**Display name:** Serial number

- **Web element:** SERIAL\_NUMBER
- **Macros:** `${ device.SERIAL_NUMBER }`

**Display name:** SMS capable

- **Web element:** IS\_SMS\_CAPABLE
- **Macros:** `${ device.IS_SMS_CAPABLE }`

**Display name:** Supervised

- **Web element:** SUPERVISED
- **Macros:** `${ device.SUPERVISED }`

**Display name:** Suspension Reason

- **Web element:** GOOGLE\_AW\_DIRECTORY\_SUSPENSION\_REASON
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_SUSPENSION_REASON }`

**Display name:** Tampered Status

- **Web element:** TAMPERED\_STATUS
- **Macros:** `${ device.TAMPERED_STATUS }`

**Display name:** Terms & Conditions

- **Web element:** TERMS\_AND\_CONDITIONS
- **Macros:** `${ device.TERMS_AND_CONDITIONS }`

**Display name:** Terms And Agreement Accepted?

- **Web element:** GOOGLE\_AW\_DIRECTORY\_AGREED\_TO\_TERMS
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS }`

**Display name:** Test Signing Enabled?

- **Web element:** WINDOWS\_HAS\_TEST\_SIGNING\_ENABLED
- **Macros:** `${ device.WINDOWS_HAS_TEST_SIGNING_ENABLED }`

**Display name:** Total RAM

- **Web element:** MEMORY
- **Macros:** `${ device.MEMORY }`

**Display name:** Total storage space

- **Web element:** TOTAL\_DISK\_SPACE
- **Macros:** `${ device.TOTAL_DISK_SPACE }`

**Display name:** TPM version

- **Web element:** TPM\_VERSION
- **Macros:** `${ device.TPM_VERSION }`

**Display name:** UDID

- **Web element:** UDID
- **Macros:** `${ device.UDID }`

**Display name:** User Account Control Status

- **Web element:** UAC\_STATUS
- **Macros:** `${ device.UAC_STATUS }`

**Display name:** User agent

- **Web element:** USER\_AGENT
- **Macros:** `${ device.USER_AGENT }`

**Display name:** User defined #1

- **Web element:** USER\_DEFINED\_1

- **Macros:** `${ device.USER_DEFINED_1 }`

**Display name:** User defined #2

- **Web element:** `USER_DEFINED_2`
- **Macros:** `${ device.USER_DEFINED_2 }`

**Display name:** User defined #3

- **Web element:** `USER_DEFINED_3`
- **Macros:** `${ device.USER_DEFINED_3 }`

**Display name:** User language (locale)

- **Web element:** `USER_LANGUAGE`
- **Macros:** `${ device.USER_LANGUAGE }`

**Display name:** Vendor

- **Web element:** `VENDOR`
- **Macros:** `${ device.VENDOR }`

**Display name:** Voice capable

- **Web element:** `IS_VOICE_CAPABLE`
- **Macros:** `${ device.IS_VOICE_CAPABLE }`

**Display name:** Voice roaming allowed

- **Web element:** `VOICE_ROAMING_ENABLED`
- **Macros:** `${ device.VOICE_ROAMING_ENABLED }`

**Display name:** VSM Enabled?

- **Web element:** `WINDOWS_HAS_VSM_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_VSM_ENABLED }`

**Display name:** Wi-Fi MAC address

- **Web element:** `WIFI_MAC`
- **Macros:** `${ device.WIFI_MAC }`

**Display name:** WINDOWS\_ENROLLMENT\_KEY

- **Web element:** `WINDOWS_ENROLLMENT_KEY`
- **Macros:** `${ device.WINDOWS_ENROLLMENT_KEY }`

**Display name:** WinPE Enabled?

- **Web element:** WINDOWS\_HAS\_WINPE
- **Macros:** \${ device.WINDOWS\_HAS\_WINPE }

**Display name:** WNS Notification Status

- **Web element:** PROPERTY\_WNS\_PUSH\_STATUS
- **Macros:** \${ device.PROPERTY\_WNS\_PUSH\_STATUS }

**Display name:** WNS Notification URL

- **Web element:** PROPERTY\_WNS\_PUSH\_URL
- **Macros:** \${ device.PROPERTY\_WNS\_PUSH\_URL }

**Display name:** WNS Notification URL expiry date

- **Web element:** PROPERTY\_WNS\_PUSH\_URL\_EXPIRY
- **Macros:** \${ device.PROPERTY\_WNS\_PUSH\_URL\_EXPIRY }

**Display name:** Endpoint Management agent ID

- **Web element:** ENROLLMENT\_AGENT\_ID
- **Macros:** {device.ENROLLMENT\_AGENT\_ID}‘

**Display name:** Endpoint Management agent revision

- **Web element:** EW\_REVISION
- **Macros:** \${ device.EW\_REVISION }

**Display name:** Endpoint Management agent version

- **Web element:** EW\_VERSION
- **Macros:** \${ device.EW\_VERSION }

**Display name:** Zebra API available

- **Web element:** ZEBRA\_MDM
- **Macros:** \${ device.ZEBRA\_MDM }

**Display name:** Zebra MXMF version

- **Web element:** ZEBRA\_MDM\_VERSION
- **Macros:** \${ device.ZEBRA\_MDM\_VERSION }

**Display name:** Zebra Patch version

- **Web element:** ZEBRA\_PATCH\_VERSION
- **Macros:** \${ device.ZEBRA\_PATCH\_VERSION }



## Macros to obtain built-in user properties

Display name	Macros
domainname (domain name; default domain)	<code>\${ user.domainname }</code>
loginname (user name plus domain name)	<code>\${ user.loginname }</code>
username (login name minus the domain, if any)	<code>\${ user.username }</code>

## Macros for all user properties

Display name	Web element	Macros
Active Directory failed logon tries	badpwdcount	<code>\${ user.badpwdcount }</code>
ActiveSync user email	asuseremail	<code>\${ user.asuseremail }</code>
ASM data source	asmpersonsource	<code>\${ user.asmpersonsource }</code>
ASM Deployment Program account name	asmdepaccount	<code>\${ user.asmdepaccount }</code>
ASM managed Apple ID	asmpersonmanagedappleid	<code>\${ user.asmpersonmanagedappleid }</code>
ASM passcode type	asmpersonpasscodetype	<code>\${ user.asmpersonpasscodetype }</code>
ASM person ID	asmpersonid	<code>\${ user.asmpersonid }</code>
ASM person status	asmpersonstatus	<code>\${ user.asmpersonstatus }</code>
ASM person title	asmpersontitle	<code>\${ user.asmpersontitle }</code>
ASM person unique ID	asmpersonuniqueid	<code>\${ user.asmpersonuniqueid }</code>
ASM source system ID	asmpersonsourcesystemid	<code>\${ user.asmpersonsourcesystemid }</code>

<b>Display name</b>	<b>Web element</b>	<b>Macros</b>
ASM student grade	asmpersongrade	<code>#{ user.asmpersongrade }</code>
BES user email	besuseremail	<code>#{ user.besuseremail }</code>
Company	company	<code>#{ user.company }</code>
Company name	companyname	<code>#{ user.companyname }</code>
Country	c	<code>#{ user.c }</code>
Department	department	<code>#{ user.department }</code>
Description	description	<code>#{ user.description }</code>
Disabled user	disableduser	<code>#{ user.disableduser }</code>
Display name	displayname	<code>#{ user.displayname }</code>
Distinguished name	distinguishedname	<code>#{ user.distinguishedname }</code>
Domain name	domainname	<code>#{ user.domainname }</code>
Email	mail	<code>#{ user.mail }</code>
First name	givenname	<code>#{ user.givenname }</code>
Home address	homestreetaddress	<code>#{ user.homestreetaddress }</code>
Home city	homecity	<code>#{ user.homecity }</code>
Home country	homecountry	<code>#{ user.homecountry }</code>
Home fax	homefax	<code>#{ user.homefax }</code>
Home phone	homephone	<code>#{ user.homephone }</code>
Home state/region	homestate	<code>#{ user.homestate }</code>
Home zip or post code	homezip	<code>#{ user.homezip }</code>
IP phone	ipphone	<code>#{ user.ipphone }</code>
Middle initial	middleinitial	<code>#{ user.middleinitial }</code>
Middle name	middlename	<code>#{ user.middlename }</code>
Mobile	mobile	<code>#{ user.mobile }</code>
Name	cn	<code>#{ user.cn }</code>

Display name	Web element	Macros
Office address	physicaldeliveryofficena	<code>\${ user. physicaldeliveryofficename }</code>
Office city	l	<code>\${ user.l }</code>
Office fax number	facsimiletelephonenumber	<code>\${ user. facsimiletelephonenumber }</code>
Office state/province	st	<code>\${ user.st }</code>
Office street address	officestreetaddress	<code>\${ user. officestreetaddress }</code>
Office telephone number	telephonenumber	<code>\${ user. telephonenumber }</code>
Office zip or post code	postalcode	<code>\${ user.postalcode }</code>
P.O. box	postofficebox	<code>\${ user.postofficebox }</code>
Pager	pager	<code>\${ user.pager }</code>
Primary group ID	primarygroupid	<code>\${ user.primarygroupid }</code>
SAM account	samaccountname	<code>\${ user.samaccountname }</code>
Street address	streetaddress	<code>\${ user.streetaddress }</code>
Surname	sn	<code>\${ user.sn }</code>
Title	title	<code>\${ user.title }</code>
User logon name	userprincipalname	<code>\${ user. userprincipalname }</code>

## Automated actions

September 9, 2021

You create automated actions in Endpoint Management to program a reaction to:

- Events

- User or device properties
- The existence of apps on user devices

When you create an automated action, the triggers defined for the action determine what happens on the user device when it is connected to Endpoint Management. When an event is triggered, you can send a notification to the user to correct an issue before more serious action is taken.

The effects that you set to happen automatically range from the following:

- Fully or selectively wiping the device.
- Setting the device to out of compliance.
- Revoking the device.
- Sending a notification to the user to correct an issue before more severe action is taken.

You can configure app lock and app wipe actions for MAM-only mode.

You can use automated actions to mark Windows 10 and Windows 11 devices joined to Azure Active Directory (AD) out of compliance in Azure AD.

**Note:**

Before you can notify users, you must configure notification servers in the Endpoint Management settings for SMTP and SMS so that Endpoint Management can send the messages. For information, see [Notifications](#). Also, set up any notification templates you plan to use before proceeding. For details, see [Create and update notification templates](#).

### Example actions

Here are some examples of using automated actions:

#### Example one

- You want to detect an app that you previously blocked (for example, “Words with Friends”). You can specify a trigger that sets the user device out of compliance after detecting the “Words with Friends” app. The action then notifies users that they must remove the app to bring their device back into compliance. You can also set a time limit for how long to wait for users to comply. After that time limit, a defined action occurs, such as selectively wiping the device.

#### Example two

- You want to verify if customers are using the latest firmware and block access to resources if users need to update their devices. You can specify a trigger that sets the user device out of compliance when a user device doesn’t have the latest version. You use automated actions to block resources and to notify customers.

#### Example three

- A user device is put into an out-of-compliance state and the user then fixes the device. You can configure a policy to deploy a package that resets the device into a compliant state.

#### Example four

- You want to mark user devices that have been inactive for a certain time period as out of compliance. You can create an automated action for inactive devices as follows:
  1. In the Endpoint Management console, go to **Settings > Network Access Control** and then select **Inactive Devices**. For more information about the **Inactive Devices** setting, see [Network Access Control](#).
  2. Follow the steps to add an action, as outlined in [Add and manage actions](#). The only difference is that you configure settings as follows on the **Action details** page:
    - **Trigger**. Select **Device property, Out of compliance**, and **True**.
    - **Action**. Select **Send notification** and select a template that you created by using **Notification Template** in **Settings**. Then set the delay in days, hours, or minutes before performing the action. Set the interval at which the action repeats until the user addresses the triggering issue.

#### Tip:

To delete inactive devices in bulk, use the [Endpoint Management Public REST API](#). You first manually obtain the device IDs for inactive devices you want to delete and then run the delete API to delete them in bulk.

## Add and manage actions

To add, edit, and filter automated actions:

1. From the Endpoint Management console, click **Configure > Actions**. The **Actions** page appears.
2. On the **Actions** page, do one of the following:
  - Click **Add** to add an action.
  - Select an existing action to edit or delete. Click the option you want to use.
3. The **Action Information** page appears.
4. On the **Action Information** page, enter or modify the following information:
  - **Name:** Type a name to identify the action. This field is required.
  - **Description:** Describe what the action is meant to do.
5. Click **Next**. The **Action details** page appears.

The following example shows how to set up an **Event** trigger. If you select a different trigger, the resulting options differ from the options shown here.

6. On the **Action details** page, enter or modify the following information:

In the **Trigger** list, click the event trigger type for this action. Select one of the following triggers:

- **Event:** Checks whether the device status matches the non-compliance event you choose, then reacts to it.
- **Device property:** Checks for a specific value for a device attribute on a device that is MDM-managed, then reacts to it. For more information, see the [Device property names and values](#) PDF.
- **User property:** Reacts to a specific value for a user attribute, usually from Active Directory.
- **Installed app name:** Reacts to an app being installed. Doesn't apply to MAM-only mode. Requires the app inventory policy to be enabled on the device. The app inventory policy is enabled on all platforms by default. For details, see [App inventory device policy](#).
- **Policy returned value:** Checks if the value returned from PowerShell scripts meets certain logic criteria. The Windows Agent policy must be enabled and configured. For more information on the Windows Agent policy, see [Windows Agent device policy](#).

7. In the next list, click the response to the trigger.

8. In the **Action** list, click the action to be performed when the trigger criterion is met. Except for the **Send notification** action, you choose a time frame in which users can resolve the issue that caused the trigger. If the issue isn't resolved within that time frame, the selected action is taken. For a definition of the actions, see [Security actions](#).

If you pick **Send notification**, use the following steps to send a notification action.

9. In the next list, select the template to use for the notification. Notification templates relevant to the selected event appear. If there's no template for the notification type, you are prompted

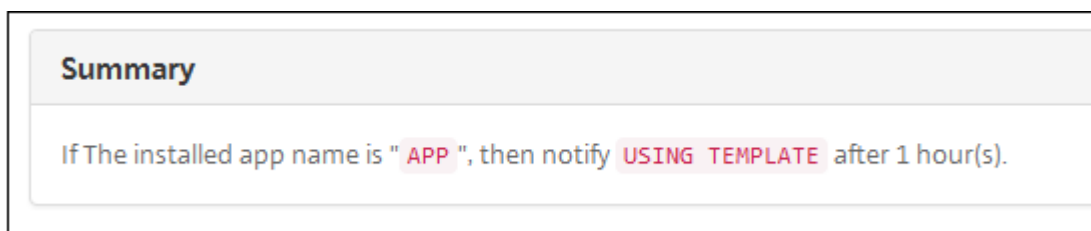
to configure a template with the message: No template for this event type. Create a template using **Notification Template** in **Settings**.

To notify users, use **Settings > Notification Server** to configure settings for SMTP and SMS so that Endpoint Management can send the messages. See [Notifications](#). Also, before proceeding, use **Settings > Notification Template** to set up any notification templates you plan to use. See [Create and update notification templates](#).

After you select the template, click **Preview notification message**.

10. In the following fields, set the delay in days, hours, or minutes before performing the action. Set the interval at which the action repeats until the user addresses the triggering issue.

11. In **Summary**, verify that you created the automated action as you intended.



12. After you configure the action details, you can configure deployment rules for each platform individually. To do so, complete step 13 for each platform you choose.
13. Configure deployment rules. For general information about configuring deployment rules, see [Deploy resources](#).

For this example:

- Device ownership must be **BYOD**.
  - Device must be passcode compliant.
  - Device mobile country code cannot be only Andorra.
14. When you are done configuring the platform deployment rules for the action, click **Next**. The **Actions assignment** page appears, where you assign the action to a delivery group or groups. This step is optional.
  15. Next to **Choose delivery groups**, type to find a delivery group or select groups in the list. The groups you select appear **Delivery groups to receive app assignment** list.
  16. Expand **Deployment Schedule** and then configure the following settings:
    - Next to **Deploy**, click **On** to schedule deployment or click **Off** to prevent deployment. The default option is **On**. If you choose **Off**, no other options are required.
    - Next to **Deployment schedule**, click **Now** or **Later**. The default option is **Now**.
    - If you click **Later**, click the calendar icon and then select the date and time for deployment.
    - Next to **Deployment condition**, click **On every connection** or click **Only when previous deployment has failed**. The default option is **On every connection**.
    - Next to **Deploy for always-on connection**, click **On** or **Off**. The default option is **Off**.

This option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.

**Note:**

This option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.

The always-on option:

- Is not available for iOS devices



- Is not available for Android, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with version 10.18.19 or later
- Is not recommended for Android, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with before version 10.18.19

The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

17. Click **Next**. The **Summary** page appears, where you can verify the action configuration.
18. Click **Save** to save the action.

### App lock and app wipe actions for MAM-only mode

You can wipe or lock apps on a device for all four categories of triggers listed in the Endpoint Management console: event, device property, user property, and installed app name.

#### To configure automatic app wipe or app lock

1. In the Endpoint Management console, click **Configure > Actions**.
2. On the **Actions** page, click **Add**.
3. On the **Action Information** page, enter a name for the action and an optional description.
4. On the **Action Details** page, select the trigger you want.
5. In **Action**, select an action.

For this step, keep the following conditions in mind:

When the trigger type is **Event** and the value is not **Active Directory disabled user**, the **App wipe** and **App lock** actions don't appear.

When the trigger type is **Device property** and the value is **MDM lost mode enabled**, the following actions don't appear:

- Selectively wipe the device
- Completely wipe the device
- Revoke the device

For each option, a 1 hour delay is automatically set, but you can select the delay period in minutes, hours or days. The intent of the delay is to give users time to fix an issue before the action occurs. For more information about the App wipe and App lock actions, see [Security actions](#).

#### Note:

If you set the trigger to **event**, the repeat interval is automatically a minimum of 1 hour. The device must carry out a refresh of the policies to synchronize with the server for the

notification to come in. Typically, a device synchronizes with the server when users sign on or manually refresh their policies through Secure Hub.

An extra delay of approximately 1 hour might occur before any action is carried out, to allow the Active Directory database to synchronize with Endpoint Management.

The screenshot shows the 'Action details' configuration page in the Citrix Endpoint Management console. The page is titled 'Action details' and includes a sidebar with 'Actions' and a main content area with sections for 'Trigger', 'Action', and 'Summary'.

**Actions**

- 1 Action Info
- 2 Details
- 3 Assignment (optional)
- 4 Summary

**Action details**

Choose a trigger event and the associated action for that event.

**Trigger\***

- Device property
- Out of compliance
- Is
- True

**Action\***

- App wipe
- 1
- Hours

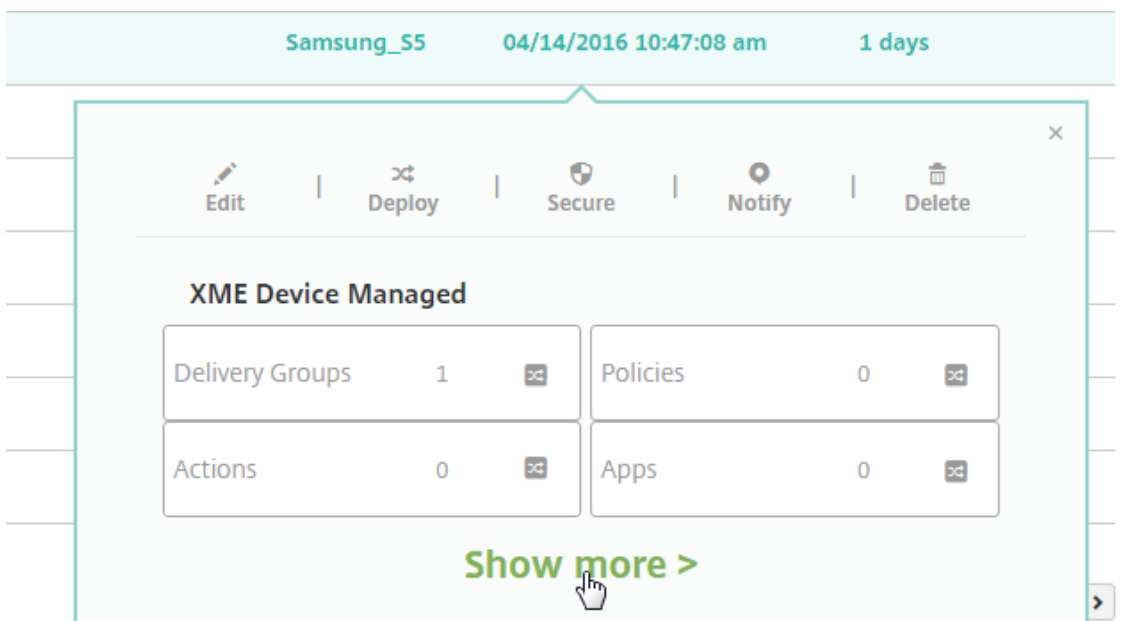
**Summary**

If device has been marked as Out of Compliance, then app wipe the device after 1 hour(s).

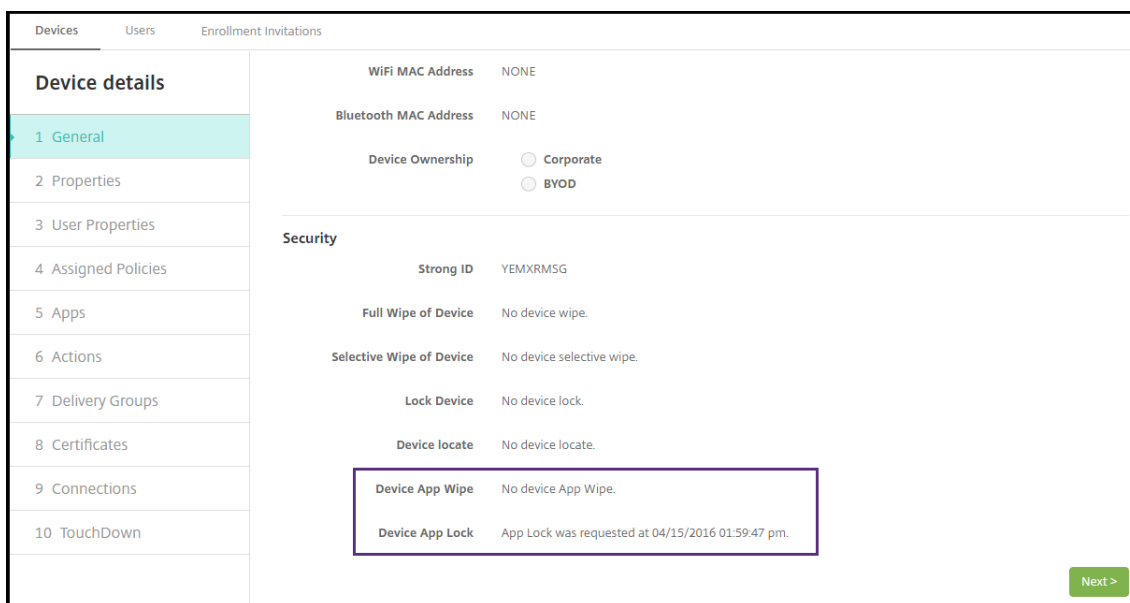
6. Configure deployment rules and then click **Next**.
7. Configure delivery group assignments and a deployment schedule and then click **Next**.
8. Click **Save**.

### To check app lock or app wipe status

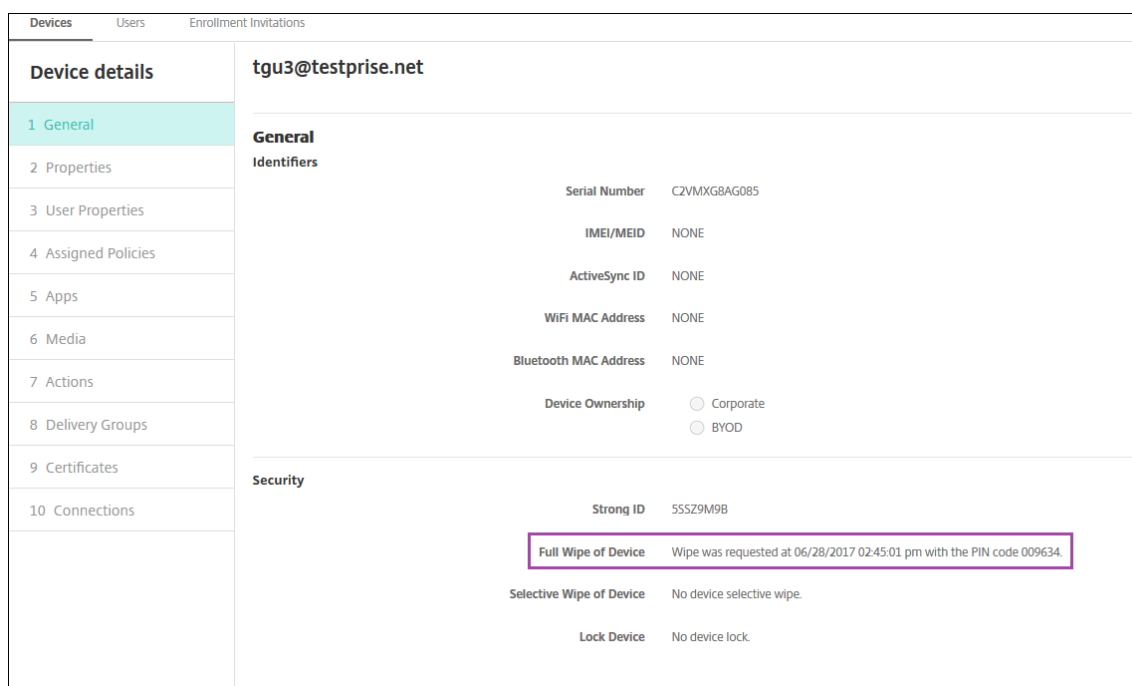
1. Go to **Manage > Devices**, click a device, and then click **Show more**.



2. Scroll to **Device App Wipe** and **Device App Lock**.



After a device gets wiped, the user is prompted to enter a PIN code. If the user forgets the code, you can look it up in the Device Details.



## Marking Windows 10 and Windows 11 devices out of compliance in Azure AD

When Windows 10 and Windows 11 devices that are joined to Azure AD are marked out-of-compliance by Endpoint Management, they can also be marked out-of-compliance in Azure AD. To enable this functionality, add permissions to the on-premises MDM application to access the Microsoft Graph API in the Azure AD portal.

1. Log in to the Azure AD portal with your Azure AD administrator credentials.
2. In the Azure AD portal, navigate to **Azure Active Directory > Mobility (MDM and MAM)**. Choose **On-premises MDM application**.
3. Click **On-premises Application Settings > Required Permissions > Add > Select an API > Microsoft Graph**. Click **Select** and save.
4. Under **Required permissions**, select **Microsoft Graph**. Under **Enable Access**, select **Read and write directory data**.
5. Under **Required permissions**, select **Microsoft Graph**. Then click **Grant permissions**.
6. Click **Yes** to grant permissions.

When an Azure AD enrolled device running Windows 10 or Windows 11 is out of compliance, Endpoint Management also marks the device as out of compliance in Azure AD.

## Create an automated action based on a Windows Agent device policy result

Use the Windows Agent device policy to deploy scripts that monitor registry values on managed Windows desktops and tablets. Based on the values returned from a script, you can then configure an automated action to run.

1. Configure a Windows Agent device policy and check the values returned by the script. For information on the Windows Agent device policy, see [Windows Agent device policy](#).

That article and this section include a sample that's based on a script named `EntApp_2019_checkFirewall.ps1`. The related Windows Agent device policy defines a config named `cName_checkFirewall`. That config runs the sample script.

After the script runs on a device, you get the info required to create an action, as described in [Windows Agent device policy](#).

2. In the Endpoint Management console, click **Configure > Actions**.
3. On the **Actions** page, click **Add**.
4. On the **Action Information** page, enter a name for the action and an optional description.
5. On the **Action Details** page, select the **Policy returned value** trigger.

6. In the fields that appear, define the trigger and the action:
  - **Windows Agent settings:** Type the policy name, config name, and key name for the Windows Agent policy you created.
  - **Drop-down menu:** Select **Is**, **Is Not**, **Contains**, or **Does Not Contain** logic. This logic applies to the next field and causes the action to trigger if the logic applies.
  - **Enter a string:** Enter the string that resulted from running the PowerShell script uploaded in your policy. For information about finding that string, see [Windows Agent device policy](#).
  - **Action:** Select an action, a value for the action, and choose a time frame for resolving the action.

In our example: If the key name `firewallEnabled` returns the value `true`, the following action marks the device as in compliance.

Actions	Action details <span>✕</span>
1 Action Info	Choose a trigger event and the associated action for that event.
2 Details	<p><b>Trigger *</b></p> <p>Policy returned value <input type="text" value=""/></p> <p>Windows Agent <input type="text" value=""/></p> <p>WinAgent_2019_checkFirewall.cName_checkFirewall.firewallEnabled <input type="text" value=""/></p> <p>Is <input type="text" value=""/></p> <p>true <input type="text" value=""/></p>
3 Assignment (optional)	<p><b>Action *</b></p> <p>Mark the device as out of compliance <input type="text" value=""/></p> <p>Is <input type="text" value=""/></p> <p>False <input type="text" value=""/></p> <p>0 <input type="text" value=""/> ⓘ</p> <p>Minutes <input type="text" value=""/></p>
4 Summary	

If the key name `firewallEnabled` returns the value **false**, the following action marks the device as out of compliance.

Actions	Action details <span>✕</span>
1 Action Info	Choose a trigger event and the associated action for that event.
2 Details	<p><b>Trigger *</b></p> <p>Policy returned value <input type="text" value=""/></p> <p>Windows Agent <input type="text" value=""/></p> <p>WinAgent_2019_checkFirewall.cName_checkFirewall.firewallEnabled <input type="text" value=""/></p> <p>Is <input type="text" value=""/></p> <p>false <input type="text" value=""/></p>
3 Assignment (optional)	<p><b>Action *</b></p> <p>Mark the device as out of compliance <input type="text" value=""/></p> <p>Is <input type="text" value=""/></p> <p>True <input type="text" value=""/></p> <p>0 <input type="text" value=""/> ⓘ</p> <p>Minutes <input type="text" value=""/></p>
4 Summary	

7. If needed, set a deployment schedule and choose delivery groups.

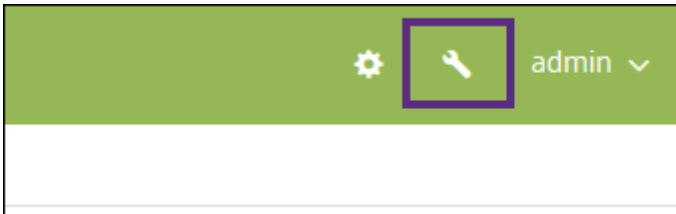
## Monitor and support

October 7, 2021

You can use the Endpoint Management Dashboard and the Endpoint Management Support page to

monitor and troubleshoot your Endpoint Management server. Use the Endpoint Management Support page to access support-related information and tools.

In the Endpoint Management console, click the wrench icon in the upper-right corner.

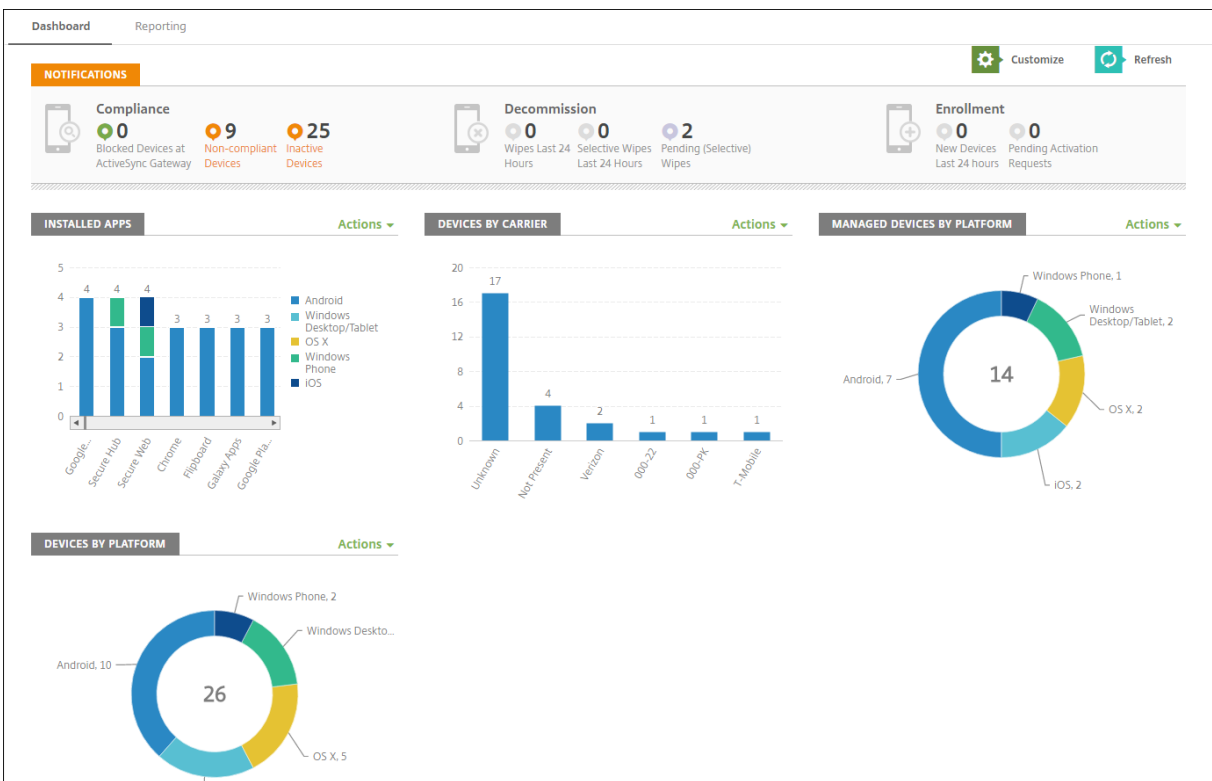


The **Troubleshooting and Support** page appears.

Use the Endpoint Management **Troubleshooting and Support** page to:

- Access diagnostics.
- Access links to Citrix Product Documentation and the Knowledge Center.
- Access log operations.
- Use advanced configuration options.
- Access a set of tools and utilities.

You can also view information at a glance by accessing your Endpoint Management console dashboard. With this information, you can see issues and successes quickly by using widgets.



The dashboard is usually the page that first appears when you sign on to the Endpoint Management console. To access the dashboard from elsewhere in the console, click **Analyze**. Click **Customize** on

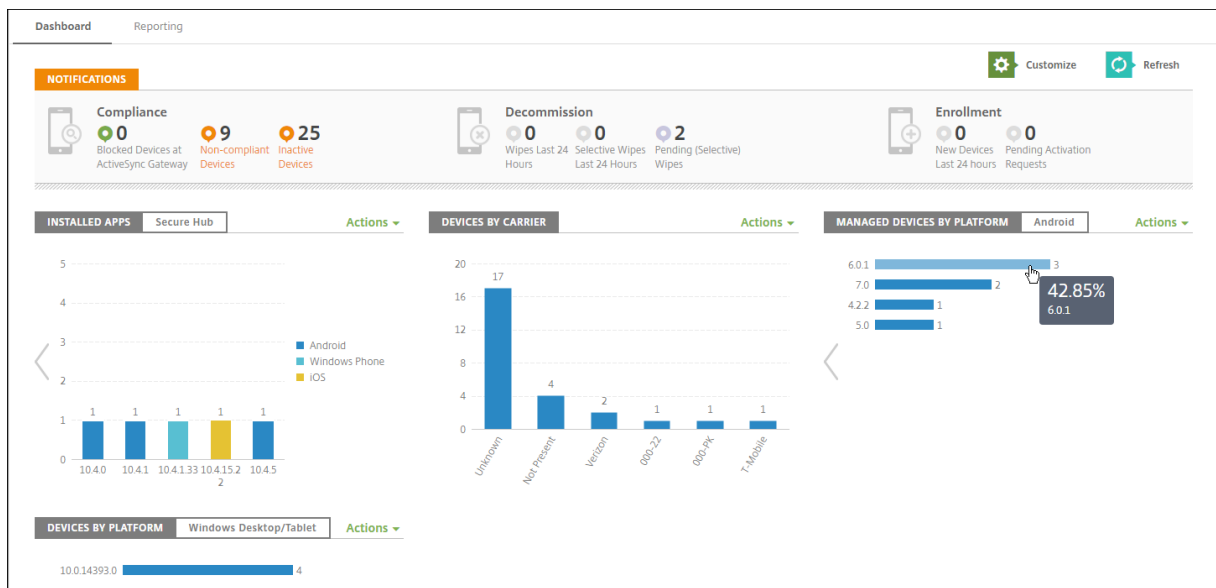
the dashboard to edit the layout of the page and to edit the widgets that appear.

- **My Dashboards:** You can save up to four dashboards. You can edit these dashboards separately and view each one by selecting the saved dashboard.
- **Layout Style:** In this row, you can select how many widgets appear on your dashboard and how the widgets are laid out.
- **Widget Selection:** You can choose which information appears on your dashboard.
  - **Notifications:** Mark the check box above the numbers on the left to add a Notifications bar above your widgets. This bar shows the number of compliant devices, inactive devices, and devices wiped or enrolled in the last 24 hours.
  - **Devices By Platform:** Displays the number of managed and unmanaged devices by platform.
  - **Devices By Carrier:** Displays the number of managed and unmanaged devices by carrier. Click each bar to see a breakdown by platform.
  - **Managed Devices By Platform:** Displays the number of managed devices by platform.
  - **Unmanaged Devices By Platform:** Displays the number of unmanaged devices by platform. Devices that appear in this chart might have an agent installed, but their privileges are revoked or the devices are wiped.
  - **Devices By ActiveSync Gateway Status:** Displays the number of devices grouped by ActiveSync Gateway status. The information shows Blocked, Allowed, or Unknown status. You can click each bar to break down the data by platform.
  - **Devices By Ownership:** Displays the number of devices grouped by ownership status. The information shows corporate-owned, employee-owned, or unknown ownership status.
  - **Failed Delivery Group Deployments:** Displays the total number of failed deployments per package. Only packages that have failed deployments appear.
  - **Devices By Blocked Reason:** Displays the number of devices blocked by ActiveSync
  - **Installed Apps:** Type an app name for a graph of app information.
  - **Volume Purchase Apps License Usage:** Displays license usage statistics for Apple volume purchase apps.

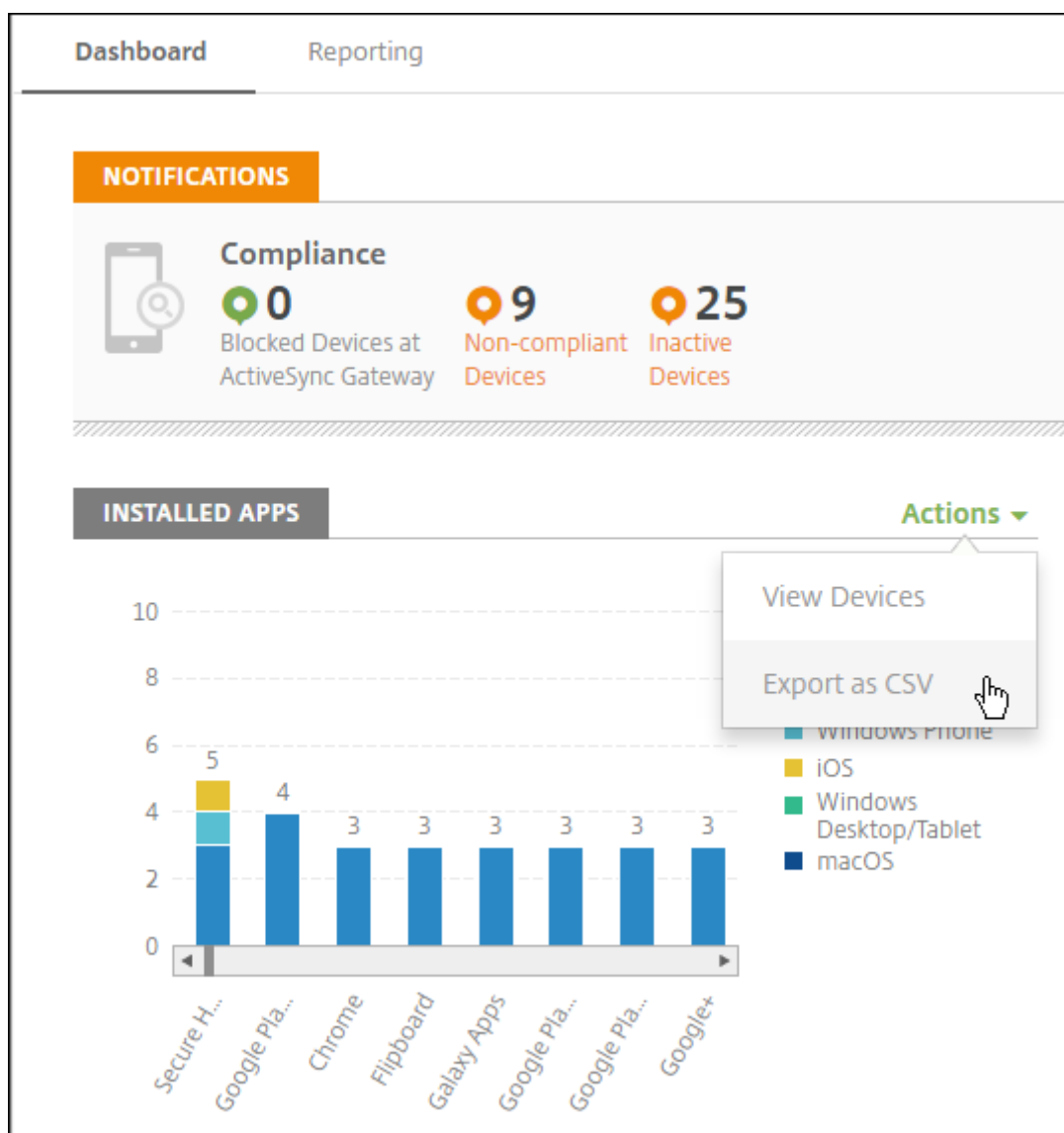
With each widget, you can click the individual parts to drill down for more information.



# Citrix Endpoint Management



You can also export the information as a .csv file by clicking the **Action** menu.



### Monitor page for help desk administrators

You can monitor and troubleshoot Endpoint Management on the **Monitor** page. This interface is customized for help desk administrators to carry out user-based troubleshooting efficiently.

Help Desk administrators must have the following permissions to access the **Monitor** page and all available workflows:

- Authorized access
  - Admin console access
  - Public api access
- Console Features
  - Monitor

- Devices
- Full Wipe Device
- View Locations
  - \* Locate Device
  - \* Track Device
- Lock device
- Unlock device
- App Lock
- App Wipe
- App

The **Monitor** page gives you a consolidated view of device policies and configuration. The view includes troubleshooting actions such as app lock/unlock, app wipe, device lock/unlock, and device wipe.

The screenshot shows the 'Device Details' page for a device named 'Test User1's Iphone' (Managed). At the top right, there are buttons for 'Device Lock', 'Device Unlock', 'Device Wipe', 'App Lock', and 'App Wipe'. The page is divided into three main sections:

- Policies:** A table showing device and application policies.
 

Policy Name	Policy Status	Resource Type
Location Tracking	SUCCESS	LOCATIONSERVICES
- Configuration:** A list of device configuration details.
 

Display Name	Test User1's Iphone	Mode	ENT
Operating System	iOS	XMAgentVersion	10.7.0
RAM	0	n	
Storage	24.82GB available of total 26.65GB	Last Activity	12/08/2017 11:30 AM
External Storage	n/a		
Battery	66%		
Location			
- Provisioned Applications:** A table showing the status of applications installed on the device.
 

Name	Created on	Last Update	Status	Type
Work Notes	11/16/2017 2:09 PM	11/16/2017 2:09 PM	FAILURE	MDX
Secure Mail	11/21/2017 12:25 PM	11/21/2017 12:25 PM	FAILURE	MDX
Secure Web	11/21/2017 12:28 PM	11/21/2017 12:28 PM	FAILURE	MDX

Use the **Monitor** page to:

- Search for an Active Directory (AD) user and device you want to troubleshoot.
- Analyze the **Device Details** page containing:
  - **Policies:** Displays device and app policies for the selected device and app. For information about modifying policies, see [Device policies](#) and [Add apps](#).
  - **Configuration:** Displays the device configuration. This panel includes icons that indicate whether the device has location services enabled, is jailbroken, and is MDM or MAM managed. The panel also shows the storage encryption status.
  - **Running Applications** table: Displays the details of the applications currently running on the device.
- Troubleshoot the device. Security actions available on this page are based on the enrollment

of the device, and the permissions available to the logged in administrator:

- Device lock/unlock
- Device wipe
- App lock/unlock (available if the device is MAM enrolled)
- App wipe (available if the device is MAM enrolled)

For more information about the actions you can take, see [Security actions](#).

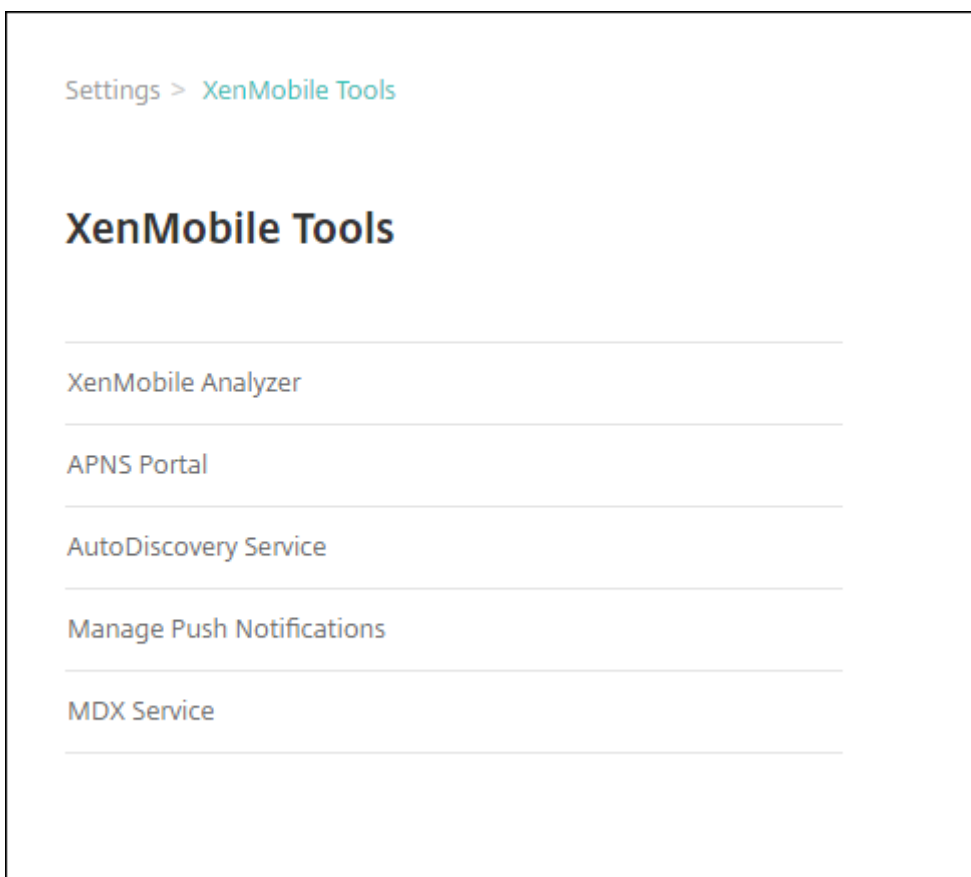
The Monitor page might not operate as expected 60 minutes after it was last loaded, because it does not handle refreshes of the login token. As a workaround, refresh the token by reloading the page: Click the **Citrix Cloud** link on your service console and then click **Endpoint Management > Manage > Monitor**.

### **Access to Endpoint Management Tools from the console**

You can access these Endpoint Management Tools from the Endpoint Management console:

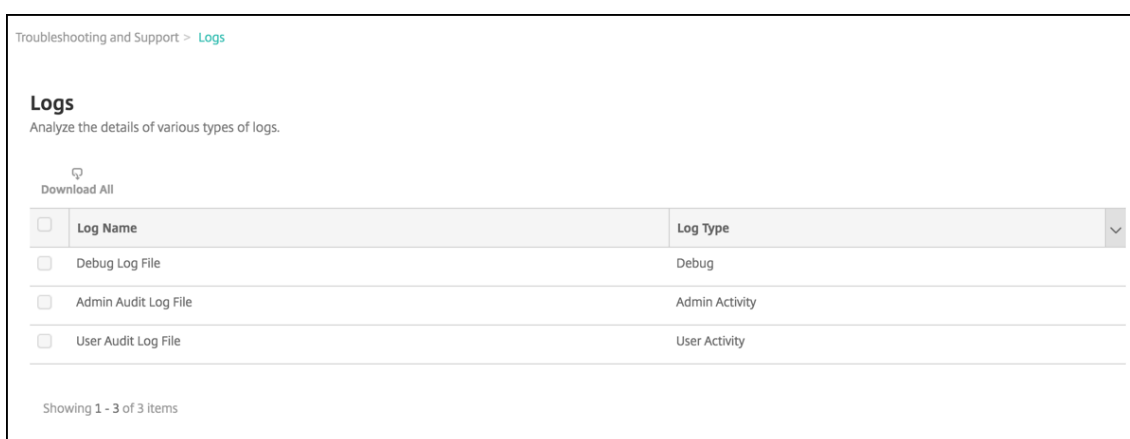
- **Endpoint Management Analyzer** – Identify and triage potential issues with your deployment.
- **APNs Portal** – Submit a request to Citrix to sign an APNs certificate, which you then submit to Apple.
- **Auto Discovery Service** – Request and configure AutoDiscovery for Endpoint Management in your domain.
- **Manage Push Notifications** – Manage push notifications for iOS and Windows mobile apps.

To access these tools, go to **Settings > Endpoint Management Tools**. This page is available to users with the Cloud Admin or Customer Admin role.



### View and analyze log files in Endpoint Management

1. In the Endpoint Management console, click the wrench icon in the upper-right corner of the console. The **Troubleshooting and Support** page opens.
2. Under **Log Operations**, click **Logs**. The **Logs** page appears. Individual logs appear in a table.



3. Select the log you want to view:

- Debug Log Files contain information useful for Citrix Support, such as error messages and server-related actions.
- Admin Audit Log Files contain audit information about activity on the Endpoint Management console.
- User Audit Log Files contain information related to configured users.

4. Use the actions at the top of the table to download all, view, or download a single log.

Log Name	Log Type
<input checked="" type="checkbox"/> Debug Log File	Debug
<input type="checkbox"/> Admin Audit Log File	Admin Activity
<input type="checkbox"/> User Audit Log File	User Activity

**Note:**

If you select multiple log files, only **Download All** is available.

5. Do one of the following:

- **Download All:** The console downloads all the logs present on the system (including debug, admin audit, user audit, server logs, and so on).
- **View:** Shows the contents of the selected log below the table.
- **Download:** The console downloads only the single log file type selected. The console also downloads any archived logs for that same type.

```

Log contents for Debug Log File
2018-11-15T06:49:40.7+0000 | INFO | localhost-startStop-1 | com.citrix.xmls.util.CloudUtil | This is a cloud build.
2018-11-15T06:49:40.44+0000 | INFO | localhost-startStop-1 | com. .... AnonymizationConfigInit | *** Initializing Anonymization Configuration ***
2018-11-15T06:49:40.46+0000 | INFO | localhost-startStop-1 | com. .... AnonymizationConfigInit | Not generating anonymize.properties for cloud servers.
2018-11-15T06:49:40.46+0000 | INFO | localhost-startStop-1 | com. .... nps.EwConfigInit | **** Inside EwConfig Initialize Method ****
2018-11-15T06:49:40.46+0000 | INFO | localhost-startStop-1 | com. .... nps.EwConfigInit | Not generating ew.config.properties for cloud servers.
2018-11-15T06:49:54.463+0000 | INFO | localhost-startStop-1 | com.citrix.init.FirstBeanInitialization | FirstBeanInitialization: Adding ..... to Java Security Providers.
2018-11-15T06:49:54.584+0000 | INFO | localhost-startStop-1 | com. .... nps.util.PkiUtil | Standard(Non-FIPS) BC lib registered
2018-11-15T06:49:54.585+0000 | INFO | localhost-startStop-1 | com.citrix.init.FirstBeanInitialization | Setting CloudSecurity to MultiTenant mode.
    
```

Endpoint Management uses the log4j syslog appender to send RFC5424 formatted syslog messages. The syslog message data is plain text with no specific format.

## Connectivity checks

July 12, 2021

From the Endpoint Management **Troubleshooting and Support** page, you can check the Endpoint Management connection to Citrix Gateway and to other servers and locations. To run Endpoint Management connectivity checks, you need the Support or the Admin role. Set this role using Role-Based Access Control (RBAC). For more information on assigning roles, see [Configure roles with RBAC](#).

## Run Endpoint Management connectivity checks

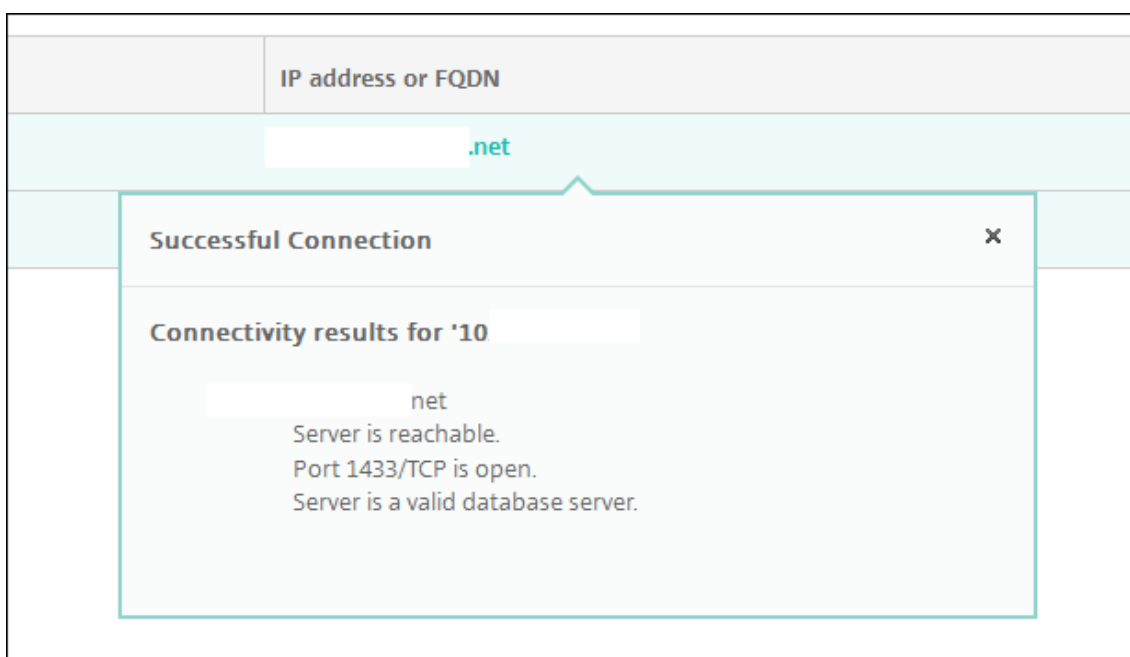
1. In the Endpoint Management console, click the wrench icon in the upper-right corner of the console. The **Troubleshooting and Support** page appears.
2. Under **Diagnostics**, click **Endpoint Management Connectivity Checks**. The **Endpoint Management Connectivity Checks** page appears. If your Endpoint Management environment contains clustered nodes, all nodes are shown.

<input type="checkbox"/>	Connectivity to	IP address or FQDN
<input type="checkbox"/>	Windows Phone Store	windowsphone.com
<input type="checkbox"/>	Database	██████████.net
<input type="checkbox"/>	Apple Feedback Push Notification Server	feedback.push.apple.com
<input type="checkbox"/>	LDAP	██████████.net
<input type="checkbox"/>	Domain Name System (DNS)	██████████
<input type="checkbox"/>	Nexmo Gateway	-
<input type="checkbox"/>	Apple Push Notification Server	gateway.push.apple.com
<input type="checkbox"/>	iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
<input type="checkbox"/>	Google Play	play.google.com
<input type="checkbox"/>	Windows Security Token Service	login.live.com

3. Select the servers you want to include in the connectivity test and then click **Test Connectivity**. The test results page appears.

<input type="checkbox"/>	Connectivity to	IP address or FQDN	
<input type="checkbox"/>	Database	net	✓
<input type="checkbox"/>	Windows Phone Store	windowsphone.com	✓

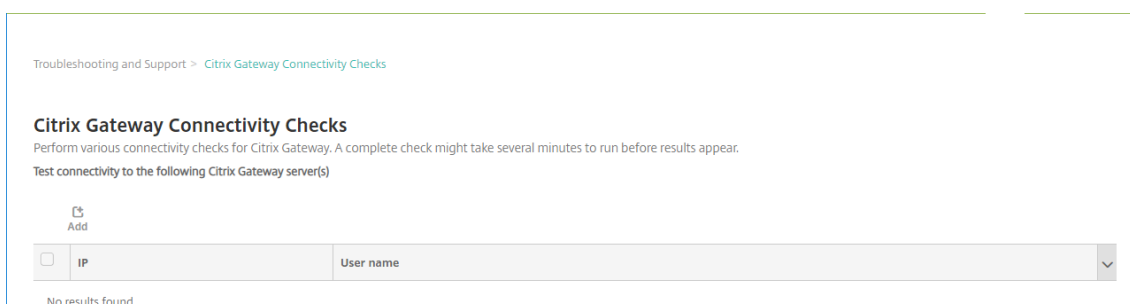
4. Select a server in the test results table to see detailed results for that server.



For information about connectivity checks that Endpoint Management can perform and their details, see Connectivity check details.

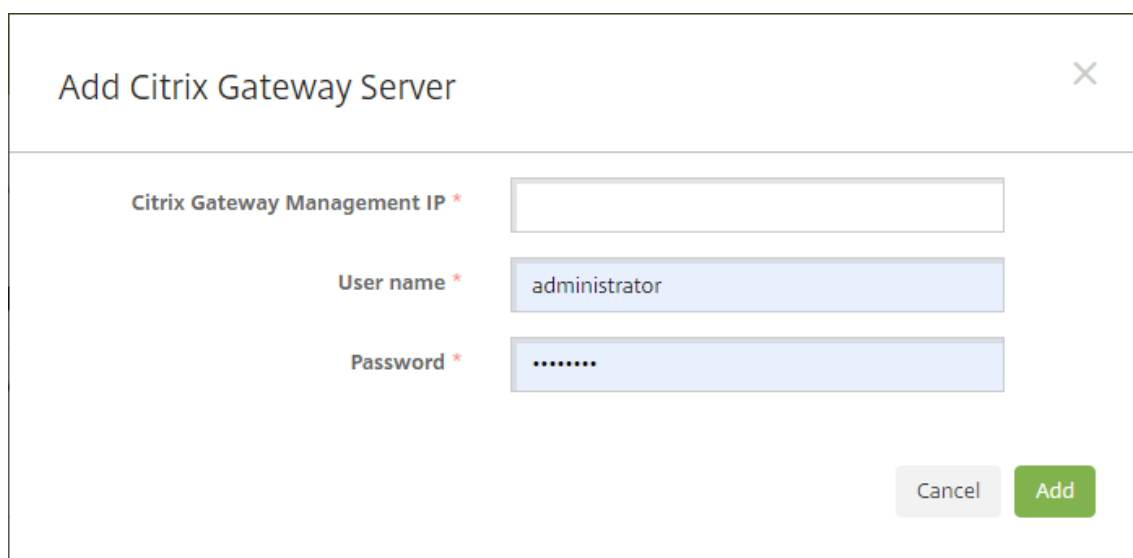
## Conducting Citrix Gateway connectivity checks

1. On the **Troubleshooting and Support** page, under **Diagnostics**, click **Citrix Gateway Connectivity Checks**. The **Citrix Gateway Connectivity Checks** page appears. The table is empty if there is no connection between Endpoint Management and Citrix Gateway.



2. Click **Add**. The **Add Citrix Gateway Server** dialog box appears.





The screenshot shows a dialog box titled "Add Citrix Gateway Server" with a close button (X) in the top right corner. The dialog contains three input fields, each with a red asterisk indicating a required field:

- Citrix Gateway Management IP \***: An empty text input field.
- User name \***: A text input field containing the value "administrator".
- Password \***: A password input field containing seven dots (•••••••).

At the bottom right of the dialog, there are two buttons: a grey "Cancel" button and a green "Add" button.

3. In **Citrix Gateway Management IP**, type the management IP address for the server running Citrix Gateway that you want to test.

If you're conducting a connectivity check for a Citrix Gateway server that has already been added before, the IP address is provided.

4. Type your administrator credentials for this Citrix Gateway.

If you're conducting a connectivity check for a Citrix Gateway server that has already been added before, the user name is provided.

5. Click **Add**. The Citrix Gateway is added to the table on the **Citrix Gateway Connectivity Checks** page.
6. Select the Citrix Gateway server and then click **Test Connectivity**. The results appear in a test results table.
7. Select a server in the test results table to see detailed results for that server.

### Connectivity check details

The following table lists various connectivity checks that Endpoint Management can perform and includes details about each check.

<b>Connectivity to</b>	<b>IP address or FQDN</b>	<b>Details</b>
Apple Push Notification Server	api.push.apple.com	Checks the connectivity between Apple Push Notification Server and the Endpoint Management node. Apple Push Notification Server is required to send messages to iOS, macOS, and tvOS devices.
Apple Feedback Push Notification Server	feedback.push.apple.com	Checks connectivity between Apple Feedback Server and the Endpoint Management node. Apple Feedback Push Notification Server gives you information about failed remote notifications sent to iOS and macOS devices.
Citrix License Server	IP address of License Server	Checks connectivity between Citrix License Server and the Endpoint Management node. Servers running Citrix products contact Citrix License Server to obtain licenses.
Citrix Gateway	FQDN of Citrix Gateway configured in Endpoint Management	Checks connectivity between Citrix Gateway and the Endpoint Management node. Citrix Gateway is used by Endpoint Management client apps (such as Secure Mail and Secure Web) to connect through a VPN server for access to internal networks.
Database	IP address or FQDN of Database Server	Checks connectivity between the Endpoint Management database and the Endpoint Management node.

<b>Connectivity to</b>	<b>IP address or FQDN</b>	<b>Details</b>
Domain Name System (DNS)	IP address configured in Endpoint Management	Checks connectivity between the DNS server and the Endpoint Management node.
Secure Ticket Authority service	localhost	Checks the Endpoint Management node connection to authentication services, STA (Secure Ticket Authority) services, and cluster services.
Firebase Cloud Messaging (FCM) Server		Checks connectivity between FCM Server and the Endpoint Management node. Using FCM, you can notify a client app that a new email or other data is available to sync. You can send notification messages to drive user engagement and retention. FCM is a substitute for Google Cloud Messaging (GCM).
Google Play	play.google.com	Checks connectivity between Google Store Server and the Endpoint Management node. Google Play is used to offer services that include a managed, private enterprise app delivery store.
iTunes Store/Volume Purchase	vpp.itunes.apple.com	Checks connectivity between Apple Store Server and the Endpoint Management node. Apple Store is used to offer services that include a managed, private enterprise app delivery store.

<b>Connectivity to</b>	<b>IP address or FQDN</b>	<b>Details</b>
LDAP	IP address or FQDN of LDAP configured in Endpoint Management	Checks connectivity between the LDAP server and the Endpoint Management node.
Microsoft Push Notification Server	sin.notify.windows.com	Checks connectivity between Windows Notification Server and the Endpoint Management node. Windows Notification Server is used to send messages to Windows devices.
Nexmo Gateway	-	Checks connectivity between Nexmo SMS Relay Server and the Endpoint Management node. Nexmo is an American and international SMS gateway provider that provides features such as messaging apps and messaging APIs, enabling businesses to send mass text messages.
Content Collaboration Service	IP address or FQDN of Content Collaboration Service configured in Endpoint Management	Checks connectivity between Content Collaboration Service and Endpoint Management. Content Collaboration Service is a secure cloud-based platform for businesses to store and share large files.

