XenMobile Server Current Release

Contents

Release notes for Rolling Patches

August 11, 2021

This section contains the release notes for recent XenMobile Server rolling patches. Click a link below to view the fixed and known issues, feature changes, and needed actions.

The latest Rolling Patch contains all fixes from the prior Rolling Patches for the same release.

Release notes for patches to the current release	Publication date
10.13 Rolling Patch 4	Aug 11, 2021
10.13 Rolling Patch 3	May 13, 2021
10.13 Rolling Patch 2	Feb 25, 2021
10.13 Rolling Patch 1	Jan 8, 2021

Release notes for patches to prior releases	Publication date
10.12 Rolling Patch 8	Jun 2, 2021
10.12 Rolling Patch 7	Mar 29, 2021
10.12 Rolling Patch 6	Jan 26, 2021
10.11 Rolling Patch 7	Nov 18, 2020
10.10 Rolling Patch 6	Jul 22, 2020

Release Notes for XenMobile Server 10.13 Rolling Patch 4 Release

August 11, 2021

These release notes describe enhancements and fixed and known issues for XenMobile Server 10.13 Rolling Patch 4.

What's New

For information about previous rolling patches for XenMobile Server 10.13.0, see Release notes for Rolling Patches.

Fixed Issues

- The server property `ios.mdm.apns.connectionPoolSize` is hidden when you switch to the HTTP/2 based API for APNs. [CXM-95479]
- On XenMobile Server version 10.12, you can't modify the VPP properties on certain apps. [CXM-96854]
- The required web apps fail to install automatically on MDM only devices. [CXM-97477]
- On XenMobile Server version 10.13 when you configure the proxy server under the **CLI**, you can't send notifications to Secure Hub running on iOS devices. [CXM-97807]
- On XenMobile Server version 10.13, you get an error while accessing **Device details**. This error occurs when the device property has a value in **”“**. [CXM-97951]

Release Notes for XenMobile Server 10.12 Rolling Patch 8 Release

June 1, 2021

These release notes describe enhancements and fixed and known issues for XenMobile Server 10.12 Rolling Patch 8.

What's New

Secure Hub APNs certificate renewal. The Secure Hub Apple Push Notification Service (APNs) certificate for XenMobile Server 10.12 expires on June 17, 2021. This update renews the Secure Hub APNs certificate, which will expire on May 7, 2022. [CXM-94513]

Fixed Issues

- Right after enrolling a device running macOS 10.14+, the device properties don't always populate in the XenMobile Server console. After the device restarts, the device properties appear as expected. [CXM-94221]
- On XenMobile Server 10.12, ShareFile intermittently fails to establish a connection. [CXM-95419]

Release Notes for XenMobile Server 10.13 Rolling Patch 3 Release

May 14, 2021

These release notes describe enhancements and fixed and known issues for XenMobile Server 10.13 Rolling Patch 3.

What's New

Secure Hub APNs certificate renewal. The Secure Hub Apple Push Notification Service (APNs) certificate for XenMobile Server 10.13 expires on June 17, 2021. This update renews the Secure Hub APNs certificate, which will expire on May 7, 2022. [CXM-94070]

Alternate port for APNs notifications. XenMobile Server now supports using port 2197 as an alternative to port 443. You use port 2197 to send APNs notifications to, and receive feedback from `api.push.apple.com`. The port uses the HTTP/2-based APNs provider API. The default value of the server property `apns.http2.alternate.port.enabled` is **`false`**. To use the alternate port, update the server property and then restart the server. [CXM-93911]

Fixed Issues

Right after enrolling a device running macOS 10.14+, the device properties don't always populate in the XenMobile Server console. After the device restarts, the device properties appear as expected. [CXM-94150]

If you enable both the **Enable system apps** and **Disable applications** settings for the same app in the Restrictions policy, the app appears in the work profile. [CXM-94097]

When you add SNMP users to the XenMobile Server console, the users don't appear under the **SNMP Monitoring Users** list or the SNMP agents become inactive. [CXM-93199]

On the XenMobile Server, the NetScaler Gateway connectivity checks don't display a result. [CXM-93134]

On the XenMobile Server console, the correct root certificate expiration date is not displayed. [CXM-93133]

What's new in XenMobile Server 10.13

March 23, 2021

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 XenMobile Server integrations with Citrix Gateway. XenMobile Server continues to support the Classic policies and no action is needed.

XenMobile Migration Service

If you're using XenMobile Server on-premises, our free 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.

To start migration, contact your local Citrix salesperson or Citrix partner. See XenMobile Migration Service.

Deprecation announcements

For advanced notice of the Citrix XenMobile features that are being phased out, see Deprecation.

Before upgrading endpoints to iOS 14.5

Citrix recommends that before upgrading any endpoint to iOS 14.5, 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. Check the MDX Toolkit download page for the latest version.

Before you upgrade an on-premises Citrix ADC

Upgrading an on-premises Citrix ADC to certain versions can result in a single sign-on error. 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 command from the ADC CLI on Citrix Gateway, run it to enable global SSO:

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

For more information, see:

- Citrix ADC Release (Feature Phase) 13.0 Build 67.39/67.43
- 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]

Before you upgrade to XenMobile 10.13 (on-premises)

Some systems requirements changed. For information, see System requirements and compatibility and XenMobile compatibility.

1. If the virtual machine running the XenMobile Server to be upgraded has less than 8 GB of RAM, we recommend increasing the RAM to at least 8 GB.
2. Update your Citrix License Server to 11.16 or later before updating to the latest version of XenMobile Server 10.13.

   The latest version of XenMobile requires Citrix License Server 11.16 (minimum version).

   > **Note:**
   >
   > The Customer Success Services date (previously, Subscription Advantage date) in XenMobile 10.13 is September 29, 2020. The Customer Success Services date on your Citrix license must be later than this date.
   >
   > You can view the date next to the license in the License Server. If you connect the latest version of XenMobile to an older License Server environment, the connectivity check fails and you can't configure the License Server.

   To renew the date on your license, download the latest license file from the Citrix Portal and upload the file to the Licensing Server. See Customer Success Services.
3. For a clustered environment: iOS policy and app deployments to devices running iOS 11 and later have the following requirement. If Citrix Gateway is configured for SSL persistence, you must open port 80 on all XenMobile Server nodes.
4. Recommendation: Before you install a XenMobile update, use the functionality in your VM to take a snapshot of your system. Also, back up your system configuration database. If you experience issues during an upgrade, complete backups enable you to recover.

To upgrade

With this release, XenMobile supports VMware ESXi 7.0. Ensure that you upgrade to 10.13 before installing or upgrading ESXi 7.0.

You can directly upgrade to XenMobile 10.13 from XenMobile 10.12.x or 10.11.x. To perform the upgrade, download the latest binary available: Go to https://www.citrix.com/downloads. Navigate to **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. On the tile for the XenMobile Server software for your hypervisor, click **Download File**.

To upload the upgrade, use the **Release Management** page in the XenMobile console. See To upgrade using the Release Management page.

After you upgrade

If functionality involving outgoing connections stop working, and you haven't changed your connections configuration, check the XenMobile Server log for errors such as the following: "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer".

- The certificate validation error means you must disable host name verification on the XenMobile Server.
- By default, host name verification is enabled on outgoing connections except for the Microsoft PKI server.
- If host name verification breaks your deployment, change the server property `disable.hostname.verification` to **`true`**. The default value of this property is **`false`**.

Platform support updates

- **iOS 14:** XenMobile Server and Citrix Mobile productivity apps are compatible with iOS 14, but don't currently support any new iOS 14 features. The MDX Service doesn't support wrapping iOS apps for iOS 14. Use the MDX Toolkit 20.8.5 or later.
- **Android 11:** XenMobile Server supports Android 11. 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.

Configure multiple device and app management modes in a single environment

You can now configure a single XenMobile site to support multiple enrollment configurations. The role of enrollment profiles expanded to include enrollment settings for device and app management.

Enrollment profiles support multiple use cases and device migration paths within a single XenMobile console. 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)

Enrollment profiles replace the now deprecated server property, `xms.server.mode`. This change does not impact your existing delivery groups and enrolled devices.

If you don't need to enroll dedicated devices, you can disable this feature by setting the server property `enable.multimode.xms` to **`false`**. See Server properties.

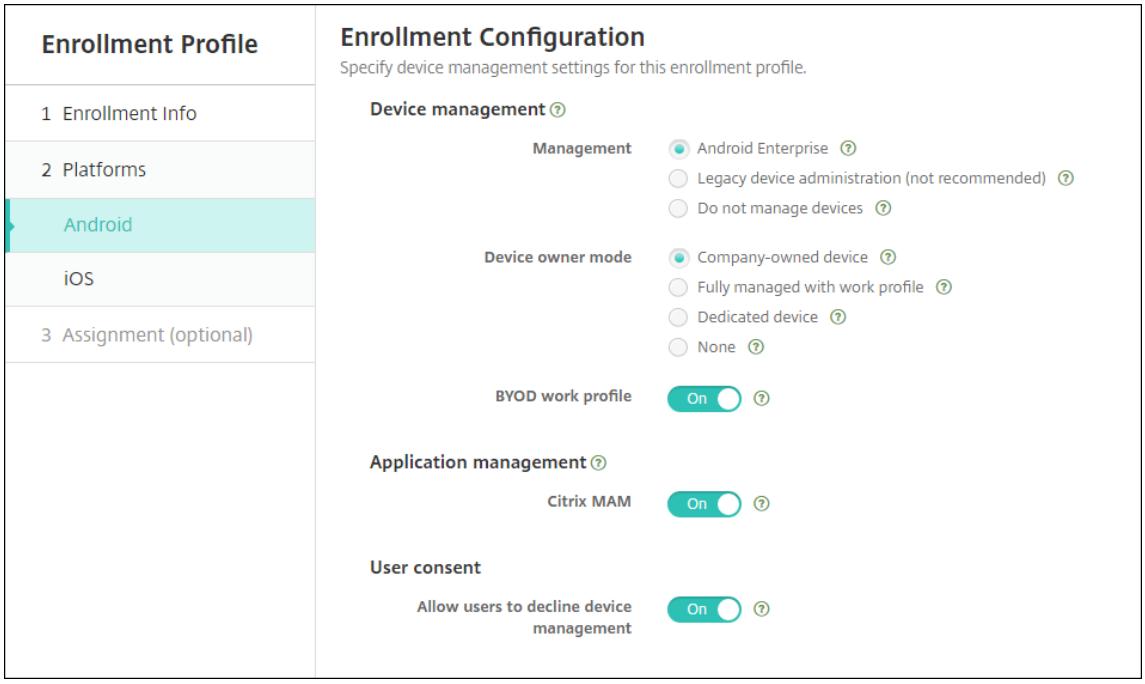
The following table shows the automated migration path from the existing server property mode to the new enrollment profile feature:

Existing server property	New management mode
ENT mode (iOS)	Apple device enrollment with Citrix MAM
ENT mode (Android)	Legacy device administrator with Citrix MAM
ENT mode (Android Enterprise)	Work profile on fully managed (previously COPE), with Citrix MAM
MAM mode (iOS and Android)	Citrix MAM
MDM mode (iOS)	Apple device enrollment
MDM mode (Android)	Legacy device administrator
MDM mode (Android Enterprise)	Work profile on fully managed

When you create a delivery group, you can attach an enrollment profile to the group. If you don't attach an enrollment profile, XenMobile attaches the Global enrollment profile.

Enrollment profiles provide the following device management features:

- **Easier migration from Android device administrator (DA) mode to Android Enterprise.** For Android Enterprise devices, settings include a device owner mode such as: Fully managed, work profile on fully managed, or dedicated. See Android Enterprise.



For this upgrade, your current XenMobile configurations for server mode and **Settings > Android Enterprise** map to the new enrollment profile settings as follows.

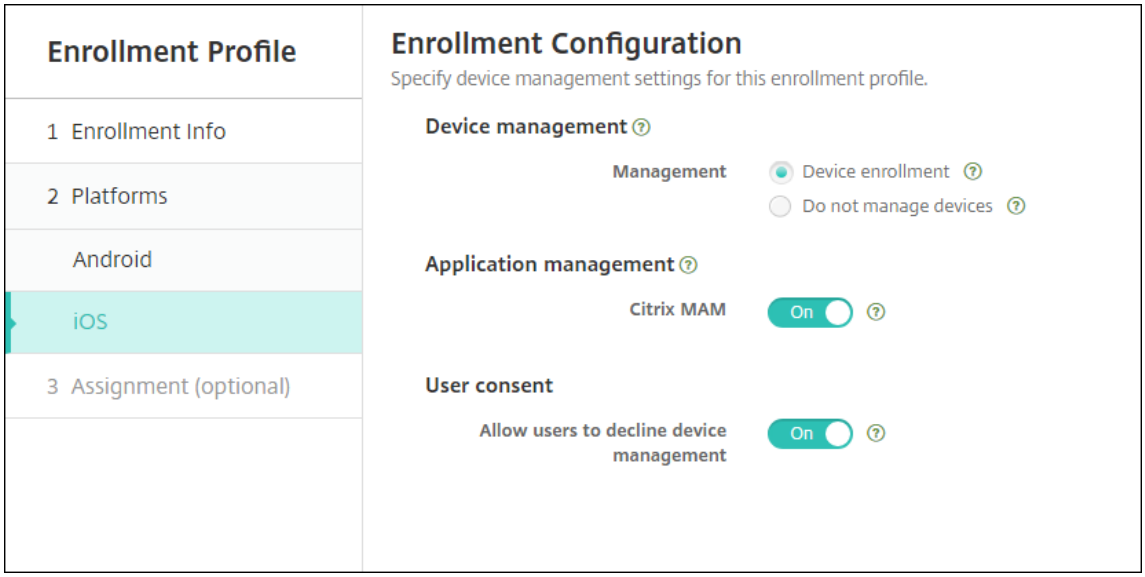
Current configuration	Management setting	Device owner mode setting	Citrix MAM setting
MDM. Managed Google Play (Android Enterprise)	Android Enterprise	Work profile on fully managed	Off
MDM; G Suite (legacy DA)	Legacy DA	not applicable	Off
MAM	Do not manage devices	not applicable	On
MDM+MAM. Managed Google Play (Android Enterprise)	Android Enterprise*	Work profile on fully managed	On
MDM+MAM; G Suite (legacy DA)	Legacy DA*	not applicable	On

* If enrollment is required, **Allow users to decline device management** is **Off**.

After the upgrade, your current enrollment profiles reflect those mappings. Consider whether you want to create other enrollment profiles to handle any new use cases as you transition away

from legacy DA.

- **Easier iOS management.** For iOS devices, settings include a choice between enrolling devices as managed or unmanaged.



For this upgrade, your prior configurations map to the new enrollment profile settings as follows.

Server mode	Management setting	Citrix MAM setting
MDM	Device enrollment	Off
MAM	Do not manage devices	On
MDM+MAM	Device enrollment	On

If enrollment is required, **Allow users to decline device management** is **Off**.

The following limitations exist for enhanced enrollment profiles:

- The enhanced enrollment profile feature isn't available for one-time PIN or two-factor authentication enrollment invitations.

See Enrollment profiles.

Support for the latest HTTP/2-based APNs provider API

Apple support for the Apple Push Notification service legacy binary protocol ends as of March 31, 2021. Apple recommends that you use the HTTP/2-based APNs provider API instead. XenMobile Server now 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.

The following versions of XenMobile Server enable support for the HTTP/2-based API by default:

- XenMobile Server 10.13
- XenMobile Server 10.12 Rolling Patch 5 and above

If you use the following versions of XenMobile Server, you must add the server property **apple.apns.http2** to enable the support:

- XenMobile Server 10.12 Rolling Patches 2-4 and above
- XenMobile Server 10.11 Rolling Patch 5 and above

We no longer support XenMobile Server 10.11 and recommend that you upgrade to the latest release.

Use a device-certificate based IPsec VPN with many iOS devices

Instead of configuring a VPN device policy and a credentials device policy for each iOS device that requires a device-certificate based IPsec VPN, automate the process.

1. Configure an iOS VPN device policy with the connection type **Always on IKEv2**.
2. Select **Device certificate based on device identity** as the device authentication method.
3. Select the **Device identity type** to use.
4. Bulk import your device certificates using the REST API.

For more information about configuring the VPN device policy, see VPN device policy. For information about importing certificates in bulk, see Upload certificates in bulk using the REST API).

Auto updates for Apple volume purchase apps

When you add a volume purchase account (**Settings > iOS Settings**), you can now enable auto updates for all iOS apps. See the **App Auto Update** setting in Apple Volume Purchase.

Password requirements for a local user account

When you add or edit a local user account in the XenMobile console, ensure that you follow the latest password requirements.

For more information, see To add a local user account.

- **Password requirements:** When you add or edit a local user account in the XenMobile Server console, follow the latest password requirements. See To add a local user account.
- **Local user account locking:** If a user reaches the maximum number of consecutive invalid login attempts, the local user account locks for 30 minutes. The system denies all further authentication attempts until the lockout period expires. To unlock the account in the XenMobile

Server console, go to **Manage > Users**, select the user account, and click **Unlock Local User**. See To unlock a local user account.

Device policies

New device policies and device policy settings have been added for Android Enterprise devices.

Hide the tray bar icon on Android Enterprise devices

You can now select whether the tray bar icon is hidden or visible for Android Enterprise devices. See XenMobile options device policy.

More certificate management features for Android Enterprise devices in work profile mode or fully managed mode

In addition to installing certificate authorities in the managed keystore, you can now manage the following features:

- **Configure the certificates used by specific managed apps.** The Credentials device policy for Android Enterprise now includes the setting **Apps to use the certificates**. You can specify the apps to use the user certificates issued by the credential provider selected in this policy. Apps are silently granted access to certificates during run time. To use the certificates for all apps, leave the apps list blank. See Credentials device policy.
- **Silently remove certificates from the managed keystore or uninstall all non-system CA certificates.** See Credentials device policy.
- **Prevent users from modifying credentials stored in the managed keystore.** The Restrictions device policy for Android Enterprise now includes the setting **Allow user to configure user credentials**. By default, that setting is **On**. See Restrictions device policy.

Easier use of the certificate alias in Android Enterprise managed configurations

Use the new **Certificate alias** setting in the **Credentials** device policy with the **Android Enterprise managed configuration** device policy. Doing so allows apps to authenticate on the VPN without user action. Instead of finding the credential alias in the app logs, you create the credential alias. Create the alias by typing it in the **Certificate alias** field of the **Android Enterprise managed configuration** device policy. Then you type the same certificate alias in the **Certificate alias** setting in the **Credentials** device policy. See Android Enterprise managed configurations policy and Credentials device policy.

Control the "Use one lock" setting on Android Enterprise devices

The new **Enable unified passcode** setting in the **Passcode** device policy lets you control whether a device requires a separate passcode for the device and the work profile. Before this setting, users controlled this behavior with the **Use one lock** setting on the device. When **Enable unified passcode** is **On**, users can use the same passcode for the device as the work profile. If **Enable unified passcode** is **Off** users can't use the same passcode for the device as the work profile. The default is **Off**. The **Enable unified lock** setting is available for Android Enterprise devices running Android 9.0 or later. See Passcode device policy.

Show the apps and shortcuts on Android Enterprise devices that are not in compliance

The Passcode device policy for Android Enterprise has a new setting, **Show apps and shortcuts while passcode is not in compliance**. Enable the setting to cause the apps and shortcuts to remain visible when the device passcode is no longer compliant. Citrix recommends you create an automated action to mark the device as out of compliance when the passcode is not in compliance. See Passcode device policy.

Disable the ability to print on the Android Enterprise work profile devices or fully managed devices

In the Restrictions device policy, the **Don't allow printing** setting lets you specify whether users can print to any printer accessible from the Android Enterprise device. See Android Enterprise settings.

Allow apps on dedicated devices by adding their package name in the Kiosk policy

You can now enter the package name that you want to allow on the Android Enterprise platform. See Android Enterprise settings.

Manage keyguard features for Android Enterprise work profile and fully managed devices

Android keyguard manages the device and work challenge lock screens. Use the Keyguard Management device policy to 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. You can also use the keyguard management policy to disable all biometric authentication for devices running Android 9.0 and later.

- 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.

See Keyguard Management device policy.

Publish enterprise apps for Android Enterprise in the XenMobile console

You no longer need to register for a Google Play developer account when you add an Android Enterprise private app. The XenMobile console opens a managed Google Play store UI for you to upload and publish the APK file. For more information, see Add an enterprise app.

Publish web apps for Android Enterprise in the XenMobile console

You no longer need to go to managed Google Play or the Google Developer portal to publish Android Enterprise web apps for XenMobile. When you click **Upload** in **Configure > Apps > Web link**, a managed Google Play store UI opens for you to upload and save the file. The app approval and publishing can take about 10 minutes. For more information, see Add a Web link.

Upload certificates to iOS devices in bulk with the XenMobile Server REST API

If uploading certificates one at a time isn't practical, use the XenMobile Server REST API to upload the certificates to iOS devices in bulk.

1. Configure an iOS VPN device policy with the connection type **Always on IKEv2**.
2. Select **Device Certificate Based on Device Identity** as the device authentication method.
3. Select the **Device identity type** to use.
4. Bulk import your device certificates with the REST API.

For information about configuring the VPN device policy, see VPN device policy. For information about importing certificates in bulk, see Upload certificates to iOS devices in bulk with the REST API.

Refresh encryption keys

The **Refresh encryption keys** option is added in the Advanced Settings of the XenMobile CLI. You can use this option to refresh the encryption keys one node at a time. See System options.

ESXi 7.0 support

With this release, XenMobile supports VMware ESXi 7.0. Ensure that you upgrade to 10.13 before installing or upgrading ESXi 7.0.

New server properties

The following server properties are now available:

- **Allow hostnames for iOS App Store links:** To add public app store apps for iOS using the public APIs rather than the console, configure a list of allowed host names if you want.
- **Local user account lockout limit:** Configure the number of sign-in attempts a local user has before their account is locked.
- **Local user account lockout time:** Configure how long a local user is locked out after too many failed sign-in attempts.
- **Maximum size of file upload restriction enabled:** Enable restricting the maximum file size for uploaded files.
- **Maximum size of file upload allowed:** Set the maximum file size for uploaded files.

For more detailed information about these properties, see Server properties.

Self-service disk cleanup

A new command-line interface option called **Disk Usage** is available in the **Troubleshooting Menu**. This option allows you to see a list of core dump files and support bundle files. After viewing the list you can choose to delete all of those files through the command-line. For more information about the command-line interface tools, see Command-line interface options.

What's new in XenMobile Server 10.12

March 30, 2021

XenMobile Server 10.12 (PDF Download)

XenMobile Migration Service

If you're using XenMobile Server on-premises, our free 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.

To start migration, contact your local Citrix salesperson or Citrix partner. For more information, see XenMobile Migration Service.

Deprecation announcements

For advanced notice of the Citrix XenMobile features that are being phased out, see Deprecation.

Prepare your Android devices for upcoming changes

These previously announced deprecations impact your Android and Android Enterprise devices:

- Device administration (DA) enrollments for Android 10:
  - **July 31, 2020:** Citrix deprecates new enrollments for the legacy Android device administration mode.
  - **November 1, 2020:** Google deprecates the legacy device administration API. Android 10 devices running in the legacy device administration mode will no longer work.
- MDX encryption:
  - **August 1, 2020:** Citrix starts enforcing migration from MDX encryption to platform encryption for Citrix mobile productivity and third-party MDX apps.
  - **September 1, 2020:** MDX encryption reaches end of life.

For devices enrolled in legacy DA

- If you don't use MDX encryption, no action is required.
- If you use MDX encryption, migrate Android devices to Android Enterprise before July 31, 2020. Devices running Android 10 must enroll or re-enroll using Android Enterprise. This requirement includes Android devices in MAM-only mode. See Migrate from device administration to Android Enterprise.

For devices already enrolled in Android Enterprise as of July 31

- If you published the apps using the Android Enterprise platform, encryption is already handled through Android Enterprise. No action is required.
- If you published the apps using the legacy Android platform, republish the apps using Android Enterprise before July 31, 2020.

Before you upgrade to XenMobile 10.12 (on-premises)

Some systems requirements changed. For information, see System requirements and compatibility and XenMobile compatibility.

1. Update your Citrix License Server to 11.16 or later before updating to the latest version of XenMobile Server 10.12.

   The latest version of XenMobile requires Citrix License Server 11.16 (minimum version).

   > **Note:**
   >
   > If you want to use your own license for the Preview, know that the Customer Success Services date (previously, Subscription Advantage date) in XenMobile 10.12 is January 20,

> 2020. The Customer Success Services date on your Citrix license must be later than this date.
>
> You can view the date next to the license in the License Server. If you connect the latest version of XenMobile to an older License Server environment, the connectivity check fails and you can't configure the License Server.

To renew the date on your license, download the latest license file from the Citrix Portal and upload the file to the Licensing Server. For more information, see Customer Success Services.

2. For a clustered environment: iOS policy and app deployments to devices running iOS 11 and later have the following requirement. If Citrix Gateway is configured for SSL persistence, you must open port 80 on all XenMobile Server nodes.
3. If the virtual machine running the XenMobile Server to be upgraded has less than 4 GB of RAM, increase the RAM to at least 4 GB. Keep in mind that the recommended minimum RAM is 8 GB for production environments.
4. Recommendation: Before you install a XenMobile update, use the functionality in your VM to take a snapshot of your system. Also, back up your system configuration database. If you experience issues during an upgrade, complete backups enable you to recover.

To upgrade

You can directly upgrade to XenMobile 10.12 from XenMobile 10.11.x or 10.10.x. To perform the upgrade, download the latest binary available: Go to https://www.citrix.com/downloads. Navigate to **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. On the tile for the XenMobile Server software for your hypervisor, click **Download File**.

To upload the upgrade, use the **Release Management** page in the XenMobile console. For more information, see To upgrade using the Release Management page.

After you upgrade

After you upgrade to XenMobile 10.12 (on-premises):

If functionality involving outgoing connections stop working, and you haven't changed your connections configuration, check the XenMobile Server log for errors such as the following: "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer".

The certificate validation error indicates that you need to disable host name verification on XenMobile Server. By default, host name verification is enabled on outgoing connections except for the Microsoft PKI server. If host name verification breaks your deployment, change the server property `disable.hostname.verification` to **`true`**. The default value of this property is **`false`**.

Additional support for iOS 13

XenMobile Server supports devices upgraded to iOS 13. The upgrade impacts your users as follows:

- During enrollment, a few new iOS Setup Assistant Option screens appear. Apple added new iOS Setup Assistant Option screens to iOS 13. The new options are included in the **Settings > Apple Device Enrollment Program (DEP)** page in this release. You can configure XenMobile Server to skip those screens. Those pages appear to users on iOS 13 devices.
- Some Restrictions device policy settings that were available on supervised or unsupervised devices for previous versions of iOS are available only on supervised devices for iOS 13+. The current XenMobile Server console tool tips don't yet indicate that these settings are for supervised devices for iOS 13+ only.
  - Allow hardware controls:
    - FaceTime
    - Installing apps
  - Allow apps:
    - iTunes Store
    - Safari
    - Safari > Autofill
  - Network - Allow iCloud actions:
    - iCloud documents & data
  - Supervised only settings - Allow:
    - Game Center > Add friends
    - Game Center > Multiplayer gaming
  - Media content - Allow:
    - Explicit music, podcasts, and iTunes U material

These restrictions apply as follows:

- If an iOS 12 (or lower) device is already enrolled in XenMobile Server and then upgrades to iOS 13, the preceding restrictions apply to unsupervised and supervised devices.
- If an unsupervised iOS 13+ device enrolls in XenMobile Server, the preceding restrictions apply only to supervised devices.
- If a supervised iOS 13+ device enrolls in XenMobile Server, the preceding restrictions apply only to supervised devices.

Apple Volume Purchase Program migration to Apple Business Manager (ABM) and Apple School Manager (ASM)

Companies and institutions using Apple Volume Purchase Program (VPP) need to migrate to Apps and Books in Apple Business Manager or Apple School Manager before December 1, 2019.

Before migrating VPP accounts in XenMobile, see this Apple support article.

If your organization or school only uses the Volume Purchase Program (VPP), you can enroll in ABM/ASM and then invite existing VPP Purchasers to your new ABM/ASM account. For ASM, navigate to https://school.apple.com. For ABM, navigate to https://business.apple.com.

To update your VPP account on XenMobile:

1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **iOS Settings**. The **Volume Purchase Program** configuration page appears.
3. Ensure that your ABM or ASM account has same app config as your previous VPP account.
4. In the ABM or ASM portal, download an updated token.
5. In the XenMobile console, do the following:
    a) Edit the existing volume purchase account with the updated token info for that location.
    b) Edit your ABM or ASM credentials. Don't change the suffix.
    c) Click **Save** twice.

For more information, see:

- Apple Deployment Program
- Bulk enrollment of Apple devices

Support for Android Enterprise COPE devices

XenMobile Server supports Android Enterprise fully managed devices with work profiles, formerly known as COPE (corporate-owned personally enabled) devices. These devices are a type of Android Enterprise fully managed devices that also have a work profile. You can apply separate policy settings to the device and the work profile. For this release:

- You can apply separate settings to the device and the work profile using these device policies: Credentials, Passcode, and Restrictions.
- You can apply the location mode setting of the Location device policy to COPE device itself but not to the work profile of COPE device. Other settings in the Location device policy are not available for COPE devices.
- You can apply the Lock security action separately to the device or the work profile.

Device policies

For Android Enterprise fully managed devices with work profiles (COPE devices), some device policies can apply separate settings to the entire device and the work profile. In the XenMobile Server console,

some device policies allow you to apply the separate settings. 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.

Security actions

For Android Enterprise fully managed devices with work profiles (COPE devices), you can apply:

- The Lock security action separately to the device or the work profile.
- All other security actions to the device.

Enrollment profiles control enrollment options for Android devices

Enrollment profiles now control how Android devices are enrolled if Android Enterprise in enabled for your XenMobile deployment. Enrollment profiles determine whether Android devices are enrolled in the default Android Enterprise mode (fully managed or work profile) or in legacy (device administrator) mode.

By default, the Global enrollment profile enrolls new and factory reset Android Enterprise devices as fully managed devices and enrolls BYOD Android Enterprise devices as work profile devices. For more information, see Android Enterprise.

Preparing legacy Android devices for Android Enterprise as default enrollment

Google is deprecating the device administrator mode of device management and encouraging 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, Android Enterprise is now the default enrollment option for Android devices.

This change means that if Android Enterprise is enabled for your XenMobile deployment, all newly enrolled or re-enrolled Android devices are enrolled as Android Enterprise devices.

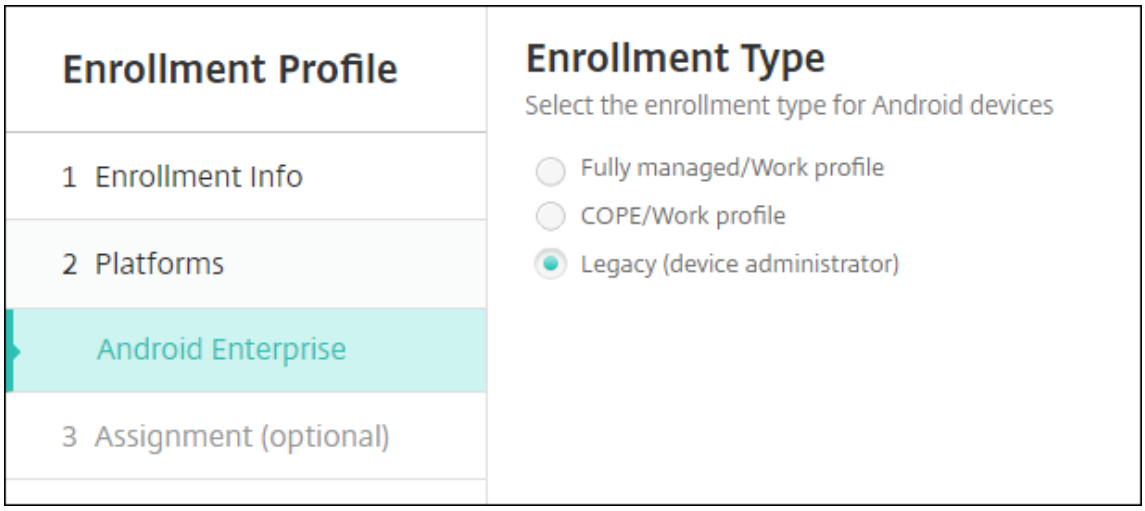
To prepare for this change, XenMobile now allows you to create enrollment profiles that control how Android devices are enrolled.

Your organization might not be ready to begin managing legacy Android devices in device owner mode or profile owner mode. In that case, you can continue to manage them in device administrator mode. Create an enrollment profile for legacy devices and re-enroll all enrolled legacy devices.

To create an enrollment profile for legacy devices:

1. In the XenMobile 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. Click **Next** or select **Android Enterprise** under **Platforms**. The Enrollment Configuration page appears.
4. Set **Management** to **Legacy (device administration)**. Click **Next** or Select **Assignment (options)**. The Delivery Group Assignment screen appears.



5. Choose the delivery group or delivery groups containing the administrators who enroll dedicated devices. Then click **Save**.

To continue managing legacy device 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.

For more information about Endpoint Management support for the transition to Android Enterprise, see the blog, Android Enterprise as default for Citrix Endpoint Management service.

Simplified app management for Android Enterprise

You no longer must go to managed Google Play or the Google Developer portal to approve or publish apps for XenMobile Server. As a result, app approval and publishing take about 10 minutes rather than hours.

Approve Android Enterprise apps for the Public App Store in the XenMobile Server console. You can now approve managed Google Play store apps without leaving the XenMobile Server console. After you enter an app name in the search field, the managed Google Play store UI opens with the instructions for you to approve and save the app. Your app then populates in the results allowing you to configure its details. See Add a public app store app.

Add MDX apps for Android Enterprise. The XenMobile Server console now supports Android Enterprise as a platform for MDX app deployment. See Add an MDX app.

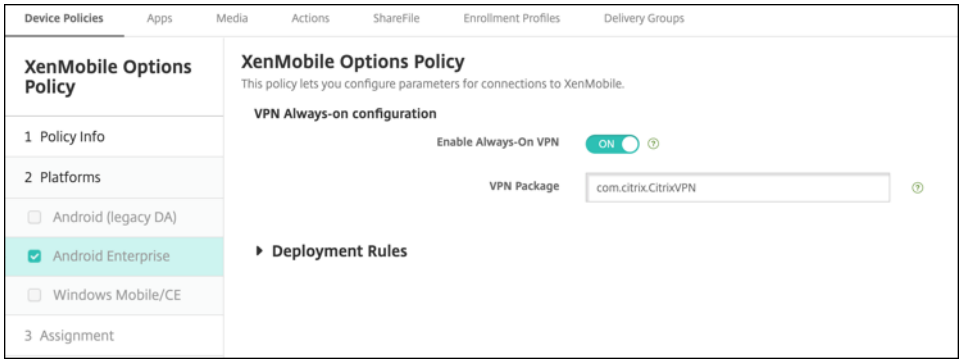
Approve MDX apps for Android Enterprise in the XenMobile Server console. You can now approve

managed Google Play store apps for Android Enterprise without leaving the XenMobile Server console. After you upload an MDX file, the managed Google Play store UI opens with the instructions for you to approve and save the app. See Add an MDX app.

Support for Always-On VPN for Android Enterprise

The XenMobile Server options device policy now lets you enable Always-On VPN for Android Enterprise.

When you configure VPN profiles for Android Enterprise, in the **Default VPN profile**, type the name of the VPN profile. XenMobile uses this profile when users tap the connect switch in the user interface of the Citrix SSO app instead of tapping 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.



Configure the product track for your Android Enterprise apps

When adding a public store app or an MDX app for Android Enterprise, configure the product track you want to push to user devices. For example, if you have a track designed for testing, you can select and assign it to a specific delivery group. To learn more about rolling out your release, see the Google Play Help Center. For information on configuring the product track, see Add an MDX app or Add a public app store app.

Force a passcode reset for macOS users

When a macOS device receives a configuration profile with a passcode policy, users must provide a passcode that meets the policy settings. You can now force a passcode reset the next time that a user authenticates. In the Passcode device policy for macOS (10.13 and later), enable the new setting **Force passcode reset**. For more information about the policy, see Passcode device policy.

What's new in XenMobile Server 10.11

October 13, 2020

XenMobile Server 10.11 (PDF Download)

XenMobile Migration Service

If you're using XenMobile Server on-premises, our free 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.

To start migration, contact your local Citrix salesperson or Citrix partner. For more information, see XenMobile Migration Service.

Apple Volume Purchase Program migration to Apple Business Manager (ABM) and Apple School Manager (ASM)

Companies and institutions using Apple Volume Purchase Program (VPP) must migrate to Apps and Books in Apple Business Manager or Apple School Manager before December 1, 2019.

Before migrating VPP accounts in XenMobile, see this Apple support article.

If your organization or school only uses the Volume Purchase Program (VPP), you can enroll in ABM/ASM and then invite existing VPP Purchasers to your new ABM/ASM account. For ASM, navigate to https://school.apple.com. For ABM, navigate to https://business.apple.com.

To update your volume purchase (formerly VPP) account on XenMobile:

1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **Volume Purchase**. The **Volume Purchase** configuration page appears.
3. Ensure that your ABM or ASM account has same app config as your previous VPP account.
4. In the ABM or ASM portal, download an updated token.
5. In the XenMobile console, do the following:
    a) Edit the existing volume purchase account with the updated token info for that location.
    b) Edit your ABM or ASM credentials. Don't change the suffix.
    c) Click **Save** twice.

Additional support for iOS 13

> **Important:**
>
> To prepare for device upgrades to iOS 12+: The Citrix VPN connection type in the VPN device policy for iOS doesn't support iOS 12+. Delete your VPN device policy and create a new VPN device policy with the Citrix SSO connection type.
>
> The Citrix VPN connection continues to operate in previously deployed devices after you delete the VPN device policy. Your new VPN device policy configuration takes effect in XenMobile Server 10.11, during user enrollment.

XenMobile Server supports devices upgraded to iOS 13. The upgrade impacts your users as follows:

- During enrollment, a few new iOS Setup Assistant Option screens appear. Apple added new iOS Setup Assistant Option screens to iOS 13. The new options are not included in the **Settings > Apple Device Enrollment Program (DEP)** page in this release. As a result, you can't configure XenMobile Server to skip those screens. Those pages appear to users on iOS 13 devices.
- Some Restrictions device policy settings that were available on supervised or unsupervised devices for previous versions of iOS are available only on supervised devices for iOS 13+. The current XenMobile Server console tool tips don't yet indicate that these settings are for supervised devices for iOS 13+ only.
  - Allow hardware controls:
    - FaceTime
    - Installing apps
  - Allow apps:
    - iTunes Store
    - Safari
    - Safari > Autofill
  - Network - Allow iCloud actions:
    - iCloud documents & data
  - Supervised only settings - Allow:
    - Game Center > Add friends
    - Game Center > Multiplayer gaming
  - Media content - Allow:
    - Explicit music, podcasts, and iTunes U material

These restrictions apply as follows:

- If an iOS 12 (or lower) device is already enrolled in XenMobile Server and then upgrades to iOS 13, the preceding restrictions apply to unsupervised and supervised devices.
- If an unsupervised iOS 13+ device enrolls in XenMobile Server, the preceding restrictions apply only to supervised devices.

- If a supervised iOS 13+ device enrolls in XenMobile Server, the preceding restrictions apply only to supervised devices.

Requirements for trusted certificates in iOS 13 and 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 Uploading certificates in XenMobile.

Upgrade from GCM to FCM

As of April 10, 2018, Google deprecated Google Cloud Messaging (GCM). Google removed the GCM server and client APIs on May 29, 2019.

> **Important requirements:**
>
> - Upgrade to the latest version of XenMobile Server.
> - Upgrade to the latest version of Secure Hub.

Google recommends upgrading to Firebase Cloud Messaging (FCM) right away to begin taking advantage of the new features available in FCM. For information from Google, see https://developers.google.com/cloud-messaging/faq and https://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.html.

To continue support for push notifications to your Android devices: If you use GCM with XenMobile Server, migrate to FCM. Then, update XenMobile Server with the new FCM key available from the Firebase Cloud Messaging Console.

The following steps reflect the enrollment workflow when you use trusted certificates.

Upgrade steps:

1. Follow the information from Google to upgrade from GCM to FCM.
2. In the Firebase Cloud Messaging Console, copy your new FCM key. You will need it for the next step.
3. In the XenMobile Server console, go to **Settings > Firebase Cloud Messaging** and configure your settings.

Devices switch over to FCM the next time they check in with XenMobile Server and do a policy refresh. To force Secure Hub to refresh policies: In Secure Hub, go to **Preferences > Device Information** and tap **Refresh Policy**.
For more information about configuring FCM, see Firebase Cloud Messaging.

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. These blogs discuss the XenMobile Migration Service:

New XenMobile Migration Service

Making the Case for XenMobile in the Cloud

Before you upgrade to XenMobile 10.11 (on-premises)

Some systems requirements changed. For information, see System requirements and compatibility and XenMobile compatibility.

1. Update your Citrix License Server to 11.15 or later before updating to the latest version of XenMobile Server 10.11.

   The latest version of XenMobile requires Citrix License Server 11.15 (minimum version).

   > **Note:**
   >
   > If you want to use your own license for the Preview, know that the Customer Success Services date (previously, Subscription Advantage date) in XenMobile 10.11 is April 9, 2019. The Customer Success Services date on your Citrix license must be later than this date.
   >
   > You can view the date next to the license in the License Server. If you connect the latest version of XenMobile to an older License Server environment, the connectivity check fails and you can't configure the License Server.

   To renew the date on your license, download the latest license file from the Citrix Portal and upload the file to the Licensing Server. For more information, see Customer Success Services.

2. For a clustered environment: iOS policy and app deployments to devices running iOS 11 and later have the following requirement. If Citrix Gateway is configured for SSL persistence, you must open port 80 on all XenMobile Server nodes.

3. If the virtual machine running the XenMobile Server to be upgraded has less than 4 GB of RAM, increase the RAM to at least 4 GB. Keep in mind that the recommended minimum RAM is 8 GB for production environments.

4. Recommendation: Before you install a XenMobile update, use the functionality in your VM to take a snapshot of your system. Also, back up your system configuration database. If you experience issues during an upgrade, complete backups enable you to recover.

To upgrade

You can directly upgrade to XenMobile 10.11 from XenMobile 10.10.x or 10.9.x. To perform the upgrade, download the latest binary available: Go to https://www.citrix.com/downloads. Navigate to **Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10**. On the tile for the XenMobile Server software for your hypervisor, click **Download File**.

To upload the upgrade, use the **Release Management** page in the XenMobile console. For more information, see To upgrade using the Release Management page.

After you upgrade

After you upgrade to XenMobile 10.11 (on-premises):

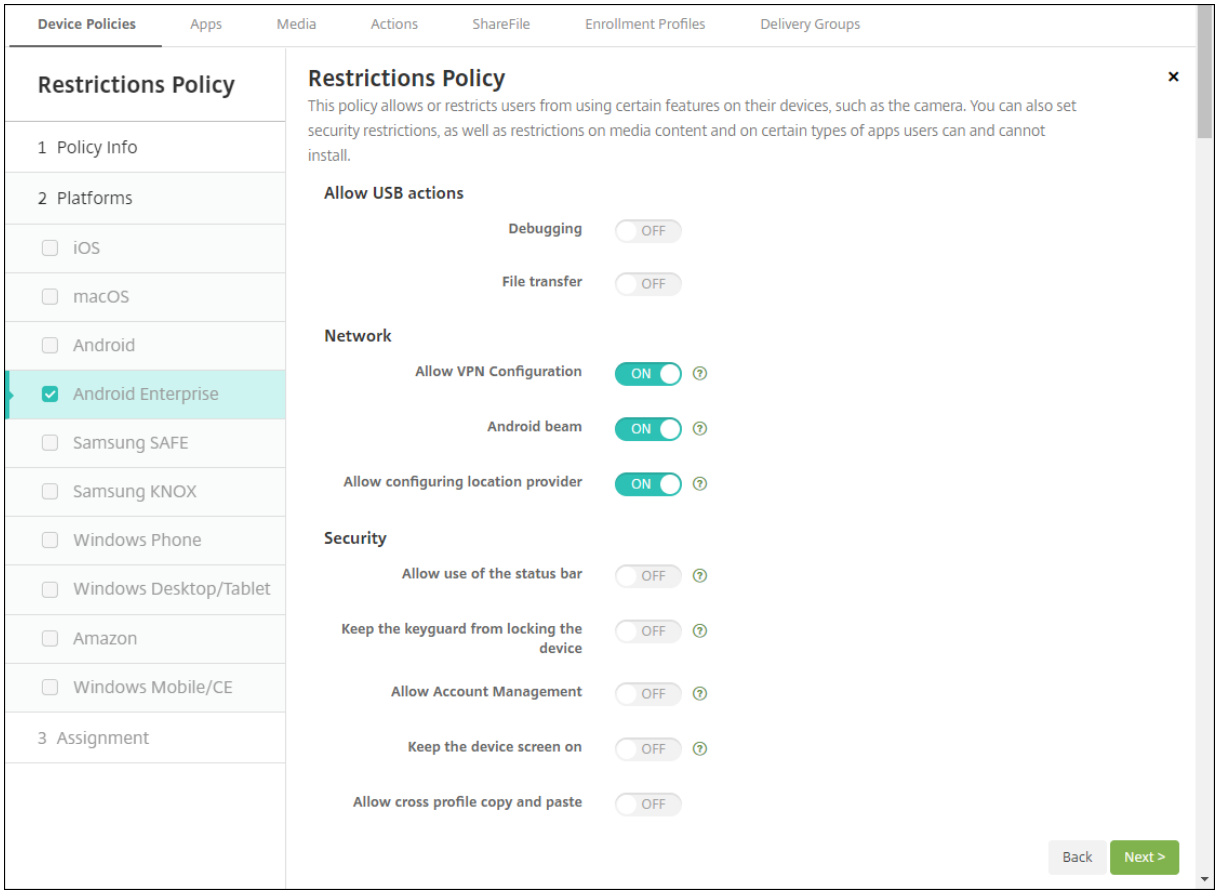
If functionality involving outgoing connections stop working, and you haven't changed your connections configuration, check the XenMobile Server log for errors such as the following: "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer".

The certificate validation error indicates that you need to disable host name verification on XenMobile Server. By default, host name verification is enabled on outgoing connections except for the Microsoft PKI server. If host name verification breaks your deployment, change the server property `disable.hostname.verification` to **`true`**. The default value of this property is **`false`**.

New and updated device policy settings for Android Enterprise devices

Samsung Knox and Android Enterprise policy unification. For Android Enterprise devices running Samsung Knox 3.0 or later and Android 8.0 or later: Knox and Android Enterprise are combined into a unified device and profile management solution.
Configure Knox settings on the Android Enterprise page of the following device policies:

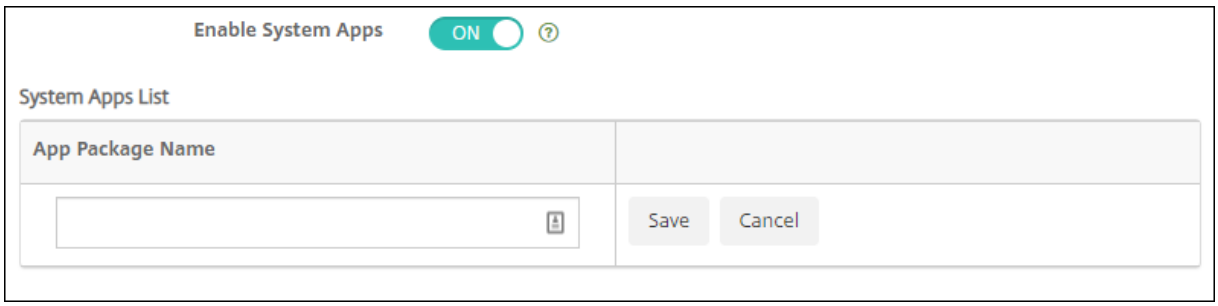
- **OS Update device policy.** Includes settings for Samsung Enterprise FOTA updates.
- **Passcode device policy.**
- **Samsung MDM license key device policy.** Configures the Knox license key.
- **Restrictions device policy settings.**



App inventory device policy for Android Enterprise. You can now collect an inventory of the Android Enterprise apps on managed devices. See App inventory device policy.

Access all Google Play apps in the managed Google Play store. The **Access all apps in the managed Google Play store** server property makes all apps from the public Google Play store accessible from the managed Google Play store. Setting this property to **true** allows the public Google Play store apps for all Android Enterprise users. Administrators can then use the Restrictions device policy to control access to these apps.

Enable system apps on Android Enterprise devices. To allow users to run pre-installed system apps in the Android Enterprise work profile mode or fully managed mode, configure the Restrictions device policy. That configuration grants user access to default device apps, such as camera, gallery, and others. To restrict access to a particular app, set app permissions using the Android Enterprise app permissions device policy.



Support for Android Enterprise dedicated devices. XenMobile now supports the management of dedicated devices, previously called corporate owned single use (COSU) 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 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.

For information about provisioning Android Enterprise devices, see Provisioning dedicated Android Enterprise devices.

Renamed policy. To align with Google terminology, the Android Enterprise app restriction device policy is now called Android Enterprise managed configurations. See Android Enterprise managed configurations device policy.

Lock and reset password for Android Enterprise

XenMobile now supports the Lock and Reset password security action for Android Enterprise devices. Those devices must be enrolled in work profile mode running Android 8.0 and greater.

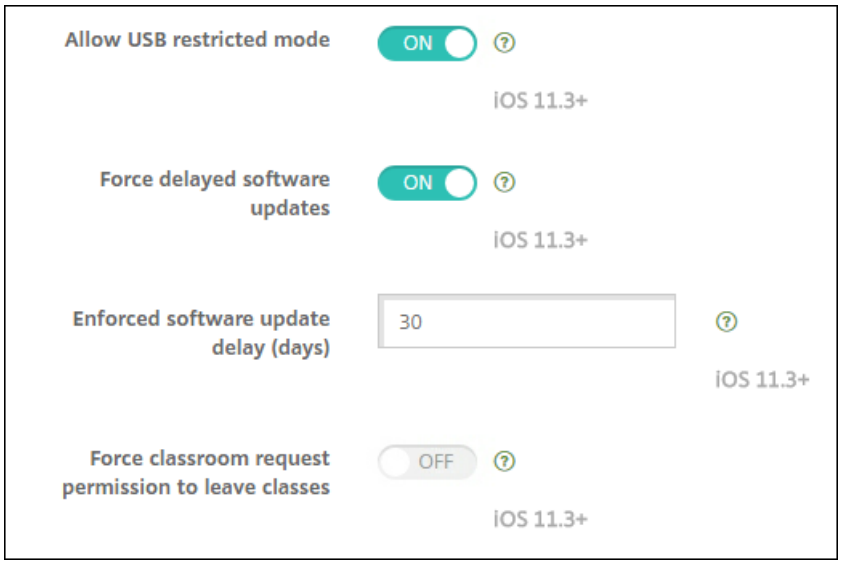
- The passcode sent locks the work profile. The device is not locked.
- If no passcode is sent or the passcode sent doesn't meet passcode requirements:
  - And no passcode is already set on the work profile, the device is locked.
  - And a passcode is already set on the work profile, the work profile is locked but device is not locked.

For more information on the lock and reset password security actions, see Security actions.

New Restrictions device policy settings for iOS or macOS

- **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.

- **Password AutoFill:** Optional. If disabled, users cannot use the AutoFill Passwords or Automatic Strong Passwords features. Default is **On**. Available as of iOS 12 and macOS 10.14.
- **Password proximity requests:** Optional. If disabled, users' devices don't request passwords from nearby devices. Default is **On**. Available as of iOS 12 and macOS 10.14.
- **Password Sharing:** Optional. If disabled, users can't share their passwords using the AirDrop Passwords feature. Default is **On**. Available as of iOS 12 and macOS 10.14.
- **Force automatic date and time:** Supervised. If enabled, users can't disable the option **General > Date & Time > Set Automatically**. Default is **Off**. Available as of iOS 12.
- **Allow USB restricted mode:** Only available for supervised devices. If set to Off, the device can always connect to USB accessories while locked. Default is **On**. Available as of iOS 11.3.
- **Force delayed software updates:** Only available for supervised devices. If set to **On**, delays user visibility of Software Updates. With this restriction in place, the user will not see a software update until the specified number of days after the software update release date. Default is **Off**. Available as of iOS 11.3 and macOS 10.13.4.
- **Enforced software update delay (days):** Only available for supervised devices. This restriction allows the admin to set how long to delay a software update on the device. The max is 90 days and the default value is **30**. Available as of iOS 11.3 and macOS 10.13.4.
- **Force classroom request permission to leave classes:** Only available for supervised devices. If set to **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 as of iOS 11.3.