<b>Connectivity to</b>	<b>IP address or FQDN</b>	<b>Details</b>
Windows Phone Store	windowsphone.com	Checks connectivity between Windows Phone Store Server and the Endpoint Management node. Windows Phone Store is used to offer services that include a managed, private app delivery store.
Windows Desktop/Tablet Store	windows.microsoft.com	Checks connectivity between the Windows Desktop/Tablet Store and the Endpoint Management node. Windows Desktop/Tablet Store is used to offer services that include a managed, private enterprise app delivery store.
Windows Security Token Service	login.live.com	Checks connectivity between Windows Security Token Server and the Endpoint Management node. Windows Security Token Service supports two-factor authentication (domain plus security token) for Windows devices.

## Mobile Service Provider

September 15, 2020

You can enable Endpoint Management to use the Mobile Service Provider interface to query BlackBerry and Exchange ActiveSync devices and issue operations.

For example, suppose that your organization has 1,000 users and each user uses one or more devices. After you direct all users to enroll their devices with Endpoint Management, the Endpoint Management console indicates the number of devices that users enroll. By configuring this setting, you can

determine how many devices connect to Exchange Server. In this way, you can do the following:

- Determine if any users still need to enroll their devices.
  - Issue commands to user devices that connect to Exchange Server, such as data wipes.
1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
  2. Under **Server**, click **Mobile Service Provider**. The **Mobile Service Provider** page appears.

Settings > Mobile Service Provider

### Mobile Service Provider

Allows XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.

Web service URL\*

User name\*

Password\*

Automatically update BlackBerry and ActiveSync device connections

3. Configure these settings:

- **Web service URL:** Type the URL of the Web service; for example, `https://XmmServer/services/xdmservice`.
- **User name:** Type the user name in the format `domain\admin`.
- **Password:** Type the password.
- **Automatically update BlackBerry and ActiveSync device connections:** Select whether to automatically update device connections. The default is **Off**
- Click **Test Connection** to verify connectivity.

4. Click **Save**.

## Reports

March 18, 2021

Endpoint Management provides the following pre-defined reports that let you analyze your app and device deployments. Each report appears as a table and a chart. You can sort and filter the tables by column. You can select elements in charts from more detailed information.

- **Total Apps Deployment Attempts:** Lists deployed apps that users tried to install on their devices.
- **Apps by Platform:** Lists apps and app versions by device platform and version.
- **Apps by Type:** Lists apps by version, type, and category.
- **Device Enrollment:** Lists all enrolled devices.
- **Devices & Apps:** Lists devices that are running managed apps.
- **Inactive Devices:** A list of devices that have not had any activity for the number of days specified by the Endpoint Management server property `device.inactivity.days.threshold`.
- **Jailbroken/Rooted Devices:** Lists jailbroken iOS devices and rooted Android devices.
- **Terms & Conditions:** Lists users who have accepted and declined Terms and Conditions agreements. You can select areas of the chart to view more details.
- **Top 10 Failed Deployments:** Lists up to 10 apps that have failed to deploy.
- **Blocked Apps by Device & User:** Lists apps on the block list that users have on their devices.
- **Non-Compliant Devices:** Lists devices that don't meet compliance criteria. Criteria include whether the device is jailbroken, the OS version running, and if the device has a passcode. The report also displays the username associated with the device and if the device is encrypted. For iOS devices, the encryption column displays N/A.

You can export the data in each table in .csv format, which opens in programs such as Microsoft Excel. Charts for each report can be exported in PDF format.

The **Reporting** tab includes device details, such as serial number, IMEI/MEID, apps, and connections. For more comprehensive reporting about a specific device, go to **Manage > Devices**, click that device, click **Show more**, and then view the **Device details** page. The **Device details** page lists device security properties, device properties, assigned policies, apps, actions, certificates, and more. For information about the **Device details** page, see [Get information about devices](#).

The following aspects determine how Endpoint Management collects information about apps deployed to or installed on managed devices:

- Device type
- Enrollment method
- Whether the [App inventory device policy](#) is deployed

For Android devices, the behavior is different depending on the device type and the enrollment method. The following table indicates where apps are listed for **Android Enterprise (Device details** page, reports, or not available). App lists include all apps unless otherwise indicated.

	MDM+MAM (all apps)	MDM (all apps)
Required apps (the App inventory policy is not deployed)	<b>Device details</b> page and reports	Public apps; <b>Device details</b> page and reports

	MDM+MAM (all apps)	MDM (all apps)
Optional apps (the App inventory policy is not deployed)	Not available	Not available
Required apps (the App inventory policy is deployed)	<b>Device details</b> page and reports	<b>Device details</b> page and reports
Optional apps (the App inventory policy is deployed)	Enterprise, MDX, public, and Web link apps; reports	<b>Device details</b> page and reports

The following table indicates where apps are listed for **Android (legacy DA)** (**Device details** page, reports, or not available). App lists include all apps unless otherwise indicated.

	MDM+MAM (all apps)	MDM (public and enterprise apps)	MAM
Required apps (the App inventory policy is not deployed)	<b>Device details</b> page and reports	<b>Device details</b> page and reports	N/A
Optional apps (the App inventory policy is not deployed)	<b>Device details</b> page and reports	<b>Device details</b> page and reports	Not available
Required apps (the App inventory policy is deployed)	<b>Device details</b> page and reports	<b>Device details</b> page and reports	N/A
Optional apps (the App inventory policy is deployed)	<b>Device details</b> page and reports	<b>Device details</b> page and reports	Not available

For iOS devices, the behavior is different depending on the enrollment method. The following table indicates where apps are listed (**Device details** page or reports). App lists include all apps unless otherwise indicated.



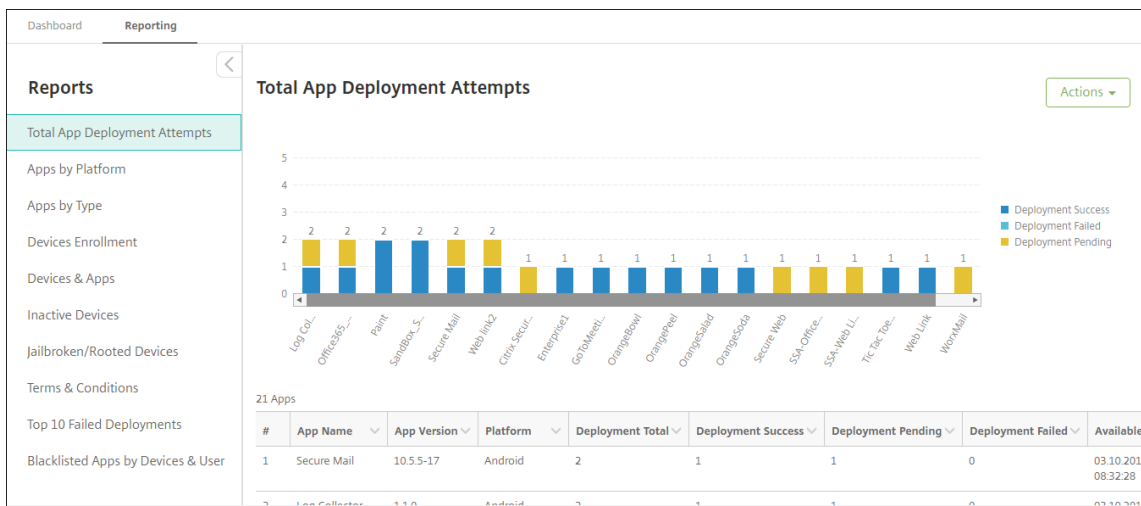
	MDM+MAM (all apps)	MDM (public and enterprise apps)	MAM (all apps)
Required apps (the App inventory policy is not deployed)	<b>Device details</b> page and reports	<b>Device details</b> page and reports	<b>Device details</b> page and reports; those apps are shown in a pending state (even if they are not installed) or remain in a pending state after they are installed manually.
Optional apps (the App inventory policy is not deployed)	<b>Device details</b> page and reports	<b>Device details</b> page and reports	Web, SaaS, and Web link apps are listed on the <b>Device details</b> page as installed apps; they are not listed in reports. Enterprise, MDX, and public apps are not listed on the <b>Device details</b> page after they are installed manually. Apps are not listed in reports after they are installed manually.

	MDM+MAM (all apps)	MDM (public and enterprise apps)	MAM (all apps)
Required apps (the App inventory policy is deployed)	<b>Device details</b> page and reports	<b>Device details</b> page and reports	The App inventory policy cannot be deployed to devices. Apps are listed on the <b>Device details</b> page and in reports. Those apps are shown in a pending state (even if they are not installed) or remain in a pending state after they are installed manually.
Optional apps (the App inventory policy is deployed)	<b>Device details</b> page and reports	<b>Device details</b> page and reports	The App inventory policy cannot be deployed to devices. Web, SaaS, and Web link apps are listed on the <b>Device details</b> page as installed apps; they are not listed in reports. Enterprise, MDX, and public apps are not listed on the <b>Device details</b> page after they are installed manually. Apps are not listed in reports after they are installed manually.

For macOS and Windows devices, Endpoint Management collects an inventory of apps *only* when the App inventory policy is deployed.

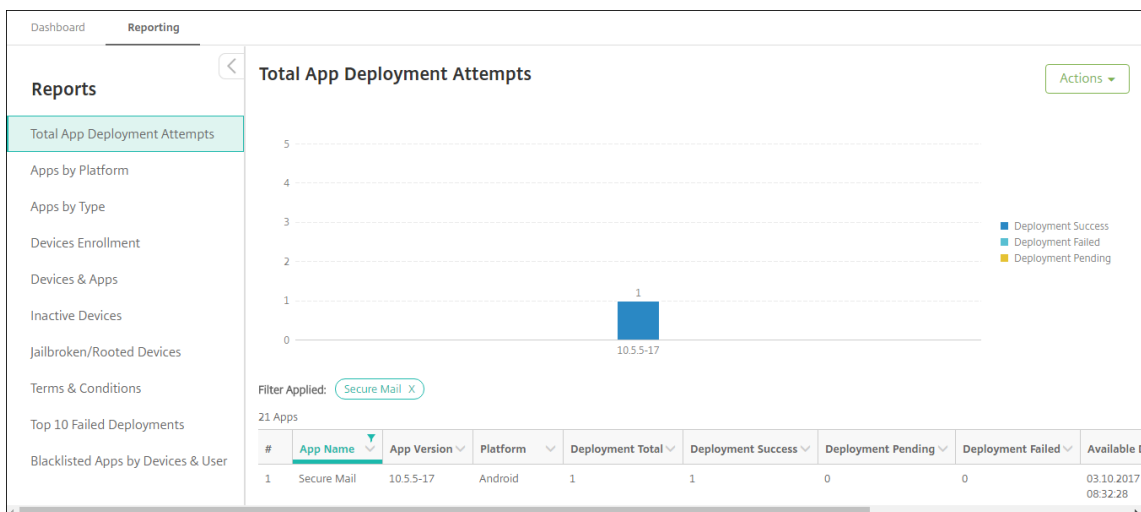
## To generate a report

1. In the Endpoint Management console, click **Analyze > Reporting**. The **Reporting** page appears.
2. Click the report you want to generate.



## To view more details of a report

1. Click areas of the chart to drill down and see more details information.



## To sort, filter, or search a table column, click the column heading

Dashboard Reporting

Reports

Total App Deployment Attempts

22 Apps

#	App Name	App Version	Platform	Deployment Total	Deployment Success	Deployment Pending	Deployment Failed	Available
1	Enterprise1			1	1	0	0	03.10.2017 09:10:10
2	SandBox_S			1	1	0	0	03.10.2017 08:38:40
3	Fonts			1	0	1	0	03.10.2017 09:45:07
4	SandBox_S			1	1	0	0	03.10.2017 08:38:40
5	GoToMeeti			1	1	0	0	03.10.2017 12:34:35
6	Secure Mail	10.5.5-17	Android	1	1	0	0	03.10.2017 08:32:28
7	GreedyPenguins		Windows Mobile	1	1	0	0	03.10.2017 13:01:50

## To filter the report by date

1. Click a column heading to view the filter settings.

Dashboard Reporting

Reports

Total App Deployment Attempts

Apps by Platform

Apps by Type

Devices Enrollment

Devices & Apps

Inactive Devices

Jailbroken/Rooted Devices

Terms & Conditions

Top 10 Failed Deployments

Blacklisted Apps by Devices & User

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:08			03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S...
Compliance	03.27.2017 09:29:08			03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Editor
Compliance	03.27.2017 09:29:08			03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre...
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_S...

2. From **Filter Condition**, choose how you want to restrict the dates reported.

The screenshot shows the 'Reporting' dashboard with a table of reports. A dropdown menu is open over the 'Last authentication' column, showing filter conditions: 'is on', 'is on or before', 'is on or after', and 'between'. The table has columns: Status, Last authentication, Last access, Enrollment state, Enrollment date, Device ownership, Location, Deployment status, and App name.

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:07	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_SP
Compliance	03.27.2017 09:29:07	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Editor
Compliance	03.27.2017 09:29:07	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_SP

3. Use the date chooser to specify dates.

The screenshot shows the 'Reporting' dashboard with a date picker calendar open over the 'Last authentication' column. The calendar is for April 2017. The table has columns: Status, Last authentication, Last access, Enrollment state, Enrollment date, Device ownership, Location, Deployment status, and App name.

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:07	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:29:07	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edito
Compliance	03.27.2017 09:29:07	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Jota Text Edito

4. A column with a date filter displays as shown the following example.

The screenshot shows the 'Reporting' dashboard with the 'Last authentication' and 'Enrollment date' columns highlighted with red boxes. The table has columns: Status, Last authentication, Last access, Enrollment state, Enrollment date, Device ownership, Location, Deployment status, and App name.

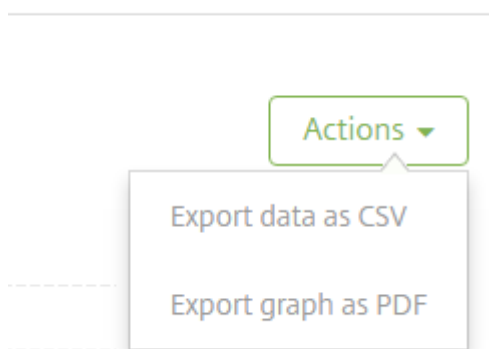
Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edito

5. To remove a filter, click the column heading and then click **Remove Filter**

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29			03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:29			03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edito
Compliance	03.27.2017 09:29			03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29			03.27.2017 07:33:27	Unknown		SUCCESS	Web Link

### To export a chart or table

- To export the chart in PDF format, click **Actions** then **Export graph as PDF**.
- To export the table data in CSV format, click **Actions** then **Export data as CVS**.



## Endpoint Management Analyzer

November 4, 2020

Endpoint Management Analyzer is a cloud-based tool that you can use to check the authentication and enrollment setup for Citrix Endpoint Management.

Configure the tool to point to your Endpoint Management server and provide information, such as server deployment type, mobile platform, authentication type, and user credentials. The tool then connects to the server and scans your environment for configuration issues. If Endpoint Management Analyzer discovers issues, the tool provides recommendations to correct the issues.

## Key features

- Secure, cloud-based micro-service to troubleshoot issues related to Endpoint Management.
- Recommendations to resolve Endpoint Management configuration issues.
- Reduced support calls and accelerated troubleshooting of Endpoint Management environments.
- Zero-day support for Endpoint Management releases.
- Health check scheduling on a daily or weekly cadence.
- Secure Mail AutoDiscovery service checks.

## Prerequisites

---

Product	Supported Version
Client Enrollment Simulation	iOS and Android

---

## Accessing Endpoint Management Analyzer

Use one of the following methods to access Endpoint Management Analyzer:

- In the Endpoint Management console, click the wrench icon in the upper-right corner to open the **Troubleshooting and Support** page.
- Use your My Citrix credentials to access the tool from <https://xmanalyzer.xm.citrix.com/>. On the Endpoint Management Analyzer Checks page, click **Endpoint Management Environment**.



Endpoint Management Analyzer contains the following options:

- **Environment Check:** This option guides you in setting up tests to check your setup. The option provides recommendations and solutions on device, user enrollment, and authentication issues.
- **Server Connectivity:** This option instructs you to test the connectivity of your servers.
- **Citrix Insight Services:** This option opens Citrix Insight Services to find issues that the environment check might not detect. You can also use this option to check your Citrix ADC configurations for Endpoint Management deployment readiness.
- **Contact Citrix support:** If you are still having issues, you can create a Citrix support case.

The following sections describe each option in more detail.

### Performing an environment check

1. Log on to Endpoint Management Analyzer and then click **Endpoint Management Environment**.
2. Click **Add Test Environment**.
3. In the new **Add Test Environment** dialog box, do the following:



**Add Test Environment** ✕

Enter test name\*

**Environment Details**    **Test Options**    **User Credentials**

FQDN, UPN login, Email or Invitation URL ?

Click to enter

Instance Name ?

Choose Platform

iOS     Android

[Advanced Deployment Options](#) ▾

Cancel Continue

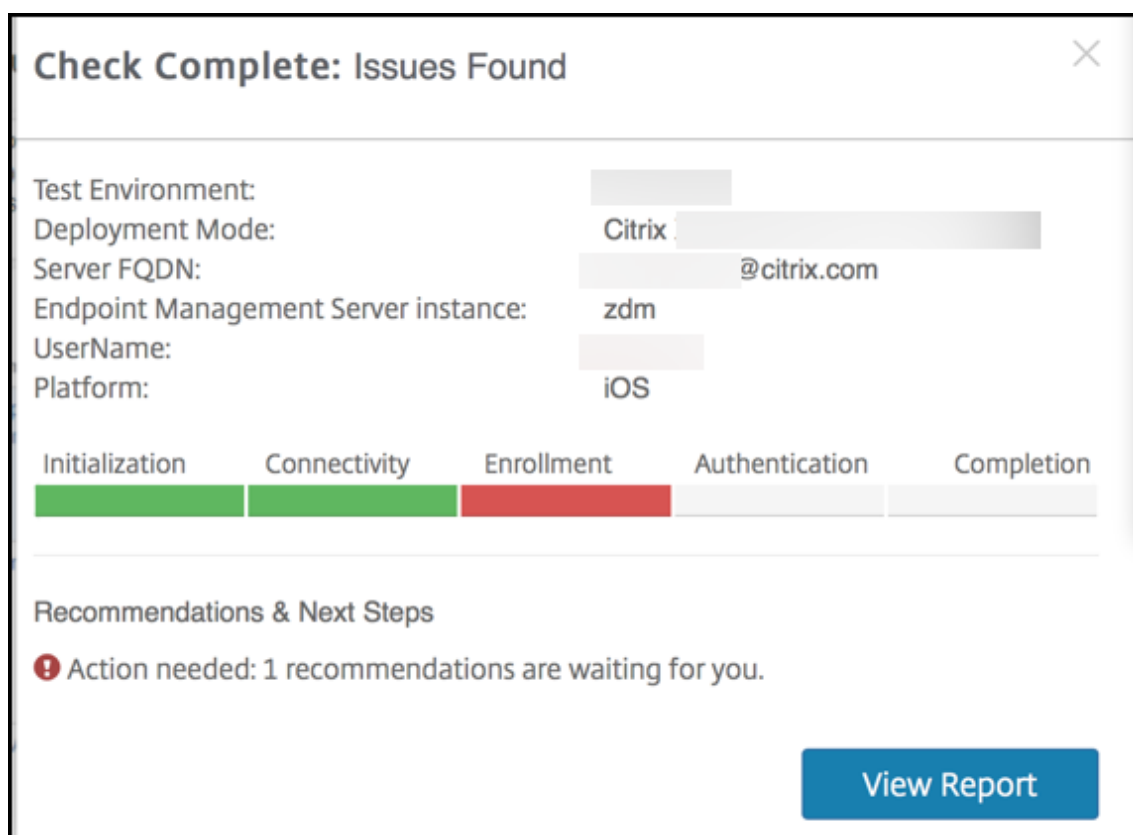
- a) Provide a unique name for the test that will help identify the test in the future.
  - b) In **FQDN, UPN login, Email or URL Invitation URL**, enter the information that is used to access the server.
  - c) In **Instance Name**, if you use a custom instance, provide that value.
  - d) In **Choose Platform**, select either **iOS** or **Android** as the platform for testing.
  - e) Expand **Advanced Deployment Options** and then in the **Deployment Mode** list, select your deployment mode. The options are:
    - **Enterprise (MDM + MAM)**
    - **App Management (MAM)**
4. Click **Continue**.
  5. On the **Test Options** tab, choose one or more of the following tests and then click **Continue**.

- **Secure Web Connectivity:** Provide an intranet URL. The tool tests for the reachability of the URL. This test detects if there are any connectivity issues that may potentially occur in Secure Web while trying to reach intranet URLs.
  - **Secure Mail ADS:** Provide a user email ID. Endpoint Management Analyzer uses this ID to test AutoDiscovery of the Exchange Server in your environment.
  - **ShareFile SSO:** Endpoint Management Analyzer tests if the ShareFile DNS resolution happens successfully. The tool also checks if ShareFile single sign-on (SSO) is compatible with the provided user credentials.
6. On the **User Credentials** tab, depending on your server setup, different Secure Hub user credentials fields appear, such as **Username**, **Username and Password**, or **Username, Password**, and **Enrollment PIN**.
  7. Click **Save & Run** to start the tests.

A progress notification appears. You can leave the progress dialog box open or close the dialog

box and the tests continue to run.

Tests that pass appear in green. Tests that fail appear as red.



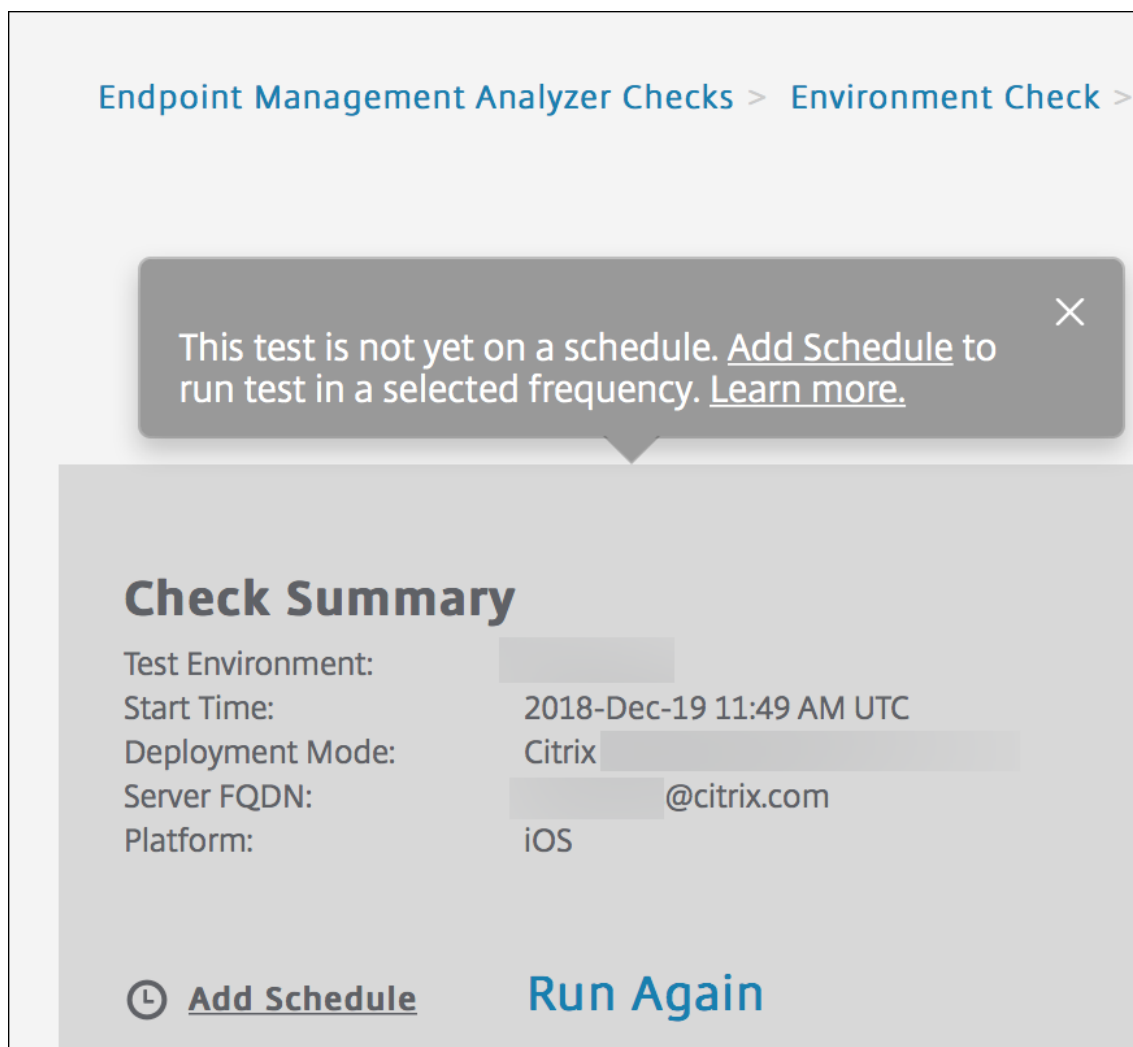
8. Click the **View Report** icon to see test results.
  - To rerun the same test, click **Run Again**.
  - To download the report, click **Download Report**.
  - To select another Endpoint Management Analyzer option, click **Go To Endpoint Management Analyzer Checks**.
  - To return to the list of tests on the **Environment Lists** page, in the upper-left of the page, click **Environment Check**.
9. On the **Environment List** page, you can copy and edit tests. To do so, select a test, click **More** and then select **Duplicate and Edit**.

A copy of the selected test is created and the **Add Test Environment** dialog box opens, allowing you to modify the new test.

### Adding a schedule to environment checks

You can configure tests to run on an automatic schedule with results sent to a list of users you configure.

1. To add a schedule, do one of the following:
  - a) On the **Environment List** page, select the environment for which you want to set up a schedule and then click **Add Schedule**.
  - b) In a test result, click **Add Schedule**.



2. The **Add Schedule** window displays a message warning you that Endpoint Management Analyzer saves credentials for running tests on a schedule. Citrix recommends that you use an account with limited access for running scheduled tests. Click **I Agree** to continue.
3. Enter a **Username** and **Password** for running the test.
4. Configure a schedule for the test to run.
  - a) Select **Daily** or **Weekly**.
  - b) Select a time of day for the test to run and a time zone.
  - c) Use the date picker to select a date for the scheduled test to stop running or leave it blank for the test to run indefinitely.

- d) Enter a list of email addresses to receive reports, separated by commas.
  - e) Click **Save**.
5. A clock symbol to the left of your test indicates that a schedule is configured. If you select your test, click **Edit Schedule** to change when the test runs.

**Edit Schedule**

Run checks automatically during this schedule **ON**

You can turn on/off schedule at any time.

When should it run?

Daily 7:00 AM (UTC-05:00) Eastern Time (US & Canada)

When should it end?

12/19/2018

Recipients

@citrix.com

Cancel Edit Credentials Save

- You can change when the test runs.
- You can disable the test, by clicking the switch at the top from **On** to **Off**.

### Known issues

The following issues are known in the Endpoint Management Analyzer:

- When performing the Secure Web Connectivity checks, typing multiple URLs in the text box is not supported.
- The shared devices authentication feature of Secure Hub is not supported.
- Secure Web tests only check the connectivity to the URLs entered and not the authentication to the corresponding sites.

## REST APIs

August 31, 2021

With the Endpoint Management REST API, you can:

- Call services that are exposed through the Endpoint Management console
- Call REST services by using any REST client

The API does not require you to sign on to the Endpoint Management console to call the services.

For the complete current set of available APIs, download the [Public API for REST Services](#) PDF.

For Endpoint Management environments that are workspace enabled, we have APIs to manage your mobile and desktop endpoint devices and configure settings for your Workspace apps. Go to <https://developer.cloud.com/citrixworkspace> and navigate to **Citrix Endpoint Management > Mobile Application Integration**.

### Permissions required to access the REST API

Access to the REST API requires one of the following permissions:

- Citrix Cloud administrator
- Public API access permission set as part of role-based access configuration. For information, see [Configuring roles with RBAC](#).
- Super user permission

To access the REST API using your Citrix Cloud account, generate the API keys:

1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. Select **API Access > Secure Clients**.
3. Type a name for your secure client and click **Create Client**.

Citrix Cloud then creates the secure client ID and client secret. Download a copy of this information and save it securely offline for your reference. Citrix Cloud doesn't store the unique identifiers after you close the dialog box.

### To invoke REST API services

You can invoke REST API services by using the REST client or cURL commands. The following examples use the Advanced REST client for Chrome.

**Note:**

In the following examples, change the host name and port number to match your environment.

## Log in

The example shown here covers logging in using a token retrieved through Citrix Cloud API.

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login/cloud`

Method type: POST

Content type: application/json

Request sample:

```
1 {
2
3   "bearerToken": "eyJ0e0iJSUzJiibGcI1Ai0NiJ9.
   eyJkIjoMDEExN1c2VIXiMzNDc1OTk4...qf0iQ"
4 }
5
6 <!--NeedCopy-->
```

You must retrieve the bearer token using the Citrix Cloud API <https://trust.citrixworkspacesapi.net/Help/Api/POST-customer-tokens-clients>. For information, see the [Developer documentation](#).

Response sample:

```
1 {
2
3   "auth_token": "q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"
4 }
5
6 <!--NeedCopy-->
```

## Related information

- [Endpoint Management REST API](#)

## ActiveSync Gateway

May 1, 2020

ActiveSync is a mobile data synchronization protocol developed by Microsoft. ActiveSync synchronizes data with handheld devices and desktop (or laptop) computers.

You can configure ActiveSync Gateway rules in Endpoint Management. The ActiveSync gateway retains a list of ActiveSync IDs for all devices configured in Endpoint Management. Based on the rules you configure, you can allow or deny devices access to ActiveSync data, based on those ActiveSync IDs. For example, if you activate the rule **Missing Required Apps**, Endpoint Management checks the App Access Policy for required apps. If the required apps are missing, the policy denies access to ActiveSync data. For each rule, you can choose either **Allow** or **Deny**. The default setting is **Allow**.

For more information about the App Access device policy, see [App access device policy](#).

Endpoint Management supports the following rules:

**Anonymous Devices:** Checks if a device is in anonymous mode. This check is available if Endpoint Management can't reauthenticate the user when a device attempts to reconnect.

**Failed Samsung Knox attestation:** Checks if a device failed a query of the Samsung Knox attestation server.

**Forbidden Apps:** Checks if a device has forbidden apps, as defined in an App Access policy.

**Implicit Allow and Deny:** This action is the default for the ActiveSync Gateway. The gateway creates a Device List of all devices that do not meet any of the other filter rule criteria. The gateway then allows or denies connections based on that list. If no rule matches, the default is **Implicit Allow**.

**Inactive Devices:** Checks if a device is inactive as defined by the **Device Inactivity Days Threshold** setting in **Server Properties**.

**Missing Required Apps:** Checks if a device is missing required apps, as defined in an App Access policy.

**Non-suggested Apps:** Checks if a device has non-suggested apps, as defined in an App Access policy.

**Noncompliant Password:** Checks if the user password is compliant. On iOS and Android devices, Endpoint Management can determine whether the password currently on the device is compliant with the passcode policy sent to the device. For instance, on iOS, the user has 60 minutes to set a password if Endpoint Management sends a passcode policy to the device. Before the user sets the password, the passcode might be non-compliant.

**Out of Compliance Devices:** Checks whether a device is out of compliance, based on the Out of Compliance device property. Automated actions or third parties using Endpoint Management APIs usually change that property.

**Revoked Status:** Checks whether the device certificate was revoked. A revoked device cannot re-enroll until it is authorized again.

**Rooted Android and Jailbroken iOS Devices:** Checks whether an Android or iOS device is jailbroken.

**Unmanaged Devices:** Check whether a device is still in a managed state, controlled by Endpoint Management. For example, a device enrolled in MAM or an unenrolled device is not managed.



**Send Android domain users to ActiveSync Gateway:** Click **YES** to make Endpoint Management send the user name and ActiveSync ID of Android device owners to the ActiveSync Gateway. Turn this feature off unless you're running a legacy configuration. In more recent configurations, this feature allows any device access to ActiveSync data as long as the user name associated with the device exists on the Gateway.

### To configure the ActiveSync Gateway settings

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Server**, click **ActiveSync Gateway**. The **ActiveSync Gateway** page appears.

Settings > ActiveSync Gateway

### ActiveSync Gateway

Allows or denies access to devices and users based on rules and properties.

All devices

Activate the following rule(s)

- Anonymous Devices
- Failed Samsung KNOX attestation
- Forbidden Apps
- Implicit Allow and Deny
- Inactive Devices
- Missing Required Apps
- Non-Suggested Apps
- Noncompliant Password
- Out of Compliance Devices
- Revoked Status
- Rooted Android and Jailbroken iOS Devices
- Unmanaged Devices

Android only

Send Android domain users to ActiveSync Gateway  **YES** ?

Cancel Save

1. In **Activate the following rules**, select one or more rules you want to activate.
2. In **Android-only**, in **Send Android domain users to ActiveSync Gateway**, click **YES** to ensure that Endpoint Management sends Android device information to the ActiveSync Gateway.
3. Click **Save**.

## Endpoint Management connector for Exchange ActiveSync

August 31, 2021

XenMobile Mail Manager is now Endpoint Management connector for Exchange ActiveSync. For details about the Citrix unified portfolio, see the [Citrix product guide](#).

The connector extends the capabilities of Endpoint Management in the following ways:

- Dynamic Access Control for Exchange Active Sync (EAS) devices. EAS devices can be automatically allowed or blocked access to Exchange services.
- The ability for Endpoint Management to access EAS device partnership information provided by Exchange.
- The ability for Endpoint Management to wipe a mobile device based on EAS status.
- The ability for Endpoint Management to access information about Blackberry devices, and to perform control operations such as Wipe and ResetPassword.

To wipe a device based on EAS status, configure an automated action with an ActiveSync trigger. See [Automated Actions](#).

### What's new in version 10.1.10

The following issues are fixed in version 10.1.10:

- Customers who experience frequent network issues may not be able to complete a Snapshot within the previously provided three attempts. With this release, an admin can configure the maximum number of attempts (1-10). This fix allows for a snapshot to incur multiple breaks in communication without abandoning the snapshot process completely. [CXM-70837]

The screenshot shows a 'Configuration' dialog box with the following settings:

- Type: On Premise
- Exchange Server: [Empty text box]
- User: [Empty text box]
- Password: [Empty text box]
- Major snapshot: Every 4 Hours
- Minor snapshot: Every 5 Minutes
- Snapshot Type: Shallow
- Default Access: Unchanged
- Command Mode: Powershell
- Connection Expiration: Every 00 Hours 30 Minutes
- Enable Diagnostics:
- Days to Keep Snapshot Data: 00
- Snapshot Maximum Attempts: 03
- View Entire Forest:
- Authentication: Kerberos
- Allow Redirection:

Buttons: Test Connectivity, Save, Cancel

- In previous versions, the Snapshot type did not appear in the list of Exchange Configurations. Now, the snapshot type appears. [CXM-70846]
- The PSRemotingTransport exception reported by PowerShell indicates that the session to Exchange is no longer viable. The status is added to the Critical Errors list in the configuration file by default. By doing so, when the PSRemotingTransportException is detected, the connection is marked as in Error for disposal later. The next communication uses a valid connection or creates a connection. [XMHELP-2184, CXM-70836]
- When a configuration change is saved, it is possible that not all previously configured internal components were disposed of properly before loading the new configuration. This issue might lead to unpredictable behavior. The behavior depends on the specific change and if the change conflicted with the previous configuration. In this release all internal components are disposed of before loading the new configuration. [XMHELP-2259, CXM-71388]

### What's new in version 10.1.9

The following issues are fixed in version 10.1.9:

- Configuration changes are now handled in a more consistent manner. When the service detects a change in configuration, each internal subsystem is stopped, which means that any active or

scheduled processing is interrupted. Next, the new configuration is loaded and the subsystems are started again, which means that all schedules and other internal infrastructure, are reestablished with new settings. This issue corrects a known issue in version 10.1.8. [CXM-47709, CXM-61330]

- During an upgrade, the existing database configuration was not merged into the new configuration file. The database configuration is now merged into the upgraded configuration file. [CXM-49326]
- In the snapshot-related diagnostics files, the column headers were missing. The headers are restored. [CXM-62680]
- When upgrading from a previous version, the defaults section of the configuration file was being overwritten by the analogous section of the configuration file in use. This issue prevented additions or improvements to the defaults section from being loaded by the service after the upgrade. As of this version, the defaults section always reflects the latest configuration. [CXM-62681]
- Admins can no longer access certain options by pressing Shift when running the application. These options were previously available with Citrix permission. Some options are now fully available, such as Allow Redirection, and others, such as Hang Detection and Count Correction, are deprecated. [CXM-62767]

The screenshot shows a 'Configuration' dialog box with the following settings:

- Type: On Premise
- Exchange Server: [Empty text box]
- User: [Empty text box]
- Password: [Empty text box]
- Major snapshot: Every 4 Hours
- Minor snapshot: Every 5 Minutes
- Snapshot Type: Shallow
- Default Access: Unchanged
- Command Mode: Powershell
- Connection Expiration: Every 00 Hours 30 Minutes
- Enable Diagnostics:
- Days to Keep Snapshot Data: 00
- View Entire Forest:
- Authentication: Kerberos
- Allow Redirection:

Buttons: Test Connectivity, Save, Cancel

## What's new in earlier versions

The following section lists the new features and fixed issues in earlier versions of Endpoint Management connector for Exchange ActiveSync.

### What's new in version 10.1.8

- It is possible that Exchange throttles back the Citrix Endpoint Management connector for Exchange ActiveSync service from issuing commands too frequently. This issue is common in connections to Office 365. The effect of throttling requires that the service pause for a specified period before sending the next command. The Configure console now shows the amount of time remaining in the pause. [CXM-48044]
- When modifications are made to the “Watchdog” and/or “SpecialistsDefaults” sections of the configuration file (config.xml), the changes are not reflected in the configuration file after an upgrade. With this release, the modifications are merged correctly into the new configuration file. [CXM-52523]
- More detail has been added to the analytics sent to Google Analytics, especially concerning snapshots. [CXM-56691]
- The Exchange test connectivity feature would attempt to initialize the connection only once. Because Office 365 connections can be throttled, it was possible that a test connectivity would appear to fail when throttled. Citrix Endpoint Management connector for Exchange ActiveSync now attempts to initiate a connection up to three times. [CXM-58180]
- To effect policies on Exchange, Citrix Endpoint Management connector for Exchange ActiveSync must compile a **Set-CASMailbox** command that includes all pertinent devices for each mailbox, in two lists: allow and block. If a device is not included in either list, Exchange falls back to its default access state. If that default access state is different than the desired state for a device, that device becomes out of compliance. Therefore, a user may lose access to their email if the Exchange default access state is blocked and it should be allowed. Or, a user whose access to email should be blocked may be granted access. Citrix Endpoint Management connector for Exchange ActiveSync now ensures that all devices with a valid desired state are included in each **Set-CasMailbox** command. [CXM-61251]

The following issue is known in version 10.1.8:

If an admin makes a change in the Configure application that modifies configuration data, while the service is performing long duration operations, such as a snapshot or policy evaluation, the service may enter an indeterminate state. A possible symptom may be that policy changes are not processed, or snapshots are not initiated. To return the service to a working state, the service must be restarted. You may need to use the Windows Services manager to terminate the service process before starting the service. [CXM-61330]

### What's new in version 10.1.7

- XenMobile Mail Manager is now Endpoint Management connector for Exchange ActiveSync.
- We have deprecated the **Disable Pipelining** option in the Exchange configuration dialog box. You can achieve the same functionality by configuring multiple steps for each command in the config.xml file. [CXM-54593]

The following issues are fixed in version 10.1.7:

- In the Snapshot History window, error messages might be shown with little context. Now, error messages are prefixed with the context of where they occurred. [CXM-49157]
- The XmmGoogleAnalytics.dll did not have the corresponding file version for the release. [CXM-52518]
- To improve diagnostics, we recently changed the string format for a list of device IDs used to set a mailbox Allowed/Blocked state. A specification of too many devices, however, exceeded the maximum string size. Now, we use an internal array data structure. This structure does not have a size limit and also formats the data appropriately for diagnostic purposes. [CXM-52610]
- When device policies that are not in sync with Exchange are detected, their commands may include devices that do not belong to the relevant mailbox. Endpoint Management connector for Exchange ActiveSync now ensures that commands to Exchange represent only devices that belong to their respective mailboxes. [CXM-54842]
- In some environments, a Microsoft assembly is not available. The required assembly is now explicitly installed with the application. [CXM-55439]
- If Distinguished Names for devices or mailboxes have spaces between the attribute name and the equals, or spaces after the equals and before the value, Endpoint Management connector for Exchange ActiveSync may not properly match a device with its mailbox and the opposite way. The result might be that some devices and/or mailboxes are rejected during the snapshot reconciliation. [CXM-56088]

**Note:**

The following What's New sections refer to Endpoint Management connector for Exchange ActiveSync by its former name of XenMobile Mail Manager. The name changed as of version 10.1.7.

### Update in version 10.1.6.20

An update to 10.1.6 contains the following fix in version 10.1.6.20:

- When device policies that are not in sync with Exchange are detected, their commands may include devices that do not belong to the relevant mailbox. XenMobile Mail Manager now insures that commands to Exchange represent only devices that belong to their respective mailboxes. [CXM-54842]

### What's new in version 10.1.6

XenMobile Mail Manager version 10.1.6 contains the following fixed issues and enhancements:

- The snapshot history window, at times, enters a state where the window is no longer updating. The windows refresh mechanism is improved to update more reliably. [CXM-47983]
- Two separate modes and code paths were used for partitioned and non-partitioned snapshots. Because non-partitioned snapshots are equivalent to partitioned snapshots with a configuration using a single "\*" partition, the non-partitioned snapshot mode is eliminated. The default snapshot mode is now partitioned snapshots with 36 partitions (0–9, A–Z). [CXM-49093]
- In the Snapshot History window, error messages are overwritten by status messages. Now, XenMobile Mail Manager provides two separate fields so that users can view status and errors simultaneously. [CXM-51942]
- When connecting to Exchange Online (Office 365), snapshot-related queries might result in a truncated dataset. This issue may occur when XenMobile Mail Manager executes a multi-command pipelined script. The upstream command cannot pass the data quickly enough to the downstream command, which then completes the work prematurely. Incomplete data occurs as a result. XenMobile Mail Manager can now mimic the pipeline itself and wait until the upstream command is done before invoking the downstream command. This change should result in all data being processed and captured. [CXM-52280]
- If a non-resolvable error occurs in a policy update command to Exchange, the same command is returned to the work queue repeatedly for a long period. This situation resulted in the command being sent to Exchange many times. In this version of XenMobile Mail Manager, a command that results in an error is only returned to the work queue a discrete number of times. [CXM-52633]
- If a policy update for a specific mailbox involved the allowing or blocking of all devices: The issued **Set-CASMailbox** command would fail due to the empty list being converted to an empty string instead of a **NULL**. The proper data is now sent. [CXM-53759]
- When processing a new device, Exchange can return the state as "DeviceDiscovery" for some time (usually 15 minutes). XenMobile Mail Manager was not specifically handling this state. XenMobile Mail Manager now handles the state. In the Monitor tab of the UI, users can filter for devices in this state. [CXM-53840]
- XenMobile Mail Manager did not check for the ability to write to the XenMobile Mail Manager database. Therefore, if permissions were restricted, the behavior might not be predicted. XenMobile Mail Manager now captures and validates required permissions from the database. XenMobile Mail Manager indicates reduced permissions when either testing the connection (message shown) or in the Database indicator (hover for message) at the bottom of the main Configure window. [CXM-54219]
- Depending on the current workload, when directed to, the XenMobile Mail Manager service may not stop promptly. Therefore, the service appears to be in an unresponsive state. Improvements allow ongoing tasks to be interrupted, resulting in a more graceful shutdown. [CXM-54282]

## What's new in version 10.1.5

XenMobile Mail Manager version 10.1.5 contains the following fixed issues:

- When Exchange is applying throttling to XenMobile Mail Manager activity, there is no indication (outside of the logs) that the throttling is occurring. With this release, a user can hover over the active snapshot and a “throttling” state appears. Also, while XenMobile Mail Manager is being throttled, the start of a major snapshot is prohibited until Exchange lifts the throttling embargo. [CXM-49617]
- If XenMobile Mail Manager is being throttled by Exchange during a major snapshot: It is possible that an insufficient amount of time is allowed to elapse before running the next attempt of a snapshot. This issue results in further throttling and a failed snapshot. XenMobile Mail Manager now waits a minimum of the time that Exchange specifies to wait between snapshot attempts. [CXM-49618]
- When diagnostics is enabled, the commands file shows **Set-CasMailbox** commands that have missing hyphens before each property name. This issue only occurs in the formatting of the diagnostics file and not the actual command to Exchange. The missing hyphen prevents a user from cutting the command and directly pasting it to a PowerShell prompt for testing or validation. The hyphens have been added. [CXM-52520]
- If a mailbox identity is of the form `lastname, firstname`, Exchange adds a backslash before the comma when returning data from a query. This backslash must be stripped when XenMobile Mail Manager uses the identity to query for more data. [CXM-52635]

## Known limitation

### Note:

The following limitation is resolved in version 10.1.6.

XenMobile Mail Manager has a known limitation that can cause commands to Exchange to fail. To apply policy changes to Exchange, a **Set\_CASMailbox** command is issued by XenMobile Mail Manager. This command can take two lists of devices: one to Allow and one to Block. The command is applied to the devices partnered with a mailbox.

These lists are limited to 256 characters each by the Microsoft API. If one of those lists exceeds the limitation, the command fails in its entirety, preventing the policies for those devices of the mailbox to be set. The error reported, which appears in the XenMobile Mail Manager logs, would look like the following. The example is for the blocked list.

“Message:’Cannot bind parameter ‘ActiveSyncBlockedDeviceIDs’ to the target. Exception setting “ActiveSyncBlockedDeviceIDs”: “The length of the property is too long. The maximum length is 256 and the length of the value provided is ...”

Device ID lengths can vary, but a good guideline is that about 10 devices or more simultaneously Al-



lowed or Blocked might exceed the limit. Although having that many devices associated with a specific mailbox is rare, it is a possibility. Until XenMobile Mail Manager is improved to handle such a scenario, we recommend that you limit the number of devices associated with a user and mailbox to 10 or fewer. [CXM-52633]

### What's new in version 10.1.4

XenMobile Mail Manager version 10.1.4 contains the following fixed issues:

- Due to its weakening security, the PCI Council is deprecating TLS 1.0 and TLS 1.1. Support for 1.2 is added to XenMobile Mail Manager. [CXM-38573, CXM-32560]
- XenMobile Mail Manager includes a new diagnostic file. When **Enable Diagnostics** is selected in the Exchange specification, a new Snapshot History file is generated. With every snapshot attempt, a line is added to the file with the results of the snapshot. [CXM-49631]
- In the Commands diagnostic file, the list of devices allowed or blocked did not appear for the **Set-CASMailbox** command. Instead the internal class name was shown in the file for the related arguments. XenMobile Mail Manager now shows the list of deviceIDs as a comma-delimited list. [CXM-50693]
- When an attempt to acquire a connection to Exchange fails due to a bad specification: An incorrect message overrides the error message: "All connections in use". More descriptive messages now appear, such as "All connections are inoperable", "Connection pool is empty", "All connections are throttled", and "No available connections". [CXM-50783]
- Sometimes, Allow/Block/Wipe commands are queued up in the XenMobile Mail Manager internal cache multiple times. This issue causes a delay in the command being sent to Exchange. XenMobile Mail Manager now only queues up one instance of each command. [CXM-51524]

### What's new in version 10.1.3

- **Google Analytics support:** We want to know how you use XenMobile Mail Manager so we can focus on where we can make the product better.
- **Setting for enabling diagnostics:** An **Enable Diagnostic** check box appears in the Configure console on the **Configuration** dialog box.

The screenshot shows a 'Configuration' dialog box with the following settings:

- Type: On Premise
- Exchange Server: [Empty text box]
- User: [Empty text box]
- Password: [Empty text box]
- Major snapshot: Every 4 Hours
- Minor snapshot: Every 5 Minutes
- Snapshot Type: Shallow
- Default Access: Unchanged
- Command Mode: Powershell
- Connection Expiration: Every 00 Hours 00 Minutes
- Enable Diagnostics:
- View Entire Forest:
- Authentication: Kerberos

Buttons: Test Connectivity, Save, Cancel

### Fixed issues in version 10.1.3

- In the **Snapshot History** window, tooltips that show the current state of the snapshot do not reflect the actual state. [CXM-5570]  
Occasionally, XenMobile Mail Manager cannot write to the Commands diagnostics file. When this occurs, the command history is not logged in its entirety. [CXM-49217]
- When an error occurs with a connection, the connection may not be marked as “errored”. As a result, a subsequent command may attempt to use the connection and cause another error. [CXM-49495]
- When throttling from the Exchange Server occurs, an exception might be thrown in the Check Health routine. As a result, connections that have experienced an error or have expired might not be purged. Also, XenMobile Mail Manager might not create connections until the throttling time expires. [CXM-49794].
- When the max session count for Exchange is exceeded, XenMobile Mail Manager reports the error “Device Capture Failed,” which is not an accurate message. Instead, the message should indicate that the two sessions that XenMobile Mail Manager normally uses for Exchange communication are in use. [CXM-49994]

### What's new in version 10.1.2

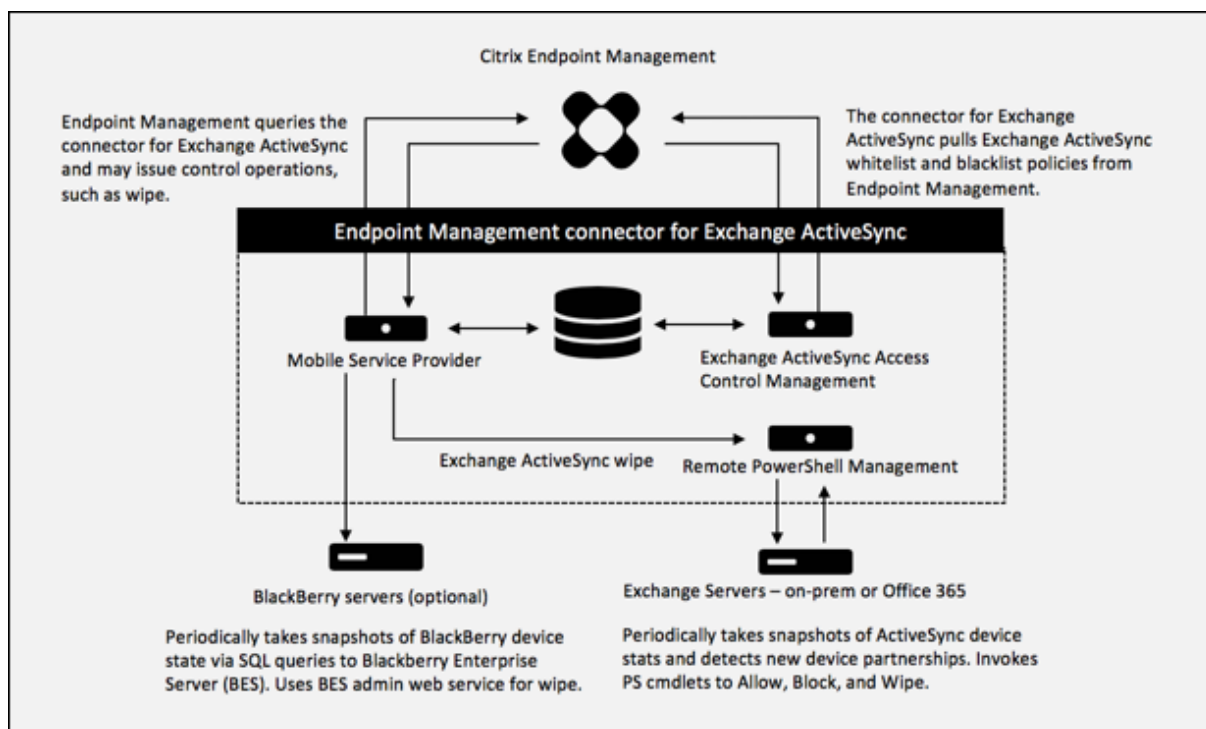
- **Improved connection to Exchange:** XenMobile Mail Manager uses PowerShell sessions to communicate with Exchange. A PowerShell session, especially when dealing with Office 365, can become unstable after a while, blocking subsequent commands from succeeding. XenMobile Mail Manager can now set an expiration period for connections. When the connection reaches its expiration time, XenMobile Mail Manager gracefully shuts down the PowerShell session and creates a session. By doing so, the PowerShell session is less likely to become unstable, significantly reducing the chance of a snapshot failure.
- **Improved snapshot workflow:** Major snapshots are a time-consuming and process-intensive operation. If an error occurs during a snapshot, XenMobile Mail Manager now attempts multiple times (up to three) to complete a snapshot. Subsequent attempts do not start from the beginning. XenMobile Mail Manager continues from where it left off. This enhancement improves the success rate of snapshots in general by allowing transient errors to pass while a snapshot is still in progress.
- **Improved diagnostics:** Troubleshooting snapshot operations are now easier with three new diagnostics files optionally generated during a snapshot. These files help identify PowerShell command issues, mailboxes with missing information, and devices that cannot be related to a mailbox. An admin can use these files to identify data that may not be correct in Exchange.
- **Improved memory usage:** XenMobile Mail Manager is now more efficient in its use of memory. Admins can schedule XenMobile Mail Manager to restart automatically to provide a clean slate to the system.
- **Microsoft .NET Framework 4.6 prerequisite:** The prerequisite version of Microsoft .NET Framework is now version 4.6.

### Fixed issues

- Prompt for credentials error: Office 365 session instability often caused this error. The Improved Connection to Exchange enhancement addresses the problem. (XMHELP-293, XMHELP-311, XMHELP-801)
- Mailbox and device count inaccuracies: XenMobile Mail Manager has an improved Mailbox-to-Device association algorithm. The Improved Diagnostics feature helps in the identification of mailboxes and devices that XenMobile Mail Manager deems are not within its realm of responsibility. (XMHELP-623)
- Allow/Block/Wipe commands not being recognized: A bug was fixed where sometimes, XenMobile Mail Manager allow/block/wipe commands are not recognized. (XMHELP-489)
- Memory management: Better memory management and mitigation. (XMHELP-419)

## Architecture

The following diagram shows the main components of Endpoint Management connector for Exchange ActiveSync. For a detailed reference architecture diagram, see [Architecture](#).



The three main components are:

- **Exchange ActiveSync Access Control Management:** Communicates with Endpoint Management to retrieve an Exchange ActiveSync policy from Endpoint Management, and merges this policy with any locally defined policy to determine the Exchange ActiveSync devices that should be allowed or denied access to Exchange. Local policy allows extending the policy rules to allow access control by Active Directory Group, User, Device Type, or Device User Agent (generally the mobile platform version).
- **Remote PowerShell Management:** Responsible for scheduling and invoking remote PowerShell commands to enact the policy compiled by Exchange ActiveSync Access Control Management. Periodically takes a snapshot of the Exchange ActiveSync database to detect new or changed Exchange ActiveSync devices.
- **Mobile Service Provider:** Provides a web service interface so that Endpoint Management can query Exchange ActiveSync, query BlackBerry devices, and issue control operations such as Wipe against ActiveSync and BlackBerry devices.

## System requirements and prerequisites

The following minimum system requirements are required to use Endpoint Management connector for Exchange ActiveSync:

- Windows Server 2016, Windows Server 2012 R2, or Windows Server 2008 R2 Service Pack 1. Must be an English-based server. Support for Windows Server 2008 R2 Service Pack 1 ends on January 14, 2020.
- Microsoft SQL Server 2016 Service Pack 2, SQL Server 2014 Service Pack 3, or SQL Server 2012 Service Pack 4.
- Microsoft .NET Framework 4.6.
- Blackberry Enterprise Service, version 5 (optional).

Minimum supported versions of Microsoft Exchange Server:

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 Service Pack 3 (support ends January 14, 2020)

### Prerequisites

- Windows Management Framework must be installed.
  - PowerShell V5, V4, and V3
- The PowerShell execution policy must be set to RemoteSigned via Set-ExecutionPolicy RemoteSigned.
- TCP port 80 must be open between the computer running the connector for Exchange ActiveSync and the remote Exchange Server.

**Device email clients:** Not all email clients consistently return the same ActiveSync ID for a device. Because the connector for Exchange ActiveSync expects a unique ActiveSync ID for each device, only email clients that consistently generate the same, unique ActiveSync ID for each device are supported. These email clients have been tested by Citrix and performed without errors:

- Samsung native email client
- iOS native email client

**Exchange:** The requirements for the on-premises computer running Exchange are as follows:

The credentials specified in the Exchange Configuration UI must be able to connect to the Exchange Server and be given full access to execute the following Exchange-specific PowerShell cmdlets.

- **For Exchange Server 2010 SP2:**
  - `Get-CASMailbox`
  - `Set-CASMailbox`

- `Get-Mailbox`
- `Get-ActiveSyncDevice`
- `Get-ActiveSyncDeviceStatistics`
- `Clear-ActiveSyncDevice`
- `Get-ExchangeServer`
- `Get-ManagementRole`
- `Get-ManagementRoleAssignment`
- **For Exchange Server 2013 and Exchange Server 2016:**
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`
- If the connector for Exchange ActiveSync is configured to view the entire forest, permission must have been granted to run: **Set-AdServerSettings -ViewEntireForest \$true**
- The supplied credentials must have been granted the right to connect to the Exchange Server via the remote Shell. By default, the user who installed Exchange has this right.
- To establish a remote connection and run remote commands, the credentials must correspond to a user who is an administrator on the remote machine. You can use `Set-PSSessionConfiguration` to eliminate the administrative requirement, but discussion of that command is beyond the scope of this document. For more information, see the Microsoft article [About Session Configurations](#).
- The Exchange Server must be configured to support remote PowerShell requests via HTTP. Typically, an administrator running the following PowerShell command on the Exchange Server is all that is required: `WinRM QuickConfig`.
- Exchange has many throttling policies. One of the policies controls how many concurrent PowerShell connections are allowed per user. The default number of simultaneous connections allowed for a user is 18 on Exchange 2010. When the connection limit is reached, the connector for Exchange ActiveSync is not able to connect to Exchange Server. There are ways to change the maximum allowed simultaneous connections via PowerShell that are beyond the scope of this documentation. If interested, investigate Exchange throttling policies as related to remote management with PowerShell.

## Requirements for Office 365 Exchange

- **Permissions:** The credentials specified in the Exchange Configuration UI must be able to connect to Office 365 and be given full access to run the following Exchange-specific PowerShell cmdlets:
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`
- **Privileges:** The supplied credentials must have been granted the right to connect to the Office 365 server via the remote Shell. By default, Office 365 online administrator has the requisite privileges.
- **Throttling policies:** Exchange has many throttling policies. One of the policies controls how many concurrent PowerShell connections are allowed per user. The default number of simultaneous connections allowed for a user is three on Office 365. When the connection limit is reached, the connector for Exchange ActiveSync is not able to connect to Exchange Server. There are ways to change the maximum allowed simultaneous connections via PowerShell that are beyond the scope of this documentation. If interested, investigate Exchange throttling policies as related to remote management with PowerShell.

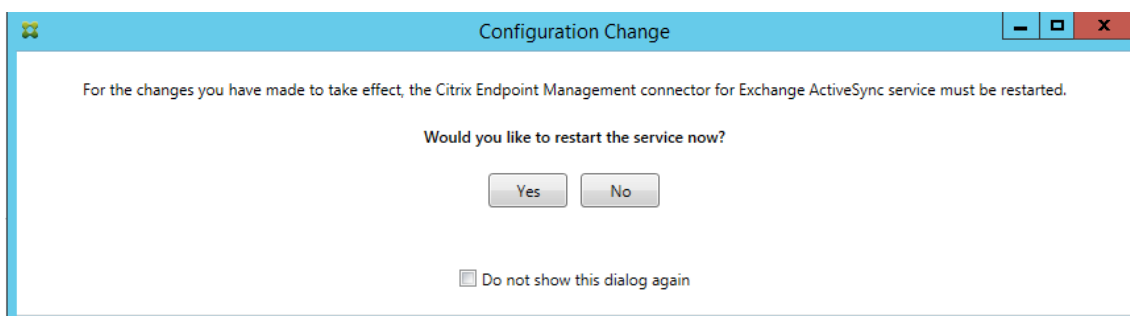
## Install and configure

1. Click the XmmSetup.msi file and then follow the prompts in the installer to install Endpoint Management connector for Exchange ActiveSync.
2. Leave **Launch the Configure utility** selected in the last screen of the setup wizard. Or, from the **Start** menu, open the connector for Exchange ActiveSync.
3. Configure the following database properties:
  - Select the **Configure > Database** tab.
  - Enter the name of the SQL Server (defaults to localhost).
  - Keep the database as the default **CitrixXmm**.
4. Select one of the following authentication modes used for SQL:
  - **SQL:** Enter the user name and password of a valid SQL user.
  - **Windows Integrated:** If you select this option, the logon credentials of the XenMobile Mail Manager Service must be changed to a Windows account that has permissions to access

the SQL Server. To do this, open **Control Panel > Administrative Tools > Services**, right-click the XenMobile Mail Manager Service entry and then click the **Log On** tab.

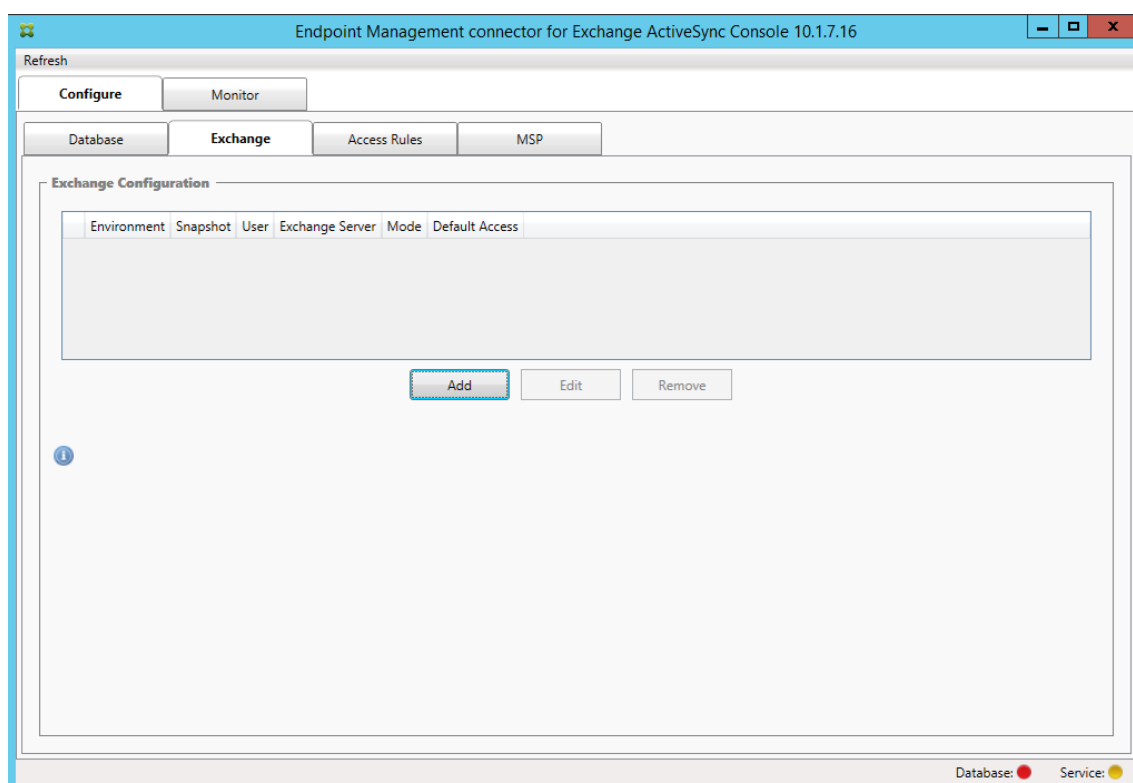
If Windows Integrated is also chosen for the BlackBerry database connection, the Windows account specified here must also be given access to the BlackBerry database.

5. Click **Test Connectivity** to check that a connection can be made to the SQL Server and then click **Save**.
6. A message prompts you to restart the service. Click **Yes**.



7. Configure one or more Exchange Servers:

- If managing a single Exchange environment, specify a single server only. If managing multiple Exchange environments, specify a single Exchange Server for each Exchange environment.
- Click the **Configure > Exchange** tab and then click **Add**.



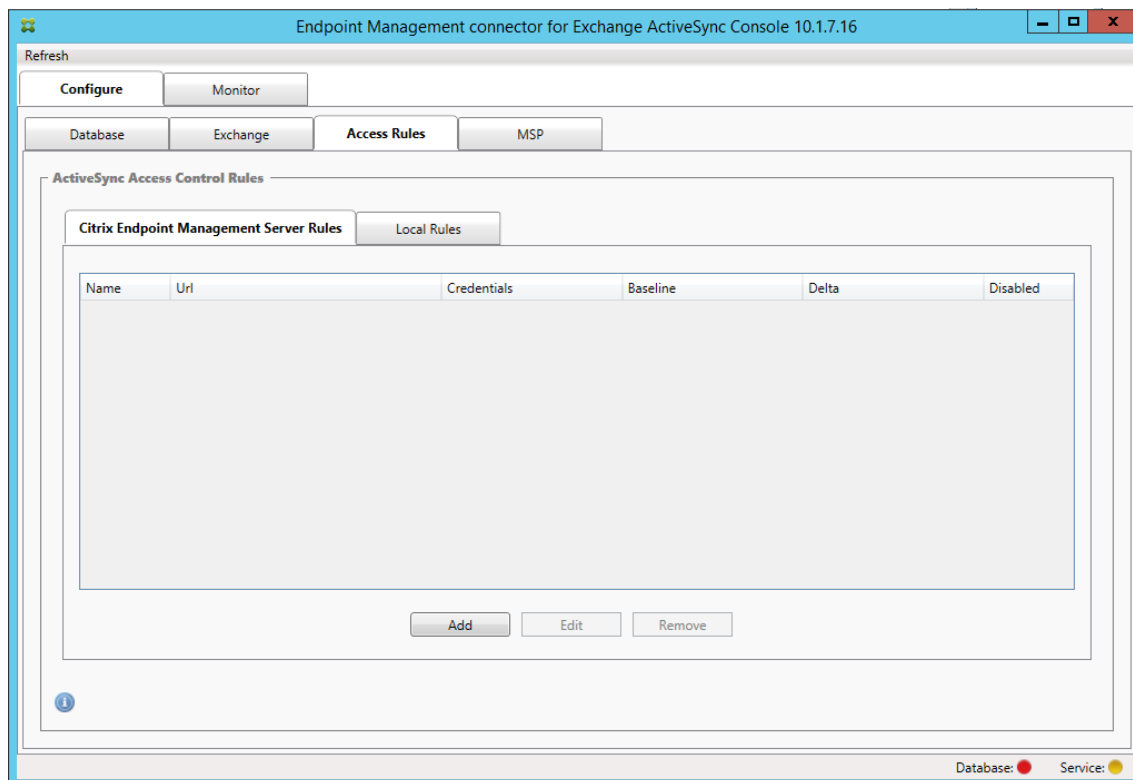


8. Select the type of Exchange Server environment: **On Premise** or **Office 365**.
- If you select **On Premise**, enter the name of the Exchange Server to use for Remote PowerShell commands.
  - Enter the **user name** of a Windows identity that has appropriate rights on the Exchange Server as specified within the Requirements section and then enter the **Password** for the user.
  - Select the schedule for running Major snapshots. A major snapshot detects every Exchange ActiveSync partnership.
  - Select the schedule for running Minor snapshots. A minor snapshot detects newly created Exchange ActiveSync partnerships.
  - Select the Snapshot Type: **Deep** or **Shallow**. Shallow snapshots are typically much faster and are sufficient to perform all the Exchange ActiveSync Access Control functions of the connector for Exchange ActiveSync. Deep snapshots may take longer and are only needed if the Mobile Service Provider is enabled for ActiveSync. This option allows Endpoint Management to query for unmanaged devices.
  - Select the Default Access: **Allow**, **Block**, or **Unchanged**. This setting controls how all devices other than those devices identified by explicit Endpoint Management or Local rules are treated. If you select **Allow**, ActiveSync access to all such devices is allowed. If you select **Block**, access is denied. If you select **Unchanged**, no change is made.
  - Select the ActiveSync Command Mode: **PowerShell** or **Simulation**.
  - In **PowerShell** mode, the connector for Exchange ActiveSync issues PowerShell commands to enact the desired access control. In Simulation mode, the connector for Exchange ActiveSync does not issue PowerShell commands, but logs the intended command and intended outcomes to the database. In Simulation mode, the user can then use the **Monitor** tab to see what would have happened if PowerShell mode was enabled.
  - In **Connection Expiration**, set the hours and minutes for the life of a connection. When a connection reaches the age specified, the connection is marked as expired, so that the connection is never used again. When the expired connection is no longer used, the connector for Exchange ActiveSync gracefully shuts down the connection. When a connection is needed again, a new connection is initialized if none is available. If none is specified, the default of 30 minutes is used.
  - Select **View Entire Forest** to configure the connector for Exchange ActiveSync to view the entire Active Directory forest in the Exchange environment.
  - Select the authentication protocol: **Kerberos** or **Basic**. The connector for Exchange ActiveSync supports Basic authentication for on-premises deployments. This enables the connector to be used when the connector server is not a member of the domain in which the Exchange server resides.
  - Click **Test Connectivity** to check that a connection can be made to the Exchange Server

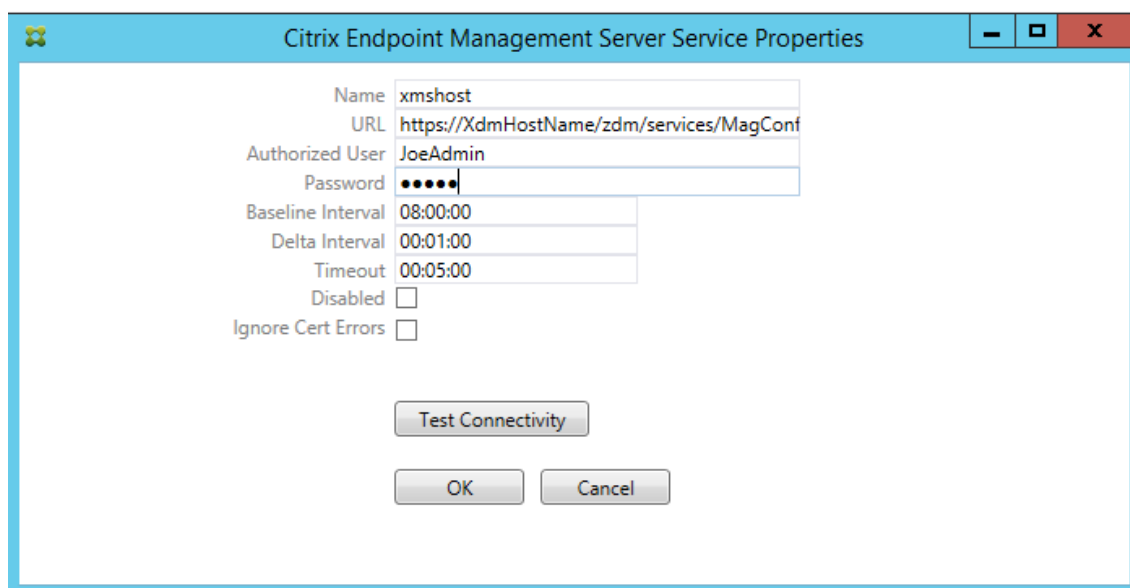
and then click **Save**.

- A message prompts you to restart the service. Click **Yes**.

9. Configure the access rules: Select the **Configure > Access Rules** tab, click the **Citrix Endpoint Management Rules** tab and then click **Add**.



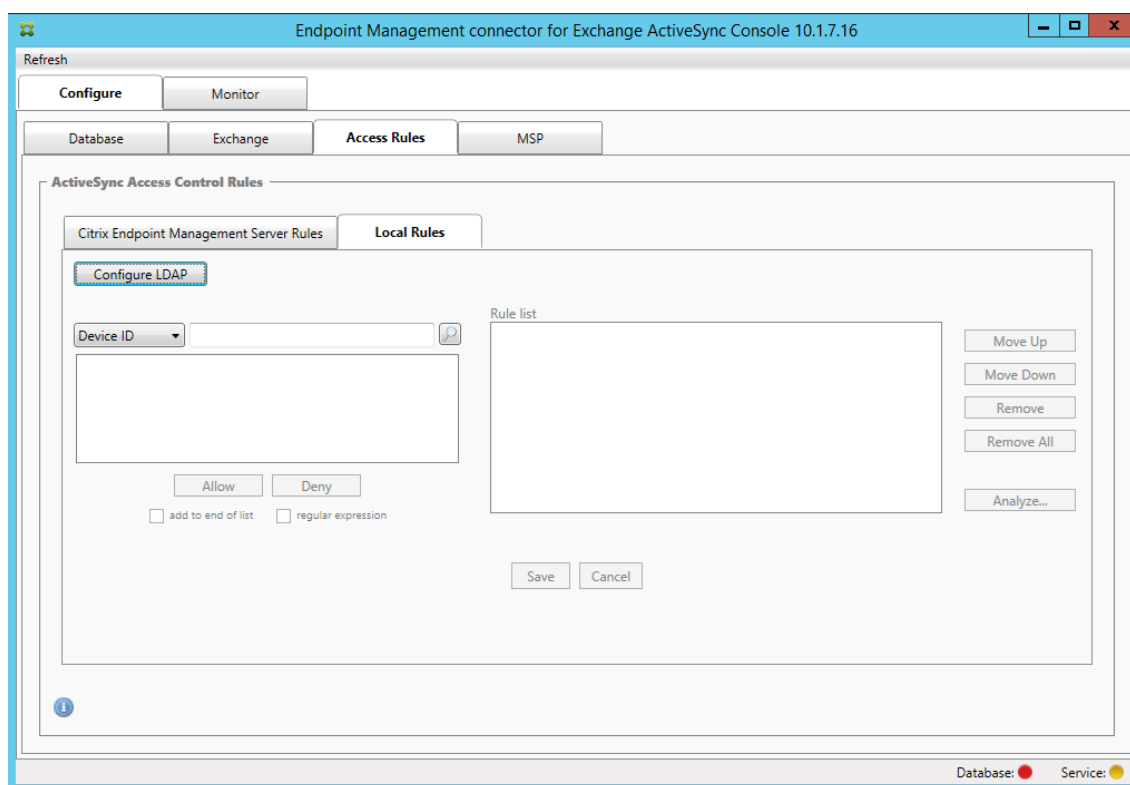
10. On the **Endpoint Management server Service Properties** page, modify the URL string to point to the Endpoint Management server. For example, if the instance name is `zdm`, enter `https://<XdmHostName>/zdm/services/MagConfigService`. In the example, replace `XdmHostName` with the IP or DNS address of the Endpoint Management server.



- Enter an authorized user of the server.
- Enter the password of the user.
- Keep the default values for the **Baseline Interval**, **Delta Interval**, and **Timeout** values.
- Click **Test Connectivity** to check the connection to the server and then click **OK**.

If the **Disabled** check box is selected, the Endpoint Management Mail Service doesn't collect policies from Endpoint Management.

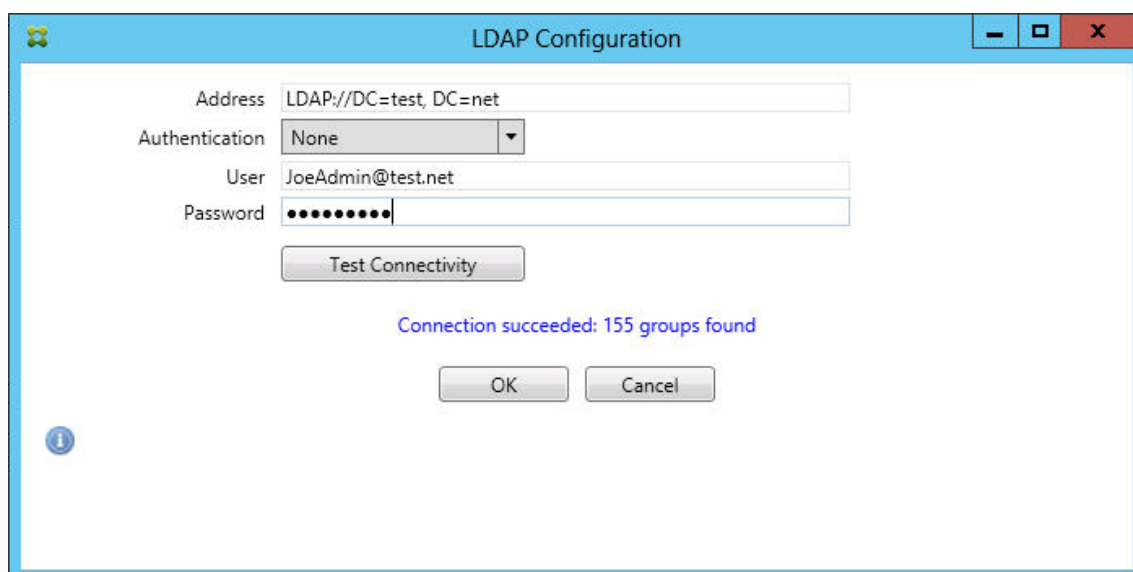
11. Click the **Local Rules** tab.



- You can add local rules based on ActiveSync Device ID, Device Type, AD Group, User, or device UserAgent. In the list, select the appropriate type.
- Enter text or text fragments in the text box. Optionally, click the query button to view the entities that match the fragment.

For all types other than Group, the system relies on the devices that have been found in a snapshot. Therefore, if you are just starting and haven't completed a snapshot, no entities are available.

- Select a text value and then click **Allow** or **Deny** to add it to the **Rule List** pane on the right side. You can change the order of rules or remove them using the buttons to the right of the **Rule List** pane. The order is important because, for a given user and device, rules are evaluated in the order shown and a match on a higher rule (nearer the top) causes subsequent rules to have no effect. For example, if you have a rule allowing all iPad devices and a subsequent rule blocking the user Matt, Matt's iPad will still be allowed because the iPad rule has a higher effective priority than the Matt rule.
  - To perform an analysis of the rules within the rules list to find any potential overrides, conflicts, or supplemental constructs, click **Analyze** and then click **Save**.
12. If you want to construct local rules that operate on Active Directory Groups, click **Configure LDAP** and then configure the LDAP connection properties.



13. To configure the Mobile Service Provider, click the **Configure > MSP** tab.

The Mobile Service Provider is optional. That setting is necessary only if Endpoint Management is also configured to use the Mobile Service Provider interface to query unmanaged devices.

- Set the Service Transport type as **HTTP** or **HTTPS** for the Mobile Service Provider service.
  - Set the **Service port** (typically 80 or 443) for the Mobile Service Provider service. If you use port 443, the port requires an SSL certificate bound to it in IIS.
  - Set the **Authorization Group** or **User**. This sets the user or set of users who will be able to connect to the Mobile Service Provider service from Endpoint Management.
  - Set whether ActiveSync queries are enabled or not. If ActiveSync queries are enabled for the Endpoint Management server, the Snapshot type for one or more Exchange Servers must be set to **Deep**. That setting might have significant performance costs for taking snapshots.
  - By default, ActiveSync devices that match the regular expression `WorxMail*` will not be sent to Endpoint Management. To change this behavior, alter the **Filter ActiveSync** field as necessary. Blank means that all devices are forwarded to Endpoint Management.
  - Click **Save**.
14. Optionally, configure one or more instances of BlackBerry Enterprise Server (BES): Click **Add** and then enter the server name of the BES SQL Server

BES Properties

BES Sql Server

Server: BesServer

Database: BesMgmt

Authentication: Sql

User name: JoeAdmin

Password: ●●●●●●

Test Connectivity

Sync Schedule: Every 30 Minutes

Blackberry Device Administration from XMS

Enabled:

BAS Server: BAServer

BAS Port: 443

Domain\User: ServerName\JoeAdmin

Password: ●●●●●●

Test Connectivity

Save Cancel

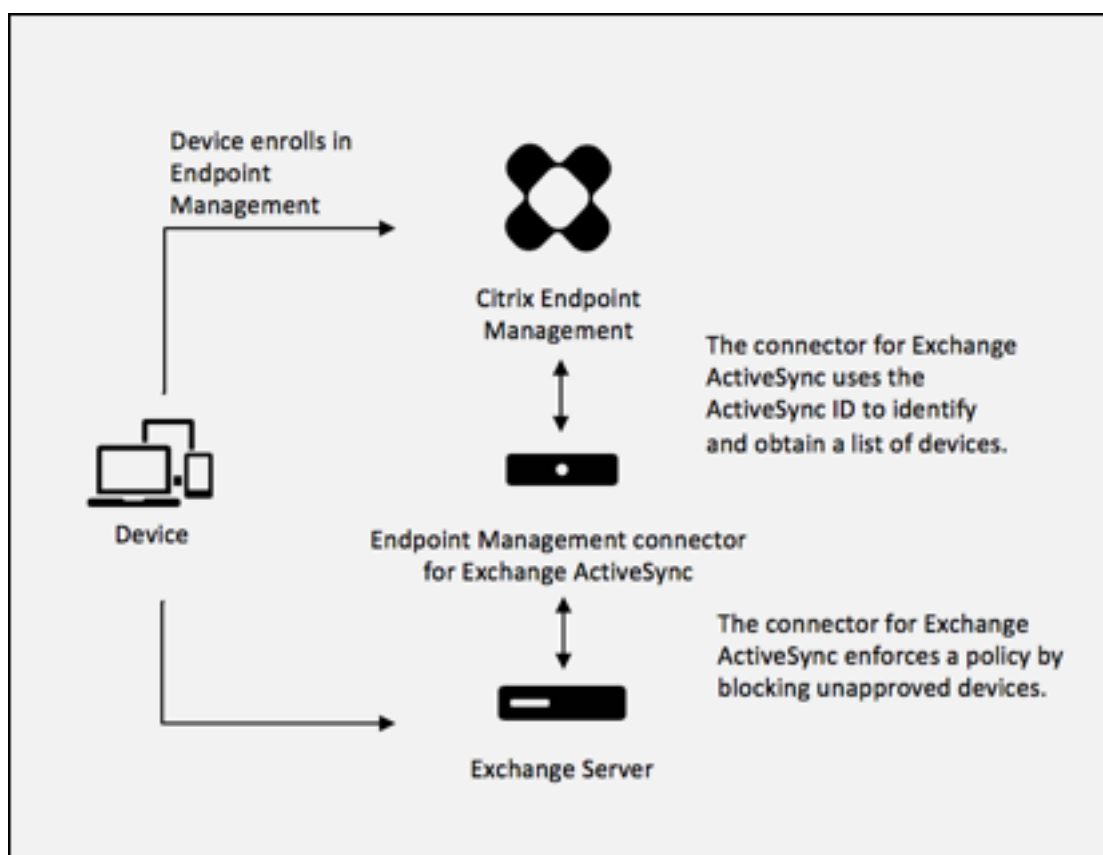
- Enter the database name of the BES management database.
- Select the **Authentication** mode. If you select Windows Integrated authentication, the user account of the connector for Exchange ActiveSync service is the account that is used to connect to the BES SQL Server. If you also choose Windows Integrated for the connector database connection, the Windows account specified here must also be given access to the connector database.
- If you select **SQL authentication**, enter the user name and password.
- Set the **Sync Schedule**. This is the schedule used to connect to the BES SQL Server and checks for any device updates.
- Click **Test Connectivity** to check connectivity to the SQL Server. If you select Windows Integrated, this test uses the current logged on user and not the connector service user and therefore does not accurately test SQL authentication.
- To support remote Wipe and ResetPassword of BlackBerry devices from Endpoint Management, select the **Enabled** check box.

- Enter the BES fully qualified domain name (FQDN).
- Enter the BES port used for the admin web service.
- Enter the fully qualified user and password required by the BES service.
- Click **Test Connectivity** to test the connection to the BES and then click **Save**.

### Enforce email policies with ActiveSync IDs

Your corporate email policy may dictate that certain devices are not approved for corporate email use. To comply with this policy, you want to ensure that employees cannot access corporate email from such devices. Endpoint Management connector for Exchange ActiveSync and Endpoint Management work together to enforce such an email policy. Endpoint Management sets the policy for corporate email access. When an unapproved device enrolls with Endpoint Management, the connector for Exchange ActiveSync enforces the policy.

The email client on a device advertises itself to Exchange Server (or Office 365) using the device ID, also known as the ActiveSync ID, which is used to identify the device. Secure Hub obtains a similar identifier and sends the identifier to Endpoint Management when the device is enrolled. By comparing the two device IDs, the connector for Exchange ActiveSync can determine whether a specific device should have corporate email access. The following figure illustrates this concept:



If Endpoint Management sends the connector for Exchange ActiveSync an ActiveSync ID that is different from the ID the device publishes to Exchange, the connector cannot indicate to Exchange what to do with the device.

Matching ActiveSync IDs works reliably on most platforms. However, Citrix has found that on some Android implementations, the ActiveSync ID from the device is different from the ID that the mail client advertises to Exchange. To mitigate this problem, you can do the following:

- On the Samsung SAFE platform, push the device ActiveSync configuration from Endpoint Management.
- On all other Android platforms, Citrix recommends that you use Citrix Secure Mail.

To guarantee that your corporate email access policy is enforced properly, you can adopt a defensive security stance. Configure Endpoint Management connector for Exchange ActiveSync to block emails by setting the static policy to **Deny** by default. This means that if an employee configures another email client on an Android device, and ActiveSync ID detection does not work, corporate email denies access to the employee.

### Access control rules

Endpoint Management connector for Exchange ActiveSync provides a rule-based approach for dynamically configuring access control for Exchange ActiveSync devices. A connector access control rule consists of two parts: a matching expression and a desired access state (Allow or Block). A rule may be evaluated against a given Exchange ActiveSync device to determine if the rule applies to, or matches the device. There are multiple kinds of matching expressions; for example, a rule may match all devices of a given Device Type, or a specific Exchange ActiveSync device ID, or all devices of a specific user, and so on.

At any point during the adding, removing, and rearranging of the rules in the rule list, clicking the **Cancel** button reverts the rules list back to the state at which it was when first opened. Unless you click **Save**, any changes made to this window are lost if you close the Configure tool.

Endpoint Management connector for Exchange ActiveSync has three types of rules: local rules, Endpoint Management server rules (also known as XDM rules), and the default access rule.

**Local rules:** Local rules have the highest priority: If a device is matched by a local rule, rule evaluation stops. Neither Endpoint Management server rules nor the default access rule will be consulted. Local rules are configured locally to the connector for Exchange ActiveSync via the **Configure > Access Rules > Local Rules** tab. Support matching is based upon a user's membership within a given Active Directory group. Support matching is based on regular expressions for the following fields:

- Active Sync Device ID
- ActiveSync Device Type
- User Principal Name (UPN)



- ActiveSync User Agent (typically the device platform or email client)

As long as a major snapshot has completed and found devices, you should be able to add either a normal or regular expression rule. If a major snapshot has not completed, you can only add regular expression rules.

**Endpoint Management server rules:** Endpoint Management server rules are references to an external Endpoint Management server that provides rules about managed devices. The Endpoint Management server can be configured with its own high-level rules that identify the devices to be allowed or blocked based on properties known to Endpoint Management, such as whether the device is jailbroken or whether the device contains forbidden apps. Endpoint Management evaluates the high-level rules and produces a set of allowed or blocked ActiveSync Device IDs, which are then delivered to XenMobile Mail Manager.

**Default access rule:** The default access rule is unique in that it can potentially match every device and is always evaluated last. This rule is the catch-all rule, which means that if a given device does not match a local or Endpoint Management server rule, the desired access state of the device is determined by the desired access state of the default access rule.

- **Default Access – Allow:** Any device that is not matched by either a local or Endpoint Management server rule will be allowed.
- **Default Access – Block:** Any device that is not matched by either a local or Endpoint Management server rule will be blocked.
- **Default Access - Unchanged:** Any device that is not matched by either a local or Endpoint Management server rule will not have its access state modified in any way by the connector for Exchange ActiveSync. If a device has been placed into Quarantine mode by Exchange, no action is taken; for example, the only way to remove a device from Quarantine mode is to have an explicitly Local or XDM rule override the quarantine.

### About Rule Evaluations

For each device that Exchange reports to the connector for Exchange ActiveSync, the rules are evaluated in sequence, from highest to lowest priority as follows:

- Local rules
- Endpoint Management server rules
- Default access rule

When a match is found, evaluation stops. For example, if a local rule matches a given device, the device will not be evaluated against any of the Endpoint Management server rules or the default access rule. This holds true within a given rule type as well. For example, if there's more than a single match for a given device in the local rule list, when the first match is encountered, evaluation stops.

The connector for Exchange ActiveSync reevaluates the currently defined set of rules when device

properties change, or when devices are added or removed, or when the rules themselves change. Major snapshots pick up device property changes and removals at configurable intervals. Minor Snapshots pick up new devices at configurable intervals.

Exchange ActiveSync has rules governing access as well. It is important to understand how these rules work in the context of the connector for Exchange ActiveSync. Exchange may be configured with three levels of rules: personal exemptions, device rules, and organization settings. The connector for Exchange ActiveSync automates access control by programmatically issuing Remote PowerShell requests to affect the personal exemptions lists. These are lists of allowed or blocked Exchange ActiveSync device IDs associated with a given mailbox. When deployed, the connector for Exchange ActiveSync effectively takes over management of the exemption lists capability within Exchange. See the Microsoft article, [Device management with Exchange and Configuration Manager](#).

Analyzing is particularly useful in situations in which multiple rules for the same field have been defined. You can troubleshoot the relationships between rules. You perform analysis from the perspective of rule fields; for example, rules are analyzed in groups based on the field that is being matched, such as ActiveSync device ID, ActiveSync device type, User, User Agent, and so on.

### Rule terminology

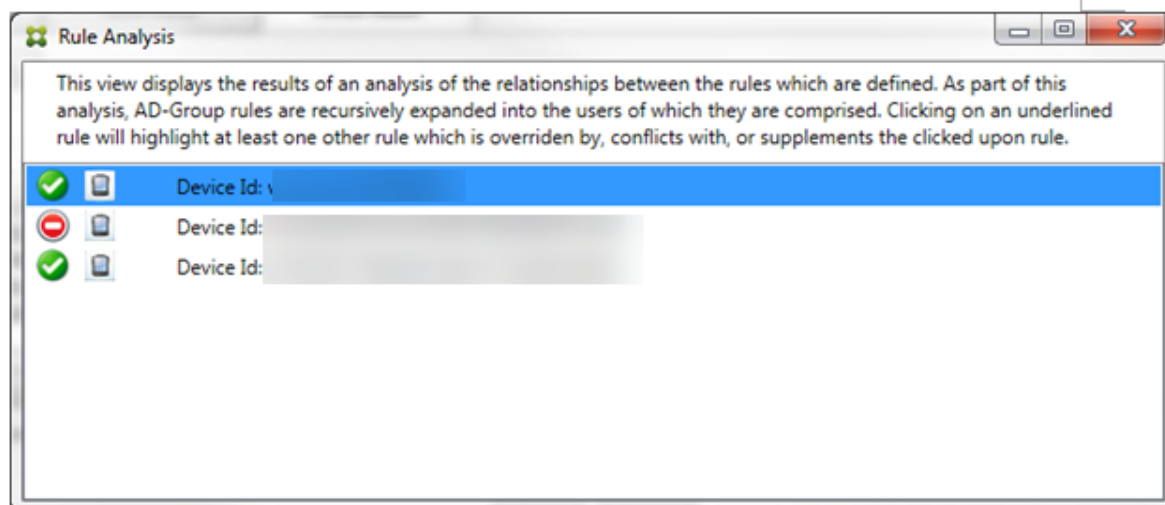
- **Overriding rule:** An override occurs when more than a single rule can apply to the same device. Because rules are evaluated by priority in the list, the later rule instance(s) which might apply might never be evaluated.
- **Conflicting rule:** A conflict occurs when more than a single rule can apply to the same device but the access (Allow/Block) does not match. If the conflicting rules are not regular expression rules, a conflict always implicitly connotes an override
- **Supplemental rule:** A supplement occurs when more than one rule is a regular expression rule and hence there might be a need to ensure that the two (or more) regular expressions can either be combined into a single regular expression rule, or are not duplicating functionality. A supplementary rule may also conflict in its access (Allow/Block).
- **Primary rule:** The primary rule is the rule that has been clicked within the dialog box. The rule is indicated visually by a solid border line that surrounds it. The rule will also have one or two green arrows pointing up or down. If an arrow points up, the arrow indicates that there are ancillary rules that precede the primary rule. If an arrow points down, this indicates that there are ancillary rules that come after the primary rule. Only a single primary rule can be active at any time.
- **Ancillary rule:** An ancillary rule is related in some way to the primary rule either through override, conflict, or a supplementary relationship. The rules are indicated visually by a dashed border that surrounds them. For each primary rule, there can be between one and many ancillary rules. When clicking on any underlined entry, the ancillary rule or rules that are highlighted are always from the perspective of the primary rule. For example, the ancillary rule is overridden

by the primary rule, or the ancillary rule will conflict in its access with the primary rule, or the ancillary rule will supplement the primary rule.

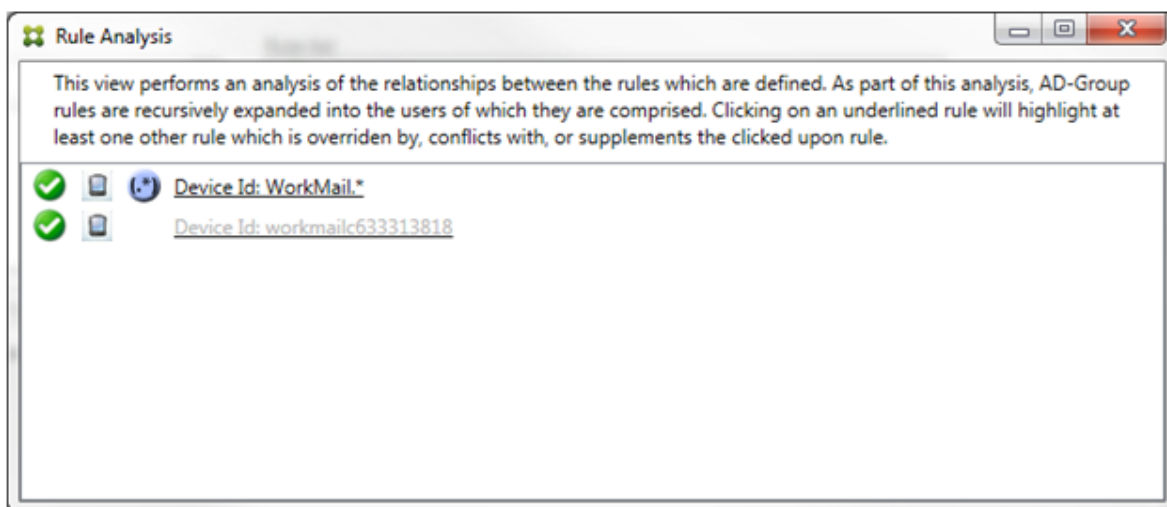
### How types of rules appear in the Rule Analysis dialog box

When there are no conflicts, overrides, or supplements, the Rule Analysis dialog box has no underlined entries. Clicking any of the items has no impact; for example, normal selected item visuals occur.

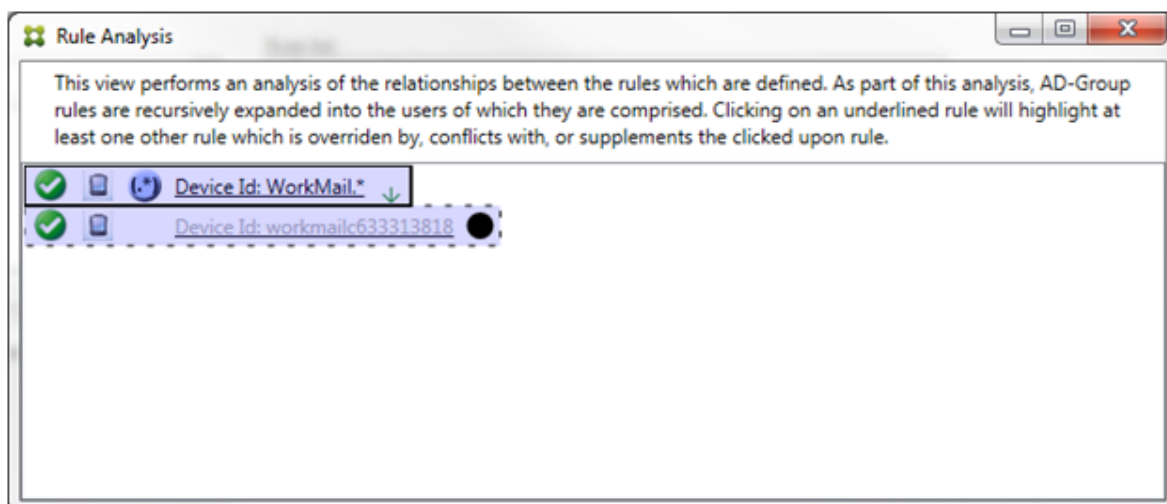
The Rule Analysis window has a check box which, when selected, displays only those rules which are conflicts, overrides, redundancies, or supplements.



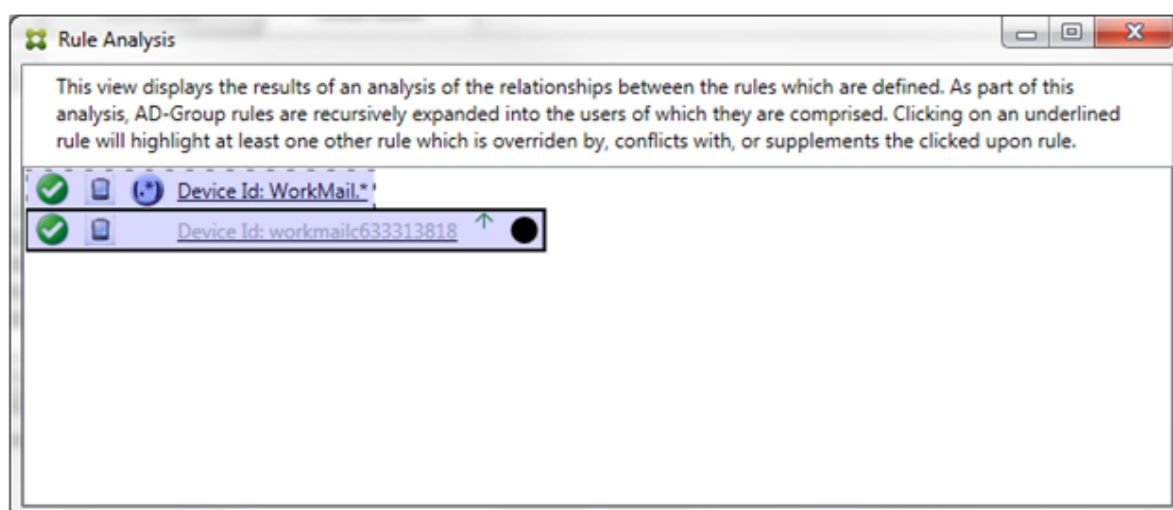
When an override occurs, at least two rules will be underlined: the primary rule and the ancillary rule or rules. At least one ancillary rule appears in a lighter font to indicate that the rule has been overridden by a higher priority rule. You can click the overridden rule to find out which rule or rules have overridden the rule. Anytime an overridden rule has been highlighted either as a result of the rule being the primary or ancillary rule, a black circle appears next to it as a further visual indication that the rule is inactive. For example, before clicking the rule, the dialog box appears as follows:



When you click the highest-priority rule, the dialog box appears as follows:

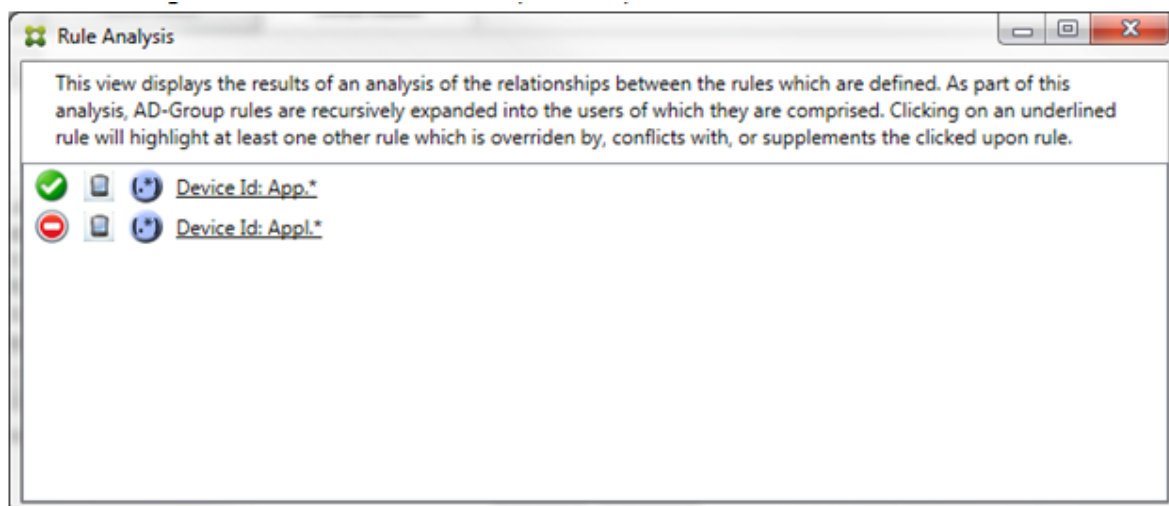


In this example, the regular expression rule `WorkMail.*` is the primary rule (indicated by the solid border) and the normal rule `workmailc633313818` is an ancillary rule (indicated by the dashed border). The black dot next to the ancillary rule is a visual cue that further indicates that the rule is inactive (will never be evaluated) due to the higher-priority regular expression rule that precedes it. After clicking the overridden rule, the dialog box appears as follows:



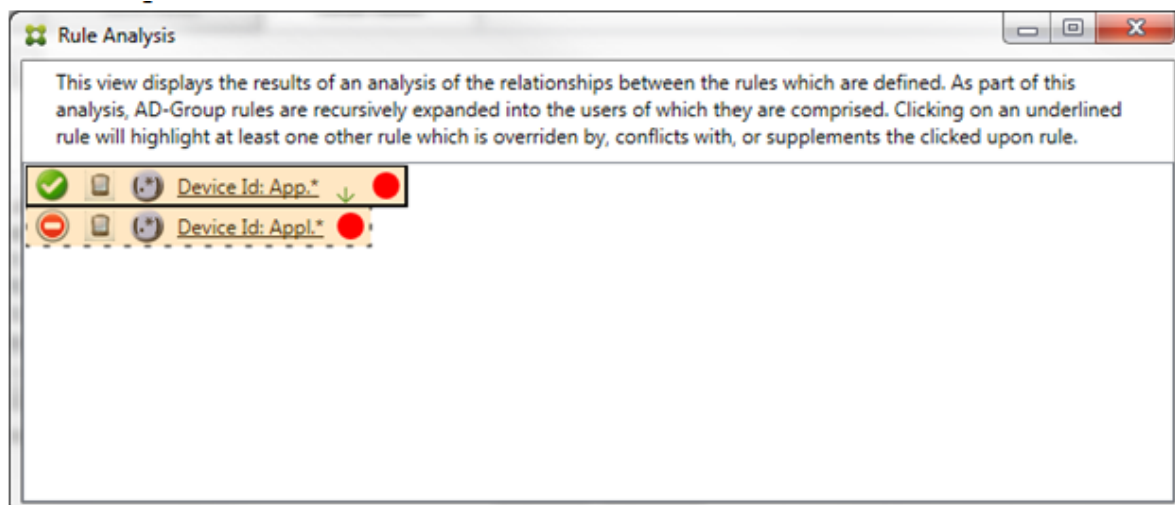
In the preceding example, the regular expression rule `WorkMail.*` is the ancillary rule (indicated by the dashed border) and the normal rule `workmailc633313818` is a primary rule (indicated by the solid border). For this simple example, there's not much difference. For a more complicated example, see the complex expression example later in this topic. In a scenario with many rules defined, clicking the overridden rule would quickly identify which rule or rules had overridden it.

When a conflict occurs, at least two rules will be underlined, the primary rule and the ancillary rule or rules. The rules in conflict are indicated by a red dot. Rules that only conflict with one another are only possible with two or more regular expression rules defined. In all other conflict scenarios, there will not only be a conflict, but an override at play. Prior to clicking either of the rules in a simple example, the dialog box appears as follows:



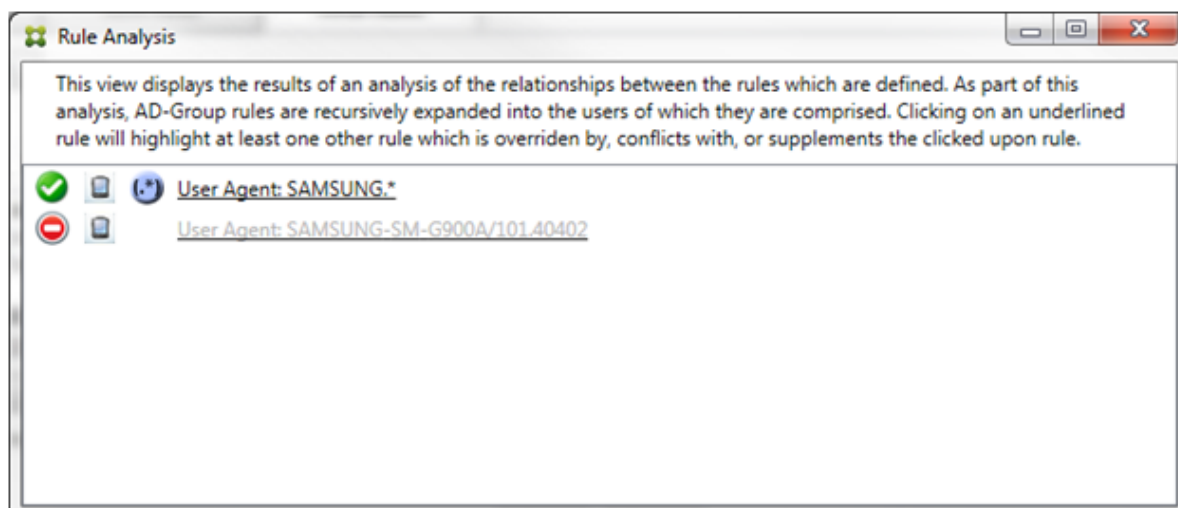
By inspecting the two regular expression rules, it's evident that the first rule allows all devices with a device ID that contains "App" and that the second rule denies all devices with a device ID that contains `AppL`. In addition, even though the second rule denies all devices with a device ID that contains `AppL`, no devices with that match criteria will ever be denied because of the higher precedence of the allow

rule. After clicking the first rule, the dialog box appears as follows:



In the preceding scenario, both the primary rule (regular expression rule `App . *`) and the ancillary rule (regular expression rule `AppL . *`) are both highlighted in yellow. This is simply a visual warning to alert you to the fact that you have applied more than a single regular expression rule to a single matchable field, which could mean a redundancy issue or something more serious.

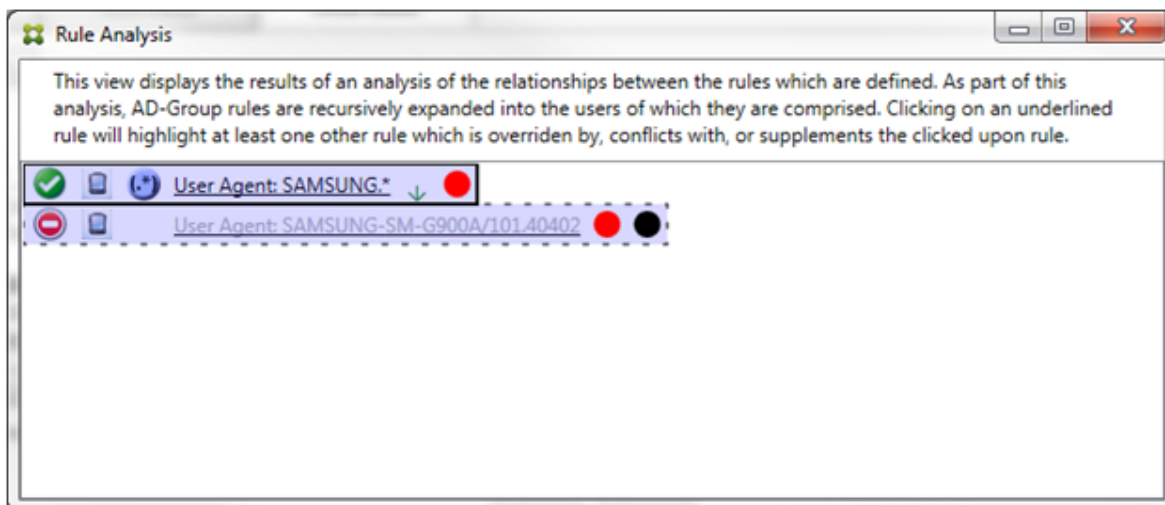
In a scenario with both a conflict and override, both the primary rule (regular expression rule `App . *`) and the ancillary rule (regular expression rule `AppL . *`) are highlighted in yellow. This is simply a visual warning to alert you to the fact that you have applied more than a single regular expression rule to a single matchable field, which could mean a redundancy issue or something more serious.



It is easy to see in the preceding example that the first rule (regular expression rule `SAMSUNG . *`) not only overrides the next rule (normal rule `SAMSUNG-SM-G900A/101.40402`), but that the two rules differ in their access (primary specifies Allow, ancillary specifies Block). The second rule (normal rule `SAMSUNG-SM-G900A/101.40402`) is displayed in lighter text to indicate that it has been overridden

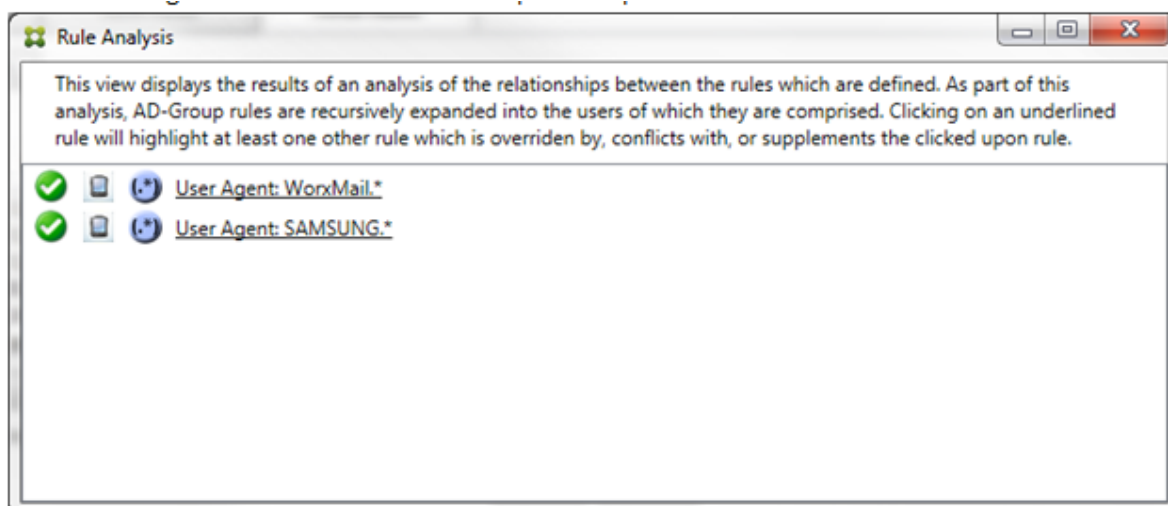
and is therefore inactive.

After clicking the regular expression rule, the dialog box appears as follows:

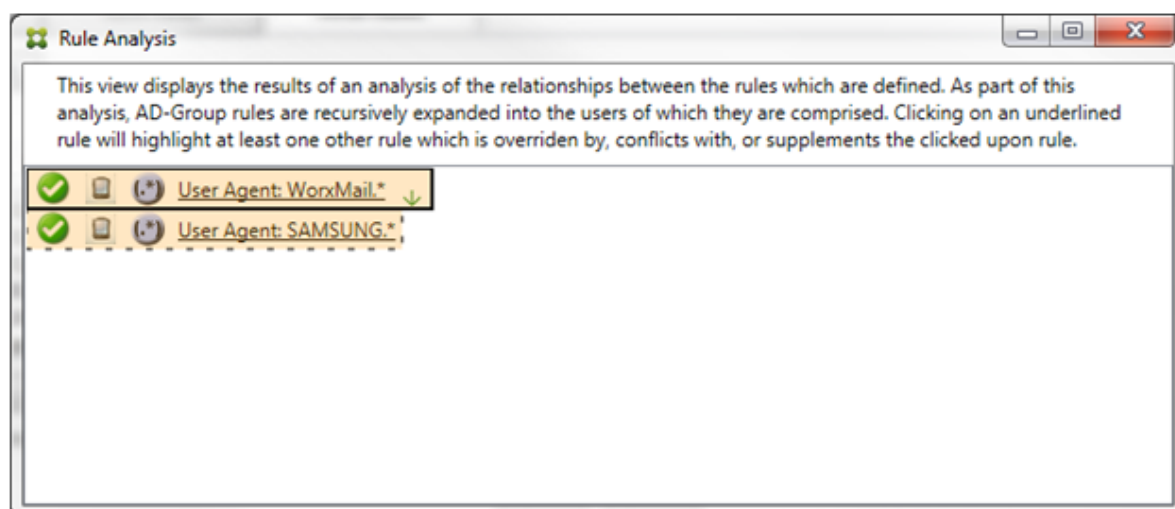


The primary rule (regular expression rule `SAMSUNG.*`) is followed by a red dot to indicate that its access state conflicts with one or more ancillary rules. The ancillary rule (normal rule `SAMSUNG-SM-G900A/101.40402`) is followed by a red dot to indicate that its access state conflicts with the primary rule. That rule is also followed by a black dot to indicate that it is overridden and therefore inactive.

At least two rules will be underlined, the primary rule and the ancillary rule or rules. Rules that only supplement one another will only involve regular expression rules. When the rules supplement one another, they are indicated with a yellow overlay. Prior to clicking either of the rules, in a simple example, the dialog box appears as follows:




Visual inspection easily reveals that both rules are regular expression rules which have both been applied to the ActiveSync device ID field in Endpoint Management connector for Exchange ActiveSync. After clicking the first rule, the dialog box looks as follows:



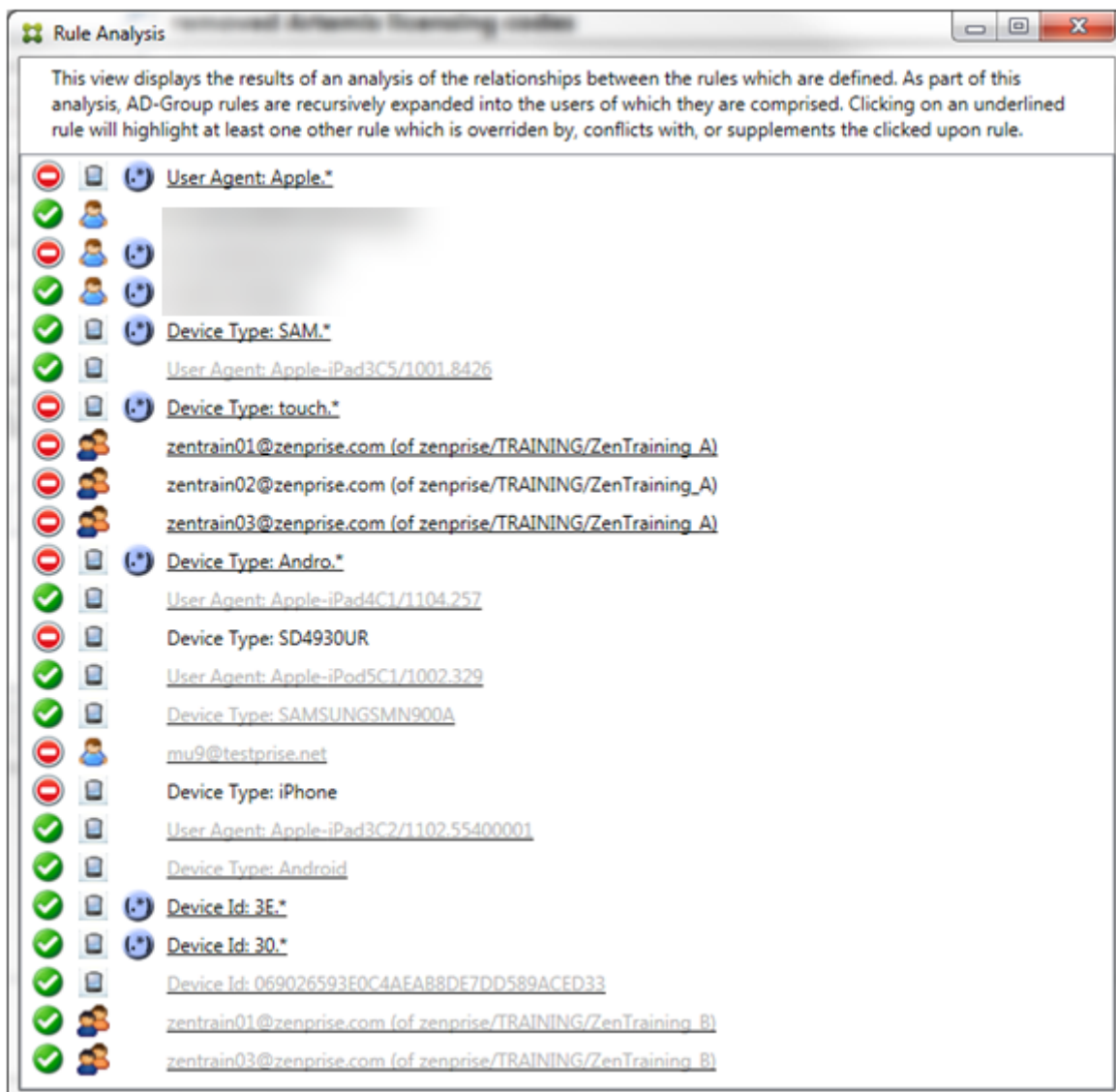
The primary rule (regular expression rule `WorkMail.*`) is highlighted with a yellow overlay to indicate that there exists at least one more ancillary rule which is a regular expression. The ancillary rule (regular expression rule `SAMSUNG.*`) is highlighted with a yellow overlay to indicate that both it and the primary rule are regular expression rules being applied to the same field within the connector for Exchange ActiveSync. In this case, that field is the ActiveSync device ID. The regular expressions may or may not overlap. It is up to you to decide if your regular expressions are properly crafted.

### Example of a complex expression

Many potential overrides, conflicts, or supplements can occur, making it impossible to give an example of all possible scenarios. The following example discusses what not to do, while also serving to illustrate the full power of the rule analysis visual construct. Most of the items are underlined in the following figure. Many of the items render in a lighter font, which indicates that the rule in question has been overridden by a higher priority rule in some manner. A number of regular expression rules

are included in the list as well, as indicated by the  icon.

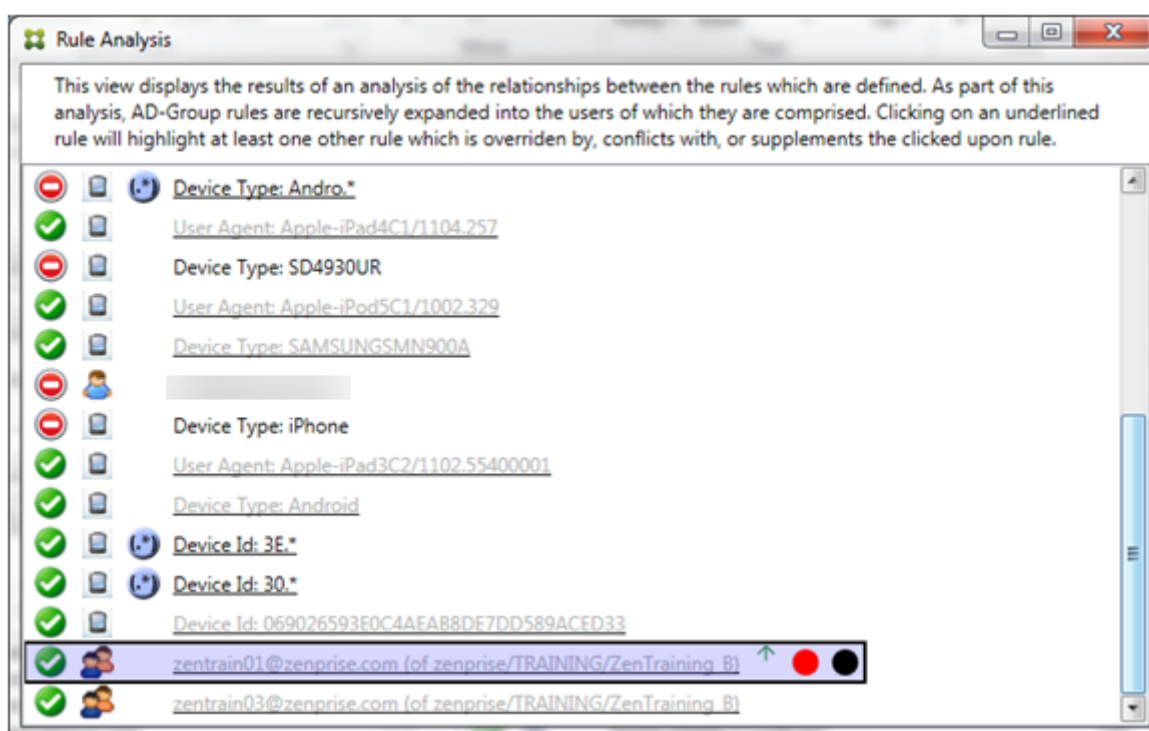




### How to analyze an override

To see which rule or rules have overridden a particular rule, you click the rule.

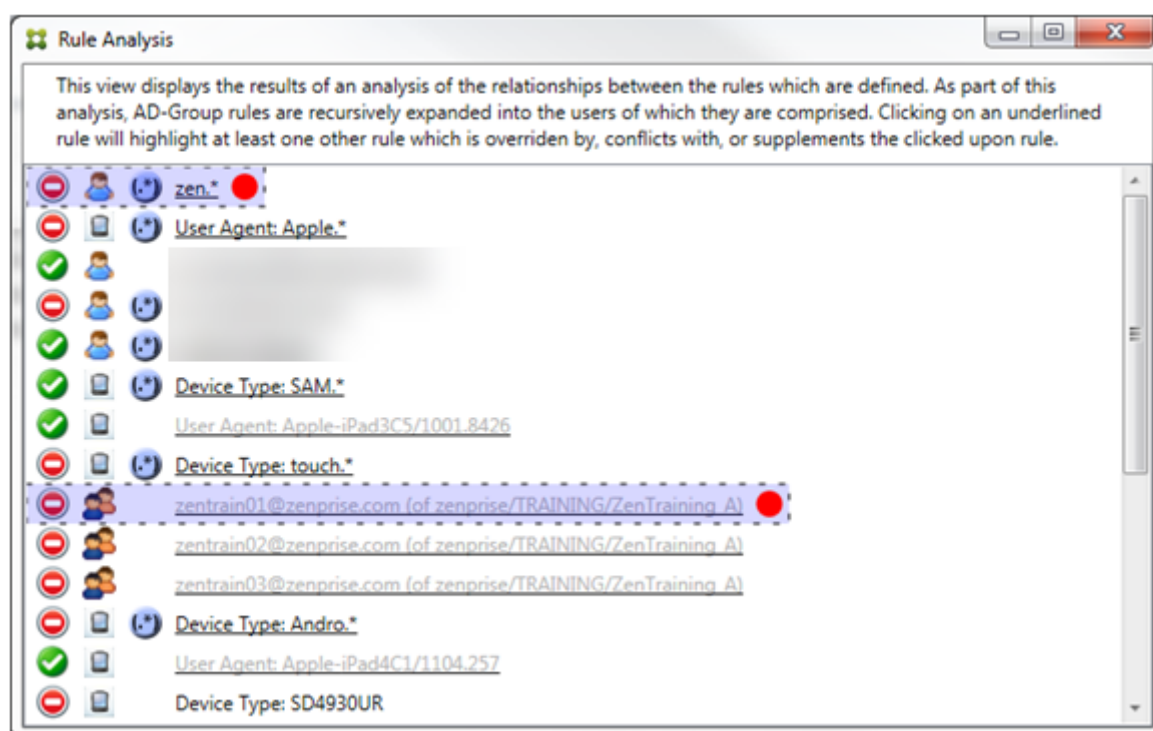
**Example 1:** This example examines why [zentrain01@zenprise.com](mailto:zentrain01@zenprise.com) has been overridden.



The primary rule (AD-Group rule `zenpraise/TRAINING/ZenTraining B`, of which `zentrain01@zenpraise.com` is a member) has the following characteristics:

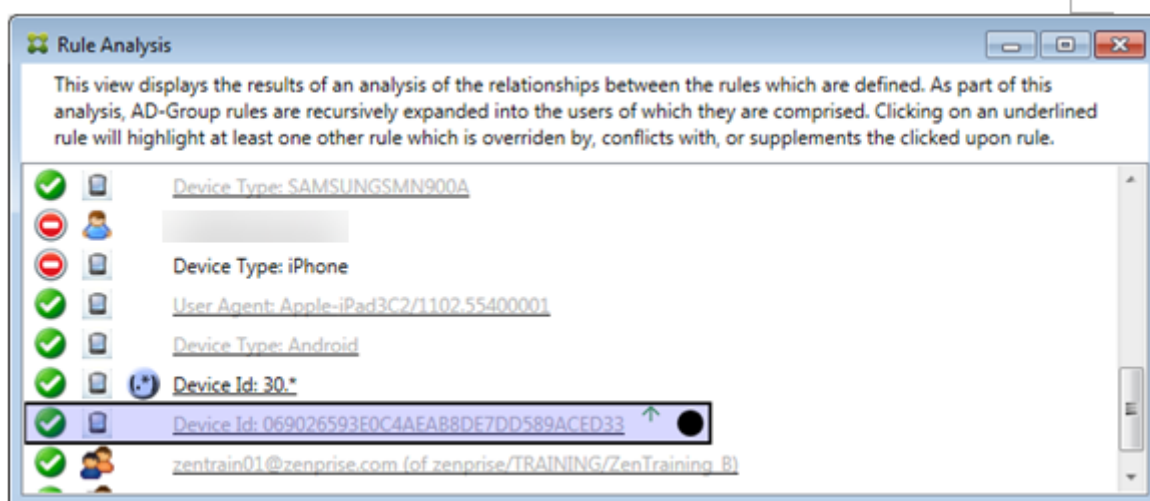
- Is highlighted in blue and has a solid border.
- Has an upwards pointing green arrow (to indicate that the ancillary rule or rules are all to be found above it).
- Is followed by both a red circle and black circle to indicate respectively that one or more ancillary rule conflicts with its access and that the primary rule has been overridden and is hence inactive.