See Restrictions device policy.

Exchange device policy updates for iOS or macOS

More S/MIME Exchange signing and encryption settings as of iOS 12. The Exchange device policy now includes settings to configure S/MIME signing and encryption.

For S/MIME signing:

- **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**.
- **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**.

For S/MIME encryption:

- **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**.
- **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**.

Exchange OAuth settings as of iOS 12. You can now configure the connection with Exchange to use OAuth for authentication.

Exchange OAuth settings as of macOS 10.14. You can now configure the connection with Exchange to use OAuth for authentication. For authentication using OAuth, you can specify the sign-in URL for a setup that doesn't use autodiscovery.

See Exchange device policy.

Mail device policy updates for iOS

More S/MIME Exchange signing and encryption settings as of iOS 12. The Mail device policy includes more settings to configure S/MIME signing and encryption.

For S/MIME signing:

- **Enable S/MIME Signing:** Select whether this account supports S/MIME signing. The default is **On**. When set to **On**, the following fields appear.
  - **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.

For S/MIME encryption:

- **Enable S/MIME Encryption:** Select whether this account supports S/MIME encryption. The default is **Off**. When set to **On**, the following fields appear.
  - **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.

See Mail device policy.

Apps notifications device policy updates for iOS

The following Apps notifications settings are available as of iOS 12.

- **Show in CarPlay:** If **On**, notifications display in Apple CarPlay. 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. Default is **Off**.

See Apps notifications device policy

Support for shared iPads used with Apple Education

The XenMobile integration with Apple Education features now supports shared iPads. Multiple students in a classroom can share an iPad for different subjects taught by one or several instructors.

Either you or instructors enroll shared iPads and then deploy device policies, apps, and media to the devices. After that, students 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.

Prerequisites for shared iPads:

- Any iPad Pro, iPad 5th generation, iPad Air 2 or later, and iPad mini 4 or later
- At least 32 GB of storage
- Supervised

For more information, see Configure shared iPads.

Role-based access control (RBAC) permissions change

The RBAC permission Add/Delete Local Users is now split into two permissions: Add Local Users and Delete Local Users.

For more information, see Configure roles with RBAC.

Third-party notices

January 29, 2019

This release of XenMobile might include third-party software licensed under the terms defined in the following documents:

XenMobile Third-Party Notices

Deprecation

May 4, 2021

The announcements in this article are intended to give you advanced notice of the XenMobile Server features that are being phased out. We provide this information 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 XenMobile Server 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 XenMobile Server.

For information about the mobile productivity apps that reached End of Life, see EOL and deprecated apps.

Item	Description	Deprecation announced	Removed	Alternative
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: June 30, 2021	Use KME to enroll in Android Enterprise mode. Android 8, 9, 10, 11 support Android Enterprise.
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	Target: 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.
Derived credentials	Deprecated support for derived credentials and the Citrix Derived Credentials Manager app.	March 25, 2021	Target: Q2 2021	See iOS for a list of authentication types supported for iOS.

Item	Description	Deprecation announced	Removed	Alternative
Internet Explorer 11	Deprecated support of Internet Explorer use with the XenMobile Server console.	January 2021	January 2021	Use the latest version of these web browsers: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari
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.
Android - Sony	Deprecated support for Android Sony devices and Sony-specific policies.	January 2021	February 2021	Use Android Enterprise
Android - HTC	Deprecated support for Android HTC devices and HTC-specific policies.	January 2021	February 2021	Use Android Enterprise
Third party component of the XenMobile dashboard	We will deprecate a third party component used as part of the XenMobile dashboard.	December 2020	January 2021	To continue using the dashboard, upgrade to XenMobile 10.12 or later

Item	Description	Deprecation announced	Removed	Alternative
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.
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 `*.push.apple.com`.	October 2020	Target: April 2021	Use port 443 or 2197 instead. See Open XenMobile ports to manage devices.

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 Plug-in (KSP) app for Android Enterprise. See Add the Knox service plug-in app.
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).
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	January 2021	When you create a CSR for a credential provider in the XenMobile console (**Settings > Credential Providers > Certificate Signing Request**), choose a stronger cipher.

Item	Description	Deprecation announced	Removed	Alternative
Database servers	Deprecated support for Microsoft SQL Server 2012 R2 and earlier and Microsoft SQL Server 2012 SP4 and earlier.	May 2020	August 2020	Update the system to one of the following supported versions: Microsoft SQL Server 2014 SP3, Microsoft SQL Server 2016 SP2, Microsoft SQL Server 2017 CU 13, or Microsoft SQL Server 2019 CTP 3.2. See the list of supported servers in System requirements and compatibility.

Item	Description	Deprecation announced	Removed	Alternative
Hypervisors	Deprecated support for Citrix XenServer 6.5.x and earlier, VMware ESXi 5.5 Update 3 and earlier, and Hyper-V 2012.	May 2020	August 2020	Update the system to one of the following supported versions: Citrix Hypervisor 8.0 and later, Citrix XenServer 7.0 and later, VMware (ESXi 6.0, ESXi 6.5.0 Update 3, ESXi 6.7 Update 2 patch 10, or ESXi 7.0), or Hyper-V (Windows Server 2016 or Windows Server 2019).
Citrix Launcher	Deprecated support for the Citrix Launcher app.	May 2020	August 2020 (remove from the app store)	Provision devices as kiosks (dedicated devices). For more information, see Citrix Launcher replacement.
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.

Item	Description	Deprecation announced	Removed	Alternative
MDX Toolkit and MDX Service	Deprecated support for the MDX Toolkit and MDX Service 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: September 2021	To continue managing your enterprise applications, use the MAM SDK.
MDX: Alternative Gateway Server	Deprecated step-up authentication for iOS and Android devices.	March 2020	Target: September 2021	No 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.

Item	Description	Deprecation announced	Removed	Alternative
MDX shared device support	Deprecated shared device support for MDX apps.	March 2020	Target: September 2021	For Android Enterprise, use shared device support for MDM. For iOS, use Apple School Manager or GroundControl.
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.

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.
MDX encryption	Deprecated MDX encryption and the MDX encryption feature in the XenMobile 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.

Item	Description	Deprecation announced	Removed	Alternative
Passcode device policy: The **No Restrictions** setting for Android Enterprise	Android Enterprise devices running Android 7 or higher only support a passcode created with character restrictions. If you previously set **Required characters** to **No Restrictions**, this update changes that value to **Numbers only**.	February 2019	April 2019	This change doesn't affect the current user sign-in experience.
Remote Support	Deprecated the Remote Support client for clustered on-premises XenMobile Server deployments.	January 2019	August 2020	No alternative

Item	Description	Deprecation announced	Removed	Alternative
Secure Hub Network Extensions for iOS	Deprecated the Network Extension framework that allowed you to customize networking features for iOS devices, as of Secure Hub release 20.3.0.	October 2018	March 2020	No alternative
TLS versions 1.0 and 1.1	To improve the security of XenMobile, Citrix now blocks any communication over Transport Layer Security (TLS) 1.0 and 1.1. As a result of its weakening security, the PCI Council is deprecating TLS 1.0 and TLS 1.1.	June 2018	March 2019	Upgrade to TLS 1.2.
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
Android TouchDown	DigiCert stopped supporting Android TouchDown. Citrix will remove the Android TouchDown platform page from the Exchange device policy.	July 2018	2021	Recommendation: Use Citrix Secure Mail.

Fixed issues

July 1, 2021

XenMobile 10.13 includes the following fixed issues:

- XenMobile Server experiences a communications error with Apple Deployment Programs (formerly DEP). For more information, see https://support.citrix.com/article/CTX267079. [CXM-76053]
- Unable to upload iOS public apps in the App Store using App Store URL. [CXM-76900]
- User ID on a single device is mapped to several user IDs. [CXM-76915]
- Intermittent deadlocks in the database server cause enrollment failures. [CXM-77336]
- Administrators with the RBAC permission to send enrollment invitations can export unlimited invitations. [CXM-77340]
- Unable to upload iOS public apps in the App Store using the public APIs for XenMobile. [CXM-77656]
- For a few installed apps, the version is blank for the app inventory shown on the **Manage > Devices > Device Details** page. [CXM-79025]
- You can't use the XenMobile Server console to edit the Exchange device policy. [CXM-79080]
- You can't use the XenMobile Server console to update the version for some VPP apps. You get the following error: **A configuration error occurred. Please try again**. [CXM-79728]

- Apple iTunes volume purchase apps can't synchronize with XenMobile. [CXM-80064]
- Unable to use the managed configurations device policy with a Knox Service plugin application. [CXM-80233]
- You are unable to import the enterprise.config file on the XenMobile Server. You get the following error: **Failed to import certificate.** [CXM-80737]
- Required and optional MDX apps added post enrollment are not displayed in Play Store. [CXM-80961]
- You can't access the XenMobile Server console using customized ports. [CXM-81841]
- You can't configure multiple bookmarks due to the character limit in the **Managed bookmarks** field. [CXM-82524]
- On the XenMobile Server, **Check for Updates** doesn't work for App details. [CXM-84259]
- On the XenMobile Server, you can't install apps from Managed Google Play when you enrol with **SamAccountName**. [CXM-84973]
- The mobile device management (MDM) enrollment of devices running iOS 14 fails consistently when the server property ios.mdm.enrollment.installRootCaIfRequired is set to true.[CXM-85028]
- Two PKC12 certificates are created for the same user, resulting in intermittent access to the internal network for that user. [CXM-87288]
- For fixed issues related to mobile productivity apps, see Secure Hub, Secure Mail, and Secure Web.
- For fixed issues in version 10.12.0 rolling patch release, see:
  - XenMobile Server 10.12.0 Rolling Patch 8
  - XenMobile Server 10.12.0 Rolling Patch 7
  - XenMobile Server 10.12.0 Rolling Patch 6

Related information

- XenMobile Support Knowledge Center

Known issues

February 22, 2021

XenMobile 10.13 includes the following known issue:

- After you import the XenMobile Server 10.8 or 10.9 image into VMware ESXi 6.7 or 6.5 Update 2: After you restart the VM, the configuration app doesn't start, XenMobile Server goes into recovery mode, and the IP settings are cleared. To work around this issue, build a new VM with a VMXNET3 NIC, then join that VM to the database of the VM that went into recovery mode. [CXM-54581]
- For known issues related to mobile productivity apps, see Secure Hub, Secure Mail, and Secure Web.
- For known issues in the latest version 10.12.0 rolling patch release, see:
  - XenMobile Server 10.12.0 Rolling Patch 5

Related information

- XenMobile Support Knowledge Center

Architecture

September 17, 2020

The device and app management requirements of your organization determine the XenMobile components in your XenMobile architecture. The components of XenMobile 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.
- XenMobile is where you manage those apps and devices.

Deploying XenMobile components: You can deploy XenMobile to enable users to connect to resources in your internal network in the following ways:

- Connections to the internal network. If your users are remote, they can connect by using a VPN or micro VPN connection through Citrix Gateway. That connection provides access to apps and desktops in the internal network.
- Device enrollment. Users can enroll mobile devices in XenMobile so you can manage the devices in the XenMobile console that connect to network resources.
- Web, SaaS, and mobile apps. Users can access their web, SaaS, and mobile apps from XenMobile through Secure Hub.
- Windows-based apps and virtual desktops. Users can connect with Citrix Receiver or a web browser to access Windows-based apps and virtual desktops from StoreFront or the Web Interface.

To achieve any of those capabilities for an on-premises XenMobile Server, Citrix recommends deploying XenMobile components in the following order:

- Citrix Gateway. You can configure settings in Citrix Gateway to enable communication with XenMobile, StoreFront, or the Web Interface by using the Quick Configuration wizard. Before using the Quick Configuration wizard in Citrix Gateway, you must install one of the following components to set up communications: XenMobile, StoreFront, or the Web Interface.
- XenMobile. After you install XenMobile, you can configure policies and settings in the XenMobile console that allow users to enroll their mobile devices. You also can configure mobile, web, and SaaS apps. Mobile apps can include apps from the Apple App Store or Google Play. Users can also connect to mobile apps you wrap with the MDX Toolkit and upload to the console.
- MAM SDK or MDX Service. The MDX wrapping technology is scheduled to reach end of life (EOL) in September 2021. 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.
  - The MDX Service securely wraps mobile apps created within your organization or outside the company. For more information, see MDX Service.
- StoreFront (optional). You can provide access to Windows-based apps and virtual desktops from StoreFront through connections with Receiver.
- Citrix Files (optional). If you deploy Citrix Files, you can enable enterprise directory integration through XenMobile, which acts as a Security Assertion Markup Language (SAML) identity provider. For more information about configuring identity providers for Citrix Content Collaboration, see the Content Collaboration support site.

XenMobile provides device management and app management through the XenMobile console. This section describes the reference architecture for the XenMobile deployment.

In a production environment, Citrix recommends deploying the XenMobile solution in a cluster configuration for both scalability and server redundancy. Also, using the Citrix ADC SSL Offload capability can further reduce the load on the XenMobile Server and increase throughput. For more information about how to set up clustering for XenMobile by configuring two load balancing virtual IP addresses on Citrix ADC, see Clustering.

For more information about configuring XenMobile for a disaster recovery deployment, see the Deployment Handbook Disaster Recovery article. That article includes an architecture diagram.

The following sections describe different reference architectures for the XenMobile deployment. For reference architecture diagrams, see the XenMobile Deployment Handbook articles, Reference Architecture for On-Premises Deployments and Architecture. For a complete list of ports, see Port requirements (on-premises) and Port requirements (cloud).

Mobile device management (MDM) mode

> **Important:**
>
> If you configure MDM mode and later change to ENT mode, be sure to use the same (Active Directory) authentication. XenMobile doesn't support changing the authentication mode after user enrollment. For more information, see Upgrade from XenMobile MDM Edition to Enterprise Edition.

XenMobile MDM Edition provides mobile device management. For platform support, see Supported device operating systems. If you plan to use only the MDM features of XenMobile, you deploy XenMobile in MDM mode. For example, if you want to do the following.

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

In the recommended model, the XenMobile Server is positioned in the DMZ with an optional Citrix ADC in front, which provides more protection for XenMobile.

Mobile app management (MAM) mode

MAM, also called MAM-only mode, provides mobile app management. For platform support, see Supported device operating systems. If you plan to use only the MAM features of XenMobile without having devices enroll for MDM, you deploy XenMobile in MAM mode. For example, if you want to do the following.

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

The devices cannot be MDM enrolled.

In this deployment model, XenMobile Server is positioned with Citrix Gateway in front, which provides more protection for XenMobile.

MDM+MAM mode

Using MDM and MAM modes together provides mobile app and data management and mobile device management. For platform support, see Supported device operating systems. If you plan to use MDM+MAM features of XenMobile, you deploy XenMobile in ENT (enterprise) mode. For example, if you want to:

- 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

In the recommended deployment model, the XenMobile Server is positioned in the DMZ with Citrix Gateway in front, which provides more protection for XenMobile.

XenMobile in the internal network: Another deployment option is to position an on-premises XenMobile Server in the internal network, rather than in the DMZ. This deployment is used if your security policy requires that only network appliances can be placed in the DMZ. In this deployment, the XenMobile Server is not in the DMZ. Therefore, there is no requirement to open ports on the internal firewall to allow access to SQL Server and PKI servers from the DMZ.

System requirements and compatibility

March 1, 2021

> **Note:**
>
> This article covers system requirements and compatibility for XenMobile Server 10.13. For system requirements for Endpoint Management, see System requirements.

For more requirements and compatibility information, see the following articles:

- XenMobile compatibility
- Supported device operating systems
- Port requirements
- Scalability
- Licensing
- FIPS 140-2 compliance
- Language support

To run XenMobile 10.13, you need the following minimum system requirements:

- One of the following:
  - Citrix Hypervisor 8.1 or 8.0, or Citrix XenServer (supported versions: 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2); for details, see XenServer
  - VMware (supported versions: ESXi 6.0, ESXi 6.5.0 Update 3, or ESXi 6.7 Update 2 patch 10, ESXi 7.0); for details, see ESXi 6.7 workaround and VMware
  - Hyper-V (supported versions: Windows Server 2016 and Windows Server 2019); for details, see Hyper-V
- Endpoint Management connector for Exchange ActiveSync 10.1.10 or Citrix Gateway connector for Exchange ActiveSync 8.5.3.19

- Dual core processor
- Four virtual CPUs
- 8 GB of RAM for production environments; 4 GB of RAM for proof of concept and test environments
- 50 GB of disk space
- Citrix License Server 11.16.

  Update your Licensing Server before upgrading your XenMobile Server.

ESXi 6.7 workaround

For ESXi 6.7 to work, you must perform the following workaround.

1. Using the OVF tool provided by VMware, extract the OVA file downloaded from citrix.com. Get the OVF tool from VMware's page(https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491).
2. Of the three files extracted, upload the .vmdk file to your data store.
3. Create a new virtual machine.
   a) Name the virtual machine and select **ESX/ESXi 4.x virtual machine** as the compatibility option.
   b) For the Guest OS family, select **Linux**.
   c) For the Guest OS version, select **Other 2.6.x Linux (64-bit)**.
   d) For data store, select **Default**.
   e) During customization, remove the default hard disk, USB controller, and CD/DVD drive.
   f) Under Network, as the adapter type, select **VMXNET3**.
   g) On ESXi, if your disks are local, select **SCSI Controller** and **LSI Logic Parallel**. If you're using a shared disk, select **VMware Paravirtual**.
   h) Click Next to finish VM creation.
4. Navigate to your data store and copy the .vmdk file you uploaded earlier. Copy it into the VM directory you created for XenMobile.
5. From the ESXi web interface, select the VM and edit the settings.
6. Click **Add Hard disk**.
7. Select the .vmdk file copied earlier and attach it to the VM.
8. Click **Save**.
9. Power on your VM.

Citrix Gateway system requirements

To run Citrix Gateway with XenMobile 10.13, you need the following minimum system requirements.

- Citrix Gateway (on-premises). Supported versions: 12.1 or above
- You also must be able to communicate with Active Directory, which requires a service account. You only need query and read access.

XenMobile 10.13 database requirements

XenMobile requires one of the following databases:

- Microsoft SQL Server

  XenMobile supports a Microsoft SQL Server database running one of the following supported versions. For more information about Microsoft SQL Server databases and their hardware requirements, see the Microsoft documentation.

  - Microsoft SQL Server 2014 SP3
  - Microsoft SQL Server 2016 SP2
  - Microsoft SQL Server 2017 CU 21
  - Microsoft SQL Server 2019 CU 8

  Your Microsoft SQL Server database requirements also depend on the size of your deployment. For more information about Microsoft SQL Server database requirements for your deployment size, see Scalability.

  XenMobile supports SQL Basic Availability Groups (Always On Availability Groups) and SQL Clustering for database high availability.

  Citrix recommends using Microsoft SQL remotely.

  For information about upgrading Microsoft SQL, see the Microsoft article Upgrade SQL Server.

- PostgreSQL (for test environments only). PostgreSQL is included with XenMobile. You can use it locally or remotely in test environments. Database migration is not supported. You can't move databases created in a test environment to a production environment.

  All XenMobile editions support Remote PostgreSQL 9.5.1 and 9.5.11 for Windows with the following limitations: Not recommended for production environments. Support for up to 300 devices. Use on-premises SQL Server for more than 300 devices. No support for clustering.

SQL Server service account requirements

Ensure that the service account of the SQL Server to be used with XenMobile has the `DBcreator` role permission. Record the SQL server account password that you specify during XenMobile Server installation. That password is required if you need to clone the XenMobile database during XenMobile Server recovery.

Secure your SQL Server databases using Transparent Data Encryption (TDE). Don't allow external access to SQL Server ports, as shown in the refernce architecture in Reference Architecture for On-Premises Deployments.

For more information about SQL Server service accounts, see the following pages on the Microsoft documentation site. These links point to information for SQL Server 2014. If you are using a different version, choose your server version from the **Other Versions** list:

- Configure Windows Service Accounts and Permissions
- Server-Level Roles

Virtual Apps and Desktops compatibility

- Virtual Apps and Desktops 7.15 LTSR CU3
- Virtual Apps and Desktops 7.1811
- Virtual Apps and Desktops 7 1906
- Virtual Apps and Desktops 7 1909
- Virtual Apps and Desktops 7 2006

StoreFront compatibility

- StoreFront 3.12.2
- StoreFront 7 1811
- StoreFront 7 1906
- StoreFront 7 1909
- StoreFront 7 2006

Other compatibility

- Endpoint Management connector for Exchange ActiveSync 10.1.10
  - Older versions aren't tested
- Citrix Gateway connector for Exchange ActiveSync 8.5.3.19
  - Older versions aren't tested

XenMobile compatibility

January 28, 2021

> **Note:**
>
> This article covers XenMobile Server compatibility. For components tested with Endpoint Management, see Endpoint Management compatibility.

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 Service and MDX Toolkit are scheduled to reach end of life (EOL) in September 2021. To continue managing your enterprise apps, you must incorporate the MAM SDK.

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

Supported versions and upgrade paths

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

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 details, see the Citrix Product Matrix.

Citrix supports the distribution of XenMobile productivity apps only from a public app store.

XenMobile Server (on-premises)

- Citrix supports upgrades from the last two versions of XenMobile Server.
- Latest version of XenMobile Server:
  - XenMobile Server 10.13
- Upgrade from:
  - XenMobile Server 10.12.x
  - XenMobile Server 10.11.x

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 and MDX Service

The MDX wrapping technology is scheduled to reach end of life (EOL) in September 2021. 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.
- Or, you can use the MDX Service to wrap apps. See MDX Service.

Browser support

The XenMobile Server 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

April 6, 2021

> **Note:**
>
> This article covers supported device operating systems for XenMobile Server 10.13. For operating systems supported for Endpoint Management, see Supported device operating systems.

XenMobile supports devices running the following platforms and operating systems for enterprise mobility management, including app and device management. Because of platform restrictions and security features, XenMobile doesn't support all functionality on all platforms.

The supported device platform information in this article also applies to XenMobile connector for Exchange ActiveSync and Citrix Gateway connector for Exchange ActiveSync.

For the latest versions of the mobile productivity apps, as well as supported devices for MDX encryption, 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 XenMobile 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

  For Android 10+, see Android Considerations.

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

  XenMobile and Citrix mobile apps are compatible with iOS 14.x, but don't currently support all new iOS 14.x features. The MDX Service currently doesn't support wrapping iOS apps for iOS 14.x. To wrap in-house enterprise apps for iOS 14.x, use the MDX Toolkit 20.8.5 or later.

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

  XenMobile 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

  XenMobile and Citrix mobile apps are compatible with macOS 11, but don't currently support all new macOS 11 features.

- **Windows 10 Desktops and Tablets:** Windows 10 RS4 and RS5 (MDM only)

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

- **Windows Mobile/CE:** (MDM only). Starting the second quarter of 2018, support for Windows Mobile/CE devices is no longer available.

- **Samsung SAFE and Knox:** On compatible Samsung devices, XenMobile supports and extends both Samsung for Enterprise (SAFE) and Samsung Knox policies. XenMobile 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.

- 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.

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.

Port requirements

April 28, 2021

To enable devices and apps to communicate with XenMobile, you open specific ports in your firewalls. The following tables list the ports that must be open.

Open ports for Citrix Gateway and XenMobile to manage apps

Open the following ports to allow user connections from Citrix Secure Hub, Citrix Receiver, and the Citrix Gateway plug-in through Citrix Gateway to the following components:

- XenMobile
- StoreFront
- Citrix Virtual Apps and Desktops
- Citrix Gateway connector for Exchange ActiveSync
- Other internal network resources, such as intranet websites

To enable traffic to Launch Darkly from Citrix ADC, you can use the IP addresses noted in this Support Knowledge Center article.

For more information about Citrix Gateway, see the Citrix Gateway documentation. That documentation includes information about Citrix ADC IP (NSIP) virtual server IP (VIP) and subnet IP (SNIP) addresses.

TCP port	Description	Source	Destination
21 or 22	Used to send support bundles to an FTP or SCP server.	XenMobile	FTP or SCP server
53 (TCP and UDP)	Used for DNS connections.	Citrix Gateway, XenMobile	DNS Server
80	Citrix Gateway passes the VPN connection to the internal network resource through the second firewall. This situation typically occurs if users log on with the Citrix Gateway plug-in.	Citrix Gateway	Intranet websites
80 or 8080; 443	XML and Secure Ticket Authority (STA) port used for enumeration, ticketing, and authentication. Citrix recommends using port 443.	StoreFront and Web Interface XML network traffic; Citrix Gateway STA	Virtual Apps or Desktops
123 (TCP and UDP)	Used for Network Time Protocol (NTP) services.	Citrix Gateway; XenMobile	NTP server
389	Used for insecure LDAP connections	Citrix Gateway; XenMobile	LDAP authentication server or Microsoft Active Directory

TCP port	Description	Source	Destination
443	Used for connections to StoreFront from Citrix Receiver or Receiver for Web to Virtual Apps and Desktops.	Internet	Citrix Gateway
443	Used for connections to XenMobile for web, mobile, and SaaS app delivery.	Internet	Citrix Gateway
443	Used for general device communication to XenMobile Server.	XenMobile	XenMobile
443	Used for connections from mobile devices to XenMobile for enrollment.	Internet	XenMobile
443	Used for connections from XenMobile to Citrix Gateway connector for Exchange ActiveSync.	XenMobile	Citrix Gateway connector for Exchange ActiveSync
443	Used for connections from Citrix Gateway connector for Exchange ActiveSync to XenMobile.	Citrix Gateway connector for Exchange ActiveSync	XenMobile
443	Used for Callback URL in deployments without certificate authentication.	XenMobile	Citrix Gateway
514	Used for connections between XenMobile and a syslog server.	XenMobile	Syslog server

TCP port	Description	Source	Destination
636	Used for secure LDAP connections.	Citrix Gateway; XenMobile	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	Virtual Apps or Desktops
1812	Used for RADIUS connections.	Citrix Gateway	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	Virtual Apps or Desktops
3268	Used for Microsoft Global Catalog insecure LDAP connections.	Citrix Gateway; XenMobile	LDAP authentication server or Active Directory
3269	Used for Microsoft Global Catalog secure LDAP connections.	Citrix Gateway; XenMobile	LDAP authentication server or Active Directory
9080	Used for HTTP traffic between Citrix ADC and the Citrix Gateway connector for Exchange ActiveSync.	Citrix ADC	Citrix Gateway connector for Exchange ActiveSync

TCP port	Description	Source	Destination
30001	Management API for initial staging of HTTPS service	Internal LAN	XenMobile Server
9443	Used for HTTPS traffic between the Citrix ADC and the Citrix Gateway connector for Exchange ActiveSync.	Citrix ADC	Citrix Gateway connector for Exchange ActiveSync
45000; 80	Used for communication between two XenMobile VMs when deployed in a cluster. Port 80 is for internode communication and for SSL offload.	XenMobile	XenMobile
8443	Used for enrollment, XenMobile Store, and mobile app management (MAM).	XenMobile; Citrix Gateway; Devices; Internet	XenMobile
4443	Used for accessing the XenMobile console by an administrator through the browser. Also used for downloading logs and support bundles for all XenMobile cluster nodes from one node.	Access point (browser); XenMobile	XenMobile
27000	Default port used for accessing the external Citrix License Server.	XenMobile	Citrix License Server

TCP port	Description	Source	Destination
7279	Default port used for checking Citrix licenses in and out.	XenMobile	Citrix Vendor Daemon
161	Used for SNMP traffic using UDP protocol.	SNMP Manager	XenMobile
162	Used for sending SNMP trap alerts to the SNMP manager from XenMobile. The source is XenMobile and the destination is the SNMP Manager.	XenMobile	SNMP Manager

Open XenMobile ports to manage devices

Open the following ports to allow XenMobile to communicate in your network.

TCP port	Description	Source	Destination
25	Default SMTP port for the XenMobile notification service. If your SMTP server uses a different port, ensure that your firewall does not block that port.	XenMobile	SMTP server

TCP port	Description	Source	Destination
80 and 443	Enterprise App Store connection to Apple iTunes App Store, Google Play (must use 80), or Windows Phone Store. Used for Apple volume purchase. Used for publishing apps from the app stores from iOS, Secure Hub for Android, or Secure Hub for Windows Phone.	XenMobile	ax.apps.apple.com and *.mzstatic.com; vpp.itunes.apple.com; login.live.com; *.notify.windows.com; play.google.com, android.clients.google.com, android.l.google.com
80 or 443	Used for outbound connections between XenMobile and Nexmo SMS Notification Relay.	XenMobile	Nexmo SMS Relay Server
389	Used for insecure LDAP connections.	XenMobile	LDAP authentication server or Active Directory
443	Used for enrollment and agent setup for Android and Windows Mobile.	Internet	XenMobile
443	Used for enrollment and agent setup for Android and Windows devices and the MDM Remote Support Client.	Internet LAN and Wi-Fi	XenMobile
1433	Used by default for connections to a remote database server (optional).	XenMobile	SQL Server

TCP port	Description	Source	Destination
443 or 2197	Used to send APNs notifications to `*.push.apple.com`	XenMobile	Internet (APNs hosts using the public IP address 17.0.0.0/8
5223	Used for APNs outbound connections from iOS devices to `*.push.apple.com`.	iOS devices	Internet (APNs hosts using the public IP address 17.0.0.0/8)
8081	Used for app tunnels from the optional MDM Remote Support Client. Defaults to 8081.	Remote Support Client	XenMobile
8443	Used for enrollment of iOS and Windows Phone devices.	Internet; LAN and Wi-Fi	XenMobile

Port requirement for AutoDiscovery service connectivity

This port configuration ensures that Android devices connecting from Secure Hub for Android can access the Citrix AutoDiscovery Service (ADS) from within the internal network. You need access to ADS to download 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, do the following prerequisites:

- **Collect XenMobile Server and Citrix ADC 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 up ADS access within the internal network is critical to enabling devices to enroll.

To allow access to the ADS for Secure Hub for Android, open port 443 for the following FQDN and IP addresses:

FQDN	IP address	Port	IP and port usage
ads.xm.cloud.com	34.194.83.188	443	Secure Hub - ADS Communication
ads.xm.cloud.com	34.193.202.23	443	Secure Hub - ADS Communication

> **Note:**
>
> For Secure Hub versions before 10.6.15, the FQDN is discovery.mdm.zenprise.com. Open port 443 for IP addresses 52.5.138.94 and 52.1.30.122.

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.

Port requirements for XenMobile

The following destination hosts must be reachable from the network to create a Managed Google Play Enterprise and to access the Managed Google Play iFrame. Google made the Managed Play iFrame available to EMM developers to simplify search and approval of apps. In order to use the Managed Play iFrame, the browser from which you access the XenMobile console must have access to Google Play.

Destination host	Port	Description
play.google.com	TCP/443	Used for Google Play store, Play Enterprise sign-up
*.googleapis.com	TCP/443	Used for Google Mobile Management, Google APIs, Google Play store APIs
accounts.youtube.com, accounts.google.com	TCP/443	Used for the account authentication
apis.google.com	TCP/443	Used for GCM and other Google web services
ogs.google.com	TCP/443	Used for iFrame UI elements

Destination host	Port	Description
notifications.google.com	TCP/443	Used for desktop and mobile notifications
fonts.googleapis.com, *.gstatic.com, *.googleusercontent.com	TCP/443	Used for Google Fonts user generated content. For example, the app icons in the store
cri.pki.goog, ocsp.pki.goog	TCP/443	Used for the certificate validation

Scalability and performance

February 12, 2020

Understanding the scale of your XenMobile infrastructure plays a significant role in how you decide to deploy and configure XenMobile. This article contains data from scalability tests and guidance on determining infrastructure requirements for performance and scalability for small- to large-scale, on-premises XenMobile enterprise deployments.

Scalability is defined here in terms of the ability of devices already enrolled in the deployment to reconnect to the deployment at the same time.

- *Scalability* is defined as the maximum number of devices enrolled in the deployment.
- *Login Rate* is defined maximum rate at which existing devices can reconnect to the deployment.

The data in this article are derived from testing on deployments ranging in size from 10,000 to 75,000 devices. The tests comprised mobile device using known workloads.

All testing was done on XenMobile Enterprise edition.

Testing was done using the Citrix Gateway 8200. Citrix ADC appliance with similar or greater capacity can be expected to produce similar or greater scalability and performance.

A summary of scalability test results follows.

Summary of Scalability test results for deployments of up to 75,000 devices

Login rate (reconnection rate of existing users) — Up to 9,375 devices per hour

Configuration used:

- Citrix Gateway

- MPX 8200
- XenMobile Enterprise Edition
- XenMobile Server 7-node cluster
- Database: Microsoft SQL Server external database

Test results by device population and hardware configuration

Number of devices	12,500	30,000	60,000	75,000
Reconnection rate of existing devices per hour	1,250	3,750	7,500	9,375
XenMobile Server – mode	Standalone	Cluster	Cluster	Cluster
XenMobile Server – cluster	N/A	3	5	7
XenMobile Server – virtual appliance	Memory = 8 GB RAM; vCPUs = 4	Memory = 16 GB RAM; vCPUs = 6	Memory = 24 GB RAM; vCPUs = 8	Memory = 24 GB RAM; vCPUs = 8
Active Directory	Memory = 4 GB RAM; vCPUs = 2	Memory = 8 GB RAM; vCPUs = 4	Memory = 16 GB RAM; vCPUs = 4	Memory = 16 GB RAM; vCPUs = 4
Microsoft SQL Server external database	Memory = 8 GB RAM; vCPUs = 4	Memory = 16 GB RAM; vCPUs = 8	Memory = 24 GB RAM; vCPUs = 16	Memory = 24 GB RAM; vCPUs = 16

Scalability profile

Active Directory Configuration	Profile used
Users	100,000
Groups	200,000
Levels of nesting	5

XenMobile Server Configuration	Total	Per user
Policies	20	20
Apps	270	50
Public app	200	0
MDX	50	30
Web and SaaS	20	20
Actions	50	
Delivery groups	20	
Active Directory groups per delivery group	10	
SQL		
Number of databases	1	

Device connections and app activities

These scalability tests collected data on the ability of devices enrolled in a deployment to reconnect over an 8-hour period.

The tests simulated a reconnect interval during which reconnecting devices obtain all entitled security policies, subjecting XenMobile Server nodes to higher than normal load conditions. During subsequent reconnections, only changed or new policies are pushed to iOS devices, lessening the load on the XenMobile Server nodes.

These tests used a mix of 50 percent iOS devices and 50 percent Android devices.

These tests assume that the reconnecting Android devices have received prior GCM notifications.

During the 8-hour test interval, the following app-related activities occurred:

- Secure Hub was opened once to enumerate entitled apps
- 2 SAML web apps were opened
- 4 MAM apps were downloaded
- 1 STA was generated for use by Secure Mail
- 240 STA ticket validations, one for each Secure Mail reconnect event over a micro VPN, were performed.

Reference architecture

For the reference architecture for deployments used in these scalability tests, see “Core MAM+MDM Reference Architecture” in Reference Architecture for On-Premises Deployments.

Caveats and limitations

Note the following when considering the scalability test results in this article:

- Windows platform was not tested.
- Policy push was tested for iOS and Android devices.
- Each XenMobile Server node supports a maximum of 12,000 devices simultaneously.

Licensing

November 9, 2020

> **Important:**
>
> The process for returning and modifying Citrix licenses changed as of November 4, 2020. For information about the changes to the “Manage Licenses” portal on Citrix.com and “My Licensing Tools” on Partner Central, see the Citrix support article, https://support.citrix.com/article/CTX285157.

XenMobile uses Citrix Licensing to manage licenses. XenMobile Server and Citrix Gateway require licenses.

For more information about Citrix Gateway licensing, see the Citrix Gateway documentation. For more information about Citrix Licensing, see The Citrix Licensing System.

When you purchase XenMobile Server, you receive an order confirmation email message containing instructions for activating your licenses. New customers must register for a license program before placing an order. For more information about XenMobile licensing models and programs, see XenMobile licensing.

Requirements

- Update your Citrix License Server to 11.16.x or later before updating to the latest version of XenMobile Server. Older license server versions do not support the latest version of XenMobile.
- You must install Citrix Licensing before downloading your XenMobile licenses. The name of the server on which you installed Citrix Licensing is required to generate the license file. When you install XenMobile, Citrix Licensing is installed on the server by default. Alternatively, you can

use an existing Citrix Licensing deployment to manage your XenMobile licenses. For more information about installing, deploying, and managing Citrix Licensing, see Licensing Your Product.

- If you intend to cluster nodes, or instances, of XenMobile, you must use Citrix Licensing on a remote server.
- Citrix recommends that you retain local copies of all license files you receive. When you save a backup copy of the configuration file, all license files are included in the backup. If, however, you reinstall XenMobile without first backing up the configuration file, you need the original license files.

XenMobile licensing considerations

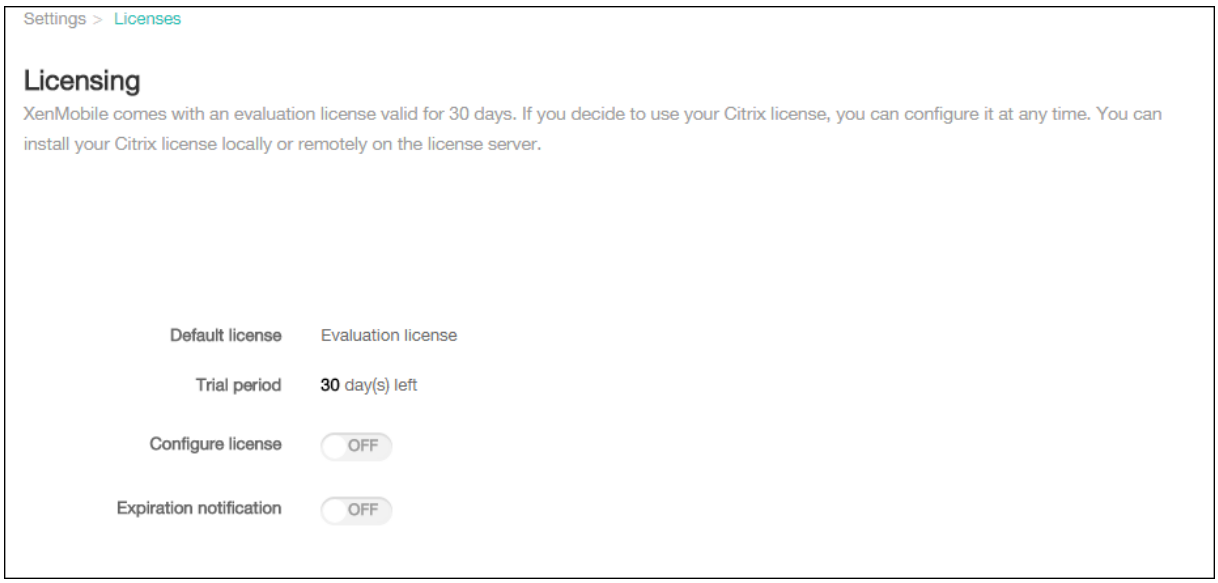
In the absence of a license, XenMobile operates fully featured in trial mode for a grace period of 30 days. This trial mode can be used only one time, with the 30-day period beginning when you install XenMobile. Access to the XenMobile web console is never blocked, whether or not a valid XenMobile license is available. In the XenMobile console, you can see how many days are left in your trial period.

Although XenMobile allows you to upload multiple licenses, only one license can be activated at a time.

When a XenMobile license expires, you can no longer perform any device management functions. For example, new users or devices cannot be enrolled, and apps and configurations deployed to enrolled devices cannot be updated. For more information about XenMobile licensing models and programs, see XenMobile licensing.

To find the Licensing page on the XenMobile console

When the **Licensing** page first appears after you install XenMobile, the license is set for the default 30-day trial mode and is not yet configured. You can add and configure licenses on this page.



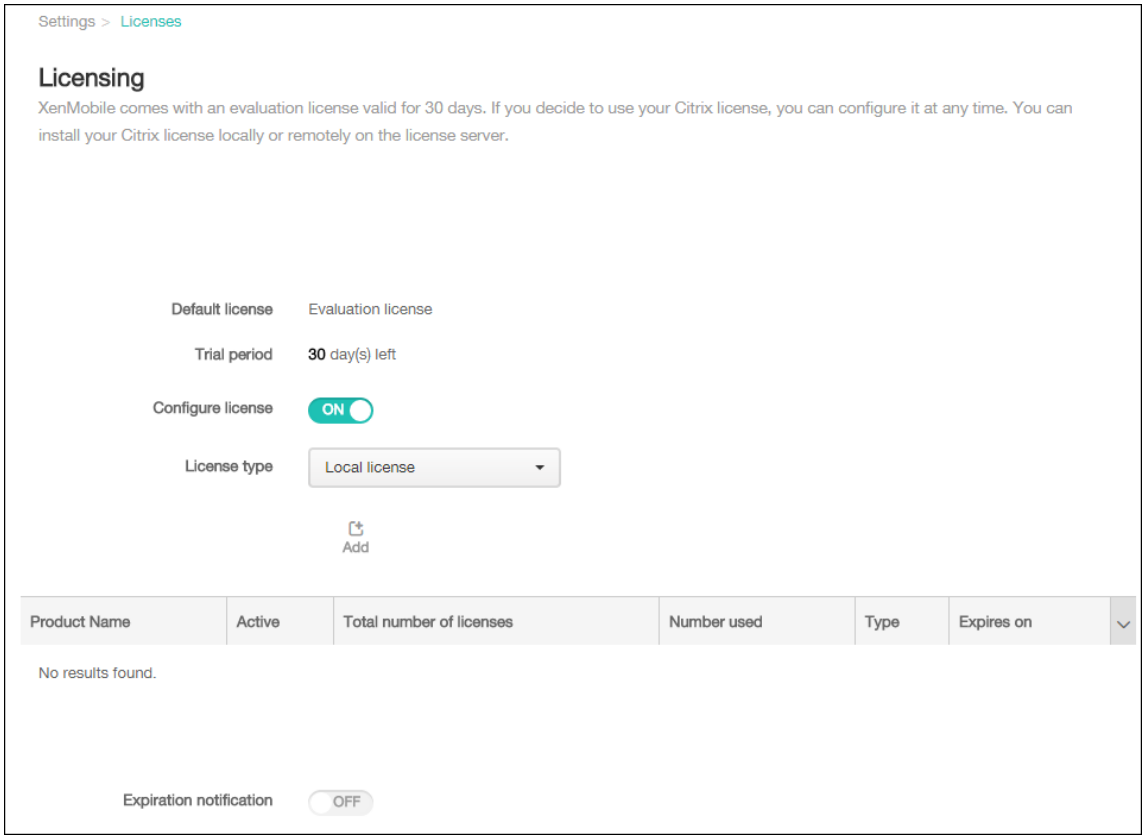
1. On the XenMobile console, click the gear icon in the upper right-hand corner. The **Settings** page appears.
2. Click **Licensing**. The **Licensing** page appears.

To add a local license

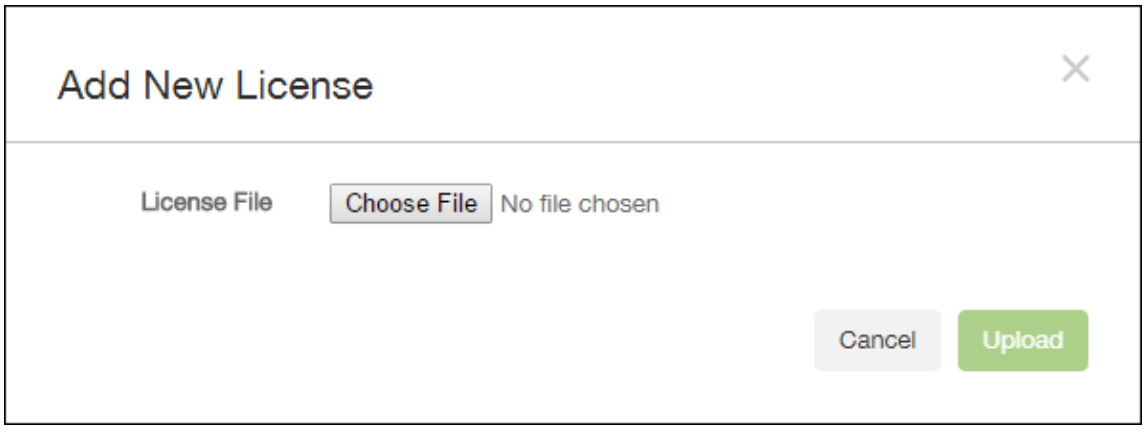
When adding new licenses, they appear in the table. The first license added is automatically activated. If you add multiple licenses of the same category, such as Enterprise and type, these licenses appear in a single row of the table. In these cases, the **Total number of licenses** and **Number used** reflect the combined amount for the common licenses. The **Expires on** date shows the latest expiration date among the common licenses.

You manage all local licenses through the XenMobile console.

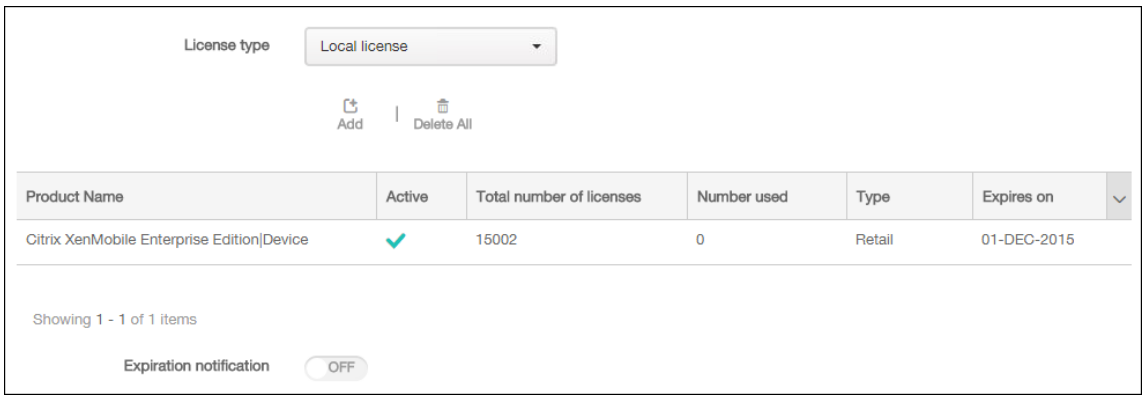
1. Get a license file from the Simple License Service, through the License Administration Console, or directly from your account on Citrix.com. For details, see the Citrix Licensing documentation.
2. On the XenMobile console, click the gear icon in the upper right corner. The **Settings** page appears.
3. Click **Licensing**. The **Licensing** page appears.
4. Set **Configure license** to **On**. The **License type** list, the **Add** button, and the **Licensing** table appear. The **Licensing** table contains licenses you have used with XenMobile. If you have not added a Citrix license yet, the table is empty.



5. Ensure that **License type** is set to **Local license** and then click **Add**. The **Add New License** dialog box appears.



6. In the **Add New License** dialog box, click **Choose File** and then browse to your license file location.
7. Click **Upload**. The license is uploaded locally and appears in the table.



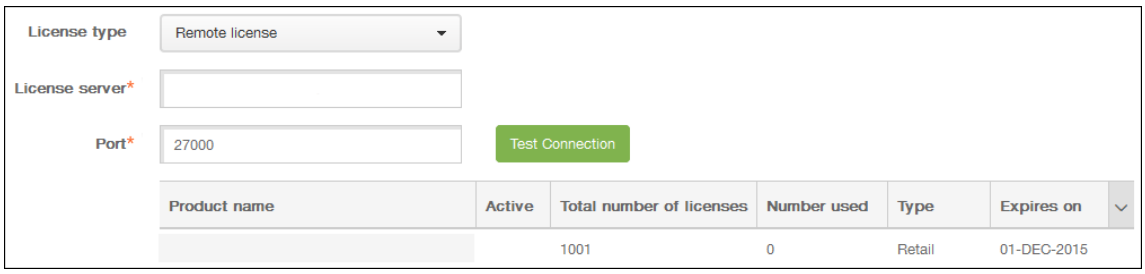
8. When the license appears in the table on the **Licensing** page, activate it. If the license is first in the table, the license is activated automatically.

To add a remote license

If you are using the remote Citrix Licensing server, you use the Citrix Licensing server to manage *all* licensing activity. For details, see Licensing Your Product.

1. Import the License server certificate into XenMobile Server (**Settings > Certificates**).
2. By default, host name verification is enabled on outgoing connections except for the Microsoft PKI server. If host name verification breaks your deployment, change the server property **disable.hostname.verification** to **true**. The default value of this property is **false**.

   When host name 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"
3. On the **Licensing** page, set **Configure license** to **On**. The **License type** list, the **Add** button, and the **Licensing** table appear. The **Licensing** table contains licenses you have used with XenMobile. If you have not added a Citrix license yet, the table is empty.
4. Set **License type** to **Remote license**. The **License server** and **Port** fields and the **Test Connection** button replace the **Add** button.



5. Configure these settings:

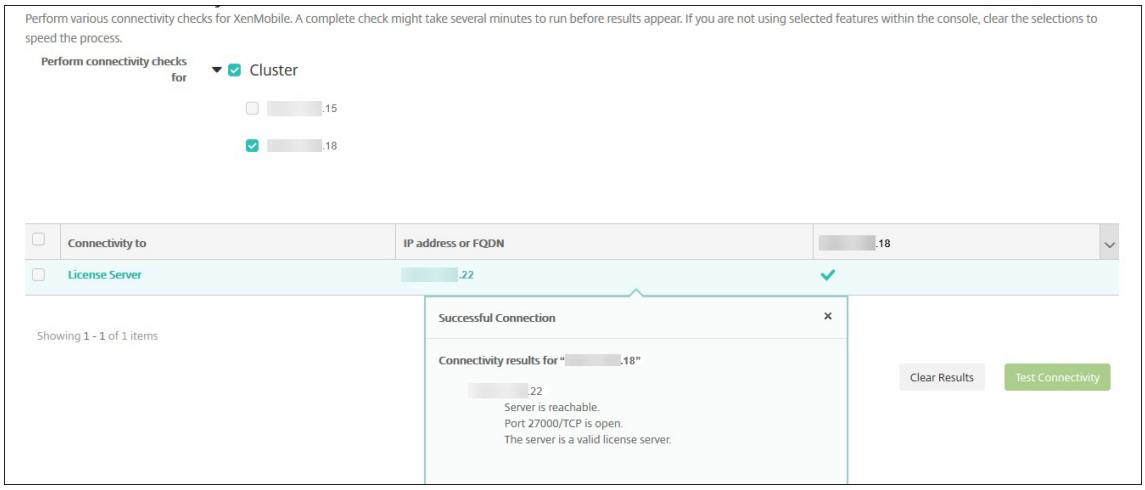
- **License server:** Type the IP address or fully qualified domain name (FQDN) of your remote licensing server.
- **Port:** Accept the default port or type the port number used to communicate with the licensing server.

6. Click **Test Connection**. If the connection is successful, XenMobile connects with the Licensing server and the Licensing table is filled with available licenses. If there is only one license, it is activated automatically.

   When you click **Test Connection**, XenMobile confirms the following:

   - XenMobile can communicate with the license server.
   - Licenses on the license server are valid.
   - The license server is compatible with XenMobile.