When you scroll up, you see the following:



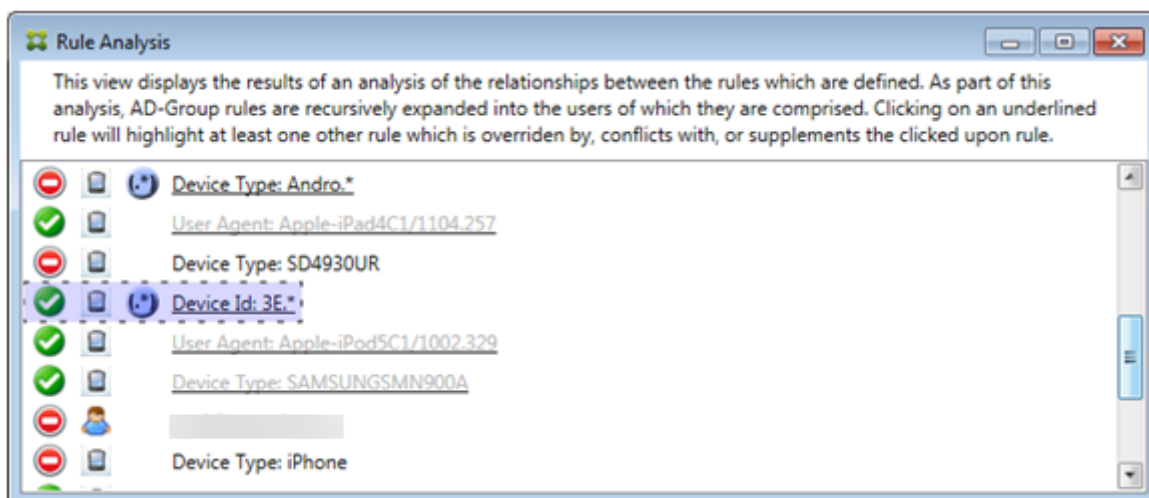
In this case, there are two ancillary rules that override the primary rule: the regular expression rule `zen.*` and the normal rule `zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining A)`. In the case of the latter ancillary rule, what has occurred is that the Active Directory Group rule `ZenTraining A` contains the user `zentrain01@zenprise.com`, and the Active Directory Group rule `ZenTraining B` also contains the user `zentrain01@zenprise.com`. Because the ancillary rule has a higher precedence than the primary rule, however, the primary rule has been overridden. The primary rule's access is Allow, and because both of the ancillary rule's access is Block, all are followed with a red circle to further indicate an access conflict.

**Example 2:** This example shows why the device with an ActiveSync device ID of `069026593E0C4AEAB8DE7DD589ACED33` has been overridden:



The primary rule (normal device ID rule 069026593E0C4AEAB8DE7DD589ACED33) has the following characteristics:

- Is highlighted in blue and has a solid border.
- Has an upwards pointing green arrow (to indicate that the ancillary rule is to be found above it).
- Is followed by a black circle to indicate an ancillary rule has overridden the primary rule and is hence inactive.

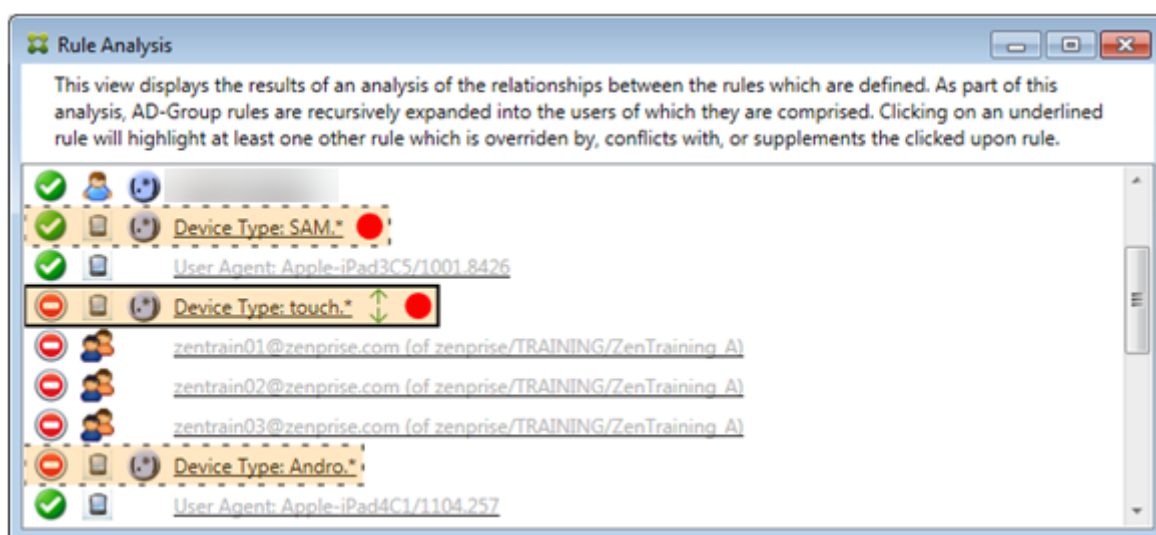


In this case, a single ancillary rule overrides the primary rule: The regular expression ActiveSync device ID rule is 3E.\* Because the regular expression 3E.\* would match 069026593E0C4AEAB8DE7DD589ACED33, the primary rule will never be evaluated.

### How to analyze a supplement and conflict

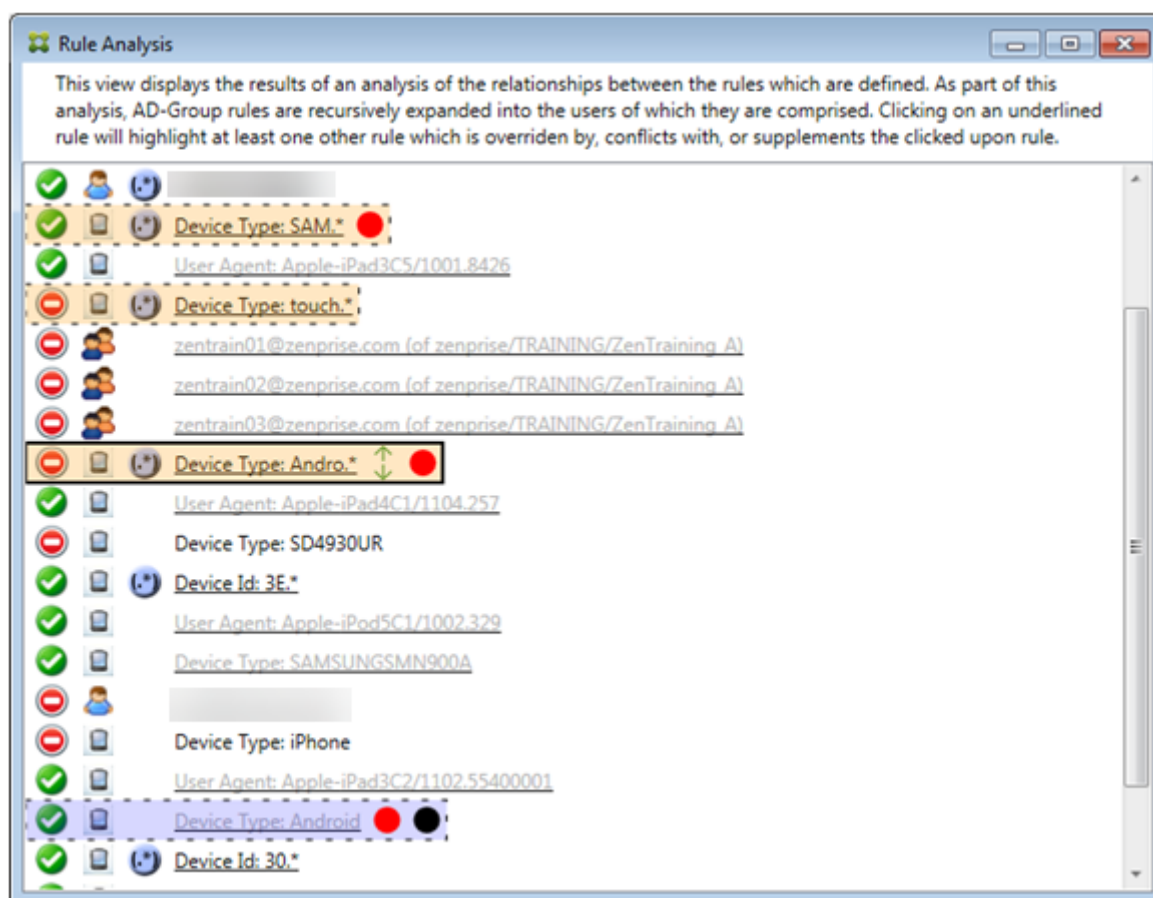
In this case, the primary rule is the regular expression ActiveSync device type rule touch.\* The characteristics are as follows:

- Is indicated by a solid border with a yellow overlay as a warning that there is more than a single regular expression rule operating against a particular rule field, in this case ActiveSync device type.
- Two arrows are pointing up and down respectively, indicating that there is at least one ancillary rule with higher priority and at least one ancillary rule with lower priority.
- The red circle next to it indicates that at least one ancillary rule has its access set to **Allow** which conflicts with the primary rule's access of **Block**
- There are two ancillary rules: the regular expression ActiveSync device type rule `SAM.*` and the regular expression ActiveSync device type rule `Andro.*`.
- Both of the ancillary rules are bordered with dashes to indicate that they are ancillary.
- Both of the ancillary rules are overlaid with yellow to indicate that they are also applied to the rule field of the ActiveSync device type.
- You should ensure in such scenarios that their regular expression rules are not redundant.



### How to further analyze the rules

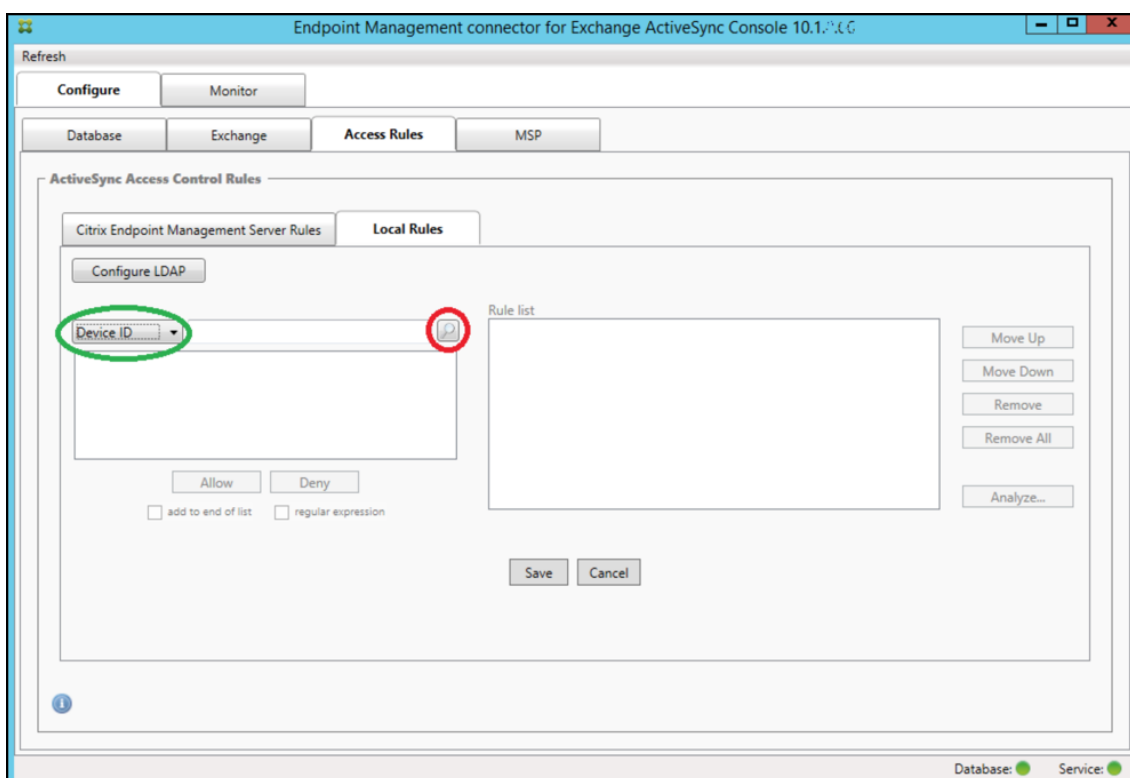
This example explores how rule relationships are always from the perspective of the primary rule. The preceding example showed how a click the regular expression rule applied to the rule field of device type with a value of `touch.*`. Clicking the ancillary rule `Andro.*` shows a different set of ancillary rules highlighted.



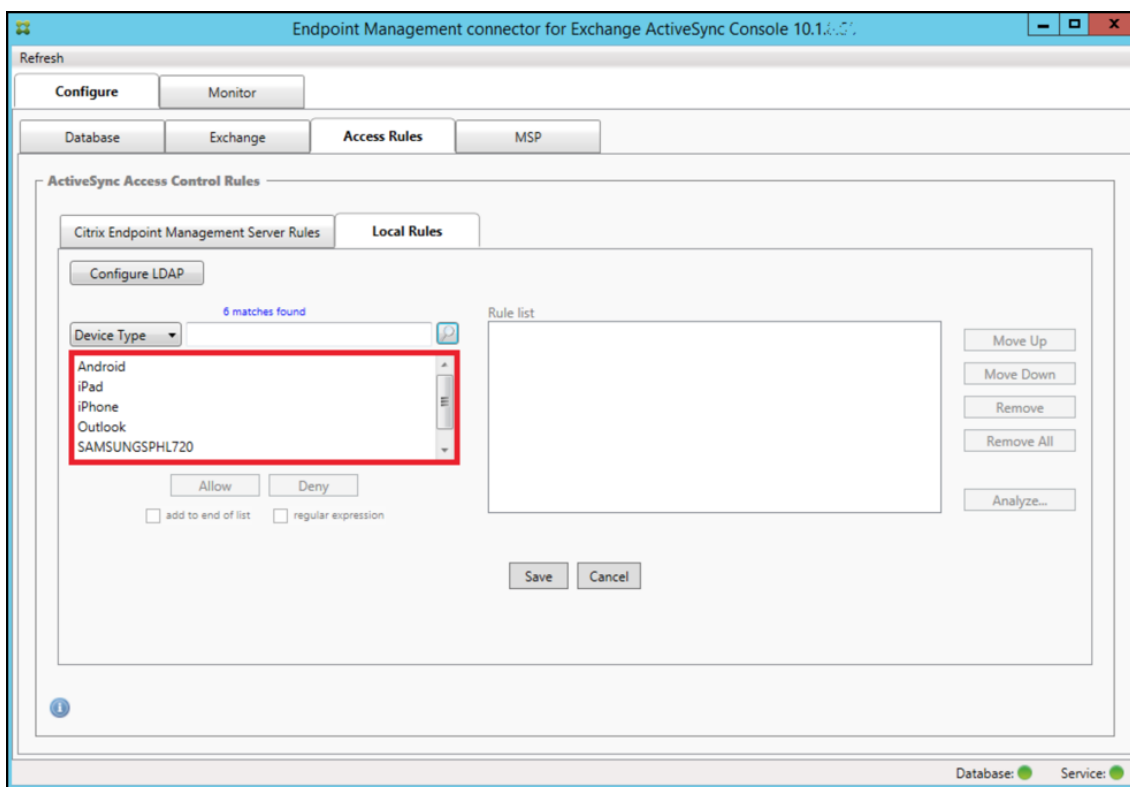
The example shows an overridden rule that is included in the rule relationship. This rule is the normal ActiveSync device type rule `Android`, which is overridden (indicated by the lightened font and the black circle next to it) and also conflicts in its access with the primary rule regular expression ActiveSync device type rule `Andro.*`. That rule was formerly an ancillary rule prior to being clicked. In the preceding example, the normal ActiveSync device type rule `Android`, was not displayed as an ancillary rule because, from the perspective of the then primary rule (the regular expression ActiveSync device type rule `touch.*`), it was not related to it.

### To configure a normal expression local rule

1. Click the **Access Rules** tab.



2. In the **Device ID** list, select the field for which you want to create a Local Rule.
3. Click the magnifying glass icon to display all of the unique matches for the chosen field. In this example, the field **Device Type** has been chosen and the choices are shown below in the list box.

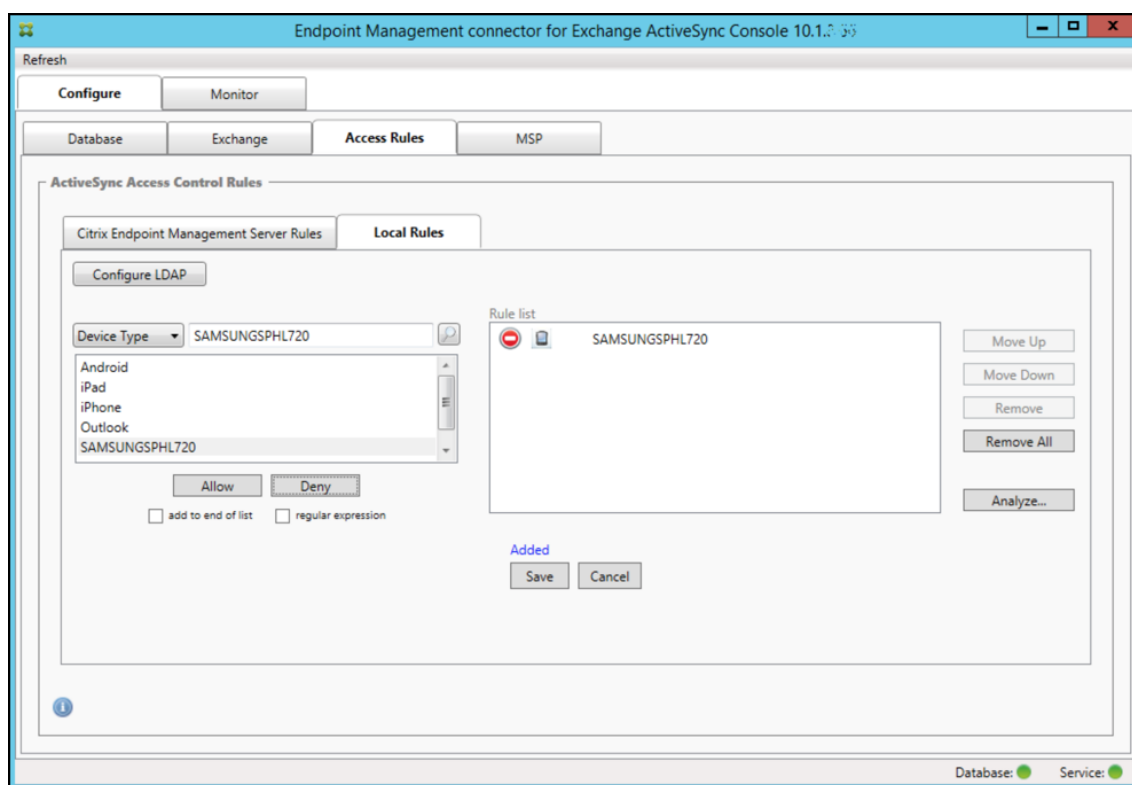


4. Click one of the items in the results list box and then click one of the following options:

- **Allow** means that Exchange will be configured to allow ActiveSync traffic for all matching devices.
- **Deny** means that Exchange will be configured to deny ActiveSync traffic for all matching devices.

In this example, all devices that have a device type of SamsungSPHL720 are denied access.





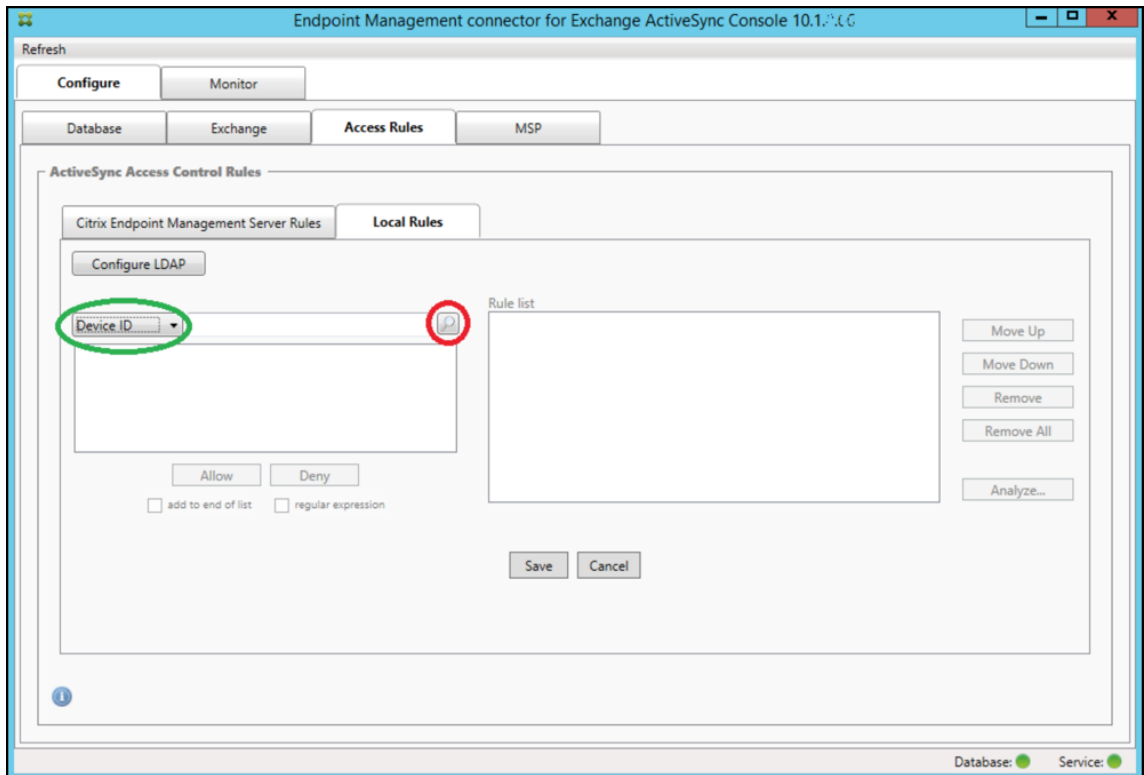
## To add a regular expression



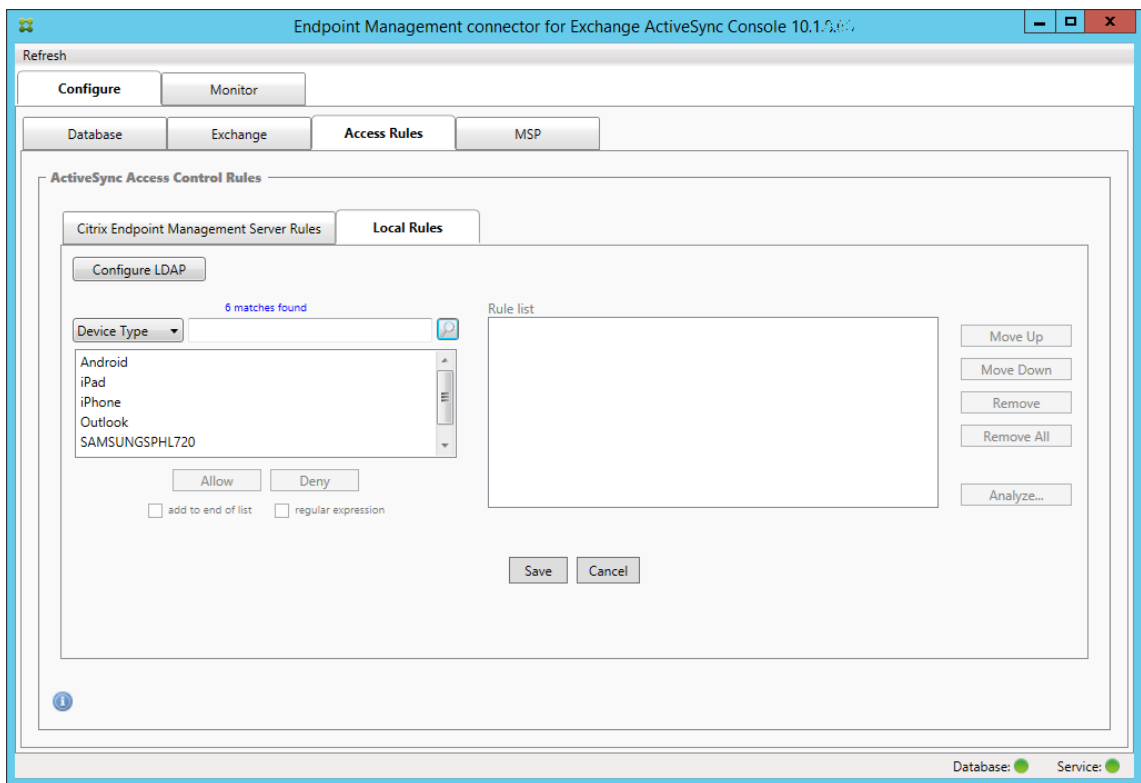
Regular expression local rules can be distinguished by the icon which appears next to them - . To add a regular expression rule, you can either build a regular expression rule from an existing value from the results list for a given field (as long as a major snapshot has completed), or you can simply type in the regular expression that you want.

## To build a regular expression from an existing field value

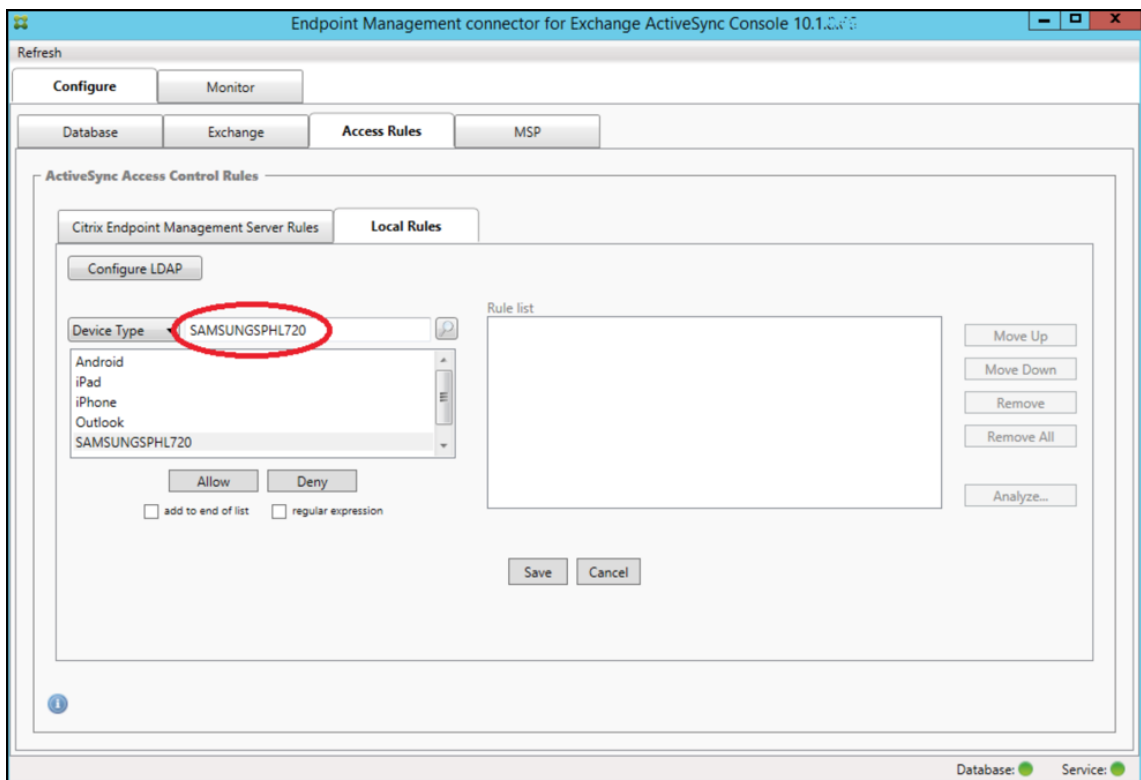
1. Click the **Access Rules** tab.



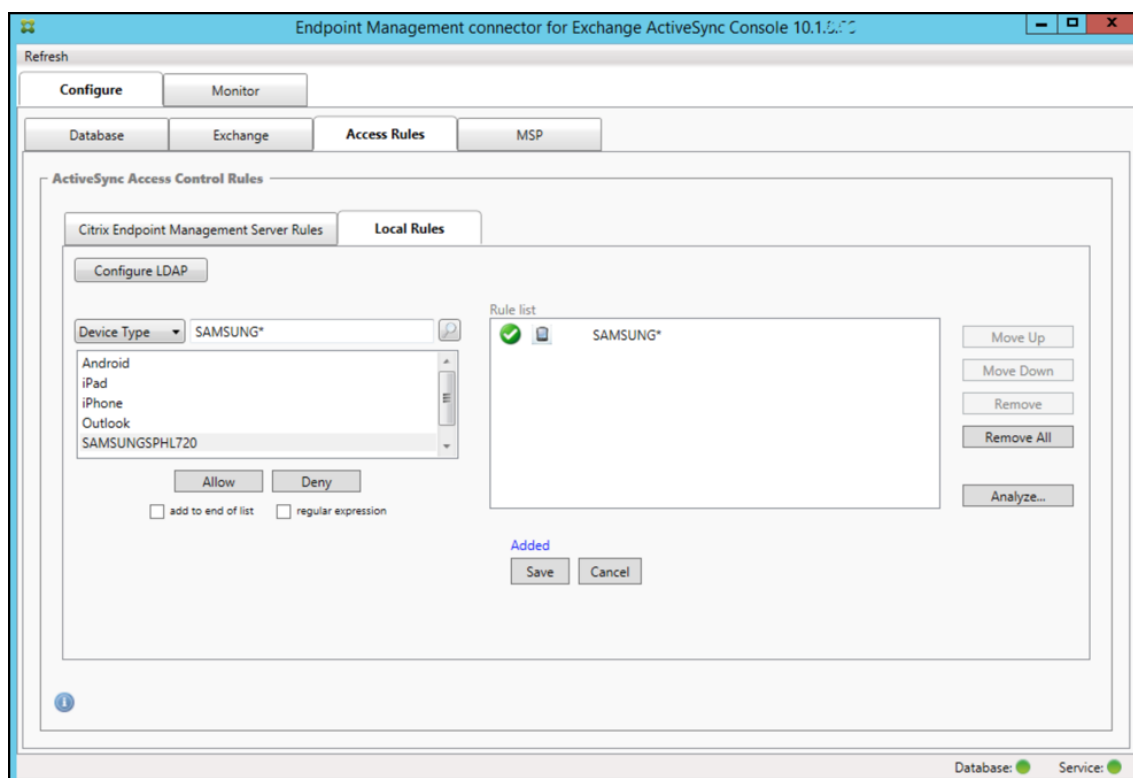
2. In the **Device ID** list, select the field for which you want to create a regular expression Local Rule.
3. Click the magnifying glass icon to display all of the unique matches for the chosen field. In this example, the field **Device Type** has been chosen and the choices are shown below in the list box.



4. Click one of the items in the results list. In this example, **SAMSUNGSPHL720** has been selected and appears in the text box adjacent to **Device Type**.

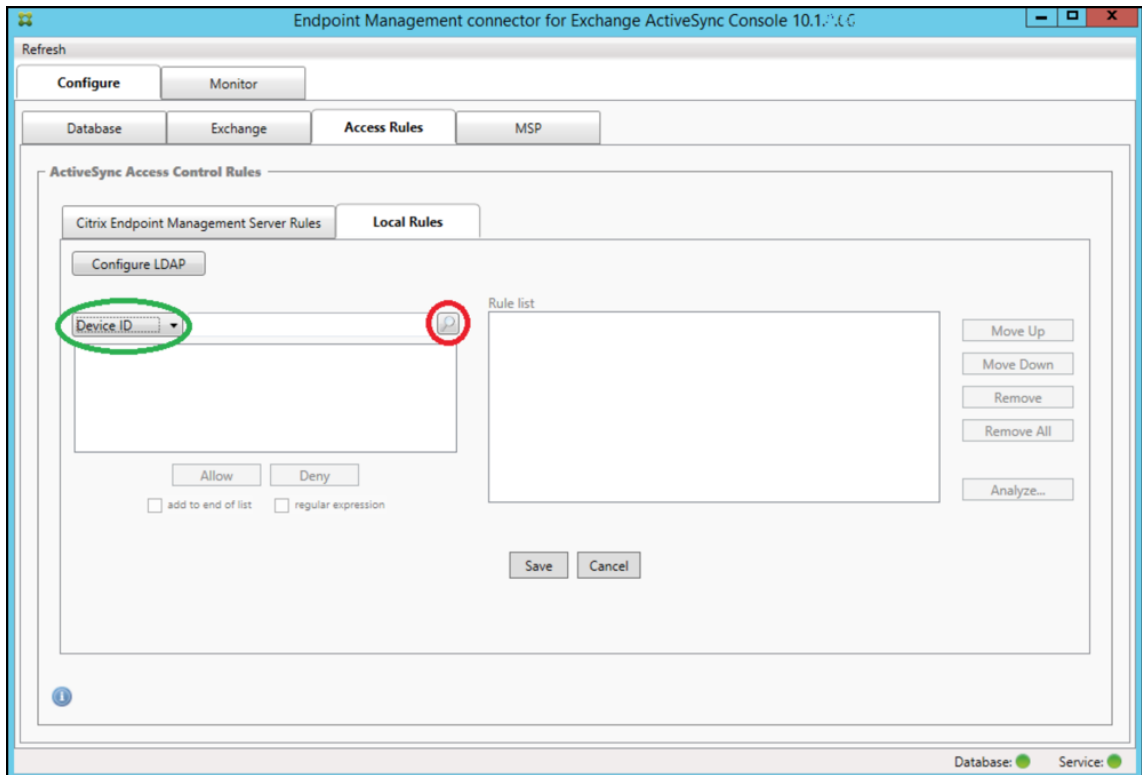


5. To allow all device types that have “Samsung” in their device type value, add a regular expression rule by following these steps:
  - a. Click within the selected item text box.
  - b. Change the text from **SAMSUNGSPHL720** to **SAMSUNG\***.
  - c. Ensure that the regular expression check box is selected.
  - d. Click **Allow**.

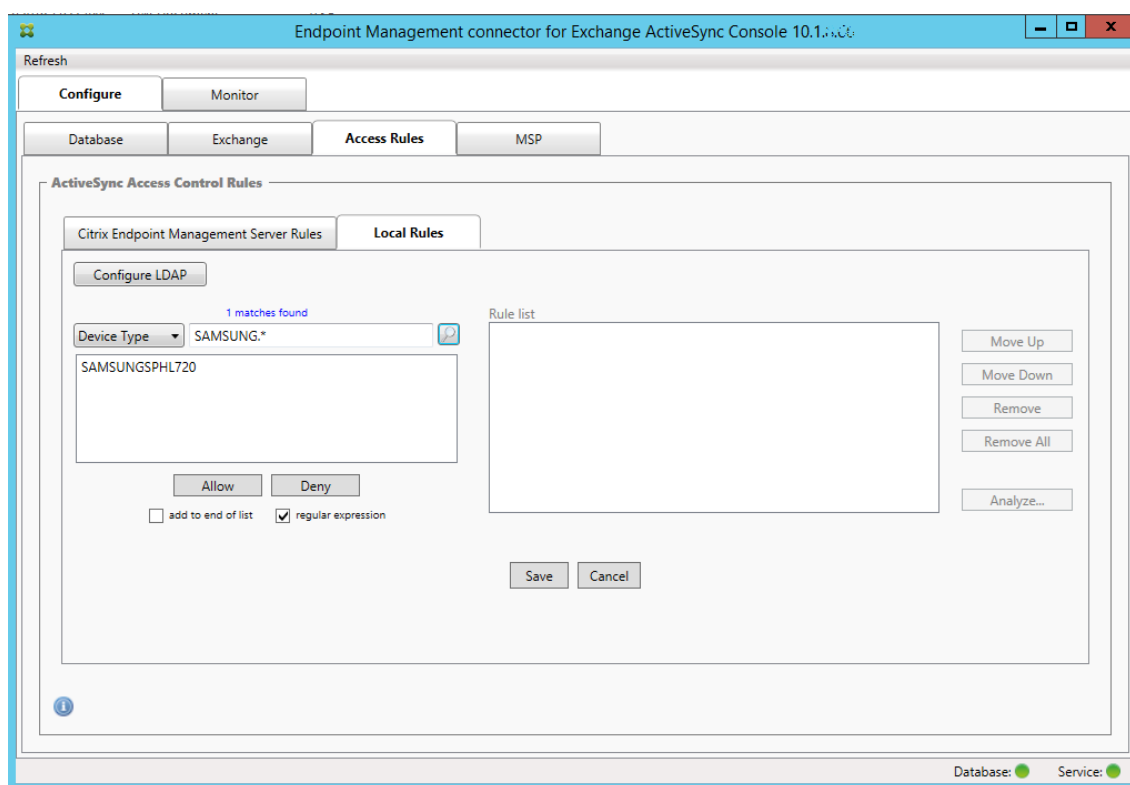


## To build an access rule

1. Click the **Local Rules** tab.
2. To enter the regular expression, you need to make use of both the Device ID list and the selected item text box.



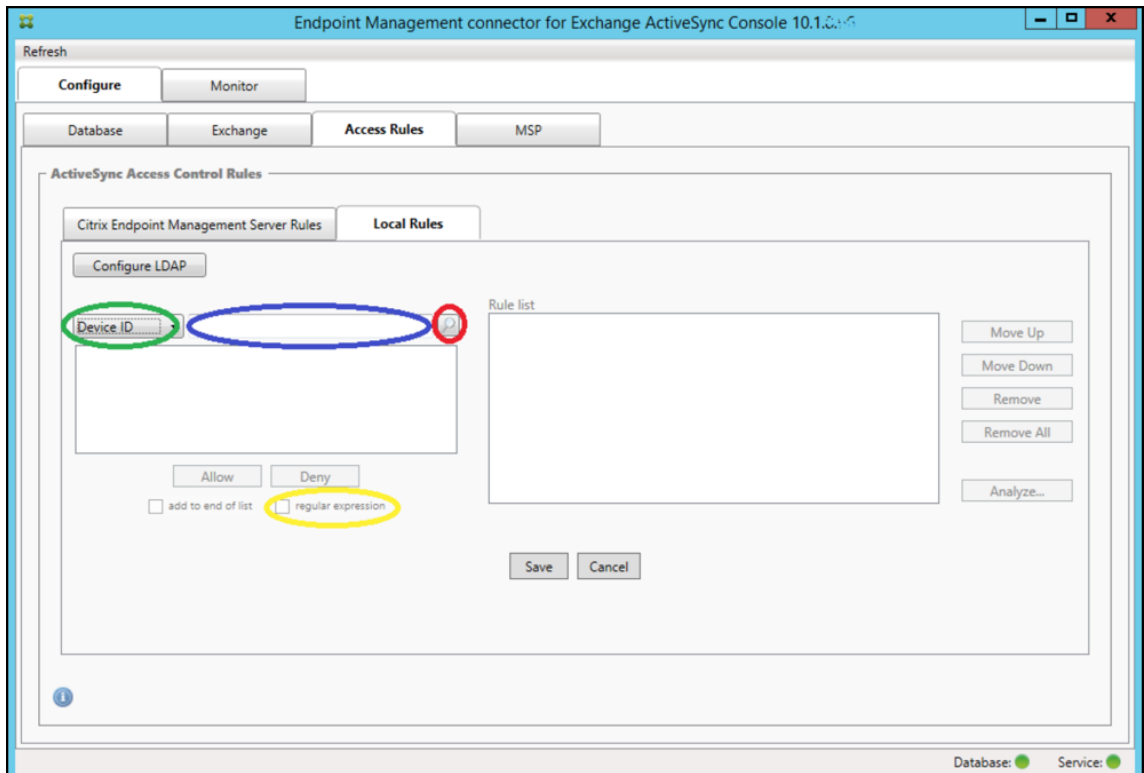
3. Select the field you want to match against. This example uses **Device Type**.
4. Type in the regular expression. This example uses `samsung.*`
5. Ensure that the regular expression check box is selected and then click **Allow** or **Deny**. In this example, the choice is **Allow**. The final result is as follows:



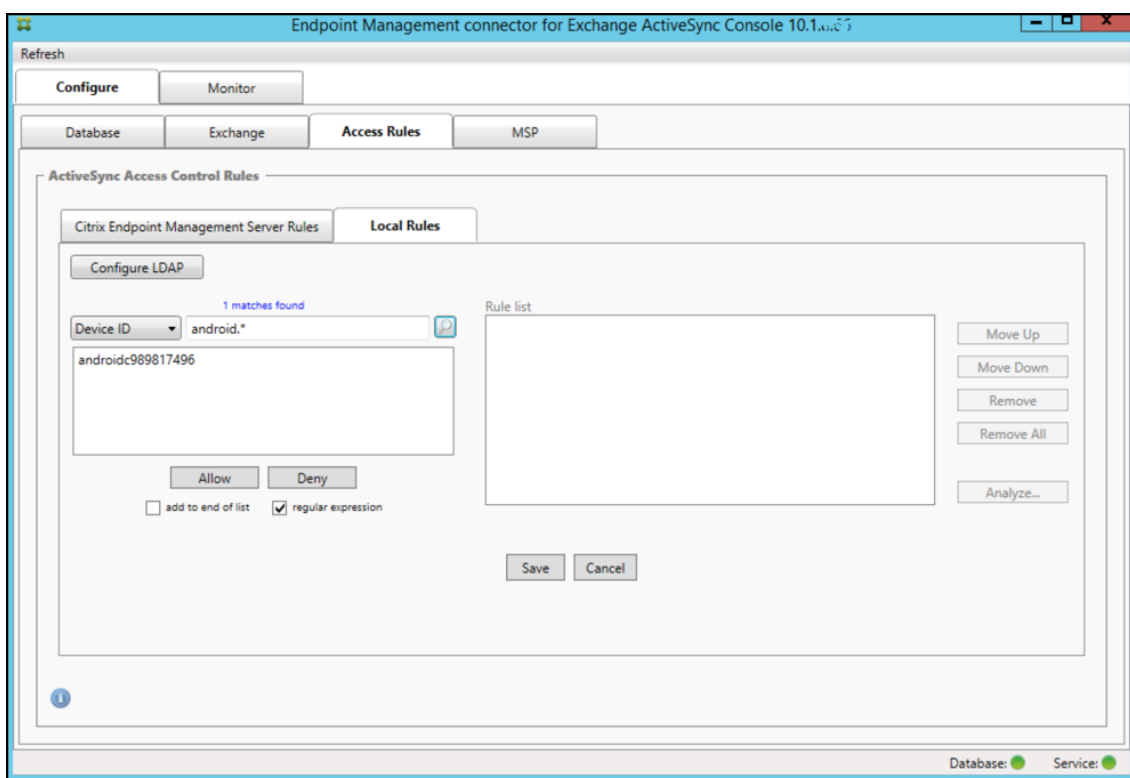
### To find devices

By selecting the regular expression check box, you can run searches for specific devices that match the given expression. This feature is only available if a major snapshot has successfully completed. You can use this feature even if there is no plan to use regular expression rules. For example, assume that you want to find all devices that have the text `workmail` in their ActiveSync device ID. To do so, follow this procedure.

1. Click the **Access Rules** tab.
2. Ensure that the device match field selector is set to Device ID (the default).



3. Click within the selected item text box (as shown in blue in the preceding figure) and then type `workmail.*`.
4. Ensure the regular expression check box is selected and then click the magnifying glass icon to display the matches as shown in the following figure.



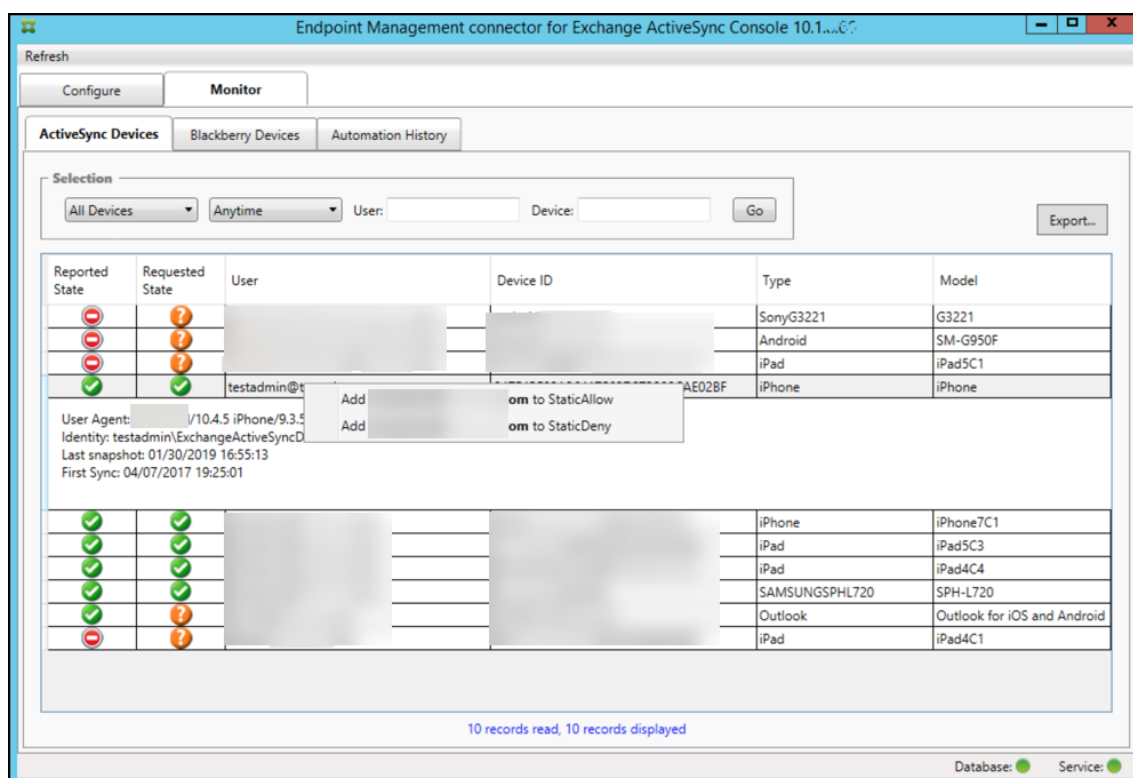
### To add an individual user, device, or device type to a static rule

You can add static rules based on user, device ID, or device type on the ActiveSync Devices tab.

1. Click the **ActiveSync Devices** tab.
2. In the list, right-click a user, device, or device type and select whether to allow or deny your selection.

The following image shows the Allow/Deny option when user1 is selected.





## Device monitoring

The **Monitor** tab in Endpoint Management connector for Exchange ActiveSync lets you browse the Exchange ActiveSync and BlackBerry devices that have been detected and the history of automated PowerShell commands that have been issued. The **Monitor** tab has the following three tabs:

- **ActiveSync Devices:**
  - You can export the displayed ActiveSync device partnerships by clicking the **Export** button.
  - You can add Local (static) rules by right-clicking the **User**, **Device ID**, or **Type** columns and selecting the appropriate allow or block rule type.
  - To collapse an expanded row, Ctrl-click the expanded row.
- **Blackberry Devices**
- **Automation History**

The **Configure** tab shows the history of all snapshots. Snapshot history shows when the snapshot took place, how long it took, how many devices were detected and any errors that occurred:

- On the **Exchange** tab, click the Info icon for the desired Exchange Server.
- Under the **MSP** tab, click the Info icon for the desired BlackBerry Server.

## Troubleshooting and diagnostics

Endpoint Management connector for Exchange ActiveSync logs errors and other operational information to its log file: *Install Folder*\log\XmmWindowsService.log. The connector for Exchange ActiveSync also logs significant events to the Windows Event Log.

### To change the logging level

Endpoint Management connector for Exchange ActiveSync includes the following logging levels: Error, Info, Warn, Debug, and Trace.

**Note:**

Each successive level generates more detail (more data). For example, the Error level provides the least detail, whereas the Trace level provides the most detail.

To change the logging level, do the following:

1. In `C:\Program Files\Citrix\Citrix Endpoint Management connector`, open the `nlog.config` file.
2. In the `<rules>` section, change the `minlevel` parameter to the logging level you prefer. For example:

```
1 <rules >
2
3 <logger name="*" writeTo="file" minlevel="Debug" />
4
5 </rules>
6 <!--NeedCopy-->
```

3. Save the file.

The changes take effect immediately. You don't need to restart the connector for Exchange ActiveSync.

### Common errors

The following list includes common errors:

- The connector for Exchange ActiveSync service doesn't start

Check the log file and the Windows Event Log for errors. Typical causes are as follows:

- The connector for Exchange ActiveSync service cannot access the SQL Server. This may be caused by these issues:
  - \* The SQL Server service is not running.

- \* Authentication failure.

If Windows Integrated authentication is configured, the user account of the connector for Exchange ActiveSync service must be an allowed SQL logon. The account of the connector for Exchange ActiveSync service defaults to Local System, but may be changed to any account that has local administrator privileges. If SQL authentication is configured, the SQL logon must be properly configured in SQL.

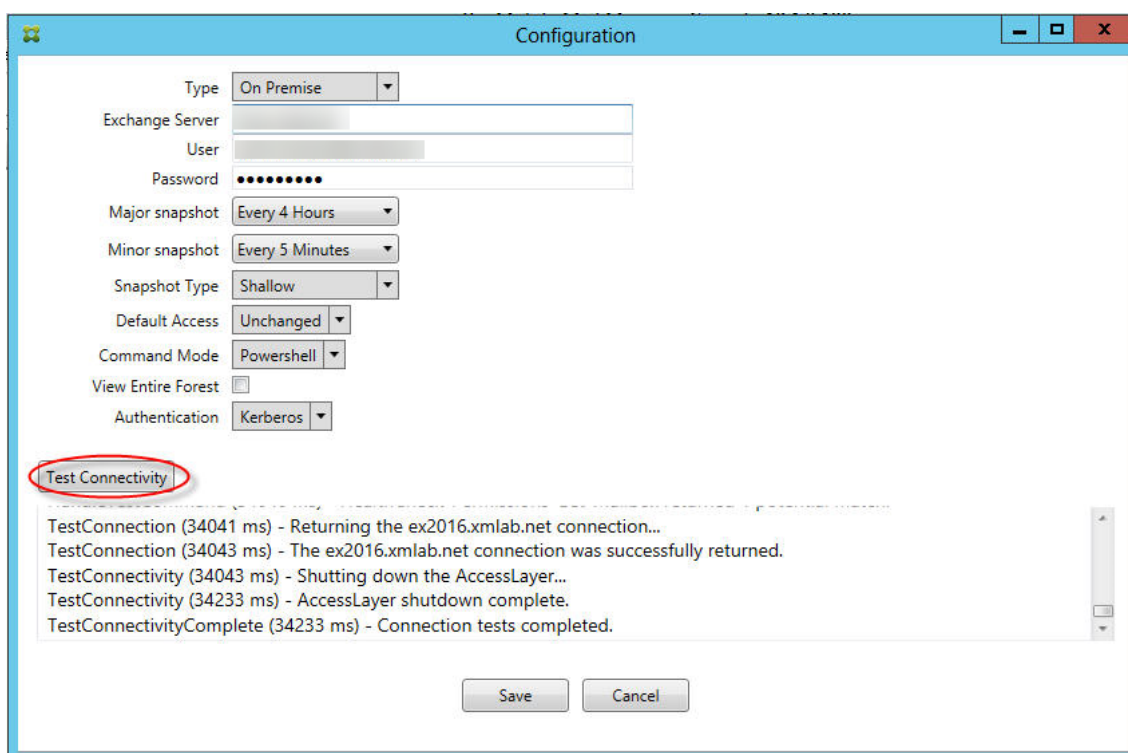
- The port configured for the Mobile Service Provider (MSP) is not available. A listening port must be selected that is not used by another process on the system.
- Endpoint Management cannot connect to the MSP

Check that the MSP service port and transport is properly configured in the **Configure > MSP** tab of the connector for Exchange ActiveSync console. Check that the Authorization Group or User is set properly.

If HTTPS is configured, a valid SSL server certificate must be installed. If IIS is installed, the IIS Manager can be used to install the certificate. For details on installing certificates if IIS is not installed, see [How to: Configure a Port with an SSL Certificate](#).

The connector for Exchange ActiveSyncr contains a utility program to test connectivity to the MSP service. Run the *InstallFolder\MspTestServiceClient.exe* program and set the URL and credentials to a URL and credentials that will be configured in the Endpoint Management and then click **Test Connectivity**. This simulates the web service requests that Endpoint Management issues. If HTTPS is configured, you must specify the actual host name of the server (the name specified in the SSL certificate).

When using **Test Connectivity**, be sure to have at least one ActiveSyncDevice record or the test may fail.



### Troubleshooting tools

A set of PowerShell utilities for troubleshooting is available in the Support\PowerShell folder.

A troubleshooting tool performs in-depth analysis of user mailboxes and devices, detecting error conditions and potential areas of failure, and in-depth RBAC analysis of users. It can save a raw output of all cmdlets to a text file.

### Citrix Gateway connector for Exchange ActiveSync

February 16, 2021

XenMobile NetScaler Connector is now the Citrix Gateway connector for Exchange ActiveSync. For more detail about the Citrix unified portfolio, see the [Citrix product guide](#).

The connector for Exchange ActiveSync provides a device-level authorization service of ActiveSync clients to Citrix Gateway acting as a reverse proxy for the Exchange ActiveSync protocol. You control authorization through a combination of:

- Policies that you define in Endpoint Management
- Rules defined locally by the Citrix Gateway connector for Exchange ActiveSync

For more information, see [ActiveSync Gateway](#).

For a detailed reference architecture diagram, see [Architecture](#).

The current release of the Citrix Gateway connector for Exchange ActiveSync is version 8.5.3.

To download the connector:

1. Go to <https://www.citrix.com/downloads>.
2. Navigate to **Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10 > Server Components**.
3. On the **Citrix Gateway Connector** tile, click **Download File**.

To install the connector, see [Installing the Citrix Gateway connector for Exchange ActiveSync](#).

### What's new in version 8.5.3

- This release adds support for ActiveSync protocols 16.0 and 16.1.
- More detail has been added to the analytics sent to Google Analytics, especially concerning snapshots. [CXM-52261]

### What's new in earlier versions

#### Note:

The following What's new section refers to the Citrix Gateway connector for Exchange ActiveSync by its former name, XenMobile NetScaler Connector. The name changed as of version 8.5.2.

### What's new in version 8.5.2

- XenMobile NetScaler Connector is now the Citrix Gateway connector for Exchange ActiveSync.

The following issues are fixed in this release:

- If more than one criteria is used in defining a policy rule and if a criteria involves the user ID, the following issue can occur: If a user has more aliases, the aliases are not also checked when applying the rule. [CXM-55355]

### What's new in version 8.5.1.11

- **System requirement change:** The current version of NetScaler Connector requires Microsoft .NET Framework 4.5.
- **Google Analytics support:** We want to know how you use the Connector so we can focus on where we can make the product better.
- **Support for TLS 1.1 and 1.2:** Due to its weakening security, the PCI Council is deprecating TLS 1.0 and TLS 1.1. Support for TLS 1.2 is added to the XenMobile NetScaler Connector.

## Monitoring Citrix Gateway connector for Exchange ActiveSync

The Citrix Gateway connector for Exchange ActiveSync configuration utility provides detailed logging. Use the logs to view all traffic passing through your Exchange Server that the Secure Mobile Gateway either allows or blocks.

Use the **Log** tab to view the history of the ActiveSync requests forwarded to the connector for Exchange ActiveSync for authorization.

Also, to ensure that the connector for the Exchange ActiveSync web service is running, load the following URL into a browser on the connector server `https://<host:port>/services/ActiveSync/Version`. If the URL returns the product version as a string, the web service is responsive.

## To simulate ActiveSync traffic with the connector for Exchange ActiveSync

You can use the Citrix Gateway connector for Exchange ActiveSync to simulate ActiveSync traffic with your policies. In the connector configuration utility, click the **Simulator** tab. The results show how your policies apply according to the rules you configured.

## Choosing filters for the connector for Exchange ActiveSync

The Citrix Gateway connector for Exchange ActiveSync filters work by analyzing a device for a given policy violation or property setting. If the device meets the criteria, the device is placed in a Device List. This Device List is neither an allow list or a block list. It is a list of devices that meet the criteria defined. The following filters are available for the connector for Exchange ActiveSync within Endpoint Management. The two options for each filter are **Allow** or **Deny**.

- **Anonymous Devices:** Allows or denies devices that are enrolled in Endpoint Management but the user's identity is unknown. For example, an enrolled user has an unknown identity if the user has an expired Active Directory password or unknown credentials.
- **Failed Samsung Knox attestation:** Samsung devices have functionality for security and diagnostics. This filter provides confirmation that the device is configured for Knox. For details, see the Endpoint Management article on [Samsung Knox](#).
- **Forbidden Apps:** Allows or denies devices based on the Device List defined by block lists in policies and the presence of apps on a block list.
- **Implicit Allow/Deny:** Creates a Device List of all devices that do not meet any of the other filter rule criteria and allows or denies based on that list. The Implicit Allow/Deny option ensures that the connector for Exchange ActiveSync status in the Devices tab is enabled and shows the connector status for your devices. The Implicit Allow/Deny option also controls all other connector filters that aren't selected. For example, the connector denies apps on the block list. However, the connector allows all other filters because the Implicit Allow/Deny option is set to **Allow**.

- **Inactive devices:** Creates a Device List of devices that have not communicated with Endpoint Management within a specified time. These devices are considered inactive. The filter allows or denies the devices accordingly.
- **Missing required apps:** When a user enrolls, the user receives a list of required apps that must be installed. The missing required apps filter indicates that one or more of the apps is no longer present; for example, the user deleted one or more apps.
- **Non-Suggested Apps:** When a user enrolls, the user receives a list of the apps to install. The non-suggested apps filter checks the device for apps that are not in that list.
- **Noncompliant password:** Creates a Device List of all devices that do not have a passcode on the device.
- **Out of Compliance Devices:** Allows you to deny or allow devices that meet your own internal IT compliance criteria. Compliance is an arbitrary setting defined by the device property named Out of Compliance, which is a Boolean flag that can be either **True** or **False**. (You can create this property manually and set the value. Or you can use automated actions to create this property on a device, based on whether the device meets specific criteria.)
  - **Out of Compliance = True:** If a device does not meet the compliance standards and policy definitions set by your IT department, the device is out of compliance.
  - **Out of Compliance = False:** If a device does meet the compliance standards and policy definitions set by your IT department, the device is compliant.
- **Revoked Status:** Creates a Device List of all revoked devices and allows or denies based on revoked status.
- **Rooted Android/Jailbroken iOS Devices:** Creates a Device List of all devices flagged as rooted and allows or denies based on rooted status.
- **Unmanaged Devices:** Creates a Device List of all devices in the Endpoint Management database. Deploy the Mobile Application Gateway in a Block Mode.

### To configure a connection to Citrix Gateway connector for Exchange ActiveSync

The Citrix Gateway connector for Exchange ActiveSync communicates with Endpoint Management and other remote configuration providers through secure web services.

1. In the connector for Exchange ActiveSync configuration utility, click the **Config Providers** tab and then click **Add**.
2. In the **Config Providers** dialog box, in **Name**, enter a user name that has administrative privileges and are used for basic HTTP authorization with the Endpoint Management server.
3. In **Url**, enter the web address of the Endpoint Management GCS, typically in the format `https://<FQDN>/<instanceName>/services/<MagConfigService>`. The *MagConfigService* name is case-sensitive.
4. In **Password**, enter the password to use for basic HTTP authorization with the Endpoint Management server.

5. In **Managing Host**, enter the connector for Exchange ActiveSync server name.
6. In **Baseline Interval**, specify a time period for when to pull a new refreshed dynamic ruleset from Endpoint Management.
7. In **Delta interval**, specify a time period for when to pull an update of the dynamic rules.
8. In **Request Timeout**, specify the server request timeout interval.
9. In **Config Provider**, select if the configuration provider server instance is providing the policy configuration.
10. In **Events Enabled**, enable this option if you want the connector for Exchange ActiveSync to notify Endpoint Management when a device is blocked. This option is required if you are using the connector rules in any of your Endpoint Management Automated Actions.
11. Click **Save** and then click **Test Connectivity** to test gateway-to-configuration provider connectivity. If the connection fails, check that the local firewall settings allow the connection or contact your administrator.
12. When the connection succeeds, clear the **Disabled** check box and then click **Save**.

When you add a configuration provider, the connector for Exchange ActiveSync automatically creates one or more policies associated with the provider. A template definition contained in `config\policyTemplates.xml` in the `NewPolicyTemplate` section defines the policies. For each Policy element defined within this section, a new policy is created.

The operator can add, remove, or modify policy elements if the following is true: The policy element conforms to the schema definition and the standard substitution strings (enclosed in braces) are not modified. Next, add new groups for the provider and update the policy to include the new groups.

### To import a policy from Endpoint Management

1. In the connector for Exchange ActiveSync configuration utility, click the **Config Providers** tab and then click **Add**.
2. In the **Config Providers** dialog box, in **Name**, enter a user name for basic HTTP authorization with Endpoint Management. The user must have administrative privileges.
3. In **Url**, enter the web address of the Endpoint Management Gateway Configuration Service (GCS), typically in the format `https://<xdmHost>/xdm/services/<MagConfigService>`. The `MagConfigService` name is case-sensitive.
4. In **Password**, enter the password that is used for basic HTTP authorization with the Endpoint Management server.
5. Click **Test Connectivity** to test gateway-to-configuration provider connectivity. If the connection fails, check that your local firewall settings allow the connection or check with your administrator.
6. When a connection is successfully made, clear the **Disabled** check box and then click **Save**.



7. In **Managing Host**, leave the default DNS name of the local host computer. This setting used to coordinate communication with Endpoint Management when multiple Forefront Threat Management Gateway (TMG) servers are configured in an array.

After you save the settings, open the GCS.

## Configuring Citrix Gateway connector for Exchange ActiveSync policy mode

The Citrix Gateway connector for Exchange ActiveSync can run in the following six modes:

- **Allow All:** This policy mode grants access for all traffic passing through the connector for Exchange ActiveSync. No other filtering rules are used.
- **Deny All:** This policy mode blocks access for all traffic passing through the connector for Exchange ActiveSync. No other filtering rules are used.
- **Static Rules: Block Mode:** This policy mode runs static rules with an implicit deny or block statement at the end. The connector for Exchange ActiveSync blocks devices that are not allowed or permitted via other filter rules.
- **Static Rules: Permit Mode:** This policy mode runs static rules with an implicit permit or allow statement at the end. Devices that are not blocked or denied via other filter rules are allowed through the connector for Exchange ActiveSync.
- **Static + ZDM Rules: Block Mode:** This policy mode runs static rules first, followed by dynamic rules from Endpoint Management with an implicit deny or block statement at the end. Devices are permitted or denied based on defined filters and Endpoint Management rules. Any devices that do not match on defined filters and rules are blocked.
- **Static + ZDM Rules: Permit Mode:** This policy mode runs static rules first, followed by dynamic rules from Endpoint Management with an implicit permit or allow statement at the end. Devices are permitted or denied based on defined filters and Endpoint Management rules. Any devices that do not match on defined filters and rules are allowed.

The connector for Exchange ActiveSync process permits or blocks for dynamic rules based on unique ActiveSync IDs for iOS and Windows-based mobile devices received from Endpoint Management. Android devices differ in their behavior based on the manufacturer and some do not readily expose a unique ActiveSync ID. To compensate, Endpoint Management sends user ID information for Android devices to make a permit or block decision. As a result, if a user has only one Android device, permits and blocks function normally. If the user has multiple Android devices, all the devices are allowed because Android devices cannot be differentiated. You can configure the gateway to statically block these devices by ActiveSyncID, if they are known. You can also configure the gateway to block based on device type or user agent.

To specify the policy mode, in the SMG Controller Configuration utility, do the following:

1. Click the **Path Filters** tab and then click **Add**.
2. In the **Path Properties** dialog box, select a policy mode from the **Policy** list and then click **Save**.

You can review the rules on the **Policies** tab of the configuration utility. The rules are processed on the connector for Exchange ActiveSync from top to bottom. The Allow policies are displayed with a green check mark. The Deny policies are shown as a red circle with a line through it. To refresh the screen and see the most updated rules, click **Refresh**. You can also modify the ordering of rules in the config.xml file.

To test the rules, click the **Simulator** tab. Specify values in the fields. You can get the values from the logs. A result message specifies Allow or Block.

### To configure static rules

Enter static rules with values that the ISAPI filtering of the ActiveSync connection HTTP requests reads. Static rules enable the connector for Exchange ActiveSync to permit or block traffic by the following criteria:

- **User:** The connector for Exchange ActiveSync uses the authorized user value and name structure that was captured during device enrollment. That structure is commonly found as `domain\username` as referenced by the server running Endpoint Management connected to Active Directory via LDAP. The **Log** tab in the connector configuration utility shows the values that pass through the connector. The values get passed if the connector must determine the value structure or if the structure differs.
- **DeviceID (ActiveSyncID):** Also known as the ActiveSyncID of the connected device. This value is commonly found within the specific device properties page in the Endpoint Management console. This value can also be screened from the **Log** tab in the connector for Exchange ActiveSync configuration utility.
- **DeviceType:** The connector for Exchange ActiveSync can determine if a device is an iPhone, iPad, or other device type and can permit or block based on that criteria. As with other values, the connector configuration utility can reveal all connected device types being processed for the ActiveSync connection.
- **UserAgent:** Contains information on the ActiveSync client that is used. Usually, the value specified corresponds to a specific operating system build and version for the mobile device platform.

The connector for Exchange ActiveSync configuration utility running on the server always manages the static rules.

1. In the SMG Controller Configuration utility, click the **Static Rules** tab and then click **Add**.
2. In the **Static Rule Properties** dialog box, specify the values that you want to use as criteria. For example, you can enter a user to allow access by entering the user name (for example, AllowedUser) and then clearing the **Disabled** check box.
3. Click **Save**.

The static rule is now in effect. Also, you can use regular expressions to define values, but you must enable the rule processing mode in the config.xml file.

### To configure dynamic rules

Device policies and properties in Endpoint Management define dynamic rules and can trigger a dynamic connector for Exchange ActiveSync filter. The triggers are based on the presence of a policy violation or property setting. The connector for Exchange ActiveSync filters work by analyzing a device for a given policy violation or property setting. If the device meets the criteria, the device is placed in a Device List. This Device List is not an allow list or a block list. It is a list of devices that meets the criteria defined. The following configuration options enable you to define whether you want to allow or deny the devices in the Device List by using the connector for Exchange ActiveSync.

#### Note:

Use the Endpoint Management console to configure dynamic rules.

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Server**, click **ActiveSync Gateway**. The ActiveSync Gateway page appears.
3. In **Activate the following rules**, select one or more rules you want to activate.
4. In Android-only, in **Send Android domain users to ActiveSync Gateway**, click **YES** to ensure that Endpoint Management sends Android device information to the Secure Mobile Gateway.

With this option enabled, Endpoint Management sends Android device information to the connector if Endpoint Management doesn't have the ActiveSync identifier for the device user.

### To configure custom policies by editing the connector for Exchange ActiveSync XML file

You can view the basic policies in the default configuration on the **Policies** tab of the connector for Exchange ActiveSync configuration utility. If you want to create custom policies, you can edit the Citrix Gateway connector for Exchange ActiveSync XML configuration file (config\config.xml).

1. Find the **PolicyList** section in the file and then add a new **Policy** element.
2. If a new group is also required, such as another static group or a group to support another GCP, add the new **Group** element to the **GroupList** section.
3. Optionally, you can change the ordering of groups within an existing policy by rearranging the **GroupRef** elements.

### Configuring the connector for Exchange ActiveSync XML File

The connector for Exchange ActiveSync uses an XML configuration file to dictate the actions of the connector. Among other entries, the file specifies the group files and associated actions the filter

take when evaluating HTTP requests. By default, the file is named config.xml and can be found at the following location: ..\Program Files\Citrix\XenMobile NetScaler Connector\config.

## GroupRef Nodes

The GroupRef nodes define the logical group names. The defaults are AllowGroup and DenyGroup.

### Note:

The order of the GroupRef nodes as they appear in the GroupRefList node is significant.

The ID value of a GroupRef node identifies a logical container or collection of members that are used for matching specific user accounts or devices. The action attributes specify how the filter treats a member that matches a rule in the collection. For example, a user account or device that matches a rule in the AllowGroup set “passes.” To pass means to be allowed to access the Exchange CAS. A user account or device that matches a rule in the DenyGroup set is “rejected.” Rejected means not to be allowed to access the Exchange CAS.

When a particular user account/device or combination meets rules in both groups, a precedence convention is used to direct the request’s outcome. Precedence is embodied in the order of the GroupRef nodes in the config.xml file from top to bottom. The GroupRef nodes are ranked in priority order. Rules for a given condition in the Allow group will always take precedence over rules for the same condition in the Deny group.

## Group Nodes

Also, the config.xml defines Group nodes. These nodes link the logical containers AllowGroup and DenyGroup to external XML files. Entries stored in the external files form the basis of the filter rules.

### Note:

In this release, only external XML files are supported.

The default installation implements two XML file in the configuration: allow.xml and deny.xml.

## Configuring Citrix Gateway connector for Exchange ActiveSync

You can configure the Citrix Gateway connector for Exchange ActiveSync to selectively block or allow ActiveSync requests based on the following properties: **Active Sync Service ID**, **Device type**, **User Agent** (device operating system), **Authorized user**, and **ActiveSync Command**.

The default configuration supports a combination of static and dynamic groups. You maintain static groups by using the SMG Controller Configuration utility. The static groups can consist of known categories of devices, such as all devices using a given user agent.

An external source called a Gateway Configuration Provider maintains dynamic groups. The connector for Exchange ActiveSync connects the groups on a periodic basis. Endpoint Management can export groups of allowed and blocked devices and users to the connector for Exchange ActiveSync.

An external source called a Gateway Configuration Provider maintains dynamic groups. The connector for Exchange ActiveSync collects dynamic groups periodically. Endpoint Management can export groups of allowed and blocked devices and users to the connector.

A policy is an ordered list of groups in which each group has an associated action (allow or block) and a list of group members. A policy can have any number of groups. Group ordering within a policy is important because when a match is found the action of the group is taken, and subsequent groups are not evaluated.

A member defines a way to match the properties of a request. It can match a single property, such as device ID, or multiple properties, such as device type and user agent.

### **Choosing a Security Model for Citrix Gateway connector for Exchange ActiveSync**

Establishing a security model is essential to a successful mobile device deployment for organizations of any size. It is common to use protected or quarantined network control to allow access to a user, computer, or device by default. This practice is not always ideal. Every organization that manages IT security might have a slightly different or tailored approach to security for mobile devices.

The same logic applies to mobile device security. Using a permissive model is a weak choice due to the multitude of mobile devices and types, mobile devices per user, and available operating system platforms and apps. In most organizations, the restrictive model is the most logical choice.

The configuration scenarios that Citrix allows for integrating the connector for Exchange ActiveSync with Endpoint Management are as follows:

#### **Permissive Model (Permit Mode)**

The permissive security model operates on the premise that everything is either allowed or granted access by default. Only through rules and filtering is something blocked and a restriction applied. The permissive security model is good for organizations that have a relatively loose security concern about mobile devices. The model only applies restrictive controls to deny access where appropriate (when a policy rule is failed).

#### **Restrictive Model (Block Mode)**

The restrictive security model is based on the premise that nothing is allowed or granted access by default. Everything passing through the security check point is filtered and inspected, and is denied

access unless the rules allowing access are passed. The restrictive security model is good for organizations that have a relatively tight security criterion about mobile devices. The mode only grants access for use and functionality with the network services when all rules to allow access have passed.

### **Managing Citrix Gateway connector for Exchange ActiveSync**

You can use the Citrix Gateway connector for Exchange ActiveSync to build access control rules. The rules either allow or block access to ActiveSync connection requests from managed devices. Access is based on device status, app allow or block lists, and other compliance conditions.

By using the connector for Exchange ActiveSync configuration utility, you can build dynamic and static rules that enforce corporate email policies. Those rules and policies allow you to block users who are in violation of compliance standards. You can also set up email attachment encryption, so that all attachments that pass through your Exchange Server to managed devices are encrypted. Only authorized users with managed devices can view encrypted attachments.

#### **To uninstall the XNC**

1. Run XncInstaller.exe with an administrator account.
2. Follow the onscreen instructions to complete the uninstallation.

#### **To install, upgrade, or uninstall the connector for Exchange ActiveSync**

1. Run XncInstaller.exe with an administrator account to install the connector for Exchange ActiveSync or allow for upgrade or removal of an existing connector.
2. Follow the onscreen instructions to complete the installation, upgrade, or uninstallation.

After you install the connector for Exchange ActiveSync, you must manually restart the Endpoint Management configuration service and the notification service.

### **Installing Citrix Gateway connector for Exchange ActiveSync**

You can install the connector for Exchange ActiveSync on its own server or on the same server where you installed Endpoint Management.

You can consider installing the connector for Exchange ActiveSync on its own server (separate from Endpoint Management) for the following reasons:

- If your Endpoint Management server is hosted remotely in the cloud (physical location)
- If you do not want restarts of the Endpoint Management server to affect the connector for Exchange ActiveSync (availability)
- If you want to devote a server's system resources entirely to the connector for Exchange ActiveSync (performance)

The CPU load that the connector for Exchange ActiveSync puts on a server depends on how many devices are managed. A general recommendation is to provision for one more CPU core if the connector is deployed on the same server as Endpoint Management. For large numbers of devices (more than 50,000), you might need to provision more cores if you do not have a clustered environment. The memory footprint of the connector is not significant enough to warrant more memory.

### **Citrix Gateway connector for Exchange ActiveSync system requirements**

The Citrix Gateway connector for Exchange ActiveSync communicates with Citrix Gateway over an SSL bridge configured on the Citrix Gateway appliance. The bridge enables the appliance to bridge all secure traffic directly to Endpoint Management. The connector for Exchange ActiveSync the following minimum system configuration:

Component	Requirement
Computer and processor	733 MHz Pentium III 733 MHz or higher processor. 2.0 GHz Pentium III or higher processor (recommended)
Citrix Gateway	Citrix Gateway appliance with software version 10
Memory	1 GB
Hard disk	NTFS-formatted local partition with 150 MB of available hard-disk space
Operating system	Windows Server 2016, Windows Server 2012 R2, or Windows Server 2008 R2 Service Pack 1. Must be an English-based server. Support for Windows Server 2008 R2 Service Pack 1 ends on January 14, 2020.
Other devices	Network adapter compatible with the host operating system for communication with the internal network
Microsoft .NET Framework	Version 8.5.1.11 requires Microsoft .NET Framework 4.5.
Display	VGA or higher-resolution monitor

The host computer for the connector for Exchange ActiveSync requires the following minimum available hard disk space:

- **Application:** 10–15 MB (100 MB recommended)
- **Logging:** 1 GB (20 GB recommended)

For information about platform support for the connector for Exchange ActiveSync, see [Supported device operating systems](#).

### Device email clients

Not all email clients consistently return the same ActiveSync ID for a device. Because the connector for Exchange ActiveSync expects a unique ActiveSync ID for each device, the following is true: Only email clients that consistently generate the same, unique ActiveSync ID for each device are supported. Citrix has tested these email clients and the clients have performed without errors:

- Samsung native email client
- iOS native email client

### Deploying Citrix Gateway connector for Exchange ActiveSync

The Citrix Gateway connector for Exchange ActiveSync enables you to use Citrix Gateway to proxy and load balance Endpoint Management server communication with Endpoint Management managed devices. The connector for Exchange ActiveSync communicates periodically with Endpoint Management to synchronize policies. You can cluster the connector for Exchange ActiveSync and Endpoint Management, together or independently.

#### The connector for Exchange ActiveSync components

- **The connector for Exchange ActiveSync service:** This service provides a REST web service interface that Citrix Gateway can invoke to determine if an ActiveSync request from a device is authorized.
- **Endpoint Management configuration service:** This service communicates with Endpoint Management to synchronize Endpoint Management policy changes with the connector for Exchange ActiveSync.
- **Endpoint Management notification service:** This service sends notifications of unauthorized device access to Endpoint Management. In this way, Endpoint Management can take appropriate measures, such as notifying the user why the device was blocked.
- **The connector for Exchange ActiveSync configuration utility:** This application allows the administrator to configure and monitor the connector for Exchange ActiveSync.

### To set up listening addresses for Citrix Gateway connector for Exchange ActiveSync

For the Citrix Gateway connector for Exchange ActiveSync to receive requests from Citrix Gateway to authorize ActiveSync traffic, do the following. Specify the port on which the connector for Exchange



ActiveSync listens to Citrix Gateway web service calls.

1. From the **Start** menu, select the connector for Exchange ActiveSync configuration utility.
2. Click the **Web Service** tab and then type the listening addresses for the connector web service. You can select **HTTP** or **HTTPS** or both. If the connector for Exchange ActiveSync is co-resident with Endpoint Management (installed on the same server), select port values that do not conflict with Endpoint Management.
3. After the values are configured, click **Save** and then click **Start Service** to start the web service.

### To configure device access control policies in Citrix Gateway connector for Exchange ActiveSync

To configure the access control policy you want to apply to your managed devices, do the following:

1. In the connector for Exchange ActiveSync configuration utility, click the **Path Filters** tab.
2. Select the first row, **Microsoft-Server-ActiveSync is for ActiveSync** and then click **Edit**.
3. From the **Policy** list, select the desired policy. For a policy that is inclusive of Endpoint Management policies, select **Static + ZDM: Permit Mode or Static + ZDM: Block Mode**. These policies combine local (or, static) rules with the rules from Endpoint Management. Permit Mode means that all devices not explicitly identified by the rules are permitted access to ActiveSync. Block Mode means that such devices are blocked.
4. After setting the policies, click **Save**.

### To configure communication with Endpoint Management

Specify the name and properties of the Endpoint Management server that you want to use with the Citrix Gateway connector for Exchange ActiveSync and Citrix Gateway.

#### Note:

This task assumes that you have already installed and configured Endpoint Management. The Exchange ActiveSync configuration utility uses the term Config Provider for Endpoint Management.

1. In the connector for Exchange ActiveSync configuration utility, click the **Config Providers** tab and then click **Add**.
2. Enter the name and URL of the Endpoint Management server you are using in this deployment. If you have multiple Endpoint Management servers deployed in a multitenant deployment, this name must be unique for each server instance.
3. In **Url**, enter the Web address of the Endpoint Management GlobalConfig Provider (GCP), typically in the format `https://<FQDN>/<instanceName>/services/<MagConfigService>`. The *MagConfigService* name is case-sensitive.

4. In **Password**, enter the password to use for basic HTTP authorization with the Endpoint Management web server.
5. In **Managing Host**, enter the server name where you installed the connector for Exchange ActiveSync.
6. In **Baseline Interval**, specify a time period for when a new refreshed dynamic ruleset is pulled from Endpoint Management.
7. In **Request Timeout**, specify the server request timeout interval.
8. In **Config Provider**, select if the config provider server instance is providing the policy configuration.
9. In **Events Enabled**, enable this option if you want Secure Mobile Gateway to notify Endpoint Management when a device is blocked. This option is required if you are using the Secure Mobile Gateway rules in any of your Endpoint Management Automated Actions.
10. After configuring the server, click **Test Connectivity** to test the connection to Endpoint Management.
11. When connectivity has been established, click **Save**.

### **Deploying Citrix Gateway connector for Exchange ActiveSync for redundancy and scalability**

To scale your Citrix Gateway connector for Exchange ActiveSync and Endpoint Management deployment, you can install instances of the connector for Exchange ActiveSync on multiple Windows Servers. All connector instances point to the same Endpoint Management instance. Then you can use Citrix Gateway to load balance the servers.

There are two modes for the connector for Exchange ActiveSync configuration:

- In non-shared mode, each connector for Exchange ActiveSync instance communicates with an Endpoint Management server and keeps its own private copy of the resulting policy. For example, for a cluster of Endpoint Management servers you can run a connector instance on each Endpoint Management server. The connector then gets policies from the local Endpoint Management instance.
- In shared mode, one connector for Exchange ActiveSync node is designated the primary node. The connector communicates with Endpoint Management. The other nodes share the resulting configuration through a Windows network share or by Windows (or third-party) replication.

The entire connector for Exchange ActiveSync configuration is in a single folder (consisting of a few XML files). The connector process detects changes to any file in this folder and automatically reloads the configuration. There is no failover for the primary node in shared mode. However, the system can tolerate the primary server being down for a few minutes (for example, to restart). The last known good configuration is cached in the connector process.

## Advanced concepts

April 3, 2020

The Endpoint Management Advanced Concepts articles offer a deeper dive into product information about Endpoint Management. The aim is to help reduce deployment time through expert techniques. The articles might cite the technical expert or experts who have authored the content.

For decision points, recommendations, common questions, and use cases for your Endpoint Management environment, see [Endpoint Management deployment](#) in this section.

For community support forums on Endpoint Management, see [Citrix Discussions](#).

## Endpoint Management deployment

August 31, 2021

There's a lot to consider when you're planning an Endpoint Management deployment. What devices should you choose? How should you manage them? How do you ensure that your network remains secure while still providing a good user experience? What hardware do you need in place and how do you troubleshoot it? The articles in this section aim to help answer such questions. Included are use cases and recommendations on topics that cover your deployment concerns.

Keep in mind that a guideline or recommendation might not apply to all environments or use cases. Be sure to set up a test environment before going live with an Endpoint Management deployment.

The articles in this section cover these areas:

- **Assess:** Common use cases and questions to consider when planning your deployment.
- **Design & Configure:** Recommendations for designing and configuring your environment
- **Operate & Monitor:** Ensuring the smooth operation of your running environment.

### Assess

As with any deployment, assessing your needs should be your first priority. What is your primary need for Endpoint Management? Is it necessary to manage every device in your environment, just the apps, or both? What level of security is needed for your Endpoint Management environment? Let's look at common use cases and questions for you to consider when planning your deployment.

- [Management modes](#)
- [Device requirements](#)
- [Security and user experience](#)

- [Apps](#)
- [User communities](#)
- [Email strategy](#)
- [Endpoint Management integration](#)

### **Design & Configure**

Once you finish assessing your deployment needs, you can decide how to design and configure your environment. The items to plan include:

- Choosing the hardware for your server
- Setting up policies for apps and devices
- Getting users enrolled

This section includes use cases and recommendations for each of these scenarios and more.

- [Integrating with Citrix Gateway and Citrix ADC](#)
- [SSO and proxy considerations for MDX apps](#)
- [Authentication](#)
- [Server properties](#)
- [Device and app policies](#)
- [User enrollment options](#)

### **Operate & Monitor**

After your Endpoint Management environment is up and running, you'll want to monitor it to ensure smooth operation. The monitoring section discusses where you can find the various logs and messages Endpoint Management and its components generate, and how to read those logs. This section also includes various common troubleshooting steps you can follow to reduce customer support feedback time.

- [App provisioning and deprovisioning](#)
- [Dashboard-based operations](#)
- [Role-based Access Control and Endpoint Management support](#)
- [Monitor and support](#)
- [Citrix support process](#)

### **Management modes**

September 8, 2021

Management modes is a term that includes Mobile Device Management (MDM) and Mobile App Management (MAM). You can configure:

- Enrollment profiles to enroll Android and iOS devices into MDM, MAM, or both (MDM+MAM). If you choose MDM+MAM, you can give users the ability to opt out of MDM.
- Enrollment profiles to enroll Windows 10 and Windows 11 devices into MDM.

You specify enrollment options in enrollment profiles, which you attach to delivery groups. For information about enrollment options, see [Enrollment profiles](#). The following sections focus on considerations for managing devices and apps.

### **Mobile device management (MDM)**

With MDM, you can configure, secure, and support mobile devices. MDM enables you to protect devices and data on devices at a system level. You can configure policies, actions, and security functions. For example, you can wipe a device selectively if the device is lost, stolen, or out of compliance.

Even if you don't choose to manage apps on devices, you can deliver mobile apps, such as public app store and enterprise apps.

Following are common use cases for MDM:

- MDM is a consideration for corporate-owned devices where device-level management policies or certain restrictions are required. Those restrictions include full wipe, selective wipe, or geo-location.
- When customers require management of an actual device, but do not require MDX policies.
- When users only need email delivered to their native email clients on their mobile devices, and Exchange ActiveSync or Client Access Server is already externally accessible. In this use case, you can use MDM to configure email delivery.
- When you deploy native enterprise apps (non-MDX), public app store apps, or MDX apps delivered from public stores. Consider that an MDM solution alone might not prevent data leakage of confidential information between apps on the device. Data leakage might occur with copy and paste or Save As operations in Office 365 apps.

### **Mobile app management (MAM)**

MAM protects app data and lets you control app data sharing. MAM also allows for the management of corporate data and resources, separately from personal data. With Endpoint Management configured for MAM, you can use MDX-enabled mobile apps to provide per-app containerization and control.

By using MDX policies, Endpoint Management provides app-level control over network access (such as micro VPN), app and device interaction, and app access.

MAM is often suitable for bring-your-own (BYO) devices because, although the device is unmanaged, corporate data remains protected. MDX has many MAM-only policies that don't require an MDM control.

MAM also supports the Citrix mobile productivity apps. This support includes:

- Secure email delivery to Citrix Secure Mail
- Data sharing between the secured Citrix mobile productivity apps
- Secure data storage in Citrix Files.

For details, see [Mobile productivity apps](#).

MAM is often suitable for the following examples:

- You deliver mobile apps, such as MDX apps, managed at the app level.
- You are not required to manage devices at a system level.

### **MDM+MAM**

Endpoint Management lets you specify whether users can opt out of device management. This flexibility is useful for environments that include a mix of use cases. These environments might require management of a device through MDM policies to access your MAM resources.

MDM+MAM is suitable for the following examples:

- You have a single use case in which both MDM and MAM are required. MDM is required to access your MAM resources.
- Some use cases require MDM while some do not.
- Some use cases require MAM while some do not.

### **Device Management and MDM Enrollment**

An Endpoint Management Enterprise environment can include a mixture of use cases, some of which require device management through MDM policies to allow access to MAM resources.

Before deploying Citrix mobile productivity apps to users, fully assess your use cases and decide whether to require MDM enrollment. If you later decide to change the requirement for MDM enrollment, users might need to re-enroll their devices. For more information, see [Enrollment profiles](#).

For information about enrollment and Citrix Gateway, see [Integrating with Citrix Gateway and Citrix ADC](#).

Following is a summary of the advantages and disadvantages (along with mitigations) of requiring MDM enrollment.

## When MDM enrollment is optional

### Advantages

- Users can access MAM resources without putting their devices under MDM management. This option can increase user adoption.
- Ability to secure access to MAM resources to protect enterprise data.
- MDX policies such as **App Passcode** can control app access for each MDX app.
- Configuring Citrix Gateway, Endpoint Management, and per-application time-outs, along with Citrix PIN, provide an extra layer of protection.
- While MDM actions do not apply to the device, some MDX policies are available to deny MAM access. The denial would be based on system settings, such as jailbroken or rooted devices.
- Users can choose whether to enroll their device with MDM during first-time use.

### Disadvantages

- MAM resources are available to devices not enrolled in MDM.
- MDM policies and actions are available only to MDM-enrolled devices.

### Mitigation options

- Have users agree to a company terms and conditions that hold them responsible if they choose to go out of compliance. Have administrators monitor unmanaged devices.
- Manage application access and security by using application timers. Decreased time-out values increase security, but can affect user experience.

## When MDM enrollment is required

### Advantages

- Ability to restrict access to MAM resources only to MDM-managed devices.
- MDM policies and actions can apply to all devices in the environment as desired.
- Users are not able to opt out of enrolling their device.

### Disadvantages

- Requires all users to enroll with MDM.
- Might decrease adoption for users who object to corporate management of their personal devices.

## Mitigation options

- Educate users about what Endpoint Management actually manages on their devices and what information administrators can access.

## Device requirements

March 9, 2021

An important point to consider for any deployment is the set of devices you plan to roll out. On the iOS, Android, and Windows platforms, the options are numerous. For a list of devices that Endpoint Management supports, see [Supported device platforms](#).

In a bring your own device (BYOD) environment, a mixture of supported platforms is possible. Consider the limitations in the Supported device platform article, however, when informing users about the devices they can enroll. Even if you only allow one or two devices in your environment, Endpoint Management functions slightly differently on iOS, Android, and Windows devices. Different feature sets are available on each platform.

Also, not all app designs target both tablet and phone form factors. Before you make widespread changes, test the apps to ensure that they fit the device screen you want to roll out.

You can consider enrollment factors as well. Apple and Google offer enterprise enrollment programs. Through the [Apple Deployment Program](#) and [Google Android Enterprise](#), you can purchase devices that are preconfigured and ready for employees to use.

For more information about enrollment, see [User enrollment options](#).

## Security and user experience

July 1, 2021

Security is important to any organization, but you need to achieve a balance between security and user experience. For example, you might have a highly secured environment that is difficult for users to use. Or, your environment might be so user-friendly that access control is not as strict. The other sections in this virtual handbook cover security features in detail. The purpose of this article is to give a general overview of common security concerns and the security options available in Endpoint Management.

Here are some key considerations to keep in mind for each use case:

- Do you want to secure certain apps, the entire device, or both?



- How do you want your users to authenticate their identity? Do you want to use LDAP, certificate-based authentication, or a combination of the two?
- How long do you want a user's session to last before it times out? Keep in mind that there are different time-out values for background services, Citrix ADC, and for being able to access apps while offline.
- Do you want users to set up a device-level passcode and an app-level passcode? How many logon attempts do you want to allow? Keep in mind the additional per-app authentication requirements that might be implemented with MAM and how users might perceive them.
- What other restrictions do you want to place on users? Do you want to give users access to cloud services such as Siri? What can they do with each app you make available to them and what can they not do? Do you want to deploy corporate network (Wi-Fi) policies to prevent cellular data plans from being used from inside the office?

### **App vs. Device**

One of the first things to consider is whether you want to secure:

- Only certain apps (mobile app management, or MAM)
- The entire device (mobile device management, or MDM).
- MDM+MAM

Most commonly, if you don't require device-level control, you only need to manage mobile apps, especially if your organization supports Bring Your Own Device (BYOD).

Users with devices that Endpoint Management doesn't manage can install apps through the app store. Instead of device-level controls, such as selective or full wipe, you control access to the apps through app policies. Depending on the values you set, the policies require the device to check Endpoint Management periodically to confirm that the apps are still allowed to run.

MDM allows you to secure an entire device, including the ability to take inventory of all the software on a device. MDM allows you to prevent enrollment if the device is jailbroken, rooted, or has unsafe software installed. Taking this level of control, however, makes users leery of allowing that much power over their personal devices and can reduce enrollment rates.

### **Authentication**

Authentication is where a great deal of the user experience takes place. If your organization is already running Active Directory, using Active Directory is the simplest way to have your users access the system.

Another significant part of the authentication user experience is time-outs. A high security environment might have users sign on every time they access the system. That option might not be ideal for all organizations or use cases.

## User Entropy

For added security, you can enable a feature called *user entropy*. Citrix Secure Hub and some other apps often share common data like passwords, PINs, and certificates to ensure everything functions properly. This information is stored in a generic vault within Secure Hub. If you enable user entropy through the **Encrypt Secrets** option, Endpoint Management creates a vault called UserEntropy. Endpoint Management moves the information from the generic vault into this new vault. For Secure Hub or another app to access the data, users must enter a password or PIN.

Enabling user entropy adds another layer of authentication in several places. As a result, whenever an app requires access to shared data in the UserEntropy vault (including passwords, PINs, and certificates), users must authenticate.

You can learn more about user entropy by reading [About the MDX Toolkit](#). To turn on user entropy, you can find the related settings in the [Client properties](#).

## Policies

Both MDX and MDM policies give a great deal of flexibility to organizations, but they can also restrict users. You might want that restriction in some situations, but policies can also make a system unusable. For instance, you might want to block access to cloud applications such as Siri or iCloud that have the potential to send sensitive data to outside locations. You can set up a policy to block access to these services, but keep in mind that such a policy can have unintended consequences. For example, the iOS keyboard mic relies on cloud access.

## Apps

Enterprise Mobility Management (EMM) segments into Mobile Device Management (MDM) and Mobile Application Management (MAM). While MDM enables organizations to secure and control mobile devices, MAM facilitates application delivery and management. With the increasing adoption of BYOD, you can typically implement a MAM solution, such as Endpoint Management, to assist with the following:

- app delivery
- software licensing
- configuration
- app life cycle management

With Endpoint Management, you can add more security to these apps by configuring specific MAM policies and VPN settings to prevent data leaks and other security threats. Endpoint Management provides organizations with the flexibility to include both MDM and MAM functionality in the same environment.

In addition to the ability to deliver apps to mobile devices, Endpoint Management offers app containerization through MDX technology. MDX secures apps through encryption that is separate from device level encryption provided by the platform. You can wipe or lock apps. Apps are subject to granular policy-based controls. Independent software vendors (ISVs) can apply these controls using the Mobile Apps SDK.

In a corporate environment, users use various mobile apps to aid in their job role. The apps can include apps from the public app store, in-house developed apps, or native apps. Endpoint Management categorizes these apps as follows:

**Public apps:** These apps include free or paid apps available in a public app store, such as the Apple App Store or Google Play. Vendors outside of the organization often make their apps available in public app stores. This option lets their customers download the apps directly from the Internet. You might use numerous public apps in your organization depending on users' needs. Examples of such apps include GoToMeeting, Salesforce, and EpicCare apps.

Citrix does not support downloading app binaries directly from public app stores, then wrapping them with the MDX Toolkit for enterprise distribution. To MDX-enable third-party applications, contact your app vendor to obtain the app binaries. You can wrap the binaries by using the MDX Toolkit or integrate the MAM SDK with the binaries.

**In-house apps:** Many organizations have in-house developers who create apps that provide specific functionality and are independently developed and distributed within the organization. In certain cases, some organizations might also have apps that ISVs provide. You can deploy such apps as native apps or you can containerize the apps by using a MAM solution, such as Endpoint Management. For example, a healthcare organization can create an in-house app that allows physicians to view patient information on mobile devices. An organization can then MAM SDK enable or MDM-wrap the app to secure patient information and enable VPN access to the back-end patient database server.

**Web and SaaS apps:** These apps include apps accessed from an internal network (web apps) or over a public network (SaaS). Endpoint Management also allows you to create custom web and SaaS apps using a list of app connectors. These app connectors can facilitate single sign-on (SSO) to existing Web apps. For details, see [App connector types](#). For example, you can use Google Apps SAML for SSO based on Security Assertion Markup Language (SAML) to Google Apps.

**Mobile productivity apps:** Mobile productivity apps are Citrix-developed apps that are included with the Endpoint Management license. For details, see [About mobile productivity apps](#). Citrix also offers other [business-ready apps](#). ISVs develop business-ready apps by using the Mobile Apps SDK.

**HDX apps:** HDX apps are Windows-hosted apps that you publish with StoreFront. If you have a Citrix Virtual Apps and Desktops environment, you can integrate the apps with Endpoint Management to make the apps available to the enrolled users.

Depending on the type of mobile apps you plan to deploy and manage with Endpoint Management, the underlying configuration and architecture differ. Suppose that multiple groups of users with vari-

ous levels of permissions consume a single app. In that case, you can create separate delivery groups to deploy two versions of the app. Make sure that the user group membership is mutually exclusive to avoid policy mismatches on user devices.

You might also want to manage iOS application licensing by using Apple volume purchase. This option requires that you register for the Apple volume purchase program. And, you must use the Endpoint Management console to configure volume purchase settings. That configuration allows you to distribute the apps with the volume purchase licenses. Various such use cases make it important to assess and plan your MAM strategy before implementing the Endpoint Management environment. You can start planning your MAM strategy by defining the following:

**Types of apps:** List the different types of apps you plan to support. Then, categorize the apps, such as public, native, Citrix mobile productivity apps, Web, in-house, and ISV apps. Also, categorize the apps for different device platforms, such as iOS and Android. This categorization helps you to align the Endpoint Management settings that are required for each type of app. For example: Certain apps might not qualify for wrapping. Or, a few apps might require use of the Mobile Apps SDK to enable special APIs for interaction with other apps.

**Network requirements:** Configure apps with specific network access requirements with the appropriate settings. For example, certain apps might need access to your internal network through VPN. Some apps might require Internet access to route access via the DMZ. To allow such apps to connect to the required network, you have to configure various settings accordingly. Define per-app network requirements to help finalize your architectural decisions up front. That work streamlines the overall implementation process.

**Security requirements:** Define the security requirements that apply to either individual apps or all the apps. Some settings, such as the MDX policies, apply to individual apps. Session and authentication settings apply across all apps. Some apps might have specific encryption, containerization, wrapping, authentication, geofencing, passcode, or data sharing requirements. Outline those requirements in advance to simplify your deployment.

**Deployment requirements:** You might want to use a policy-based deployment to allow only compliant users to download the published apps. For example, you might want certain apps to require that:

- device platform-based encryption is enabled
- the device is managed
- the device meets a minimum operating system version
- certain apps are available only to corporate users

Outline such requirements in advance so that you can configure the appropriate deployment rules or actions.

**Licensing requirements:** Record app-related licensing requirements. Such notes help you to manage license usage effectively and to decide if you need to configure specific features in Endpoint Man-

agement to facilitate licensing. For example, if you deploy a free or paid iOS app, Apple enforces licensing requirements on the app by making users sign on to their Apple Store account. You can register for Apple volume purchase to distribute and manage these apps through Endpoint Management. Volume purchase allows users to download the apps without having to sign into their Apple Store account. Also, tools, such as Samsung SAFE and Samsung Knox, have special licensing requirements, which you need to complete before deploying those features.

**Allow list and block list requirements:** You likely want to prevent users from installing or using some apps. Create an allow list of apps that make a device out of compliance. Then, set up policies to trigger when a device becomes non-compliant. On the other hand, an app might be acceptable for use but might fall under the block list for some reason. In that case, you can add the app to an allow list and indicate that the app is acceptable to use, but isn't required. Also, keep in mind that the apps pre-installed on new devices can include some commonly used apps that are not part of the operating system. Those apps might conflict with your block list strategy.

### Apps use case

A healthcare organization plans to deploy Endpoint Management to serve as a MAM solution for their mobile apps. Mobile apps are delivered to corporate and BYOD users. IT decides to deliver and manage the following apps:

- **Mobile productivity apps:** iOS and Android apps provided by Citrix.
- **Citrix Files:** App to access shared data and to share, sync, and edit files.

### Public app store

- **Secure Hub:** Client used by all mobile devices to communicate with Endpoint Management. IT pushes security settings, configurations, and mobile apps to mobile devices via the Secure Hub client. Android and iOS devices enroll in Endpoint Management through Secure Hub.
- **Citrix Workspace app:** Mobile app that allows users to open on mobile devices apps hosted by Citrix Virtual Apps.
- **GoToMeeting:** An online meeting, desktop sharing, and video conferencing client that lets users meet with other computer users, customers, clients, or colleagues via the Internet in real time.
- **SalesForce1:** Salesforce1 lets users access Salesforce from mobile devices and brings all Chatter, CRM, custom apps, and business processes together in a unified experience for any Salesforce user.
- **RSA SecurID:** Software-based token for two-factor authentication.
- **EpicCare apps:** These apps give healthcare practitioners secure and portable access to patient charts, patient lists, schedules, and messaging.
  - **Haiku:** Mobile app for the iPhone and Android phones.
  - **Canto:** Mobile app for the iPad

- **Rover:** Mobile apps for iPhone and iPad.

**HDX:** Citrix Virtual Apps delivers HDX apps to Citrix Workspace.

- **Epic Hyperspace:** Epic client application for electronic health record management.

## ISV

- **Vocera:** HIPAA compliant voice-over IP and messaging mobile app that extends the benefits of Vocera voice technology anytime, anywhere via iPhone and Android smartphones.

## In-house apps

- **HCMail:** App that helps compose encrypted messages, search address books on internal mail servers, and send the encrypted messages to the contacts using an email client.

## In-house web apps

- **PatientRounding:** Web application used to record patient health information by different departments.
- **Outlook Web Access:** Allows the access of email via a web browser.
- **SharePoint:** Used for organization-wide file and data sharing.

The following table lists the basic information required for MAM configuration.

App Name	App Type	MDX Wrapping	iOS	Android
Secure Mail	Mobile productivity app	No for version 10.4.1 and later	Yes	Yes
Secure Web	Mobile productivity app	No for version 10.4.1 and later	Yes	Yes
Citrix Files	Mobile productivity app	No for version 10.4.1 and later	Yes	Yes
Secure Hub	Public App	NA	Yes	Yes
Citrix Workspace app	Public App	NA	Yes	Yes
GoToMeeting	Public App	NA	Yes	Yes
SalesForce1	Public App	NA	Yes	Yes
RSA SecurID	Public App	NA	Yes	Yes
Epic Haiku	Public App	NA	Yes	Yes

App Name	App Type	MDX Wrapping	iOS	Android
Epic Canto	Public App	NA	Yes	No
Epic Rover	Public App	NA	Yes	No
Epic Hyperspace	HDX App	NA	Yes	Yes
Vocera	ISV App	Yes	Yes	Yes
HCMail	In-House App	Yes	Yes	Yes
PatientRounding	Web App	NA	Yes	Yes
Outlook Web Access	Web App	NA	Yes	Yes
SharePoint	Web App	NA	Yes	Yes

The following tables list specific requirements you can consult when configuring MAM policies in End-point Management.

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Device platform-based encryption
Secure Mail	Y	Selectively Allowed	Allowed	Not required
Secure Web	Y	Allowed	Allowed	Not required
Citrix Files	Y	Allowed	Allowed	Not required
Secure Hub	Y	N/A	N/A	N/A
Citrix Workspace app	Y	N/A	N/A	N/A
GoToMeeting	N	N/A	N/A	N/A
SalesForce1	N	N/A	N/A	N/A
RSA SecurID	N	N/A	N/A	N/A
Epic Haiku	Y	N/A	N/A	N/A
Epic Canto	Y	N/A	N/A	N/A
Epic Rover	Y	N/A	N/A	N/A
Epic Hyperspace	Y	N/A	N/A	N/A
Vocera	Y	Blocked	Blocked	Not required

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Device platform-based encryption
HCMail	Y	Blocked	Blocked	Required
PatientRounding	Y	N/A	N/A	Required
Outlook Web Access	Y	N/A	N/A	Not required
SharePoint	Y	N/A	N/A	Not required

App Name	Proxy Filtering	Licensing	Geofencing	Mobile Apps SDK	Minimum Operating System Version
Secure Mail	Required	N/A	Selectively Required	N/A	Enforced
Secure Web	Required	N/A	Not required	N/A	Enforced
Secure Notes	Required	N/A	Not required	N/A	Enforced
Citrix Files	Required	N/A	Not required	N/A	Enforced
Secure Hub	Not required	Volume purchase	Not required	N/A	Not enforced
Citrix Workspace app	Not required	Volume purchase	Not required	N/A	Not enforced
GoToMeeting	Not required	Volume purchase	Not required	N/A	Not enforced
SalesForce1	Not required	Volume purchase	Not required	N/A	Not enforced
RSA SecurID	Not required	Volume purchase	Not required	N/A	Not enforced
Epic Haiku	Not required	Volume purchase	Not required	N/A	Not enforced
Epic Canto	Not required	Volume purchase	Not required	N/A	Not enforced



App Name	Proxy Filtering	Licensing	Geofencing	Mobile Apps SDK	Minimum Operating System Version
Epic Rover	Not required	Volume purchase	Not required	N/A	Not enforced
Epic Hyperspace	Not required	N/A	Not required	N/A	Not enforced
Vocera	Required	N/A	Required	Required	Enforced
HCMail	Required	N/A	Required	Required	Enforced
PatientRound- ing	Required	N/A	Not required	N/A	Not enforced
Outlook Web Access	Required	N/A	Not required	N/A	Not enforced
SharePoint	Required	N/A	Not required	N/A	Not enforced

## User Communities

Every organization consists of diverse user communities that operate in different functional roles. These user communities perform different tasks and office functions using various resources that you provide through user devices. Users might work from home or in remote offices using mobile devices that you provide. Or, users might own their mobile devices, which allows them to access tools that are subject to certain security compliance rules.

As more user communities start using mobile devices in their job role, Enterprise Mobility Management (EMM) becomes critical to prevent data leaks. EMM is also critical to enforce an organization's security restrictions. For efficient and more sophisticated mobile device management, you can categorize your user communities. Doing so simplifies the mapping of users to resources and aligns the appropriate security policies to users.

The following example illustrates how the user communities of a healthcare organization are classified for EMM.

### User communities use case

This example healthcare organization provides technology resources and access to multiple users, including network and affiliate employees and volunteers. The organization has chosen to roll out the EMM solution to non-executive users only.

User roles and functions for this organization can be broken into subgroups including: clinical, non-clinical, and contractors. Selected users receive corporate mobile devices, while others can access limited company resources from their personal devices. To enforce the right level of security restrictions and prevent data leaks, the organization decided that corporate IT manages each enrolled device. Those devices might be corporate-owned or Bring Your Own Device (BYOD). Also, users can only enroll a single device.

The following section provides an overview of the roles and functions of each subgroup:

### **Clinical**

- Nurses
- Physicians (Doctors, Surgeons, and so on)
- Specialists (Dietitians, anesthesiologists, radiologists, cardiologists, oncologists, and so on)
- Outside physicians (Non-employee physicians and office workers that work from remote offices)
- Home Health Services (Office and mobile workers performing physician services for patient home visits)
- Research Specialist (Knowledge Workers and Power Users at six Research Institutes performing clinical research to find answers to issues in medicine)
- Education and Training (Nurses, physicians, and specialists in education and training)

### **Non-Clinical**

- Shared Services (Office workers performing various back-office functions, including HR, Payroll, Accounts Payable, and Supply Chain Service)
- Physician Services (Office workers performing various healthcare management, administrative services, and business process solutions to providers, including: Administrative Services, Analytics and Business Intelligence, Business Systems, Client Services, Finance, Managed Care Administration, Patient Access Solutions, Revenue Cycle Solutions, and so on)
- Support Services (Office workers performing various non-clinical functions including: Benefits Administration, Clinical Integration, Communications, Compensation & Performance Management, Facility & Property Services, HR Technology Systems, Information Services, Internal Audit & Process Improvement, and so o.)
- Philanthropic Programs (Office and mobile workers that perform various functions in support of philanthropic programs)

### **Contractors**

- Manufacturer and vendor partners (Onsite and remotely connected via site-to-site VPN providing various non-clinical support functions)

Based on the preceding information, the organization created the following entities. For more information about delivery groups in Endpoint Management, see [Deploy resources](#).

### **Active Directory Organizational Units (OUs) and Groups**

For OU = Endpoint Management Resources:

- OU = Clinical; Groups =
  - XM-Nurses
  - XM-Physicians
  - XM-Specialists
  - XM-Outside Physicians
  - XM-Home Health Services
  - XM-Research Specialist
  - XM-Education and Training
- OU = Non-Clinical; Groups =
  - XM-Shared Services
  - XM-Physician Services
  - XM-Support Services
  - XM-Philanthropic Programs

### **Endpoint Management Local Users and Groups**

For Group= Contractors, Users =

- Vendor1
- Vendor2
- Vendor 3
- ... Vendor 10

### **Endpoint Management Delivery Groups**

- Clinical-Nurses
- Clinical-Physicians
- Clinical-Specialists
- Clinical-Outside Physicians
- Clinical-Home Health Services
- Clinical-Research Specialist
- Clinical-Education and Training
- Non-Clinical-Shared Services
- Non-Clinical-Physician Services
- Non-Clinical-Support Services

- Non-Clinical-Philanthropic Programs

### Delivery Group and User Group mapping

Active Directory Groups	Endpoint Management Delivery Groups
XM-Nurses	Clinical-Nurses
XM-Physicians	Clinical-Physicians
XM-Specialists	Clinical-Specialists
XM-Outside Physicians	Clinical-Outside Physicians
XM-Home Health Services	Clinical-Home Health Services
XM-Research Specialist	Clinical-Research Specialist
XM-Education and Training	Clinical-Education and Training
XM-Shared Services	Non-Clinical-Shared Services
XM-Physician Services	Non-Clinical-Physician Services
XM-Support Services	Non-Clinical-Support Services
XM-Philanthropic Programs	Non-Clinical-Philanthropic Programs

### Delivery Group and Resource mapping

The following tables illustrate the resources assigned to each delivery group in this use case. The first table shows the mobile app assignments. The second table shows the public app, HDX apps, and device management resources.

Endpoint Management Delivery Groups	Citrix Mobile Apps	Public Mobile Apps	HDX Mobile Apps
Clinical-Nurses	X		
Clinical-Physicians			
Clinical-Specialists			
Clinical-Outside Physicians	X		
Clinical-Home Health Services	X		

Endpoint Management Delivery Groups			
Groups	Citrix Mobile Apps	Public Mobile Apps	HDX Mobile Apps
Clinical-Research Specialist	X		
Clinical-Education and Training		X	X
Non-Clinical-Shared Services		X	X
Non-Clinical-Physician Services		X	X
Non-Clinical-Support Services	X	X	X
Non-Clinical-Philanthropic Programs	X	X	X
Contractors	X	X	X

Endpoint Management Delivery Groups	Public	Public	HDX App:	Passcode	Device Re-	Automated	Network
	App: RSA SecurID	App: EpicCare Haiku	HDX App: Epic Hy-perspace	Policy	strictions	Actions	Policy
Clinical-Nurses							X
Clinical-Physicians					X		
Clinical-Specialists							
Clinical-Outside Physicians							

Endpoint Management Delivery Groups	Public App: RSA SecurID	Public App: EpicCare Haiku	HDX App: Epic Hy-perspace	Passcode Policy	Device Restrictions	Automated Actions	Network Policy
Clinical-Home Health Services							
Clinical-Research Specialist							
Clinical-Education and Training		X	X				
Non-Clinical-Shared Services		X	X				
Non-Clinical-Physician Services		X	X				
Non-Clinical-Support Services		X	X				

**Notes and considerations**

- Endpoint Management creates a default delivery group named All Users during the initial configuration. If you do not disable this delivery group, all Active Directory users have rights to enroll into Endpoint Management.
- Endpoint Management synchronizes Active Directory users and groups on demand using a dynamic connection to the LDAP server.
- If a user is part of a group that is not mapped in Endpoint Management, that user cannot enroll. Likewise, if a user is a member of multiple groups, Endpoint Management only categorizes the

user as part of the groups mapped to Endpoint Management.

## Security requirements

The scope of security considerations related to an Endpoint Management environment can quickly become overwhelming. There are many interlocking pieces and settings. You might not know where to begin or what to choose to ensure an acceptable level of protection is available. To make these choices simpler, Citrix provides recommendations for High, Higher, and Highest Security, as outlined in the following table.

Security concerns aren't the only consideration for the mode in which your devices enroll: MAM, MDM+MAM with MDM optional, or MDM+MAM with MDM required. It is important to also review the requirements of the use case and decide if you can mitigate security concerns before choosing your management mode.

**High:** Using these settings provides an optimal user experience while maintaining a basic level of security acceptable to most organizations.

**Higher:** These settings create a stronger balance between security and usability.

**Highest:** Following these recommendations provides a high level of security at the cost of usability and user adoption.

## Management mode security considerations

The following table specifies the management modes for each security level.

High Security	Higher Security	Highest Security
MAM, MDM+MAM	MDM+MAM	MDM+MAM

### Notes:

- Depending on the use case, a MAM-only deployment can meet security requirements and provide a good user experience.
- For use cases like BYOD in which all business and security requirements might be satisfied with app containerization only, Citrix recommends MAM-only mode.
- For high security environments (and corporate issued devices), Citrix recommends MDM+MAM to take advantage of all security capabilities available.

### Citrix ADC and Citrix Gateway security considerations

The following table specifies the Citrix ADC and Citrix Gateway recommendations for each security level.

High Security	Higher Security	Highest Security
Citrix ADC is recommended. Citrix Gateway is required for MAM and MDM+MAM	Standard NetScaler for XenMobile wizard configuration with SSL bridge if Endpoint Management is in the DMZ.	SSL Offload with end-to-end encryption

#### Notes:

- Exposing the Endpoint Management server to the Internet via NAT or existing third-party proxies/load-balancers might be an option for MDM. However, in that case, the SSL traffic terminates on an Endpoint Management server, which poses a potential security risk.
- For high security environments, Citrix Gateway with the default Endpoint Management configuration typically meets or exceeds security requirements.
- For MDM enrollments with the highest security needs, SSL termination at Citrix Gateway enables you to inspect traffic at the perimeter, while maintaining end-to-end SSL encryption.
- Options to define SSL/TLS ciphers.
- For more information, see [Integrating with Citrix Gateway and Citrix ADC](#).

### Enrollment security considerations

The following table specifies the Citrix ADC and Citrix Gateway recommendations for each security level.

High Security	Higher Security	Highest Security
Active Directory Group membership only. All users Delivery Group disabled.	Invitation only enrollment security mode. Active Directory Group membership only. All users Delivery Group disabled	Enrollment security mode tied to Device ID. Active Directory Group membership only. All users Delivery Group disabled

#### Notes:

- Citrix generally recommends that you restrict enrollment to users in predefined Active Di-



- rectory groups only. This restriction requires disabling the built-in All users delivery group.
- You can use enrollment invitations to restrict enrollment to users with an invitation. Enrollment invitations aren't available for Windows devices.
  - You can use one-time PIN (OTP) enrollment invitations as a two-factor authentication solution and to control the number of devices a user can enroll. (OTP invitations aren't available for Windows devices.)

### Device passcode security considerations

The following table specifies the device passcode recommendations for each security level.

High Security	Higher Security	Highest Security
Recommended. High security is required for device-level encryption. Can be enforced with MDM. Can be set as required for MAM-only by using the MDX policy, Non-compliant device behavior.	Enforced by using an MDM, MAM, or MDM+MAM policy.	Enforced by using an MDM and MDX policy. MDM Complex passcode policy.

#### Notes:

- Citrix recommends the use of a device passcode.
- You can enforce a device passcode via an MDM policy.
- You can use an MDX policy to make a device passcode a requirement for using managed apps; for example, for BYOD use cases.
- Citrix recommends combining the MDM and MDX policy options for increased security for MDM+MAM enrollments.
- For environments with the highest security requirements, you can configure complex passcode policies and enforced them with MDM. You can configure automatic actions to notify administrators or issue selective/full device wipes when a device doesn't comply with a passcode policy.

## Apps

October 7, 2021

Enterprise Mobility Management (EMM) segments into Mobile Device Management (MDM) and Mobile Application Management (MAM). While MDM enables organizations to secure and control mobile devices, MAM facilitates application delivery and management. With the increasing adoption of BYOD, you can typically implement a MAM solution, such as Endpoint Management. Endpoint Management assists with application delivery, software licensing, configuration, and application life cycle management. You can require or allow users to also opt into MDM management.

With Endpoint Management, you secure apps by configuring MAM policies and VPN settings to prevent data leak and other security threats. Endpoint Management provides organizations with the flexibility to enroll devices as MAM-only or MDM+MAM.

In addition to the ability to deliver apps to mobile devices, Endpoint Management offers app containerization through MDX technology. The apps are subject to granular policy-based controls. Independent software vendors (ISVs) can apply these controls using the Mobile Apps SDK.

In a corporate environment, users use various mobile apps to aid in their job role. The apps can include apps from the public app store, in-house developed apps, or native apps. Endpoint Management categorizes these apps as follows:

- **Public apps:** These apps include free or paid apps available in a public app store, such as the Apple App Store or Google Play. Vendors outside of the organization often make their apps available in public app stores. This option lets their customers download the apps directly from the Internet. You might use numerous public apps in your organization depending on users' needs. Examples of such apps include GoToMeeting, Salesforce, and EpicCare apps.
  - **If you use the MAM SDK:** Obtain the app binaries from your app vendor. Then, integrate the MAM SDK into the app.
  - **If you use the MDX Toolkit:** Citrix does not support downloading app binaries directly from public app stores, and then wrapping them with the MDX Toolkit for enterprise distribution. To wrap third-party applications, work with your app vendor to obtain the app binaries. You can then wrap the binaries by using the MDX Toolkit.
- **In-house apps:** Many organizations have in-house developers who create apps that provide specific functionality and are independently developed and distributed within the organization. In certain cases, some organizations might also have apps that ISVs provide. You can deploy such apps as native apps or you can containerize the apps by using a MAM solution, such as Endpoint Management.

For example, a healthcare organization might create an in-house app that allows physicians to view patient information on mobile devices. An organization can then secure patient information and enable VPN access to the patient database by using one of the following:

- MAM SDK
- MDX Toolkit

- **Web and SaaS apps:** These apps include apps accessed from an internal network (web apps) or over a public network (SaaS). Endpoint Management also allows you to create custom web and SaaS apps using a list of app connectors. These app connectors can facilitate single sign-on (SSO) to existing Web apps. For details, see [App connector types](#). For example, you can use Google Apps SAML for SSO based on Security Assertion Markup Language (SAML) to Google Apps.
- **Mobile productivity apps:** Mobile productivity apps are Citrix-developed apps that are included with the Endpoint Management license. For details, see [About mobile productivity apps](#). Citrix also offers other [business-ready apps](#) that ISVs develop by using the Mobile Apps SDK.
- **HDX apps:** HDX apps are Windows-hosted apps that you publish with StoreFront. If you use Citrix Virtual Apps and Desktops and Citrix Workspace, HDX apps are available to enrolled users.

Depending on the type of mobile apps you plan to deploy and manage with Endpoint Management, the underlying configuration might differ. For example, multiple groups of users with different level of permissions might consume a single app. In that case you can create separate delivery groups to deploy two separate versions of the same app. In addition, you must make sure the user group membership is mutually exclusive to avoid policy mismatches on users' devices.

You can also manage iOS application licensing by using Apple volume purchase. This option requires you to register for the volume purchase program and configure the volume purchase settings in the Endpoint Management console. That configuration allows you to distribute the apps with the volume purchase licenses. Various use cases make it important to assess and plan your MAM strategy before implementing the Endpoint Management environment. You can start planning your MAM strategy by defining the following:

- **Types of apps:** List the different types of apps you plan to support and categorize them, such as public, native, Web, in-house, or ISV apps. Also, categorize the apps for different device platforms, such as iOS and Android. This categorization helps with aligning the various Endpoint Management settings that are required for each type of app. For example, a few apps might require use of the Mobile Apps SDK to enable special APIs for interaction with other apps.
- **Network requirements:** Configure the settings of apps that have specific network access requirements. For example, certain apps might need access to your internal network through VPN. Some apps might require Internet access to route access via the DMZ. To allow such apps to connect to the required network, you must configure various settings accordingly. Defining per-app network requirements help in finalizing your architectural decisions early on, which streamlines the overall implementation process.
- **Security requirements:** You can define security requirements to apply to either individual apps or all apps.
  - Settings, such as the MDX policies, apply to individual apps

- Session and authentication settings apply across all apps
- Some apps might have specific containerization, MDX, authentication, geofencing, passcode, or data sharing requirements

Outline those requirements in advance to simplify your deployment. For details on security in Endpoint Management, see [Security and user experience](#).

- **Deployment requirements:** You might want to use a policy-based deployment to allow only compliant users to download the published apps. For example, certain apps can require that the device is managed or that the device meets a minimum operating system version. You might also want certain apps to be available only to corporate users. Outline such requirements in advance so that you can configure the appropriate deployment rules or actions.
- **Licensing requirements:** Keep a record of the app-related licensing requirements. Your notes can help you manage license usage effectively and decide whether to configure specific features in Endpoint Management to facilitate licensing. For example, if you deploy a free or paid iOS app, Apple enforces licensing requirements on the app. As a result, users must sign in to their Apple App Store account.

However, you can register for Apple volume purchase to distribute and manage these apps by using Endpoint Management. Volume purchase allows users to download the apps without having to sign into their Apple App Store account.

Some platforms, such as Samsung SAFE and Samsung Knox, have special licensing requirements to complete before deploying those features.

- **Allow list and block list requirements:** You might identify apps that you do not want users to install or use. Creating a block list defines an out of compliance event. You can then set up policies to trigger when the event occurs. On the other hand, an app might be acceptable for use but can fall under the block list for some reason. In that case, you can add the app to an allow list and indicate that the app is acceptable to use but is not required. Also, keep in mind that the apps pre-installed on new devices can include some commonly used apps that are not part of the operating system. Such apps can conflict with your block list strategy.

## Use Case

A healthcare organization plans to deploy Endpoint Management to serve as a MAM solution for their mobile apps. Mobile apps are delivered to corporate and BYOD users. IT decides to deliver and manage the following apps:

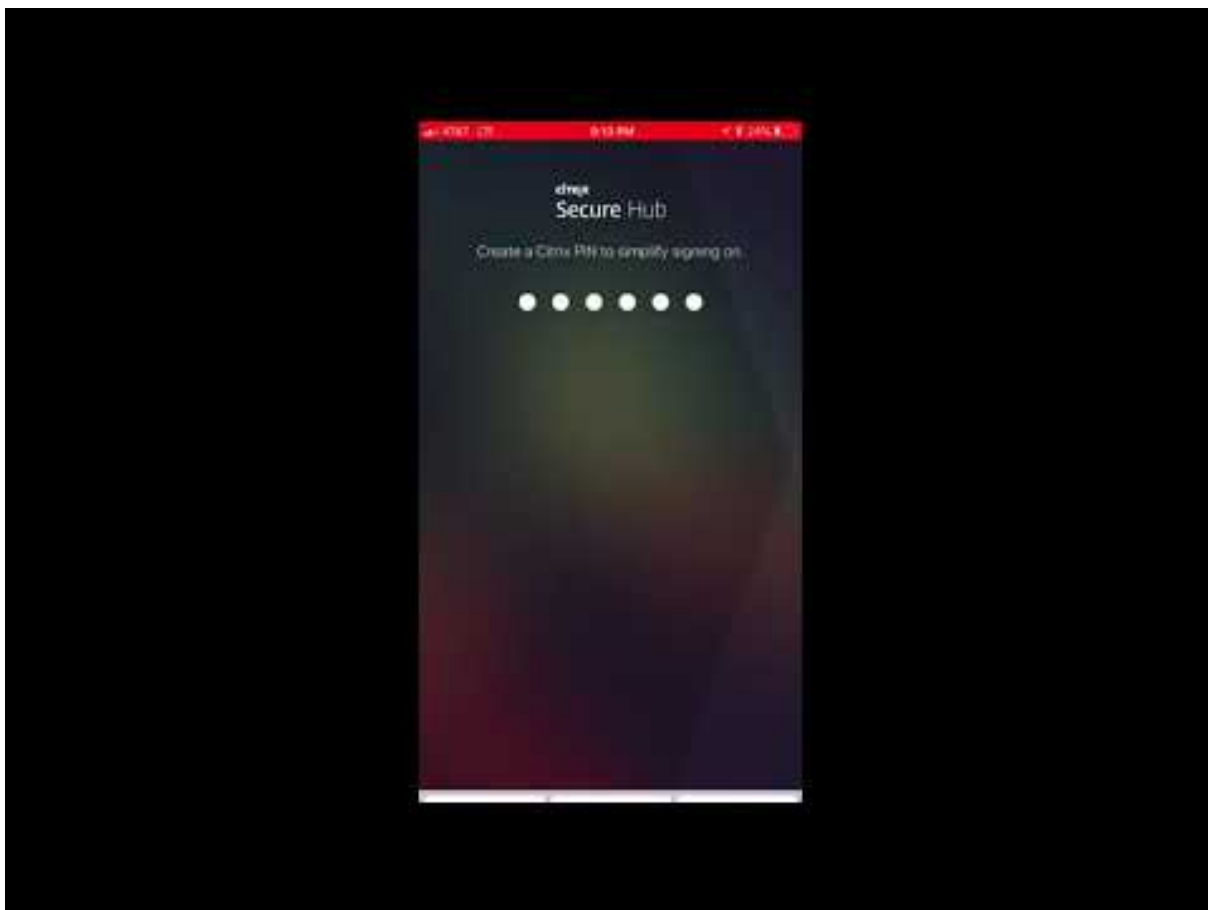
**Mobile productivity apps:** iOS and Android apps provided by Citrix. For details, see [Mobile productivity apps](#).

**Citrix Secure Hub:** For customers who onboarded before Endpoint Management 10.18.14: You push security settings, configurations, and mobile apps to mobile devices by using Secure Hub. Android

and iOS devices enroll in Endpoint Management through Secure Hub.

For new customers as of Endpoint Management 10.18.14: Secure Hub supports the use of the Workspace apps store. When opening Secure Hub, users no longer see the Secure Hub store. Now, an Add Apps button takes users to the Workspace apps store.

Following is a video that shows an iOS device performing an enrollment to Citrix Endpoint Management using the Citrix Workspace app.



**Citrix Workspace app:** The Citrix Workspace app incorporates existing Citrix Receiver technology, Secure Hub, and other Citrix Workspace client technologies. Workspace app provides end users with a unified, contextual experience.

**GoToMeeting:** An online meeting, desktop sharing, and video conferencing client that lets users meet with other computer users, customers, clients, or colleagues via the Internet in real time.

**SalesForce1:** Salesforce1 lets users access Salesforce from mobile devices and brings all Chatter, CRM, custom apps, and business processes together in a unified experience for any Salesforce user.

**RSA SecurID:** Software-based token for two-factor authentication.

**EpicCare apps:** These apps give healthcare practitioners secure and portable access to patient charts, patient lists, schedules, and messaging.

**Haiku:** Mobile app for the iPhone and Android phones.

**Canto:** Mobile app for the iPad

**Rover:** Mobile apps for iPhone and iPad.

**HDX:** These apps are delivered via Citrix Virtual Apps in Citrix Workspace.

- **Epic Hyperspace:** Epic client application for electronic health record management.

**ISV:**

- **Vocera:** HIPAA compliant voice-over IP and messaging mobile app that extends the benefits of Vocera voice technology anytime, anywhere via iPhone and Android smartphones.

**In-house apps:**

- **HCMail:** App that helps compose encrypted messages, search address books on internal mail servers, and send the encrypted messages to the contacts using an email client.

**In-house web apps:**

- **PatientRounding:** Web application used to record patient health information by different departments.
- **Outlook Web Access:** Allows the access of email via a web browser.
- **SharePoint:** Used for organization-wide file and data sharing.

The following table lists the basic information required for MAM configuration.

App Name	App Type	MDX-enabled	iOS	Android
Secure Mail	Mobile productivity app	No	Yes	Yes
Secure Web	Mobile productivity app	No	Yes	Yes
Citrix Files	Mobile productivity app	No	Yes	Yes
Secure Hub	Public App	N/A	Yes	Yes
Citrix Workspace app	Public App	N/A	Yes	Yes
GoToMeeting	Public App	N/A	Yes	Yes
SalesForce1	Public App	N/A	Yes	Yes
RSA SecurID	Public App	N/A	Yes	Yes
Epic Haiku	Public App	N/A	Yes	Yes
Epic Canto	Public App	N/A	Yes	No

App Name	App Type	MDX-enabled	iOS	Android
Epic Rover	Public App	N/A	Yes	No
Epic Hyperspace	HDX App	N/A	Yes	Yes
Vocera	ISV App	Yes	Yes	Yes
HCMail	In-House App	Yes	Yes	Yes
PatientRounding	Web App	N/A	Yes	Yes
Outlook Web Access	Web App	N/A	Yes	Yes
SharePoint	Web App	N/A	Yes	Yes

The following table lists specific requirements you can consult configuring MAM policies in Endpoint Management.