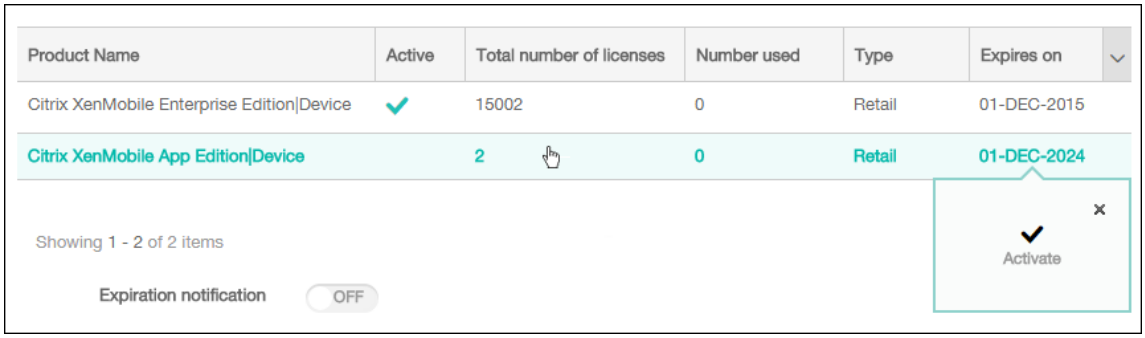
   If the connection is unsuccessful, review the displayed error message, make the necessary corrections, and then click **Test Connection**.



To activate a different license

If you have multiple licenses, you can choose the license you want to activate. You can have only one license active at a time, however.

1. On the **Licensing** page, in the **Licensing table**, click the row of the license you want to activate. An **Activate** confirmation dialog appears next to the row.



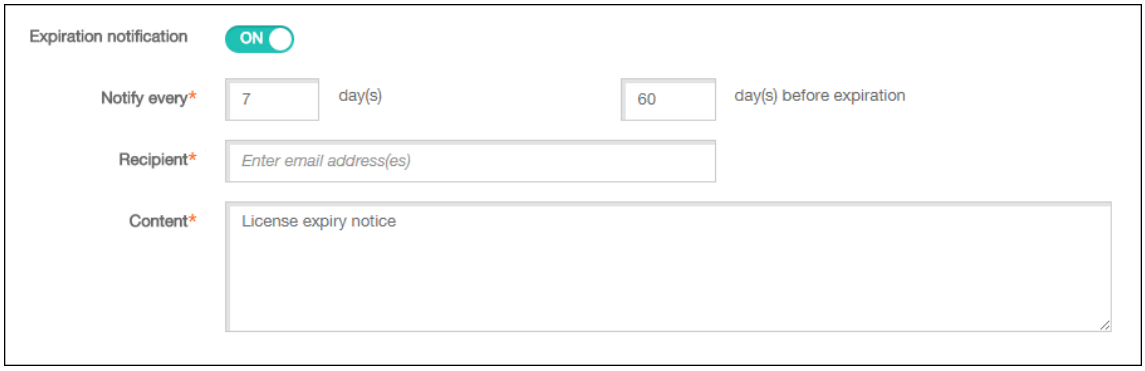
2. Click **Activate**. The **Activate** dialog box appears.
3. Click **Activate**. The selected license is activated.

> **Important:**
>
> If you activate the selected license, the currently active license is deactivated.

To automate an expiration notification

After you have activated remote or local licenses, you can configure XenMobile to notify you or a designate when the license expiration date approaches.

1. On the **Licensing** page, set **Expiration notification** to **On**. New notification-related fields appear.



2. Configure these settings:
   - **Notify every:** Type:
   - The frequency with which the notifications are sent, such as every **7** days.
   - When to begin sending the notification, such as 60 days before the license expires.
   - **Recipient:** Type your email address or the email address of the person responsible for the license.
   - **Content:** Type an expiration notification message that the recipient sees in the notification.

3. Click **Save**. Based on your settings, XenMobile begins sending email messages containing the text you typed in **Content** to the recipient you typed in **Recipient**. The notifications are sent with the frequency you set.

FIPS 140-2 compliance

August 18, 2020

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.

> **Important:**
>
> - You can enable XenMobile FIPS mode only during initial installation.
> - XenMobile mobile device management-only, XenMobile mobile app management-only, and XenMobile MDM+MAM are all FIPS compliant provided that no HDX apps are used.

All data-at-rest and data-in-transit cryptographic operations on iOS use FIPS-validated cryptographic modules provided by Citrix and Apple. 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 provided by Microsoft.

All data-at-rest and data-in-transit cryptographic operations for XenMobile MDM use FIPS-validated cryptographic modules provided by Citrix. 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 provided by Citrix.

Language support

October 6, 2020

Mobile productivity apps and the XenMobile 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 XenMobile.

XenMobile console and the Self Help Portal

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

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	QuickEdit
Japanese	X	X	X	X
Simplified Chinese	X	X	X	X
Traditional Chinese	X	X	X	X
French	X	X	X	X
German	X	X	X	X
Spanish	X	X	X	X
Korean	X	X	X	X
Portuguese	X	X	X	X
Dutch	X	X	X	X
Italian	X	X	X	X
Danish	X	X	X	X

Language	Secure Hub	Secure Mail	Secure Web	QuickEdit
Swedish	X	X	X	X
Hebrew	X	X	X	iOS only
Arabic	X	X	X	X
Russian	X	X	X	X
Turkish	X	X	Android only	-
Polish	X	X	X	-

Windows

Language	Secure Hub	Secure Mail	Secure Web
French	X	X	X
German	X	X	X
Spanish	X	X	X
Italian	X	X	X
Danish	X	X	X
Swedish	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

Install and configure

November 9, 2020

Before you start

You can use the following preinstallation checklist to note the prerequisites and settings for installing XenMobile on-premises. Each task or note includes a column indicating the component or function for which the requirement applies.

Planning a XenMobile deployment involves many considerations. For recommendations, common questions, and use cases for your complete XenMobile environment, see the XenMobile Deployment Handbook.

For installation steps, see the Install XenMobile section later in this article.

Preinstallation checklist

Basic Network Connectivity

The following are the network settings you need for the XenMobile solution.

Prerequisite or setting	Component or function	Note the setting
Note the fully qualified domain name (FQDN) to which remote users connect.	XenMobile and Citrix Gateway	
Note the public and local IP address.		
You need these IP addresses to configure the firewall to set up network address translation (NAT).	XenMobile and Citrix Gateway	

Prerequisite or setting	Component or function	Note the setting	
Note the subnet mask.	XenMobile and Citrix Gateway		
Note the DNS IP addresses.	XenMobile and Citrix Gateway		
Write down the WINS server IP addresses (if applicable).	Citrix Gateway		
Identify and write down the Citrix Gateway host name.	Citrix Gateway	This item is not the FQDN. The FQDN is contained in the signed server certificate that is bound to the virtual server and to which users connect. You can configure the host name by using the Setup Wizard in Citrix Gateway.	Citrix Gateway
Note the IP address of XenMobile. Reserve one IP address if you install one instance of XenMobile. If you configure a cluster, note all IP addresses that you need.	XenMobile		

Prerequisite or setting	Component or function	Note the setting	
One public IP address configured on Citrix Gateway	Citrix Gateway		
One external DNS entry for Citrix Gateway	Citrix Gateway		
Note the web proxy server IP address, port, proxy host list, and the administrator user name and password. These settings are optional if you deploy a proxy server in your network (if applicable).	Citrix Gateway	You can use either the sAMAccountName or the User Principal Name (UPN) when configuring the user name for the web proxy.	XenMobile and Citrix Gateway
Note the default gateway IP address.	XenMobile and Citrix Gateway		
Note the system IP (NSIP) address and subnet mask.	Citrix Gateway		
Note the subnet IP (SNIP) address and subnet mask.	Citrix Gateway		

Prerequisite or setting	Component or function	Note the setting
Note the Citrix Gateway virtual server IP address and FQDN from the certificate. To configure multiple virtual servers, note all virtual IP addresses and FQDNs from the certificates.	Citrix Gateway	
Note the internal networks that users can access through Citrix Gateway. Example: 10.10.0.0/24. Enter all internal networks and network segments that users need access to in these cases: When users connect with Secure Hub or the Citrix Gateway Plug-in when split tunneling is set to On.	Citrix Gateway	

Prerequisite or setting	Component or function	Note the setting
Ensure that the network connectivity between the XenMobile Server, Citrix Gateway, the external Microsoft SQL Server, and the DNS server are reachable.	XenMobile and Citrix Gateway	

Licensing

XenMobile requires you to purchase licensing options for Citrix Gateway and XenMobile. For more information about Citrix Licensing, see The Citrix Licensing System.

Prerequisite	Component	Note the location
Obtain Universal licenses from the Citrix website. For details, see Licensing in the Citrix Gateway documentation.	Citrix Gateway, XenMobile, and Citrix License Server	

Certificates

XenMobile and Citrix Gateway require certificates to enable connections with other Citrix products and app and from user devices. For details, see the Certificates and Authentication section in the XenMobile documentation.

Prerequisite	Component	Notes
Obtain and install required certificates.	XenMobile and Citrix Gateway	

Ports

Open ports to allow communication with the XenMobile components.

Prerequisite	Component	Notes
Open ports for XenMobile	XenMobile and Citrix Gateway	

Database

XenMobile requires database connection configuration. The XenMobile repository requires a Microsoft SQL Server database running on one of the supported versions noted in System requirements and compatibility. Citrix recommends using Microsoft SQL remotely. PostgreSQL is included with XenMobile. Use PostgreSQL locally or remotely *only* in test environments.

By default, XenMobile uses the jTDS database driver. To use the Microsoft JDBC driver for on-premises installations of XenMobile Server, see SQL Server drivers.

Prerequisite	Component	Notes
Microsoft SQL Server IP address and port. Ensure that the service account of the SQL Server to be used on XenMobile has the DBcreator role permission.	XenMobile	

Active Directory Settings

Prerequisite	Component	Notes
Note the Active Directory IP address and port for the primary and secondary servers. If you use port 636, install a root certificate from a CA on XenMobile, and change the Use secure connections option to Yes.	XenMobile and Citrix Gateway	

Prerequisite	Component	Notes
Note the Active Directory domain name.	XenMobile and Citrix Gateway	
Note the Active Directory service account, which requires a user ID, password, and domain alias.		
The Active Directory service account is the account that XenMobile uses to query Active Directory.	XenMobile and Citrix Gateway	
Note the User Base DN, which is the directory level under which users are located. For example: `cn=users,dc=ace,dc=com`. Citrix Gateway and XenMobile use the User Base DN to query Active Directory.	XenMobile and Citrix Gateway	
Note the Group Base DN, which is the directory level under which groups are located. Citrix Gateway and XenMobile use this DN to query Active Directory.	XenMobile and Citrix Gateway	

Connections between XenMobile and Citrix Gateway

Prerequisite	Component	Note the setting
Note the XenMobile host name.	XenMobile	
Note the FQDN or IP address of XenMobile.	XenMobile	
Identify the apps users can access.	Citrix Gateway	

Prerequisite	Component	Note the setting
Note the Callback URL.	XenMobile	

User Connections: Access to Citrix Virtual Apps and Desktops and Citrix Secure Hub

Citrix recommends that you use the Quick Configuration wizard in Citrix ADC to configure connection settings between XenMobile and Citrix Gateway and between XenMobile and Secure Hub. You create a second virtual server to enable user connections from Citrix Receiver and web browsers. Those connections are to Windows-based applications and virtual desktops in Virtual Apps and Desktops. Citrix recommends that you also use the Quick Configuration wizard in Citrix ADC to configure these settings.

Prerequisite	Component	Note the setting
Note the Citrix Gateway host name and external URL. The external URL is the web address with which users connect.	XenMobile	
Note the Citrix Gateway callback URL.	XenMobile	
Note the IP addresses and subnets masks for the virtual server.	Citrix Gateway	
Note the path for Program Neighborhood Agent or a Virtual Apps and Desktops Site.	Citrix Gateway and XenMobile	
Note the FQDN or IP address of the Citrix Virtual Apps and Desktops server running the Secure Ticket Authority (STA) (for ICA connections only).	Citrix Gateway	
Note the public FQDN for XenMobile.	Citrix Gateway	
Note the public FQDN for Secure Hub.	Citrix Gateway	

Flowchart for XenMobile deployment

You can use this flowchart to guide you through the main steps for deploying XenMobile. Links to topics on each step follow the figure.

1: System requirements and compatibility

2: Install and configure

3 and 4: Preinstallation checklist (this article)

5: Configure XenMobile in the Command Prompt Window (this article)

6: Configure XenMobile in a web browser (this article)

7: Configuring Settings for Your XenMobile Environment

8: Port requirements

Install XenMobile

The XenMobile virtual machine (VM) runs on Citrix XenServer, VMware ESXi, or Microsoft Hyper-V. You can use XenCenter or vSphere management consoles to install XenMobile.

> **Note:**
>
> Ensure that the hypervisor is configured with the correct time – either using an NTP server or a manual configuration - because XenMobile uses that time. If you have time zone issues when syncing XenMobile time with a hypervisor, you can avoid the issues by pointing XenMobile to an NTP server. To do that, use the XenMobile CLI, as described in Command-line interface options.

XenServer or VMware ESXi prerequisites. Before installing XenMobile on XenServer or VMware ESXi, you must do the following. For details, see your XenServer or VMware documentation.

- Install XenServer or VMware ESXi on a computer with adequate hardware resources.
- Install XenCenter or vSphere on a separate computer. The computer that hosts XenCenter or vSphere connects to the XenServer or VMware ESXi host through the network.

Hyper-V prerequisites. Before installing XenMobile on Hyper-V, you must do the following. For details, see your Hyper-V documentation.

- Install Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 with Hyper-V enabled, role enabled, on a computer with adequate system resources. While installing the Hyper-V role, be sure to specify the NICs on the server that Hyper-V uses to create the virtual networks. You can reserve some NICs for the host.
- Delete the file Virtual Machines/<*build-specific UUID*>.xml
- Move the file Legacy/<*build-specific UUID*>.exp into Virtual Machines

If you install Windows Server 2008 R2 or Windows Server 2012, do the following:

These steps are necessary because there are two different versions of the Hyper-V manifest file representing the VM configuration (.exp and .xml). The Windows Server 2008 R2 and Windows Server 2012 releases support only .exp. For these releases, you must have only the .exp manifest file in place before installation.

Windows Server 2012 R2 does not require these extra steps.

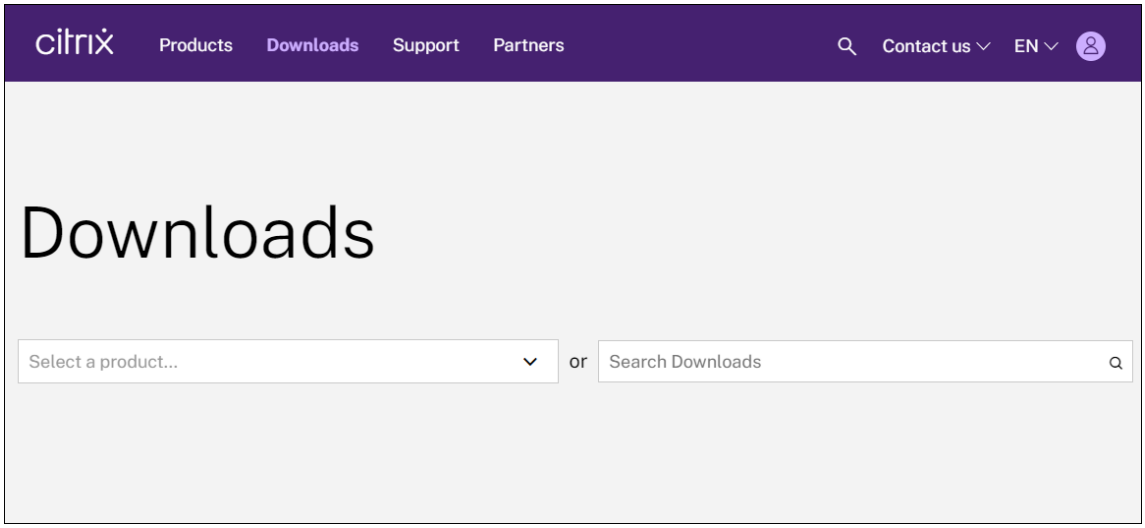
FIPS 140-2 mode. To install XenMobile Server in FIPS mode, complete a prerequisite group, as discussed in Configure FIPS with XenMobile.

Download XenMobile product software

You can download product software from the Citrix website. Log on to the site and then use the Downloads link to navigate to the page containing the software you want to download.

To download the software for XenMobile

1. Go to the Citrix website.
2. Next to the Search box, click **Log On** and log on to your account.
3. Click the **Downloads** tab.
4. On the Downloads page, from the **select a product** list, click **Citrix Endpoint Management (and Citrix XenMobile Server)**. The Citrix Endpoint Management (and Citrix XenMobile Server) page automatically appears.



5. Expand **XenMobile Server (on-premises)**.
6. Expand **Product Software**.

7. Click **XenMobile Server 10**.
8. Click the **Jump to Download** menu and choose the appropriate virtual image to use to install XenMobile. Alternatively, scroll down the page to locate the **Download File** button for the image you want to install.
9. Follow the instructions on your screen to download the software.

To download the software for Citrix Gateway

You can use this procedure to download the Citrix Gateway virtual appliance or software upgrades to your existing Citrix Gateway appliance.

1. Go to the Citrix website.
2. If you are not already logged on to the Citrix website, next to the Search box, click **Log On** and log on to your account.
3. Click the **Downloads** tab.
4. On the Downloads page, from the select product list, click **Citrix Gateway**.
5. Click **Go**. The Citrix Gateway page appears.
6. On the Citrix Gateway page, expand the version of Citrix Gateway you are running.
7. Under **Firmware**, click the appliance software version you want to download.

   > **Note:**
   >
   > You can also click **Virtual Appliances** to download Citrix ADC VPX. When you select this option, you receive a list of software for the virtual machine for each hypervisor.

8. Click the appliance software version you want to download.
9. On the appliance software page for the version you want to download, click **Download** for the appropriate virtual appliance.
10. Follow the instructions on your screen to download the software.

Configure XenMobile for First-Time Use

1. To configure the IP address and subnet mask, default gateway, DNS servers, and other settings for XenMobile: Use the XenCenter or vSphere command-line console.

   > **Note:**
   >
   > When you use a vSphere web client: We recommend that you don't configure networking properties during the time you deploy the OVF template on the **Customize template** page. By doing so in a high availability configuration: You avoid an issue with the IP address that

> occurs when you clone and then restart the second XenMobile virtual machine.

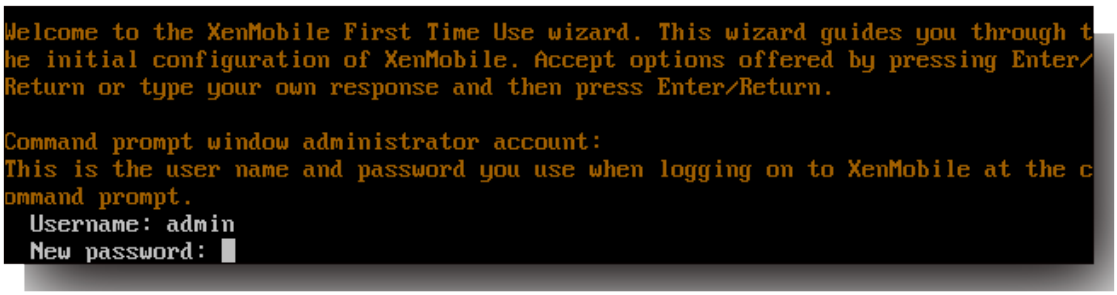
2. Access the XenMobile management console only through the XenMobile Server fully qualified domain name or the IP addresses of the node.
3. Log on and then follow the steps in the initial logon screens.

Configure XenMobile in the Command Prompt Window

1. Import the XenMobile virtual machine into Citrix XenServer, Microsoft Hyper-V, or VMware ESXi. For details, see XenServer, Hyper-V, or VMware documentation.
2. In your hypervisor, select the imported XenMobile virtual machine and start the command prompt view. For details, see the documentation for your hypervisor.
3. From the hypervisor console page, create an administrator account for XenMobile in the command prompt window by typing the administrator user name and password.

   When you create or change passwords for the command prompt administrator account, Public Key Infrastructure (PKI) server certificates, and FIPS: XenMobile enforces the following rules for all users except Active Directory users whose passwords are managed outside of XenMobile.

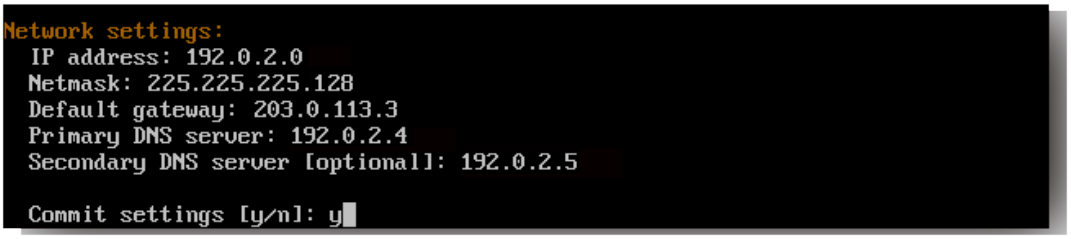
   - The password must be at least eight characters long.
   - The password must meet at least three of the following complexity criteria:
     - Uppercase letters (A through Z)
     - Lowercase letters (a through z)
     - Numerals (0 through 9)
     - Special characters (such as ! ## $ %)



   No characters, such as asterisks, appear when you type the new password.

4. Provide the following network information and then, type **y** to commit the settings:
   a) IP address of the XenMobile Server
   b) Netmask
   c) Default gateway, which is the IP address of the default gateway in the DMZ
   d) Primary DNS server, which is the IP address of the DNS server

e) Secondary DNS server (optional)



> **Note:**
>
> The addresses shown in this and following images are non-working and are provided as examples only.

5. Type **y** to increase security by generating a random encryption passphrase or **n** to provide your own passphrase. Citrix recommends typing **y** to generate a random passphrase.

   The passphrase is used as part of the protection of the encryption keys used to secure your sensitive data. A hash of the passphrase, stored in the server file system, is used to retrieve the keys during the encryption and decryption of data. The passphrase cannot be viewed.

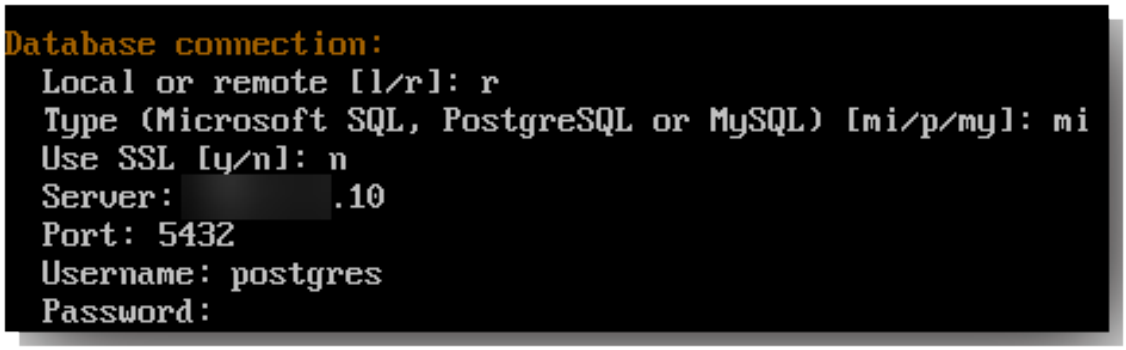
   > **Note:**
   >
   > If you intend to extend your environment and configure more servers, provide your own passphrase. If you select a random passphrase, you can't view it.

6. Optionally, enable Federal Information Processing Standard (FIPS). For details about FIPS, see FIPS. Also, be sure to complete a prerequisite group, as discussed in Configure FIPS with XenMobile.

7. Provide the following information to configure the database connection.

- Your database can be local or remote. Type **l** for local or **r** for remote.
- Select the database type. Type **mi** for Microsoft SQL or type **p** for PostgreSQL.

  > **Important:**
  >
  > – Citrix recommends using Microsoft SQL remotely. PostgreSQL is included with XenMobile. Use PostgreSQL locally or remotely *only* in test environments.
  > – Database migration is not supported. Databases created in a test environment cannot be moved to a production environment.

- Optionally, type **y** to use SSL authentication for your database.
- Provide the fully qualified domain name (FQDN) for the server hosting XenMobile. This one host server provides both device management and app management services.
- Type your database port number if it is different from the default port number. The default port for Microsoft SQL is 1433 and the default port for PostgreSQL is 5432.
- Type your database administrator user name.
- Type your database administrator password.
- Type the database name.
- Press **Enter** to commit the database settings.

8. Optionally, type **y** to enable clustering XenMobile nodes, or instances.

   > **Important:**
   >
   > If you enable a XenMobile cluster, after system configuration completes, open port 80 to enable real-time communication between cluster members. Complete that setup on all cluster nodes.

9. Type the XenMobile Server fully qualified domain name (FQDN).

10. Press **Enter** to commit the settings.
11. Identify the communication ports. For details on ports and their uses, see Port Requirements.

    > **Note:**
    >
    > Accept the default ports by pressing **Enter** (Return on a Mac).


```
HTTP [80]: 80
HTTPS with certificate authentication [443]: 443
HTTPS with no certificate authentication [8443]: 8443
HTTPS for management [4443]: 4443
```

12. Skip the next question about upgrading from a previous XenMobile release because you are installing XenMobile for the first time.
13. Type **y** if you want to use the same password for each Public Key Infrastructure (PKI) certificate. For details on the XenMobile PKI feature, see Uploading Certificates.

```
The wizard will now generate an internal Public Key Infrastructure (PKI):
- A root certificate
- An intermediate certificate to issue device certificates during enrollment
- An intermediate certificate to issue an SSL certificate
- An SSL certificate for your connectors
Do you want to use the same password for all the certificates of the PKI [y]:
New password:
Re-enter new password:
```

> **Important:**
>
> If you intend to cluster nodes, or instances, of XenMobile together, provide identical passwords for subsequent nodes.

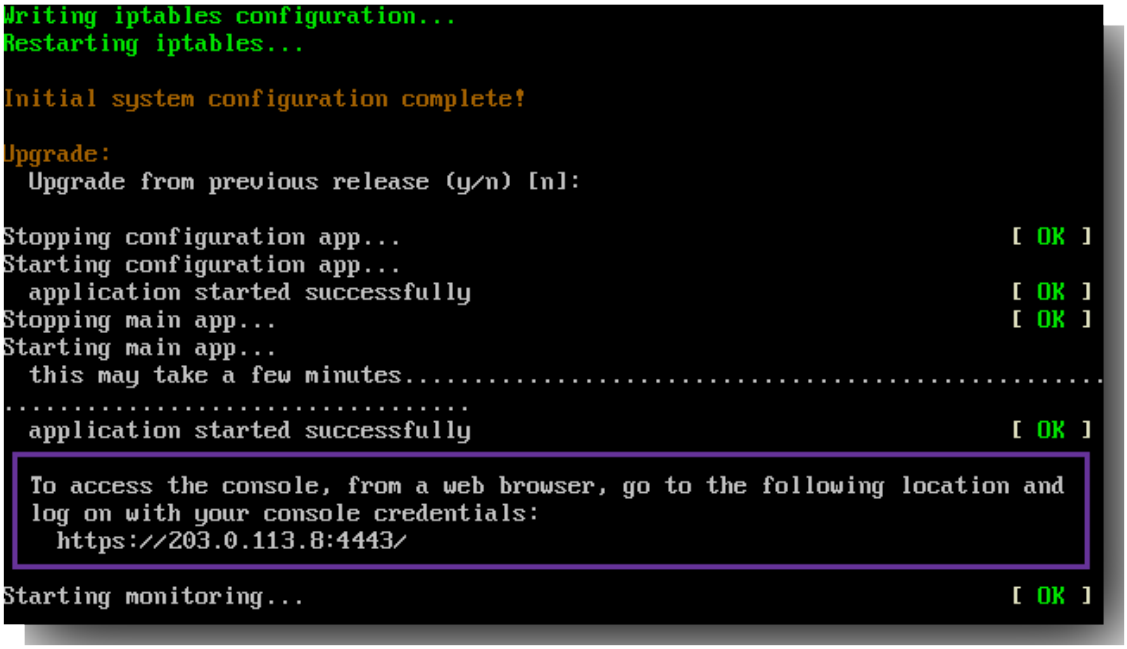
14. Type the new password and then, reenter the new password to confirm it.

    No characters, such as asterisks, appear when you type the new password.
15. Press **Enter** to commit the settings.
16. Create an administrator account for logging on to the XenMobile console with a web browser. Be sure to record these credentials for later use.

```
XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile cons
ole through a web browser.
  Username [administrator]: administrator
  Password:
  Re-enter new password:
```

> **Note:**
>
> No characters, such as asterisks, appear when you type the new password.

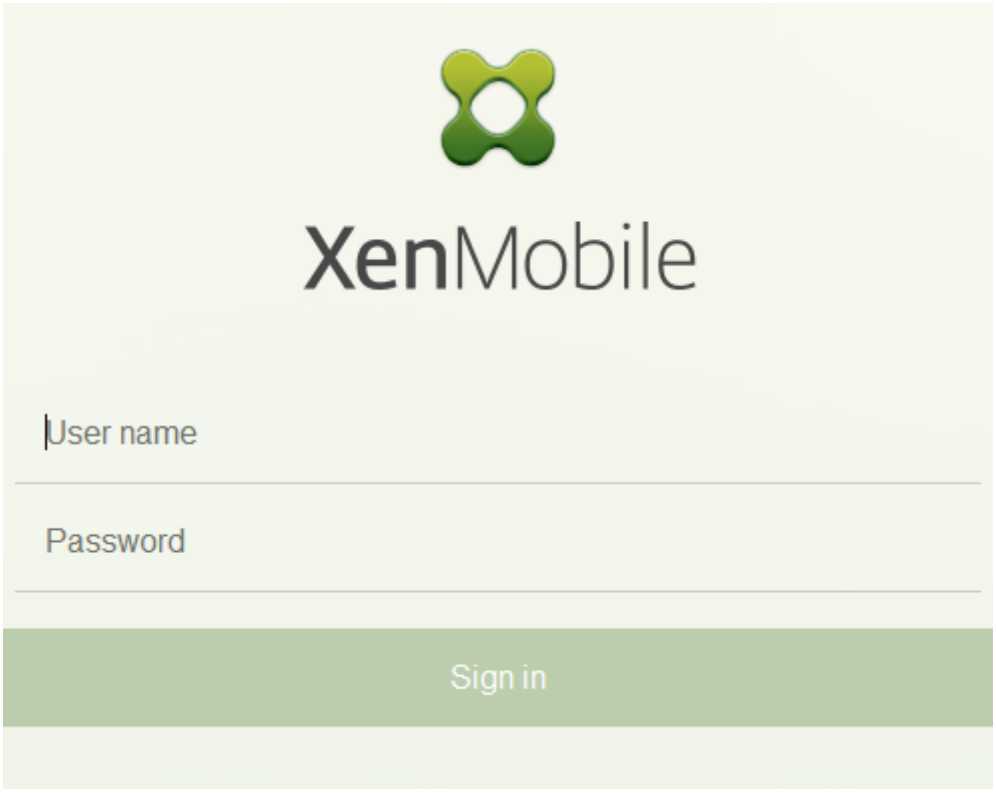
17. Press **Enter** to commit the settings. The initial system configuration is saved.
18. When asked if you're upgrading, type **n** because it is a new installation.
19. Copy the complete URL that appears on the screen and continue this initial XenMobile configuration in your web browser.



Configure XenMobile in a web browser

After completing the initial portion of the XenMobile configuration in your hypervisor command prompt window, complete the process in your web browser.

1. In your web browser, navigate to the location provided at the conclusion of the command prompt window configuration.
2. Type the XenMobile console administrator account user name and password you created in the command prompt window.



3. On the Get Started page, click **Start**. The **Licensing** page appears.
4. Configure the license. If you don't upload a license, you use an evaluation license valid for 30 days. For details on adding and configuring licenses and configuring expiration notifications, see Licensing.

   > **Important:**
   >
   > If you intend to use XenMobile clustering by adding cluster nodes, or instances, of XenMobile, you must use the Citrix Licensing on a remote server.

5. On the **Certificates** page, click **Import**. The Import dialog box appears.
6. Import your APNs and SSL Listener certificate. iOS device management requires an APNs certificate. For details on working with certificates, see Certificates.

   > **Note:**
   >
   > This step requires restarting the server.

7. If appropriate to the environment, configure Citrix Gateway. For details on configuring Citrix Gateway, see Citrix Gateway and XenMobile and Configuring Settings for Your XenMobile Environment.

> **Note:**
>
> - You can deploy Citrix Gateway at the perimeter of your internal network (or intranet). That deployment provides a secure single point of access to the servers, apps, and other network resources that reside in the internal network. In this deployment, all remote users must connect to Citrix Gateway before they can access any resources in the internal network.
> - Although Citrix Gateway is an optional setting: After you enter data on the page, you must clear or complete the required fields before you can leave the page.

8. Complete the LDAP configuration to access users and groups from Active Directory. For details on configuring the LDAP connection, see LDAP Configuration.
9. Configure the notification server to be able to send messages to users. For details on notification server configuration, see Notifications.

Post-requisite. Restart the XenMobile Server to activate your certificates.

Configure FIPS with XenMobile

January 28, 2021

Federal Information Processing Standards (FIPS) mode in XenMobile supports U.S. federal government customers by using only FIPS 140-2 certified libraries for all encryption operations. Installing your XenMobile Server with FIPS mode ensures that all data for the XenMobile client and server are fully compliant with FIPS 140-2. That compliance applies to data at rest and data in transit.

Before installing a XenMobile Server in FIPS mode, complete the following prerequisites.

- Use an external SQL Server 2014 for the XenMobile database. The SQL Server also must be configured for secure SSL communication. For instructions on configuring secure SSL communication to SQL Server, see Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager).
- Secure SSL communication requires that you install a trusted SSL certificate from a well-known certificate authority (CA) on your SQL Server. Be aware that SQL Server 2014 cannot accept a wildcard certificate. Citrix recommends, therefore, that you request an SSL certificate with the FQDN of the SQL Server.

Configuring FIPS mode

You can enable FIPS mode only during the initial setup of XenMobile Server. It is not possible to enable FIPS after installation is complete. Therefore, if you plan on using FIPS mode, you must install the

XenMobile Server with FIPS mode from the start. Also, for XenMobile clusters, all cluster nodes must have FIPS enabled. You cannot have a mix of FIPS and non-FIPS XenMobile Servers in the same cluster.

There is a **Toggle FIPS mode** option in the XenMobile command-line interface that is not for production use. This option is intended for non-production, diagnostic use and is not supported on a production XenMobile Server.

1. During initial setup, enable **FIPS mode**.
2. Upload the root CA certificate for your SQL Server.
3. Specify the server name and port of your SQL Server, the credentials for logging into SQL Server, and the database name to create for XenMobile.

   > **Note:**
   >
   > You can use either a SQL logon or an Active Directory account to access SQL Server, but the logon you use must have the DBcreator role.

4. To use an Active Directory account, enter the credentials in the format domain\username.
5. Once these steps are complete, proceed with the XenMobile initial setup.

To confirm that the configuration of FIPS mode is successful, log on to the XenMobile command-line interface. The phrase **In FIPS Compliant Mode** appears in the logon banner.

Importing Certificates

The following procedure describes how to configure FIPS on XenMobile by importing the certificate, which is required when you use a VMware hypervisor.

SQL Prerequisites

1. The connection to the SQL instance from XenMobile must be secure and must be SQL Server version 2012 or SQL Server 2014. To secure the connection, see How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console.
2. If the service does not restart properly, check the following: Open **Services.msc**.
   a) Copy the logon account information used for the SQL Server service.
   b) Open MMC.exe on the SQL Server.
   c) Go to **File > Add/Remove Snap-in** and then double-click the certificates item to add the certificates snap-in. Select the computer account and local computer in the two pages on the wizard.
   d) Click **OK**.

e) Expand **Certificates (Local Computer) > Personal > Certificates** and find the imported SSL certificate.

f) Right-click the imported certificate (selected in the SQL Server Configuration Manager) and then click **All Tasks > Manage Private Keys**.

g) Under **Group or User names**, click **Add**.

h) Enter the SQL service account name you copied in the earlier step.

i) Clear the **Allow Full Control** option. By default the service account will be given both Full control and Read permissions, but it only needs to be able to read the private key.

j) Close **MMC** and start the SQL service.

3. Ensure the SQL service is started correctly.

Internet Information Services (IIS) Prerequisites

1. Download the root certificate (base 64).
2. Copy the root certificate to the default site on the IIS server, C:\inetpub\wwwroot.
3. Check the **Authentication** check box for the default site.
4. Set **Anonymous** to **enabled**.
5. Select the **Failed Request Tracking** rules check box.
6. Ensure that .cer is not blocked.
7. Browse to the location of the .cer in a web browser from the local server, `https://localhost/certname.cer`. The root cert text appears in the browser.
8. If the root cert does not appear in your web browser, ensure that ASP is enabled on the IIS server as follows.

   a) Open Server Manager.

   b) Navigate to the wizard in **Manage > Add Roles and Features**.

   c) In the server roles, expand **Web Server (IIS)**, expand **Web Server**, expand **Application Development**, and then select **ASP**.

   d) Click **Next** until the install completes.

9. Browse to `https://localhost/cert.cer`.

   For more information, see Web Server (IIS).

> **Note:**
>
> You can use the IIS instance of the CA for this procedure.

Importing the Root Certificate During Initial FIPS Configuration

When you complete the steps to configure XenMobile for the first time in the command-line console, you must complete these settings to import the root certificate. For details on the installation steps, see Installing XenMobile.

- Enable FIPS: Yes
- Upload Root Certificate: Yes
- Copy(c) or Import(i): i
- Enter HTTP URL to import: `https://<FQDN of IIS server>/cert.cer`
- Server: *FQDN of SQL Server*
- Port: 1433
- User name: Service account which can create the database (`domain\username`).
- Password: The password for the service account.
- Database Name: A name of your choice.

Enable FIPS mode on mobile devices

By default, FIPS mode is disabled on mobile devices. To enable FIPS mode, go to **Settings > Client Properties**, edit the **Enable FIPS Mode** property, and set the value to **true**. For more information, see Client properties.

Configure clustering

November 9, 2020

To configure clustering, configure the following two load balancing virtual IP addresses on Citrix ADC.

- **Mobile device management (MDM) load balancing virtual IP address:** An MDM load balancing virtual IP address is required to communicate with the XenMobile nodes that are configured in a cluster. This load balancing is done in SSL Bridge mode.
- **Mobile app management (MAM) load balancing virtual IP address:** MAM load balancing virtual IP addresses are required for Citrix Gateway to communicate with XenMobile nodes that are configured in a cluster. In XenMobile, by default, all traffic from Citrix Gateway routes to the load balancing virtual IP address on port 8443.

The procedures in this article explain how to create a new XenMobile virtual machine (VM) and joining the new VM to an existing VM. Those steps create a cluster setup.

Prerequisites

- You have fully configured the required XenMobile node.
- Configure NTP on all cluster nodes and the XenMobile database. For clustering to work properly, all of those servers must have the same time.
- One public IP address for MDM load balancer and one private IP address for MAM.
- Server certificates.
- One free IP for Citrix Gateway virtual IP address.
- With XenMobile deployed in a cluster setup and in MDM-only or Enterprise mode (MDM+MAM): Modify your Citrix ADC load balancer configuration to use **Source IP persistence** for all Citrix ADC MDM load balancers, that is, virtual servers set up for ports 8443 and 443. Complete that configuration before user devices upgrade to iOS 11. For more information, see this Citrix Knowledge Center article: https://support.citrix.com/article/CTX227406.
- To install apps from the XenMobile Store on iOS 11 devices, you must enable port 80 on XenMobile Server.

For reference architectural diagrams for XenMobile 10.x in clustered configurations, see Architecture.

Installing the XenMobile Cluster Nodes

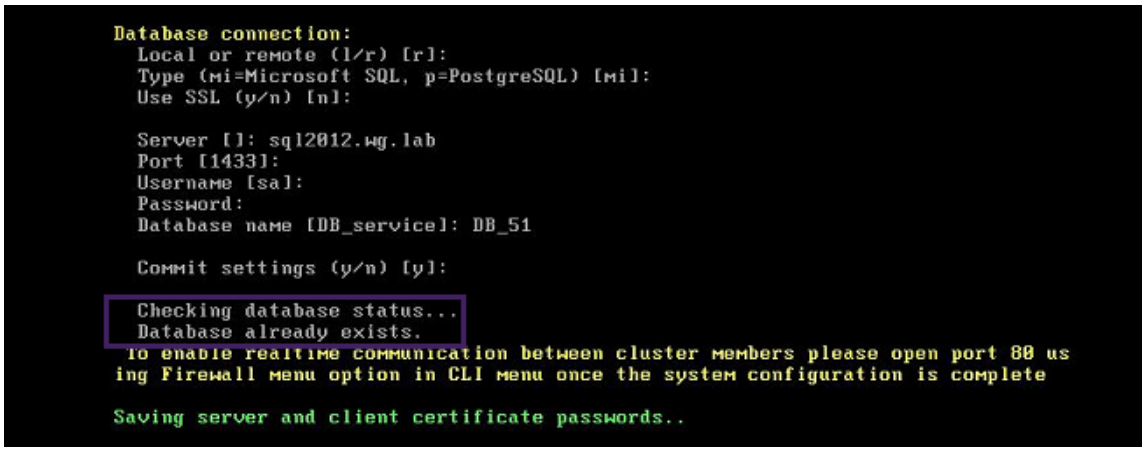
Based on the number of nodes you require, you create XenMobile VMs. You point the new VMs to the same database and provide the same PKI certificate passwords.

1. Open the command-line console of the new VM and enter the new password for the administrator account.
2. Provide the network configuration details as shown in the following figure.

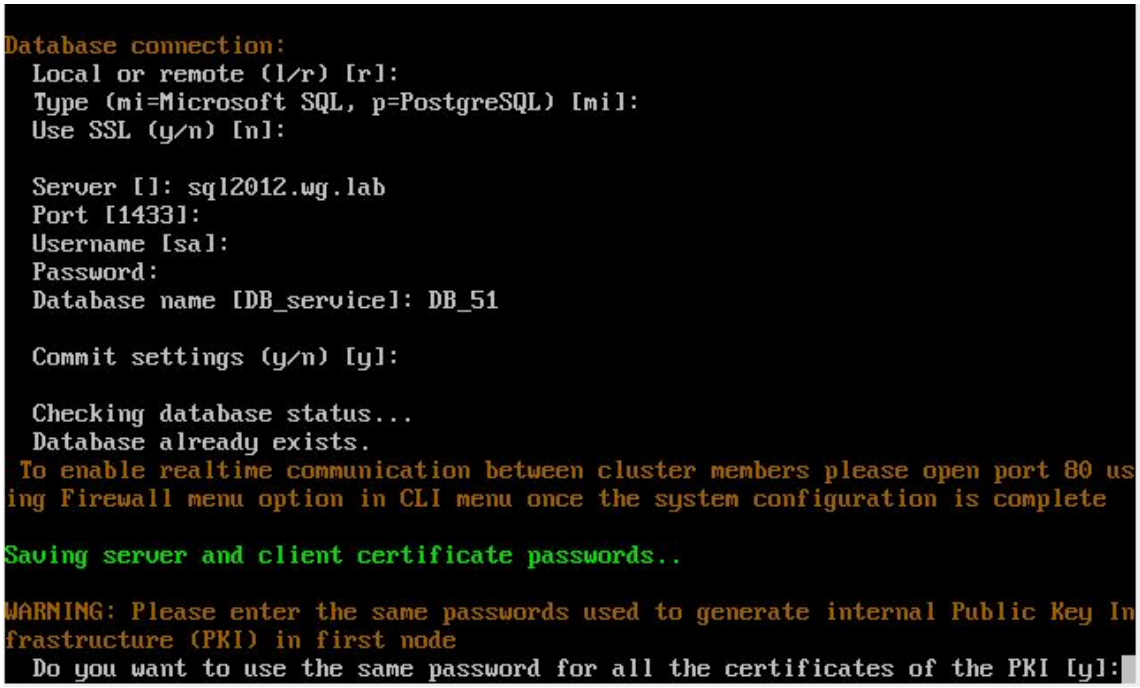
3. If you want to use the default password for data protection, type **y**; or, type **n** and enter a new password.

4. If you want to use FIPS, type **y**; or, type **n**.

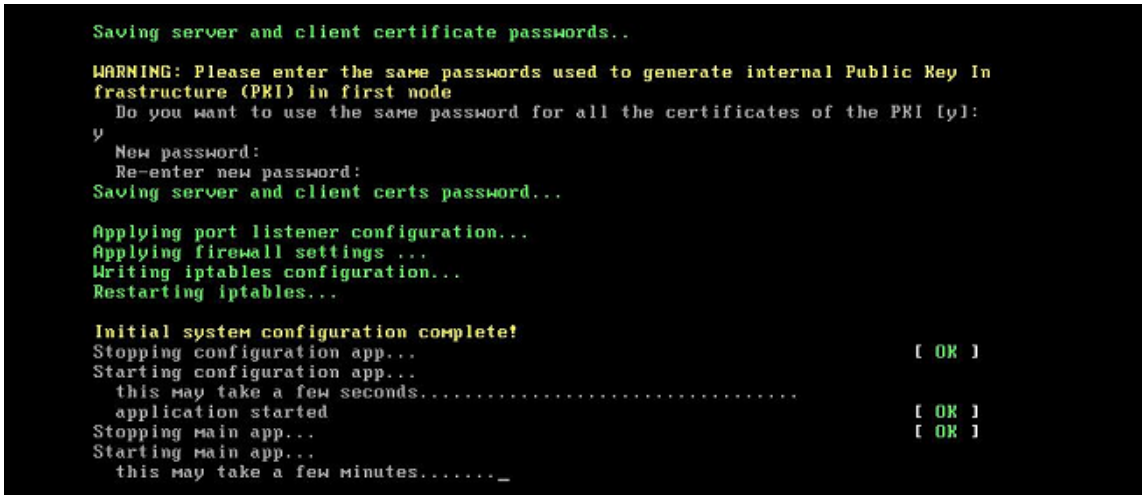
5. Configure the database so that you point to same database that the earlier fully configured VM pointed to. You see the message: Database already exists.



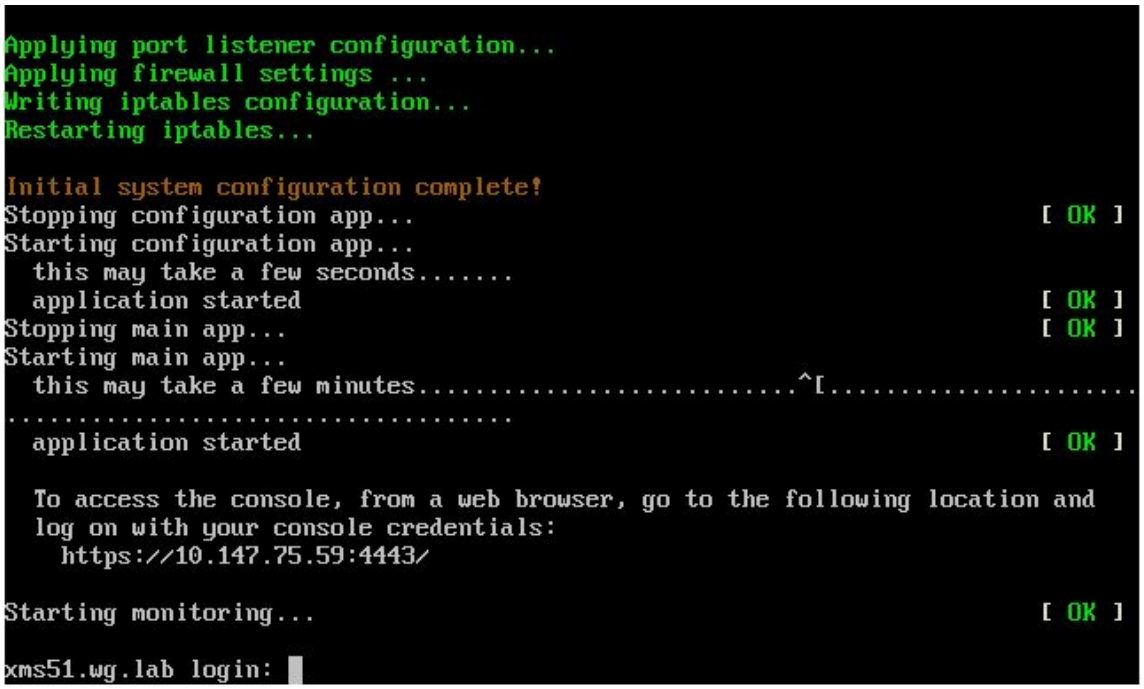
6. Enter the same passwords for the certificates that you provided for the first VM.



After you have entered the password, the initial configuration on second node will complete.



7. When the configuration is complete, the server restarts and the logon dialog box appears.

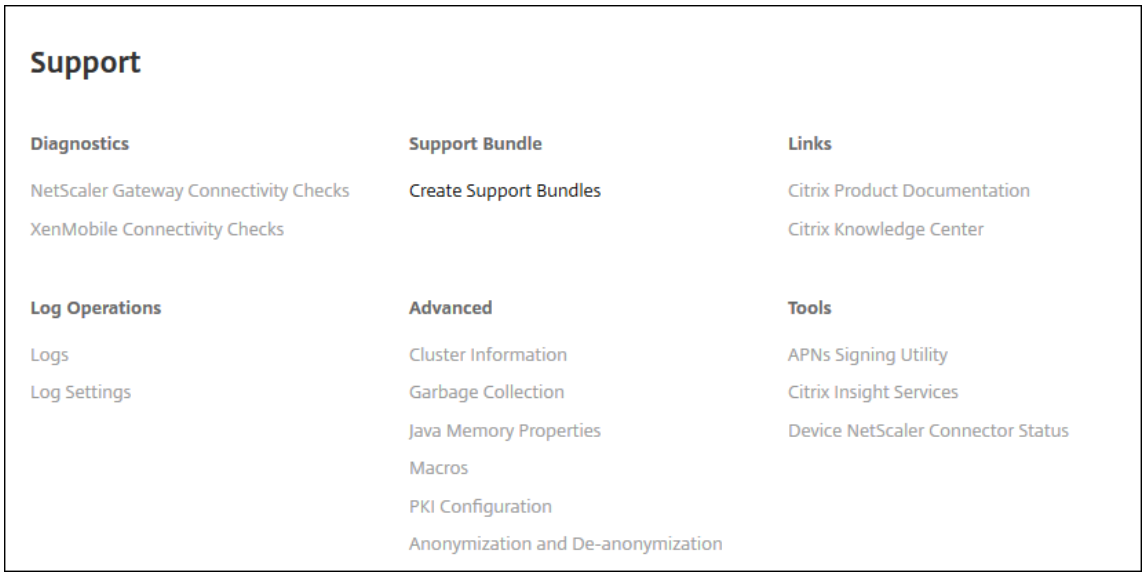


> **Note:**
>
> The logon dialog box is identical to the logon dialog box of the first VM. The match is a way for you to confirm that both VMs are using the same database server.

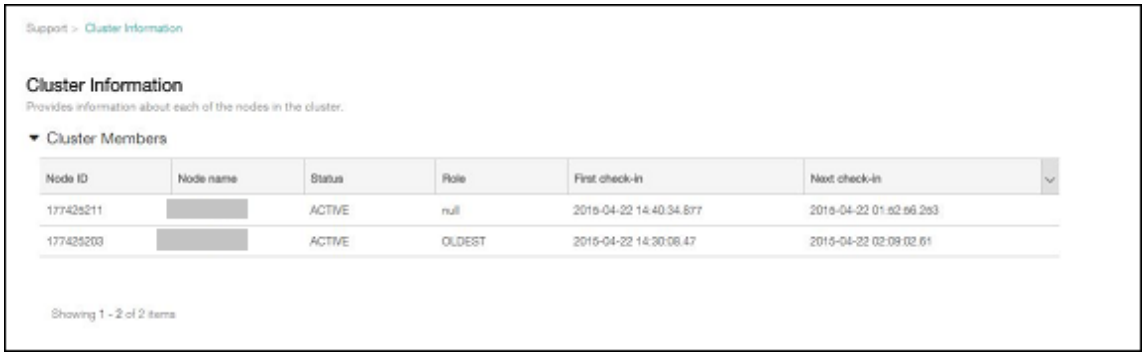
8. Use the fully qualified domain name (FQDN) of XenMobile to open the XenMobile console in a web browser.
9. In the XenMobile console, click the wrench icon in the upper-right corner of the console.

The **Support** page opens.

10. Under **Advanced**, click **Cluster Information**.



All of the information about the cluster, including cluster member, device connection information, tasks, and so on, appear. The new node is now a member of the cluster.

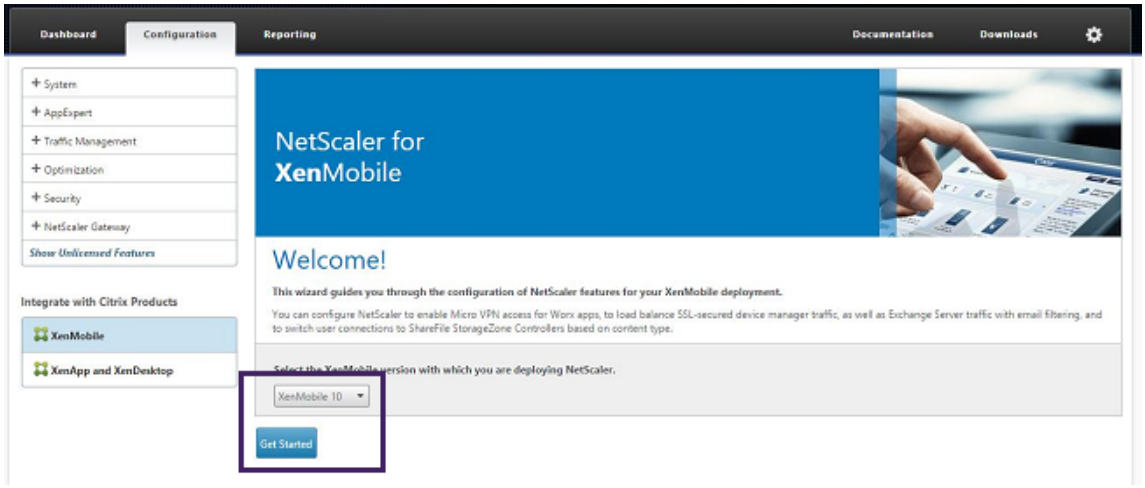


You can add other nodes by following the same steps. The first node added to the cluster has a Role of **OLDEST**. Nodes added after that show a Role of **NONE** or **null**.

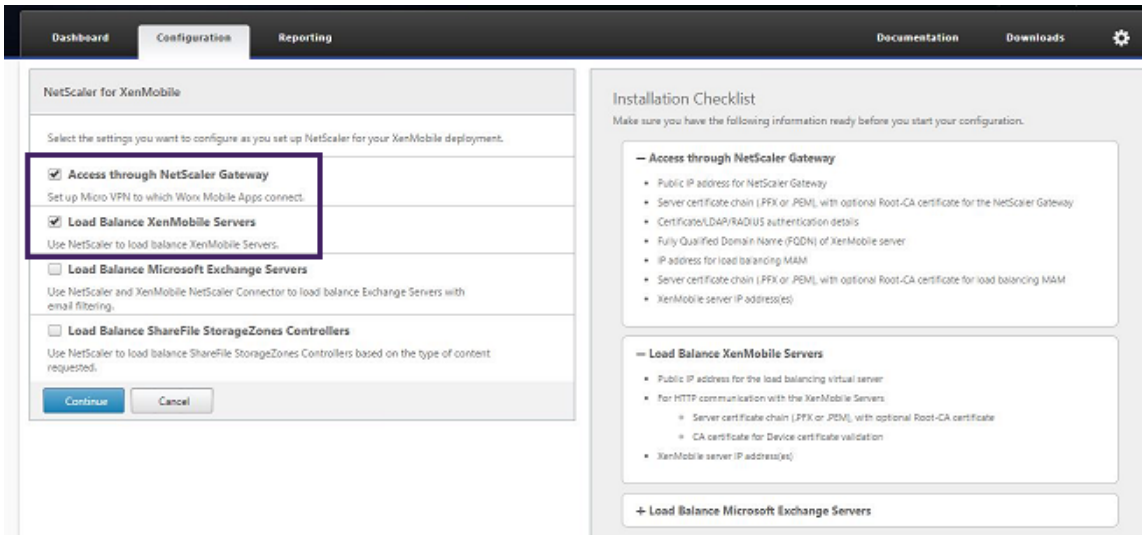
To configure load balancing for the XenMobile cluster in Citrix ADC

After you add the required nodes as members of the XenMobile cluster, load balance the nodes so you can access the clusters. Load balancing is done by running XenMobile Wizard available in Citrix ADC. The following steps describe how to load balance XenMobile by running the wizard.

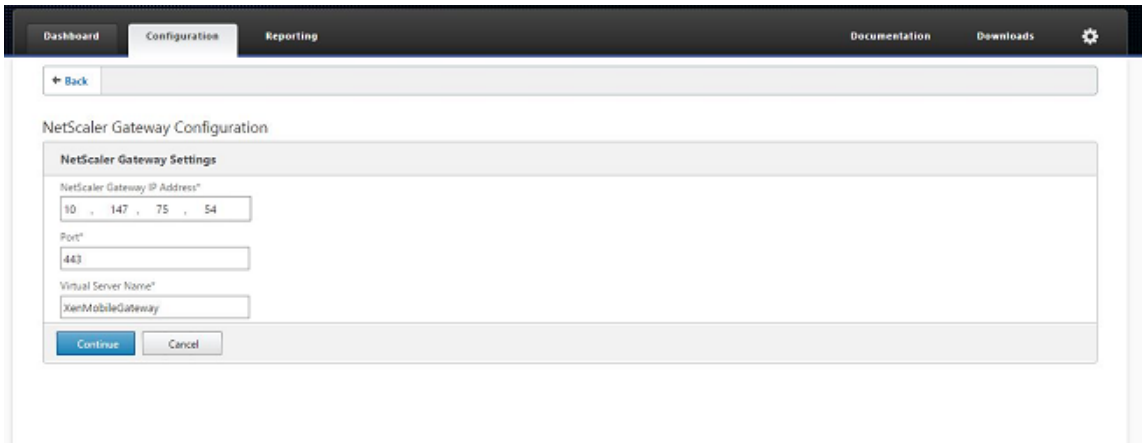
1. Log on to Citrix ADC.
2. On the Configuration tab, click **XenMobile** and then click **Get Started**.



3. Select the **Access through Citrix Gateway** check box and the **Load Balance XenMobile Servers** check box and then click **Continue**.



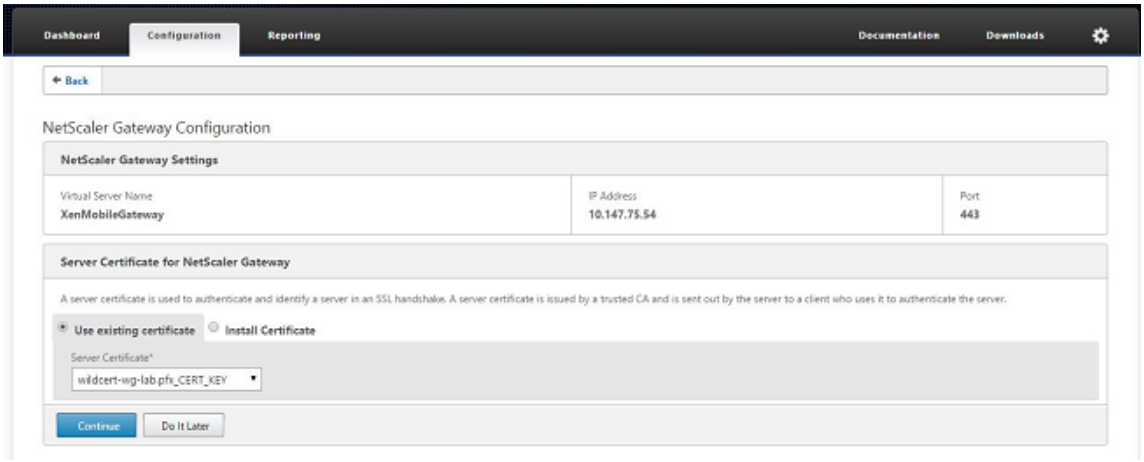
4. Enter the IP address for Citrix Gateway and then click **Continue**.



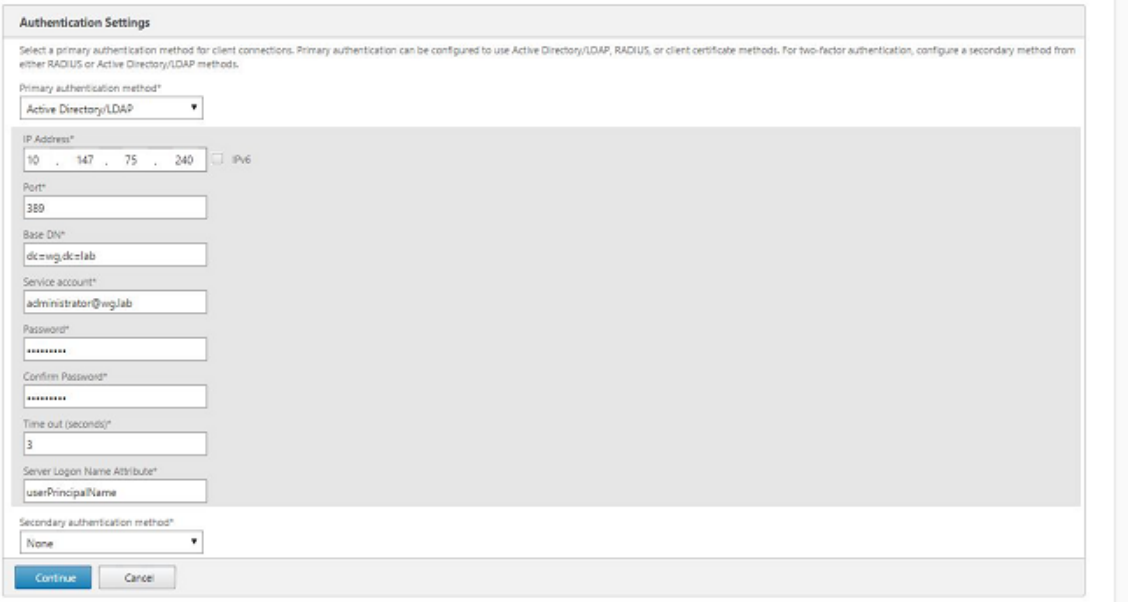
5. Bind the server certificate to the Citrix Gateway virtual IP address by doing one of the following

and then click **Continue**.

- In **Use existing certificate**, choose the server certificate from the list.
- Click the **Install Certificate** tab to upload a new server certificate.

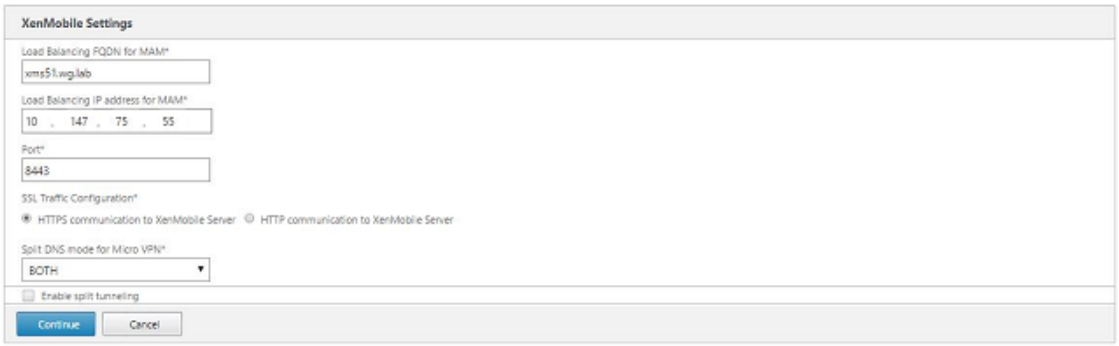


6. Enter the Authentication server details and then click **Continue**.



> **Note:**
>
> Ensure the Server Logon Name Attribute is same as you provided in the XenMobile LDAP configuration.

7. Under XenMobile settings, enter the Load Balancing FQDN for MAM and then click **Continue**.

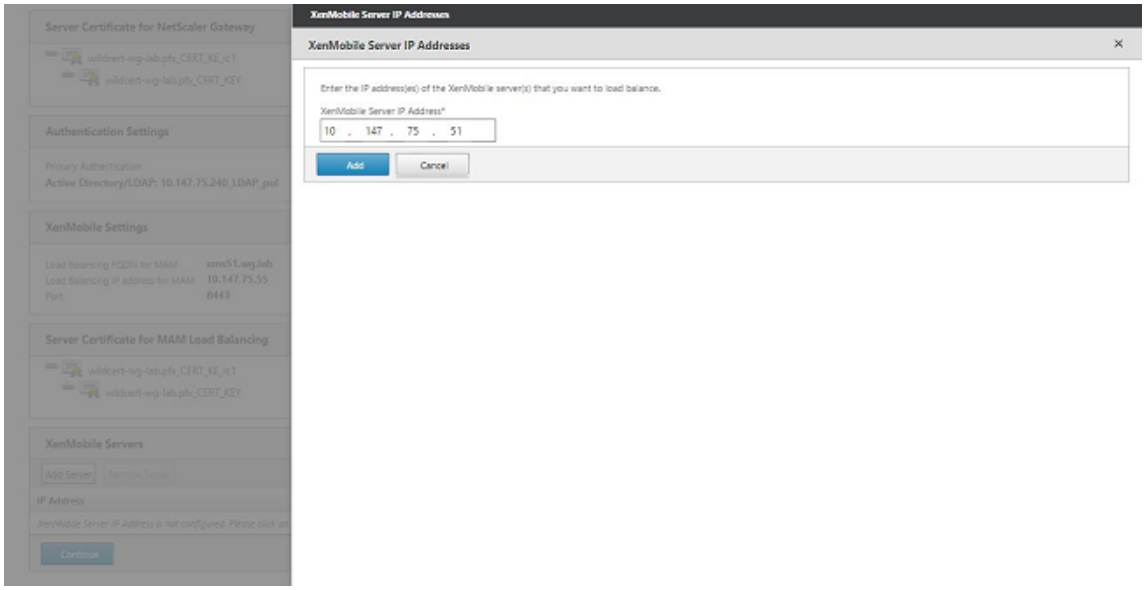


> **Note:**
>
> Ensure the FQDN of the MAM load balancing virtual IP address and the FQDN of XenMobile are the same.

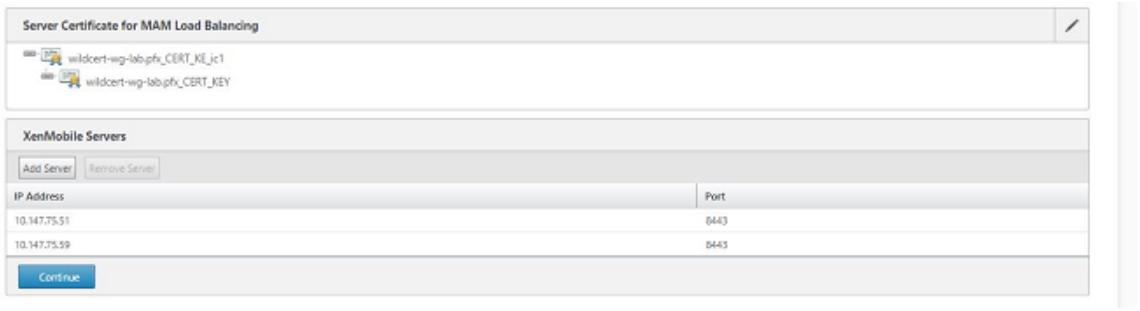
8. If you want to use SSL Bridge mode (HTTPS), select **HTTPS communication to XenMobile Server**. However, if you want to use SSL offload, select **HTTP communication to XenMobile Server**, as shown in the preceding figure. For the purposes of this article, the choice is SSL Bridge mode (HTTPS).
9. Bind the server certificate for the MAM load balancing virtual IP address and then click Continue.

10. Under XenMobile Servers, click **Add Server** to add the XenMobile nodes.

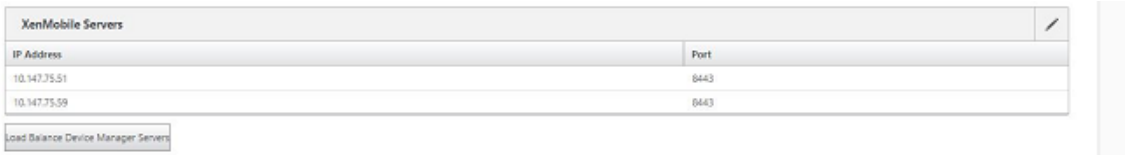
11. Enter the IP address of the XenMobile node and then click Add.



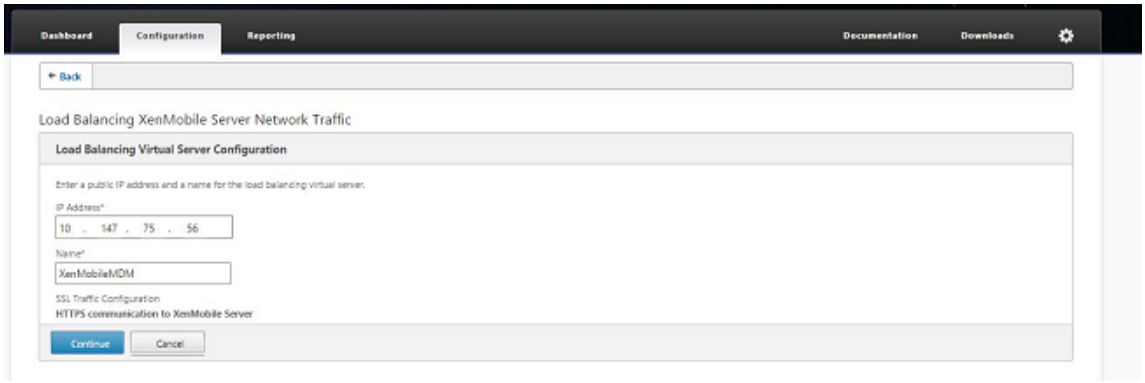
12. Repeat steps 10 and 11 to add more XenMobile nodes that are part of the XenMobile cluster. You see all the XenMobile nodes that you have added. Click Continue.



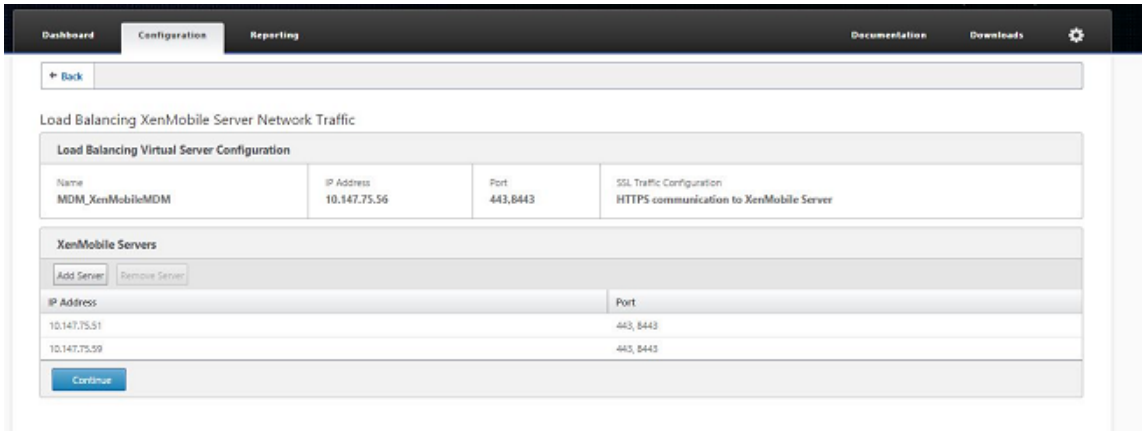
13. Click **Load Balance Device Manager Servers** to continue with the MDM load balancing configuration.



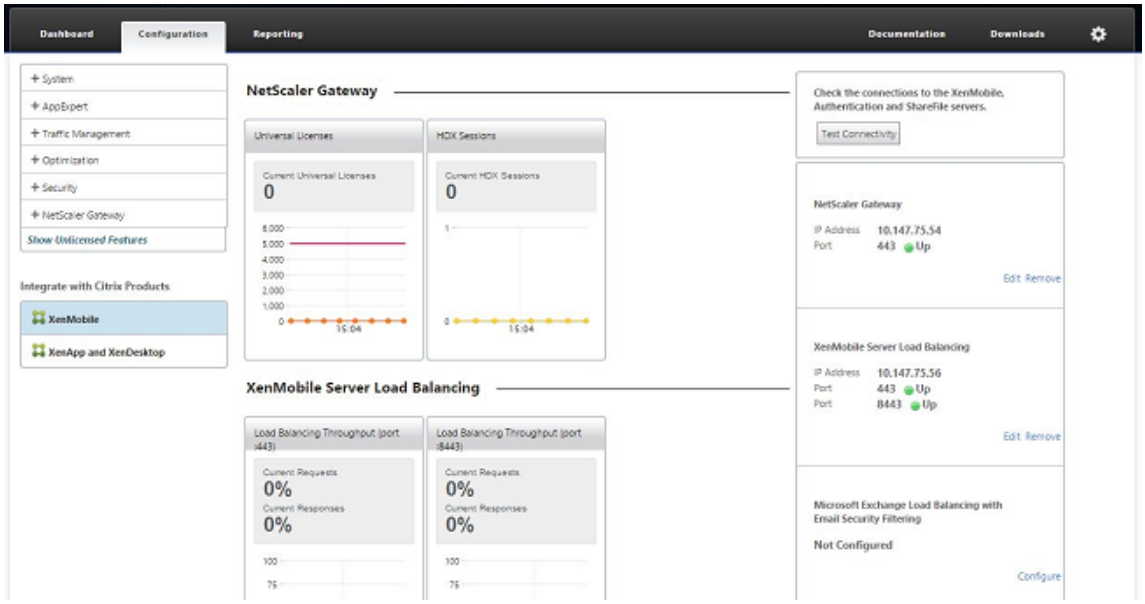
14. Enter the IP address to be used for MDM load balancing IP address and then click **Continue**.



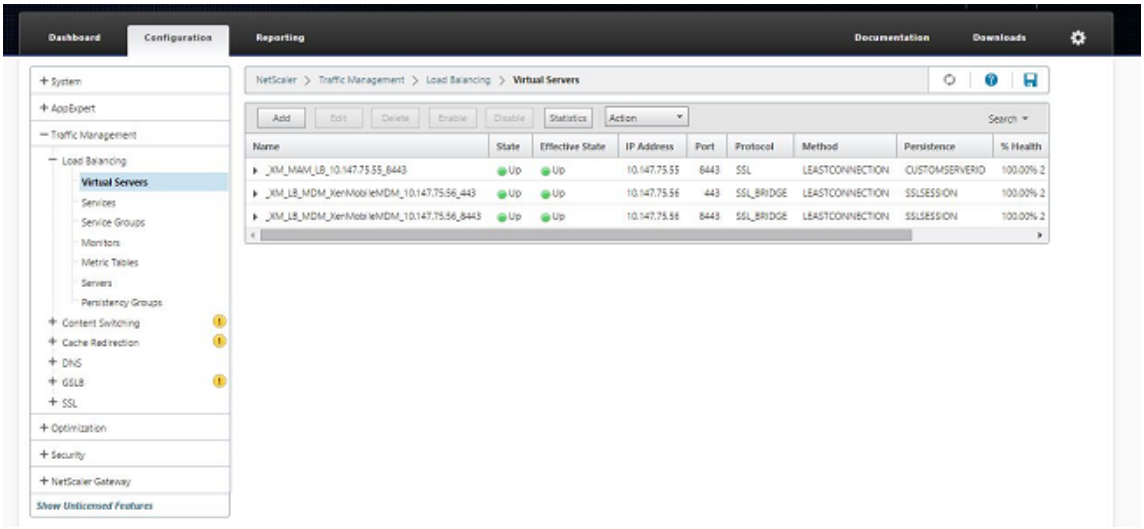
15. Once you see the XenMobile nodes in the list, click **Continue** and then click Done to finish the process.



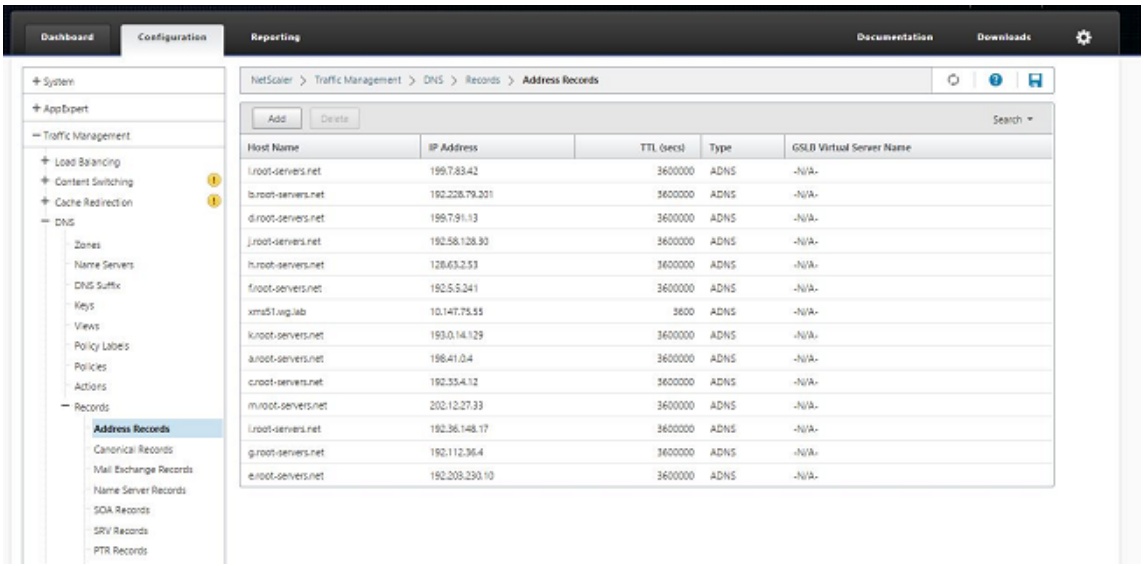
You see the virtual IP address status on the XenMobile page.



16. To confirm if the virtual IP addresses are up and running, click the Configuration tab and then navigate to **Traffic Management > Load Balancing > Virtual Servers**.



You also see that the DNS entry in Citrix ADC points to the MAM load balancing virtual IP address.



Disaster recovery guide

June 18, 2018

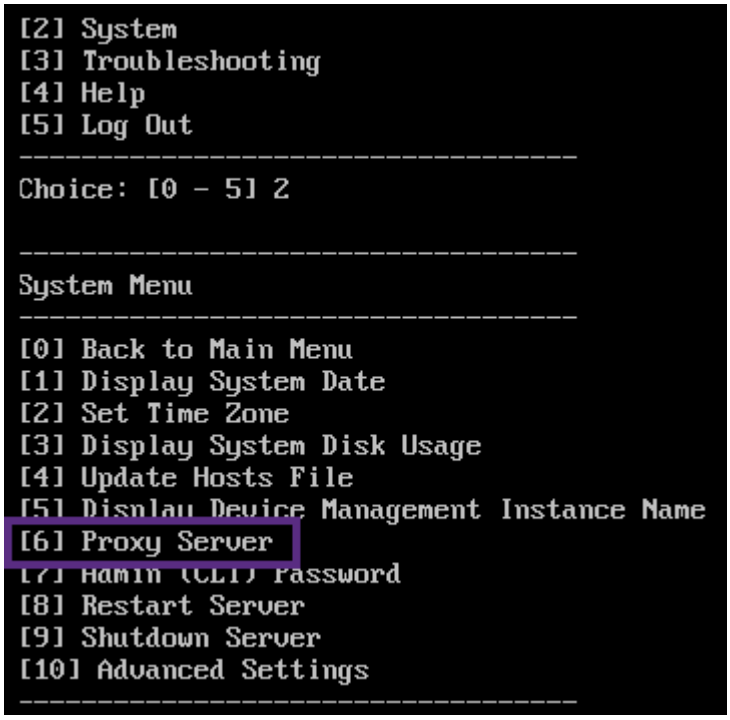
You can architect and configure XenMobile deployments that include multiple sites for disaster recovery using an active-passive failover strategy. For details, see the XenMobile Deployment Handbook Disaster Recovery article.

Enable proxy servers

December 18, 2019

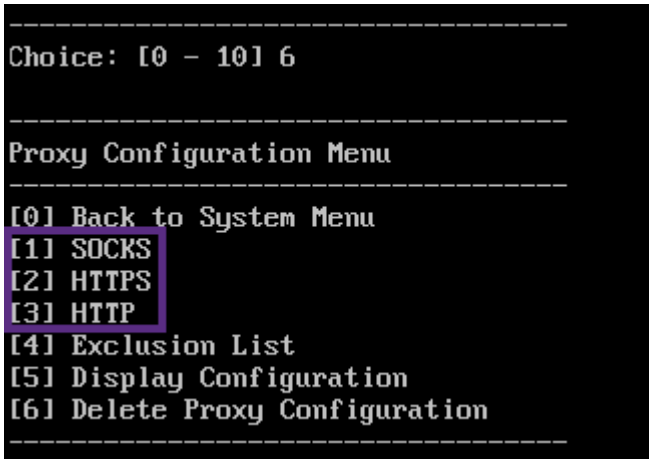
To control outbound internet traffic, you can set up a proxy server in XenMobile to carry that traffic. You set up a proxy server through the command-line interface (CLI). Setting up the proxy server requires restarting your system.

1. In the XenMobile CLI main menu, type **2** to select the System Menu.
2. In the System Menu, type **6** to select the Proxy Server Menu.



3. In the Proxy Configuration Menu, type **1** to select SOCKS.

   Before you save this setup, you must also configure HTTPS. The proxy won't work unless you save the SOCKS and HTTPS settings in the same configuration.



4. Type your proxy server IP address, port number, and target. See the following table for supported target types for each proxy server type.

Proxy type	Supported targets
SOCKS	APNS
HTTP	APNS, Web, PKI
HTTPS	Web, PKI
HTTP with authentication	Web, PKI
HTTPS with authentication	Web, PKI


```
-----------------------------------
Proxy Configuration Menu
-----------------------------------
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----------------------------------
Choice: [0 - 6] 1

Enter socks proxy information

Address []: 203.0.113.23

Port[]: 1080

Target - APNS
Proxy configuration updated successfully.
Please restart all nodes in the cluster for the changes to take effect
Are you sure to restart the system? [y/n]:
```

5. Type **n**, type **2** to select HTTPS, and then type your proxy server IP address, port number, and target.
6. If you choose to configure a user name and password for authentication on your proxy server, type **y**, and then type the user name and password.

```
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----------------------------------
Choice: [0 - 6] 2

Enter https proxy information

Address []: 203.0.113.23

Port[]: 4443

Configure username & password [y/n]: y

Username: Justaname

Password:

Target - WEB
WEB proxy configured. Override proxy settings?[y/n]:
```

7. Type **y** to save the setup.

Configure SQL Server

April 9, 2020

For connections to SQL Server from an on-premises XenMobile Server, you can use any of the following drivers:

- The default driver
- jTDS
- Microsoft Java Database Connectivity (JDBC) driver

The jTDS driver is the default driver when you:

- Install XenMobile Server on-premises.
- Upgrade from a XenMobile Server that's configured to use the jTDS driver.

For both drivers, XenMobile supports SQL Server authentication or Windows authentication. For those combinations of authentication and driver, SSL can be on or off.

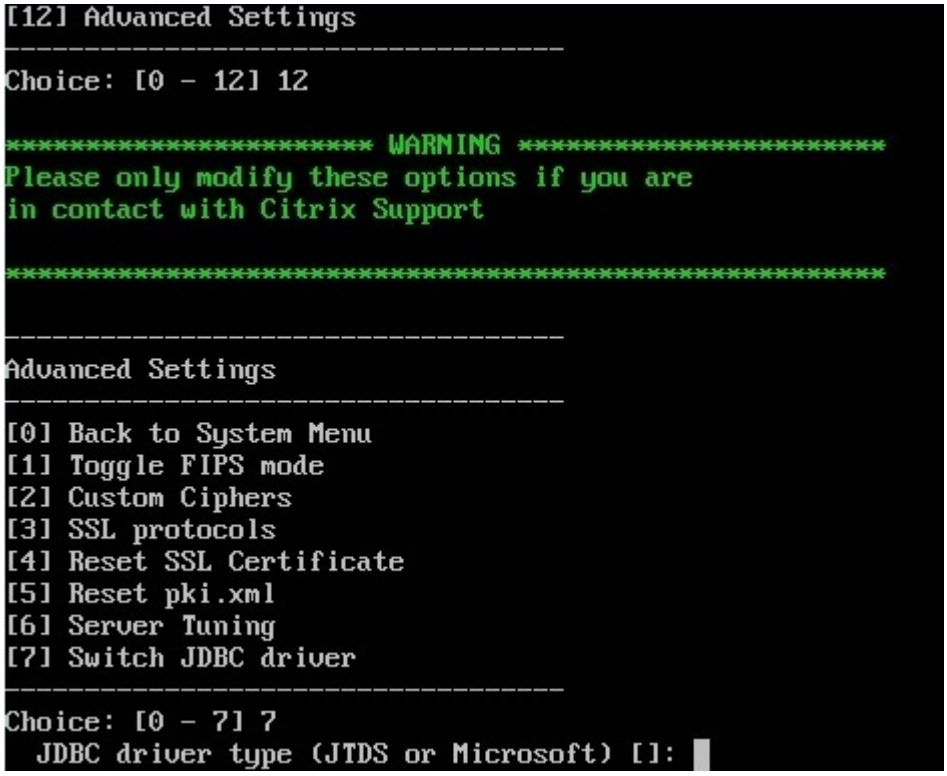
When you use Windows authentication with the Microsoft JDBC driver, the driver uses integrated authentication with Kerberos. XenMobile contacts Kerberos to obtain the Kerberos Key Distribution Center (KDC) details. If the required details aren't available, the XenMobile CLI prompts for the IP address of the Active Directory server.

To switch from the jTDS driver to the JDBC driver, SSH to all your XenMobile Server nodes and use the XenMobile CLI for configuration. The steps vary according to your current jTDS driver configuration, as follows.

Switch to Microsoft JDBC (SQL Server authentication)

To complete these steps, you need the SQL Server user name and password.

1. SSH to all XenMobile Server nodes.
2. In the XenMobile CLI main menu, type **2** to select the **System Menu**.
3. Type **12** to select Advanced Settings.
4. Type **7** to select Switch JDBC driver, and then type **m** for Microsoft.



5. When prompted, type **y** to choose SQL authentication and then type the SQL Server user name and password.
6. Repeat the steps for each XenMobile Server node.
7. Restart each XenMobile Server node.

Switch to Microsoft JDBC (SSL is off; Windows authentication)

To complete these steps, you need the Active Directory user name and password, the Kerberos KDC realm, and the KDC user name.

1. SSH to all XenMobile Server nodes.
2. In the XenMobile CLI main menu, type **2** to select the **System Menu**.
3. Type **12** to select Advanced Settings.
4. Type **7** to select Switch JDBC driver, and then type **m**.
5. When prompted whether to use SQL Server authentication, type **n**.
6. When prompted, type the Active Directory user name and password configured for the SQL server.
7. If XenMobile doesn't auto-discover the Kerberos KDC realm, it prompts for the KDC details, including the SQL server FQDN.

8. When prompted whether to use SSL, type **n**. XenMobile saves the configuration. If XenMobile can't save the configuration because of errors, it shows an error message and the details that you entered.
9. Repeat the steps for each XenMobile Server node.
10. Restart each XenMobile Server node.

To change the XenMobile database password

Follow this guidance to change the XenMobile database password, such as when Citrix Support directs you to make a password change.

If your SQL server uses Windows authentication, make database password changes in Windows Active Directory. Then, refresh the database administrator account on the database server to synchronize the password change. You can then change the password in XenMobile, as follows.

> **Important:**
>
> - Plan a scheduled maintenance window for changing the database password in XenMobile. A password change must occur during system downtime.
> - When you change the password, ensure that all XenMobile nodes are connected to the network. After you change the password, restart XenMobile.
>
>   If you don't restart XenMobile after a password change, XenMobile goes into recovery mode. In that case, revert to the old password in SQL server, restart XenMobile, and change the password again.

1. Verify that all XenMobile Server nodes are running. For a clustered environment, bring up all nodes.
2. Block the incoming device traffic to XenMobile at the Citrix ADC load balancer by disabling the virtual server.
3. To change the database password in SQL server: Log in to the XenMobile CLI, navigate to **Configuration > Database**, and enter the changed password when prompted:

```
Server []: <ipAddress>
Port [1433]: 1433
Username [sa]: <userName>
Password: <****>
<!--NeedCopy-->
```

4. Choose **Y** to restart the server.
5. Repeat steps 3 and 4 for all the other nodes in the cluster.

6. Unblock the incoming device traffic by enabling the virtual server at the Citrix ADC load balancer.

Server properties

August 20, 2020

XenMobile has many properties that apply to server-wide operations. This article describes many of the server properties and details how to add, edit, or delete server properties.

Some properties are Custom Keys. To add a custom key, click **Add** and then, from **Key**, choose **Custom Key**.

For information about the properties typically configured, see Server Properties in the XenMobile virtual handbook.

Server Property Definitions

Add Device Always

- If **true**, XenMobile adds a device to the XenMobile console, even if it fails enrollment, so 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 XenMobile 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 Log Cleanup Execution Time

- The time to start the audit log cleanup, formatted as HH:MM AM/PM. Example: 04:00 AM. Defaults to **02:00 AM**.

Audit Log Cleanup Interval (in Days)

- The number of days that XenMobile retains the audit log. Defaults to **1**.

Audit Logger

- If **False**, does not log user interface (UI) events. Defaults to **False**.

Audit Log Retention (in Days)

- The number of days that XenMobile retains the audit log. Defaults to **7**.

auth.ldap.connect.timeout and auth.ldap.read.timeout

- To compensate for slow LDAP responses, Citrix recommends that you add server properties for the following Custom Keys.
  - Key: **Custom Key**
  - Key: **auth.ldap.connect.timeout**
  - Value: **60000**
  - Display Name: **auth.ldap.connect.timeout**
  - Description: **LDAP connection timeout**
  - Key: **Custom Key**
  - Key: **auth.ldap.read.timeout**
  - Value: **60000**
  - Display Name: **auth.ldap.read.timeout**
  - Description: **LDAP read timeout**

Certificate Renewal in Seconds

- The number of seconds before a certificate expires that XenMobile starts to renew certificates. For example, if a certificate will expire December 30 and this property is set to 30 days: If the device connects between December 1 and December 30, XenMobile attempts to renew the certificate. Defaults to **2592000** seconds (30 days).

Connection Timeout

- The session inactivity timeout, in minutes, after which XenMobile closes the TCP connection to a device. The session remains open. Applies to Android and Windows CE devices and Remote Support. Defaults to **5** minutes.

Connection Time out to Microsoft Certification Server

- The number of seconds that XenMobile waits for a response from the certificate server. If the certificate server is slow and has much traffic, 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).

Default deployment channel

- Determines how XenMobile deploys a resource to a device: At the user-level (**DEFAULT_TO_USER**) or device-level. Defaults to **DEFAULT_TO_DEVICE**.

Deploy Log Cleanup (in Days)

- The number of days that XenMobile retains the deployment log. Defaults to **7**.

Disable Host Name Verification

- By default, host name verification is enabled on outgoing connections except for the Microsoft PKI server. When host name 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 host name 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 your XenMobile Server
  - The Microsoft CA server is the certificate issuer
  - An internal CA, whose root XenMobile Server doesn't trust, signed your certificate.

Defaults to **True**.

Enable Console

- If **true**, enables user access to the Self-Help Portal Console. 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 XenMobile connections to 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. XenMobile 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**.

force.server.push.required.apps

- Enables the forced deployment of required apps on Android and iOS devices in situations such as the following:
  - You upload a new app and mark it as required.
  - You mark an existing app as required.
  - As user deletes a required app.
  - A Secure Hub update is available.

Forced deployment of required apps is **false** by default. Create the custom key and set **Value** to **true** to enable forced deployment. During forced deployment, MDX-enabled required apps, including enterprise apps and public app store apps, upgrade immediately. The upgrade occurs even if you configure an MDX policy for an app update grace period and the user chooses to upgrade the app later.

- Key: **Custom Key**
- Key: **force.server.push.required.apps**
- Value: **false**
- Display Name: **force.server.push.required.apps**
- Description: **Force required apps to deploy**

Full Pull of ActiveSync Allowed and Denied Users

- The interval in (in seconds) that XenMobile pulls a complete list (baseline) of ActiveSync allowed and denied users. Defaults to **28800** seconds.

hibernate.c3p0.idle_test_period

- This XenMobile Server property, a Custom Key, determines the idle time in seconds before a connection is automatically validated. Configure the key as follows. Default is **30**.
- Key: **Custom Key**
- Key: **hibernate.c3p0. idle_test_period**

- Value: **30**
- Display Name: **hibernate.c3p0. idle_test_period =*nnn***
- Description: **Hibernate idle test period**

hibernate.c3p0.max_size

- This Custom Key determines the maximum number of connections that XenMobile can open to the SQL Server database. XenMobile uses the value you specify for this custom key as an upper limit. The connections open only if you need them. Base your settings on the capacity of your database server. For more information, see Tuning XenMobile Operations. Configure the key as follows. Default is **1000**.
- Key: **hibernate.c3p0.max_size**
- Value: **1000**
- Display Name: **hibernate.c3p0.max_size**
- Description: **DB connections to SQL**

hibernate.c3p0.min_size

- This Custom Key determines the minimum number of connections that XenMobile opens to the SQL Server database. Configure the key as follows. Default is **100**.
- Key: **hibernate.c3p0.min_size**
- Value: **100**
- Display Name: **hibernate.c3p0.min_size**
- Description: **DB connections to SQL**

hibernate.c3p0.timeout

- This Custom Key determines the idle time-out, in seconds. Default is **120**.
- Key: **Custom Key**
- Key: **hibernate.c3p0.timeout**
- Value: **120**
- Display Name: **hibernate.c3p0.timeout**
- Description: **Database idle timeout**

Identifies if telemetry is enabled or not

- Identifies if telemetry (Customer Experience Improvement Program, or CEIP) is enabled. You can opt in to CEIP when you install or upgrade XenMobile. If XenMobile has 15 consecutive failed uploads, it disables telemetry. Defaults to **false**.

Inactivity Timeout in Minutes

- If the **WebServices timeout type** server property is **INACTIVITY_TIMEOUT:** This property defines the number of minutes after which XenMobile logs out an inactive administrator who did the following:
  - Used the XenMobile Public API for REST Services to access the XenMobile console
  - Used the XenMobile Public API for REST Services to access any third-party app. A timeout of **0** means that an inactive user remains logged in.

Defaults to **5**.

iOS Device Management Enrollment Auto-Install Enabled

- If true, this property reduces the amount of user interaction required during device enrollment. Users must click **Root CA install** (if needed) and **MDM Profile install**.

iOS Device Management Enrollment First Step Delayed

- After a user enters their credentials during device enrollment, this value specifies how long to wait before prompting for the root CA. 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 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 XenMobile 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 XenMobile iOS agent identities. Defaults to **1024**.

iOS Device Management Identity Renewal Days

- Specifies the number of days before the certificate expiration that XenMobile 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, XenMobile issues a new certificate. Defaults to **30** days.

iOS MDM APNS Private Key Password

- This property contains the APNs password, which is required for XenMobile 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 XenMobile disconnects it. Defaults to **7** days.

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, with a larger number of threads, such as 6, a volume purchase import results in high CPU usage.

Citrix ADC Single Sign-On

- If **False**, disables the XenMobile callback feature during single sign-on from Citrix ADC to XenMobile. If the Citrix Gateway configuration includes a callback URL, XenMobile 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. XenMobile increments the value when an upload fails. After 15 upload failures, XenMobile disables CEIP, also called telemetry. For more information, see the server property **Identifies if telemetry is enabled or not**. XenMobile 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**.

Pull of Incremental Change of Allowed and Denied Users

- The number of seconds that XenMobile waits for a response from the domain when executing 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 XenMobile 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**.

Session Log Cleanup (in Days)

- The number of days that XenMobile retains the session log. Defaults to **7**.

Server Mode

- Determines whether XenMobile runs in MAM, MDM, or ENT (enterprise) mode, corresponding to app management, device management, or app and device management. Set the Server Mode property according to how you want devices to register, as noted in the table below. Server Mode defaults to **ENT**, regardless of license type.

If you have a XenMobile MDM Edition license, the effective server mode is always MDM regardless of how you set the server mode in Server Properties. If you have an MDM Edition license, you cannot enable app management by setting the server mode to either MAM or ENT.

Your licenses are this Edition	You want devices to register in this mode	Set Server Mode property to
Enterprise / Advanced	MDM mode	MDM
Enterprise / Advanced	MDM+MAM mode	ENT
MDM	MDM mode	MDM

The effective server mode is a combination of the license type and server mode. For an MDM license, the effective server mode is always MDM, regardless of the server mode setting. For Enterprise and Advanced licenses, the effective server mode matches the server mode, if the server mode is **ENT** or **MDM**. If the server mode is **MAM**, the effective server mode is ENT.

XenMobile adds the server mode to the server log for each of these activities: A license is activated, a license is deleted, and you change the server mode in Server Properties. For information about creating and viewing log files, see Logs and View and analyze log files in XenMobile.

Content Collaboration configuration type

- Specifies the SCitrix Files storage type. **ENTERPRISE** enables Citrix Files Enterprise mode. **CONNECTORS** provides access only to storage zone connectors that you create through the XenMobile console. Defaults to **NONE**, which shows the initial view of the **Configure > ShareFile** 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 XenMobile logs out an administrator after using the following:
  - The XenMobile Public API for REST Services to access the XenMobile console.
  - The XenMobile 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. XenMobile 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 XenMobile 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**.

User-Defined Device Properties N

- Used for Windows CE devices only. This custom key enables you to obtain properties that you create in the registry of Windows CE devices. After those properties are in the XenMobile database, you can create deployment rules based on the value of the properties.

- Key: **Custom Key**
- Key: **device.properties.userDefinedN**
- Value: *administrator-defined*
- Display Name: *administrator-defined*
- Description: *administrator-defined*

Users only from Exchange

- If **true**, disables user authentication for ActiveSync Exchange users. Defaults to **false**.

VP baseline interval

- The minimum interval that XenMobile reimports volume purchase licenses from Apple. Refreshing license information ensures that XenMobile reflects all changes, such as when you manually delete an imported app from volume purchase. By default, XenMobile refreshes the volume purchase license baseline a minimum of every **720** 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 XenMobile updated with the changes. The minimum interval between two baselines is 60 minutes. In addition, XenMobile 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**, XenMobile considers an authentication token as expired after the value specified in the server property **Static Timeout in Minutes**.

If **INACTIVITY_TIMEOUT**, XenMobile considers an authentication token as expired after the token is inactive for the value specified in 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 XenMobile 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**.

XenMobile MDM Self-Help Portal console max inactive interval (minutes)

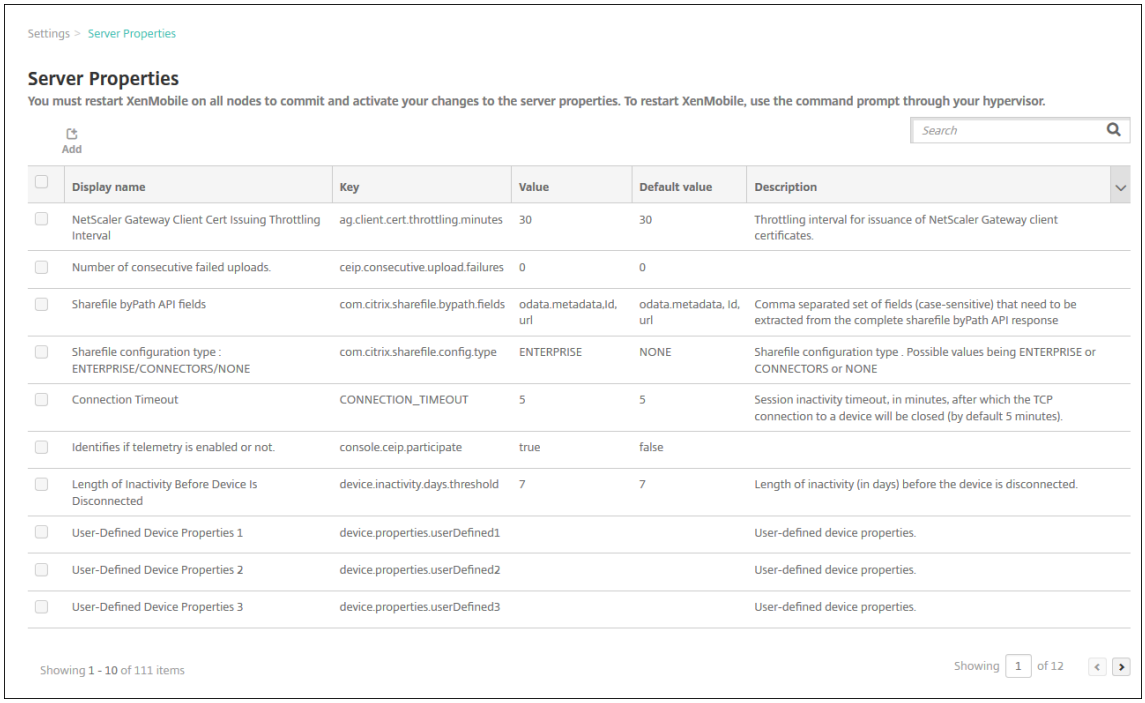
- The number of minutes after which XenMobile logs out an inactive user from the XenMobile Self-Help Portal. A timeout of **0** means that an inactive user remains logged in. Defaults to **30**.

Adding, Editing, or Deleting Server Properties

In XenMobile, you can apply properties to the server. After making changes, ensure that you restart XenMobile on all nodes to commit and activate changes.

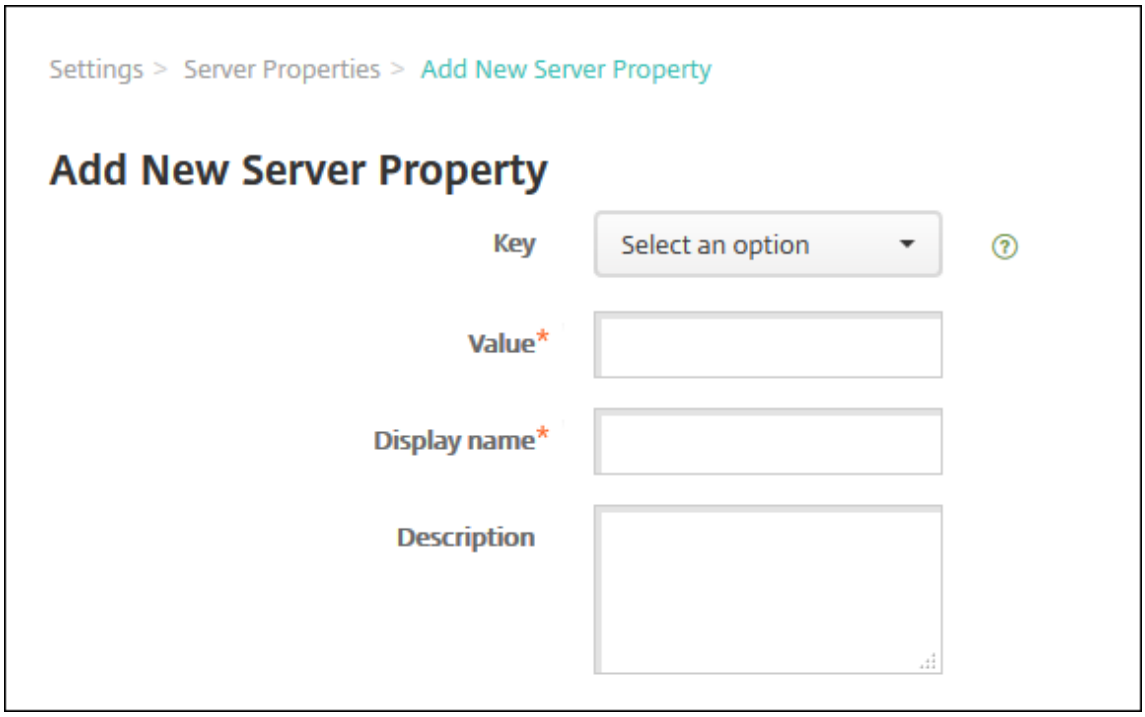
> **Note:**
>
> To restart XenMobile, use the command prompt through your hypervisor.