App Name	VPN Required	Interaction		Proxy Filtering	Licensing	Geo-fencing	Mobile Apps SDK	Minimum Operating System Version
		(with apps out-side of con-tainer)	(from apps out-side of con-tainer)					
Secure Mail	Y	Selective Allowed	Allowed	Required	N/A	Selective Re-quired	N/A	Enforced
Secure Web	Y	Allowed	Allowed	Required	N/A	Not re-quired	N/A	Enforced
Citrix Files	Y	Allowed	Allowed	Required	N/A	Not re-quired	N/A	Enforced
Secure Hub	Y	N/A	N/A	Not re-quired	Volume purchase	Not re-quired	N/A	Not enforced
Citrix Workspac app	Y	N/A	N/A	Not re-quired	Volume purchase	Not re-quired	N/A	Not enforced

App Name	VPN Required	Interaction		Proxy Filtering	Licensing	Geo-fencing	Mobile Apps SDK	Minimum Operating System Version
		(with apps outside of container)	(from apps outside of container)					
GoToMeeting	Y	N/A	N/A	Not required	Volume purchase	Not required	N/A	Not enforced
SalesForce	N	N/A	N/A	Not required	Volume purchase	Not required	N/A	Not enforced
RSA SecurID	N	N/A	N/A	Not required	Volume purchase	Not required	N/A	Not enforced
Epic Haiku	Y	N/A	N/A	Not required	Volume purchase	Not required	N/A	Not enforced
Epic Canto	Y	N/A	N/A	Not required	Volume purchase	Not required	N/A	Not enforced
Epic Rover	Y	N/A	N/A	Not required	Volume purchase	Not required	N/A	Not enforced
Epic Hyper-space	Y	N/A	N/A	Not required	N/A	Not required	N/A	Not enforced
Vocera	Y	Blocked	Blocked	Required	N/A	Required	Required	Enforced
HCMail	Y	Blocked	Blocked	Required	N/A	Required	Required	Enforced
PatientRc ing	Y	N/A	N/A	Required	N/A	Not required	N/A	Not enforced
Outlook Web Access	Y	N/A	N/A	Required	N/A	Not required	N/A	Not enforced



App Name	VPN Required	Interaction		Proxy Filtering	Geo-fencing	Mobile Apps SDK	Minimum Operating System Version
		(with apps out-side of container)	(from apps out-side of container)				
SharePoint	Y	N/A	N/A	Required	N/A	Not required	Not enforced

## User communities

March 17, 2021

Every organization consists of diverse user communities that operate in different functional roles. These user communities perform different tasks and office functions using various resources that you provide through user mobile devices. Users might work from home or in remote offices using mobile devices that you provide. Or, users might use personal mobile devices, which allows them to access tools that are subject to certain security compliance rules.

With more user communities using mobile devices, Enterprise Mobility Management (EMM) becomes critical to prevent a data leak and to enforce organizational security restrictions. For efficient and more sophisticated mobile device management, you can categorize your user communities. Doing so simplifies the mapping of users to resources and ensures that the right security policies apply to the right users.

Categorizing user communities can include use of the following components:

- Active Directory Organizational Units (OUs) and Groups

Users added to specific Active Directory security groups can receive policies and resources such as apps. Removing users from the Active Directory security groups removes access to previously allowed Endpoint Management resources.

- Endpoint Management local users and groups

For users who don't have an account in Active Directory, you can create the users as local Endpoint Management users. You can add local users to delivery groups and provision resources to them in the same manner as Active Directory users.

- Endpoint Management delivery groups

If multiple groups of users with different levels of permissions are to consume a single app, you might want to create separate delivery groups. With separate delivery groups, you can deploy two separate versions of the same app. Citrix recommends creating delivery groups before you create device policies.

- Delivery group and user group mapping

Delivery group to Active Directory group mappings can be either one-to-one, or one-to-many. Assign base policies and apps to a one-to-many delivery group mapping. Assign function-specific policies and apps to one-to-one delivery group mappings.

- Delivery Group and Resource Mapping of Apps

Assign specific apps to each delivery group.

- Delivery Group and Resource Mapping of MDM Resources

Assign apps and specific device management resources to each delivery group. For example, configure a delivery group with any mix of the following: Types of apps (public, HDX, and so on), specific apps per app type, and resources such as device policies and automated actions.

The following example illustrates how the user communities of a healthcare organization are classified for EMM.

### **Use case**

This example healthcare organization provides technology resources and access to multiple users, including network and affiliate employees and volunteers. The organization has chosen to roll out the EMM solution to non-executive users only.

You can divide user roles and functions for this organization into subgroups including: clinical, non-clinical, and contractors. A selected set of users receives corporate mobile devices, while others can access limited company resources from their personal devices (BYOD). To enforce the appropriate level of security restrictions and prevent data leak, the organization decided that corporate IT manages each enrolled device. Also, users can only enroll a single device.

The following sections provide an overview of the roles and functions of each subgroup.

### **Clinical**

- Nurses
- Physicians (Doctors, Surgeons, and so on)
- Specialists (Dieticians, anesthesiologists, radiologists, cardiologists, oncologists, and so on)
- Outside physicians (Non-employee physicians and office workers that work from remote offices)

- Home Health Services (Office and mobile workers performing physician services for patient home visits)
- Research Specialist (Knowledge Workers and Power Users at six Research Institutes performing clinical research to find answers to issues in medicine)
- Education and Training (Nurses, physicians, and specialists in education and training)

### **Non-clinical**

- Shared Services (Office workers performing various back-office functions including: HR, Payroll, Accounts Payable, Supply Chain Service, and so on)
- Physician Services (Office workers performing various healthcare management, administrative services, and business process solutions to providers, including: Administrative Services, Analytics and Business Intelligence, Business Systems, Client Services, Finance, Managed Care Administration, Patient Access Solutions, Revenue Cycle Solutions, and so on)
- Support Services (Office workers performing various non-clinical functions including: Benefits Administration, Clinical Integration, Communications, Compensation & Performance Management, Facility & Property Services, HR Technology Systems, Information Services, Internal Audit & Process Improvement, and so on.)
- Philanthropic Programs (Office and mobile workers that perform various functions in support of philanthropic programs)

### **Contractors**

- Manufacturer and vendor partners (Onsite and remotely connected via site-to-site VPN providing various non-clinical support functions)

Based on the preceding information, the organization created the following entities. For more information about delivery groups in Endpoint Management, see [Deploy resources](#) in the Endpoint Management product documentation.

### **Active Directory Organizational Units (OUs) and Groups**

**For OU =** Endpoint Management Resources

- OU = Clinical; Groups =
  - XM-Nurses
  - XM-Physicians
  - XM-Specialists
  - XM-Outside Physicians
  - XM-Home Health Services
  - XM-Research Specialist

- XM-Education and Training
- OU = Non-Clinical; Groups =
  - XM-Shared Services
  - XM-Physician Services
  - XM-Support Services
  - XM-Philanthropic Programs

### **Endpoint Management Local Users and Groups**

For Group= Contractors, Users =

- Vendor1
- Vendor2
- Vendor 3
- ... Vendor 10

### **Endpoint Management Delivery Groups**

- Clinical-Nurses
- Clinical-Physicians
- Clinical-Specialists
- Clinical-Outside Physicians
- Clinical-Home Health Services
- Clinical-Research Specialist
- Clinical-Education and Training
- Non-Clinical-Shared Services
- Non-Clinical-Physician Services
- Non-Clinical-Support Services
- Non-Clinical-Philanthropic Programs

### **Delivery Group and User Group mapping**

---

Active Directory Groups	Endpoint Management Delivery Groups
XM-Nurses	Clinical-Nurses
XM-Physicians	Clinical-Physicians
XM-Specialists	Clinical-Specialists
XM-Outside Physicians	Clinical-Outside Physicians
XM-Home Health Services	Clinical-Home Health Services

Active Directory Groups	Endpoint Management Delivery Groups
XM-Research Specialist	Clinical-Research Specialist
XM-Education and Training	Clinical-Education and Training
XM-Shared Services	Non-Clinical-Shared Services
XM-Physician Services	Non-Clinical-Physician Services
XM-Support Services	Non-Clinical-Support Services
XM-Philanthropic Programs	Non-Clinical-Philanthropic Programs

**Delivery Group and Resource mapping of apps**

	Secure Mail	Secure Web	Citrix Files	Workspace app	RSA SecurID	EpicCare Haiku	Epic Hyper-space
Clinical-Nurses	X	X	X				
Clinical-Physicians							
Clinical-Specialist							
Clinical-Outside Physicians	X		X				
Clinical-Home Health Services	X		X				
Clinical-Research Specialist	X		X				

	Secure Mail	Secure Web	Citrix Files	Workspace app	SalesForce	RSA SecurID	EpicCare Haiku	Epic Hyper-space
Clinical-Education and Training							X	X
Non-Clinical-Shared Services							X	X
Non-Clinical-Physician Services							X	X
Non-Clinical-Support Services	X		X				X	X
Non-Clinical-Philanthr Programs	X		X				X	X
Contractor	X		X	X	X		X	X

**Delivery Group and Resource mapping of MDM Resources**

	MDM: Passcode policy	MDM: Device Restrictions	MDM: Automated Actions	MDM: Network policy
Clinical-Nurses				X

	MDM: Passcode policy	MDM: Device Restrictions	MDM: Automated Actions	MDM: Network policy
Clinical-Physicians		X		
Clinical-Specialists				
Clinical-Outside Physicians				
Clinical-Home Health Services				
Clinical-Research Specialist				
Clinical-Education and Training				
Non-Clinical-Shared Services				
Non-Clinical-Physician Services				
Non-Clinical-Support Services				
Non-Clinical-Philanthropic Programs				
Contractors				X

**Notes and considerations**

- Endpoint Management creates a default delivery group named All Users during the initial configuration. If you do not disable this Delivery Group, all Active Directory users have rights to enroll into Endpoint Management.
- Endpoint Management synchronizes Active Directory users and groups on demand using a dynamic connection to the LDAP server.
- If a user is part of a group that is not mapped in Endpoint Management, that user cannot enroll.

Likewise, if a user is a member of multiple groups, Endpoint Management only categorizes the user as being in the groups mapped to Endpoint Management.

## Email strategy

January 6, 2021

Secure access to email from mobile devices is one of the main drivers behind any organization's mobility management initiative. Deciding on the proper email strategy is often a key component of any Endpoint Management design. Endpoint Management offers several options to accommodate different use cases, based on security, user experience, and integration requirements. This article covers the typical design decision process and considerations for choosing the right solution, from client selection to mail traffic flow.

### Choosing your email clients

Client selection is generally at the top of the list for the overall email strategy design. You can choose from several clients: Citrix Secure Mail, native mail that is included with a particular mobile platform operating system, or other third-party clients available through the public app stores. Depending on your needs, you can possibly support the user communities with a single (standard) client or you may need to use a combination of clients.

The following table outlines some design considerations for the different client options available:

---

Topic	Secure Mail	Native (for example, iOS Mail)	Third-party mail
Configuration	Exchange account profiles configured via an MDX policy.	Exchange account profiles configured via an MDM policy. Android support is limited to: SAFE/Knox and Android Enterprise. All other clients are considered third-party clients.	Generally requires manual configuration by the user.



Security	Secure by design, providing the highest security. Uses MDX policies with added data encryption levels. Secure Mail is a fully managed app via an MDX policy. Added layer of authentication with Citrix PIN.	Based on vendor/app feature set. Provides higher security. Uses device encryption settings. Relies on device-level authentication for access to the app.	Based on vendor/app feature set. Provides high security.
Integration	Allows interaction with managed (MDX) apps by default. Open web URLs with Citrix Secure Web. Save files to and attach files from Citrix Files. Directly join and dial in to GoToMeeting.	Can only interact with other unmanaged (non-MDX) apps by default.	Can only interact with other unmanaged (non-MDX) apps by default.
Deployment/ Licensing	You can push Secure Mail through MDM, directly from public app stores. Included with Endpoint Management Advanced and Enterprise licensing.	Client app included with platform operating system. No additional licensing requirements.	Can push via MDM, as an enterprise app or directly from public app stores. Associated licensing model/costs based on app vendor.

Support	Single vendor support for the client and EMM solution (Citrix). Embedded support contact info in Secure Hub/app debug logging capabilities. One client to support.	Vendor defined support (Apple/Google). May need to support different clients based on device platform.	Vendor-defined support. One client to support, assuming that the third-party client is supported on all managed device platforms.
---------	--	--	---

### Mail traffic flow and filtering considerations

This section discusses the three main scenarios and design considerations regarding the flow of mail (ActiveSync) traffic in the context of Endpoint Management.

#### Scenario 1: Exposed Exchange

Environments that support external clients commonly have Exchange ActiveSync services exposed to the internet. Mobile ActiveSync clients connect through this externally facing path through a reverse proxy (for example, Citrix Gateway) or through an edge server. This option is required for the use of native or third-party mail clients, making these clients the popular choice for this scenario. Although not a common practice, you can also use the Secure Mail client in this scenario. By doing so, you benefit from the security features offered by the use of MDX policies and management of the app.

#### Scenario 2: Tunneled via Citrix Gateway (micro VPN and STA)

This scenario is the default when using the Secure Mail client, due to its micro VPN capabilities. In this case, the Secure Mail client establishes a secure connection to ActiveSync via Citrix Gateway. In essence, you can consider Secure Mail to be the client connecting directly to ActiveSync from the internal network. Citrix customers often standardize on Secure Mail as the mobile ActiveSync client of choice. That decision is part of an initiative to avoid exposing ActiveSync services to the internet on an exposed Exchange Server, as described in the first scenario.

Only apps that are MAM SDK enabled or MDX-wrapped can use the micro VPN function. This scenario does not apply to native clients if you use MDX wrapping. Even though it may be possible to wrap third-party clients with the MDX Toolkit, this practice is not common. The use of device-level VPN clients to allow tunneled access for native or third-party clients has proven to be cumbersome and not a viable solution.

### Scenario 3: Cloud-hosted Exchange services

Cloud-hosted Exchange services, such as Microsoft Office 365, are becoming more popular. In the context of Endpoint Management, this scenario may be treated in the same way as the first scenario, because the ActiveSync service is also exposed to the internet. In this case, cloud service provider requirements dictate client choices. The choices generally include support for most ActiveSync clients, such as Secure Mail and other native or third-party clients.

Endpoint Management can add value in three areas for this scenario:

- Clients with MDX policies and app management with Secure Mail
- Client configuration with the use of an MDM policy on supported native email clients
- ActiveSync filtering options with the use of the Endpoint Management connector for Exchange ActiveSync

### Mail traffic filtering considerations

As with most services exposed to the internet, you must secure the path and provide filtering for authorized access. The Endpoint Management solution includes two components designed specifically to provide ActiveSync filtering capabilities for native and third-party clients: Citrix Gateway connector for Exchange ActiveSync and Endpoint Management connector for Exchange ActiveSync.

### Citrix Gateway connector for Exchange ActiveSync

Citrix Gateway connector for Exchange ActiveSync provides ActiveSync filtering at the perimeter, by using Citrix Gateway as a proxy for ActiveSync traffic. As a result, the filtering component sits in the path of mail traffic flow, intercepting mail as it enters or leaves the environment. The connector for Exchange ActiveSync acts as an intermediary between Citrix Gateway and Endpoint Management. When a device communicates with Exchange through the ActiveSync virtual server on the Citrix Gateway, Citrix Gateway performs an HTTP callout to the connector for Exchange ActiveSync service. That service then checks the device status with Endpoint Management. Based on the status of the device, the connector for Exchange ActiveSync replies to Citrix Gateway to either allow or deny the connection. You may also configure static rules to filter access based on user, agent, and device type or ID.

This setup allows Exchange ActiveSync services to be exposed to the internet with an added layer of security to prevent unauthorized access. Design considerations include the following:

- **Windows Server:** The connector for Exchange ActiveSync component requires a Windows Server.
- **Filtering rule set:** The connector for Exchange ActiveSync is designed for filtering based on device state and information, rather than user information. Although you may configure static rules to filter by user ID, no options exist for filtering based on Active Directory group mem-

bership, for example. If there is a requirement for Active Directory group filtering, you can use Endpoint Management connector for Exchange ActiveSync instead.

- **Citrix Gateway scalability:** Given the requirement to proxy ActiveSync traffic via Citrix Gateway: Proper sizing of the Citrix Gateway instance is critical to support the added workload of all ActiveSync SSL connections.
- **Citrix Gateway Integrated Caching:** The connector for Exchange ActiveSync configuration on the Citrix Gateway uses the Integrated Caching function to cache responses from the connector. As a result of that configuration, Citrix Gateway doesn't need to issue a request to the connector for every ActiveSync transaction in a given session. That configuration is also critical for adequate performance and scale. Integrated Caching is available with the Citrix Gateway Platinum Edition.
- **Custom filtering policies:** You might need to create custom Citrix Gateway policies to restrict certain ActiveSync clients outside of the standard native mobile clients. This configuration requires knowledge on ActiveSync HTTP requests and Citrix Gateway responder policy creation.
- **Secure Mail clients:** Secure Mail has micro VPN capabilities which eliminate the need for filtering at the perimeter. The Secure Mail client would generally be treated as an internal (trusted) ActiveSync client when connected through the Citrix Gateway. If support for both native and third-party (with the connector for Exchange ActiveSync) and Secure Mail clients is required: Citrix recommends that Secure Mail traffic does not flow via the Citrix Gateway virtual server used for the connector. You can accomplish this traffic flow via DNS and keep the connector policy from affecting Secure Mail clients.

For a diagram of Citrix Gateway connector for Exchange ActiveSync in an Endpoint Management deployment, see [Architecture](#).

## Endpoint Management connector for Exchange ActiveSync

Endpoint Management connector for Exchange ActiveSync is an Endpoint Management component that provides ActiveSync filtering at the Exchange service level. As a result, filtering only occurs once the mail reaches the exchange service, rather than when it enters the Endpoint Management environment. Mail Manager uses PowerShell to query Exchange ActiveSync for device partnership information and control access through device quarantine actions. Those actions take devices in and out of quarantine based on Endpoint Management connector for Exchange ActiveSync rule criteria.

Similar to Citrix Gateway connector for Exchange ActiveSync, the connector for Exchange ActiveSync checks the device status with Endpoint Management to filter access based on device compliance. You may also configure static rules to filter access based on device type or ID, agent version, and Active Directory group membership.

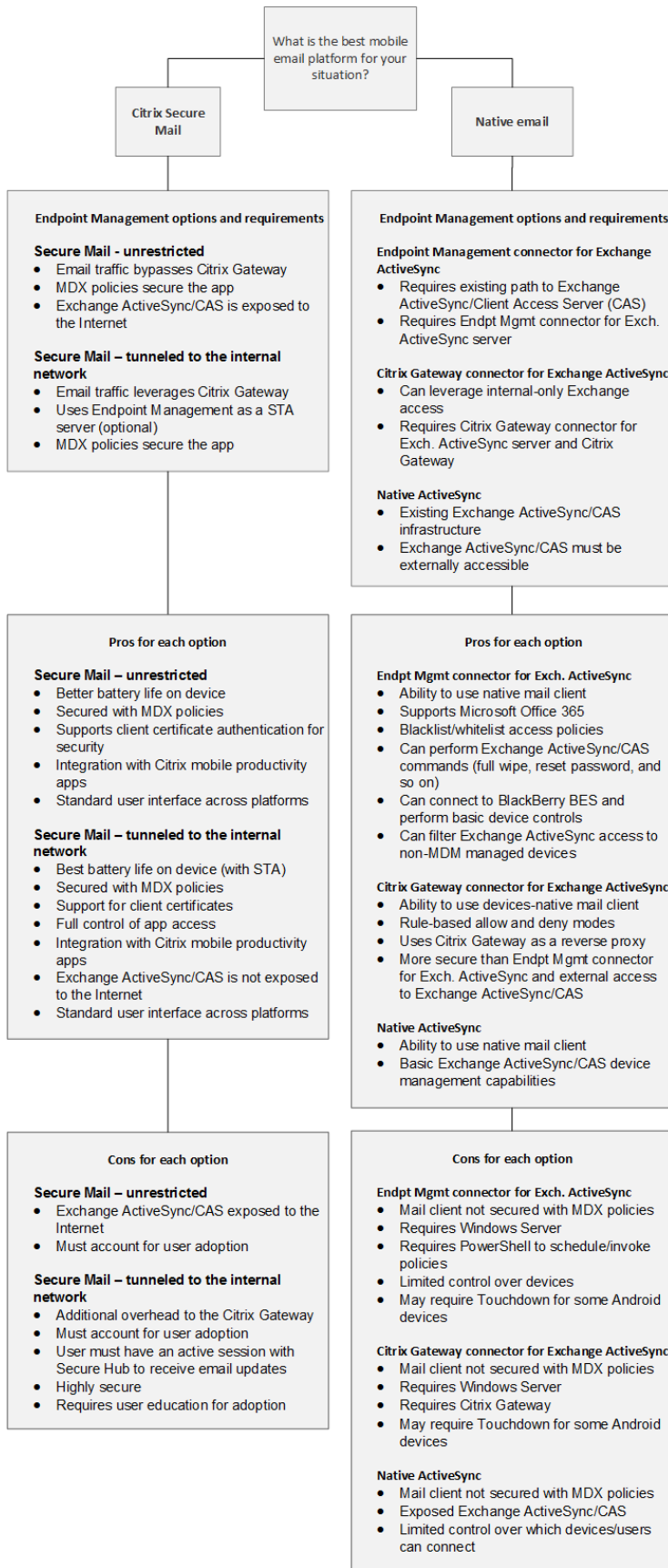
This solution does not require the use of Citrix Gateway. You can deploy the connector for Exchange ActiveSync without changes routing for the existing ActiveSync traffic. Design considerations include:

- **Windows Server:** The connector for Exchange ActiveSync requires you to deploy Windows Server.
- **Filtering rule set:** Just like Citrix Gateway connector for Exchange ActiveSync, the connector for Exchange ActiveSync includes filtering rules to evaluate device state. Additionally, the connector for Exchange ActiveSync also supports static rules to filter based on Active Directory group membership.
- **Exchange integration:** The connector for Exchange ActiveSync requires direct access to the Exchange Client Access Server (CAS) hosting the ActiveSync role and control over device quarantine actions. This requirement might present a challenge depending on the environment architecture and security posture. It is critical that you evaluate this technical requirement up front.
- **Other ActiveSync clients:** Because the connector for Exchange ActiveSync is filtering at the ActiveSync service level, consider other ActiveSync clients outside the Endpoint Management environment. You can configure the connector for Exchange ActiveSync static rules to avoid unintended impact to other ActiveSync clients.
- **Extended Exchange functions:** Through direct integration with Exchange ActiveSync, the connector for Exchange ActiveSync provides the ability for Endpoint Management to perform an Exchange ActiveSync wipe on a mobile device. The connector for Exchange ActiveSync also allows Endpoint Management to access information about Blackberry devices and to perform other control operations.

For a diagram of Endpoint Management connector for Exchange ActiveSync in an Endpoint Management deployment, see [Architecture](#).

### Email platform decision tree

The following figure helps you distinguish the pros and cons between using native email or Secure Mail solutions in your Endpoint Management deployment. Each choice allows for associated Endpoint Management options and requirements to enable server, network, and database access. The pros and cons include details on security, policy, and user interface considerations.



## Endpoint Management integration

August 31, 2021

This article covers what to consider when planning how Endpoint Management is to integrate with your existing network and solutions. For example, if you're already using Citrix Gateway for Citrix Virtual Apps and Desktops:

- Do you want to use the existing Citrix Gateway instance or a new, dedicated instance?
- Do you want to integrate with Endpoint Management the HDX apps that are published using StoreFront?
- Do you plan to use Citrix Files with Endpoint Management?
- Do you have a Network Access Control solution that you want to integrate into Endpoint Management?

### Citrix Gateway

Citrix Gateway is required for Endpoint Management. Citrix Gateway provides a micro VPN path for access to all corporate resources and provides strong multifactor authentication support.

You can use existing Citrix Gateway instances or set up new ones for Endpoint Management. The following sections note the advantages and disadvantages of using existing or new, dedicated Citrix Gateway instances.

### Shared Citrix Gateway MPX with a Citrix Gateway VIP created for Endpoint Management

#### Advantages:

- Uses a common Citrix Gateway instance for all Citrix remote connections: Citrix Virtual Apps, full VPN, and clientless VPN.
- Uses the existing Citrix Gateway configurations, such as for certificate authentication and for accessing services like DNS, LDAP, and NTP.
- Uses a single Citrix Gateway platform license.

#### Disadvantages:

- It is more difficult to plan for scale when you handle two different use cases on the same Citrix Gateway.
- Sometimes you need a specific Citrix Gateway version for a Citrix Virtual Apps use case. That same version might have known issues for Endpoint Management. Or Endpoint Management might have known issues for the Citrix Gateway version.
- If a Citrix Gateway exists, you cannot run the NetScaler for XenMobile wizard a second time to create the Citrix Gateway configuration for Endpoint Management.

- Except when Platinum licenses are used for Citrix Gateway 11.1 or later: User access licenses installed on Citrix Gateway and required for VPN connectivity are pooled. Because those licenses are available to all Citrix Gateway virtual servers, services other than Endpoint Management can potentially consume them.

### **Dedicated Citrix Gateway VPX/MPX instance**

#### **Advantages:**

Citrix recommends using a dedicated instance of Citrix Gateway.

- Easier to plan for scale and separates Endpoint Management traffic from a Citrix Gateway instance that might already be resource constrained.
- Avoids issues when Endpoint Management and Citrix Virtual Apps need different Citrix Gateway software versions. The recommendation generally is to use the latest compatible Citrix Gateway version and build for Endpoint Management.
- Allows Endpoint Management configuration of Citrix Gateway through the built-in NetScaler for XenMobile wizard.
- Virtual and physical separation of services.

#### **Disadvantages:**

- Requires setup of extra services on Citrix Gateway to support Endpoint Management configuration.
- Requires another Citrix Gateway platform license. License each Citrix Gateway instance for Citrix Gateway.

For information about what to consider when integrating Citrix Gateway and Citrix ADC for Endpoint Management management modes, see [Integrating with Citrix Gateway and Citrix ADC](#).

### **StoreFront**

If you have a Citrix Virtual Apps and Desktops environment, you can integrate HDX applications with Endpoint Management using StoreFront. When you integrate HDX apps with Endpoint Management:

- The apps are available to users who are enrolled with Endpoint Management.
- The apps display in the app store along with other mobile apps.
- Endpoint Management uses Citrix Receiver on StoreFront.
- When the Citrix Workspace app is installed on a device, HDX apps start using that app.

StoreFront has a limitation of one services site per StoreFront instance. Suppose that you have multiple stores and want to segment it from other production usage. In that case, Citrix generally recommends that you consider a new StoreFront Instance and services site for Endpoint Management.

#### **Considerations include:**



- Are there any different authentication requirements for StoreFront? The StoreFront services site requires Active Directory credentials for logon. Customers only using certificate-based authentication cannot enumerate applications through Endpoint Management using the same Citrix Gateway.
- Use the same store or create a store?
- Use the same or a different StoreFront server?

The following sections note the advantages and disadvantages of using separate or combined store-fronts for Citrix Workspace and Citrix mobile productivity apps.

### **Integrate your existing StoreFront instance with Endpoint Management**

#### **Advantages:**

- Same store: No additional configuration of StoreFront is required for Endpoint Management, assuming that you use the same Citrix Gateway VIP for HDX access. Suppose that you choose to use the same store and want to direct Citrix Workspace access to a new Citrix Gateway VIP. In that case, add the appropriate Citrix Gateway configuration to StoreFront.
- Same StoreFront server: Uses the existing StoreFront installation and configuration.

#### **Disadvantages:**

- Same store: Any reconfiguration of StoreFront to support Citrix Virtual Apps and Desktops workloads might adversely affect Endpoint Management.
- Same StoreFront server: In large environments, consider the additional load from Endpoint Management usage of Citrix Receiver for app enumeration and start-up.

### **Use a new, dedicated StoreFront instance for integration with Endpoint Management**

#### **Advantages:**

- New store: Any configuration changes of the StoreFront store for Endpoint Management don't affect existing Virtual Apps and Desktops workloads.
- New StoreFront server: Server configuration changes don't affect Virtual Apps and Desktops workflows. Also, load outside of Endpoint Management usage of Citrix Receiver for app enumeration and launch don't affect scalability.

#### **Disadvantages:**

- New store: StoreFront store configuration.
- New StoreFront server: Requires new StoreFront installation and configuration.

For more information, see [Citrix Virtual Apps and Desktops through the app store](#).

## **Citrix Content Collaboration and Citrix Files**

Citrix Content Collaboration enables you to easily and securely exchange documents, send large documents by email, and securely handle document transfers to third parties. The Citrix Files app enables users to access and sync all of their data from any device. With Citrix Files, users can securely share data with people both inside and outside the organization.

Integration of Citrix Content Collaboration with Endpoint Management differs depending on whether your site is Workspace-enabled.

### **If Endpoint Management is Workspace-enabled**

When using Citrix Workspace and Citrix Workspace app along with the Citrix Content Collaboration service, you can:

- Access all of your files from the Files tab in Citrix Workspace.
- View all your Favorites, Personal and Shared Folders, and access your cloud connectors.
- Submit files for Feedback and Approval, view your File Box, manage your Recycle Bin, and edit files.
- For information about Citrix Collaboration features not supported in Workspace, see [Deploy](#) and [Create or link a Content Collaboration \(ShareFile\) account to Citrix Cloud](#).

### **If Endpoint Management isn't Workspace-enabled**

If Endpoint Management isn't Workspace-enabled, you integrate Content Collaboration with Endpoint Management. Endpoint Management provides Citrix Files with:

- Single sign-on authentication for mobile productivity app users.
- Active Directory-based user account provisioning.
- Comprehensive access control policies.

Mobile users can benefit from the full Enterprise account feature set.

Alternatively, you can configure Endpoint Management to integrate only with storage zone connectors. Through storage zone connectors, Citrix Files provides access to:

- Documents and folders
- Network file shares
- In SharePoint sites: Site collections and document libraries.

Connected file shares can include the same network home drives used in Citrix Virtual Apps and Desktops environments. You use the Endpoint Management console to configure the integration with Enterprise accounts or storage zone connectors. For more information, see [Citrix Files for Endpoint Management](#).

The following sections note the questions to ask when making design decisions for Citrix Files.

## **Integrate with Citrix Files or only storage zone connectors**

### **Questions to ask:**

- Do you want to store data in Citrix-managed storage zones?
- Do you want to provide users with file sharing and sync capabilities?
- Do you want to enable users to access files on the Citrix Files website? Or to access Office 365 content and Personal Cloud connectors from mobile devices?

### **Design decision:**

- If the answer to any of those questions is “yes,” integrate with an Enterprise account.
- An integration with only storage zone connectors gives iOS users secure mobile access to existing on-premises storage repositories, such as SharePoint sites and network file shares. In this configuration, you don’t set up a Citrix Files subdomain, provision users to Citrix Files, or host Citrix Files data. Using storage zone connectors with Endpoint Management complies with security restrictions against leaking user information outside of the corporate network.

## **Storage zones controller server location**

### **Questions to ask:**

- Do you require on-premises storage or features such as storage zone connectors?
- If using on-premises features of Citrix Files, where will the storage zones controllers sit in the network?

### **Design decision:**

- Determine whether to locate the storage zones controller servers in the Citrix Files cloud, in your on-premises single-tenant storage system, or in supported third-party cloud storage.
- Storage zones controllers require some internet access to communicate with the Citrix Files Control Plane. You can connect in several ways, including direct access or NAT/PAT configurations.

## **Storage zone connectors**

### **Questions to ask:**

- What are the CIFS share paths?
- What are the SharePoint URLs?

### **Design decision:**

- Determine if on-premises storage zones controllers are required to access those locations.
- Due to storage zone connector communication with internal resources such as file repositories, CIFS shares, and SharePoint: Citrix recommends that storage zones controllers reside in the internal network behind DMZ firewalls and fronted by Citrix Gateway.

## SAML integration with Endpoint Management

### Questions to ask:

- Is Active Directory authentication required for Citrix Files?
- Does first time use of the Citrix Files app for Endpoint Management require SSO?
- Is there a standard IdP in your current environment?
- How many domains are required to use SAML?
- Are there multiple email aliases for Active Directory users?
- Are there any Active Directory domain migrations in progress or scheduled soon?

### Design decision:

You might choose to use SAML as the authentication mechanism for Citrix Files. The authentication options are:

- Use the Endpoint Management server as the Identity Provider (IdP) for SAML

This option can provide excellent user experience, automate Citrix Files account creation, and enable mobile app SSO features.

The Endpoint Management server is enhanced for this process: It does not require the synchronization of Active Directory.

Use the Citrix Files User Management Tool for user provisioning.

- Use a supported third-party vendor as the IdP for SAML

If you have an existing and supported IdP and don't require mobile app SSO capabilities, this option might be the best fit for you. This option also requires the use of the Citrix Files User Management Tool for account provisioning.

Using third-party IdP solutions such as ADFS might also provide SSO capabilities on the Windows client side. Be sure to evaluate use cases before choosing your Citrix Files SAML IdP.

- Or, to satisfy both use cases, see [Citrix Content Collaboration single sign-on configuration guide for dual identity providers](#).

## Mobile apps

### Questions to ask:

- Which Citrix Files mobile app do you plan to use (public, MDM, MDX)?

### Design decision:

- You distribute Citrix mobile productivity apps from the Apple App Store and Google Play Store. With that public app store distribution, you obtain wrapped apps from the Citrix downloads page.

- If your security requirements are low and you don't require containerization, the public Citrix Files app might not be suitable.
- For more information, see [Apps](#) and [Citrix Files for Endpoint Management](#).

## **Security, policies, and access control**

### **Questions to ask:**

- What restrictions do you require for desktop, web, and mobile users?
- What standard access control settings do you want for users?
- What file retention policy do you plan to use?

### **Design decision:**

- Citrix Files lets you manage employee permissions. For information, see [Employee Permissions](#).
- Some Citrix Files device security settings and MDX policies control the same features. In those cases, Endpoint Management policies take precedence, followed by the Citrix Files device security settings. Examples: If you disable external apps in Citrix Files, but enable them in Endpoint Management, the external apps get disabled in Citrix Files. You can configure the apps so that Endpoint Management doesn't require a PIN/passcode, but the Citrix Files app requires a PIN/passcode.

## **Standard vs. restricted storage zones**

### **Questions to ask:**

- Do you require restricted storage zones?

### **Design decision:**

- A standard storage zone is intended for non-sensitive data and enables employees to share data with non-employees. This option supports workflows that involve sharing data outside of your domain.
- A restricted storage zone protects sensitive data: Only authenticated domain users can access the data stored in the zone.

## **Access control**

Enterprises can manage mobile devices inside and outside of networks. Enterprise Mobility Management solutions such as Endpoint Management are great at providing security and controls for mobile devices, independent of location. However, when you combine them with a Network Access Control (NAC) solution, you can add QoS and more fine-grained control to devices that are internal to your

network. That combination enables you to extend the Endpoint Management device security assessment through your NAC solution. Your NAC solution then can use the Endpoint Management security assessment to facilitate and handle authentication decisions.

You can use any of these solutions to enforce NAC policies:

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

Citrix doesn't guarantee integration for other NAC solutions.

Advantages of a NAC solution integration with Endpoint Management include the following:

- Better security, compliance, and control for all endpoints on an enterprise network.
- A NAC solution can:
  - Detect devices at the instant they attempt to connect to your network.
  - Query Endpoint Management for device attributes.
  - Use that device information to determine whether to allow, block, limit, or redirect those devices. Those decisions depend on the security policies you choose to enforce.
- A NAC solution provides IT administrators with a view of unmanaged and non-compliant devices.

For a description of the NAC compliance filters supported by Endpoint Management and a configuration overview, see [Network Access Control](#).

## Integrating with Citrix Gateway and Citrix ADC

October 7, 2021

When integrated with Endpoint Management, Citrix Gateway provides an authentication mechanism for remote device access to the internal network for MAM devices. The integration enables Citrix mobile productivity apps to connect to corporate servers in the intranet through a micro VPN. Endpoint Management creates a micro VPN from the apps on the device to Citrix Gateway. Citrix Gateway provides a micro VPN path for access to all corporate resources and provides strong multifactor authentication support.

When a user opts out of MDM enrollment, devices enroll using the Citrix Gateway FQDN.

Citrix Cloud Operations manages Citrix ADC load balancing.

## Design Decisions

The following sections summarize the many design decisions to consider when planning a Citrix Gateway integration with Endpoint Management.

### Certificates

Decision detail:

- Do you require a higher degree of security for enrollments and access to the Endpoint Management environment?
- Is LDAP not an option?

Design guidance:

The default configuration for Endpoint Management is user name and password authentication. To add another layer of security for enrollment and access to the Endpoint Management environment, consider using certificate-based authentication. You can use certificates with LDAP for two-factor authentication, providing a higher degree of security without needing an RSA server.

If you don't allow LDAP and use smart cards or similar methods, configuring certificates allows you to represent a smart card to Endpoint Management. Users then enroll using a unique PIN that Endpoint Management generates for them. After a user has access, Endpoint Management creates and deploys the certificate later used to authenticate to the Endpoint Management environment.

Endpoint Management supports Certificate Revocation List (CRL) only for a third party Certificate Authority. If you have a Microsoft CA configured, Endpoint Management uses Citrix Gateway to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the Citrix Gateway Certificate Revocation List (CRL) setting, **Enable CRL Auto Refresh**. This step ensures that the user of a device enrolled in MAM only can't authenticate using an existing certificate on the device. Endpoint Management reissues a new certificate, because it doesn't restrict a user from generating a user certificate if one is revoked. This setting increases the security of PKI entities when the CRL checks for expired PKI entities.

### Dedicated or shared Citrix Gateway VIPs

Decision detail:

- Do you currently use Citrix Gateway for Citrix Virtual Apps and Desktops?
- Will Endpoint Management use the same Citrix Gateway as Citrix Virtual Apps and Desktops?
- What are the authentication requirements for both traffic flows?

Design guidance:

When your Citrix environment includes Endpoint Management, plus Virtual Apps and Desktops, you can use the same Citrix Gateway virtual server for both. Due to potential versioning conflicts and

environment isolation, a dedicated Citrix Gateway is recommended for each Endpoint Management environment.

If you use LDAP authentication, Citrix Workspace and Secure Hub can authenticate to the same Citrix Gateway with no issues. If you use certificate-based authentication, Endpoint Management pushes a certificate in the MDX container and Secure Hub uses the certificate to authenticate with Citrix Gateway. The Workspace app is separate from Secure Hub and can't use the same certificate as Secure Hub to authenticate to the same Citrix Gateway.

You might consider this work around, which allows you to use the same FQDN for two Citrix Gateway VIPs. You can create two Citrix Gateway VIPs with the same IP address. The one for Secure Hub uses the standard 443 port and the one for Citrix Virtual Apps and Desktops (which deploys the Citrix Workspace app) uses port 444. Then, one FQDN resolves to the same IP address. For this work around, you might need to configure StoreFront to return an ICA file for port 444, instead of the default, port 443. This workaround doesn't require users to enter a port number.

### Citrix Gateway time-outs

Decision detail:

- How do you want to configure the Citrix Gateway time-outs for Endpoint Management traffic?

Design guidance:

Citrix Gateway includes the settings Session time-out and Forced time-out. For details, see [Recommended configurations](#). Keep in mind that there are different time-out values for background services, Citrix Gateway, and for accessing applications while offline.

### Enrollment FQDN

#### Important:

To change the enrollment FQDN requires a new SQL Server database and an Endpoint Management server rebuild.

### Secure Web traffic

Decision detail:

- Will you restrict Secure Web to internal web browsing only?
- Will you enable Secure Web for both internal and external web browsing?

Design guidance:

If you plan to use Secure Web for internal web browsing only, the Citrix Gateway configuration is straightforward. However, if Secure Web can't reach all internal sites by default, you might need to configure firewalls and proxy servers.



If you plan to use Secure Web for both internal and external browsing, you must enable the SNIP to have outbound internet access. IT generally views enrolled devices (using the MDX container) as an extension of the corporate network. Thus, IT typically wants Secure Web connections to come back to Citrix Gateway, go through a proxy server, and then go out to the Internet. By default, Secure Web access tunnels to the internal network. Secure Web uses a per-application VPN tunnel back to the internal network for all network access and Citrix Gateway uses split tunnel settings.

For a discussion of Secure Web connections, see [Configuring User Connections](#).

### **Push Notifications for Secure Mail**

Decision detail:

- Will you use push notifications?

Design guidance for iOS:

If your Citrix Gateway configuration includes Secure Ticket Authority (STA) and split tunneling is off: Citrix Gateway must allow traffic from Secure Mail to the Citrix listener service URLs. Those URLs are specified in push notifications for Secure Mail for iOS.

Design guidance for Android:

Use Firebase Cloud Messaging (FCM) to control how and when Android devices need to connect to Endpoint Management. With FCM configured, any security action or deploy command triggers a push notification to Secure Hub to prompt the user to reconnect to the Endpoint Management server.

### **HDX STAs**

Decision detail:

- What STAs to use if you will integrate HDX application access?

Design guidance:

HDX STAs must match the STAs in StoreFront and must be valid for the Virtual Apps and Desktops site.

### **Citrix Files and Citrix Content Collaboration**

Decision detail:

- Will you use storage zones controller in the environment?
- What Citrix Files VIP URL will you use?

Design guidance:

If you will include storage zones controller in your environment, ensure that you correctly configure the following:

- Citrix Files Content Switch VIP (used by the Citrix Files Control Plane to communicate with the storage zones controller servers)
- Citrix Files Load Balancing VIPs
- All required policies and profiles

For information, see the documentation for [Storage zones controller](#).

### **SAML IdP**

#### **Decision detail:**

- If SAML is required for Citrix Files, do you want to use Endpoint Management as the SAML IdP?

#### **Design guidance:**

The recommended best practice is to integrate Citrix Files with Endpoint Management, a simpler alternative to configuring SAML-based federation. Endpoint Management provides Citrix Files with:

- Single sign-on (SSO) authentication of Citrix mobile productivity apps users
- User account provisioning based on Active Directory
- Comprehensive access control policies.

The Endpoint Management console enables you to perform Citrix Files configuration and to monitor service levels and license usage.

There are two types of Citrix Files clients: Citrix Files for Endpoint Management (also known as wrapped Citrix Files) and Citrix Files mobile clients (also known as unwrapped Citrix Files). To understand the differences, see [How Citrix Files for Endpoint Management Clients differ from Citrix Files mobile clients](#).

You can configure Endpoint Management and Citrix Files to use SAML to provide SSO access to:

- Citrix Files apps that are MAM SDK enabled or wrapped by using the MDX Toolkit
- Non-wrapped Citrix Files clients, such as the website, Outlook plug-in, or sync clients

If you want to use Endpoint Management as the SAML IdP for Citrix Files, ensure that the proper configurations are in place. For details, see [SAML for SSO with Citrix Files](#).

### **ShareConnect direct connections**

#### **Decision detail:**

- Will users access a host computer from a computer or mobile device running ShareConnect using direct connections?

#### **Design guidance:**

ShareConnect enables users to connect securely to their computers through iPads, Android tablets, and Android phones to access their files and applications. For direct connections, Endpoint Management uses Citrix Gateway to provide secure access to resources outside of the local network. For configuration details, see [ShareConnect](#).

### Enrollment FQDN for each management mode

Management mode	Enrollment FQDN
MDM+MAM with mandatory MDM enrollment	Endpoint Management server FQDN
MDM+MAM with optional MDM enrollment	Endpoint Management server FQDN or Citrix Gateway FQDN
MAM-only	Endpoint Management server FQDN
MAM-only (legacy)	Citrix Gateway FQDN

### Deployment Summary

If you have multiple Endpoint Management instances, such as for test, development, and production environments, you must configure Citrix Gateway for the additional environments manually. When you have a working environment, take note of the settings before attempting to configure Citrix Gateway manually for Endpoint Management.

A key decision is whether to use HTTPS or HTTP for communication to the Endpoint Management server. HTTPS provides secure back-end communication, as traffic between Citrix Gateway and Endpoint Management is encrypted. The re-encryption impacts Endpoint Management server performance. HTTP provides better Endpoint Management server performance. Traffic between Citrix Gateway and Endpoint Management is not encrypted. The following tables show the HTTP and HTTPS port requirements for Citrix Gateway and Endpoint Management.

### HTTPS

Citrix typically recommends SSL Bridge for Citrix Gateway MDM virtual server configurations. For Citrix Gateway SSL Offload use with MDM virtual servers, Endpoint Management supports only port 80 as the back-end service.

Management mode	Citrix Gateway load balancing method	SSL re-encryption	Endpoint Management server port
MAM	SSL Offload	Enabled	8443
MDM+MAM	MDM: SSL Bridge	N/A	443, 8443
MDM+MAM	MAM: SSL Offload	Enabled	8443

## HTTP

Management mode	Citrix Gateway load balancing method	SSL re-encryption	Endpoint Management server port
MAM	SSL Offload	Enabled	8443
MDM+MAM	MDM: SSL Offload	Not supported	80
MDM+MAM	MAM: SSL Offload	Enabled	8443

For diagrams of Citrix Gateway in Endpoint Management deployments, see [Architecture](#).

## SSO and proxy considerations for MDX apps

November 9, 2020

Endpoint Management integration with Citrix Gateway enables you to provide users with single sign-on (SSO) to all back end HTTP/HTTPS resources. Depending on your SSO authentication requirements, you can configure user connections for an MDX app to use either of these options:

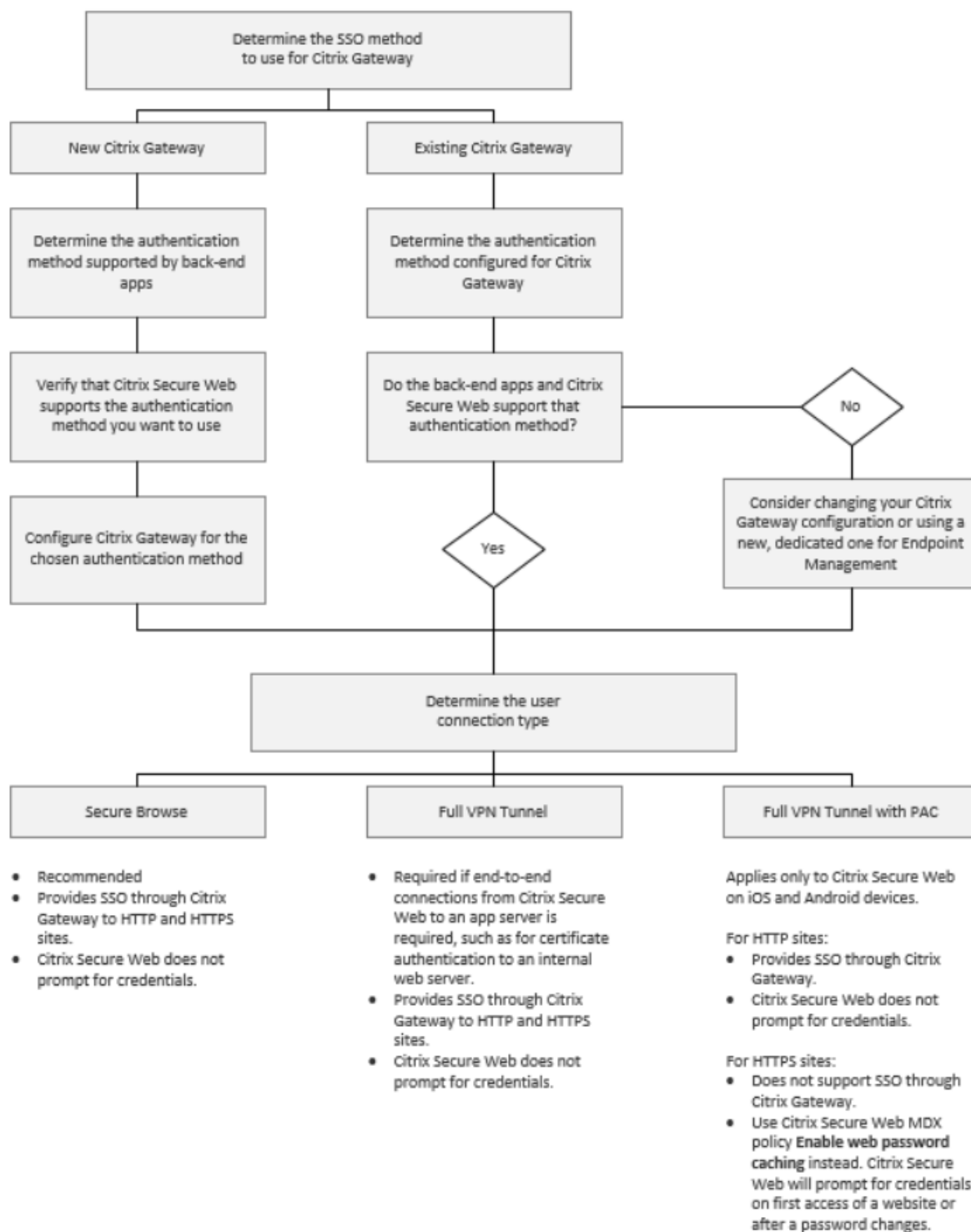
- Secure Browse (Tunneled - Web SSO), which is a type of clientless VPN
- Full VPN Tunnel (not available for Citrix Mobile productivity apps for iOS)

### Important:

Citrix deprecated support for a full VPN tunnel and a Proxy Automatic Configuration (PAC) file with a full VPN tunnel deployment for iOS and Android devices. For more information, see [Deprecation](#).

If Citrix Gateway isn't the best way to provide SSO in your environment, you can set up an MDX app with policy-based local password caching. This article explores the various SSO and proxy options, with a focus on Secure Web. The concepts apply to other MDX apps.

The following flow chart summarizes the decision flow for SSO and user connections.



## Citrix Gateway authentication methods

This section provides general information about the authentication methods supported by Citrix Gateway.

### SAML authentication

When you configure Citrix Gateway for Security Assertion Markup Language (SAML), users can connect to web apps that support the SAML protocol for single sign-on. Citrix Gateway supports the identity provider (IdP) single sign-on for SAML web apps.

Required configuration:

- Configure SAML SSO in the Citrix Gateway Traffic profile.
- Configure the SAML IdP for the requested service.

### NTLM authentication

If SSO to web apps is enabled in the session profile, Citrix Gateway performs NTLM authentication automatically.

Required configuration:

- Enable SSO in the Citrix Gateway Session or Traffic profile.

### Kerberos impersonation

Endpoint Management supports Kerberos for Secure Web only. When you configure Citrix Gateway for Kerberos SSO, Citrix Gateway uses impersonation when a user password is available to Citrix Gateway. Impersonation means that Citrix Gateway uses user credentials to get the ticket required to gain access to services, such as Secure Web.

Required configuration:

- Configure the Citrix Gateway [Worx](#) Session policy to allow it to identify the Kerberos Realm from your connection.
- Configure a Kerberos Constrained Delegation (KCD) account on Citrix Gateway. Configure that account with no password and bind it to a traffic policy on your Endpoint Management gateway.
- For those and other configuration details, see the Citrix blog: [WorxWeb and Kerberos Impersonation SSO](#).

### Kerberos Constrained Delegation

Endpoint Management supports Kerberos for Secure Web only. When you configure Citrix Gateway for Kerberos SSO, Citrix Gateway uses constrained delegation when a user password is not available

to Citrix Gateway.

With constrained delegation, Citrix Gateway uses a specified administrator account to get tickets on behalf of users and services.

Required configuration:

- Configure a KCD account in Active Directory with the required permissions and a KDC account on Citrix Gateway.
- Enable SSO in the Citrix Gateway Traffic profile.
- Configure the back-end website for Kerberos authentication.

### **Form Fill Authentication**

When you configure Citrix Gateway for Form-based single sign-on, users can log on one time to access all protected apps in your network. This authentication method applies to apps that use Tunneled - Web SSO or Full VPN modes.

Required configuration:

- Configure Form-based SSO in the Citrix Gateway Traffic profile.

### **Digest HTTP authentication**

If you enable SSO to web apps in the session profile, Citrix Gateway performs digest HTTP authentication automatically. This authentication method applies to apps that use Tunneled - Web SSO or Full VPN modes.

Required configuration:

- Enable SSO in the Citrix Gateway Session or Traffic profile.

### **Basic HTTP authentication**

If you enable SSO to web apps in the session profile, Citrix Gateway performs basic HTTP authentication automatically. This authentication method applies to apps that use Tunneled - Web SSO or Full VPN modes.

Required configuration:

- Enable SSO in the Citrix Gateway Session or Traffic profile.

### **Secure Tunneled - Web SSO, Full VPN Tunnel, or Full VPN Tunnel with PAC**

The following sections describe the user connection types for Secure Web.

### Full VPN Tunnel

Connections that tunnel to the internal network can use a full VPN tunnel. Use the Secure Web Preferred VPN mode policy to configure full VPN tunnel. Citrix recommends a full VPN tunnel for connections that use client certificates or end-to-end SSL to a resource in the internal network. A full VPN tunnel handles any protocol over TCP.

You can use a full VPN tunnel with Windows and Mac devices. Full VPN isn't available for Citrix Mobile productivity apps for iOS.

In Full VPN Tunnel mode, Citrix Gateway does not have visibility inside an HTTPS session.

### Tunneled - Web SSO

Connections that tunnel to the internal network can use a variation of a clientless VPN, referred to as Tunneled - Web SSO. Tunneled - Web SSO is the default configuration specified for the Secure Web **Preferred VPN mode** policy. Citrix recommends Tunneled - Web SSO for connections that require single sign-on (SSO).

In Tunneled - Web SSO mode, Citrix Gateway breaks the HTTPS session into two parts:

- From the client to Citrix Gateway
- From Citrix Gateway to the back-end resource server.

In this manner, Citrix Gateway has full visibility into all transactions between the client and server, enabling it to provide SSO.

You can also configure proxy servers for Secure Web when used in Tunneled - Web SSO mode. For details, see the blog [Endpoint Management WorxWeb Traffic Through Proxy Server in Secure Browse Mode](#).

### Full VPN Tunnel with PAC

**Note:**

Citrix announced the deprecation of Full VPN tunnel with PAC. See [Deprecation](#).

Endpoint Management supports proxy authentication provided by Citrix Gateway. A PAC file contains rules that define how web browsers select a proxy to access a given URL. PAC file rules can specify handling for both internal and external sites. Secure Web parses PAC file rules and sends the proxy server information to Citrix Gateway. Citrix Gateway is unaware of the PAC file or proxy server.

For authentication to HTTPS websites: The Secure Web MDX policy, **Enable web password caching**, enables Secure Web to authenticate and provide SSO to the proxy server through MDX.



## Citrix Gateway Split Tunneling

When planning your SSO and proxy configuration, you must also decide whether to use Citrix Gateway split tunneling. Citrix recommends that you use Citrix Gateway split tunneling only if needed. This section provides a high-level look at how split tunneling works: Citrix Gateway determines the traffic path based on its routing table. When Citrix Gateway split tunneling is on, Secure Hub distinguishes internal (protected) network traffic from Internet traffic. Secure Hub makes that determination based on the DNS suffix and Intranet applications. Secure Hub then tunnels only the internal network traffic through the VPN tunnel. When Citrix Gateway split tunneling is off, all traffic goes through the VPN tunnel.

- If you prefer to monitor all the traffic due to security considerations, disable Citrix Gateway split tunneling. As a result, all traffic goes through the VPN tunnel.
- If you use Full VPN Tunnel with PAC, you must disable Citrix Gateway split tunneling. If split tunneling is on and you configure a PAC file, the PAC file rules override the Citrix Gateway split tunneling rules. A proxy server configured in a traffic policy does not override the Citrix Gateway split tunneling rules.

Citrix Gateway also has a micro VPN reverse split tunnel mode. This configuration supports an exclusion list of IP addresses that aren't tunneled to the Citrix Gateway. Instead, those addresses are sent by using the device internet connection. For more information about reverse split tunneling, see the Citrix Gateway documentation.

Endpoint Management includes a **Reverse split tunnel exclusion list**. To prevent certain websites from tunneling through Citrix Gateway: Add a comma-separated list of fully qualified domain names (FQDN) or DNS suffixes that connect by using the LAN instead. This list applies only to Tunneled - Web SSO mode with Citrix Gateway configured for reverse split tunneling.

## Authentication

October 7, 2021

In an Endpoint Management deployment, several considerations come into play when deciding how to configure authentication. This section describes the various factors that affect authentication:

- The main MDX policies, Endpoint Management client properties, and Citrix Gateway settings involved with authentication.
- The ways these policies, client properties, and settings interact.
- The tradeoffs of each choice.

This article also includes three examples of recommended configurations for increasing degrees of security.

Broadly speaking, stronger security results in a less-optimal user experience, because users have to authenticate more often. How you balance those concerns depends on your organization's needs and priorities. Review the three recommended configurations to understand the interplay of the various authentication options.

## Authentication Modes

**Online authentication:** Allows users into the Endpoint Management network. Requires an Internet connection.

**Offline authentication:** Happens on the device. Users unlock the secure vault and have offline access to items, such as downloaded mail, cached websites, and notes.

## Methods of Authentication

### Single Factor

**LDAP:** You can configure a connection in Endpoint Management to one or more directories that are compliant with the Lightweight Directory Access Protocol (LDAP). This method is commonly used to provide single sign-on (SSO) for company environments. You might opt for Citrix PIN with Active Directory password caching to improve the user experience with LDAP. At the same time, you can provide the security of complex passwords on enrollment, password expiration, and account lockout.

For more details, see [Domain or domain plus security token authentication](#).

**Client certificate:** Endpoint Management can integrate with industry-standard certificate authorities to use certificates as the sole method of online authentication. Endpoint Management provides this certificate after user enrollment, which requires either a one-time password, invitation URL, or LDAP credentials. When using a client certificate as the primary method of authentication, a Citrix PIN is required in client certificate-only environments to secure the certificate on the device.

Endpoint Management supports Certificate Revocation List (CRL) only for a third-party Certificate Authority. If you have a Microsoft CA configured, Endpoint Management uses Citrix Gateway to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the Citrix Gateway Certificate Revocation List (CRL) setting, Enable CRL Auto Refresh. This step ensures that a device enrolled only in MAM can't authenticate using an existing certificate on the device. Endpoint Management reissues a new certificate, because it doesn't restrict a user from generating a user certificate if one is revoked. This setting increases the security of PKI entities when the CRL checks for expired PKI entities.

For a diagram that shows the deployment needed for certificate-based authentication or the use of your enterprise Certificate Authority (CA) to issue device certificates, see [Architecture](#).

## Two-factor authentication

**LDAP + Client Certificate:** This configuration is the best combination of security and user experience for Endpoint Management. Using both LDAP and client certificate authentication:

- Has the best SSO possibilities coupled with security provided by two-factor authentication at the Citrix Gateway.
- Provides security with something users know (their Active Directory passwords) and something they have (client certificates on their devices).

Secure Mail can automatically configure and provide a seamless first-time user experience with client certificate authentication. That feature requires a properly configured Exchange client access server environment.

For optimal usability, you can combine LDAP and client certificate authentication with Citrix PIN and Active Directory password caching.

**LDAP + Token:** This configuration allows for the classic configuration of LDAP credentials, plus a one-time password, using the RADIUS protocol. For optimal usability, you can combine this option with Citrix PIN and Active Directory password caching.

## Important policies, settings, and client properties for authentication

The following policies, settings, and client properties come into play with the following three recommended configurations:

### MDX policies

**App passcode:** If **On**, a Citrix PIN or passcode is required to unlock the app when it starts or resumes after a period of inactivity. Default is **On**.

To configure the inactivity timer for all apps, set the `INACTIVITY_TIMER` value in minutes in the Endpoint Management console in **Client Properties** on the **Settings** tab. The default is 15 minutes. To disable the inactivity timer, so that a PIN or passcode prompt appears only when the app starts, set the value to zero.

**micro VPN session required:** If **On**, the user must have a connection to the enterprise network and an active session to access the app on the device. If **Off**, an active session is not required to access the app on the device. Default is **Off**.

**Maximum offline period (hours):** Defines the maximum period an app can run without reconfirming app entitlement and refreshing policies from Endpoint Management. When the following conditions are met, an iOS app retrieves new policies for MDX apps from Endpoint Management without any interruption to users:

- You set the Maximum offline period and

- Secure Hub for iOS has a valid Citrix Gateway token.

If Secure Hub doesn't have a valid Citrix Gateway token, users must authenticate through Secure Hub before app policies can update. The Citrix Gateway token can become invalid due to Citrix Gateway session inactivity or a forced session time-out policy. When users sign on to Secure Hub again, they can continue running the app.

Users are reminded to sign on at 30, 15, and 5 minutes before the period expires. After expiration, the app is locked until users sign on. Default is **72 hours (3 days)**. Minimum period is 1 hour.

**Note:**

Keep in mind that in a scenario in which users travel often and use international roaming, the default of 72 hours (3 days) might be too short.

**Background services ticket expiration:** The time period that a background network service ticket remains valid. When Secure Mail connects through Citrix Gateway to an Exchange Server running ActiveSync, Endpoint Management issues a token. Secure Mail uses that token to connect to the internal Exchange Server. This property setting determines the duration that Secure Mail can use the token without requiring a new token for authentication and the connection to the Exchange Server. When the time limit expires, users must log on again to generate a new token. Default is **168 hours (7 days)**. When this time-out expires, mail notifications discontinue.

**micro VPN session required grace period:** Determines how many minutes a user can use the app offline until the online session is validated. The default is **0** (no grace period).

For information about authentication policies, see:

- If you use the MAM SDK: [MAM SDK overview](#)
- If you use the MDX Toolkit: [Endpoint Management MDX Policies for iOS](#) and [Endpoint Management MDX Policies for Android](#)

### Endpoint Management client properties

**Note:**

Client properties are global settings that apply to all devices that connect to Endpoint Management.

**Citrix PIN:** For a simple sign-on experience, you might choose to enable the Citrix PIN. With the PIN, users do not have to enter other credentials repeatedly, such as their Active Directory user names and passwords. You can configure the Citrix PIN as a standalone offline authentication only, or combine the PIN with Active Directory password caching to streamline authentication for optimal usability. You configure the Citrix PIN in **Settings > Client > Client Properties** in the Endpoint Management console.

Following is a summary of a few important properties. For more information, see [Client properties](#).

ENABLE\_PASSCODE\_AUTH

**Display name:** Enable Citrix PIN Authentication

This key allows you to turn on Citrix PIN functionality. With the Citrix PIN or passcode, users are prompted to define a PIN to use instead of their Active Directory password. Enable this setting if **ENABLE\_PASSWORD\_CACHING** is enabled or if Endpoint Management is using certificate authentication.

**Possible values:** **true** or **false**

**Default value:** **false**

ENABLE\_PASSWORD\_CACHING

**Display name:** Enable User Password Caching

This key lets you allow the users' Active Directory password to be cached locally on the mobile device. When you set this key to true, users are prompted to set a Citrix PIN or passcode. The **ENABLE\_PASSCODE\_AUTH** key must be set to true when you set this key to **true**.

**Possible values:** **true** or **false**

**Default value:** **false**

PASSCODE\_STRENGTH

**Display name:** PIN Strength Requirement

This key defines the strength of the Citrix PIN or passcode. When you change this setting, users are prompted to set a new Citrix PIN or passcode the next time they are prompted to authenticate.

**Possible values:** **Low**, **Medium**, or **Strong**

**Default value:** **Medium**

INACTIVITY\_TIMER

**Display name:** Inactivity timer

This key defines the time in minutes that users can leave their devices inactive and then access an app without being prompted for a Citrix PIN or passcode. To enable this setting for an MDX app, you must set the App Passcode setting to **On**. If the App Passcode setting is set to **Off**, users are redirected to Secure Hub to perform a full authentication. When you change this setting, the value takes effect the next time users are prompted to authenticate. The default is 15 minutes.

ENABLE\_TOUCH\_ID\_AUTH

**Display name:** Enable Touch ID Authentication

Allows the use of the fingerprint reader (in iOS only) for offline authentication. Online authentication still requires the primary authentication method.

ENCRYPT\_SECRETS\_USING\_PASSCODE

**Display name:** Encrypt secrets using Passcode

This key lets sensitive data be stored on the mobile device in a secret vault instead of in a platform-based native store, such as the iOS keychain. This configuration key enables strong encryption of key artifacts, but also adds user entropy (a user-generated random PIN code that only the user knows).

**Possible values:** **true** or **false**

**Default value:** **false**

### Citrix Gateway Settings

**Session time-out:** If you enable this setting, Citrix Gateway disconnects the session if Citrix Gateway detects no network activity for the specified interval. This setting is enforced for users who connect with the Citrix Gateway Plug-in, Citrix Workspace, Secure Hub, or through a web browser. Default is **1440 minutes**. If you set this value to zero, the setting is disabled.

**Forced time-out:** If you enable this setting, Citrix Gateway disconnects the session after the time-out interval elapses no matter what the user is doing. When the time-out interval elapses, there is no action the user can take to prevent the disconnection. This setting is enforced for users who connect with the Citrix Gateway Plug-in, Citrix Workspace, Secure Hub, or through a web browser. If Secure Mail is using STA, a special Citrix Gateway mode, this setting doesn't apply to Secure Mail sessions. Default is no value, which means sessions are extended for any activity.

For more information about time-out settings for Citrix Gateway, see the Citrix Gateway documentation.