1. In the XenMobile 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.



To add a server property

1. Click **Add**. The **Add New Server Property** page appears.



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.

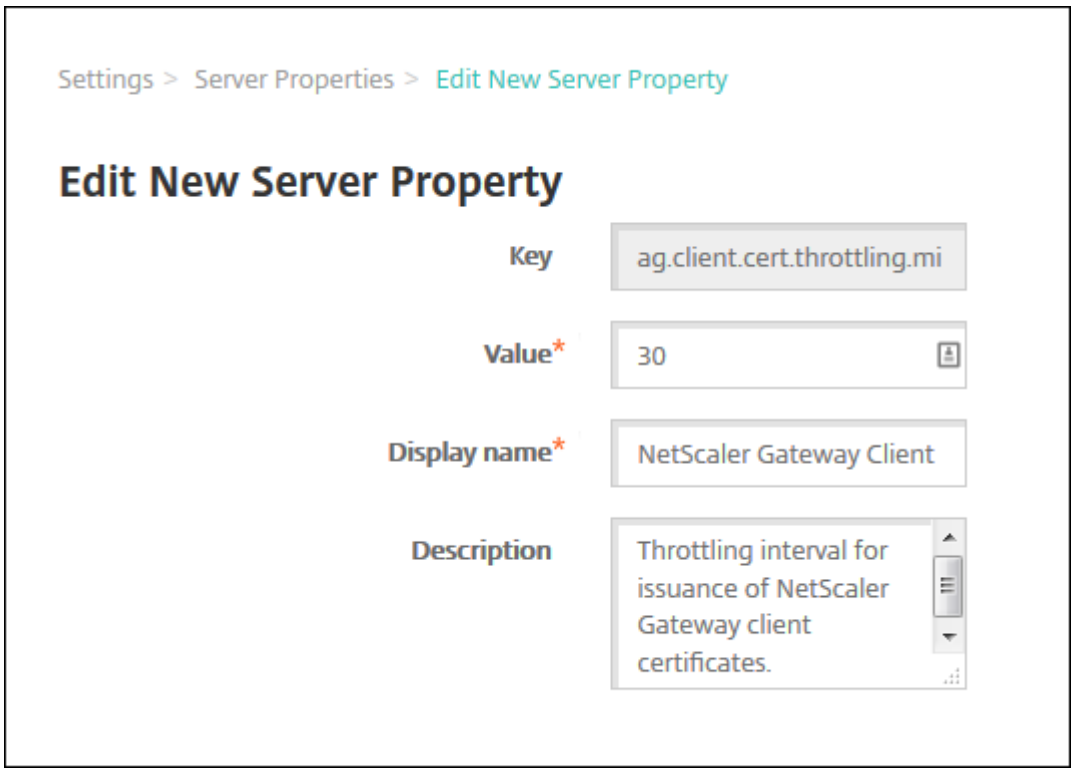
3. Click **Save**.

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.



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 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.

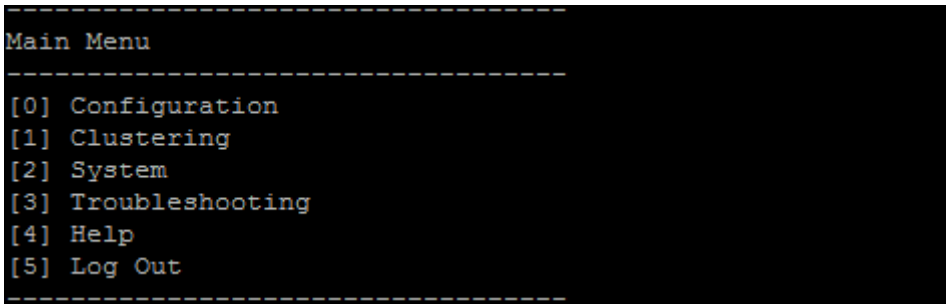
Command-line interface options

October 16, 2020

For an on-premises installation of XenMobile Server, you can access the CLI options as follows:

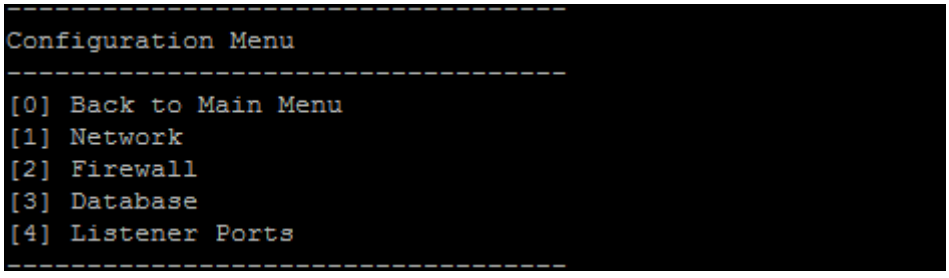
- **From the hypervisor on which you installed XenMobile:** In your hypervisor, select the imported XenMobile virtual machine, start the command prompt view, and log on to your administrator account for XenMobile. For details, see the documentation for your hypervisor.
- **If SSH is enabled in your firewall, by using SSH:** Log on to your administrator account for XenMobile.

You can perform various configuration and troubleshooting tasks using the CLI. The following figure shows the top-level menu for the CLI.



Configuration options

Following are samples of the **Configuration Menu** and the settings displayed for each option.



[1] Network

```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  IP address [10.207.87.75]:10.200.87.75
  Netmask [255.255.254.0]:255.255.254.0
  Default gateway [10.207.86.1]:10.200.86.1
  Primary DNS server [10.207.86.50]:10.200.86.50
  Secondary DNS server (optional) []:

Applying network settings...

Are you sure to restart the system? [y/n]:
```

[2] Firewall

```
Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:
 - comma separated list of hosts or networks
 - e.g. 10.20.5.3, 10.20.6.0/24
 - an empty value means no access restriction
 - enter c as value to clear list

  HTTP service
    Port: 80
    Enable access (y/n) [y]: y
    Access white list []:

  Management HTTPS service
    Port: 4443
    Enable access (y/n) [y]:
    Access white list []:

  SSH service
    Port [22]:
    Enable access (y/n) [y]:
    Access white list []:

  Management API (for initial staging) HTTPS service
    Port [30001]:
    Enable access (y/n) [n]:

  Remote support tunnel
    Port [8081]:
    Enable access (y/n) [n]:

Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
```


[3] Database

```
  Type: [mi]
  Use SSL (y/n) [n]:
  Server [10.207.86.64]:
  Port [1433]:
  Username [sa]:
  Password:
  Database name [RC]:

 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]:
```

[4] Listener Ports

```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  HTTP [80]:
  HTTPS with certificate authentication [443]:
  HTTPS with no certificate authentication [8443]:
  HTTPS for management [4443]:
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
Are you sure to restart the system? [y/n]:
```

Clustering options

Following are samples of the **Clustering Menu** and the settings displayed for each option.

```
---------------------------------
Clustering Menu
---------------------------------
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
---------------------------------
```

[1] Show Cluster Status

```
Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75  status: ACTIVE  role: OLDEST
node: 10.207.87.77  status: ACTIVE  role: NONE
node: 10.207.87.88  status: ACTIVE  role: NONE
```


[2] Enable/Disable cluster

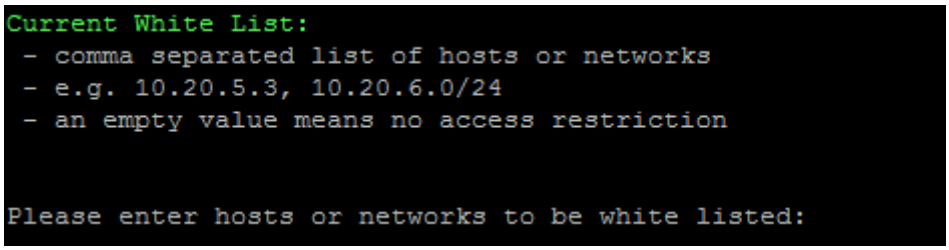
When you choose to enable clustering, the following message appears:

```
To enable real-time communication between cluster members, please open port
 80 using the Firewall menu option in CLI menu. Also configure Access white
 list under Firewall settings for restricted access.
```

When you choose to disable clustering, the following message appears:

```
You have chosen to disable clustering. Access to port 80 is not needed.
Please disable it.
```

[3] Cluster member white list



[4] Enable or disable SSL offload

When you select to enable or disable SSL offloading, the following message appears:

```
Enabling SSL offload opens port 80 for everyone. Please configure Access
white list under Firewall settings for restricted access.
```

[5] Display Hazelcast Cluster

When you select to display the Hazelcast Cluster, the following options appear:

Hazelcast Cluster Members:

[IP addresses listed]

> **Note:**
>
> If a configured node is not part of the cluster, restart that node.

System options

From the **System Menu**, you can display or set system-level information, restart, or shut down the server, or access **Advanced Settings**.


```
-----------------------------------
System Menu
-----------------------------------
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Set NTP Server
[4] Display NTP Status
[5] Display System Disk Usage
[6] Update Hosts File
[7] Display Device Management Instance Name
[8] Proxy Server
[9] Admin (CLI) Password
[10] Restart Server
[11] Shutdown Server
[12] Advanced Settings
-----------------------------------
```

Set NTP Server enables you to specify NTP server information. If you have time zone issues when syncing XenMobile time with a hypervisor, you can avoid the issues by pointing XenMobile to an NTP server. Restart all cluster servers after changing this option.

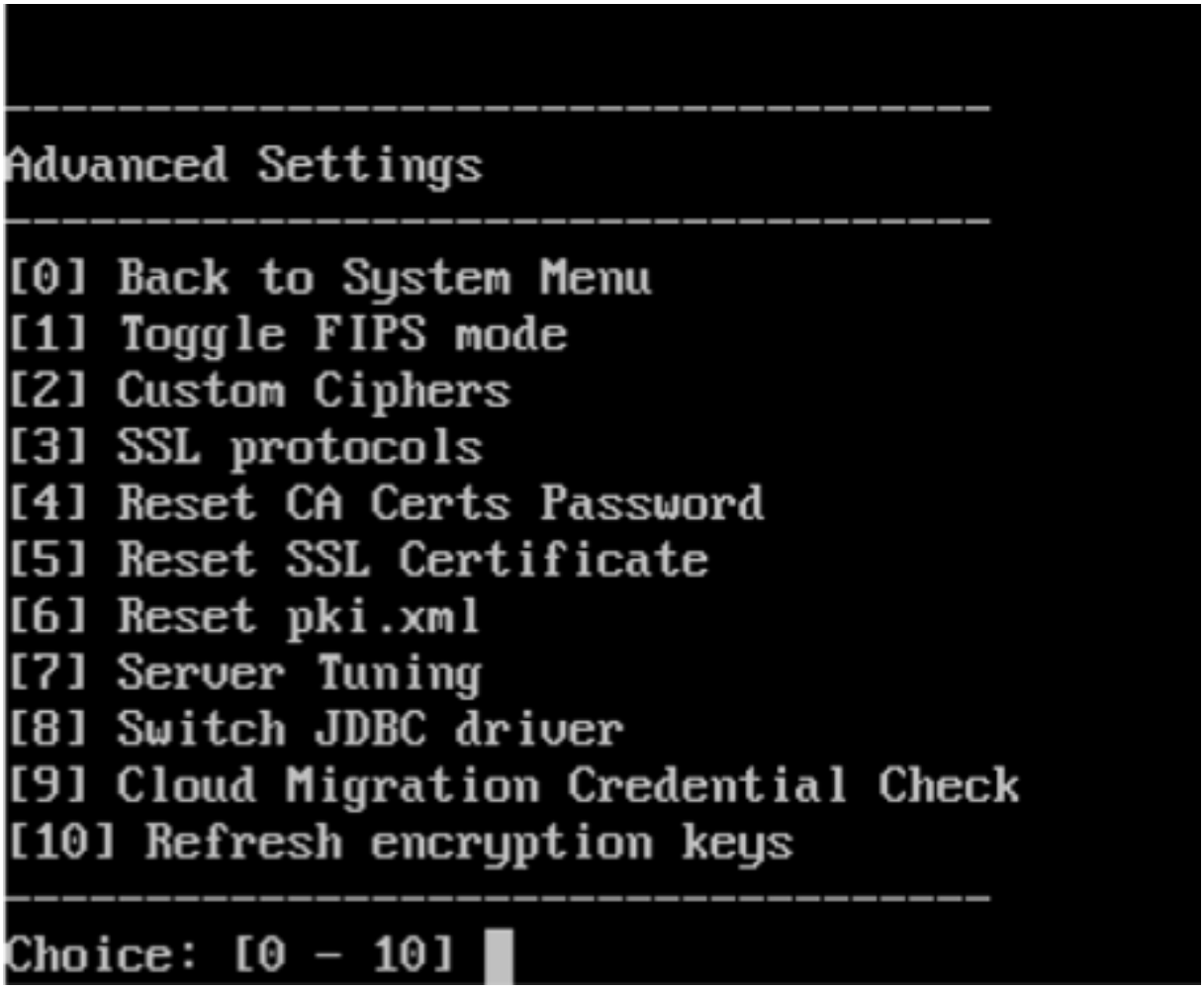
You can also check the disk space by viewing the **[5] Display System Disk Usage** menu item.

About shutting down server nodes

When you shut down a single server node in a cluster, other nodes can generally handle the workload if they meet the requirements documented in Scalability and performance. The impact can vary depending on how many nodes are down at the same time, the total number of users, and how long the nodes are down.

- Users can still access Secure Hub and the store.
- Users can still access and launch deployed managed apps, if an available node can handle the number of users. Connections might be slower, resulting in slower device check-ins.
- Device policies continue to work unless all nodes are down. Depending on resources and number of devices, policies might deploy more slowly.

[12] Advanced Settings



SSL protocols options default to all allowed protocols. After the prompt **New SSL protocols to enable**, type the protocols you want to enable. XenMobile disables any protocols that you don't include in your response. For example: To disable TLSv1, type `TLSv1.2,TLSv1.1` and then type **y** to restart XenMobile Server.

Server Tuning options include the server connection timeout, maximum connections (by port), and maximum threads (by port).

Switch JDBC driver options are **jTDS** and **Microsoft** JDBC. The default driver is jTDS. For information about switching to the Microsoft JDBC driver, see SQL Server drivers.

Troubleshooting options

Following are samples of the **Troubleshooting Menu** and the settings displayed for each option.


```
-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
-----------------------------------
Choice: [0 - 4] 4
```

[1] Network Utilities

```
---------------------------------
Network Menu
---------------------------------
[0] Back to Troubleshooting Menu
[1] Network Information
[2] Show Routing Table
[3] Show Address Resolution Protocol (ARP) Table
[4] PING
[5] Traceroute
[6] DNS Lookup
[7] Network Trace
---------------------------------
```

[2] Logs

```
---------------------------------
Logs Menu
---------------------------------
[0] Back to Troubleshooting Menu
[1] Display Log File
---------------------------------
```

[3] Support Bundle

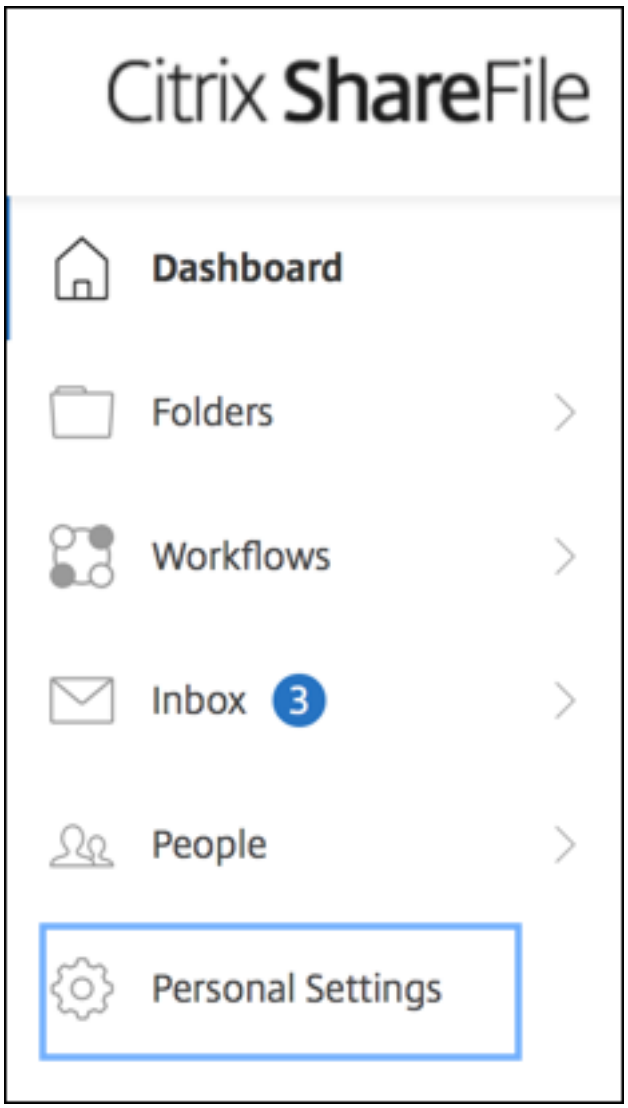
```
---------------------------------
Support Bundle Menu
---------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
---------------------------------
```

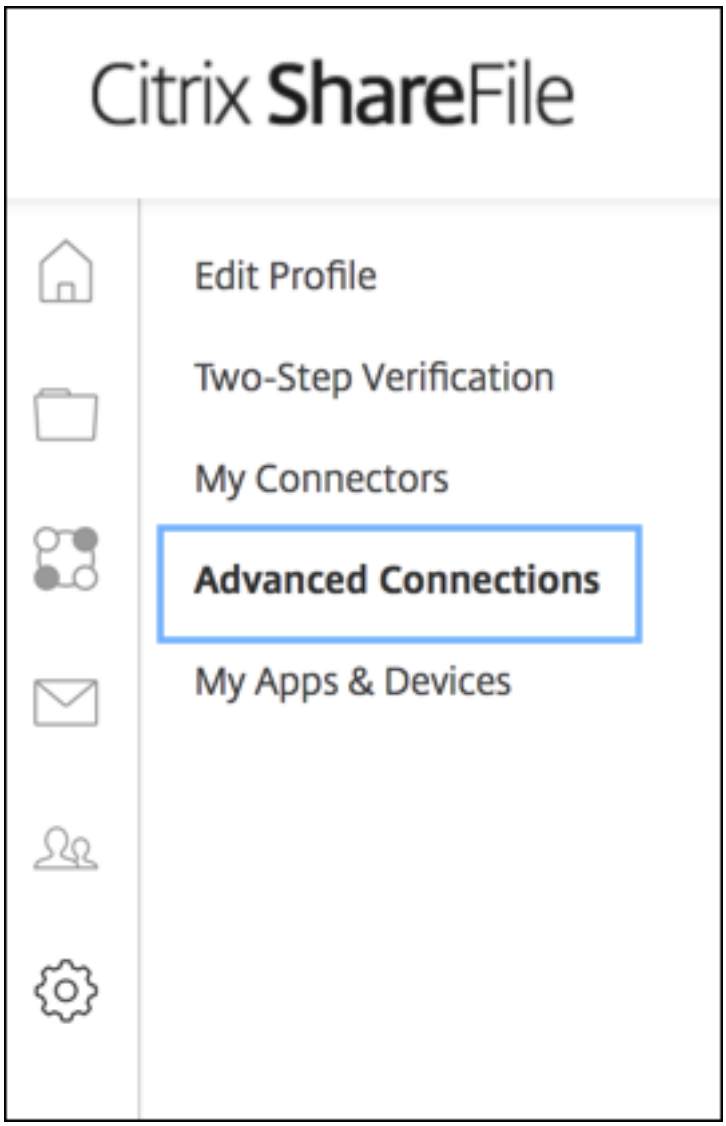

[4] Disk Usage

To upload a support bundle by using Citrix Files as the FTP site

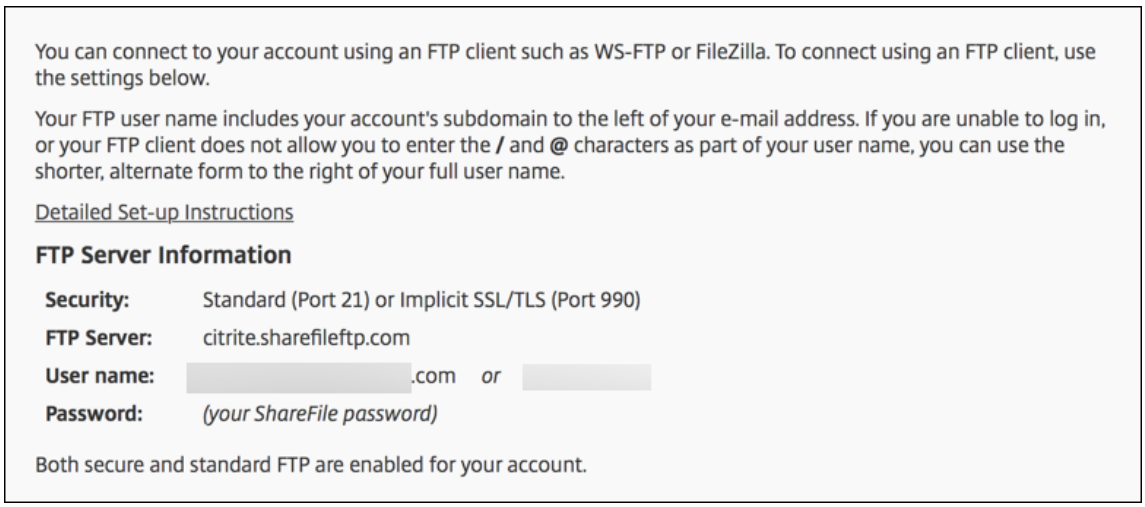
Before you initiate the upload of a support bundle, configure the following prerequisites on Citrix Files:

1. Verify the FTP logon details.
   a. In a web browser, open https://citrix.sharefile.com.
   b. Click **Personal Settings** and then click **Advanced connections**.





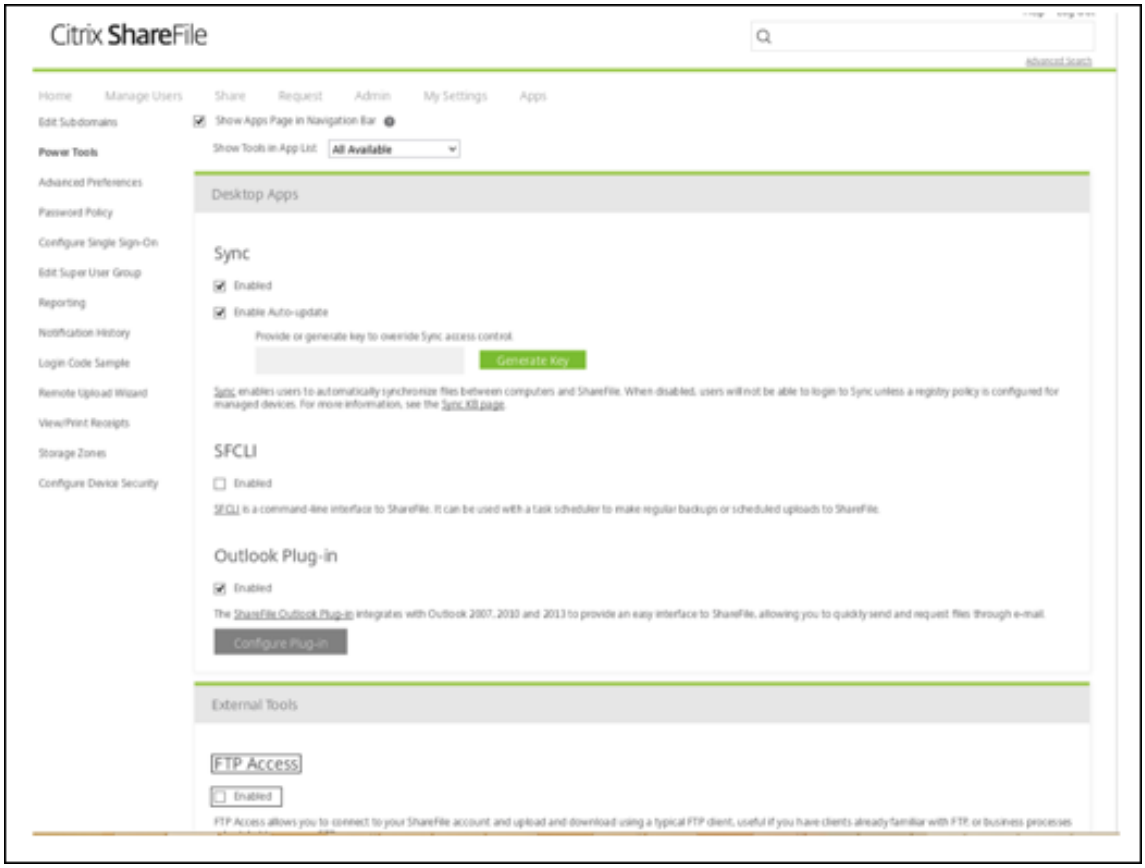
c. In FTP Server information, for User name, verify that an alphanumeric user ID appears, along with the default Subdomain/username details.



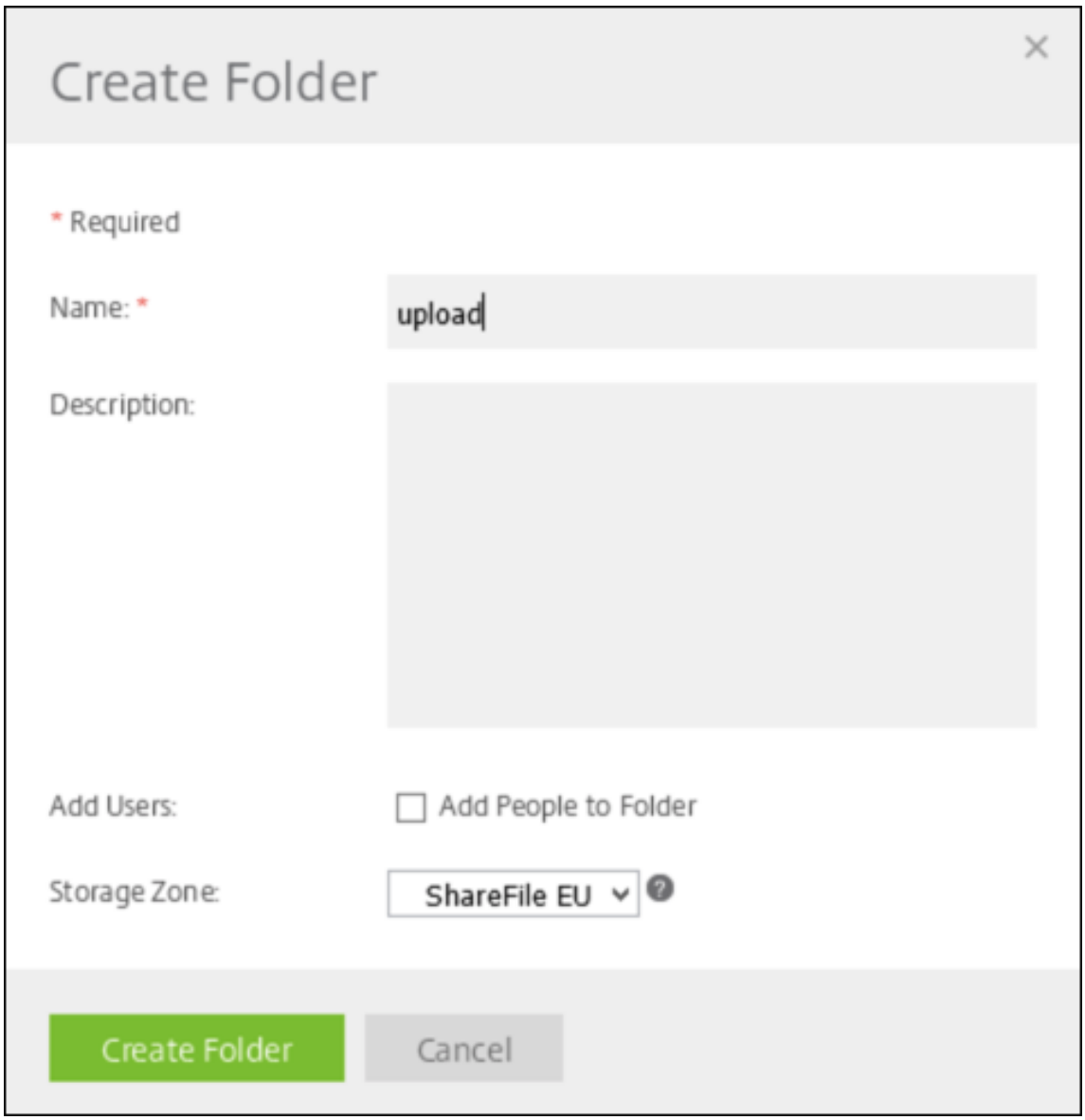
> **Notes:**
>
> - The file you are uploading from XenMobile is a Linux CLI-based FTP client. As a result, you cannot enter backslash () and at sign (@) characters as part of your user name.
> - If you don't see the alphanumeric user ID, you can request this user ID from your Content Collaboration admin or Content Collaboration support.

2. Verify that the Citrix Files server is enabled for FTP communication along with FTPS. Ideally, Content Collaboration admins allow a user account to be opened for FTP communication. Sometimes, however, only FTPS communication is allowed.

   A user with administrator rights can verify and enable this setting by clicking **Settings**, **Admin Settings**, **Advanced Preferences** and then **Enable ShareFile Tools.** In **External Apps**, **FTP Access**, verify that the **Enable** check box is selected.



3. Create a shared folder for the FTP client to use as a directory for file uploads. Click **Home**, click **Folders**, and then click **Personal Folders**.
4. On the far right, click the plus sign (+) icon, click **Create Folder** and then enter a name for the folder.



5. In the XenMobile Server CLI, on the **Main Menu**, select **Troubleshooting > Support Bundle**. Then, on the **Support Bundle Menu**, select **Generate Support Bundle**.

> **Note:**
>
> If a support bundle exists, when prompted, type **y** to override the bundle.

6. Upload the support bundle to the FTP server:

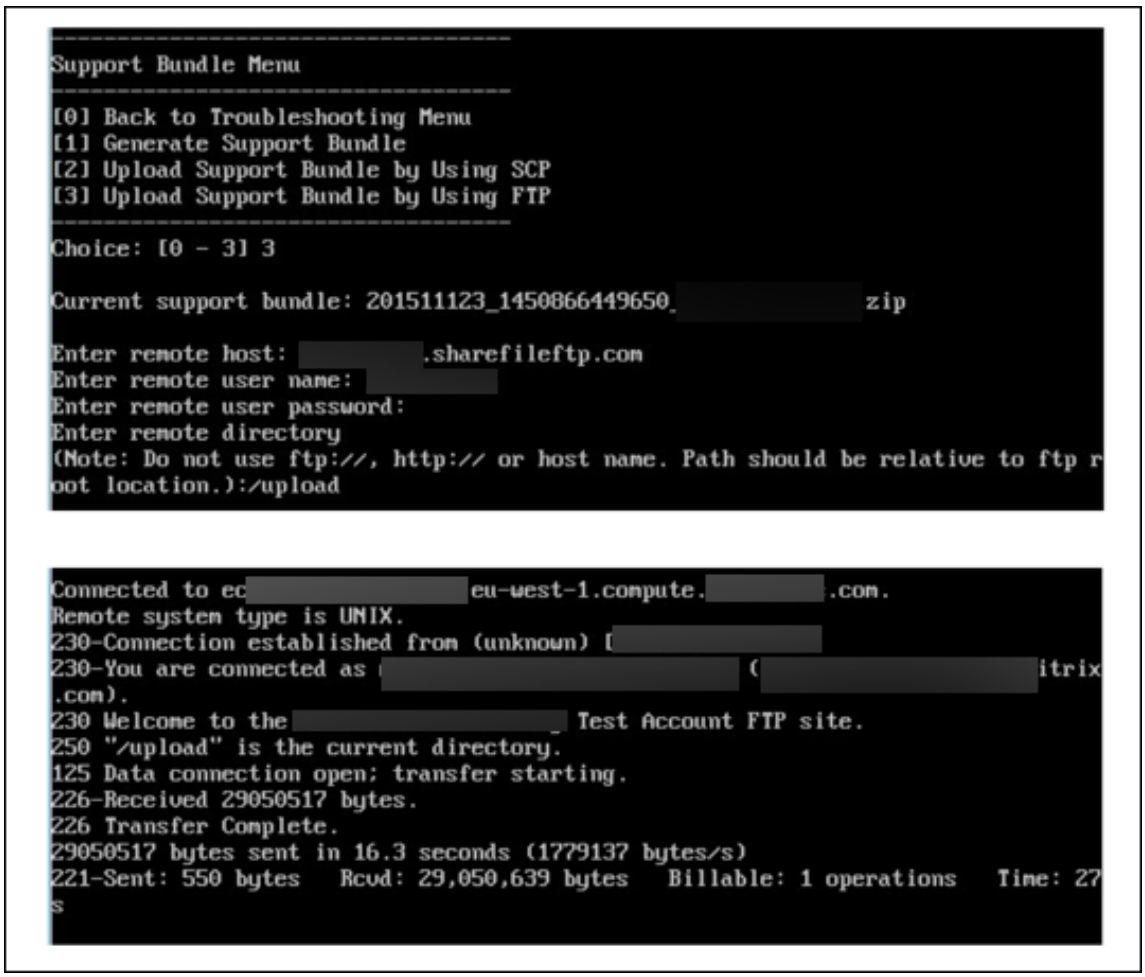
   a. Select **Upload Support Bundle by using FTP**.

   b. **Enter remote host:** When prompted, type your FTP server name. When Citrix Files is used as FTP server, type your company name followed by Citrix Files FTP site name. For example citrix.sharefileftp.com.

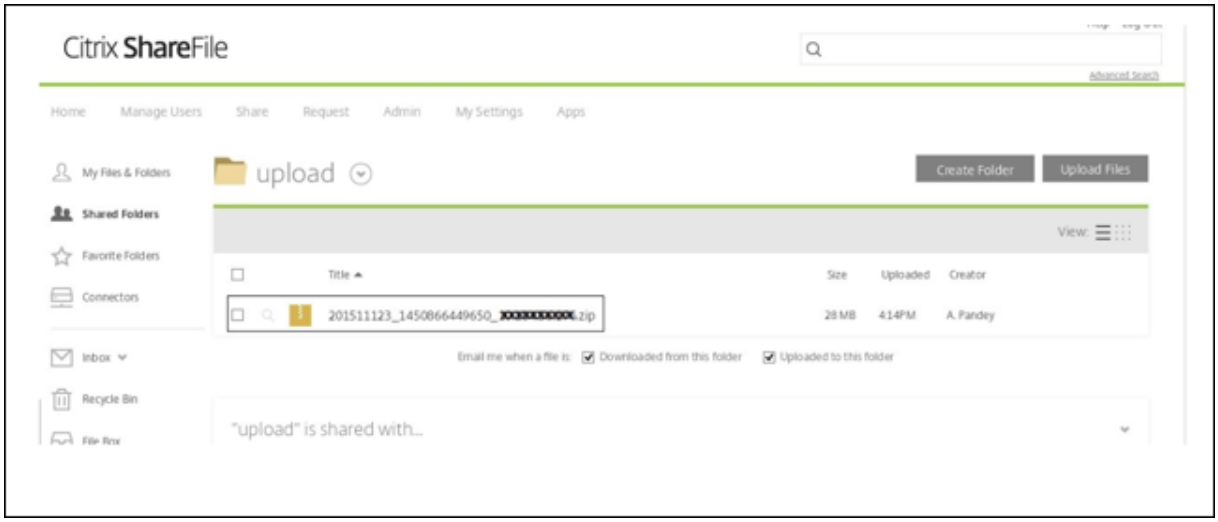
c. **Enter remote user name:** When prompted, type the alphanumeric user ID.

d. **Enter remote user password:** When prompted, enter your password.

e. **Enter remote directory:** When prompted, enter the shared folder name you created in Citrix Files and then press **Enter**.



You can view the uploaded support bundle in the shared folder you created in Citrix Files.



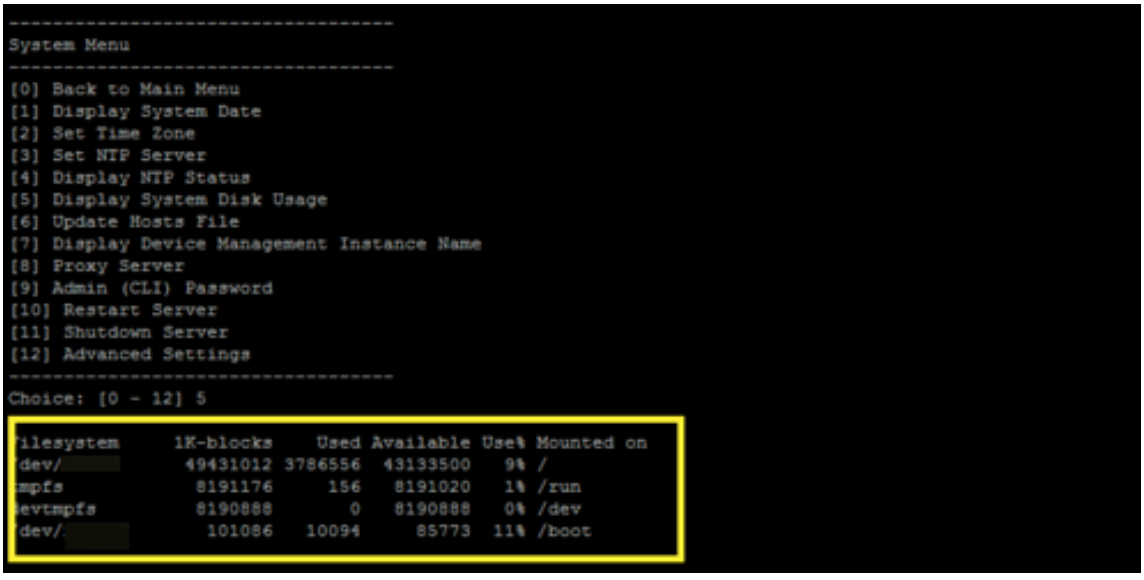
For more information about Citrix Files FTP, see this Citrix Support Knowledge Center article.

To check the disk space

You can check the system disk space in the CLI as follows:

1. On the main menu, select the **System** menu.
2. In the **System** menu, select the **Display System Disk Usage** option.

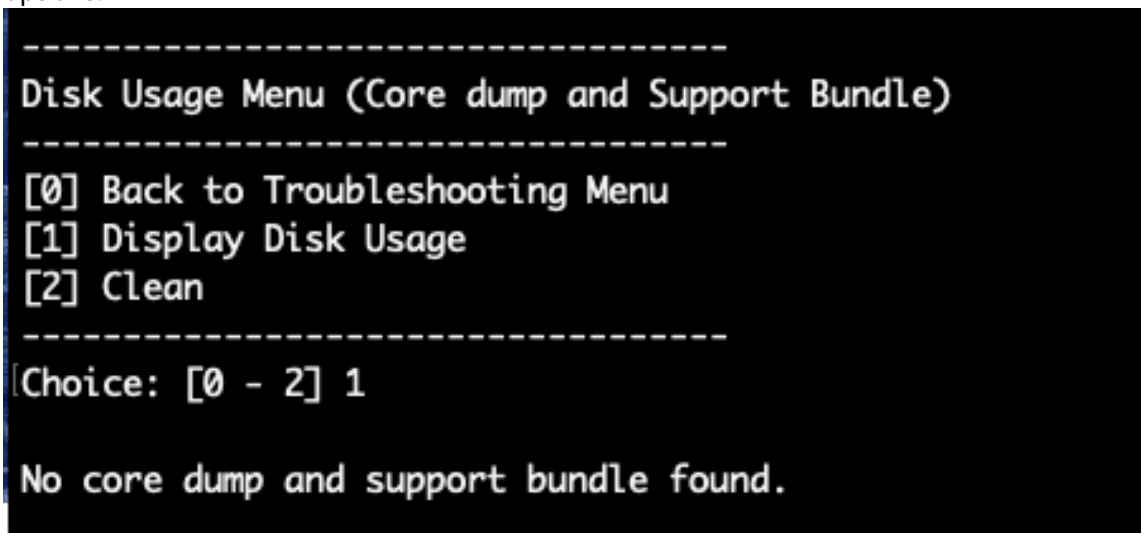
   The file system information appears.



To perform self-service disk cleanup

You can clean up the disk in the CLI as follows:

1. On the **Troubleshooting Menu**, select **Disk Usage**. The **Disk Usage Menu** has the following options:



2. Type 1 to list the core dump file and support bundles file types. If there no files exist, you get the following message: **No core dump and support bundles found.**
3. Type 2 to clean the scanned core dump file and support bundle file.

Getting started workflows for XenMobile console

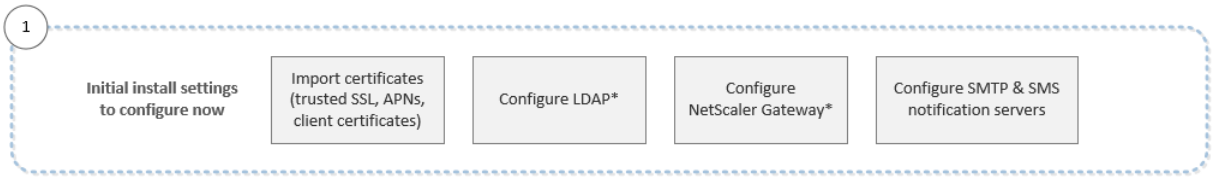
June 23, 2021

The XenMobile console is the unified management tool in XenMobile. This article assumes you've installed XenMobile and are ready to work in the console. If you have yet to install XenMobile, see Installing XenMobile. For details on browser support for the XenMobile console, the XenMobile Compatibility article.

Initial settings workflow

After you finish configuring XenMobile first in the command-line console and next in the XenMobile console, the dashboard opens. You cannot return to the initial configuration screens. If you skipped some install configurations, you can configure the following settings in the console. Before you start adding users, apps, and devices, you consider completing these install settings. To start, click the gear icon in the upper-right corner of the console.

> **Note:**
>
> The items with an asterisk are optional.



For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and sections:

- Authentication
- Citrix Gateway and XenMobile
- Notifications

To support Android, iOS, and Windows platforms, you must have the following account-related setup.

Android

- Create Google Play credentials. For details, see Google Play Launch.
- Create an Android Enterprise administrator account. For details, see Android Enterprise.
- Verify your domain name with Google. For details, see Verify your domain for Google Workspace.
- Enable APIs and create a service account for Android Enterprise. For details, see Android enterprise Help.

iOS

- Create an Apple ID and developer account. For details, see the Apple Developer Program website.
- Create an Apple Push Notification Service (APNs) certificate. If you plan to manage iOS devices with your XenMobile Server deployment, you need an Apple APNs certificate. If you use push notification for your Secure Mail deployment, you also need an Apple APNs certificate. For details about obtaining Apple APNs certificates, see the Apple Push Certificates Portal. For more information about XenMobile and APNs, see APNs certificates and Push Notifications for Secure Mail for iOS.
- Create a volume purchase company token. For details, see Apple Volume Purchasing Program.

Windows

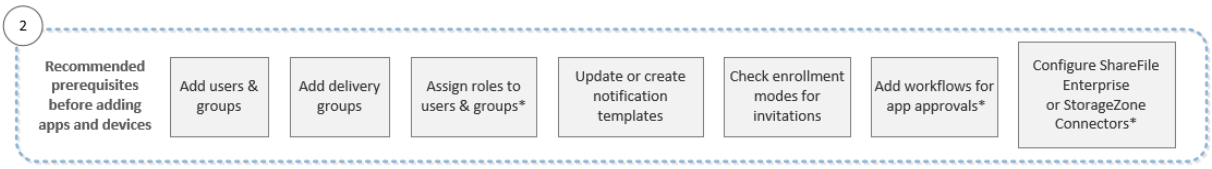
- Create a Microsoft Windows Store developer account. For details, see Account types, locations, and fees.
- Obtain a Microsoft Windows Store Publisher ID. For details, see Manage account settings and profile info.

- Acquire an enterprise certificate from DigiCert. For details, see Company app distribution for Windows Phone.
- Ensure that you have a public SSL certificate available if you plan to use XenMobile autodiscovery for your Windows Phone enrollment. For details, see XenMobile AutoDiscovery Service.
- Create an Application Enrollment Token (AET). For details, see How to generate an application enrollment token for Windows Phone.

Console prerequisites workflow

This workflow shows prerequisites for you to configure before you add apps and devices.

> **Note:**
>
> The items with an asterisk are optional.



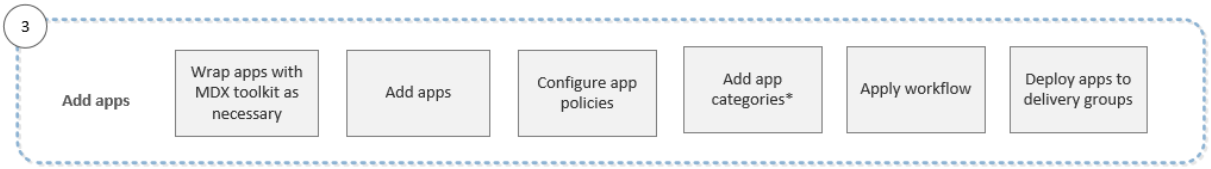
For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and sections:

- User accounts, roles, and enrollment
- Deploy resources
- Configure roles with RBAC
- Notifications
- Apply workflows
- Use Citrix Content Collaboration with XenMobile

Add apps workflow

This workflow shows a recommended order to follow when adding apps to XenMobile.

> **Note:**
>
> The items with an asterisk are optional.



For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and sections:

- About the MDX Toolkit
- Add apps
- MDX Policies at a Glance
- Apply workflows
- Deploy resources

Add devices workflow

This workflow shows a recommended order to follow when adding and registering devices in XenMobile.

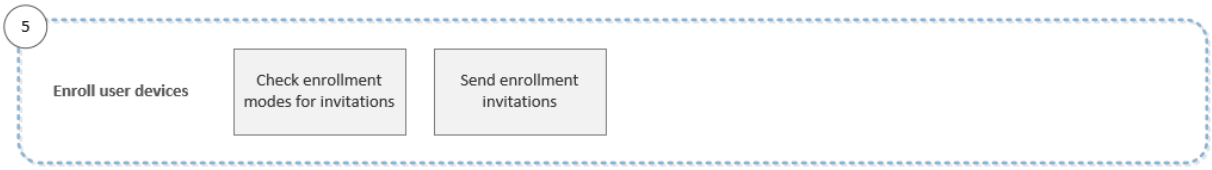
> **Note:**
>
> The items with an asterisk are optional.

For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles and sections:

- Devices
- Supported device operating systems
- Deploy resources
- Monitor and support
- Automated actions

Enroll user devices workflow

This workflow shows a recommended order to follow when enrolling user devices in XenMobile.



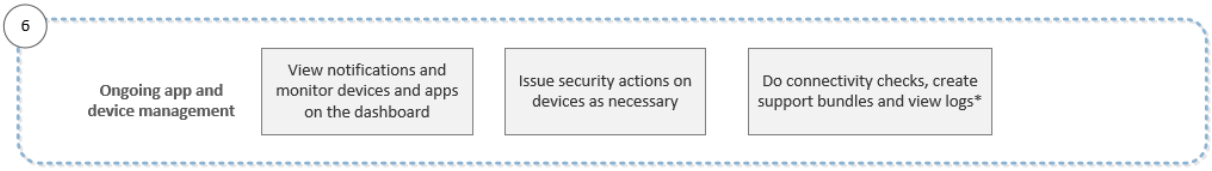
For more information about each setting, along with step-by-step procedures, see the following Citrix Product Documentation articles:

- User accounts, roles, and enrollment
- Notifications

Ongoing app and device management workflow

This workflow shows app and device management activities that you can do in the console.

> **Note:**
>
> The items with an asterisk are optional.



For more information about the support options found from clicking the wrench icon in the upper-right corner of the console, see Monitor and support.

Certificates and authentication

February 9, 2021

Several components play a role in authentication during XenMobile operations:

- **XenMobile Server:** The XenMobile 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. Through client properties in XenMobile, you can enable Citrix PIN authentication and configure the complexity and expiration time of the PIN.
- **Citrix ADC:** Citrix ADC provides termination for micro VPN SSL sessions. Citrix ADC 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 XenMobile Server work together in enrollment operations. Secure Hub is the entity on a device that talks to the Citrix ADC: When a session expires, Secure Hub gets an authentication ticket from Citrix ADC 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 the Citrix ADC 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 the Citrix ADC, enforce offline mode restrictions, and enforce client policies, such as time-outs.

For more information about configuring authentication, including an overview of single-factor and two-factor authentication methods, see the Deployment Handbook article, Authentication.

You use certificates in XenMobile to create secure connections and authenticate users. The remainder of this article discusses certificates. For other configuration details, see the following articles:

- Domain or domain plus security token authentication
- Client certificate or certificate plus domain authentication
- PKI entities
- Credential providers
- APNs certificates
- SAML for single sign-on with Citrix Files
- Microsoft Azure Active Directory server settings
- To send a certificate to devices to authenticate to the Wi-Fi server: Wi-Fi 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

Certificates

XenMobile generates a self-signed Secure Sockets Layer (SSL) certificate during installation to secure the communication flows to the server. You must replace the SSL certificate with a trusted SSL certificate from a well-known CA.

XenMobile 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 XenMobile-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 XenMobile, 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 XenMobile component:

XenMobile component	Certificate format	Required certificate type
Citrix Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Root (Citrix Gateway converts PFX to PEM automatically.)
XenMobile Server	.p12 (.pfx on Windows-based computers)	SSL, SAML, APNs (XenMobile also generates a full PKI during the installation process.) Important: XenMobile Server 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 the XenMobile Server.
StoreFront	PFX (PKCS #12)	SSL, Root

XenMobile supports SSL listener certificates and client certificates with bit lengths of 4096, 2048, and 1024. 1024-bit certificates are easily compromised.

For Citrix Gateway and the XenMobile Server, 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 XenMobile 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 XenMobile.

> **Important: Requirements for trusted certificates in iOS, iPadOS, and macOS**
>
> 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.
>
> 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.

Uploading certificates in XenMobile

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, you choose a server certificate that satisfies the context-dependent criteria. For example, you might want to configure XenMo-

bile to integrate with your Microsoft certification authority (CA). The connection to the Microsoft CA must be authenticated by using a client certificate.

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.

Private key requirements

XenMobile may or may not possess the private key for a given certificate. Likewise, XenMobile may or may not require a private key for uploaded certificates.

Uploading certificates

You have two options for uploading certificates:

- Upload the certificates to the console individually.
- Perform a bulk upload of certificates to iOS devices with the REST API.

When uploading certificates to the console, you have two main options:

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

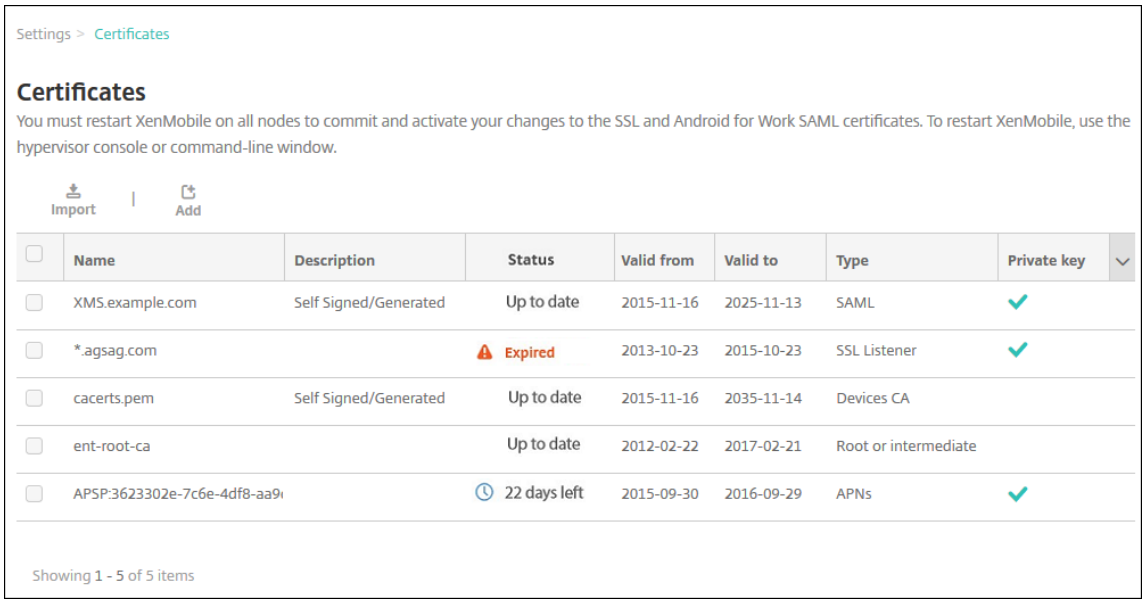
When configuring the Microsoft CA entity, you specify the CA certificate. You select the CA certificate from a list of all server certificates that are CA certificates. Likewise, when configuring client authentication, you can select from a list of all the server certificates for which XenMobile has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

To import a keystore

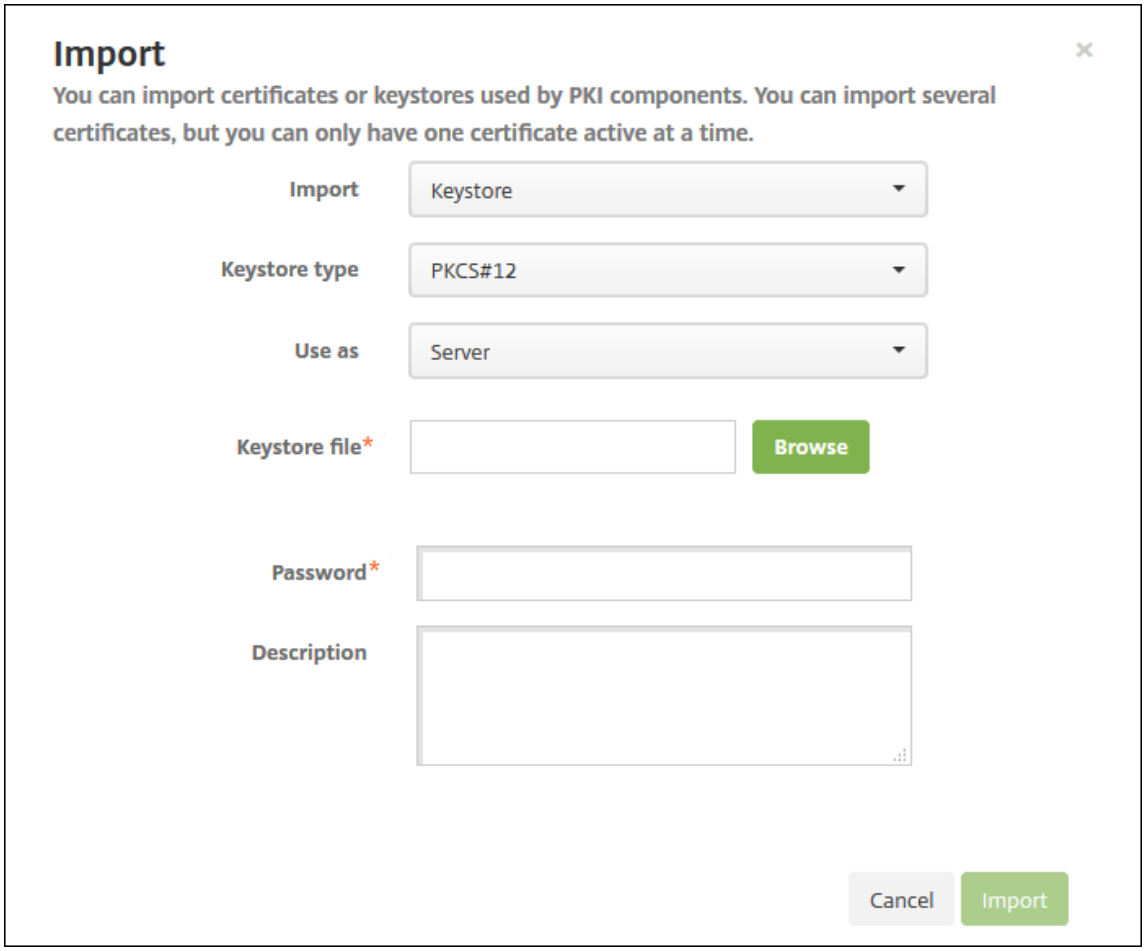
By design, keystores, which are repositories of security certificates, can contain multiple entries. When loading from a keystore, therefore, you are prompted to specify the entry alias that identifies the entry you want to load. If you do not specify an alias, the first entry from the store is loaded. Because PKCS #12 files usually contain only one entry, the alias field does not appear when you select PKCS #12 as the keystore type.

1. In the XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.

2. Click **Certificates**. The **Certificates** page appears.



3. Click **Import**. The **Import** dialog box appears.
4. Configure these settings:
   - **Import:** In the list, click **Keystore**. The **Import** dialog box changes to reflect available keystore options.



- **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 the XenMobile Server that are uploaded to the XenMobile web console. They 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 XenMobile of SSL cryptographic activity.
- **Keystore file:** Browse to find the keystore you want to import of the file type .p12 (or .pfx on Windows-based computers).
- **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.

5. Click **Import**. The keystore is added to the Certificates table.

To import a certificate

When importing a certificate, either from a file or a keystore entry, XenMobile attempts to construct a certificate chain from the input. XenMobile imports all certificates in that chain to create a server certificate entry for each. This operation only works if the certificates in the file or keystore entry do form a chain. For example, if each subsequent certificate in the chain is 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 XenMobile console, click the gear icon in the upper-right corner of the console and then click **Certificates**.
2. On the **Certificates** page, click **Import**. The **Import** dialog box appears.
3. In the **Import** dialog box, in **Import**, if it is not already selected, click **Certificate**.
4. The **Import** dialog box changes to reflect available certificate options. In **Use as**, select how you plan to use the keystore. The available options are:
   - **Server**. Server certificates are certificates used functionally by the XenMobile Server that are uploaded to the XenMobile web console. They 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 XenMobile of SSL cryptographic activity.
5. Browse to find the keystore you want to import of the file type .p12 (or .pfx on Windows-based computers).
6. Browse to find an optional private key file for the certificate. The private key is used for encryption and decryption along with the certificate.
7. Type a description for the certificate, optionally, to help you identify it from your other certificates.
8. Click **Import**. The certificate is added to the Certificates table.

Upload certificates to iOS devices in bulk with the REST API

If uploading certificates one at a time isn't practical, you can bulk upload them to iOS devices with 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 tha 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:

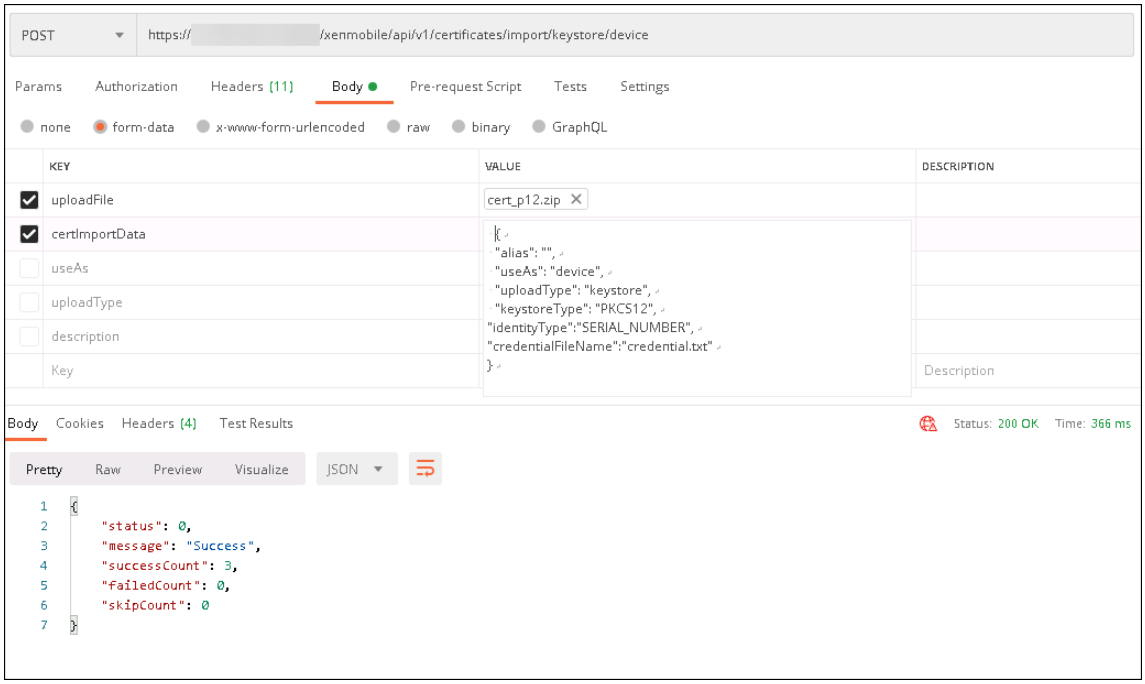
   ```
   A12BC3D4EFGH.p12=password1!
   A12BC3D4EFIJ.p12=password2@
   A12BC3D4EFKL.p12=password3#
   <!--NeedCopy-->
   ```

3. Pack all the certificates and the text file you created into a .zip file.

4. Launch your REST API client, log in to XenMobile, and get an authentication token.

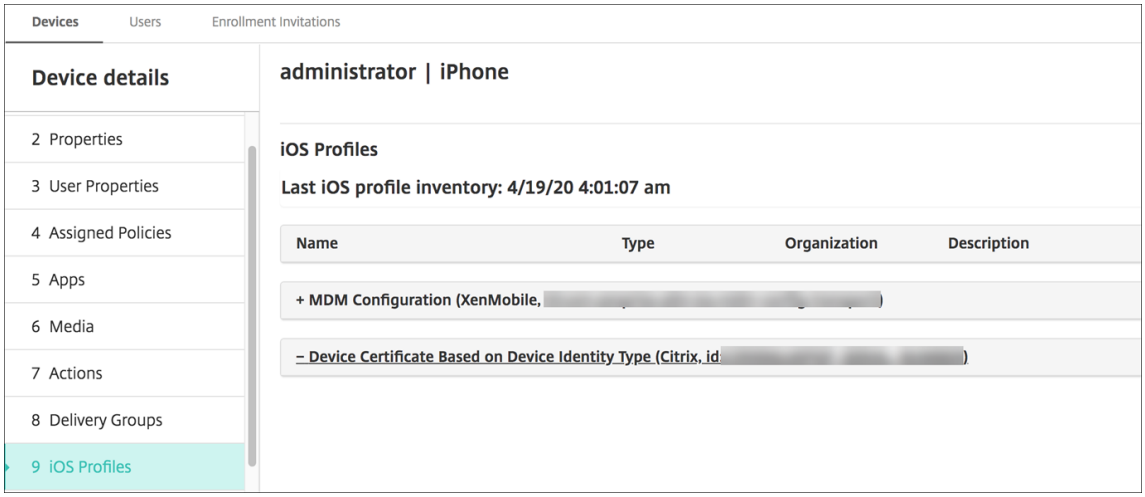
5. Import your certificates, ensuring you put the following in the message body:

   ```
   {

       "alias": "",
       "useAs": "device",
       "uploadType": "keystore",
       "keystoreType": "PKCS12",
       "identityType":"SERIAL_NUMBER",        # identity type can be
          "SERIAL_NUMBER","IMEI","MEID"
       "credentialFileName":"credential.txt"   # The credential file
          name in .zip
    }

   <!--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 XenMobile console.

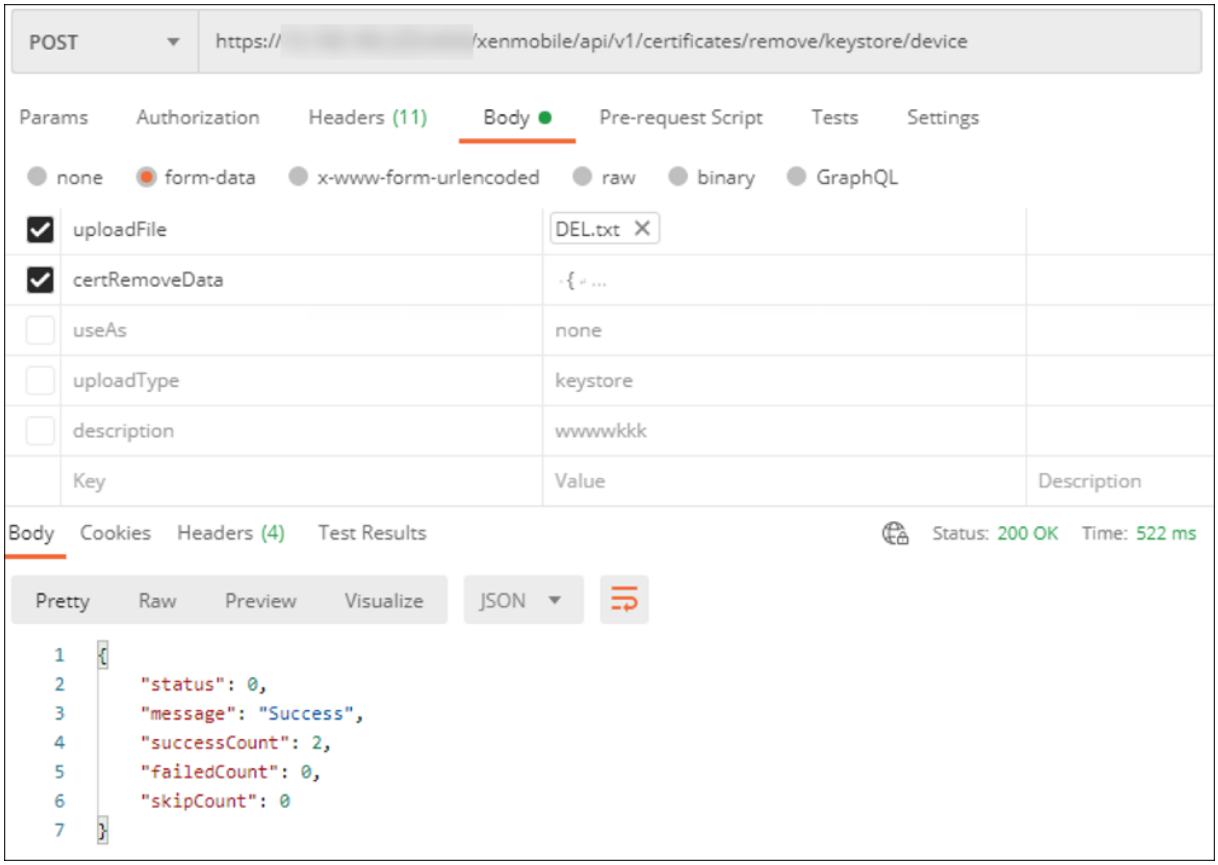


You can also delete certificates in bulk by creating a text file with the `device_identity_value` listed for each certificate to delete. In the REST API, call the delete API and use the following request, replacing `device_identity_value` with the appropriate identifier:

```
```
{

    "identityType"="device_identity_value"
 }

<!--NeedCopy--> ```
```

 
```



Updating a certificate

XenMobile 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 either replace the existing entry or delete the entry.

To most effectively update your certificates, in the XenMobile console, do the following. Click the gear icon on the upper-right corner of the console to open the **Settings** page and then click **Certificates**. In the **Import** dialog box, import the new certificate.

When you update a server certificate, components that were 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.

Renewing a certificate

XenMobile Server uses the following certificate authorities internally for PKI: Root CA, device CA, and server CA. Those CAs are classified as a logical group and provided a group name. When a new XenMobile Server instance is provisioned, the three CAs are generated and given the group name “default”.

You can renew the CAs for supported iOS, macOS, and Android devices by using the XenMobile Server console or the public REST API. For enrolled Windows devices, users must re-enroll their devices to receive a new device CA.

The following APIs are available for renewing or regenerating the internal PKI CAs in XenMobile Server and renewing the device certificates issued by these certificate authorities.

- Create group certificate authorities (CAs).
- Activate new CAs and deactivate old CAs.
- Renew the device certificate on a configured list of devices. Already enrolled devices continue to work without disruption. A device certificate is issued when a device connects back to the server.
- Return a list of devices still using the old CA.
- Delete the old CA after all devices have the new CA.

For information, see the following sections in the Public API for REST Services PDF:

- Section 3.16.58, Renew Device Certificate
- Section 3.23, Internal PKI CA Groups

The **Manage Devices** console includes the security action, **Certificate Renewal**, used to renew the enrollment certificate on a device.

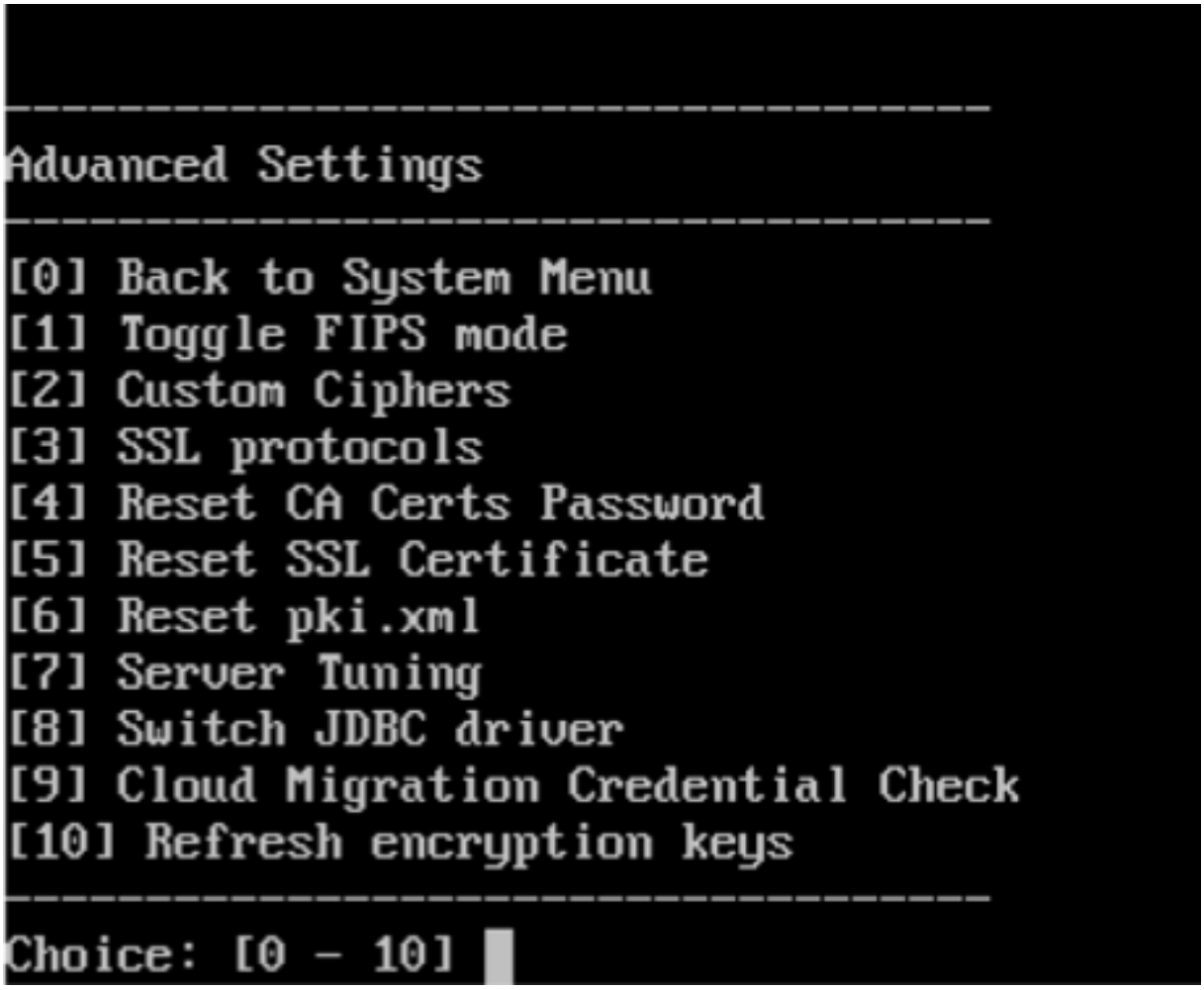
Prerequisites

- By default, this certificate refresh feature is disabled. To activate the certificate refresh features, set the value for the server property **refresh.internal.ca** to **True**.

> **Important:**
>
> If your Citrix ADC is set up for SSL Offload, when you generate a new certificate, ensure that you update your load balancer with the new cacert.perm. For more information on Citrix Gateway setup, see To use SSL Offload mode for Citrix ADC VIPs.

CLI option to reset the server CA certificate password for cluster nodes

After you generate a server CA certificate on one XenMobile Server node, use the XenMobile CLI to reset the certificate password on other cluster nodes. From the CLI Main menu, choose **System > Advanced Settings > Reset CA certs password**. If you reset the password when there is no new CA certificate, XenMobile doesn't reset the password.



XenMobile Certificate Administration

We recommend that you list the certificates you use in your XenMobile deployment, especially on their expiration dates and associated passwords. This section intends to help you make certificate administration in XenMobile easier.

Your environment may include some or all of the following certificates:

- XenMobile Server
  - SSL Certificate for MDM FQDN
  - SAML Certificate (For Citrix Files)
  - Root and Intermediate CA Certificates for the preceding certificates and any other internal resources (StoreFront/Proxy, and so on)
  - APN Certificate for iOS Device Management
  - Internal APNs Certificate for XenMobile Server Secure Hub Notifications
  - PKI User Certificate for connectivity to PKI

- 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 ADC
  - 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 & Intermediate CA Certificates for the preceding certificates

XenMobile Certificate Expiration Policy

If you allow a certificate to expire, the certificate becomes invalid. You can no longer run secure transactions on your environment and you cannot access XenMobile resources.

> **Note:**
>
> The Certification Authority (CA) prompts you to renew your SSL certificate before the expiration date.

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 XenMobile, set up and create an APNs certificate from Apple. If the certificate expires, users cannot enroll in XenMobile 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:

```
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.

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.

Thank You,

Apple Push Notification Service
<!--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 the MDX Toolkit. 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 XenMobile Server certificates are valid, do the following:

1. In the XenMobile 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 cannot install an app published and signed by the company, or start a company app that was installed on the phone.

Citrix ADC

For details on how to handle certificate expiration for Citrix ADC, see How to handle certificate expiry on NetScaler in the Citrix Support Knowledge Center.

An expired Citrix ADC 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 ADC certificates. The Center notifies you when the certificate expires. These tools assist to monitor the following Citrix ADC 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 XenMobile

September 3, 2020

When you configure Citrix Gateway using XenMobile, you establish the authentication mechanism for remote device access to the internal network. This functionality enables apps on a mobile device to access corporate servers located in the intranet. XenMobile creates a micro VPN from the apps on the device to Citrix Gateway.

You configure Citrix Gateway for use with XenMobile by exporting a script from XenMobile that you run on Citrix Gateway.

Prerequisites for using the Citrix Gateway configuration script

Citrix ADC requirements:

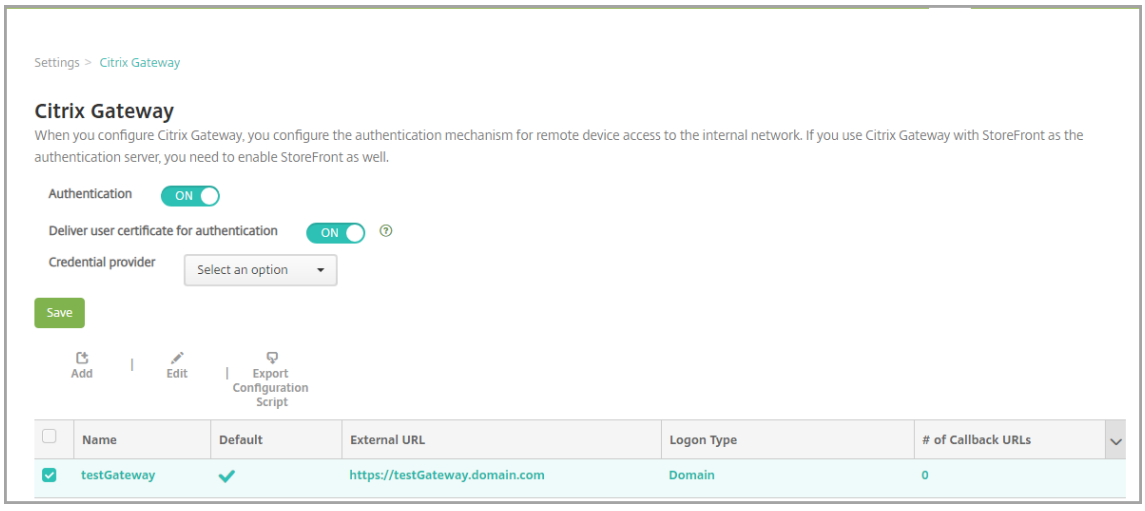
- Citrix ADC (minimum version 11.0, Build 70.12).
- Citrix ADC IP address is configured and has connectivity to the LDAP server, unless LDAP is load balanced.
- Citrix ADC Subnet (SNIP) IP address is configured, has connectivity to the necessary back end servers, and has public network access over port 8443/TCP.
- DNS can resolve public domains.
- Citrix ADC is licensed with Platform/Universal or Trial licenses. For information, see https://support.citrix.com/article/CTX126049.
- A Citrix Gateway SSL certificate is uploaded and installed on the Citrix ADC. For information see, https://support.citrix.com/article/CTX136023.

XenMobile requirements:

- XenMobile Server (minimum version 10.6).
- LDAP server is configured.

Configure authentication for remote device access to the internal network

1. In the XenMobile 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.



3. Configure these settings:
   - **Authentication:** Select whether to enable authentication. The default is **ON**.

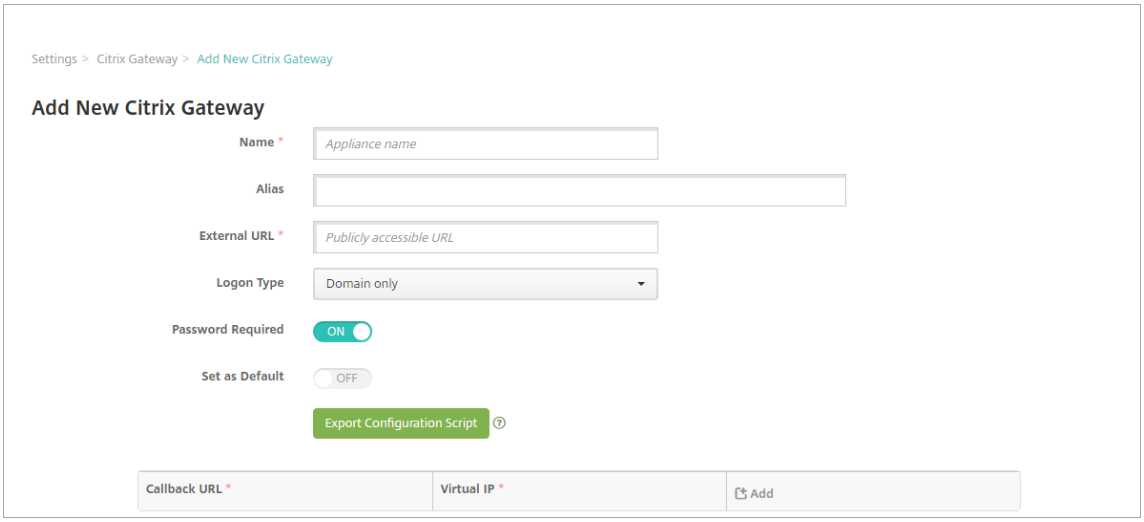
- **Deliver user certificate for authentication:** Select whether you want XenMobile to share the authentication certificate with Secure Hub, to enable the Citrix Gateway to handle client certificate authentication. The default is **OFF**.
- **Credential Provider:** In the list, click the credential provider to use. For more information, see Credential Providers.

4. Click **Save**.

Add a Citrix Gateway instance

After you save the authentication settings, you add a Citrix Gateway instance to XenMobile.

1. In the XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page opens.
2. Under **Server**, click **Citrix Gateway**. The **Citrix Gateway** page appears.
3. Click **Add**. The **Add New Citrix Gateway** page appears.



4. Configure these settings:

- **Name:** Type a name for the Citrix Gateway instance.
- **Alias:** Optionally include an alias name for the Citrix Gateway.
- **External URL:** Type the publicly accessible URL for Citrix Gateway. For example, `https://receiver.com`.
- **Logon Type:** Choose a logon type. Types include **Domain only**, **Security token only**, **Domain and security token**, **Certificate**, **Certificate and domain**, and **Certificate and security token**. The default setting for the **Password Required** field changes based on the **Logon Type** you select. The default is **Domain only**.

If you have multiple domains, use **Certificate and domain**. For more information about configuring multiple-domain authentication with XenMobile and Citrix Gateway, see Configure au-

thentication for multiple domains.

If you use **Certificate and security token**, some additional configuration is required on Citrix Gateway to support Secure Hub. For information, see Configuring XenMobile for Certificate and Security Token Authentication.

For more information, see Authentication in the Deployment Handbook.

- **Password Required:** Select whether you want to require password authentication. The default varies based on the **Logon Type** chosen.
- **Set as Default:** Select whether to use this Citrix Gateway as the default. The default is **OFF.**
- **Export Configuration Script:** Click the button to export a configuration bundle that you upload to Citrix Gateway to configure it with XenMobile settings. For information, see "Configure an on-premises Citrix Gateway for use with XenMobile Server" after these steps.
- **Callback URL** and **Virtual IP:** Save your settings before adding these fields. For information, see Add a callback URL and Citrix Gateway VPN virtual IP in this article.

5. Click **Save**.

   The new Citrix Gateway is added and appears in the table. To edit or delete an instance, click the name in the list.

Configure Citrix Gateway for use with XenMobile Server

To configure an on-premises Citrix Gateway for use with XenMobile, you perform the following general steps, detailed in this article:

1. Download a script and related files from XenMobile Server. See the readme file provided with the script for the latest detailed instructions.
2. Verify that your environment meets the prerequisites.
3. Update the script for your environment.
4. Run the script on Citrix ADC.
5. Test the configuration.

The script configures these Citrix Gateway settings required by XenMobile:

- Citrix Gateway virtual servers needed for MDM and MAM
- Session policies for the Citrix Gateway virtual servers
- XenMobile Server details
- Authentication Policies and Actions for the Citrix Gateway virtual server.
  The script describes the LDAP configuration settings.
- Traffic actions and policies for the proxy server

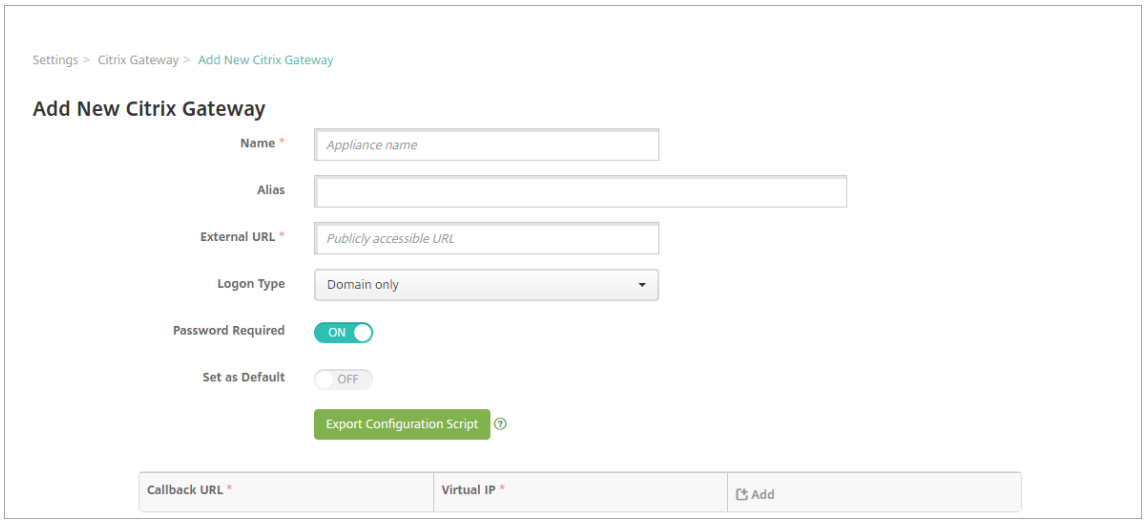
- Clientless access profile
- Static local DNS record on Citrix ADC
- Other bindings: Service policy, CA certificate

The script doesn't handle the following configuration:

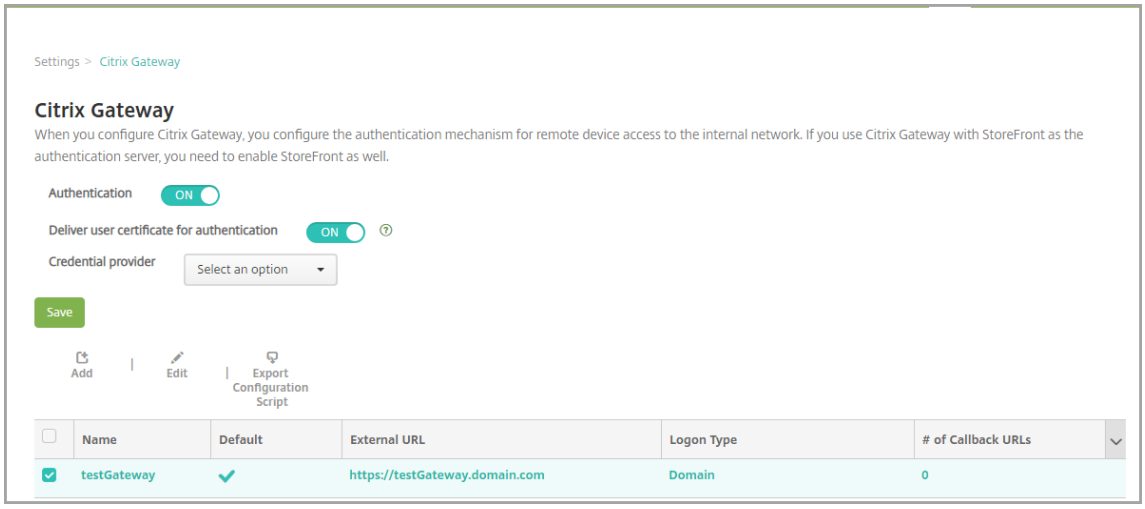
- Exchange load balancing
- Citrix Files load balancing
- ICA Proxy configuration
- SSL Offload

To download, update, and run the script

1. If you're adding a Citrix Gateway, click **Export Configuration Script** on the **Add New Citrix Gateway** page.



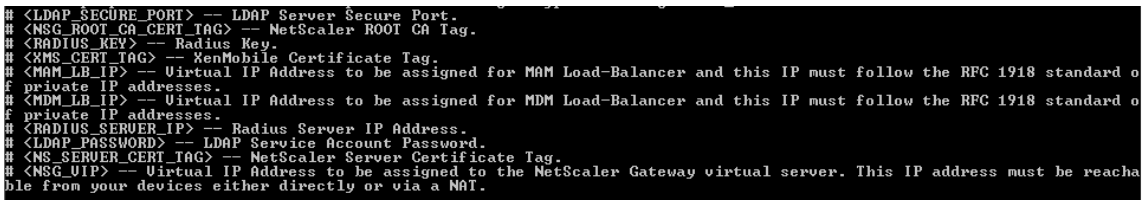
   Or, if you add a Citrix Gateway instance and click **Save** before you export the script: Return to **Settings > Citrix Gateway**, select the Citrix ADC, click **Export Configuration Script**, and then click **Download**.



After you click **Export Configuration Script**, XenMobile creates a .tar.gz script bundle. The script bundle includes:

- Readme file with detailed instructions
- Script that contains the Citrix ADC CLI commands used to configure the required components in Citrix ADC
- Public Root CA certificate and the Intermediate CA certificate of XenMobile Server (these certificates, for SSL offload, are not needed for the current release)
- Script that contains the Citrix ADC CLI commands used to remove the Citrix ADC configuration

2. Edit the script (NSGConfigBundle_CREATESCRIPT.txt) to replace all placeholders with details from your environment.



3. Run your edited script in the Citrix ADC 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/NSGConfigBundle_CREATESCRIPT.txt"
```



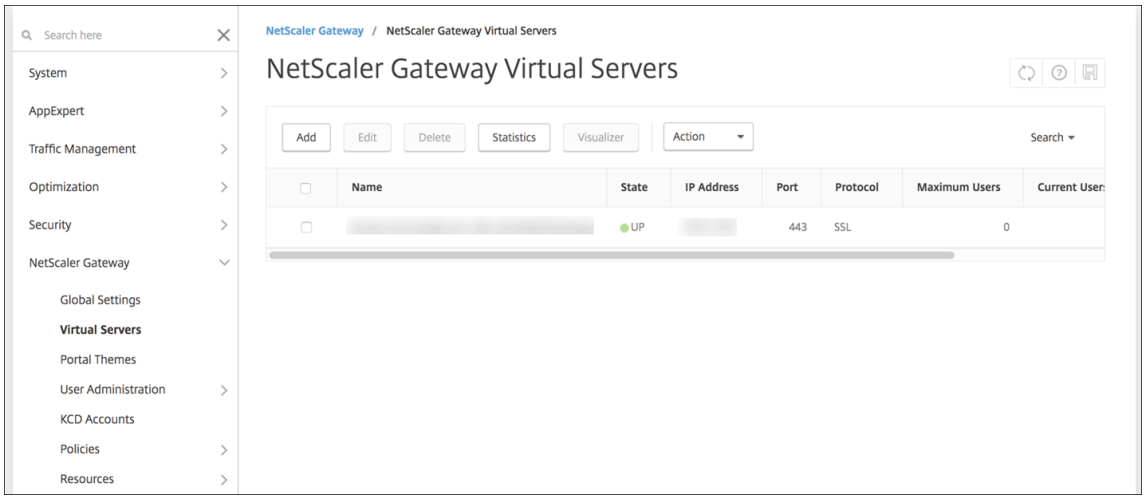
```
login as: nsroot
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you 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.

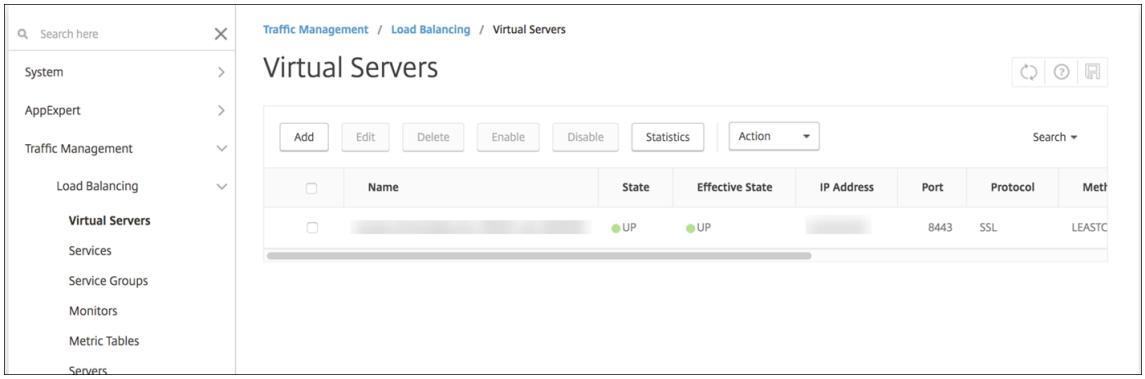
```
exec: save ns config
 Done
 Done
root@ns#
```

Test the configuration

1. Validate that the 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 fails, this message appears: HTTP Status 404 - Not Found
4. Enroll a device and ensure it gets both MDM and MAM enrollment.

Add a callback URL and Citrix Gateway VPN virtual IP

After adding the Citrix Gateway instance, you can add a callback URL and specify a Citrix Gateway virtual IP address. These settings are optional, but can be configured for extra security, especially when the XenMobile Server is in the DMZ.

1. In **Settings > Citrix Gateway**, select the Citrix Gateway and then click **Edit**.
2. In the table, click **Add**.
3. For **Callback URL** type the fully qualified domain name (FQDN). The callback URL verifies that a request originated from Citrix Gateway.

   Ensure that the callback URL resolves to an IP address that is reachable from the XenMobile Server. The callback URL can be an external Citrix Gateway URL or some other URL.
4. Type the Citrix Gateway **Virtual IP** address and then click **Save**.

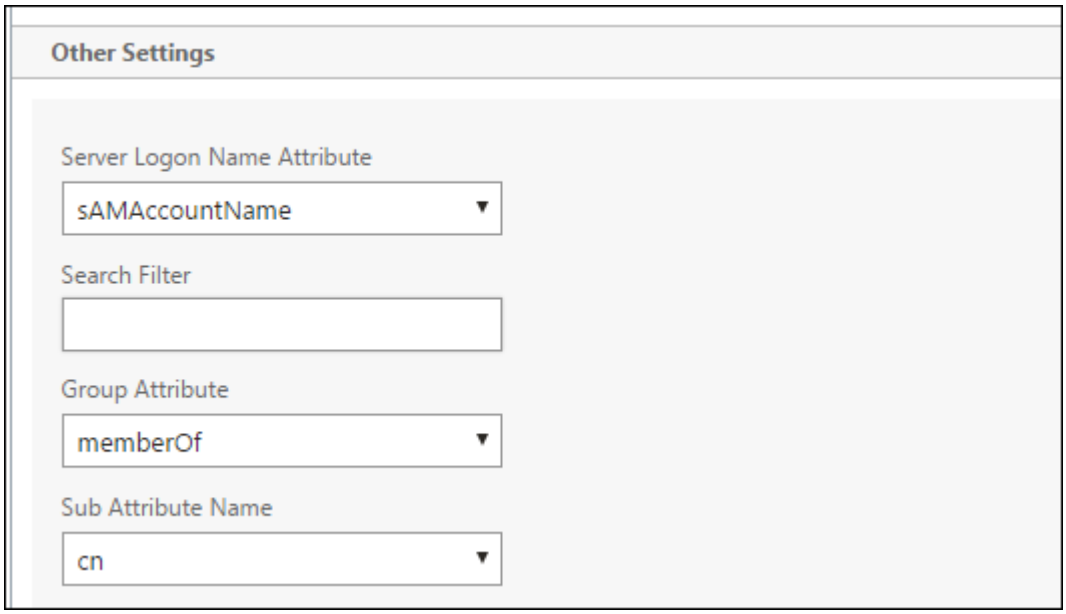
Configure authentication for multiple domains

If you have multiple XenMobile Server instances, such as for test, development, and production environments, you configure Citrix Gateway for the additional environments manually. (You can use the Citrix ADC 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 so you have it when configuring LDAP settings in the XenMobile console.

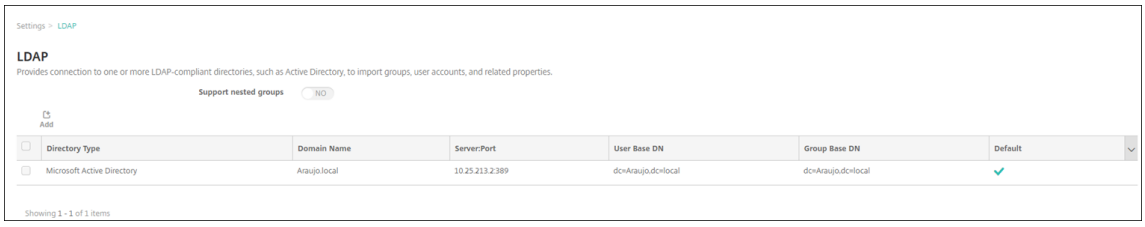


4. Repeat those steps for each LDAP policy. A separate LDAP policy is required for each domain.
5. In the session policy bound to the Citrix Gateway virtual server, navigate to **Edit session profile > Published Applications**. Make sure that **Single Sign-On Domain** is blank.

XenMobile Server configuration

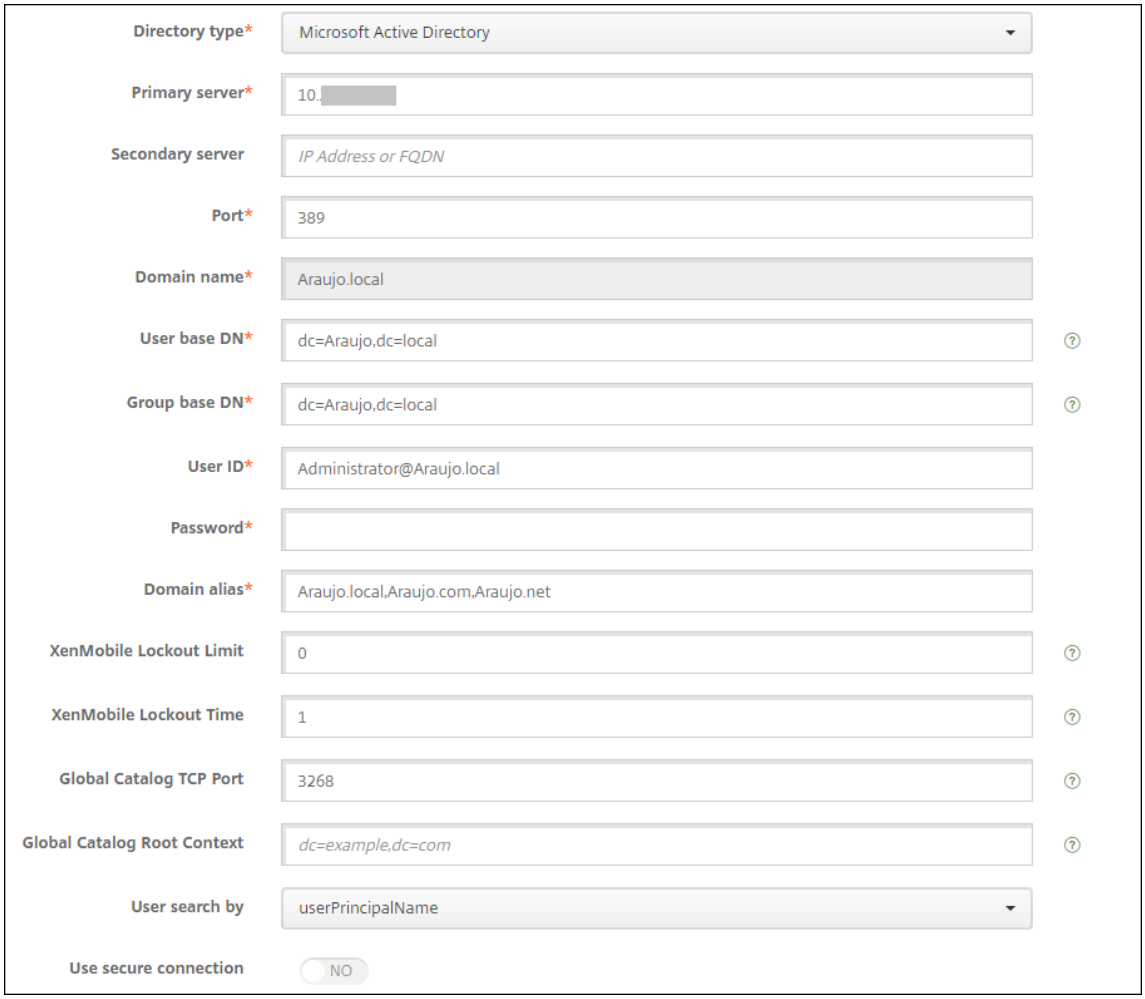
To configure LDAP for a multi-domain XenMobile environment:

1. In the XenMobile console, go to **Settings > LDAP** and add or edit a directory.



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.



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, configure the two MDM load balancer virtual servers (one for port 443 and one for port 8443) on Citrix Gateway. Use the following information as a template for your settings.

> **Important:**
>
> The following updates are only for a Citrix Gateway configured for SSL offload.

1. Create a pattern set with the name `XMS_DropURLs`.

```
1 add policy patset XMS_DropURLs
```



```
<!--NeedCopy-->
```

2. Add the following URLs to the new pattern set. Customize this list as required.

```
bind policy patset XMS_DropURLs /zdm/shp/console -index 6

bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5

bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4

bind policy patset XMS_DropURLs /zdm/log.jsp -index 3

bind policy patset XMS_DropURLs /zdm/login.jsp -index 2

bind policy patset XMS_DropURLs /zdm/console -index 1
<!--NeedCopy-->
```

3. Create a policy to drop all traffic to these URLs, unless the connection request originates from the specified subnet.

```
add responder policy XMS_DROP_pol  “CLIENT.IP.SRC.IN_SUBNET
    (192.168.0.0/24).NOT &&
HTTP.REQ.URL.CONTAINS_ANY(” XMS_DropURLs” )”  DROP -comment "Allow
     only subnet 192.168.0.0/24 to access these URLs. All other
    connections are DROPed"
<!--NeedCopy-->
```

4. Bind the new policy to both MDM load balancer virtual servers (ports 443 and 8443).

```
bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName
    XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
    REQUEST

bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName
    XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
    REQUEST
<!--NeedCopy-->
```

Domain or domain plus security token authentication

February 25, 2021

XenMobile supports domain-based authentication against one or more directories that are compliant with the Lightweight Directory Access Protocol (LDAP). You can configure a connection in XenMobile to one or more directories and then use the LDAP configuration to import groups, user accounts, and related properties.

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.

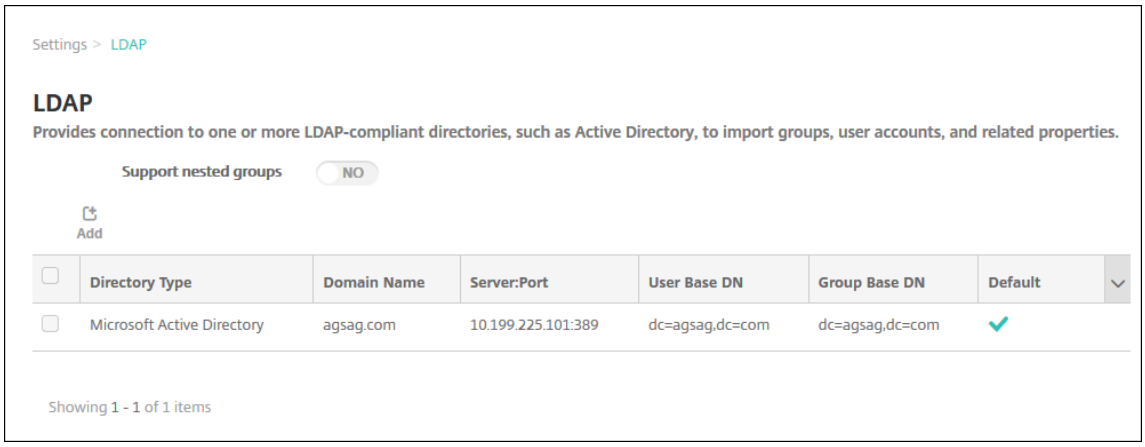
A common usage of LDAP is to provide single sign-on (SSO) for users, where a single password (per user) is shared among multiple services. Single sign-on enables a user to log on one time to a company website, for authenticated access to the corporate intranet.

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.

> **Important:**
>
> XenMobile doesn't support changing the authentication mode from domain authentication to a different authentication mode after users enroll devices in XenMobile.