For more information on the scenarios that prompt users to authenticate with Endpoint Management by entering credentials on their devices, see [Authentication Prompt Scenarios](#).

### Default configuration settings

These settings are the defaults provided by the:

- NetScaler for XenMobile wizard
- MAM SDK or MDX Toolkit
- Endpoint Management console

---

Setting	Where to Find the Setting	Default Setting
Session time-out	Citrix Gateway	1440 minutes
Forced time-out	Citrix Gateway	No value (off)
Maximum offline period	MDX Policies	72 hours

Setting	Where to Find the Setting	Default Setting
Background services ticket expiration	MDX Policies	168 hours (7 days)
micro VPN session required	MDX Policies	Off
micro VPN session required grace period	MDX Policies	0
App passcode	MDX Policies	On
Encrypt secrets using passcode	Endpoint Management client properties	false
Enable Citrix PIN Authentication	Endpoint Management client properties	false
PIN Strength Requirement	Endpoint Management client properties	Medium
PIN Type	Endpoint Management client properties	Numeric
Enable User Password Caching	Endpoint Management client properties	false
Inactivity Timer	Endpoint Management client properties	15
Enable Touch ID Authentication	Endpoint Management client properties	false

## Recommended Configurations

This section gives examples of three Endpoint Management configurations that range from the lowest security and optimal user experience to the highest security and more intrusive user experience. These examples provide you with helpful reference points to determine where on the scale you want to place your own configuration. Modifying these settings might require you to alter other settings. For instance, the maximum offline period must not exceed the session time-out.

### Highest Security

This configuration offers the highest level of security but contains significant usability trade-offs.

<b>Setting</b>	<b>Where to Find the Setting</b>	<b>Recommended Setting</b>	<b>Behavior Impact</b>
Session time-out	Citrix Gateway	1440	Users enter their Secure Hub credentials only when online authentication is required-every 24 hours.
Forced time-out	Citrix Gateway	No value	Sessions are extended if there's any activity.
Maximum offline period	MDX Policies	23	Requires policy refresh every day.
Background services ticket expiration	MDX Policies	72 hours	Time out for STA, which allows for long-lived sessions without a Citrix Gateway session token. For Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop. In that case, Secure Mail doesn't prompt the user if they don't open the app before the session expires.
micro VPN session required	MDX Policies	Off	Ensures a valid network connection and Citrix Gateway session to use apps.



micro VPN session required grace period	MDX Policies	0	No grace period (if you enabled micro VPN session required).
App passcode	MDX Policies	On	Require a passcode for an application.
Encrypt secrets using passcode	Endpoint Management client properties	true	A key derived from user entropy protects the vault.
Enable Citrix PIN Authentication	Endpoint Management client properties	true	Enable Citrix PIN for simplified authentication experience.
PIN Strength Requirement	Endpoint Management client properties	Strong	High password complexity requirements.
PIN Type	Endpoint Management client properties	Alphanumeric	PIN is an alphanumeric sequence.
Enable Password Caching	Endpoint Management client properties	false	Active Directory password is not cached and a Citrix PIN is used for offline authentications.
Inactivity Timer	Endpoint Management client properties	15	If a user doesn't use MDX apps or Secure Hub for this period, prompt for offline authentication.
Enable Touch ID Authentication	Endpoint Management client properties	false	Disables Touch ID for offline authentication use cases in iOS.

## Higher Security

A more middle-of-the-road approach, this configuration requires users to authenticate more often - every 3 days, at most, instead of 7 - and stronger security. The increased number of authentications lock the container more often, ensuring data security when devices aren't in use.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Session time-out	Citrix Gateway	4320	Users enter their Secure Hub credentials only when online authentication is required - every 3 days
Forced time-out	Citrix Gateway	No value	Sessions are extended if there's any activity.
Maximum offline period	MDX Policies	71	Requires policy refresh every 3 days. The hour difference is to allow for refresh ahead of session time-out.
Background services ticket expiration	MDX Policies	168 hours	Time out for STA, which allows for long-lived sessions without a Citrix Gateway session token. For Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop without prompting the user.

micro VPN session required	MDX Policies	Off	Ensures a valid network connection and Citrix Gateway session to use apps.
micro VPN session required grace period	MDX Policies	0	No grace period (if you enabled micro VPN session required).
App passcode	MDX Policies	On	Require a passcode for an application.
Encrypt secrets using passcode	Endpoint Management client properties	false	Do not require user entropy to encrypt the vault.
Enable Citrix PIN Authentication	Endpoint Management client properties	true	Enable Citrix PIN for simplified authentication experience.
PIN Strength Requirement	Endpoint Management client properties	Medium	Enforces medium password complexity rules.
PIN Type	Endpoint Management client properties	Numeric	PIN is a numeric sequence.
Enable Password Caching	Endpoint Management client properties	true	The user PIN caches and protects the Active Directory password.
Inactivity Timer	Endpoint Management client properties	30	If a user doesn't use MDX apps or Secure Hub for this period, prompt for offline authentication.
Enable Touch ID Authentication	Endpoint Management client properties	true	Enables Touch ID for offline authentication use cases in iOS.

## High Security

This configuration, the most convenient to users, provides base-level security.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Session time-out	Citrix Gateway	10080	Users enter their Secure Hub credentials only when online authentication is required - every 7 days
Forced time-out	Citrix Gateway	No value	Sessions are extended if there's any activity.
Maximum offline period	MDX Policies	167	Requires policy refresh every week (every 7 days). The hour difference is to allow for refresh ahead of session time-out.
Background services ticket expiration	MDX Policies	240	Time out for STA, which allows for long-lived sessions without a Citrix Gateway session token. For Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop. In that case, Secure Mail doesn't prompt the user if they don't open the app before the session expires.

micro VPN session required	MDX Policies	Off	Ensures a valid network connection and Citrix Gateway session to use apps.
micro VPN session required grace period	MDX Policies	0	No grace period (if you enabled micro VPN session required).
App passcode	MDX Policies	On	Require a passcode for an application.
Encrypt secrets using passcode	Endpoint Management client properties	false	Do not require user entropy to encrypt the vault.
Enable Citrix PIN Authentication	Endpoint Management client properties	true	Enable Citrix PIN for simplified authentication experience.
PIN Strength Requirement	Endpoint Management client properties	Low	No password complexity requirements
PIN Type	Endpoint Management client properties	Numeric	PIN is a numeric sequence.
Enable Password Caching	Endpoint Management client properties	true	The user PIN caches and protects the Active Directory password.
Inactivity Timer	Endpoint Management client properties	90	If a user doesn't use MDX apps or Secure Hub for this period, prompt for offline authentication.
Enable Touch ID Authentication	Endpoint Management client properties	true	Enables Touch ID for offline authentication use cases in iOS.

### Using Step-Up Authentication

Some apps might require enhanced authentication. For example, a secondary authentication factor, such as a token or aggressive session time-outs. You control this authentication method through an MDX policy. The method also requires a separate virtual server to control the authentication methods (on either the same or on separate Citrix Gateway appliances).

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Alternate Citrix Gateway	MDX Policies	Requires the FQDN and port of the secondary Citrix Gateway appliance.	Allows for enhanced authentication controlled by the secondary Citrix Gateway appliance authentication and session policies.

If a user opens an app that uses the alternate Citrix Gateway, all other apps use that Citrix Gateway instance to communicate with the internal network. The session only switches back to the lower security Citrix Gateway instance when the session times out from the Citrix Gateway instance with enhanced security.

### Using micro VPN session required

For certain applications, such as Secure Web, you can ensure that users run an app only when they have an authenticated session. This policy enforces that option and allows for a grace period so users can finish their work.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
micro VPN session required	MDX Policies	On	Ensures a device is online and has a valid authentication token.
micro VPN session required grace period	MDX Policies	15	Allows a 15-minute grace period before the user can no longer use apps

## Server properties

June 29, 2021

Server properties are global properties that apply to operations, users, and devices across an entire Endpoint Management instance. Citrix recommends that you evaluate for your environment the server properties covered in this article. Be sure to consult with Citrix before changing other server properties.

To update server properties, go to **Settings > Server Properties**.

### Adding, Editing, or Deleting Server Properties

In Endpoint Management, you can apply properties to the server.

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Server**, click **Server Properties**. The **Server Properties** page appears. You can add, edit, or delete server properties from this page.

Settings > Server Properties

### Server Properties

You must restart XenMobile on all nodes to commit and activate your changes to the server properties. To restart XenMobile, use the command prompt through your hypervisor.

<input type="checkbox"/>	Display name	Key	Value	Default value	Description
<input type="checkbox"/>	NetScaler Gateway Client Cert Issuing Throttling Interval	ag.client.cert.throttling.minutes	30	30	Throttling interval for issuance of NetScaler Gateway client certificates.
<input type="checkbox"/>	Number of consecutive failed uploads.	ceip.consecutive.upload.failures	0	0	
<input type="checkbox"/>	Sharefile byPath API fields	com.citrix.sharefile.bypath.fields	odata.metadata, id, url	odata.metadata, id, url	Comma separated set of fields (case-sensitive) that need to be extracted from the complete sharefile byPath API response
<input type="checkbox"/>	Sharefile configuration type : ENTERPRISE/CONNECTORS/NONE	com.citrix.sharefile.config.type	ENTERPRISE	NONE	Sharefile configuration type. Possible values being ENTERPRISE or CONNECTORS or NONE
<input type="checkbox"/>	Connection Timeout	CONNECTION_TIMEOUT	5	5	Session inactivity timeout, in minutes, after which the TCP connection to a device will be closed (by default 5 minutes).
<input type="checkbox"/>	Identifies if telemetry is enabled or not.	console.ceip.participate	true	false	
<input type="checkbox"/>	Length of Inactivity Before Device Is Disconnected	device.inactivity.days.threshold	7	7	Length of inactivity (in days) before the device is disconnected.
<input type="checkbox"/>	User-Defined Device Properties 1	device.properties.userDefined1			User-defined device properties.
<input type="checkbox"/>	User-Defined Device Properties 2	device.properties.userDefined2			User-defined device properties.
<input type="checkbox"/>	User-Defined Device Properties 3	device.properties.userDefined3			User-defined device properties.

Showing 1 - 10 of 111 items Showing 1 of 12

### To add a server property

1. Click **Add**. The **Add New Server Property** page appears.

Settings > Server Properties > Add New Server Property

### Add New Server Property

Key  ?

Value\*

Display name\*

Description

Cancel Save

2. Configure these settings:

- Key: In the list, select the appropriate key. Keys are case-sensitive. Contact Citrix Support before you edit property values or to request a special key.
- Value: Enter a value depending on the key you selected.
- Display Name: Enter a name for the new property value that appears in the **Server Properties** table.
- Description: Optionally, type a description for the new server property.

3. Click **Save**.

### To edit a server property

1. In the **Server Properties** table, select the server property you want to edit.

When you select the check box next to a server property, the options menu appears above the server property list. Click anywhere else in the list to open the options menu on the right side of the listing.

2. Click **Edit**. The **Edit New Server Property** page appears.



Settings > Server Properties > Edit New Server Property

### Edit New Server Property

**Key** ag.client.cert.throttling.mi

**Value\*** 30

**Display name\*** NetScaler Gateway Client

**Description** Throttling interval for issuance of NetScaler Gateway client certificates.

Cancel Save

3. Change the following information as appropriate:

- **Key:** You cannot change this field.
- **Value:** The property value.
- **Display Name:** The property name.
- **Description:** The property description.

4. Click **Save** to save your changes or **Cancel** to leave the property unchanged.

### To delete a server property

1. In the **Server Properties** table, select the server properties you want to delete.
2. Click **Delete**. A confirmation dialog box appears. Click **Delete** again.

## Server Property Definitions

### Access all apps in the managed Google Play store

- If **true**, Endpoint Management makes all apps from the public Google Play store accessible from the managed Google Play store. You can use the [Restrictions device policy](#) to control access to these apps. Defaults to **false**.

### Add Device Always

- If **true**, Endpoint Management adds a device to the Endpoint Management console, even if it fails enrollment. As a result, you can see which devices attempted to enroll. Defaults to **false**.

### **AG Client Cert Issuing Throttling Interval**

- The grace period between generating certificates. This interval prevents Endpoint Management from generating multiple certificates for a device in a short time period. Citrix recommends that you don't change this value. Defaults to **30** minutes.

### **Audit Logger**

- If **False**, does not log user interface (UI) events. Defaults to **False**.

### **Block Enrollment of Rooted Android and Jailbroken iOS Devices**

When this property is **true**, Endpoint Management blocks enrollments for rooted Android devices and jailbroken iOS devices. Recommended setting is **true** for all security levels. Defaults to **true**.

### **cdn.s3.retry.interval and cdn.s3.max.retry**

The `cdn.s3.retry.interval` and `cdn.s3.max.retry` server properties work together to set the maximum time limit on every macOS PKG file upload. By default, Endpoint Management limits file upload times to 100 seconds. If a file upload exceeds that limit, the upload fails. To change the default, configure the `cdn.s3.retry.interval` and `cdn.s3.max.retry` keys as follows:

- `cdn.s3.retry.interval`. Lets you define the interval, in milliseconds, at which Endpoint Management verifies whether a file upload completes successfully. The default is 10000.
- `cdn.s3.max.retry`. Lets you define the maximum number of verification retries after which the upload fails. The default is 10.

The two keys work together to limit file upload times. By default, the time limit is 100 seconds (10000\*10 milliseconds).

### **Certificate Renewal in Seconds**

- The number of seconds before a certificate expires that Endpoint Management starts to renew certificates. An example is when a certificate expires on December 30 and this property is set to 30 days. If the device connects between December 1 and December 30, Endpoint Management attempts to renew the certificate. Defaults to **2592000** seconds (30 days).

### **Connection Timeout**

- The session inactivity timeout, in minutes, after which Endpoint Management closes the TCP connection to a device. The session remains open. Applies to Android devices. Defaults to **5** minutes.

### Default deployment channel

- Determines how Endpoint Management deploys a resource to a device: At the user-level (**DEFAULT\_TO\_USER**) or device-level. Defaults to **DEFAULT\_TO\_DEVICE**.

### Device tagging

- If you set `enable.device.tagging` to **true**, Endpoint Management tags devices by device type automatically. You can use device tags to deploy policies and apps or configure delivery groups. Endpoint Management applies tags to devices for the following:
  - BYOD tags
    - \* iOS User Enrollment
    - \* Android Enterprise work profile
  - Corporate tags
    - \* Android Enterprise fully managed corporate devices
    - \* Bulk enrollment
      - Apple Business Manager devices
      - Apple School Manager devices
      - Windows AutoPilot devices
      - Android Enterprise bulk enrollment

### Disable Hostname Verification

- By default, hostname verification is enabled on outgoing connections except for the Microsoft PKI server. When hostname verification fails, the server log includes errors such as: “Unable to connect to the volume purchase Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer”. If hostname verification breaks your deployment, change this property to **true**. Defaults to **false**.

### Disable SSL Server Verification

- If **True**, disables SSL server certificate validation when all the following conditions are met:
  - You enabled certificate-based authentication on Endpoint Management
  - The Microsoft CA server is the certificate issuer
  - An internal CA, whose root Endpoint Management doesn't trust, signed your certificate.

Defaults to **True**.

### Enable Crash Reporting

- If **true**, Citrix collects crash reports and diagnostics to help troubleshoot issues with Secure Hub for iOS and Android. If **false**, no data is collected. Default value is **true**.

### Enable/Disable Hibernate statistics logging for diagnostics

- If **True**, enables Hibernate statistics logging to assist with troubleshooting application performance issues. Hibernate is a component used for Endpoint Management connections to a Microsoft SQL Server. By default, the logging is disabled because it impacts application performance. Enable logging only for a short duration to avoid creating a huge log file. Endpoint Management writes the logs to `/opt/sas/logs/hibernate_stats.log`. Defaults to **False**.

### Enable macOS OTAE

- If **false**, prevents the use of an enrollment link for macOS devices, meaning macOS users can enroll only by using an enrollment invitation. Defaults to **true**.

### Enable Notification Trigger

- Enables or disables Secure Hub client notifications. The value **true** enables notifications. Defaults to **true**.

### Full Pull of ActiveSync Allowed and Denied Users

- The interval in (in seconds) that Endpoint Management pulls a complete list (baseline) of ActiveSync allowed and denied users. Defaults to **28800** seconds.

### Identifies if telemetry is enabled or not

- Identifies if telemetry is enabled. Telemetry is also referred to as the Customer Experience Improvement Program (CEIP). You can opt in to CEIP when you install or upgrade Endpoint Management. If Endpoint Management has 15 consecutive failed uploads, it disables telemetry. Defaults to **false**.

### Inactivity Timeout in Minutes

- The number of minutes after which Endpoint Management logs out an inactive user. The user must have used the Endpoint Management Public API to access the Endpoint Management console or any third-party app. A time-out value of **0** means that an inactive user remains logged

in. For third-party apps that access the API, remaining logged in is typically necessary. Default is **5**.

- If the **WebServices timeout type** server property is **INACTIVITY\_TIMEOUT**: This property defines the number of minutes after which Endpoint Management logs out an inactive administrator who did the following:
  - Used the Public API for REST Services to access the Endpoint Management console
  - Used the Public API for REST Services to access any third-party app. A timeout of **0** means that an inactive user remains logged in.

### **include.device.properties.during.search**

- Includes all device properties in a device search. The default is **Off**, which limits the search scope to these device properties, for fast searching:
  - Serial Number
  - IMEI
  - Wi-Fi MAC address
  - Bluetooth MAC address
  - Active Sync ID
  - User Name

When this property is **On**, device searches can take longer.

### **ios.delayBeforeDeclareUnreachable; macos.delayBeforeDeclareUnreachable**

- Specifies the number of days after which an offline iOS or macOS device is considered unreachable. When an iOS or macOS device reaches the limit specified, they stop checking back with Endpoint Management. Both properties default to **45** days.

### **iOS Device Management Enrollment Install Root CA if Required**

- The server property **ios.mdm.enrollment.installRootCalfRequired** is set to **False** for all Endpoint Management environments. Endpoint Management uses a publicly trusted certificate chain, thus it isn't necessary to push a root CA to devices. (This property is used only for on-premises environments.)

### **iOS Device Management Enrollment Last Step Delayed**

- During device enrollment, this property value specifies the amount of time to wait between installing the MDM profile and starting the Agent on the device. Citrix recommends that you

edit this property only for network latency or speed issues. In that case, don't set to the value to more than 5000 milliseconds (5 seconds). Defaults to **1000** milliseconds (1 second).

### **iOS Device Management Identity Delivery Mode**

- Specifies whether Endpoint Management distributes the MDM certificate to devices using **SCEP** (recommended for security reasons) or **PKCS12**. In PKCS12 mode, the key pair is generated on the server and no negotiation is performed. Defaults to **SCEP**.

### **iOS Device Management Identity Key Size**

- Defines the size of private keys for MDM identities, iOS profile service, and Endpoint Management iOS agent identities. Defaults to **2048**.

### **iOS Device Management Identity Renewal Days**

- Specifies the number of days before the certificate expiration that Endpoint Management starts renewing certificates. For example: If a certificate expires in 10 days and this property is **10** days: When a device connects 9 days before expiration, Endpoint Management issues a new certificate. Defaults to **30** days.

### **iOS MDM APNS Private Key Password**

- This property contains the APNs password, which is required for Endpoint Management to push notifications to Apple servers.

### **Length of Inactivity Before Device Is Disconnected**

- Specifies how long a device can remain inactive, including the last authentication, before Endpoint Management disconnects it. Defaults to **7** days.

### **local.user.account.lockout.time**

- Specifies the number of minutes a user must wait after exceeding the lockout limit. Supported values are 0–999. The default is **30** minutes.

### **local.user.account.lockout.limit**

- Specifies the maximum number of consecutive invalid login attempts per user. Supported values are 0–999. The default is **6** attempts.

### **mac.dep.admin.passwd.rotate**

This server property lets you configure administrator password rotation intervals for macOS devices enrolled through the Apple Deployment Program. Endpoint Management checks whether to rotate the password of the administrator account daily. By default, Endpoint Management rotates the password every 10,080 minutes (7 days). Configure the `mac.dep.admin.passwd.rotate` key as follows:

- Value: *administrator-defined*  
The interval, in minutes, at which Endpoint Management rotates the password. Type a value equal to or greater than 360 (6 hours). Endpoint Management ignores values smaller than 360 and rotates the password every 360 minutes (6 hours) instead.
- Display name: *administrator-defined*
- Description: *administrator-defined*

### **MAM Only Device Max**

- This Custom Key limits the number of MAM-only devices that each user can enroll. Configure the key as follows. A **Value** of **0** allows unlimited device enrollments.
- Key = **number.of.mam.devices.per.user**
- Value = **5**
- Display name = **MAM Only Device Max**
- Description = **Limits the number of MAM devices each user can enroll.**

### **MaxNumberOfWorker**

- The number of threads used when importing many volume purchase licenses. Defaults to **3**. If you need further optimization, you can increase the number of threads. However, a larger number of threads results in high CPU usage.

### **Citrix Gateway (NetScaler) Single Sign-On**

- If **False**, disables the Endpoint Management callback feature during single sign-on from Citrix Gateway to Endpoint Management. If the Citrix Gateway configuration includes a callback URL, Endpoint Management uses the callback feature to verify the Citrix Gateway session ID. Defaults to **False**.

### **Number of consecutive failed uploads**

- Displays the number of consecutive failures during Customer Experience Improvement Program (CEIP) uploads. Endpoint Management increments the value when an upload fails. After

15 upload failures, Endpoint Management disables CEIP, also called telemetry. For more information, see the server property **Identifies if telemetry is enabled or not**. Endpoint Management resets the value to **0** when an upload succeeds.

### **Number of Users Per Device**

- The maximum number of users who can enroll the same device in MDM. The value **0** means that an unlimited number of users can enroll the same device. Defaults to **0**.

### **optional.user.identity.attributes**

- This server property lets you customize the optional Active Directory user attributes.

Create the custom key and, in the **Values** field, edit user attributes to define which attributes Endpoint Management can access to create a user account. For more information, see [Customize user properties](#).

- Key: **Custom Key**
- Key: **optional.user.identity.attributes**
- Value: **commonName, firstName, lastName, displayName, streetAddress, city, state, country, workPhone, homePhone, mobilePhone, company, department, description, employeeID, faxNumber, initials, ipPhone, manager, homePostalAddress, otherMobile, pager, physicalDeliveryOfficeName, postalCode, postOfficeBox, title, organization, preferredLanguage**
- Display Name: **optional.user.identity.attributes**
- Description: **Optional Active Directory user attributes**

### **Organization Name for macOS and iOS/iPadOS Enrollment Profiles**

- The value you type for `apple.mdm.enrollment.profile.organization.name` corresponds to the name of the organization that provides the enrollment profile. The name displays when users enroll their device to Endpoint Management. The default name that displays is **Citrix Workspace**.

### **Pull of Incremental Change of Allowed and Denied Users**

- The number of seconds that Endpoint Management waits for a response from the domain when running a PowerShell command to get a delta of ActiveSync devices. Defaults to **60** seconds.



### **Read Timeout to Microsoft Certification Server**

- The number of seconds that Endpoint Management waits for a response from the certificate server when performing a read. If the certificate server is slow and has much traffic, you can increase this value to 60 seconds or more. A certificate server that doesn't respond after 120 seconds requires maintenance. Defaults to **15000** milliseconds (15 seconds).

### **REST Web Services**

- Enables the REST Web Service. Defaults to **true**.

### **Retrieves devices information in chunks of specified size**

- This value is used internally for multithreading during device exports. If the value is higher, a single thread parses more devices. If the value is lower, more threads fetch the devices. Reducing the value might increase the performance of exports and device list fetches, yet might reduce available memory. Defaults to **1000**.

### **shp.console.enable**

- If **False**, prevents access to the Self-Help Portal. Users who navigate to the portal on port 4443 get an "Access Denied" message. If **True**, provides access to the Self-Help Portal over port 443. Defaults to **False**.

### **enable.new.shp**

- If **False**, prevents users from enabling their devices from the Self-Help Portal. If **True**, users can enable their devices from the Self-Help Portal.

The BitLocker recovery key feature requires that you set this property to **False** and the `shp.console.enable` property to **True**.

Defaults to **False**.

### **Session Log Cleanup (in Days)**

- The number of days that Endpoint Management retains the session log. Defaults to **7**.

### Content Collaboration configuration type

- Specifies the Citrix Files storage type. **ENTERPRISE** enables Citrix Files Enterprise mode. **CONNECTORS** provides access only to storage zone connectors that you create through the Endpoint Management console. Defaults to **NONE**, which shows the initial view of the **Configure > Citrix Files** screen where you choose between Citrix Files Enterprise and Connectors. Defaults to **NONE**.

### Static Timeout in Minutes

- If the **WebServices timeout type** server property is **STATIC\_TIMEOUT**: This property defines the number of minutes after which Endpoint Management logs out an administrator after using the following:
  - The Public API for REST Services to access the Endpoint Management console.
  - The Public API for REST Services to access any third-party app.

Defaults to **60**.

### Trigger Agent Message Suppression

- Enables or disables Secure Hub client messaging. The value **false** enables messaging. Defaults to **true**.

### Trigger Agent Sound Suppression

- Enables or disables Secure Hub client sounds. The value **false** enables sounds. Defaults to **true**.

### Unauthenticated App Download for Android Devices

- If **True**, you can download self-hosted apps to Android devices running Android Enterprise. Endpoint Management needs this property if the Android Enterprise option to provide a download URL in the Google Play Store statically is enabled. In that case, download URLs can't include a one-time ticket (defined by the **XAM One-Time Ticket server** property) which has the authentication token. Defaults to **False**.

### Unauthenticated App Download for Windows Devices

- Used only for older Secure Hub versions which don't validate one-time tickets. If **False**, you can download unauthenticated apps from Endpoint Management to Windows devices. Defaults to **False**.

### Use ActiveSync ID to Conduct an ActiveSync Wipe Device

- If **true**, Endpoint Management connector for Exchange ActiveSync uses the ActiveSync identifier as an argument for the **asWipeDevice** method. Defaults to **false**.

### Users only from Exchange

- If **true**, disables user authentication for ActiveSync Exchange users. Defaults to **false**.

### Volume purchase baseline interval

- The minimum interval that Endpoint Management reimports volume purchase licenses from Apple. Refreshing license information ensures that Endpoint Management reflects all changes, such as when you manually delete an imported app from volume purchase. By default, Endpoint Management refreshes the volume purchase license baseline a minimum of every **1440** minutes.
  - If you have many volume purchase licenses installed (for example, more than 50,000): Citrix recommends that you increase the baseline interval to reduce the frequency and overhead of importing licenses.
  - If you expect frequent volume purchase license changes from Apple: Citrix recommends that you lower the value to keep Endpoint Management updated with the changes.
  - The minimum interval between two baselines is 60 minutes. In addition, Endpoint Management performs a delta import every 60 minutes, to capture the changes since the last import. Therefore, if the volume purchase baseline interval is 60 minutes, the interval between baselines might be delayed up to 119 minutes.

### WebServices Timeout Type

- Specifies how to expire an authentication token retrieved from the public API.
  - If **STATIC\_TIMEOUT**: Endpoint Management considers a token expired, based on the value of the server property **Static Timeout in Minutes**.
  - If **INACTIVITY\_TIMEOUT**: Endpoint Management considers a token expired, based on the value of the server property **Inactivity Timeout in Minutes**. Defaults to **STATIC\_TIMEOUT**.

### Windows Phone MDM Certificate Extended Validity (5y)

- The validity period of the device certificate issued by MDM for Windows Phone and Tablet. Devices use a device certificate to authenticate to the MDM server during device management. If **true**, the validity period is five years. If **false**, the validity period is two years. Defaults to **true**.

### **Windows WNS Channel - Number of Days Before Renewal**

- The renewal frequency for the ChannelURI. Defaults to **10** days.

### **Windows WNS Heartbeat Interval**

- How long Endpoint Management waits before connecting to a device after connecting to it every three minutes five times. Defaults to **6** hours.

### **XAM One-Time Ticket**

- The number of milliseconds that a one-time authentication token (OTT) is valid for downloading an app. This property and the properties **Unauthenticated App download for Android** and **Unauthenticated App download for Windows** work together. Those properties specify whether to allow unauthenticated app downloads. Defaults to **3600000**.

### **Endpoint Management MDM Self-Help Portal console max inactive interval (minutes)**

- This property name reflects the older Endpoint Management versions. The property controls the Endpoint Management console max inactive interval. That interval is the number of minutes after which Endpoint Management logs an inactive user out of the Endpoint Management console. A time-out of **0** means that an inactive user remains logged in. Default is **30**.

## **Device and app policies**

October 7, 2021

Endpoint Management device and app policies enable you to optimize a balance between factors, such as:

- Enterprise security
- Corporate data and asset protection
- User privacy
- Productive and positive user experiences

The optimum balance between those factors can vary. For example, highly regulated organizations, such as finance, require stricter security controls than other industries, such as education and retail, in which user productivity is a primary consideration.

You can centrally control and configure policies based on users' identity, device, location, and connectivity type to restrict malicious usage of corporate content. If a device is lost or stolen, you can disable,

lock, or wipe business applications and data remotely. The overall result is a solution that increases employee satisfaction and productivity, while ensuring security and administrative control.

The primary focus of this article is the many device and app policies related to security.

### **Policies that address security risks**

Endpoint Management device and app policies address many situations that might pose a security risk, such as when:

- Users try to access apps and data from untrusted devices and unpredictable locations
- Users pass data between devices
- An unauthorized user tries to access data
- A user who has left the company had used their own device (BYOD)
- A user misplaces a device
- Users must access the network securely always
- Users have their own device managed and you must separate work data from personal data
- A device is idle and requires verification of user credentials again
- Users copy and paste sensitive content into unprotected email systems
- Users receive email attachments or web links with sensitive data on a device that holds both personal and company accounts

Those situations relate to two main areas of concern when protecting company data, which are when data is:

- At rest
- In transit

### **How Endpoint Management protects data at rest**

Data stored on mobile devices is referred to as data at rest. Endpoint Management uses the device encryption provided by the iOS and Android platforms. Endpoint Management supplements platform-based encryption with features such as compliance checking, available through the Citrix MAM SDK.

The mobile application management (MAM) capabilities in Endpoint Management enable complete management, security, and control over Citrix mobile productivity apps, MDX-enabled apps, and their associated data.

The Mobile Apps SDK enables apps for Endpoint Management deployment through use of the Citrix MDX app container technology. The container technology separates corporate apps and data from personal apps and data on a user device. The data separation allows you to secure any custom-developed, third-party, or BYO mobile app with comprehensive policy-based controls.

Endpoint Management also includes app-level encryption. Endpoint Management separately encrypts data stored within any MDX-enabled app without requiring a device passcode and without requiring that you manage the device to enforce the policy.

- On iOS devices, Endpoint Management uses strong FIPS-validated cryptographic services and libraries such as keychain.
- OpenSSL provides FIPS-validated modules for various device platforms. OpenSSL further secures data in motion and the certificates required to manage and enroll devices.
- Endpoint Management uses the MAM SDK shared vault API to share managed content between apps that have the same keychain access group. For example, you can share user certificates through an enrolled app so that apps can obtain a certificate from the secure vault.
- Endpoint Management uses the device encryption provided by the platforms.
- Endpoint Management MAM controls at the app level perform a compliance check to validate that device encryption is enabled at every app launch.

### **How Endpoint Management protects data in transit**

Data on the move between your user's mobile devices and your internal network is referred to as data in transit. MDX app container technology provides application-specific VPN access to your internal network through Citrix Gateway.

Consider the situation where an employee wants to access the following resources residing in the secure enterprise network from a mobile device:

- The corporate email server
- An SSL-enabled web application hosted on the corporate intranet
- Documents stored on a file server or Microsoft SharePoint

MDX enables access to all these enterprise resources from mobile devices through an application-specific micro VPN. Each device has its own dedicated micro VPN tunnel.

Micro VPN functionality does not require a device-wide VPN, which can compromise security on untrusted mobile devices. As a result, the internal network is not exposed to malware or attacks that can infect the entire corporate system. Corporate mobile apps and personal mobile apps are able to coexist on one device.

To offer even stronger levels of security, you can configure MDX-enabled apps with an Alternate Citrix Gateway policy. The policy is used for authentication and for micro VPN sessions with an app. You can use an Alternate Citrix Gateway with the micro VPN session required policy to force apps to reauthenticate to the specific gateway. Such gateways would typically have different (higher assurance) authentication requirements and traffic management policies.

In addition to security features, the micro VPN feature also offers data optimization techniques, including compression algorithms. Compression algorithms ensure that:

- Only minimal data is transferred
- The transfer is done in the quickest time possible. Speed improves user experience, which is a key success factor in mobile device adoption.

Reevaluate your device policies periodically, such as in these situations:

- When a new version of Endpoint Management includes new or updated policies due to the release of device operating system updates
- When you add a device type:

Although many policies are common to all devices, each device has a set of policies specific to its operating system. As a result, you might find differences between iOS, Android, and Windows devices, and even between Android devices from different manufacturers.

- To keep Endpoint Management operation in sync with enterprise or industry changes, such as new corporate security policies or compliance regulations
- When a new version of the MAM SDK includes new or updated policies
- When you add or update an app
- To integrate new workflows for your users as a result of new apps or new requirements

## App policies and Use case scenarios

Although you can choose which apps are available through Secure Hub, you might also want to define how those apps interact with Endpoint Management. Use app policies:

- If you want users to authenticate after a certain time period passes.
- If you want to provide users offline access to their information.

The following sections include some of the policies and example usage.

- For a list of the third-party policies you can integrate in your iOS and Android app by using the MAM SDK, see [MAM SDK overview](#).
- For a list of all MDX policies per platform, see [MDX Policies at a Glance](#).

## Authentication policies

- **Device passcode**

**Why use this policy:** Enable the Device passcode policy to enforce that a user can access an MDX app only if the device has a device passcode enabled. This feature ensures use of iOS encryption at the device level.

**User example:** Enabling this policy means that the user must set a passcode on their iOS device before they can access the MDX app.

- **App passcode**

**Why use this policy:** Enable the App passcode policy to have Secure Hub prompt a user to authenticate to the managed app before they can open the app and access data. The user might authenticate with their Active Directory password, Citrix PIN, or iOS TouchID, depending what you configure under **Settings > Client Properties** in the Endpoint Management console. You can set an inactivity timer in Client Properties so that Secure Hub doesn't prompt the user to reauthenticate to the managed app until the timer expires.

The app passcode differs from a device passcode. With a device passcode policy pushed to a device, Secure Hub prompts the user to configure a passcode or PIN. The user must unlock their device when they turn on the device or when the inactivity timer expires. For more information, see [Authentication in Endpoint Management](#).

**User example:** When opening the Citrix Secure Web application on the device, the user must enter their Citrix PIN before they can browse websites if the inactivity period is expired.

- **micro VPN session required**

**Why use this policy:** If an application requires access to a web app (web service) to run, enable this policy. Endpoint Management then prompts the user to connect to the enterprise network or have an active session before using the app.

**User example:** When a user attempts to open an MDX app that has the micro VPN session required policy enabled: They can't use the app until they connect to the network. The connection must use a cellular or Wi-Fi service.

- **Maximum offline period**

**Why use this policy:** Use this policy as an extra security option. The policy ensures that users who run an app offline for a specified duration must reconfirm app entitlement and refresh policies.

**User example:** If you configure an MDX app with a Maximum offline period, the user can open and use the app offline until the offline timer period expires. At that point, the user must connect back to the network via cellular or Wi-Fi service and reauthenticate, if prompted.

### Miscellaneous access policies

- **App update grace period (hours)**

**Why use this policy:** The app update grace period is the time available to the user before they must update an app that has a newer version released in the app store. At the point of expiry, the user must update the app before they can gain access to the data in the app. When setting this value, keep in mind the needs of your mobile workforce, particularly users who might experience long periods offline when traveling internationally.



**User example:** You load a new version of Secure Mail in the app store and then set an app update grace period of 6 hours. Secure Hub users then have 6 hours to upgrade Secure Mail before they are routed to the app store.

- **Active poll period (minutes)**

**Why use this policy:** The active poll period is the interval at which Endpoint Management checks apps for when to perform security actions, such as App Lock and App Wipe.

**User example:** If you set the Active poll period policy to 60 minutes and then send the App Lock command, the lock occurs within 60 minutes of the last poll.

### **Non-compliant device behavior policies**

When a device falls below the minimum compliance requirements, the Non-compliant device behavior policy allows you to select the action to take. For information, see [Non-compliant device behavior](#).

### **App interaction policies**

**Why use these policies:** Use App Interaction policies to control the flow of documents and data from MDX apps to other apps on the device. For example, you can prevent a user from:

- moving data to their personal apps outside of the container
- pasting data from outside the container into the containerized apps

**User example:** You set an App interaction policy to Restricted, which means a user can copy text from Secure Mail to Secure Web. The user can't copy that data to their personal Safari or Chrome browser that is outside the container. In addition, a user can open an attached document from Secure Mail into Citrix Files or QuickEdit. The user can't open the attached document in their own personal file viewing apps that are outside the container.

### **App Restrictions policies**

**Why use these policies:** Use App Restriction policies to control what features users can access from an MDX app while it is open. The restrictions help to ensure that no malicious activity can take place while the app is running. The App Restriction policies vary slightly between iOS and Android. For example, in iOS you can block access to iCloud while the MDX app is running. In Android, you can stop NFC use while the MDX app is running.

**User example:** Suppose that you enable the App Restriction policy to block dictation on iOS in an MDX app. As a result, the user can't use the dictate function on the iOS keyboard while the MDX app is running. Thus, data that users dictate isn't passed to the unsecure third-party cloud dictation service. When the user opens their personal app outside of the container, the dictate option remains available to the user for their personal communications.

### **App Network Access policies**

**Why use these policies:** Use the App Network Access policies to provide access from an MDX app in the container on the device to data sitting inside your corporate network. The Tunneled - Web SSO option allows only the tunneling of HTTP and HTTPS traffic. That option provides single sign-on (SSO) for HTTP and HTTPS traffic and PKINIT authentication.

**User example:** When a user opens an MDX app that has tunneling enabled, the browser opens an intranet site without requiring the user to start a VPN. The app automatically accesses the internal site using the micro VPN technology.

### **App Geolocation and Geofencing policies**

**Why use these policies:** The policies that control app geolocation and geofencing include center point longitude, center point latitude, and radius. Those policies contain access to the data in the MDX apps to a specific geographical area. The policies define a geographic area by a radius of latitude and longitude coordinates. If a user attempts to use an app outside of the defined radius, the app remains locked and the user cannot access the app data.

**User example:** A user can access merger and acquisition data while they are in their office location. When they move outside of their office location, this sensitive data becomes inaccessible.

### **Secure Mail App policies**

- **Background network services**

**Why use this policy:** Background network services in Secure Mail use Secure Ticket Authority (STA), which is effectively a SOCKS5 proxy to connect through Citrix Gateway. STA supports long-lived connections and provides better battery life compared to micro VPN. Thus, STA is ideal for mail that connects constantly. Citrix recommends that you configure these settings for Secure Mail. The NetScaler for XenMobile wizard automatically sets up STA for Secure Mail.

**User example:** When STA isn't enabled and an Android user opens Secure Mail, they are prompted to open a VPN, which remains open on the device. When STA is enabled and the Android user opens Secure Mail, Secure Mail connects seamlessly with no VPN required.

- **Default sync interval**

**Why use this policy:** This setting specifies the default days of email that synchronize to Secure Mail when the user accesses Secure Mail for the first time. Two weeks of email take longer to sync than three days of email. More data to sync prolongs the setup process for the user.

**User example:** Suppose that the default sync interval is set to three days when the user first sets up Secure Mail. The user can see any emails in their Inbox that they received from the present to three days in the past. If a user wants to see emails that are older than three days, they can do

a search. Secure Mail then shows the older emails stored on the server. After installing Secure Mail, each user can change this setting to better suit their needs.

## Device policies and use case behavior

Device policies, sometimes referred to as MDM policies, determine how Endpoint Management manages devices. Although many policies are common to all devices, each device has a set of policies specific to its operating system. The following list includes some of the device policies and discusses how you might use them. For a list of all device policies, see the articles under [Device policies](#).

- **App inventory policy**

**Why use this policy:** To see the apps installed by a user, deploy the App inventory policy to a device. If you don't deploy the policy, you can see only the apps that a user installed from the app store, not personally installed apps. Use the App inventory policy to block certain apps from running on corporate devices.

**User example:** A user with an MDM-managed device cannot disable this functionality. The user's personally installed applications are visible to Endpoint Management administrators.

- **App lock policy**

**Why use this policy:** The App Lock policy, for Android, allows you to place apps on an allow list or block list. For example, for allowed apps you can configure a kiosk device. Typically, you deploy the App lock policy only to corporate owned devices, because it limits the apps that users can install. You can set an override password to provide user access to blocked apps.

**User example:** Suppose that you deploy an App lock policy that blocks the Angry Birds app. The user can install the Angry Birds app from Google Play, yet when they open the app a message advises them that their administrator blocked the app.

- **Connection scheduling policy**

**Why use this policy:** The Connection scheduling policy enables Windows Mobile devices to connect back to Endpoint Management for MDM management, app push, and policy deployment. For Android, Android Enterprise, and Chrome OS devices, use Google Firebase Cloud Messaging (FCM) instead. FCM controls connections to Endpoint Management. The Scheduling options are as follows:

- **Never:** Connect manually. Users must initiate the connection from Endpoint Management on their devices. Citrix doesn't recommend this option for production deployments because it prevents you from deploying security policies to devices. As a result, users don't receive new apps or policies. The **Never** option is enabled by default.
- **Every:** Connects at the designated interval. When you send a security policy, such as a lock or a wipe, Endpoint Management processes the policy on the device the next time the device connects.

- **Define schedule:** Endpoint Management attempts to reconnect the user's device to the Endpoint Management server after a network connection loss. Endpoint Management monitors the connection by transmitting control packets at regular intervals within the timeframe you define.

**User example:** You want to deploy a passcode policy to enrolled devices. The scheduling policy ensures that the devices connect back to the server at a regular interval to collect the new policy.

- **Credentials Policy**

**Why use this policy:** Often used with a network policy, the Credentials policy lets you deploy certificates for authentication to internal resources that require certificate authentication.

**User example:** You deploy a network policy that configures a wireless network on the device. The Wi-Fi network requires a certificate for authentication. The Credentials policy deploys a certificate that is then stored in the operating system keystore. The user can then select the certificate when connected to the internal resource.

- **Exchange policy**

**Why use this policy:** With Endpoint Management, you have two options to deliver Microsoft Exchange ActiveSync email.

- **Secure Mail app:** Deliver email by using the Secure Mail app that you distribute from the public app store or the app store.
- **Native email app:** Enable ActiveSync email for the native email client on the device. You can use macros to populate the user data from their Active Directory attributes, such as `#{ user.username }` to populate the user name and `#{ user.domain }` to populate the user domain.

**User example:** When you push the Exchange policy, you send Exchange Server details to the device. Secure Hub then prompts the user to authenticate and their email begins to sync.

- **Location policy**

**Why use this policy:** The Location policy lets you geolocate devices on a map, if the device has GPS enabled for Secure Hub. After you deploy this policy and then send a locate command from Endpoint Management, the device responds back with the location coordinates.

**User example:** When you deploy the Location policy and GPS is enabled on the device: If users misplace their device, they can log on to the Endpoint Management Self-Help Portal and choose the locate option to see their device location on a map. A user chooses whether to allow Secure Hub to use location services. You cannot enforce the use of location services when users enroll a device themselves. Another consideration for using this policy is the effect on battery life.

- **Passcode policy**

**Why use this policy:** The passcode policy allows you to enforce a PIN code or password on a managed device. This passcode policy allows you to set the complexity and time-outs for the passcode on the device.

**User example:** When you deploy a passcode policy to a managed device, Secure Hub prompts the user to configure a passcode or PIN. The passcode or PIN gives the user access to their device during start-up or when the inactivity timer expires.

- **Profile removal policy**

**Why use this policy:** Suppose that you deploy a policy to a group of users and later must remove that policy from a subset of the users. You can remove the policy for selected users by creating a Profile removal policy. Then, use deployment rules to deploy the Profile removal policy only to specified users.

**User example:** When you deploy a Profile removal policy to user devices, users might not notice the change. For example, if the Profile removal policy removes a restriction that disabled the device camera, the user doesn't know about the change. Consider letting users know when changes affect their user experience.

- **Restrictions policy**

**Why use this policy:** The restriction policy gives you many options to lock down and control features and functionality on the managed device. You can enable hundreds of restriction options for supported devices. For example, you can: disable the camera or microphone on a device, enforce roaming rules, and enforce access to third-party services like app stores.

**User example:** If you deploy a restriction to an iOS device, the user might not be able to access iCloud or the Apple App Store.

- **Terms and conditions policy**

**Why use this policy:** It might be necessary to advise users of the legal implications of having their device managed. In addition, you might want to ensure that users are aware of the security risks when corporate data is pushed to the device. The Terms and Conditions document allows you to publish rules and notices before the user enrolls.

**User example:** A user sees the Terms and Conditions information during the enrollment process. If they decline to accept the conditions stated, the enrollment process ends and they cannot access corporate data. You can generate a report to provide to HR/Legal/Compliance teams to show who accepted or declined the terms.

- **VPN policy**

**Why use this policy:** Use the VPN policy to provide access to back-end systems using older VPN Gateway technology. The policy supports various VPN providers, including Cisco AnyConnect, Juniper, and Citrix VPN. It is also possible to link this policy to a CA and enabled VPN on-demand, if the VPN gateway supports this option.

**User example:** With the VPN policy enabled, a user's device opens a VPN connection when the user accesses an internal domain.

- **Web clip policy**

**Why use this policy:** Use the Web clip policy if you want to push to devices an icon that opens directly to a website. A web clip contains a link to a website and can include a custom icon. On a device a web clip looks like an app icon.

**User example:** A user can click a web clip icon to open an internet site to gain access to needed services. Using a web link is more convenient than typing a link address in a browser.

- **Network policy**

**Why use this policy:** The network policy lets you deploy Wi-Fi network details, such as the SSID, authentication data, and configuration data, to a managed device.

**User example:** When you deploy the network policy, the device automatically connects to the Wi-Fi network and authenticates the user so they can gain access to the network.

- **Windows Information Protection policy**

**Why use this policy:** Use the Windows Information Protection (WIP) policy to protect against the potential leakage of enterprise data. You can specify the apps that require Windows Information Protection at the enforcement level you set. For example, you can block any inappropriate data sharing or warn about inappropriate data sharing and allow users to override the policy. You can run WIP silently while logging and permitting inappropriate data sharing

**User example:** Suppose that you configure the WIP policy to block inappropriate data sharing. If a user copies or saves a protected file to a non-protected location, a message similar to the following appears: You can't place work protected content in this location.

- **Endpoint Management Store policy**

**Why use this policy:** The app store is a unified app store where administrators can publish all the corporate apps and data resources needed by their users. An administrator can add:

- Web apps, SaaS apps, and MAM SDK enabled apps or MDX-wrapped apps
- Citrix mobile productivity apps
- Native mobile apps such as .ipa or .apk files
- Apple App Store and Google Play apps
- Web links
- Citrix Virtual Apps published using Citrix StoreFront

**User example:** After a user enrolls their device into Endpoint Management, they access the app store through the Citrix Secure Hub app or, if using Citrix Workspace, through the workspace. The user can then see all the corporate apps and services available to them. Users can click an

app to install it, access the data, rate and review the app, and download app updates from the app store.

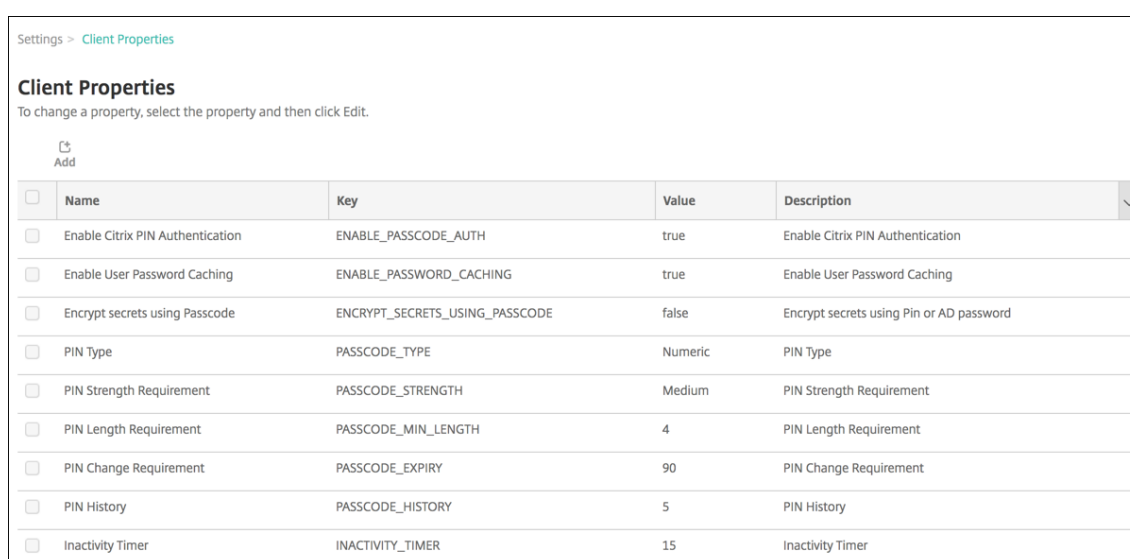
## Client properties

October 22, 2021

Client properties contain information that is provided directly to Secure Hub on user devices. You can use these properties to configure advanced settings, such as the Citrix PIN. You obtain client properties from Citrix support.

Client properties are subject to change with every release of Secure Hub and occasionally for client apps. For details about more commonly configured client properties, see Client property reference, later in this article.


1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Client**, click **Client Properties**. The **Client Properties** page appears. You can add, edit, and delete client properties from this page.



Settings > Client Properties

### Client Properties

To change a property, select the property and then click Edit.

 Add

<input type="checkbox"/>	Name	Key	Value	Description
<input type="checkbox"/>	Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	true	Enable Citrix PIN Authentication
<input type="checkbox"/>	Enable User Password Caching	ENABLE_PASSWORD_CACHING	true	Enable User Password Caching
<input type="checkbox"/>	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
<input type="checkbox"/>	PIN Type	PASSCODE_TYPE	Numeric	PIN Type
<input type="checkbox"/>	PIN Strength Requirement	PASSCODE_STRENGTH	Medium	PIN Strength Requirement
<input type="checkbox"/>	PIN Length Requirement	PASSCODE_MIN_LENGTH	4	PIN Length Requirement
<input type="checkbox"/>	PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
<input type="checkbox"/>	PIN History	PASSCODE_HISTORY	5	PIN History
<input type="checkbox"/>	Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer

### To add a client property

1. Click **Add**. The **Add New Client Property** page appears.

2. Configure these settings:

- **Key:** In the list, click the property key that you want to add. **Important:** Contact Citrix Support before updating the settings. You can request a special key.
- **Value:** The value of the selected property.
- **Name:** A name for the property.
- **Description:** A description of the property.

3. Click **Save**.

### To edit a client property

1. In the **Client Properties** table, select the client property you want to edit.

Select the check box next to a client property to open the options menu above the client property list. Click anywhere else in the list to open the options menu on the right side of the listing.

2. Click **Edit**. The **Edit Client Property** page appears.

3. Change the following information as appropriate:



- **Key:** You cannot change this field.
  - **Value:** The property value.
  - **Name:** The property name.
  - **Description:** The property description.
4. Click **Save** to save your changes or **Cancel** to leave the property unchanged.

### To delete a client property

1. In the **Client Properties** table, select the client property you want to delete.  
You can select more than one property to delete by selecting the check box next to each property.
2. Click **Delete**. A confirmation dialog box appears. Click **Delete** again.

### Client property reference

The predefined client properties and their default settings for Endpoint Management are as follows.

#### • **ALLOW\_CLIENTSIDE\_PROXY**

- Display name: ALLOW\_CLIENTSIDE\_PROXY
- If your users need to use a proxy they've configured on their iOS phones, set this custom policy to **true**. The default is **false**.

Some users might already have a proxy configured in **Settings > Wi-Fi > Configure Proxy** on their devices. If Secure Hub won't open for those users, have them perform one of these actions:

- \* Remove the proxy configuration from the device and then restart Secure Hub.
  - \* Connect the device to another Wi-Fi network. After Secure Hub re-authenticates, it gets the **ALLOW\_CLIENTSIDE\_PROXY** property and opens.
- If **ALLOW\_CLIENTSIDE\_PROXY** is **false** and users configure a proxy on their device, Endpoint Management detects the proxy. However, Secure Hub doesn't use the proxy and displays an error message. If a device connects to an access point or router that has a proxy enabled, Endpoint Management doesn't detect the proxy. For the highest security, we recommend that you use certificate pinning. For information about enabling certificate pinning for Secure Hub, see [Certificate pinning](#).
  - To configure this custom client policy, go to **Settings > Client Properties**, add the custom key **ALLOW\_CLIENTSIDE\_PROXY**, and set the **Value**.

#### • **CONTAINER\_SELF\_DESTRUCT\_PERIOD**

- Display name: MDX Container Self-Destruct Period

- Self-destruct prevents access to Secure Hub and managed apps, after a specified number of days of inactivity. After the time limit, apps are no longer usable. Wiping the data includes clearing the app data for each installed app, including the app cache and user data.

The inactivity time is when the server doesn't receive an authentication request to validate the user over a specific length of time. Suppose this property is 30 days. If the user doesn't use the apps for more than 30 days, the policy takes effect.

This global security policy applies to iOS and Android platforms and is an enhancement of the existing app lock and wipe policies.

- To configure this global policy, go to **Settings > Client Properties** and add the custom key **CONTAINER\_SELF\_DESTRUCT\_PERIOD**.
  - Value: Number of days

- **DEVICE\_LOGS\_TO\_IT\_HELP\_DESK**

- Display name: Send device logs to IT help desk
- This property enables or disables the ability to send logs to the IT help desk.
- Possible values: **true** or **false**
- Default value: **false**

- **DISABLE\_LOGGING**

- Display name: Disable Logging
- Use this property to prevent users from collecting and uploading logs from their devices. This property disables logging for Secure Hub and for all installed MDX apps. Users can't send logs for any app from the Support page. Even though the mail composition dialog box appears, logs aren't attached. A message indicates that logging is disabled. This setting also prevents you from updating log settings in the Endpoint Management console for Secure Hub and MDX apps.

When this property is set to **true**, Secure Hub sets **Block application logs** to **true**. As a result, MDX apps stop logging when the new policy is applied.

- Possible values: **true** or **false**
- Default value: **false** (logging is not disabled)

- **ENABLE\_CRASH\_REPORTING**

- Display name: Enable Crash Reporting
- If **true**, Citrix collects crash reports and diagnostics to help troubleshoot issues with Secure Hub for iOS and Android. If **false**, no data is collected.
- Possible values: **true** or **false**
- Default value: **true**

- **ENABLE\_CREDENTIAL\_STORE**

- Display name: Enable Credential Store
- Enabling the credential store means that Android or iOS users enter their password one time when accessing Citrix mobile productivity apps. You can use the credential store whether you enable Citrix PIN. If you don't enable Citrix PIN, users enter their Active Directory password. Endpoint Management supports the use of Active Directory passwords with the credential store only for Secure Hub and public store apps. If you use Active Directory passwords with the credential store, Endpoint Management doesn't support PKI authentication.
- Automatic enrollment in Secure Mail requires that you set this property to **true**.
- To configure this custom client policy, go to **Settings > Client Properties**, add the custom key **ENABLE\_CREDENTIAL\_STORE**, and set the **Value** to **true**.

- **ENABLE\_PASSCODE\_AUTH**

- Display name: Enable Citrix PIN Authentication
- This property allows you to turn on Citrix PIN functionality. With the Citrix PIN or passcode, users are prompted to define a PIN to use instead of their Active Directory password. This setting is automatically enabled when **ENABLE\_PASSWORD\_CACHING** is enabled or when Endpoint Management is using certificate authentication.

For offline authentication, the Citrix PIN is validated locally and users are allowed to access the app or content they requested. For online authentication, the Citrix PIN or passcode unlocks the Active Directory password or certificate, which is then sent to perform authentication with Endpoint Management.

If **ENABLE\_PASSCODE\_AUTH** is true and **ENABLE\_PASSWORD\_CACHING** is false, online authentication always prompts for the password because Secure Hub doesn't save it.

- Possible values: **true** or **false**
- Default value: **false**

- **ENABLE\_PASSWORD\_CACHING**

- Display name: Enable User Password Caching
- This property enables Active Directory passwords to cache locally on the mobile device. When you set this property to **true**, you must also set the **ENABLE\_PASSCODE\_AUTH** property to **true**. With user password caching enabled, Endpoint Management prompts users to set a Citrix PIN or passcode.
- Possible values: **true** or **false**
- Default value: **false**

- **ENABLE\_TOUCH\_ID\_AUTH**

- Display name: Enable Touch ID Authentication
- For devices that support Touch ID authentication, this property enables or disables Touch ID authentication on the device. Requirements:

User devices must have Citrix PIN or LDAP enabled. If LDAP authentication is off (for example, because only certificate-based authentication is used), users must set a Citrix PIN. In this case, Endpoint Management requires the Citrix PIN even if the client property **ENABLE\_PASSCODE\_AUTH** is **false**.

Set **ENABLE\_PASSCODE\_AUTH** to **false** so that when users launch an app, they must respond to a prompt to use Touch ID.

- Possible values: **true** or **false**
- Default value: **false**

- **ENABLE\_WORXHOME\_CEIP**

- Display name: Enable Secure Hub CEIP
- This property turns on the Customer Experience Improvement Program. That feature sends anonymous configuration and usage data to Citrix periodically. The data helps Citrix improve the quality, reliability, and performance of Endpoint Management.
- Value: **true** or **false**
- Default value: **false**

- **ENABLE\_WORXHOME\_GA**

- Display name: Enable Google Analytics in Secure Hub
- This property enables or disables the ability to collect data using Google Analytics in Secure Hub. When you change this setting, the new value is set only when the user next logs on to Secure Hub.
- Possible values: **true** or **false**
- Default value: **true**

- **ENCRYPT\_SECRETS\_USING\_PASSCODE**

- Display name: Encrypt secrets using Passcode
- This property stores sensitive data on the device in a secret vault instead of in a platform-based native store, such as the iOS keychain. This property enables strong encryption of key artifacts and adds user entropy. User entropy is a user-generated random PIN code that only the user knows.

Citrix recommends that you enable this property to help provide higher security on user devices. As a result, users experience more authentication prompts for the Citrix PIN.

- Possible values: **true** or **false**

- Default value: **false**
- **INACTIVITY\_TIMER**
  - Display name: Inactivity Timer
  - This property defines how long users can leave their device inactive and then access an app without a prompt for a Citrix PIN or passcode. To enable this setting for an MDX app, set the App Passcode setting to On. If the App Passcode setting is set to Off, users are redirected to Secure Hub to perform a full authentication. When you change this setting, the value takes effect the next time that users are prompted to authenticate.

On iOS, the Inactivity Timer also governs access to Secure Hub for MDX and non-MDX apps.
  - Possible values: Any positive integer
  - Default value: **15** (minutes)
- **ON\_FAILURE\_USE\_EMAIL**
  - Display name: On failure Use Email to Send device logs to IT help desk
  - This property enables or disables the ability to use email to send device logs to IT.
  - Possible values: **true** or **false**
  - Default value: **true**
- **PASSCODE\_EXPIRY**
  - Display name: PIN Change Requirement
  - This property defines how long the Citrix PIN or passcode is valid, after which the user is forced to change their Citrix PIN or passcode. When you change this setting, the new value is set only when the current Citrix PIN or passcode expires.
  - Possible values: **1** through **99** recommended. To eliminate PIN resets, set the value to a high number (for example, 100,000,000,000). If you originally set the expiry period to between 1 and 99 days and then change to the large number during that period: PINs still expire at the end of the initial period, but never again afterward.
  - Default value: **90** (days)
- **PASSCODE\_HISTORY**
  - Display name: PIN History
  - This property defines the number of previously used Citrix PINs or passcodes that users cannot reuse when changing their Citrix PIN or passcode. When you change this setting, the new value is set the next time that users reset their Citrix PIN or passcode.
  - Possible values: **1** through **99**
  - Default value: **5**
- **PASSCODE\_MAX\_ATTEMPTS**
  - Display name: PIN Attempts

- This property defines how many wrong Citrix PIN or passcode attempts users can make before being prompted for full authentication. After users successfully perform a full authentication, they are prompted to create a Citrix PIN or passcode.
- Possible values: Any positive integer
- Default value: **15**

• **PASSCODE\_MIN\_LENGTH**

- Display name: PIN Length Requirement
- This property defines the minimum length of Citrix PINs.
- Possible values: **4** through **10**
- Default value: **6**

• **PASSCODE\_STRENGTH**

- Display name: PIN Strength Requirement
- This property defines the strength of a Citrix PIN or passcode. When you change this setting, users are prompted to create a Citrix PIN or passcode the next time they are prompted to authenticate.
- Possible values: **Low, Medium, High, or Strong**
- Default value: **Medium**
- The password rules for each strength setting based on the PASSCODE\_TYPE setting are as follows:

Rules for numeric passcodes:

Passcode strength	Rules for numeric passcode type		
		Allowed	Not allowed
Low	All numbers, any sequence allowed	444444, 123456, 654321	
Medium (default setting)	All numbers cannot be the same or consecutive.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
High	Adjacent numbers cannot be the same.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199

Passcode strength	Rules for numeric passcode type	Allowed	Not allowed
	Strong	Do not use the same number more than twice. Do not use three or more consecutive numbers in a row. Do not use three or more consecutive numbers in the reverse order.	102983, 085085, 824673, 132312

## Rules for alphanumeric passcodes:

Passcode strength	Rules for alphanumeric passcode type	Allowed	Not allowed
	Low	Must contain at least one number and one letter	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa
Medium (default setting)	In addition to the rules for Low passcode strength, letters and all numbers cannot be the same. Letters cannot be consecutive and numbers cannot be consecutive.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, or aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, or cba123
High	Include at least one capital letter and one small letter.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2

Passcode strength	Rules for alphanumeric	Allowed	Not allowed
	passcode type		
Strong	Include at least one number, one special symbol, one capital letter, and one small letter.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

#### • **PASSCODE\_TYPE**

- Display name: PIN Type
- This property defines whether users are able to define a numerical Citrix PIN or an alphanumeric passcode. When you select **Numeric**, users can use numbers only (Citrix PIN). When you select **Alphanumeric**, users can use a combination of letters and numbers (passcode).  
If you change this setting, users must set a new Citrix PIN or passcode the next time that they are prompted to authenticate.
- Possible values: **Numeric** or **Alphanumeric**
- Default value: **Numeric**

#### • **REFRESHINTERVAL**

- Display name: REFRESHINTERVAL
- By default, Endpoint Management pings the AutoDiscovery Server (ADS) for pinned certificates every 3 days. To change the refresh interval, go to **Settings > Client Properties**, add the custom key **REFRESHINTERVAL**, and set the **Value** to the number of hours.
- Default value: **72** hours (3 days)

#### • **SEND\_LDAP\_ATTRIBUTES**

- For MAM-only deployments of Android, iOS, or macOS devices: You can configure Endpoint Management so that users who enroll in Secure Hub with email credentials are automatically enrolled in Secure Mail. As a result, users don't provide extra information or take extra steps to enroll in Secure Mail.
- To configure this global client policy, go to **Settings > Client Properties**, add the custom key **SEND\_LDAP\_ATTRIBUTES**, and set the **Value** as follows.
- Value: `userPrincipalName=${ user.userprincipalname } ,sAMAccountName=${ user.samaccountname } , displayName=${ user.displayName } ,mail=${ user.mail }`
- The attribute values are specified as macros, similar to MDM policies.



- Here is a sample account service response for this property:

```
<property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,email=user@site.com\,user@site.com" name="SEND_LDAP_ATTRIBUTES"/>
```

- For this property, Endpoint Management treats comma characters as string terminators. Therefore, if an attribute value includes a comma, precede it with a backslash. The backslash prevents the client from interpreting the embedded comma as the end of the attribute value. Represent backslash characters with "\\\".