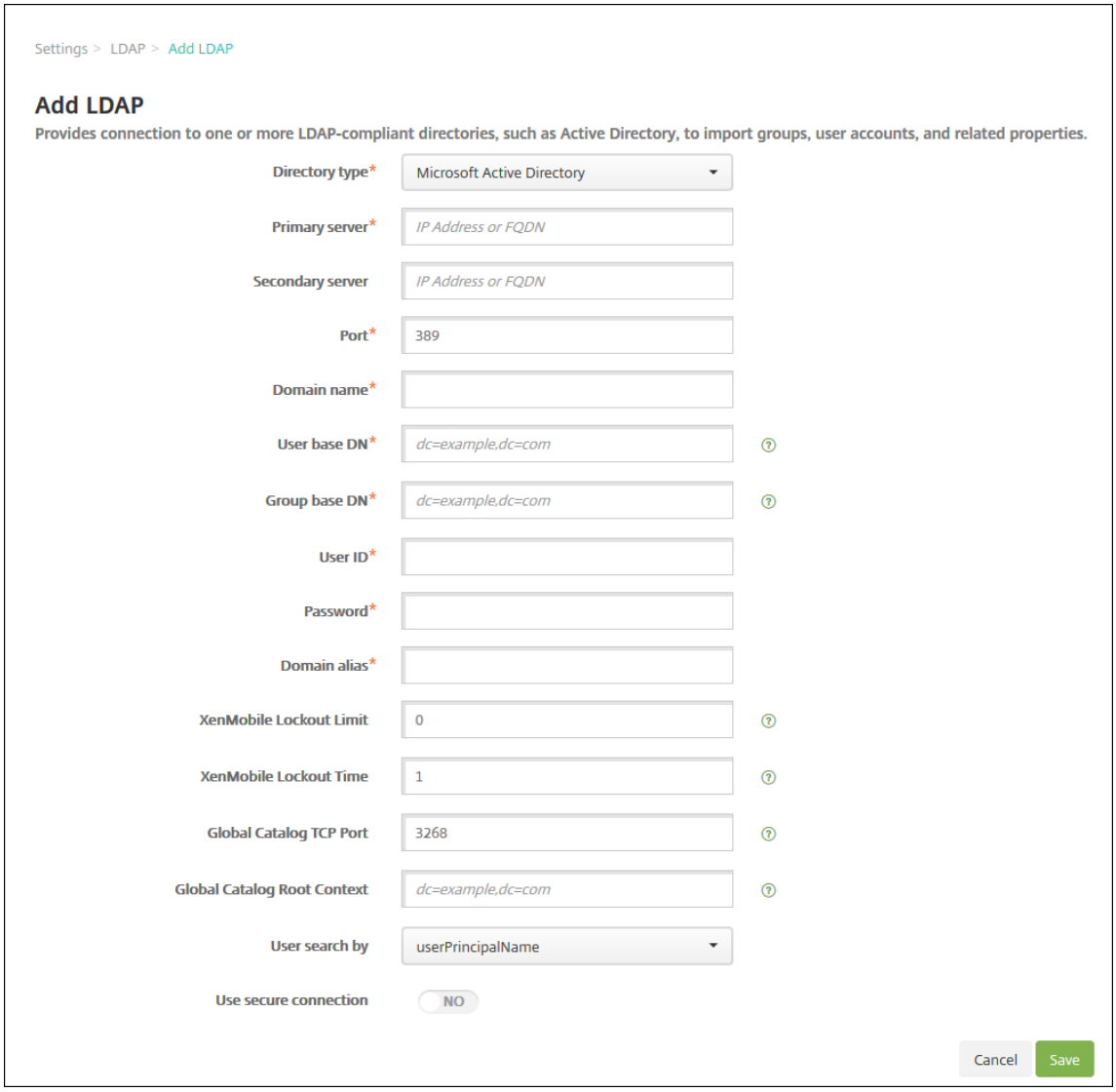
To add LDAP connections in XenMobile

1. In the XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Under **Server**, click **LDAP**. The **LDAP** page appears. You can add, edit, or delete LDAP-compliant directories, as described in this article.



To add an LDAP-compliant directory

1. On the **LDAP** page, click **Add**. The **Add LDAP** page appears.



2. 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.
- **XenMobile Lockout Limit:** Type a number between **0** and **999** for the number of failed logon attempts. A value of **0** means that XenMobile never locks out the user based on failed logon attempts.
- **XenMobile 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.
- **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:** In the list, click either **userPrincipalName**, or **sAMAccountName**. The default is **userPrincipalName**. If you change the **User search by** setting after enrollment, users must re-enroll.
- **Use secure connection:** Select whether to use secure connections. The default is **NO**.

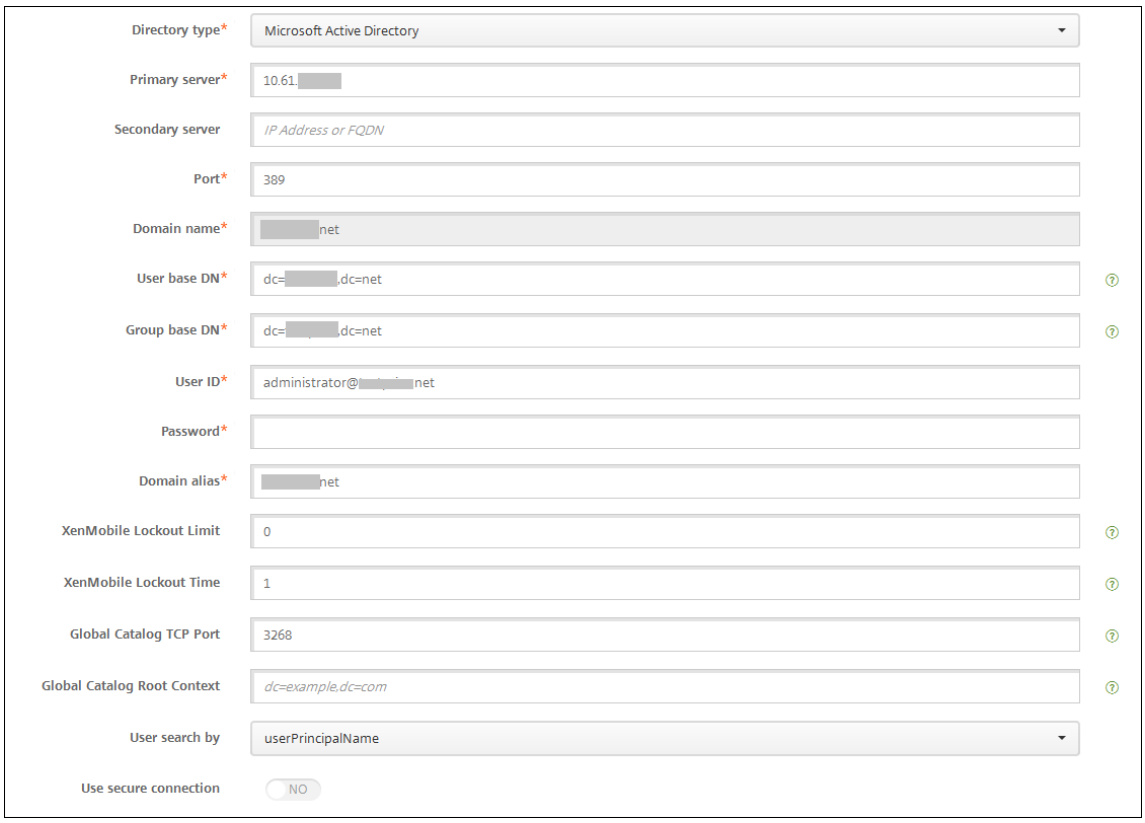
3. Click **Save**.

To edit an LDAP-compliant directory

1. In the **LDAP** table, select the directory to edit.

   When you select the check box next to a directory, the options menu appears above the LDAP list. Click anywhere else in the list and the options menu appears on the right side of the listing.

2. Click **Edit**. The **Edit LDAP** page appears.



3. Change the following information as appropriate:

   - **Directory type:** In the list, click the appropriate directory type.
   - **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, type the IP address or FQDN for the secondary server (if one has been configured).
   - **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:** You cannot change this field.
   - **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 group base DN group name specified as `cn=groupname`. For example, `cn=users`, `dc=servername`, `dc=net` where `cn=users` is the group name. `DN` and `servername` represent the name of the server running 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.

- **XenMobile Lockout Limit:** Type a number between **0** and **999** for the number of failed logon attempts. A value of **0** means that XenMobile never locks out the user based on failed logon attempts.
- **XenMobile 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.
- **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:** In the list, click either **userPrincipalName**, or **sAMAccountName**. If you change the **User search by** setting after enrollment, users must re-enroll.
- **Use secure connection:** Select whether to use secure connections.

4. Click **Save** to save your changes or **Cancel** to leave the property unchanged.

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 authentication for multiple domains

To configure XenMobile Server to use multiple domain suffixes in an LDAP configuration, see the procedure in the Citrix Endpoint Management documentation, Configure authentication for multiple domains. The steps are the same in the on-premises version of XenMobile Server and the Endpoint Management cloud release.

Configure domain plus security token authentication

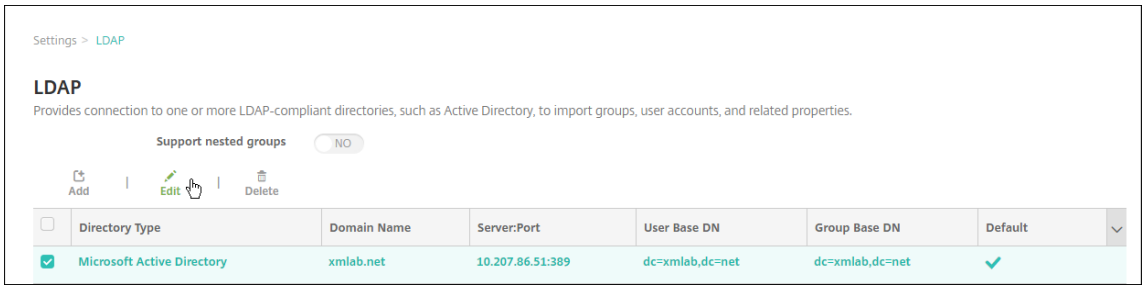
You can configure XenMobile to require users to authenticate with their LDAP credentials plus a one-time password, using the RADIUS protocol.

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.

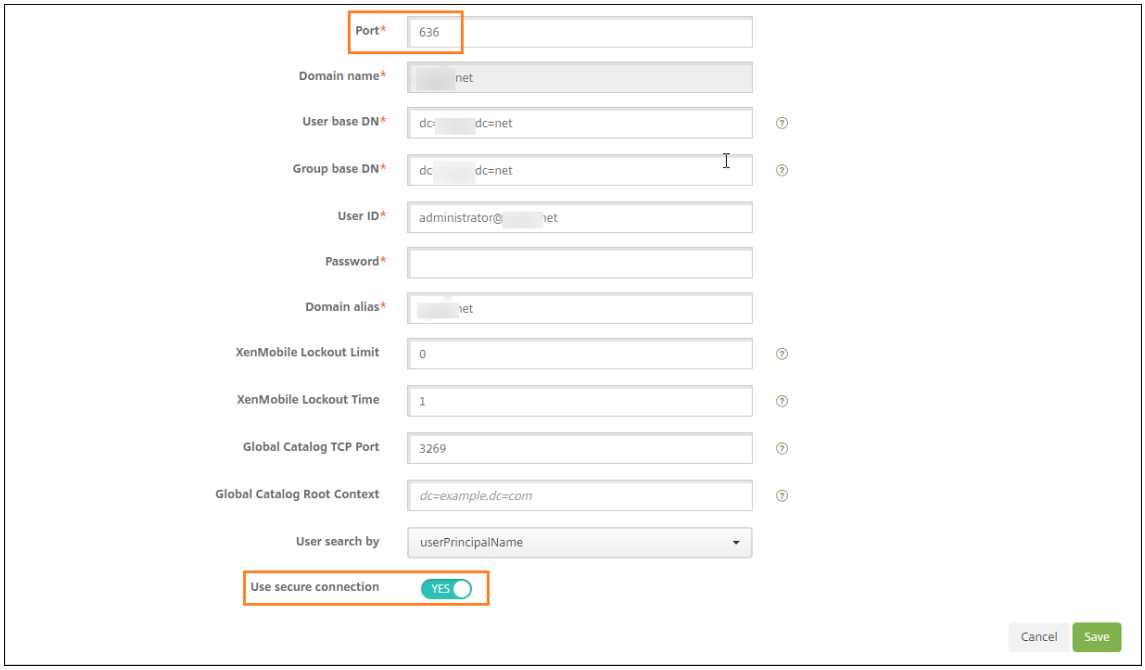
Configure LDAP settings

Use of LDAP for authentication requires that you install an SSL certificate from a Certificate Authority on XenMobile. For information, see Uploading certificates in XenMobile.

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**.

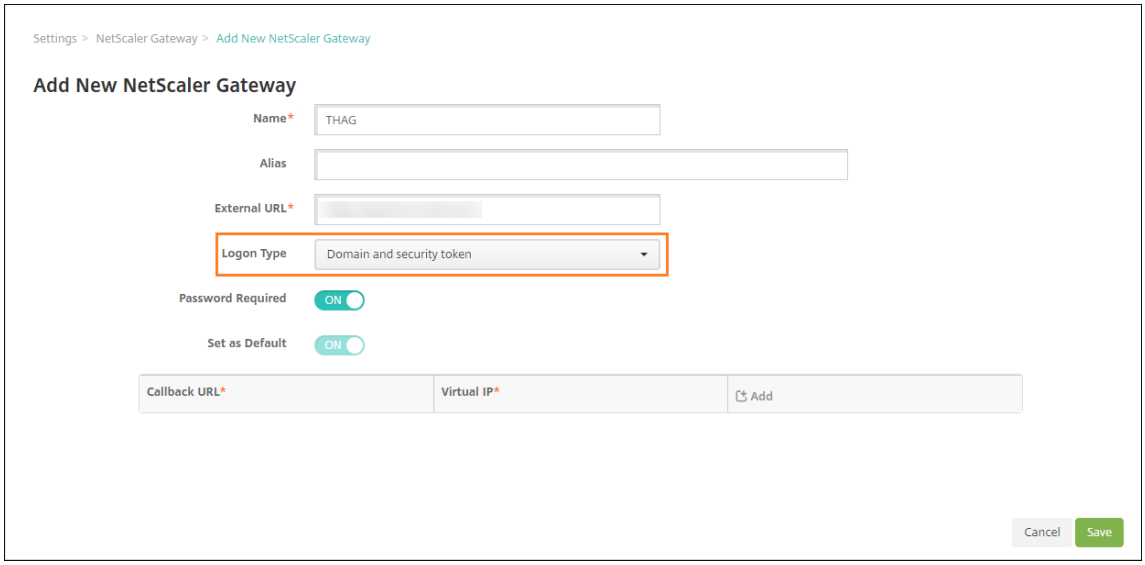


Configure Citrix Gateway settings

The following steps assume that you already have added a Citrix Gateway instance to XenMobile. To add a Citrix Gateway instance, see Add a Citrix Gateway instance.

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 XenMobile. For information, see the Citrix Gateway documentation.

Client certificate or certificate plus domain authentication

May 26, 2021

The default configuration for XenMobile is user name and password authentication. To add another layer of security for enrollment and access to the XenMobile environment, consider using certificate-based authentication. In the XenMobile environment, this configuration is the best combination of security and user experience. Certificate plus domain authentication has the best SSO possibilities coupled with the security provided by two-factor authentication at Citrix ADC.

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:**
>
> XenMobile doesn't support changing the authentication mode from domain authentication to some other authentication mode after users enroll devices in XenMobile.

If you don't allow LDAP and use smart cards or similar methods, configuring certificates allows you to represent a smart card to XenMobile. Users then enroll using a unique PIN that XenMobile generates for them. After a user has access, XenMobile then creates and deploys the certificate used to authenticate to the XenMobile environment.

You can use the Citrix ADC for XenMobile wizard to perform the configuration required for XenMobile when using Citrix ADC certificate-only authentication or certificate plus domain authentication. You can run the Citrix ADC 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 XenMobile for Certificate and Security Token Authentication.

Client certificate authentication is available for XenMobile MAM mode (MAM-only) and ENT mode (when users enroll into MDM). Client certificate authentication isn't available for XenMobile ENT mode when users enroll into legacy MAM mode. To use client certificate authentication for XenMobile ENT and MAM modes, you must configure the Microsoft server, the XenMobile Server, 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 the XenMobile Server:

1. Upload the certificate to XenMobile.
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

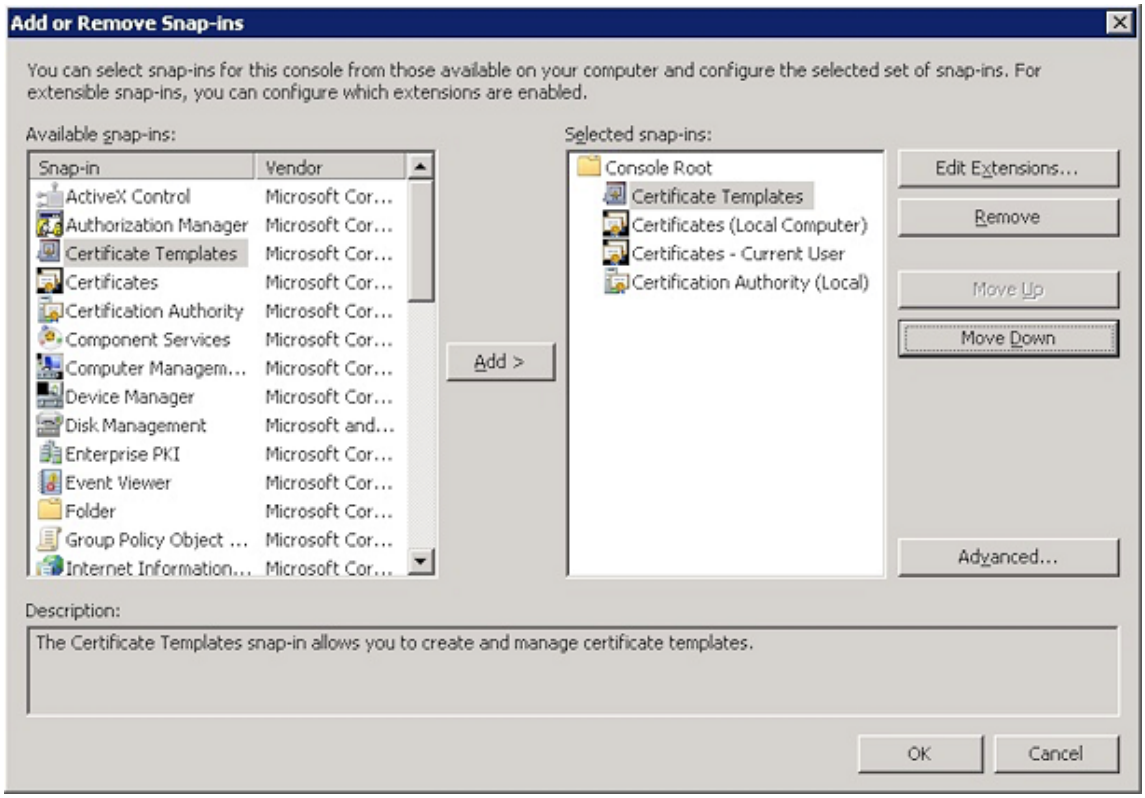
- When you create a Microsoft Certificate Services Entity template, avoid possible authentication issues with enrolled devices by excluding special characters. For example, don't use these characters in the template name: `: ! $ ()## % + * ~ ? | { } []`
- For Windows Phone 8.1 devices using certificate authentication and SSL Offload, disable SSL session reuse for port 443 on both load balancing virtual servers in Citrix ADC. To do that, run the following command on the virtual server for port 443:

  ```
  set ssl vserver <ssl lb vserver> sessReuse DISABLE
  ```

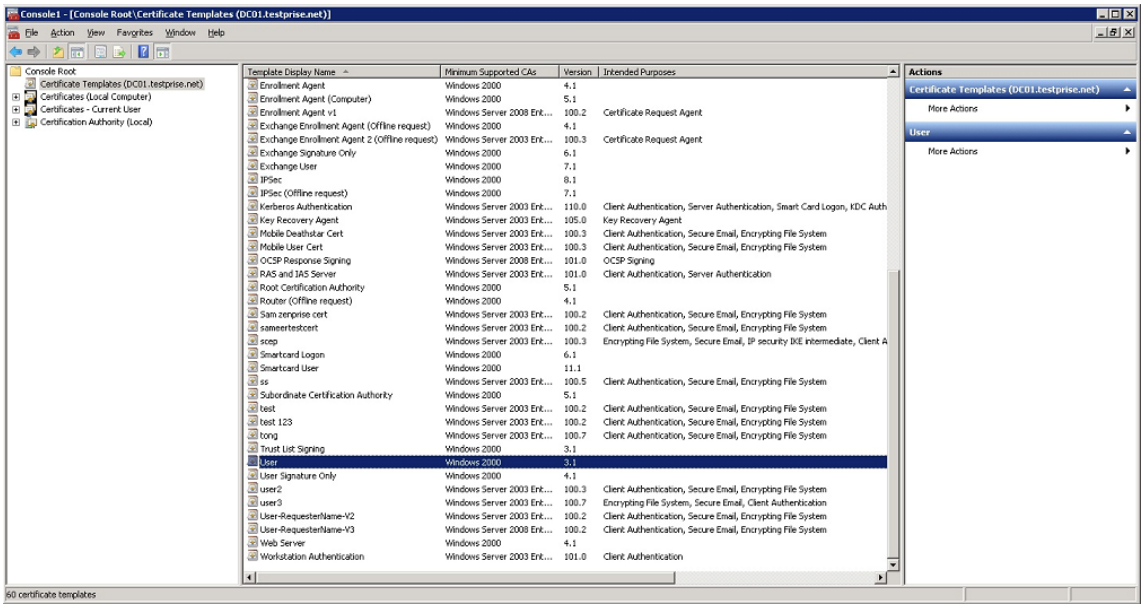
  Disabling SSL session reuse disables some of the optimizations that Citrix ADC provides, which can result in a performance decrease on the Citrix ADC.
- To configure Certificate-based Authentication for Exchange ActiveSync, see this Microsoft blog. Configure the certificate authority (CA) server site 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 necessary 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 XenMobile 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

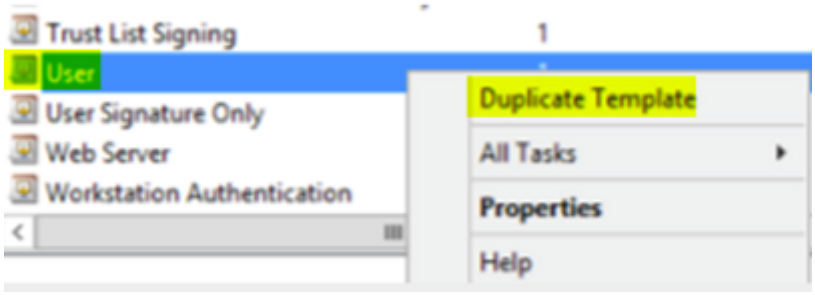
1. Open the console and then click **Add/Remove Snap-ins**.
2. Add the following snap-ins:
   - Certificate Templates
   - Certificates (Local Computer)
   - Certificates - Current User
   - Certificate Authority (Local)



3. Expand **Certificate Templates**.



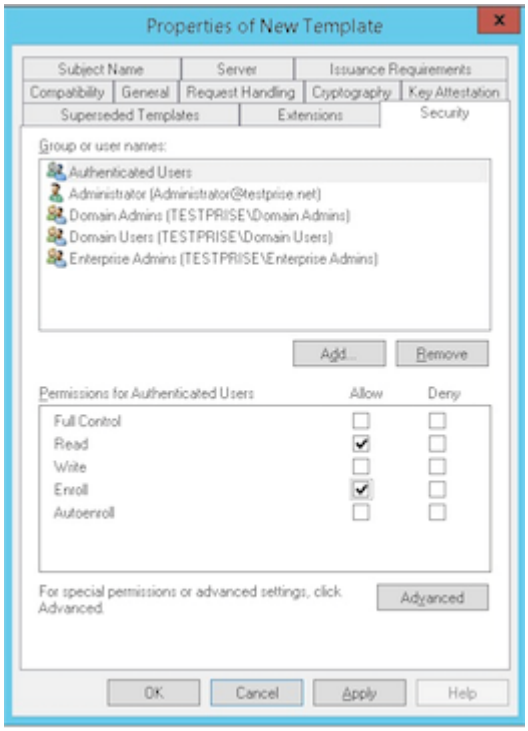
4. Select the **User** template and **Duplicate Template**.



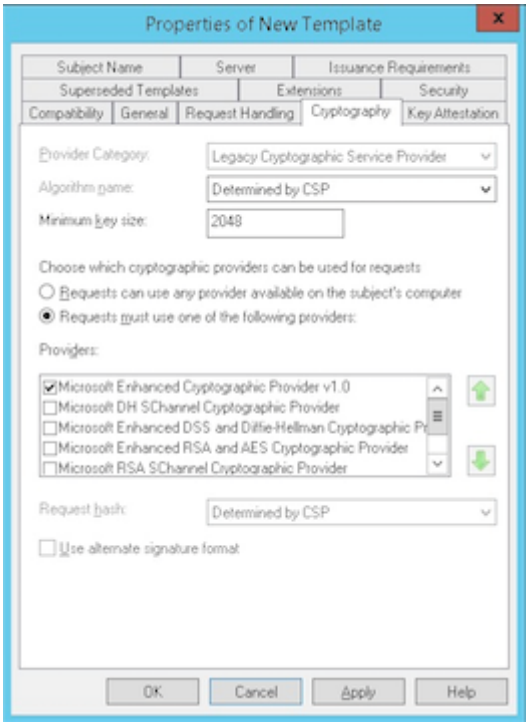
5. Provide the Template display name.

> **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.

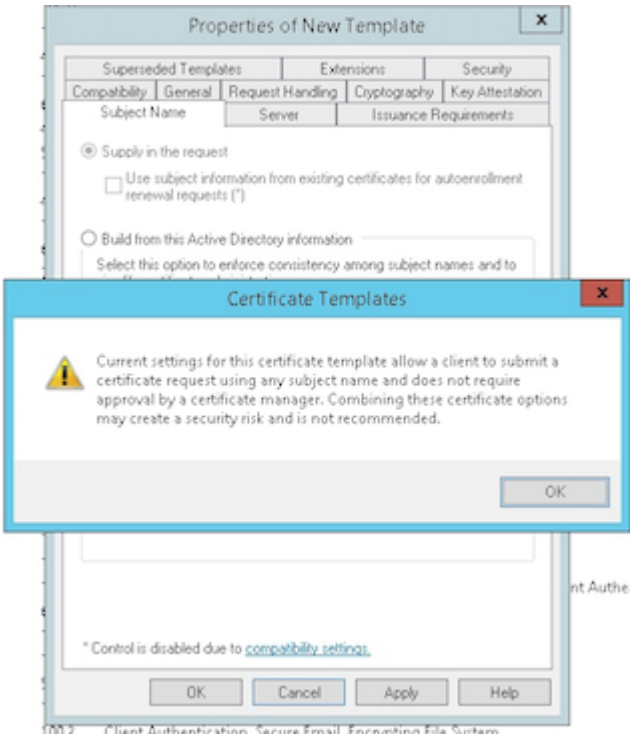
6. Select **Windows 2003 Server** for the template type. In Windows 2012 R2 server, under **Compatibility**, select **Certificate authority** and set the recipient as **Windows 2003**.
7. Under **Security**, select the **Enroll** option in the **Allow** column for the authenticated users.



8. Under **Cryptography**, ensure that you provide the key size. You later enter the key size when configuring XenMobile.



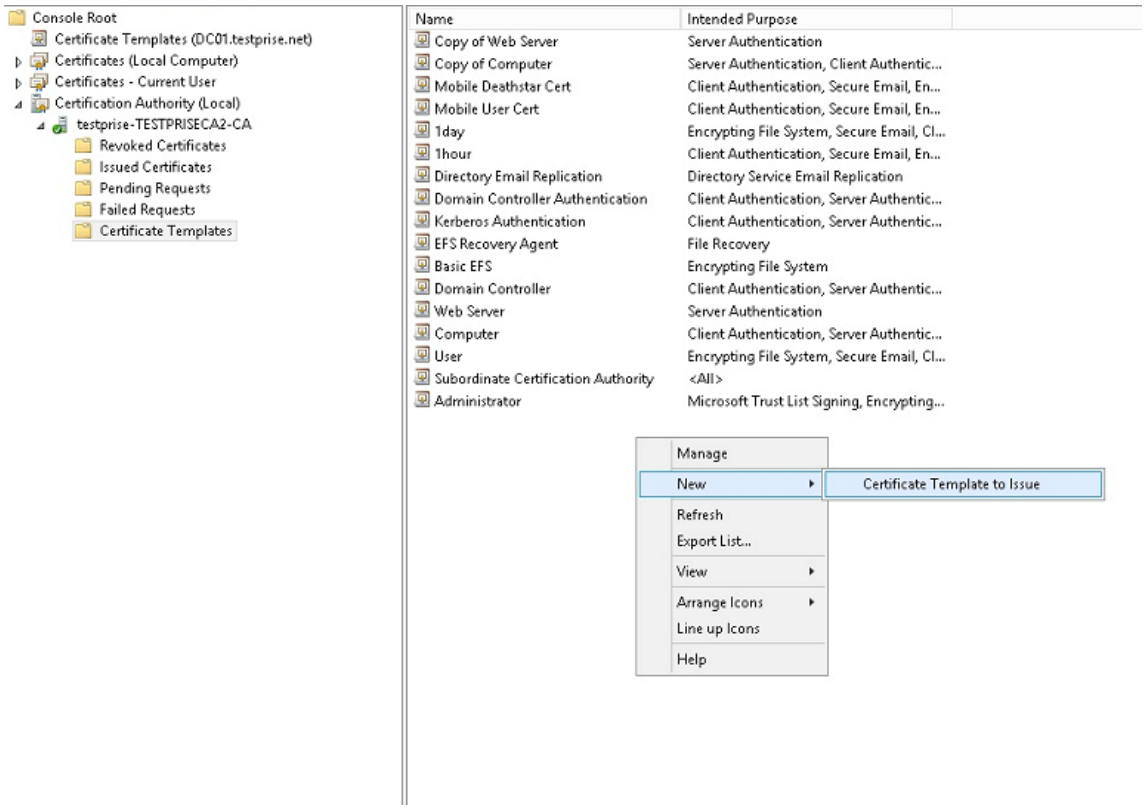
9. Under **Subject Name**, select **Supply in the request**. Apply the changes and then save.



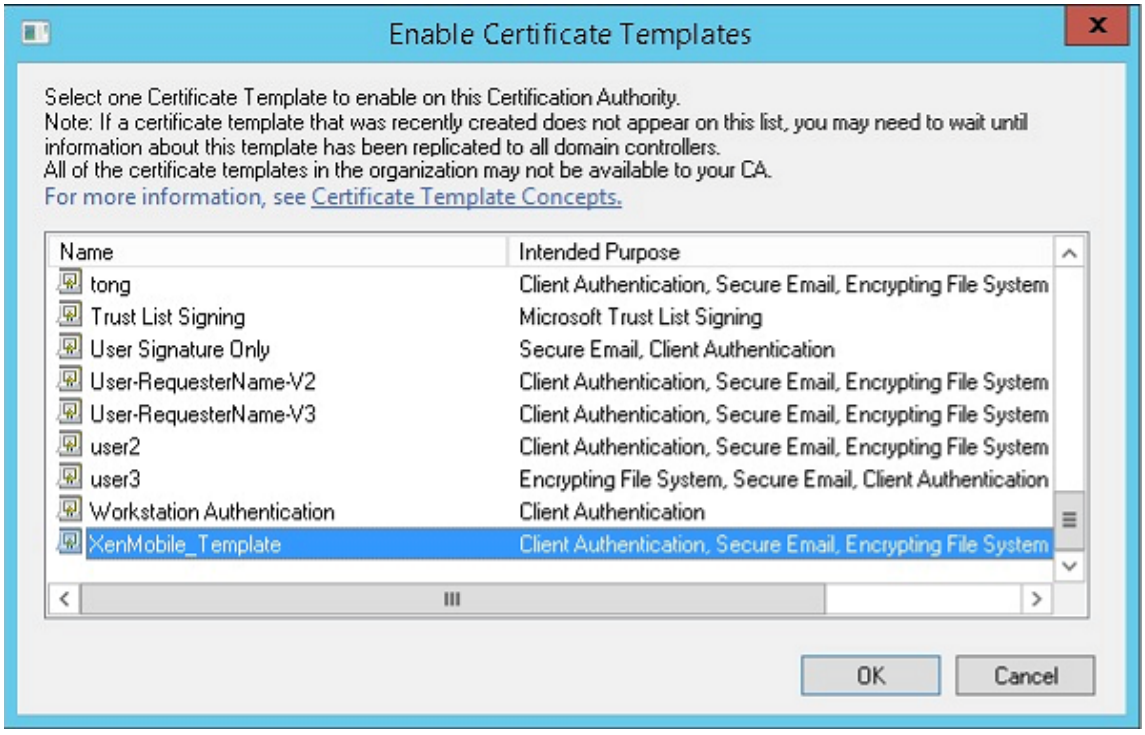
Adding the template to Certificate Authority

1. Go to **Certificate Authority** and select **Certificate Templates**.

2. Right-click in the right pane and then select **New > Certificate Template to Issue**.

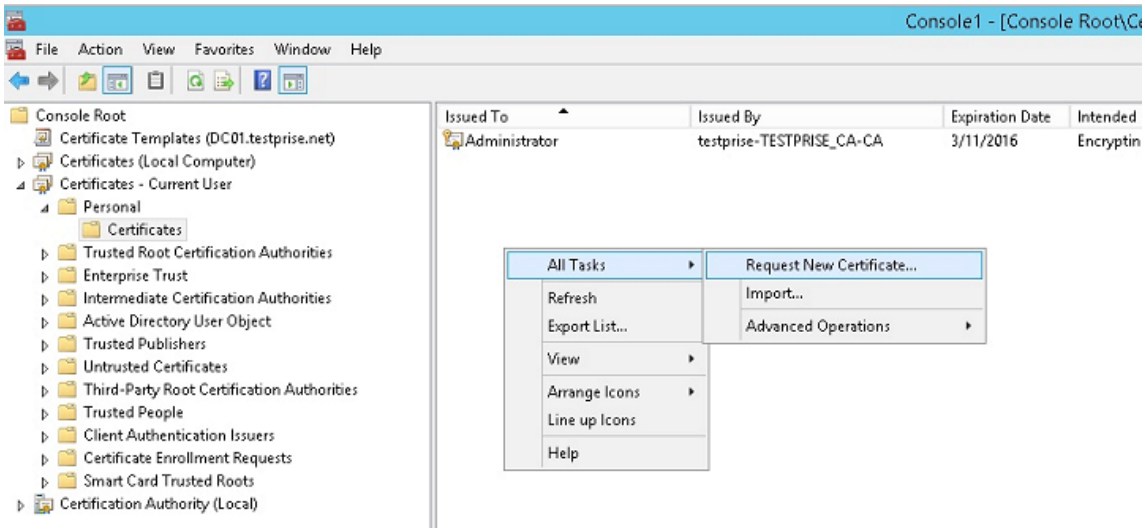


3. Select the template you created in the previous step and then click **OK** to add it into the **Certificate Authority**.

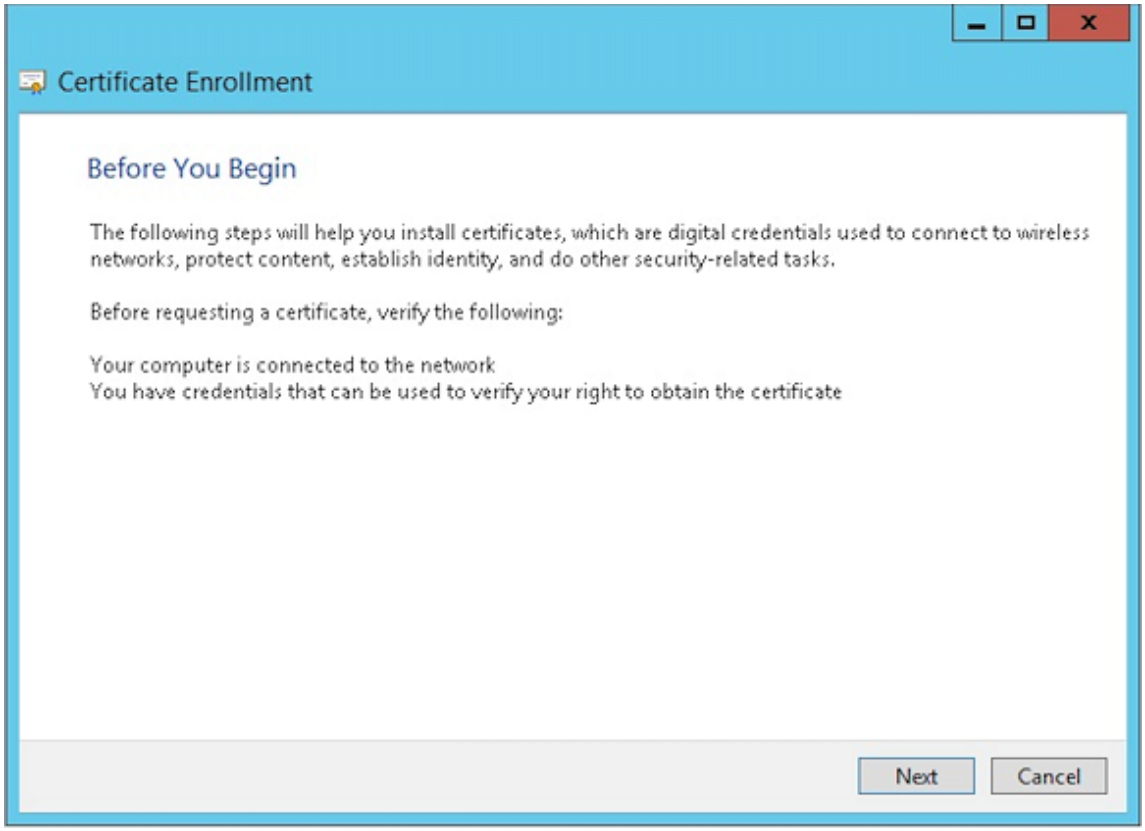


Creating a PFX certificate from the CA server

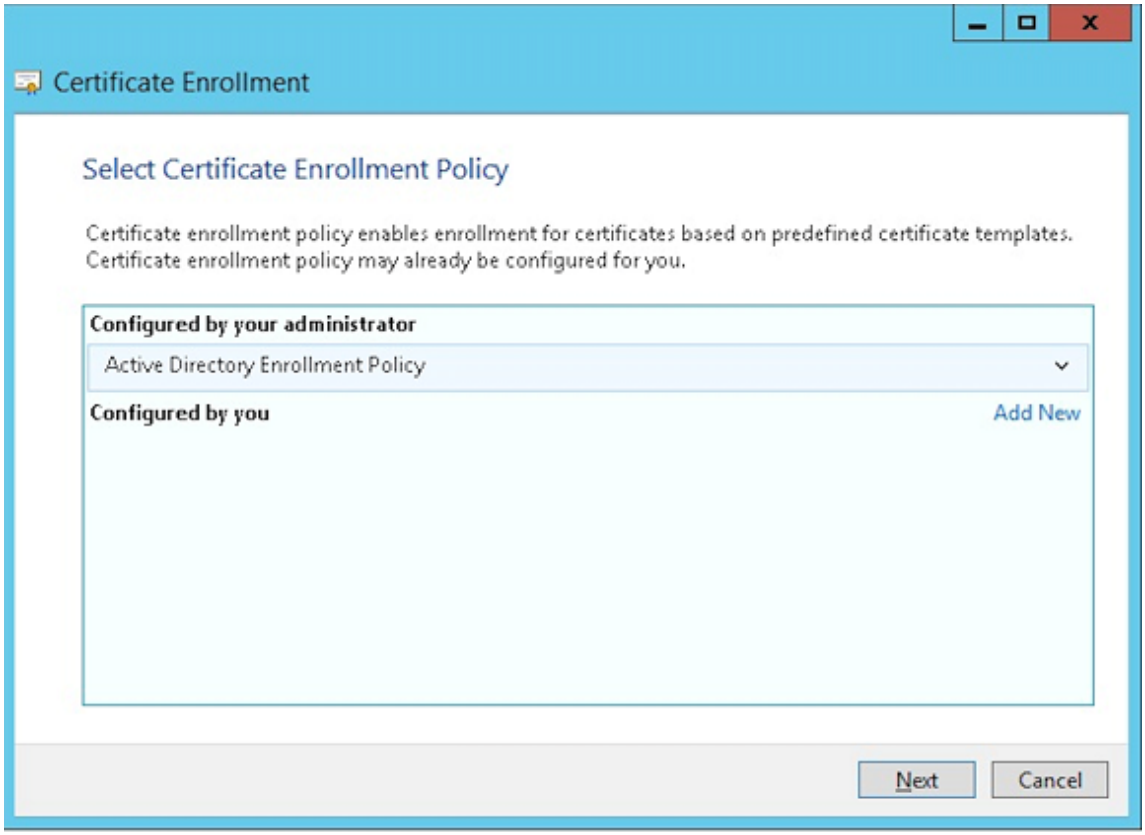
1. Create a user .pfx cert using the service account with which you logged in. The .pfx is uploaded to XenMobile, which then requests a user certificate on behalf of the users who enroll their devices.
2. Under **Current User**, expand **Certificates**.
3. Right-click in the right pane and then click **Request New Certificate**.



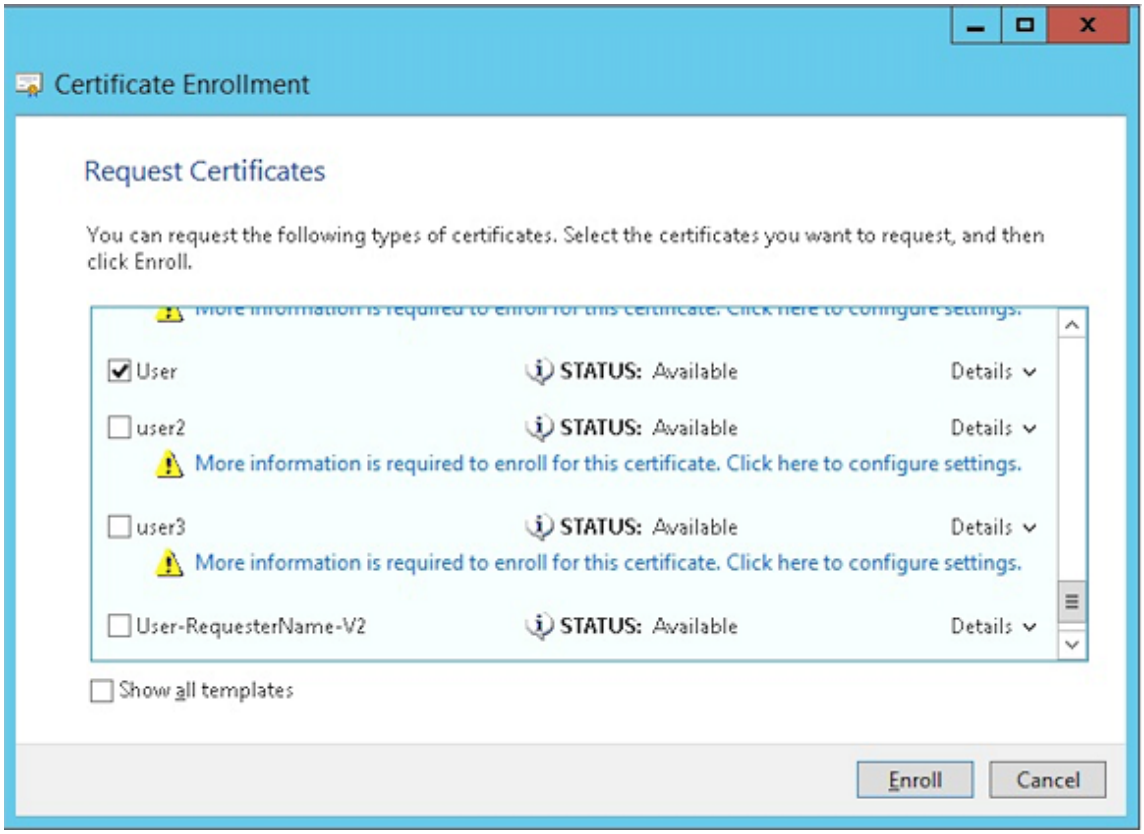
4. The **Certificate Enrollment** screen appears. Click **Next**.



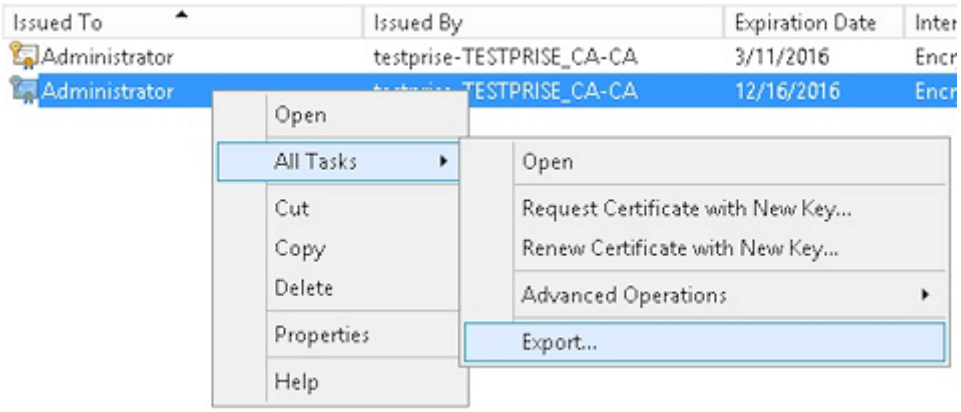
5. Select **Active Directory Enrollment Policy** and then click **Next**.



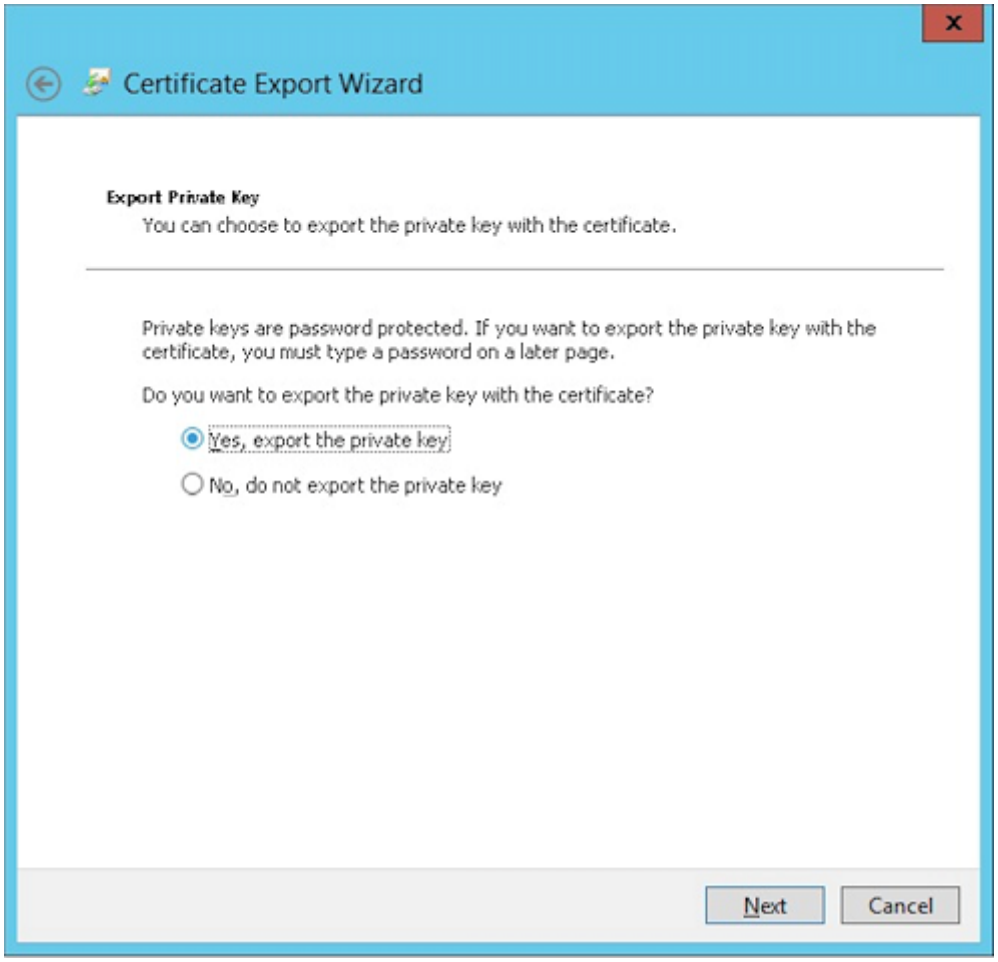
6. Select the **User** template and then click **Enroll**.



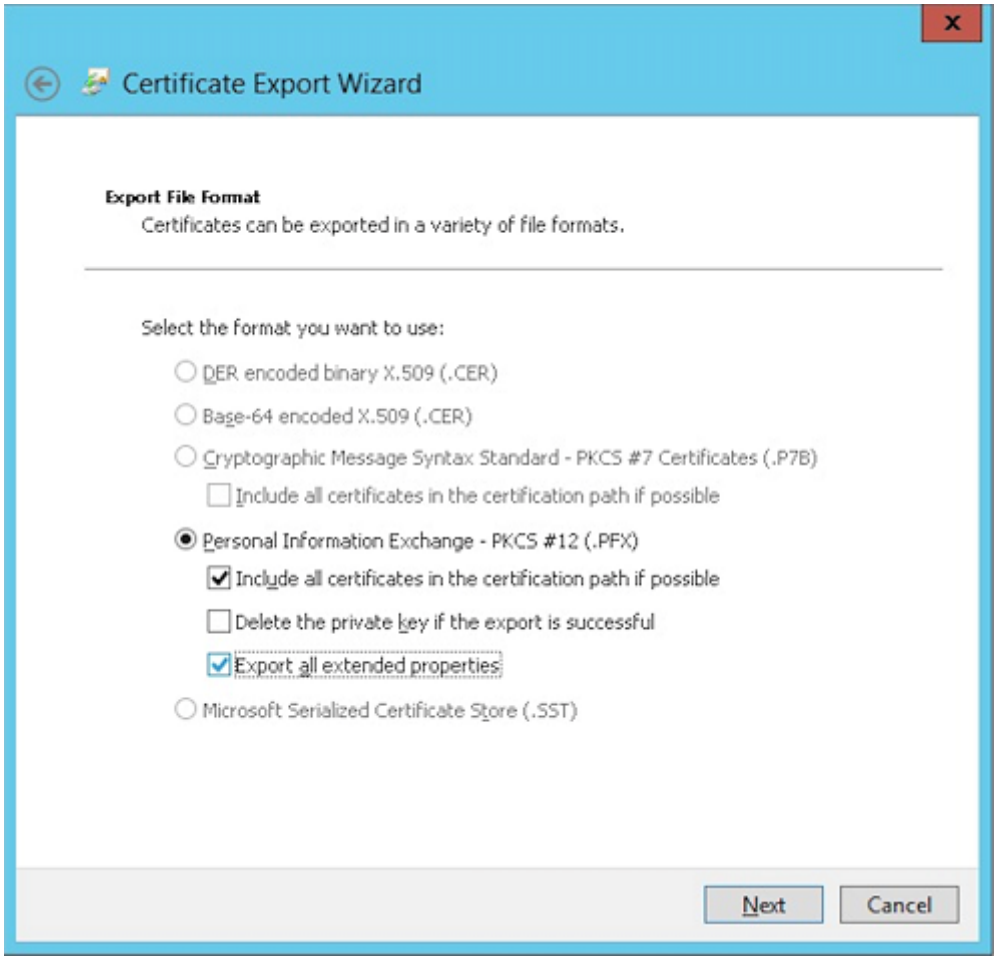
7. Export the .pfx file that you created in the previous step.