- **HIDE\_THREE\_FINGER\_TAP\_MENU**

- When this property is not set or is set to **false**, users can access the hidden features menu by performing a three-finger tap on their devices. The hidden features menu allowed users to reset application data. Setting this property to **true** disables users access to the hidden features menu.
- To configure this global client policy, go to **Settings > Client Properties**, add the custom key **HIDE\_THREE\_FINGER\_TAP\_MENU**, and set the **Value**.

- **TUNNEL\_EXCLUDE\_DOMAINS**

- Display name: Tunnel Exclude Domains
- By default, MDX excludes from micro VPN tunneling some service endpoints that Mobile Apps SDKs and apps use for various features. For example, those endpoints include services that don't require routing through enterprise networks, such as Google Analytics, Citrix Cloud services, and Active Directory services. Use this client property to override the default list of domains excluded.
- To configure this global client policy, go to **Settings > Client Properties**, add the custom key **TUNNEL\_EXCLUDE\_DOMAINS**, and set the **Value**.
- Value: To replace the default list with the domains that you want to exclude from tunneling, type a comma-separated list of domain suffixes. To include all domains in tunneling, type **none**. Default is:

```
app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net, mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com, stream.launchdarkly.com
```

## User enrollment options

July 12, 2021

You can have users enroll their devices in Endpoint Management in several ways. Before considering the specifics, decide which devices you want to enroll in MDM+MAM, MDM, or MAM. For more information about those management modes, see [Management modes](#).

At the highest level, there are four enrollment options:

- **Enrollment Invitation:** Send an enrollment invitation or invitation URL to users. Enrollment invitations and URLs aren't available for Windows devices.
- **Self-Help Portal:** Set up a portal that users can visit to download Secure Hub, request enrollment, and view device information.
- **Manual Enrollment:** Send out an email, handbook, or some other communication letting users know that the system is up and that they can enroll. Users then download Secure Hub and enroll their devices manually.
- **Enterprise:** Another option for device enrollment is through an Apple Deployment Program and Google Android Enterprise. Through each of these programs, you can purchase devices that are pre-configured and ready for employees to use. For more information, see Apple Deployment Program articles in [Apple Support](#) and Google Android Enterprise documentation on the [Android Enterprise website](#).

### Enrollment Invitation

You can email an enrollment invitation to users with iOS, macOS, Android Enterprise, and legacy Android devices. Enrollment invitations aren't available for Windows devices.

You can also send an installation link through SMTP or SMS to users with iOS, macOS, Android Enterprise, Android, or Windows devices. For more information, see [Enroll devices](#).

If you choose to use the enrollment invitation method, you can:

- Choose **Invitation URL**, **Invitation URL + PIN**, or **Invitation URL + Password** enrollment security modes.
- Use any combination of the modes.
- Enable or disable the modes from the Endpoint Management **Settings** page.

For information on each enrollment security mode, see [Configure enrollment security modes](#).

Invitations serve many purposes. The most common use of invitations is to notify users that the system is available, and that they can enroll. Invitation URLs are unique. After a user uses an invitation URL, the URL is no longer available. You can use this property to limit the users or devices enrolling to your system.

When configuring an enrollment profile, you can control the number of devices specific users can enroll, based on Active Directory groups. For example, you might allow your Finance division only one device per user.

Be aware of the extra costs and pitfalls of certain enrollment options. To send invitations using SMS requires extra infrastructure. For more information on this option, see [Notifications](#).

In addition, to send invitations by email, ensure that users have a way of accessing email outside of Secure Hub. You can use one-time password (OTP) enrollment security modes as an alternative to Active Directory passwords for MDM enrollment.

### Self-Help Portal

The Self-Help Portal can be accessed at the same URL that admins use to access the Endpoint Management console. End users see the Self-Help Portal instead of the admin console. Users can download Secure Hub, request enrollment, and view device information in the Self-Help Portal.

To set up a portal, update these server properties in **Settings > Server Properties**:

- `shp.console.enable`: Set to **True** to provide access to the Self-Help Portal.
- `enable.new.shp`: Set to **True** to allow users to enable their devices from the Self-Help Portal.

### Manual Enrollment

With manual enrollment, users connect to Endpoint Management either through AutoDiscovery or by entering the server information. With AutoDiscovery, users log on with only their email address or Active Directory credentials in User Principal Name format. Without AutoDiscovery, they must enter the server address and their Active Directory credentials. For more information about setting up AutoDiscovery, see [Set up Endpoint Management AutoDiscovery service](#).

You can facilitate manual enrollment in several ways. You can create a guide, distribute it to users, and have them enroll themselves. You can have your IT department manually enroll groups of users in certain time slots. You can use any similar method where users must enter their credentials or server information.

### User Onboarding

After you have your environment set up, you need to decide how to get users into your environment. An earlier section in this article discusses the specifics of user enrollment security modes. This section discusses the way you reach out to users.

### Open Enrollment vs. Selective Invitation

When onboarding users, you can allow enrollment through two basic methods:

- Open enrollment. By default, any user with LDAP credentials and the Endpoint Management environment information can enroll.
- Limited enrollment. You can limit the number of users by only allowing users with invitations to enroll. You can also limit open enrollment by Active Directory group.

With the invitation method, you can also limit the number of devices a user can enroll. In most situations, open enrollment is acceptable, but there are a few things to consider:

- For MAM enrollment, you can easily limit open enrollment through Active Directory group membership.
- For MDM enrollment, you can limit the number of devices that can enroll based on Active Directory group membership. If you only allow corporate devices in your environment, that limitation typically isn't an issue. You might want to consider this method, however, in a BYOD workplace if you want to limit the number of devices in your environment.

Selective invitation is typically performed less often because it requires a bit more work than open enrollment. In order for users to enroll their devices in your environment, you must send an invitation unique to each user. For information on how to send an enrollment invitation, see [Enrollment invitations](#).

Send an invitation for each user or group whom you want enrolled in your environment. That process can take a long time depending on the size of your organization. It is possible to use Active Directory groups to create invitations in batches, but you must carry out this approach in waves.

### **First Contact with Users**

After deciding whether to use open enrollment or selective invitation and you set up those environments, inform users about their enrollment options.

If you use the selective invitation method, email and SMS messages are a part of the process. You can send emails through the Endpoint Management console for open enrollment as well. For details, see [Enrollment invitations](#).

In either case, keep in mind that for email, you need an SMTP server. For text messages, you need an SMS server. Those servers might be extra costs to consider when making your decision. Before you select a method, consider how you expect new users to access information, like email. If you want all users to access their email through Endpoint Management, sending them an invitation email would be problematic.

You can also send communications by another means outside of Endpoint Management for an open enrollment environment. For that option, be sure to include all the relevant information. Let users know where they can get the Secure Hub app and what method to use to enroll. If you have discovery turned off, also provide users the Endpoint Management server address. To learn more about discovery, see [Set up Endpoint Management AutoDiscovery service](#).

## App provisioning and deprovisioning

October 7, 2021

Application provisioning revolves around mobile app lifecycle management: Preparing, configuring, delivering, and managing mobile apps within an Endpoint Management environment. In some instances, developing or modifying application code might also be part of the provisioning process. Endpoint Management is equipped with various tools and processes that you can use for app provisioning.

Before reading this article on app provisioning, we recommend you read [Apps](#) and [User communities](#). When you have finalized the type of apps your organization plans to deliver to users, you can then outline the process for managing the apps throughout their lifecycle.

Consider the following points when defining your app provisioning process:

- **App profiling:** Your organization might start with a limited number of apps. However, the number of apps you manage can rapidly increase as user adoption rates increase and your environment grows. Define specific app profiles up front to make app provisioning easy to manage. App profiling helps you categorize apps into logical groups from a nontechnical perspective. For example, you can create app profiles based on the following factors:
  - Version: App version for tracking
  - Instances: Multiple instances that are deployed for different set of users, for example, with different levels of access
  - Platform: iOS, Android, or Windows
  - Target Audience: Standard users, departments, C-level executives
  - Ownership: Department that owns the app
  - Type: MDX, Public, Web and SaaS, or Web links
  - Upgrade Cycle: How often the app is upgraded
  - Licensing: Licensing requirements and ownership
  - MAM SDK or MDX policies: To apply MDX capabilities to your mobile apps
  - Network Access: Type of access, such as tunneling HTTP and HTTPS traffic with single sign-on (Tunneled - Web SSO).

Example:

Factor	Secure Mail	Mail	In-House	Epic Rover
Version	10.1	10.1	X.x	X.x
Instance	VIP	Physicians	Clinical	Clinical
Platform	iOS	iOS	iOS	iOS
Target Users	VIP Users	Physicians	Clinical Users	Clinical Users

Factor	Secure Mail	Mail	In-House	Epic Rover
Ownership	IT	IT	IT	IT
Type	MDX	MDX	Native	Public
Upgrade Cycle	Quarterly	Quarterly	Yearly	N/A
Licensing	N/A	N/A	N/A	Volume purchase
MDX Policies	Yes	Yes	Yes	No
Network Access	VPN	VPN	VPN	Public

- **App versioning:** Maintaining and tracking app versions is a critical part of the provisioning process. Versioning is typically transparent to users. They only receive notifications when a new version of the app is available for download. From your perspective, reviewing and testing each app version in a non-production capacity is also critical to avoid impacting a production site.

It is also important to evaluate if a specific upgrade is required. App upgrades are usually of two types: A minor upgrade, such as a fix to a specific bug, or a major release, which introduces significant changes. In either case, carefully review the release notes of the app to evaluate if the upgrade is necessary.

- **App development:** When you integrate the MAM SDK in the mobile apps that you develop, you apply MDX capabilities to those apps. See [MAM SDK overview](#).

The MAM SDK replaces the MDX Toolkit, which is scheduled for deprecation in March 2022. For information about app wrapping, see [MDX Toolkit](#). The app provisioning process for a wrapped app differs from the provisioning process for a standard non-wrapped app.

- **App security:** You define the security requirements of individual apps or app profiles as part of the provisioning process. You can map security requirements to specific MDM or MAM policies before deploying the apps. That planning simplifies and expedites app deployment. For example:
  - You might deploy certain apps differently.
  - You might want to make architectural changes to your Endpoint Management environment. The changes depend on the type of security compliance that the apps require. For example, a particular app might require end-to-end SSL encryption or geofencing.
- **App delivery:** Endpoint Management allows you to deliver apps as MDM apps or as MAM apps. The MDM apps appear in the app store. This store allows you to conveniently deliver public or native apps to users. Other than enforcing device level restrictions, no other app controls are needed. However, delivering apps by using MAM allows full control over app delivery and over the app itself. Delivering the apps through MAM is typically more suitable.

- **Application maintenance:**

- Perform an initial audit: Track the app version that is present in your production environment, and the last upgrade cycle. Make note of specific features or bug fixes that required the upgrade to take place.
- Establish baselines: Maintain a list of the latest stable release of each app. Be ready to fall back to an earlier app version if unexpected issues occur after an upgrade. Develop a rollback plan. Test app upgrades in a test environment before deploying to production. If possible, deploy the upgrade to a subset of production users first and then to the entire user base.
- Subscribe to Citrix software update notifications and any third-party software vendor notifications: Keeping up to date with the latest release of the apps is critical. An early access release (EAR) build might be available for testing ahead of time.
- Devise a strategy to notify users: Define a strategy to notify users when app upgrades are available. Prepare users with training before deployment. Consider sending multiple notifications before updating the apps. Depending on the app, the best notification method might be email notifications or websites.

App lifecycle management involves the complete lifecycle of an app from its initial deployment through retirement. The lifecycle of an app has these phases:

1. Requirements for specifications: Start with business case and user requirements.
2. Development: Validate that the app meets business needs.
3. Testing: Identify test users, issues, and bugs.
4. Deployment: Deploy the app to production users.
5. Maintenance: Update app version. Deploy the app in a test environment before updating the app in a production environment.

## Dashboard-based operations

November 1, 2019

You can view information at a glance by accessing your Endpoint Management console dashboard. With this information, you can see issues and successes quickly by using widgets.

The dashboard is usually the screen that appears when you first sign on to the Endpoint Management console. To access the dashboard from elsewhere in the console, click **Analyze**. Click **Customize** on the dashboard to edit the layout of the page and to edit the widgets that appear.

- **My Dashboards:** You can save up to four dashboards. You can edit these dashboards separately and view each one by selecting the saved dashboard.

- **Layout Style:** In this row, you can select how many widgets appear on your dashboard and how the widgets are laid out.
- **Widget Selection:** You can choose which information appears on your dashboard.
  - **Notifications:** Mark the check box above the numbers on the left to add a Notifications bar above your widgets. This bar shows the number of compliant devices, inactive devices, and devices wiped or enrolled in the last 24 hours.
  - **Devices By Platform:** Displays the number of managed and unmanaged devices by platform.
  - **Devices By Carrier:** Displays the number of managed and unmanaged devices by carrier. Click each bar to see a breakdown by platform.
  - **Managed Devices By Platform:** Displays the number of managed devices by platform.
  - **Unmanaged Devices By Platform:** Displays the number of unmanaged devices by platform. Devices that appear in this chart may have an agent installed on them, but have had their privileges revoked or have been wiped.
  - **Devices By ActiveSync Gateway Status:** Displays the number of devices grouped by ActiveSync Gateway status. The information shows Blocked, Allowed, or Unknown status. You can click each bar to break down the data by platform.
  - **Devices By Ownership:** Displays the number of devices grouped by ownership status. The information shows corporate-owned, employee-owned, or unknown ownership status.
  - **Failed Delivery Group Deployments:** Displays the total number of failed deployments per package. Only packages that have failed deployments appear.
  - **Devices By Blocked Reason:** Displays the number of devices blocked by ActiveSync
  - **Installed Apps:** By using this widget, you can type an app name, and a graph displays information about that app.
  - **Volume Purchase Apps License Usage:** Displays license usage statistics for Apple volume purchase apps.

## Use cases

Some examples for the many ways you can use dashboard widgets to monitor your environment are as follows.

- You have deployed Citrix mobile productivity apps and are receiving support tickets regarding mobile productivity apps failing to install on devices. Use the **Out of Compliance Devices** and **Installed Apps** widgets to see the devices that do not have Citrix mobile productivity apps installed.
- You'd like to monitor inactive devices so that you can remove the devices from your environment and reclaim licenses. Use the **Inactive Devices** widget to track this statistic.
- You are receiving support tickets concerning data not being synced properly. You may want to use the **Devices by ActiveSync Gateway Status** and **Devices By Blocked Reason** widgets to



determine whether the issue is ActiveSync related.

## Reporting

After your environment is setup and users enroll, you can run reports to learn about your deployment. Endpoint Management comes with a number of reports built in to help you get a better picture of the devices running on your environment. For details, see [Reports](#).

## Role-based access control and Endpoint Management support

January 21, 2021

Endpoint Management uses role-based access control (RBAC) to restrict user and group access to Endpoint Management system functions, such as the Endpoint Management console, Self-Help Portal, and public API. This article describes the roles built in to Endpoint Management and includes considerations for deciding on a support model for Endpoint Management that leverages RBAC.

### Built-In roles

You can change the access granted to the following built-in roles and you can add roles. For the full set of access and feature permissions associated with each role and their default setting, download [Role-Based Access Control Defaults](#). For a definition of each feature, see [Configure roles with RBAC](#).

### Admin role

Default access granted:

- Full system access except to the Self-Help Portal.
- By default, administrators can perform some support tasks, such as check connectivity and create support bundles.

Considerations:

- Do some or all of your administrators need access to the Self-Help Portal? If so, you can edit the Admin role or add Admin roles.
- To restrict access further for some administrators or administrator groups, add roles based on the Admin template and edit the permissions.

### User

Default access granted:

- Access to the Self-Help Portal, which lets authenticated users generate enrollment links. The links allow them to enroll their devices or send themselves an enrollment invitation.
- Restricted access to the Endpoint Management console: device features (such as wipe, lock/unlock device; lock/unlock container; see location and set geographic restrictions; ring the device; reset container password); add, remove, and send enrollment invitations.

Considerations:

- The User role enables you to enable users to help themselves.
- To support shared devices, create a user role for shared device enrollment.

### **Considerations for a Endpoint Management support model**

The support models that you can adopt can vary widely and might involve third parties who handle level 1 and 2 support while employees handle level 3 and 4 support. Regardless of how you distribute the support load, keep in mind the considerations in this section specific to your Endpoint Management deployment and user base.

#### **Do users have corporate-owned or BYO devices?**

The primary question that influences support is who owns the user devices in your Endpoint Management environment. If your users have corporate-owned devices, you might offer a lower level of support, as a way to lock down the devices. In that case, you might provide a help desk that assists users with device issues and how to use the devices. Depending on the types of devices you need to support, consider how you might use the RBAC Device Provisioning and Support roles for your help desk.

If your users have BYO devices, your organization might expect users to find their own sources for device support. In that case, the support your organization provides is more of an administrative role focused around Endpoint Management-specific issues.

#### **What is your support model for desktops?**

Consider whether your support model for desktops is appropriate for other corporate-owned devices. Can you use the same support organization? What additional training will they need?

#### **Do you want to give users access to the Endpoint Management Self-Help Portal?**

Although some organizations prefer not to grant users access to Endpoint Management, giving users some self-support capabilities can ease the load on your support organization. If the default User role for RBAC includes permissions that you don't want to grant, consider creating a new role with only the permissions you want to include. You can create as many roles as needed to meet your requirements.

## Citrix Support process

August 31, 2021

You can turn Citrix Technical Support Services to help with issues related to Citrix products. The group offers workarounds and resolutions and works hand in hand with development teams to offer solutions.

Citrix Consulting Services or Citrix Education Services offer help related to product training, advice on product usage, configuration, installation, or environment design and architecture.

Citrix Consulting helps with Citrix product-related projects, including proof of concepts, economic impact assessment, infrastructure health checks, design requirements analysis, architecture design verification, integration, and operational process development.

Citrix Education offers best-in-class IT training and certification on Citrix Virtualization, Cloud, and networking technologies.

Citrix recommends that you take full advantage of the Citrix Self-Help Resources and recommendations before creating a support case. For instance, there are several places where you can access articles and bulletins written by Citrix technical experts, see product documentation for Citrix solutions and technologies, or read straight talk from Citrix executives, product teams, and technical experts. See the [Knowledge Center](#), [Product documentation](#), and [Blogs](#) pages respectively.

For more interactive assistance, you can participate in discussion forums where you can ask questions and get real-world answers from other customers, share ideas, opinions, technical information, and best practices within user groups and interest groups, or interact with Citrix Support engineers who monitor Citrix Support social networking sites. See the [Support Forums](#) and [Citrix Community](#) pages respectively.

You also have access to training and certification courses to build your skills. See [Citrix Education](#).

Citrix Insight Services provides a simple, online troubleshooting platform and health-checker for your Citrix environment. Available for Citrix Endpoint Management, Citrix Virtual Apps and Desktops, Citrix Hypervisor, and Citrix Gateway. See [Analysis Tool](#).

To seek technical support, you can create a support case either by phone or via the web. You can use the web for low- and medium-severity issues and use the phone option for high-severity issues. To contact support for Endpoint Management issues, see [Citrix Support Services](#).

If you seek a highly trained single point of contact with extensive experience delivering Citrix solutions, Citrix Services offers a Technical Relationship Manager. For more information about Citrix services offering and benefits, see [Citrix Worldwide Services](#).

## Sending group enrollment invitations in Endpoint Management

July 9, 2021

Author:

John Bartel III

You can send enrollment invitations to groups and nested groups in Endpoint Management. Enrollment invitations aren't available for Windows devices.

When setting up the group invitation, you can specify one or multiple device platforms. You can also tag devices so that you can, for example, distinguish corporate-owned devices from employee-owned devices. Then, you set the authentication type for user devices.

### Note:

If you plan to use custom notification templates, you must set up the templates before you configure enrollment security modes. For more information about notification templates, see [Create and update notification templates](#).

For more information on basic configurations on user accounts, roles, and enrollment security modes and invitations, see [User accounts, roles, and enrollment](#).

### General steps

1. Within the Endpoint Management console, navigate to **Manage > Enrollment Invitations**.
2. Click **Add** toward the upper left of the screen and then click **Add Invitation**.
3. Click **Group** from the **Recipient** menu.

This step lets you choose one or multiple platforms. If you have a mix of different operating system platforms within your company, choose all platforms. Only clear the platform selection if you are sure that no users are using the particular platform.

4. You can choose to tag devices during the invite process. Choose **Corporate** or **Employee**.

Tagging makes it easy to separate corporate-owned devices and employee-owned devices.

5. In the **Domain** list, choose the domain in which the group exists.
6. In the **Group** list, select the Active Directory group you want to send the invites to.
7. The **Enrollment mode** allows you to set the type of enrollment security that you prefer for users.
  - User name + Password
  - High Security
  - Invitation URL

- Invitation URL + PIN
- Invitation URL + Password
- Two Factor
- User name + PIN

**Note:**

We deprecated **High Security** enrollment security mode. To send enrollment invitations, you can use only **Invitation URL**, **Invitation URL + PIN**, or **Invitation URL + Password** enrollment security modes. For devices enrolling with **User name + Password**, **Two Factor**, or **User name + PIN**, users must download Secure Hub and manually enter their credentials.

8. For the **Agent Download**, **Enrollment URL**, **Enrollment PIN**, and **Enrollment Confirmation** templates, choose the custom notification template that you have created in the past. Or, choose the default that is listed.

For these notification templates, use your configured SMTP server setup within Endpoint Management. Set your SMTP information first before proceeding.

**Note:**

The **Expire after** and **Maximum Attempts** options change based on the **Enrollment mode** option that you choose. You cannot change these options.

9. Select On for **Send invitation** and then click **Save and Send** to complete the process.

## Nested group support

You can use nested groups to send invites. Typically, nested groups are used in large-scale environments where groups with similar permissions are bound to each other.

Navigate to **Settings > LDAP** and then enable the **Support nested group** option.

## Troubleshooting and known limitations

**Issue:** Invites are being sent out to users even though they have been removed from an Active Directory group.

**Solution:** Depending on how large your Active Directory environment is, it could take up to six hours for changes to propagate to all servers. If a user or nested group is removed recently, Endpoint Management may still consider those users as a part of the group.

Therefore, it's best to wait up to six hours before sending out another group invite to your users.

## Configuring certificate-based authentication with EWS for Secure Mail push notifications

October 21, 2020

For Secure Mail push notifications to work, you must do the following:

- Configure Exchange Server for certificate-based authentication. This requirement is especially necessary when Secure Hub is enrolled in Endpoint Management with certificate-based authentication.
- Configure the Active Sync and Exchange Web Services (EWS) virtual directory on the Exchange Mail Server with certificate-based authentication.

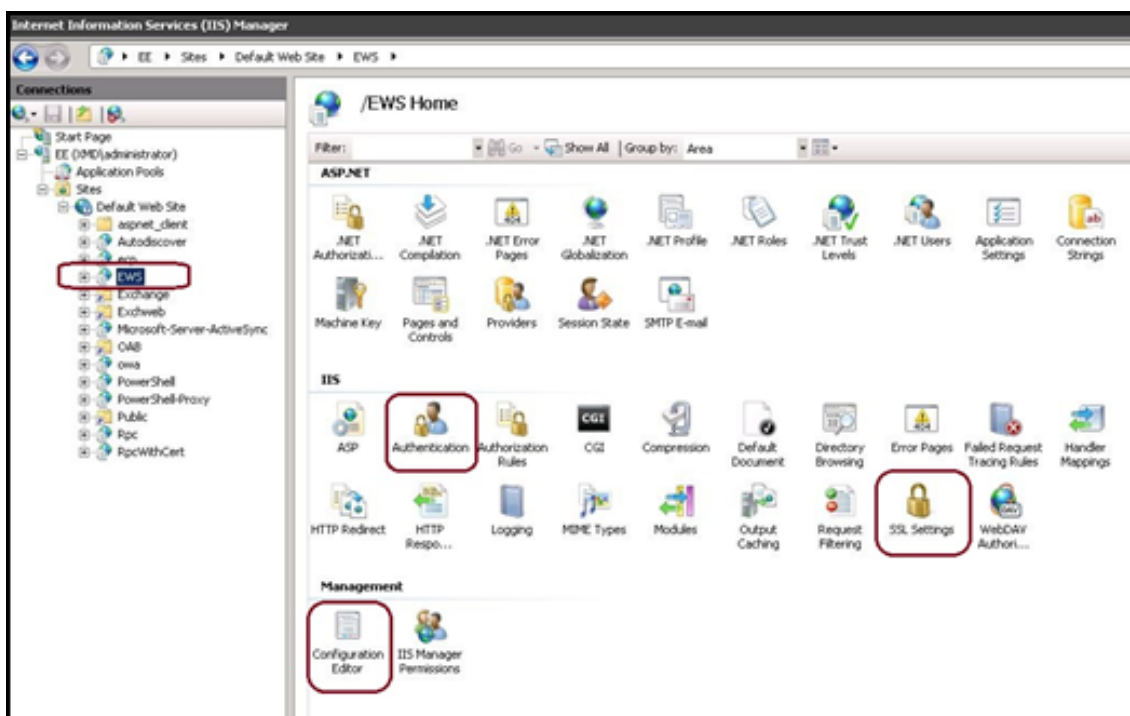
Unless you complete these configurations, the subscription to Secure Mail push notifications fails and no badge updates occur in Secure Mail.

This article describes the steps to configure certificate-based authentication. The configurations are specifically against the EWS virtual directory on Exchange Server.

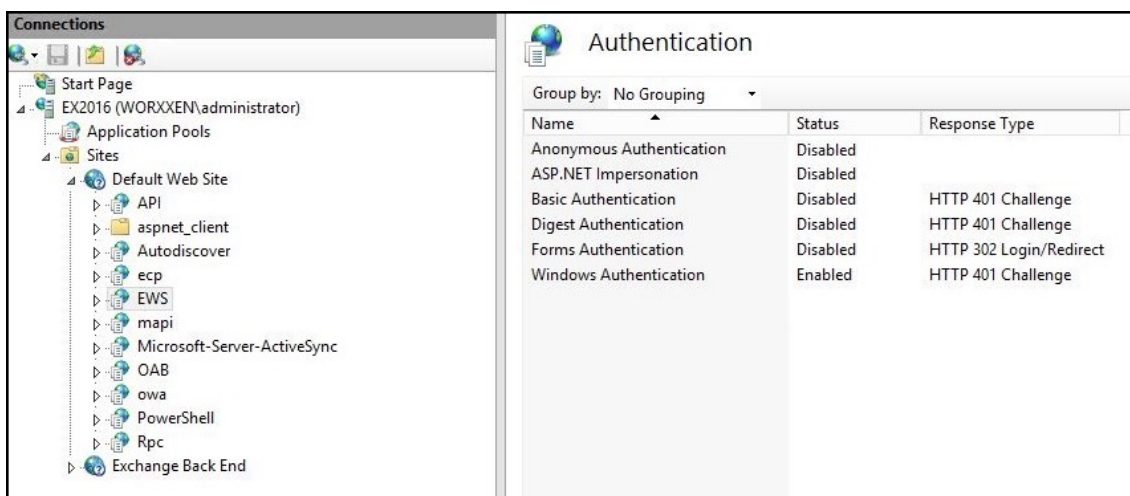
To get started with the configuration, do the following:

1. Log on to the server or servers where the EWS virtual directory is installed.
2. Open the IIS Manager Console.
3. Under the **Default Web Site**, click the EWS virtual directory.

The Authentication, SSL, Configuration Editor snap-ins are on the right side of the IIS Manager Console

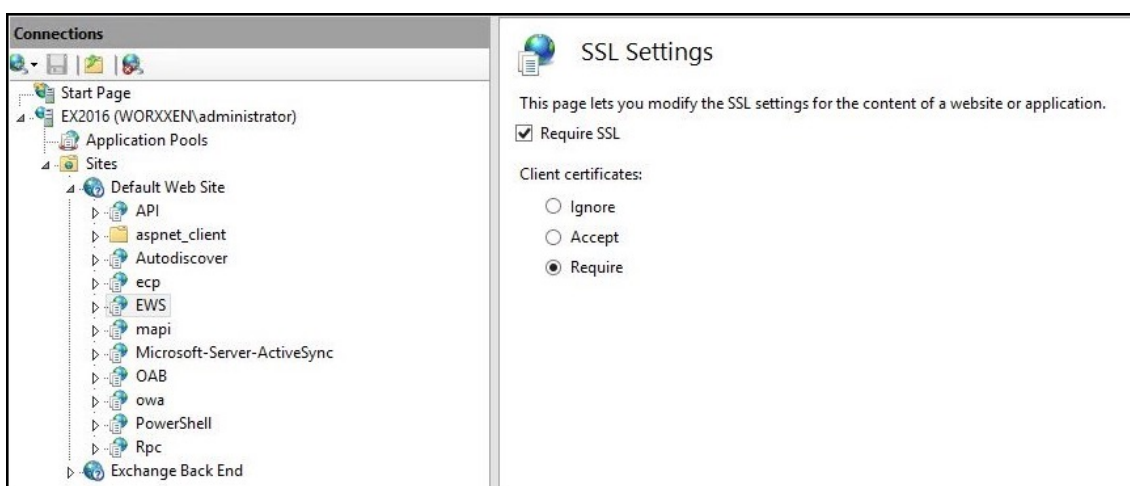


4. Ensure that the **Authentication** settings for EWS are configured as shown in the following figure.



5. Configure the **SSL Settings** for the EWS virtual directory.

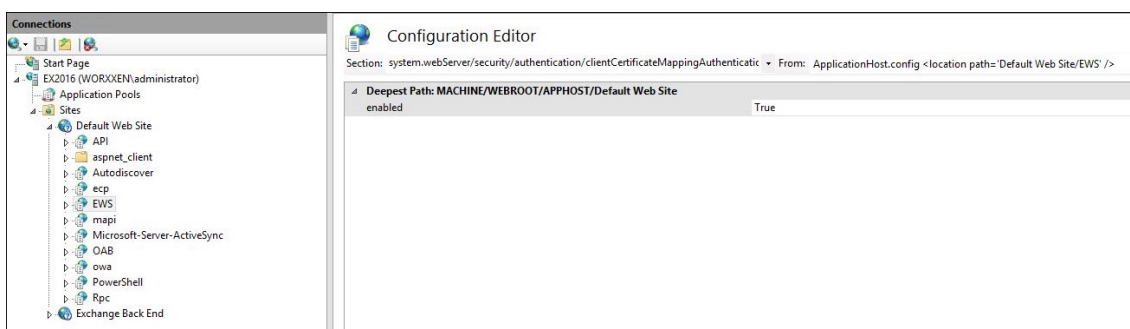
- a) Select the **Require SSL** check box.
- b) Under **Client Certificates**, click **Require**. Or, if other EWS mail clients use user name and password to authenticate to the Exchange Server, click **Accept**.



6. Click **Configuration Editor** and in the **Section** drop-down list, navigate to the following section:

- **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. Set the **enabled** value to **True**.



8. Click **Configuration Editor** and in the **Section** drop-down list, navigate to the following section:

- **system.webServer/serverRuntime**

9. Set the **uploadReadAheadSize** value to **10485760** (10 MB) or **20971520** (20 MB) or to a value as required by your organization.

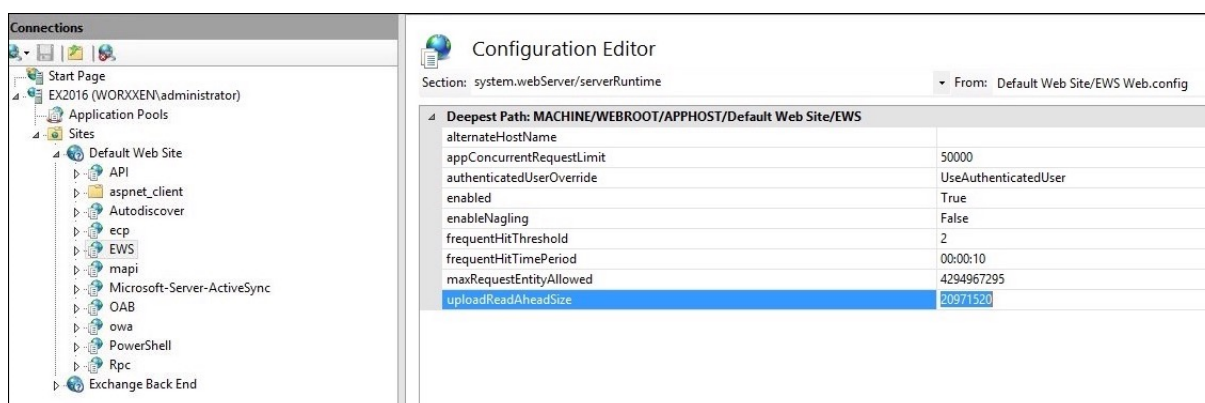
**Important:**

If you don't set this value correctly, certificate-based authentication while subscribing to EWS push notifications can fail with an error code of 413.

Do not set this value to **0**.

For more information, see the Microsoft article, [Microsoft IIS server runtime](#).





For more information about troubleshooting Secure Mail issues with iOS push notifications, see this [Citrix Support Knowledge Center](#) article.

## Related information

[Push notifications for Secure Mail for iOS](#)

## Configuring an on-premises Device Health Attestation server

September 8, 2021

You can enable Device Health Attestation (DHA) for Windows 10 and Windows 11 mobile devices through an on-premises Windows server. To enable DHA on-premises, you first configure a DHA server.

After you configure the DHA server, you create an Endpoint Management policy to enable the on-premises DHA service. For information, see [Device Health Attestation device policy](#).

### Prerequisites for a DHA server

- A server running Windows Server Technical Preview 5 or later, installed using the Desktop Experience installation option.
- One or more Windows 10 and Windows 11 client devices. These devices must have TPM 1.2 or 2.0 running the latest version of Windows.
- These certificates:
  - **DHA SSL certificate:** An x.509 SSL certificate that chains to an enterprise trusted root with an exportable private key. This certificate protects DHA data communications in transit including:
    - \* server to server (DHA service and MDM server) communications

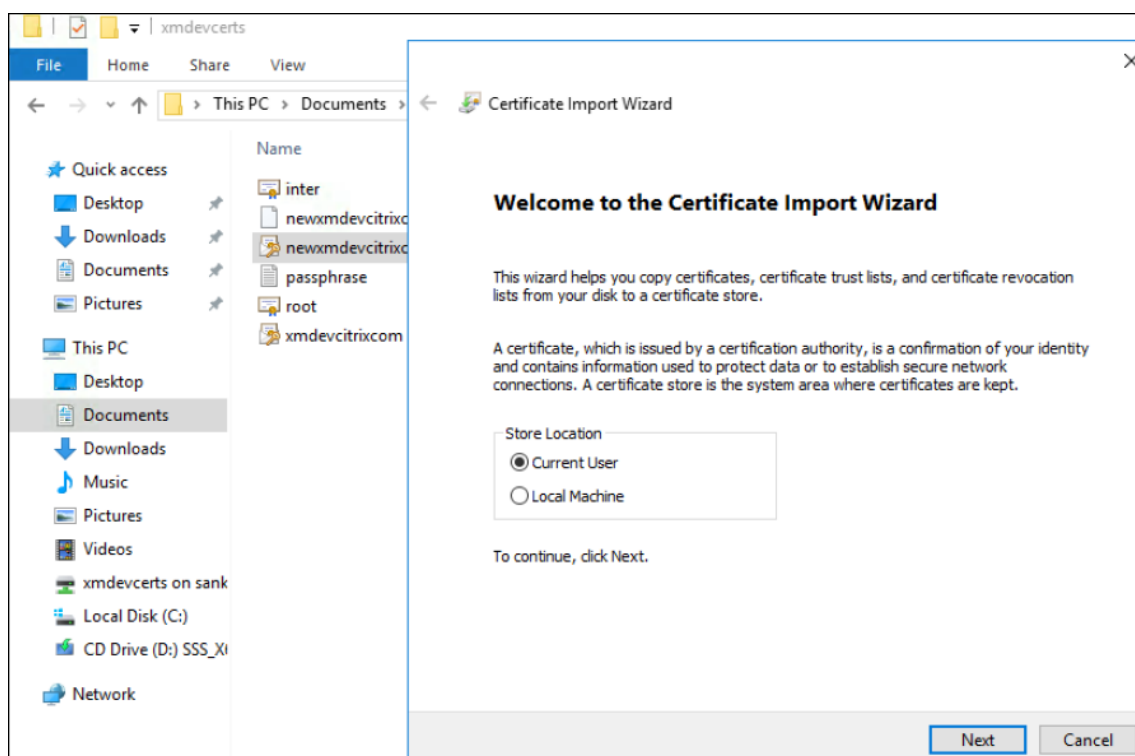
- \* server to client (DHA service and a Windows 10 or Windows 11 device) communications
- **DHA signing certificate:** An x.509 certificate that chains to an enterprise trusted root with an exportable private key. The DHA service uses this certificate for digital signing.
- **DHA encryption certificate:** An x.509 certificate that chains to an enterprise trusted root with an exportable private key. The DHA service also uses this certificate for encryption.
- Choose one of these certificate validation modes:
  - **EKCert:** EKCert validation mode is optimized for devices in organizations that are not connected to the Internet. Devices connecting to a DHA service running in EKCert validation mode do not have direct access to the Internet.
  - **AIKCert:** AIKCert Validation Mode is optimized for operational environments that do have access to the Internet. Devices connecting to a DHA service running in AIKCert validation mode must have direct access to the Internet and are able to get an AIK certificate from Microsoft.

### Add the DHA server role to the Windows server

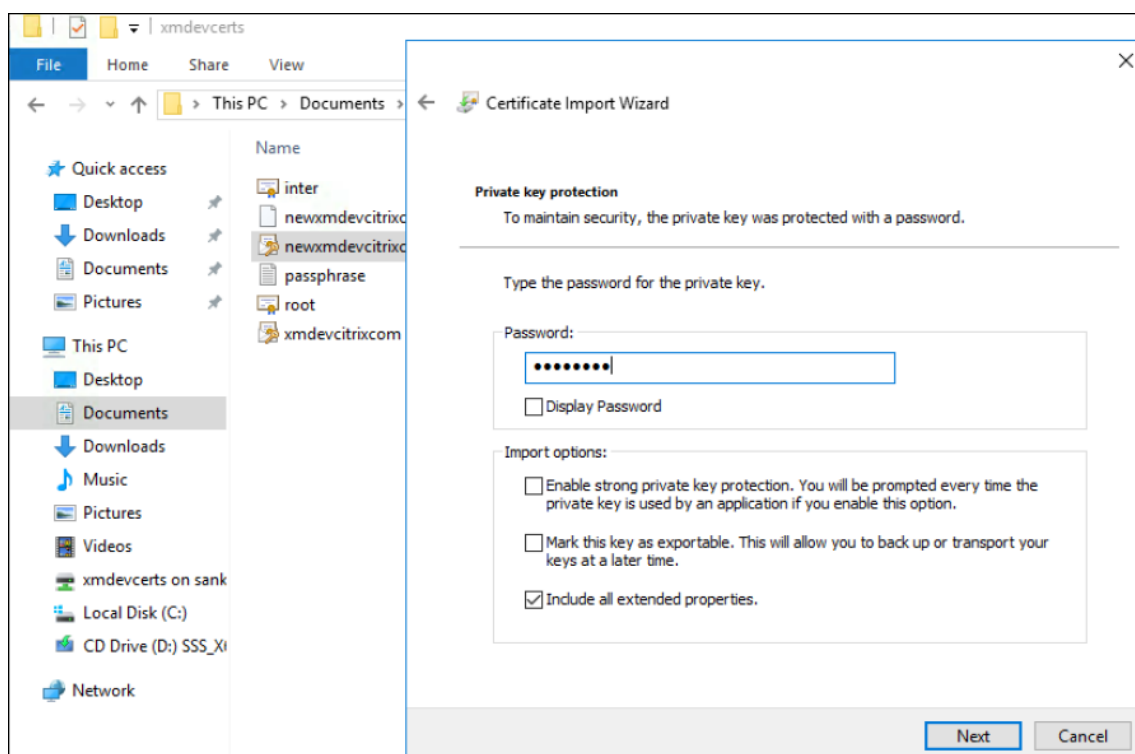
1. On the Windows server, if the Server Manager is not already open, click **Start** and then click **Server Manager**.
2. Click **Add roles and features**.
3. On the **Before you begin** page, click **Next**.
4. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
5. On the **Select destination server** page, click **Select a server from the server pool**, select the server, and then click **Next**.
6. On the **Select server roles** page, select the Device Health Attestation check box.
7. Optional: Click **Add Features** to install other required role services and features.
8. Click **Next**.
9. On the **Select features** page, click **Next**.
10. On the **Web Server Role (IIS)** page, click **Next**.
11. On the **Select role services** page, click **Next**.
12. On the **Device Health Attestation Service** page, click **Next**.
13. On the **Confirm installation selections** page, click **Install**.
14. When the installation is done, click **Close**.

### Add the SSL certificate to the certificate store of the server

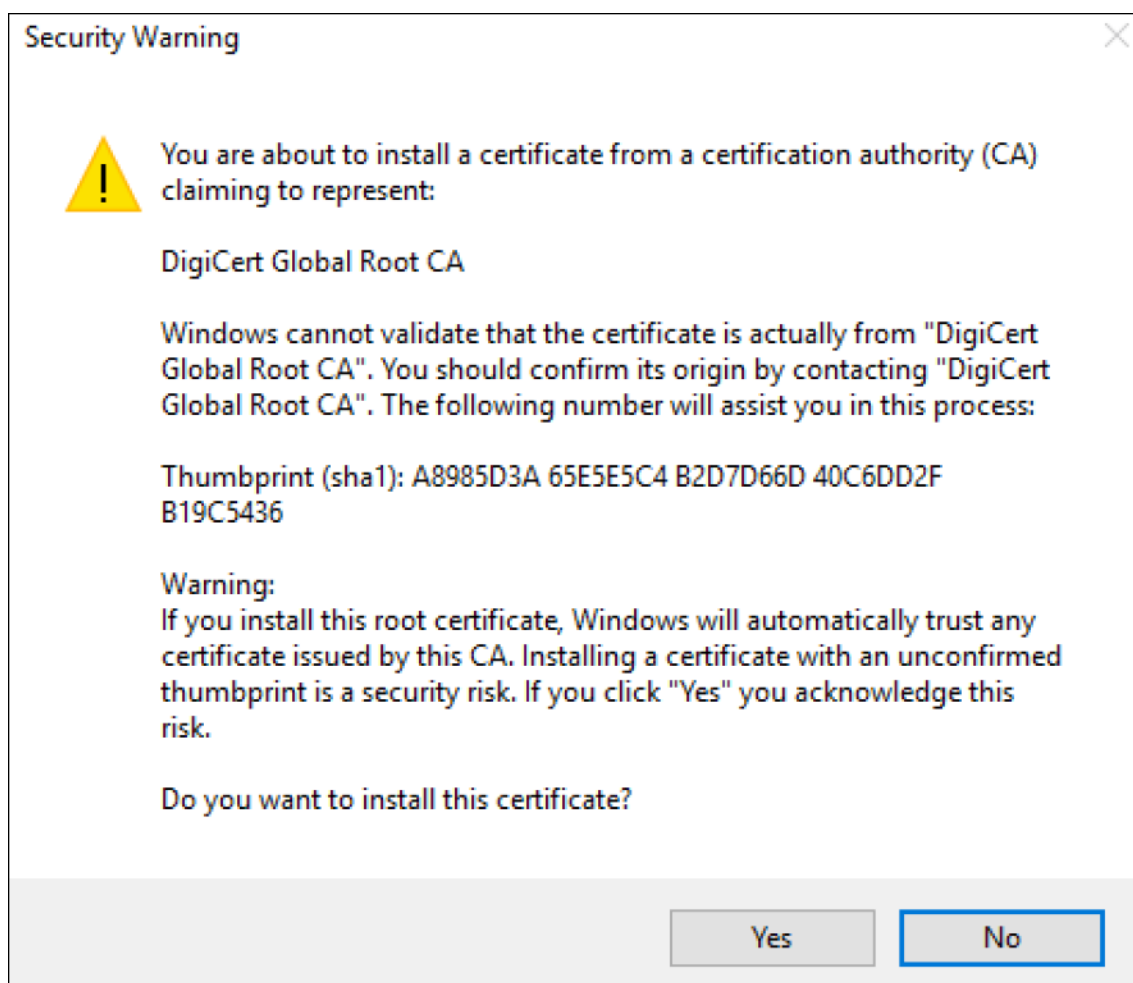
1. Go to the SSL certificate file and select it.
2. For the store location, select **Current user** and then click **Next**.



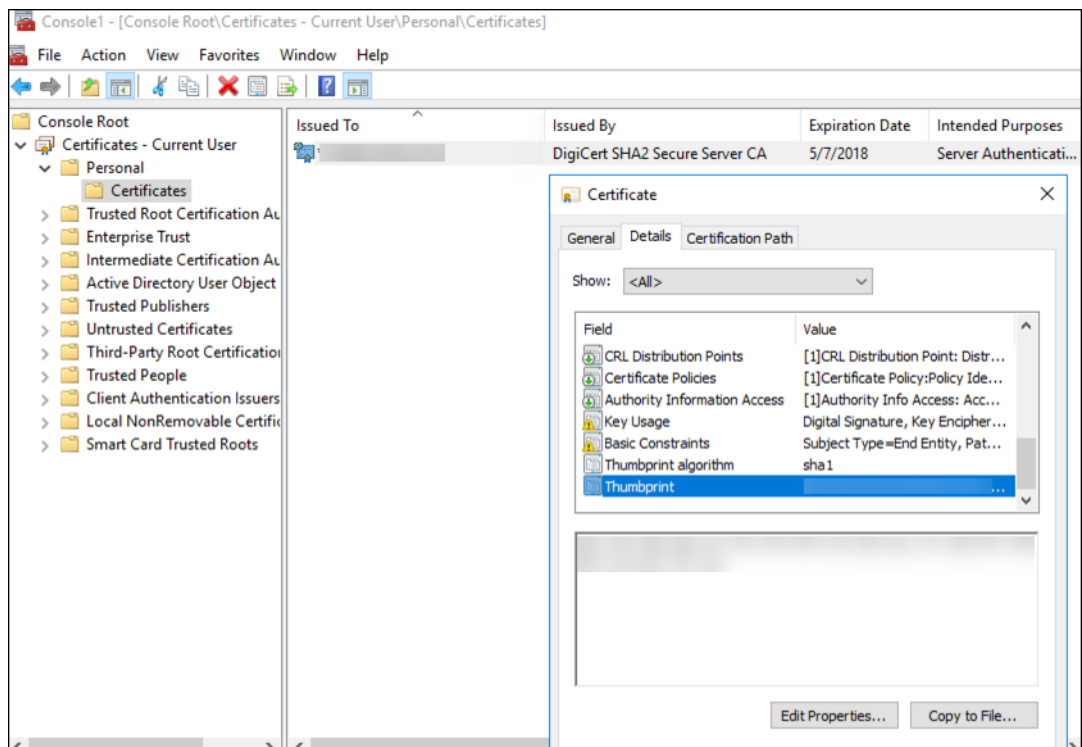
3. Type the password for the private key.
4. Ensure the import option **Include all extended properties** is selected. Click **Next**.



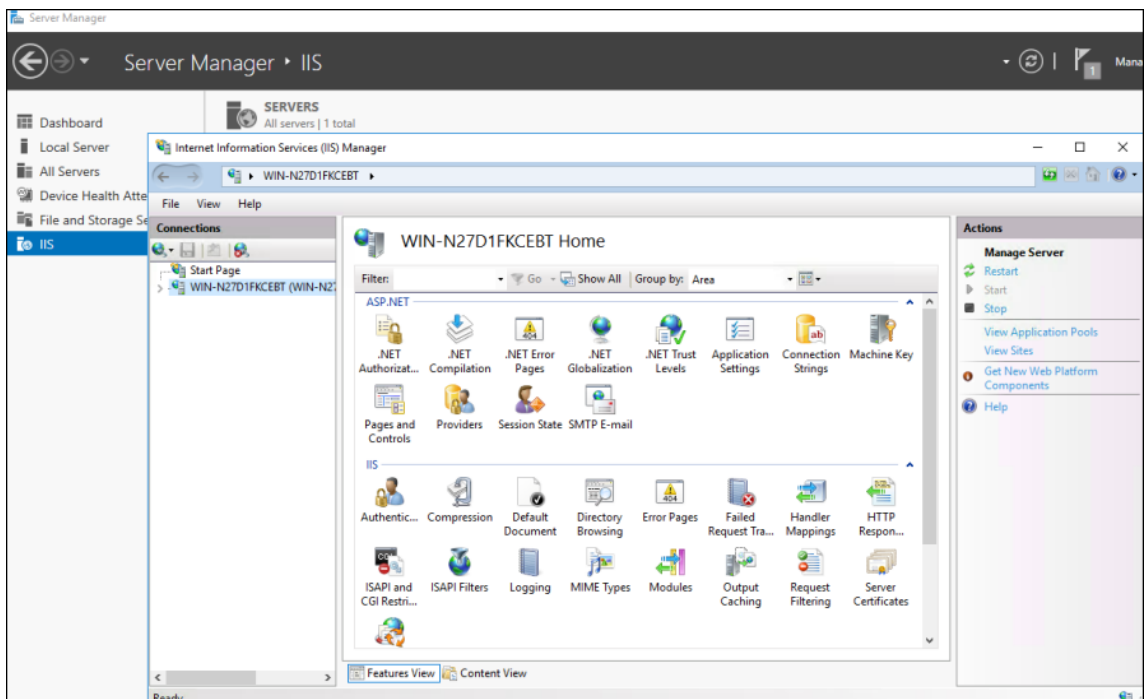
5. When this window appears, click **Yes**.



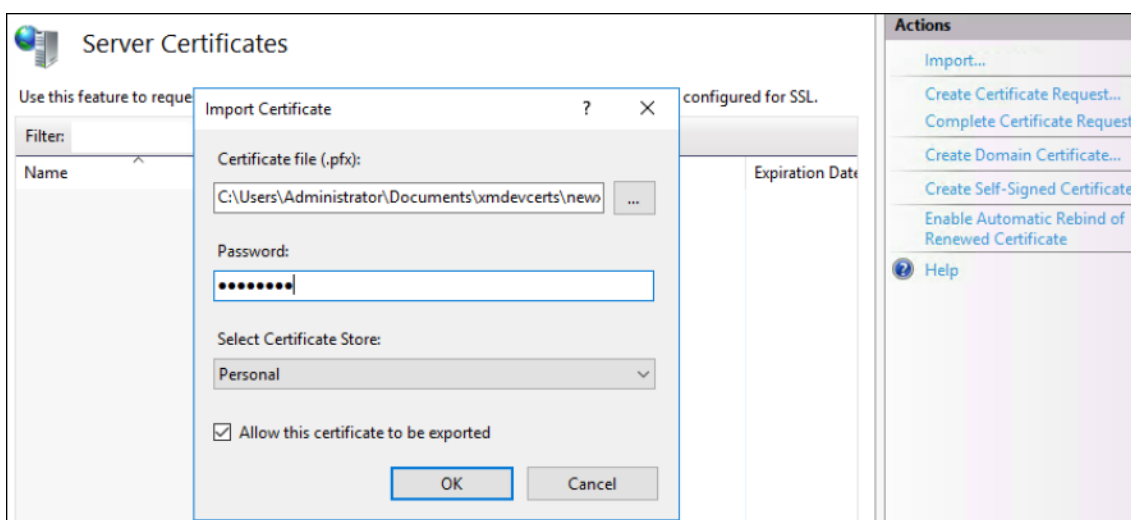
6. Confirm that the certificate is installed:
  - a) Open a Command Prompt window.
  - b) Type `mmc` and press the Enter key. To view certificates in the local machine store, you must be in the Administrator role.
  - c) On the File menu, click **Add/Remove Snap In**.
  - d) Click **Add**.
  - e) In the Add Standalone Snap-in dialog box, select **Certificates**.
  - f) Click **Add**.
  - g) In the Certificates snap-in dialog box, select **My User account**. (If you are signed in as service account holder, select **Service account**.)
  - h) In the Select Computer dialog box, click **Finish**.



7. Go to **Server Manager** > **IIS** and select **Server Certificates** from the list of icons.

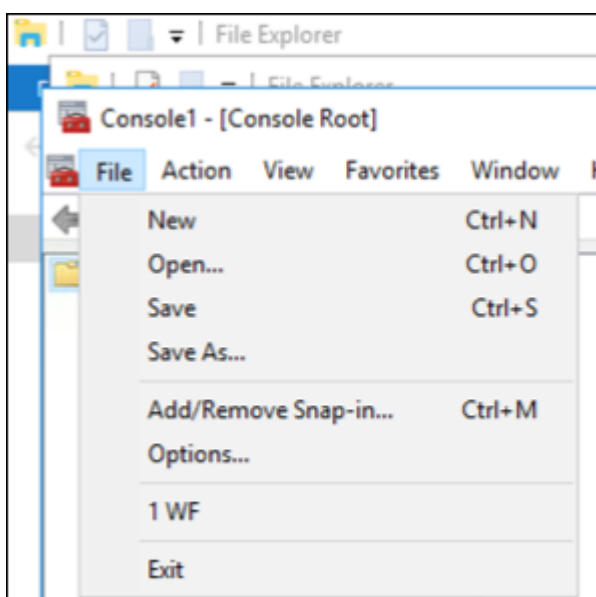


8. From the Action menu, select **Import...** to import the SSL certificate.

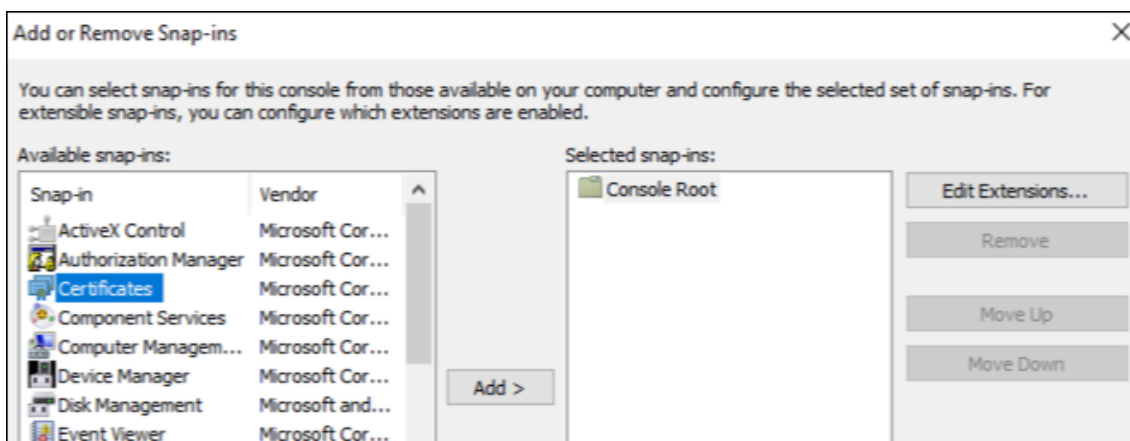


### Retrieve and save the thumbprint of the certificate

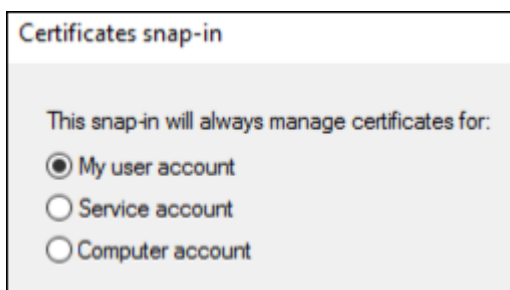
1. In the File Explorer search bar, type mmc.
2. In the Console Root window, click **File > Add/Remove Snap-in**.



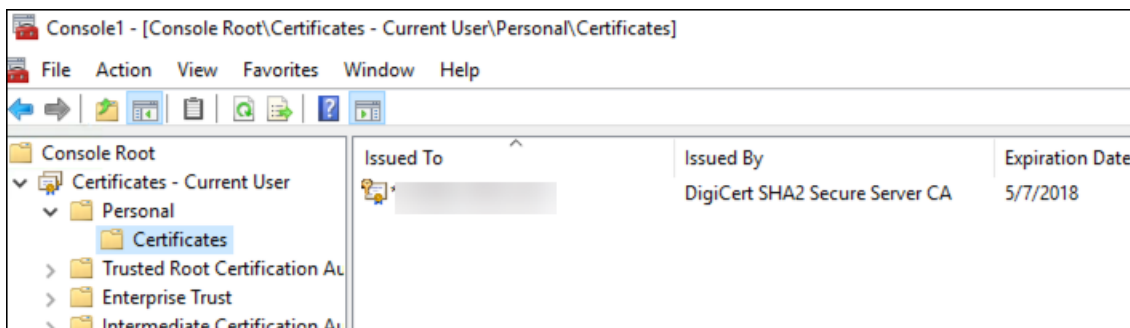
3. Select the certificate from available snap-in and add it to selected snap-ins.



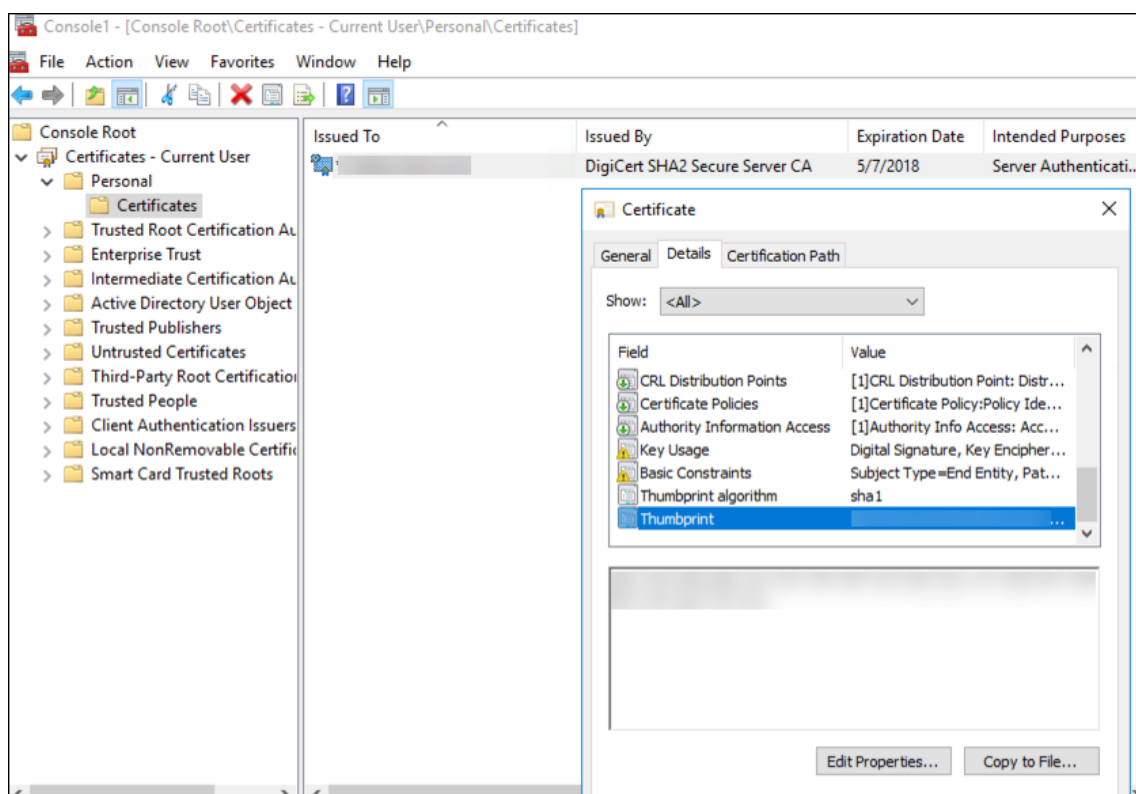
4. Select **My user account**.



5. Select the certificate and click **OK**.



6. Double-click on the certificate and select the **Details** tab. Scroll down to see the certificate thumbprint.



- Copy the thumbprint to a file. Remove the spaces when using the thumbprint in PowerShell commands.

### Install the signing and encryption certificates

Run these PowerShell commands on the Windows server to install the signing and encryption certificates.

Replace the placeholder `ReplaceWithThumbprint` and enclose it inside double-quotation marks as shown.

```

1 $key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
2   $_.Thumbprint -like "ReplaceWithThumbprint" }
3
4
5 $keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName
6
7 $keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys\" +
8   $keyname icacls $keypath /grant IIS_IUSRS`:R
9 <!--NeedCopy-->

```



## Extract the TPM roots certificate and install the trusted certificate package

Run these commands on the Windows server:

```
1 mkdir .\TrustedTpm
2
3 expand -F:\* .\TrustedTpm.cab .\TrustedTpm
4
5 cd .\TrustedTpm
6
7 .\setup.cmd
8 <!--NeedCopy-->
```

## Configure the DHA service

Run this command on the Windows server to configure the DHA service.

Replace the placeholder ReplaceWithThumbprint.

```
1 Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
   ReplaceWithThumbprint
2
3 -SigningCertificateThumbprint ReplaceWithThumbprint
4
5 -SslCertificateStoreName My -SslCertificateThumbprint
   ReplaceWithThumbprint
6
7 -SupportedAuthenticationSchema "AikCertificate"
8 <!--NeedCopy-->
```

Run these commands on the Windows server to set up the certificate chain policy for the DHA service:

```
1 $policy = Get-DHASCertificateChainPolicy
2
3 $policy.RevocationMode = "NoCheck"
4
5 Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
6 <!--NeedCopy-->
```

Respond to these prompts, as follows:

```
1 Confirm
2
3 Are you sure you want to perform this action?
4
```

```
5     Performing the operation "Install-DeviceHealthAttestation" on
      target "[Machine Name]".
6
7     [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?]
      Help (default is "Y"): A
8
9     Adding SSL binding to website 'Default Web Site'.
10
11    Add SSL binding?
12
13    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
14
15    Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17    Add application pool?
18
19    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
20
21    Adding web application 'DeviceHealthAttestation' to website '
      Default Web Site'.
22
23    Add web application?
24
25    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
26
27    Adding firewall rule 'Device Health Attestation Service' to allow
      inbound connections on port(s) '443'.
28
29    Add firewall rule?
30
31    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
32
33    Setting initial configuration for Device Health Attestation Service
      .
34
35    Set initial configuration?
36
37    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
38
39    Registering User Access Logging.
40
41    Register User Access Logging?
42
43    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
44    <!--NeedCopy-->
```

## Check the configuration

To check whether the DHASActiveSigningCertificate is active, run this command on the server:

```
Get-DHASActiveSigningCertificate
```

If the certificate is active, the certificate type (Signing) and thumbprint is displayed.

To check whether the DHASActiveSigningCertificate is active, run these commands on the server

Replace the placeholder ReplaceWithThumbprint and enclose it inside double-quotation marks as shown.

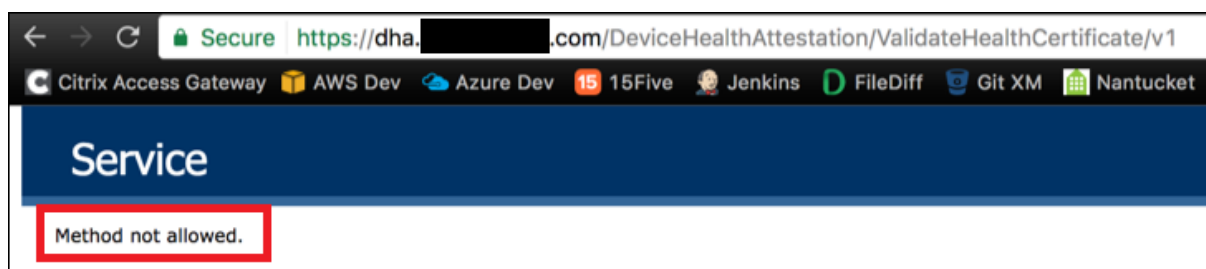
```
1 Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
   -Force
2
3 Get-DHASActiveEncryptionCertificate
4 <!--NeedCopy-->
```

If the certificate is active, the thumbprint appears.

To perform a final check, go to this URL:

```
https://<dha.myserver.com>/DeviceHealthAttestation/ValidateHealthCertificate/v1
```

If the DHA service is running, “Method not allowed” appears.



**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States  
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2021 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).