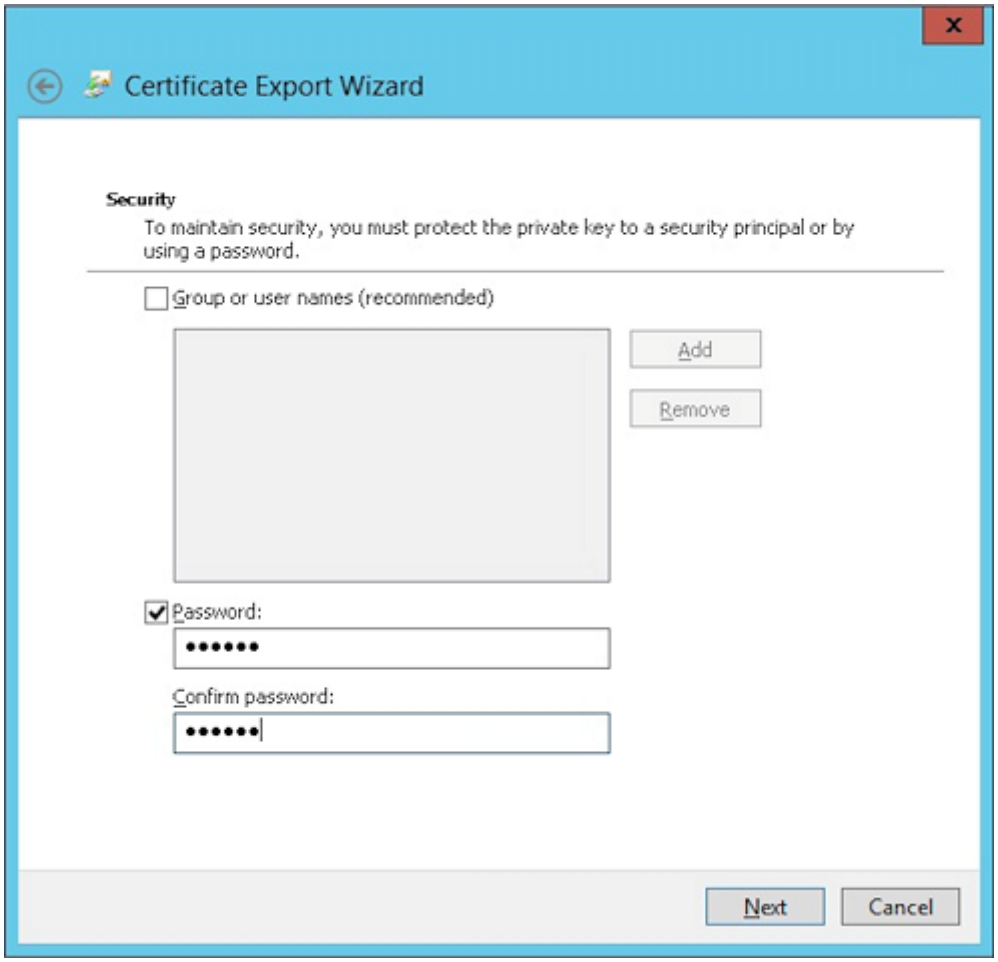
8. Click **Yes, export the private key**.



9. Select **Include all certificates in the certification path if possible** and select the **Export all extended properties** check box.



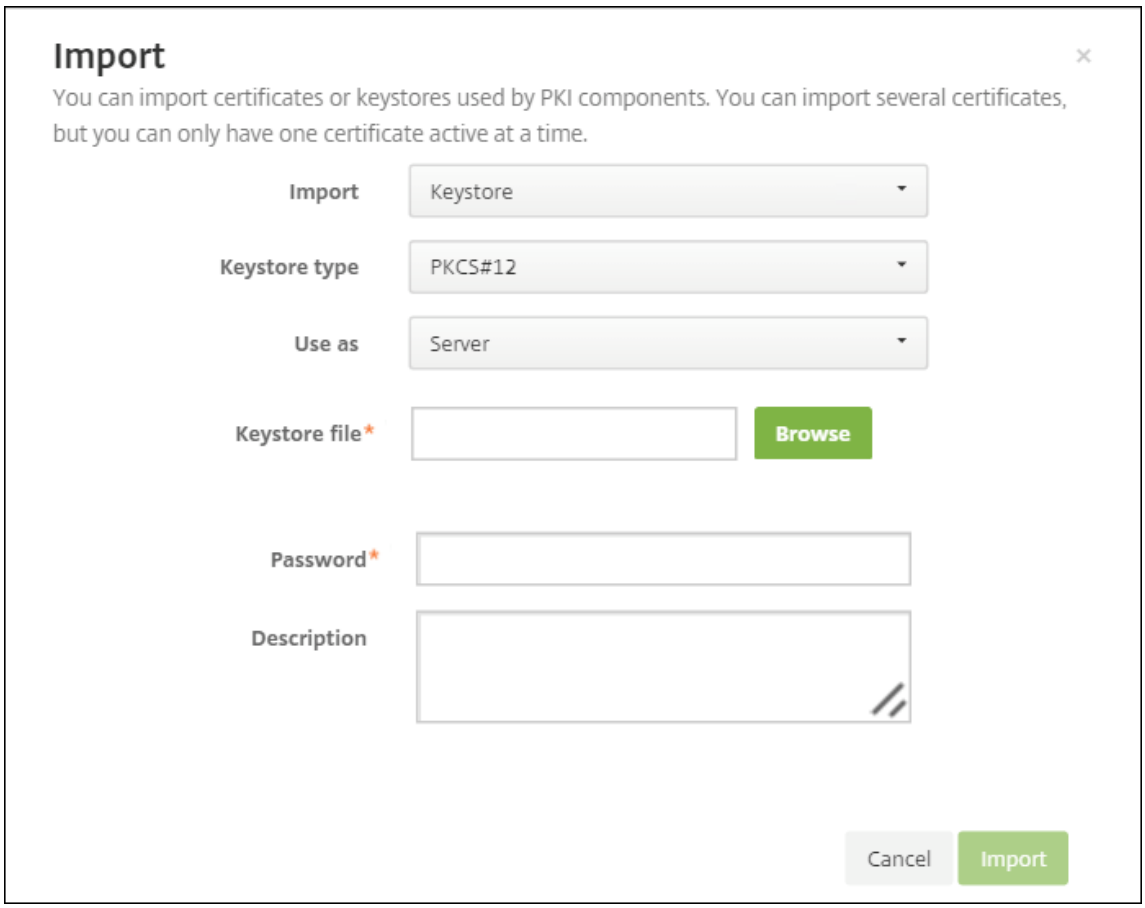
10. Set a password to use when uploading this certificate into XenMobile.



11. Save the certificate onto your hard drive.

Uploading the certificate to XenMobile

1. In the XenMobile 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 created.
   - **Password:** Enter the password you created for this certificate.

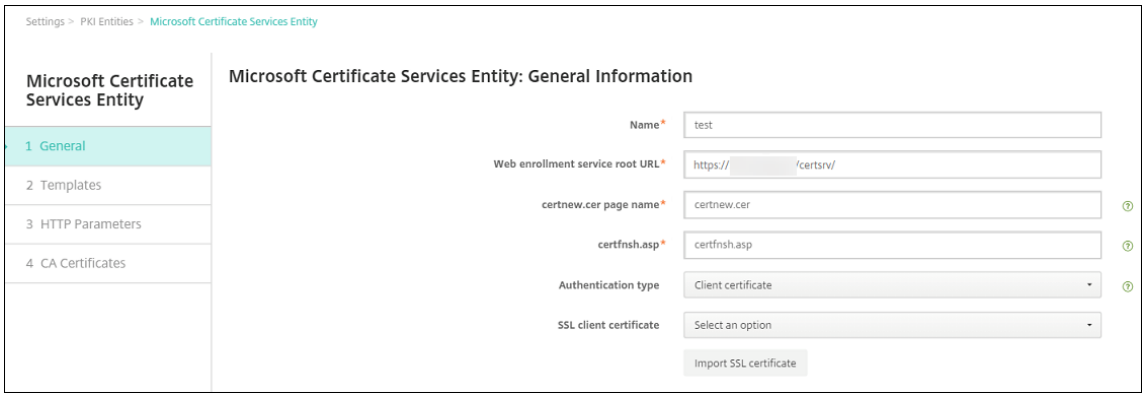


4. Click **Import**.
5. Verify that the certificate installed correctly. A correctly installed certificate displays as a User certificate.

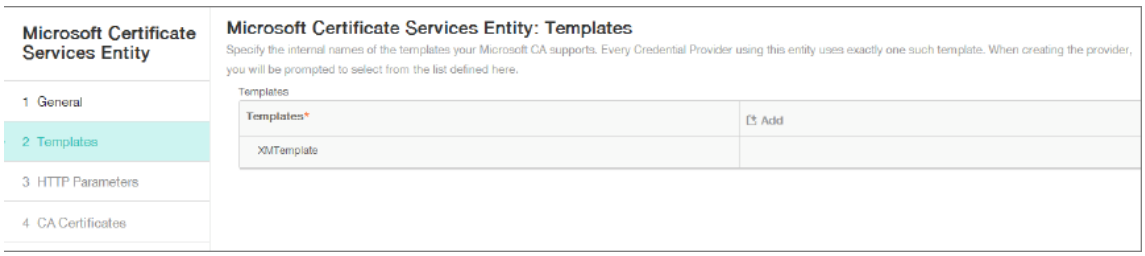
Creating the PKI entity for certificate-based authentication

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

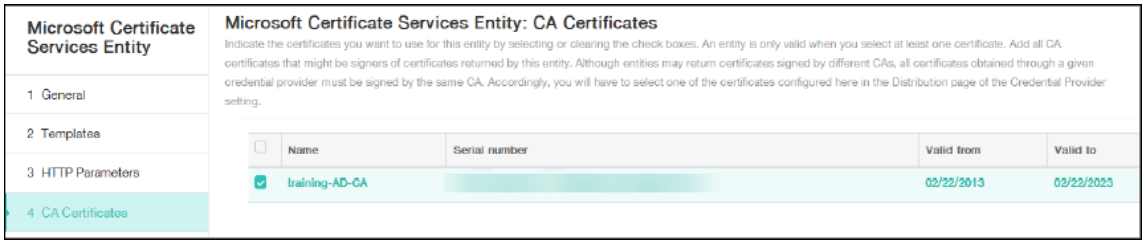
- **SSL client certificate:** Select the User Certificate to be used to issue the XenMobile client certificate.



4. Under **Templates**, add the template that you created when configuring the Microsoft certificate. Don't add spaces.



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 XenMobile client certificate.

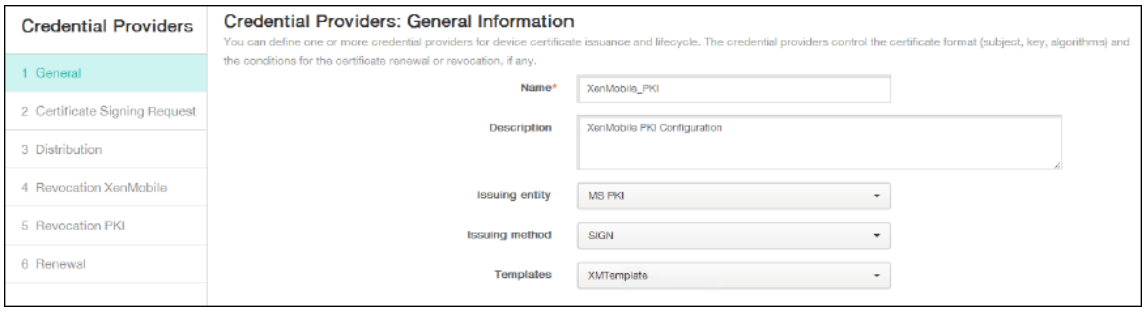


7. Click **Save**.

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.



4. Click **Certificate Signing Request** and then enter the following parameters:

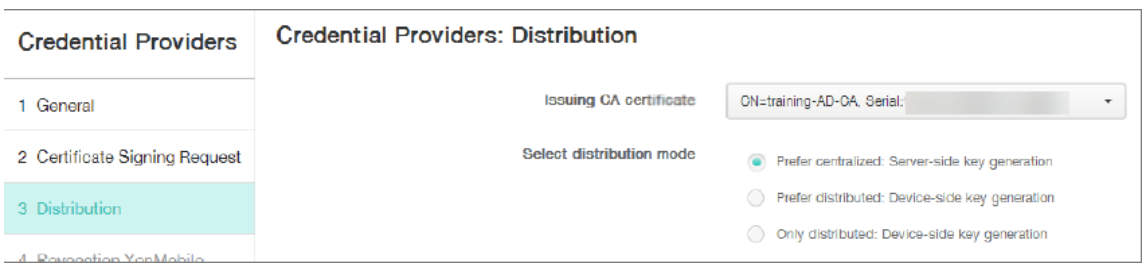
   - **Key algorithm:** RSA
   - **Key size:** 2048
   - **Signature algorithm:** SHA256withRSA
   - **Subject name:** `cn=$user.username`

   For **Subject Alternative Names**, click **Add** and then enter the following parameters:

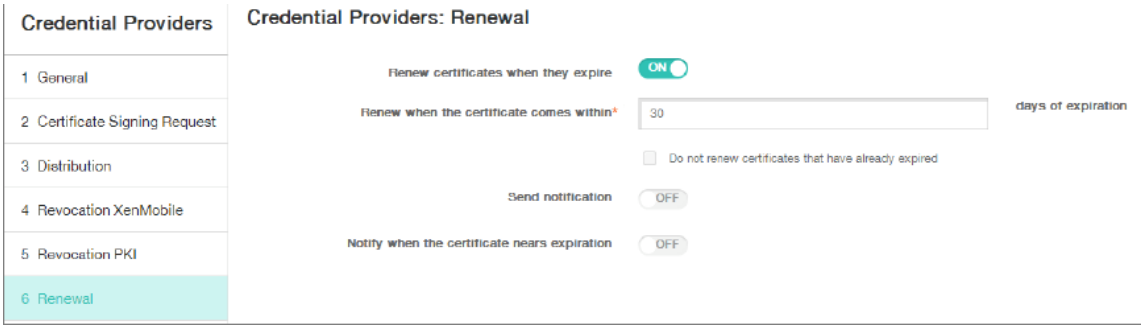
   - **Type:** User Principal name
   - **Value:** `$user.userprincipalname`

5. Click **Distribution** and enter the following parameters:

   - **Issuing CA certificate:** Select the Issuing CA that signed the XenMobile Client Certificate.
   - **Select distribution mode:** Select **Prefer centralized: Server-side key generation**.



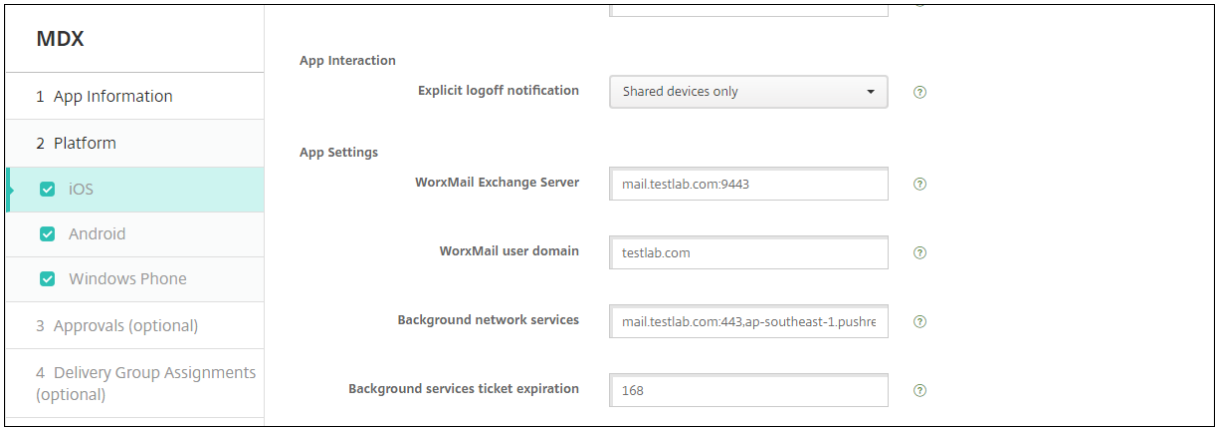
6. For the next two sections, **Revocation XenMobile** and **Revocation PKI**, set the parameters as required. In this example, both options are skipped.
7. Click **Renewal**.
8. For **Renew certificates when they expire**, select **ON**.
9. Leave all other settings as default or change them as required.



10. Click **Save**.

Configuring Secure Mail to use certificate-based authentication

When you add Secure Mail to XenMobile, be sure to configure the Exchange settings under **App Settings**.

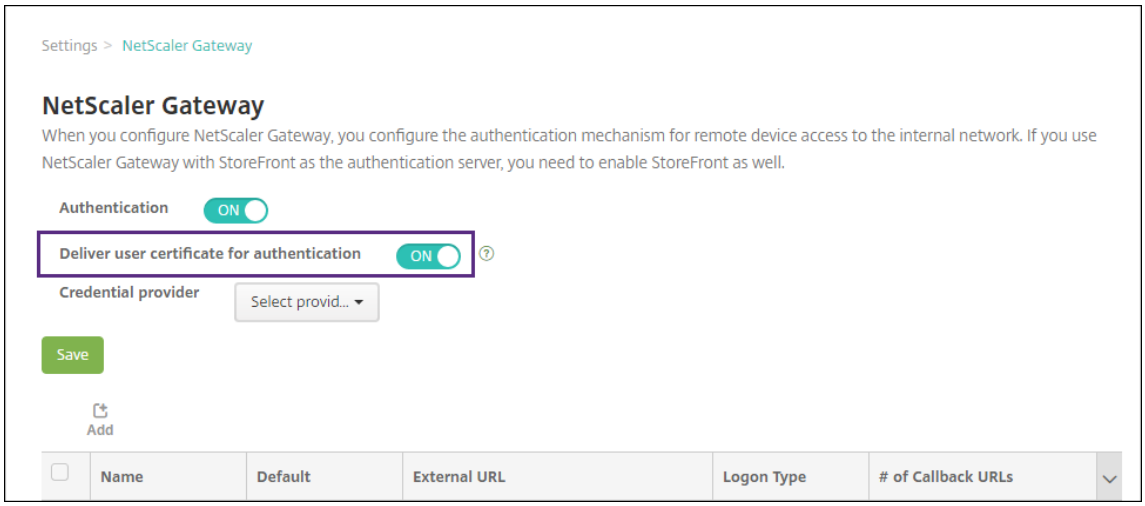


Configuring Citrix ADC certificate delivery in XenMobile

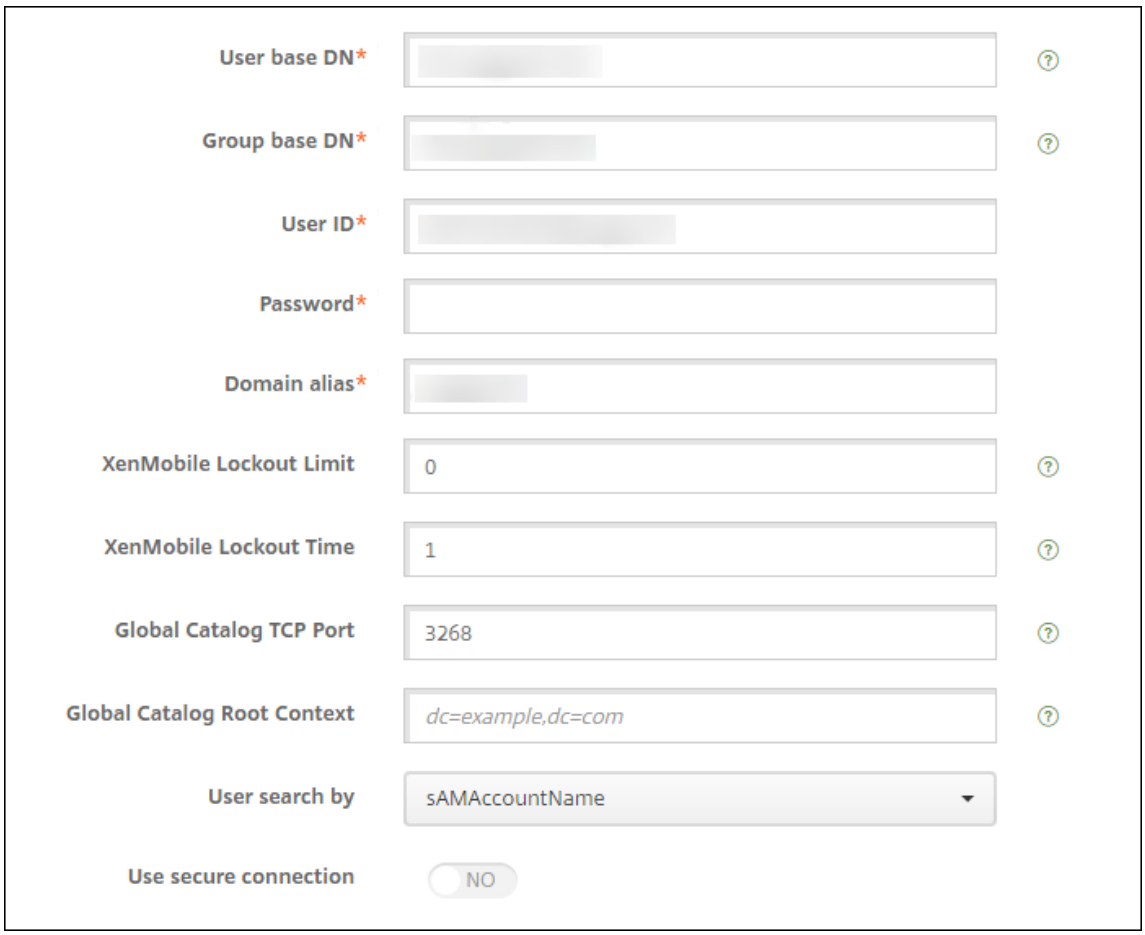
1. Log on to the XenMobile console and click the gear icon in the upper-right corner. The **Settings** screen appears.
2. Under **Server**, click **Citrix Gateway**.
3. If Citrix Gateway isn't already added, click **Add** and specify the settings:
   - **External URL:** `https://YourCitrixGatewayURL`

- **Logon Type:** Certificate and domain
- **Password Required:** OFF
- **Set as Default:** ON

4. For **Deliver user certificate for authentication**, select **On**.



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 XenMobile as follows: Go to **Settings > LDAP**, select the directory and click **Edit**, and select **sAMAccountName** in **User search by**.



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.

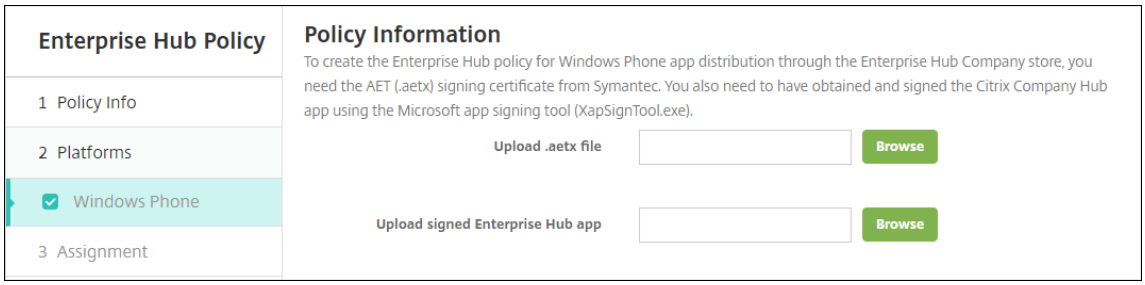
Creating an Enterprise Hub policy for Windows Phone

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 XenMobile console, click **Configure > Device Policies**.

2. Click **Add** and then, under **More > XenMobile 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.



4. Assign the policy to delivery groups and save it.

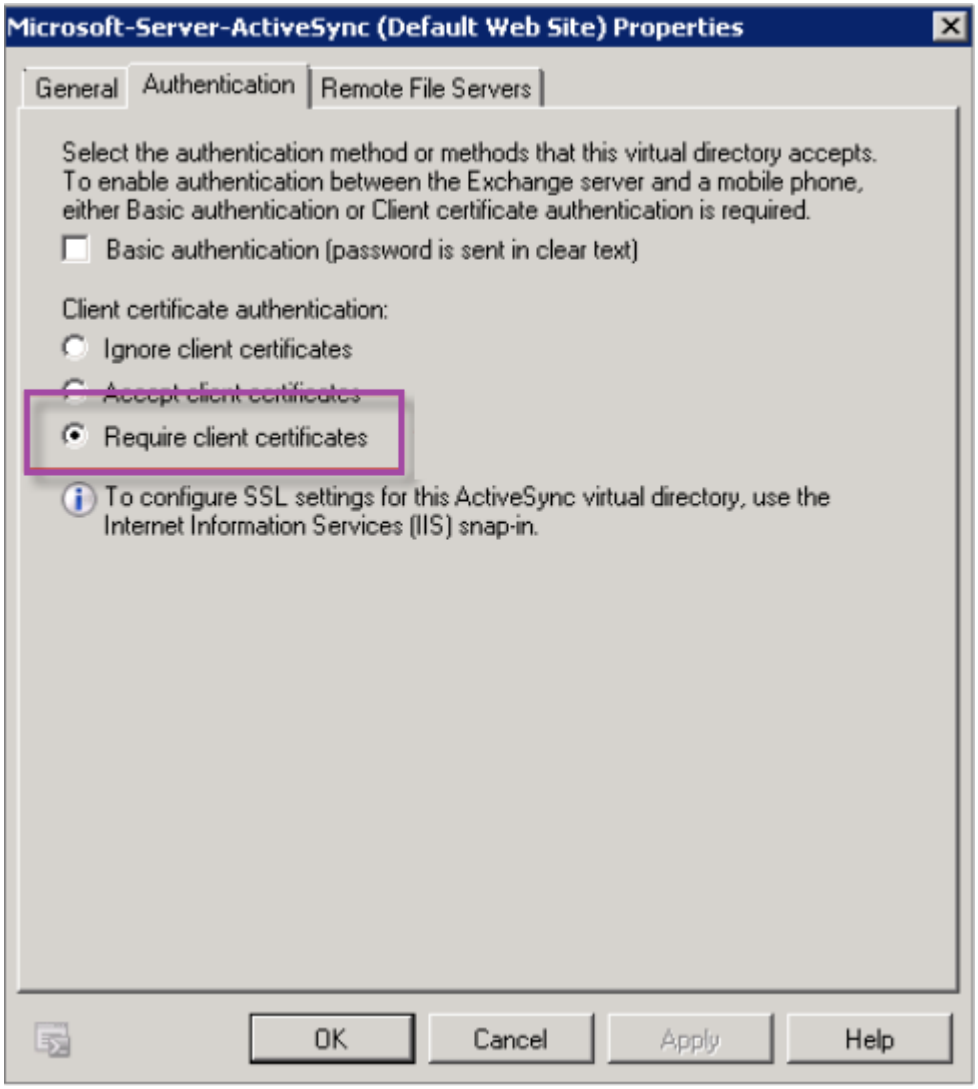
Troubleshooting your client certificate configuration

After a successful configuration of the preceding configuration plus the Citrix Gateway configuration, the user workflow is as follows:

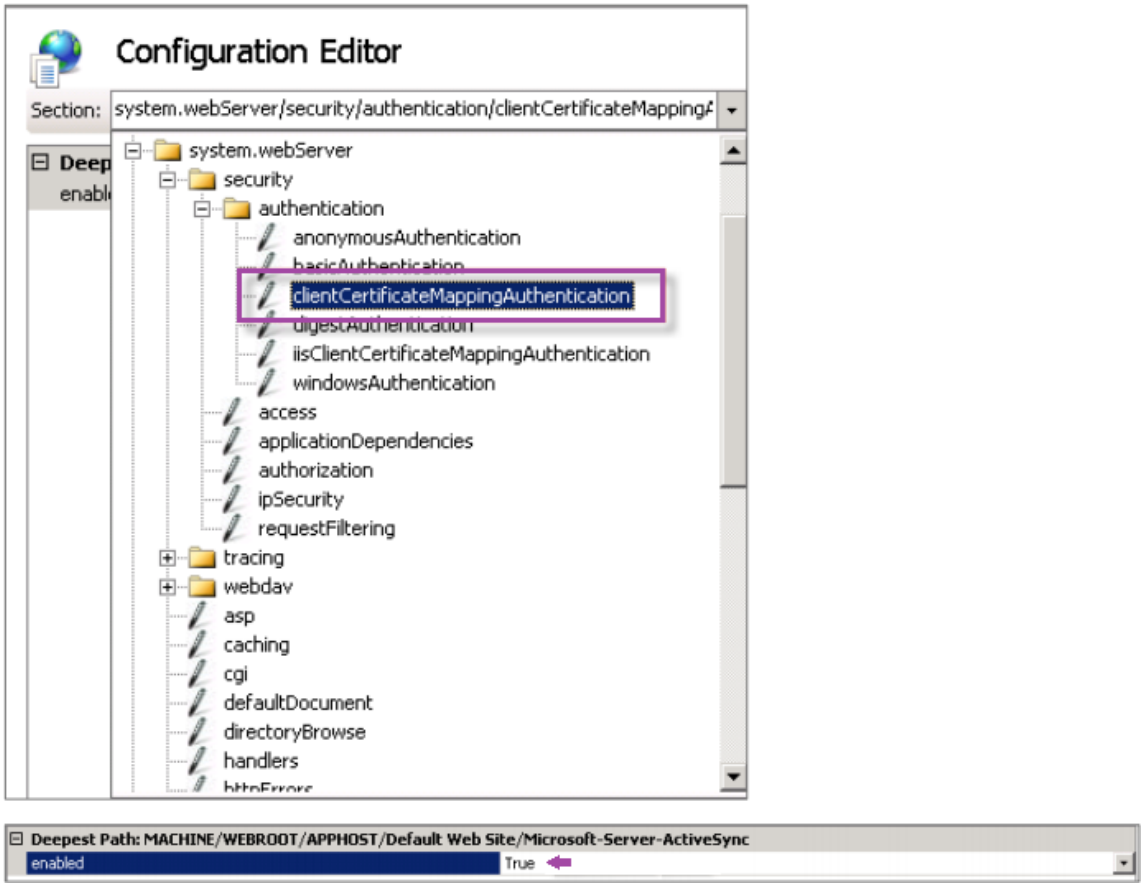
1. Users enroll their mobile device.
2. XenMobile prompts users to create a Citrix PIN.
3. Users are then redirected to the XenMobile Store.
4. When users start Secure Mail, XenMobile doesn't prompt them for user credentials for mailbox configuration. Instead, Secure Mail requests the client certificate from Secure Hub and submits it to the Microsoft Exchange Server for authentication. If XenMobile 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 the 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 XenMobile 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 XenMobile 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=609da5df280d1f54a7deb714fb2c54
 appid={ 4dc3e181-e14b-4a21-b022-59fc669b0914 } certstorename=ExampleCertStoreNam
 verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly
=Disable UsageCheck=Enable clientcertnegotiation=Enable
```

If you cannot deliver Root/Intermediate certificates to a Windows Phone 8.1 device through XenMobile:

- 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 XenMobile 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

March 5, 2021

A XenMobile 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 XenMobile. Internal components are referred to as discretionary. External components are part of your corporate infrastructure.

XenMobile supports the following types of PKI entities:

- Generic PKIs (GPKIs)

  XenMobile Server GPKI support includes DigiCert Managed PKI.

- Microsoft Certificate Services
- Discretionary Certificate Authorities (CAs)

XenMobile supports the following CA servers:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

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 XenMobile 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 CAs as part of the PKI entity configuration. To do so, upload the certificates to XenMobile 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 XenMobile protocol running over a SOAP Web Service layer for purposes of uniform interfacing with various PKI solutions. The GPKI protocol defines the following three 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 XenMobile with that WSDL definition, either through a URL or by uploading the file itself.

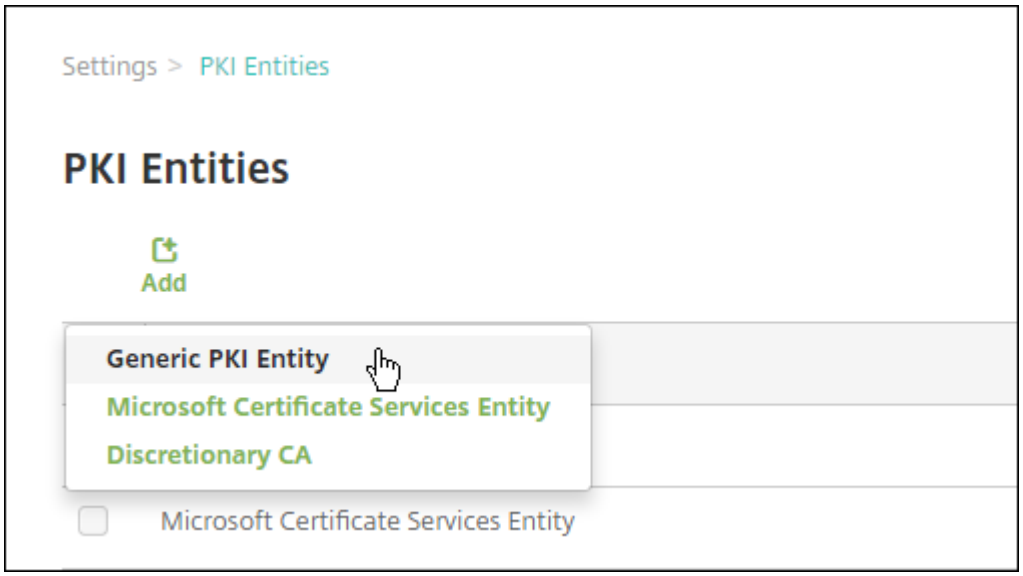
Support for each of the PKI operations in an adapter is optional. If an adapter supports a given operation, the adapter is said to have the corresponding capability (sign, fetch, or revoke). Each of these capabilities may be associated with a set of user parameters.

User parameters are parameters that the GPKI adapter defines for a specific operation and for which you must provide values to XenMobile. XenMobile 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 XenMobile and the GPKI adapter.

To add a generic PKI

1. In the XenMobile 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.

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 may 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

XenMobile Server GPKI support includes DigiCert Managed PKI, also referred to as MPKI. This section describes how to set up Windows Server and XenMobile Server for DigiCert Managed PKI.

Prerequisites

- Access to DigiCert Managed PKI Infrastructure

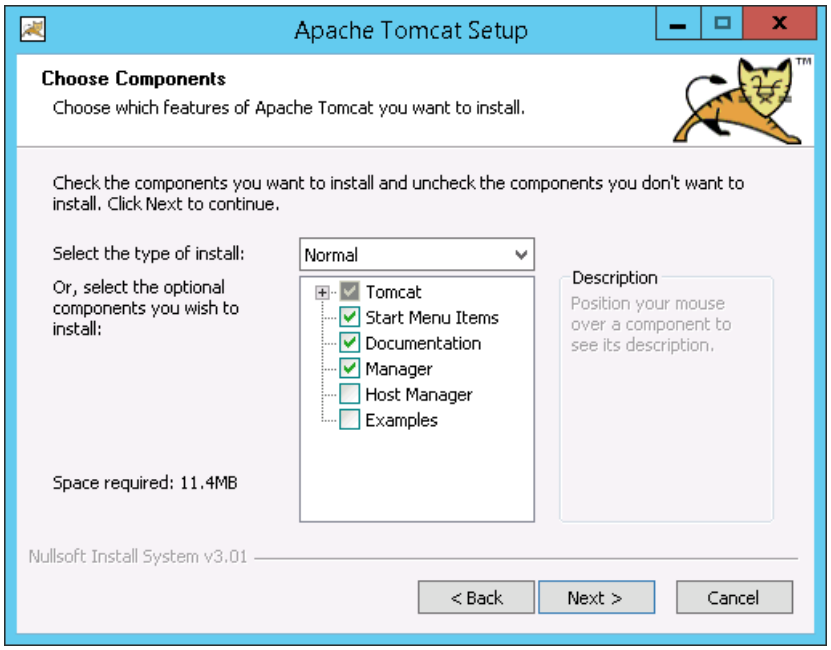
- Windows Server 2012 R2 server with the following components installed, as described in this article:
  - Java
  - Apache Tomcat
  - DigiCert PKI Client
  - Portecle
- Access to the XenMobile downloads site

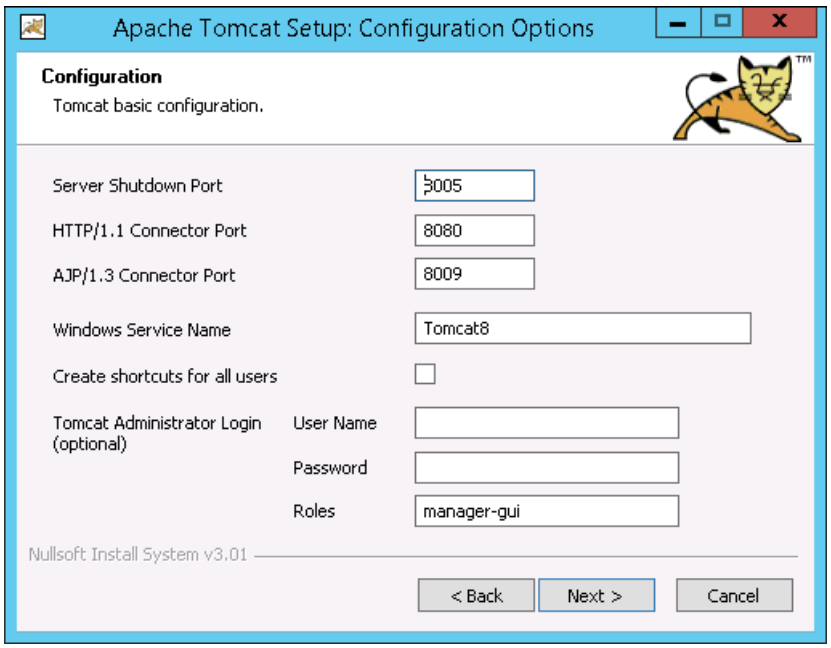
Install Java on Windows Server

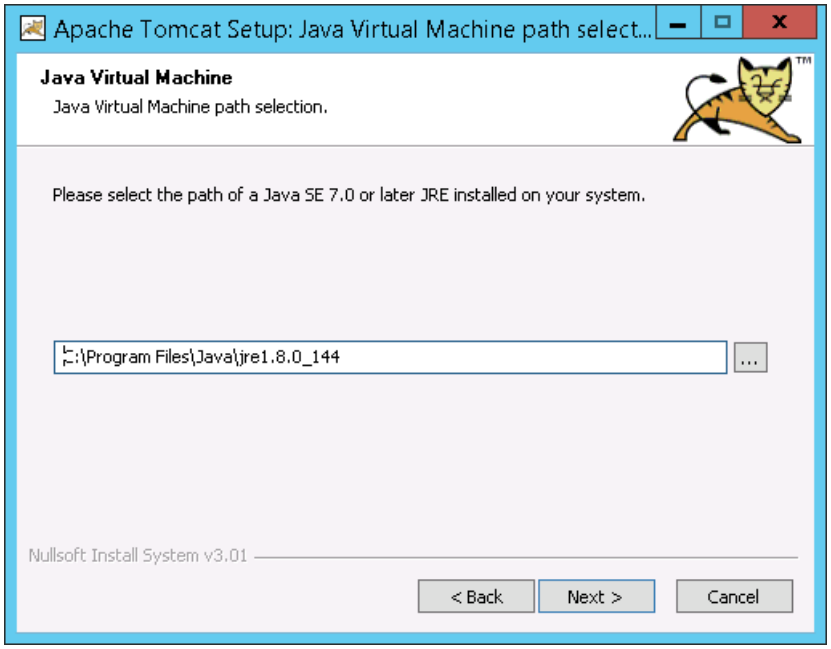
Download Java from https://java.com/en/download/faq/java_win64bit.xml and then install it. In the Security Warning dialog box, click **Run**.

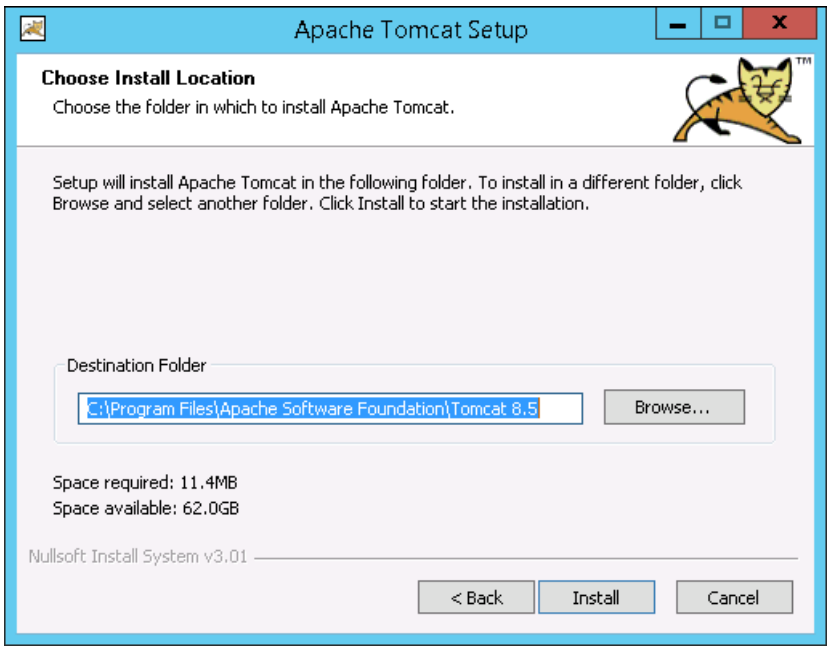
Install Apache Tomcat on Windows Server

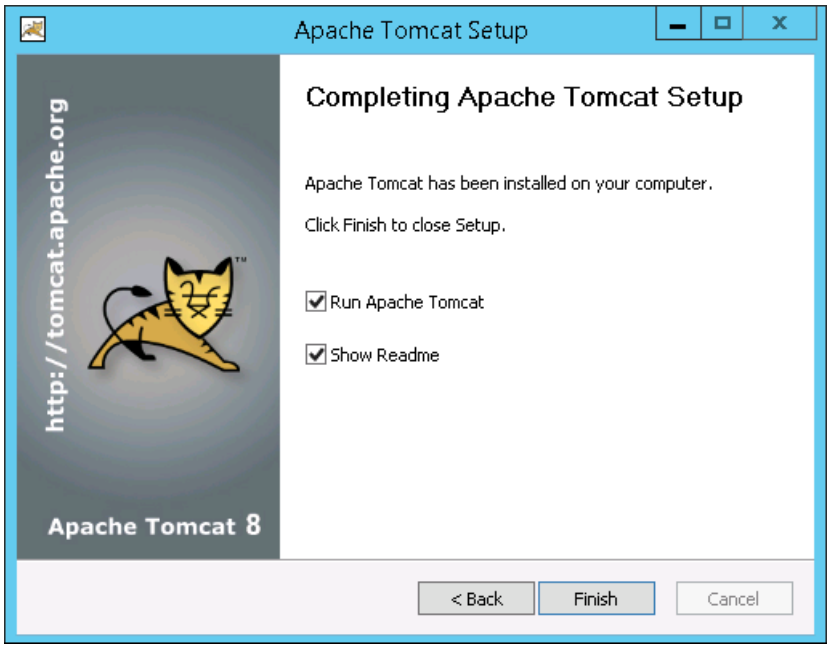
Download the Apache Tomcat 32-bit/64-bit Windows Service Installer from https://tomcat.apache.org/download-80.cgi and then install it. In the Security Warning dialog box, click **Run**. Complete the Apache Tomcat setup, using the following examples as a guide.



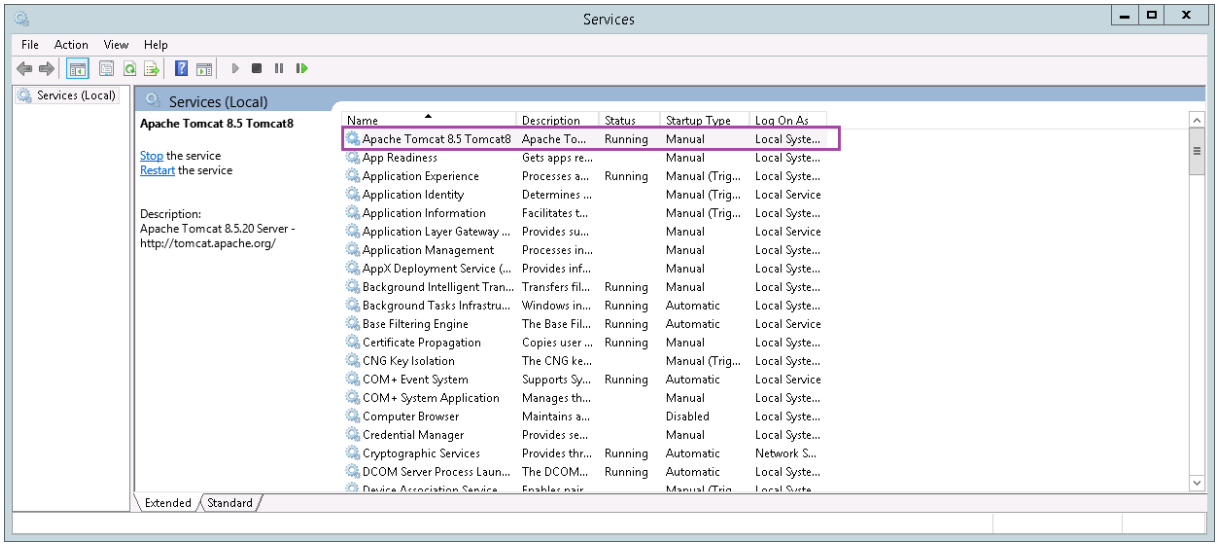


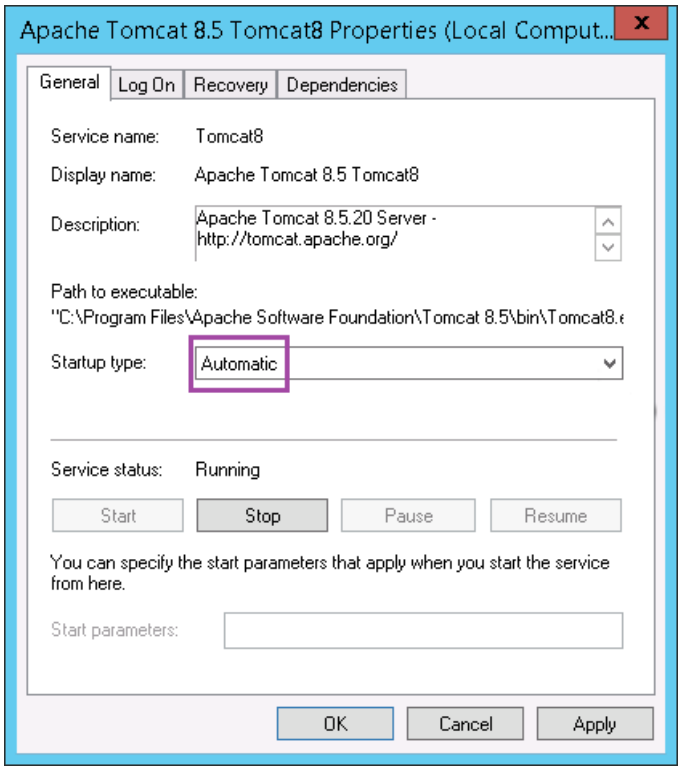






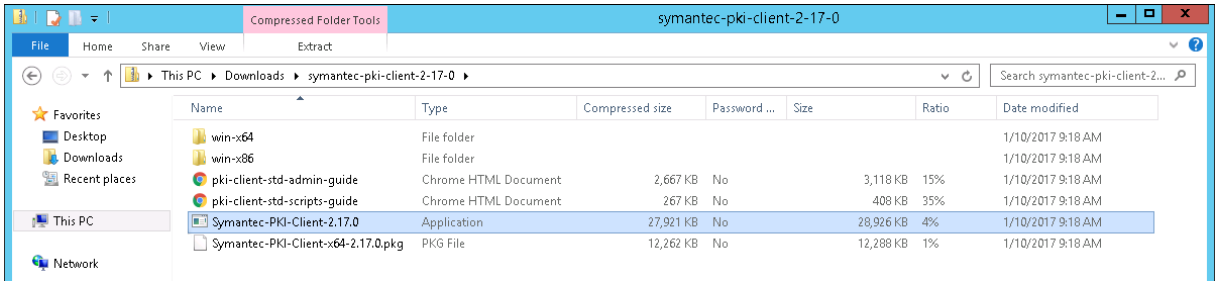
Next, go to Windows Services and change **Startup Type** from **Manual** to **Automatic**.

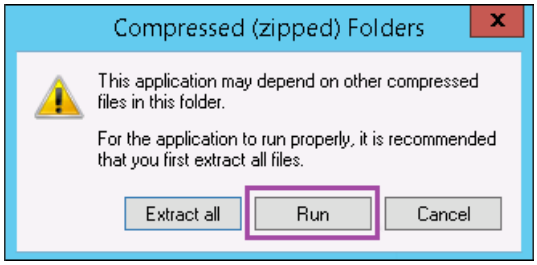




Install DigiCert PKI Client on Windows Server

Download the installer from the PKI Manager console. If you don't have access to 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

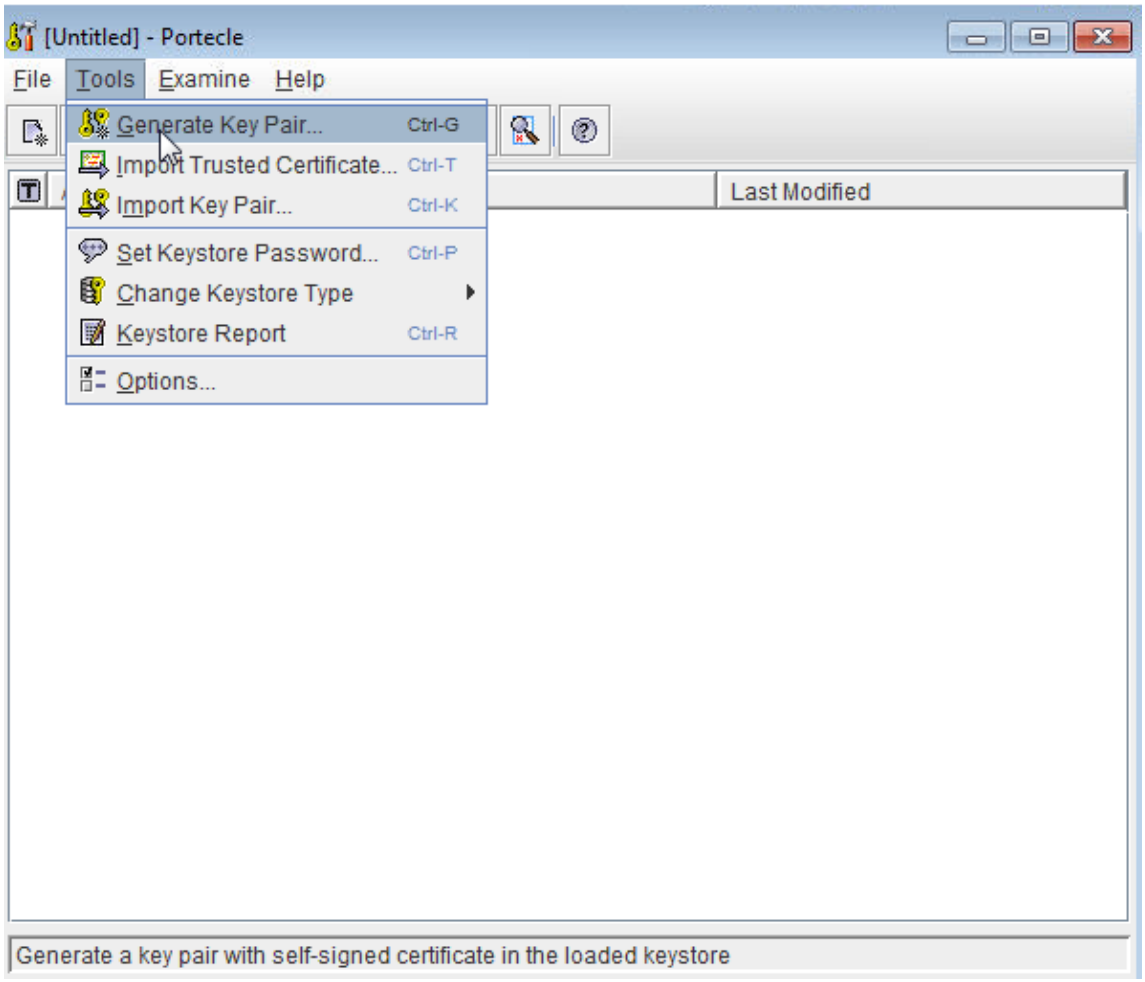
Download the installer from https://sourceforge.net/projects/portecleinstall/files/ and then unzip and run the installer.

Generate the registration authority (RA) certificate for DigiCert Managed PKI

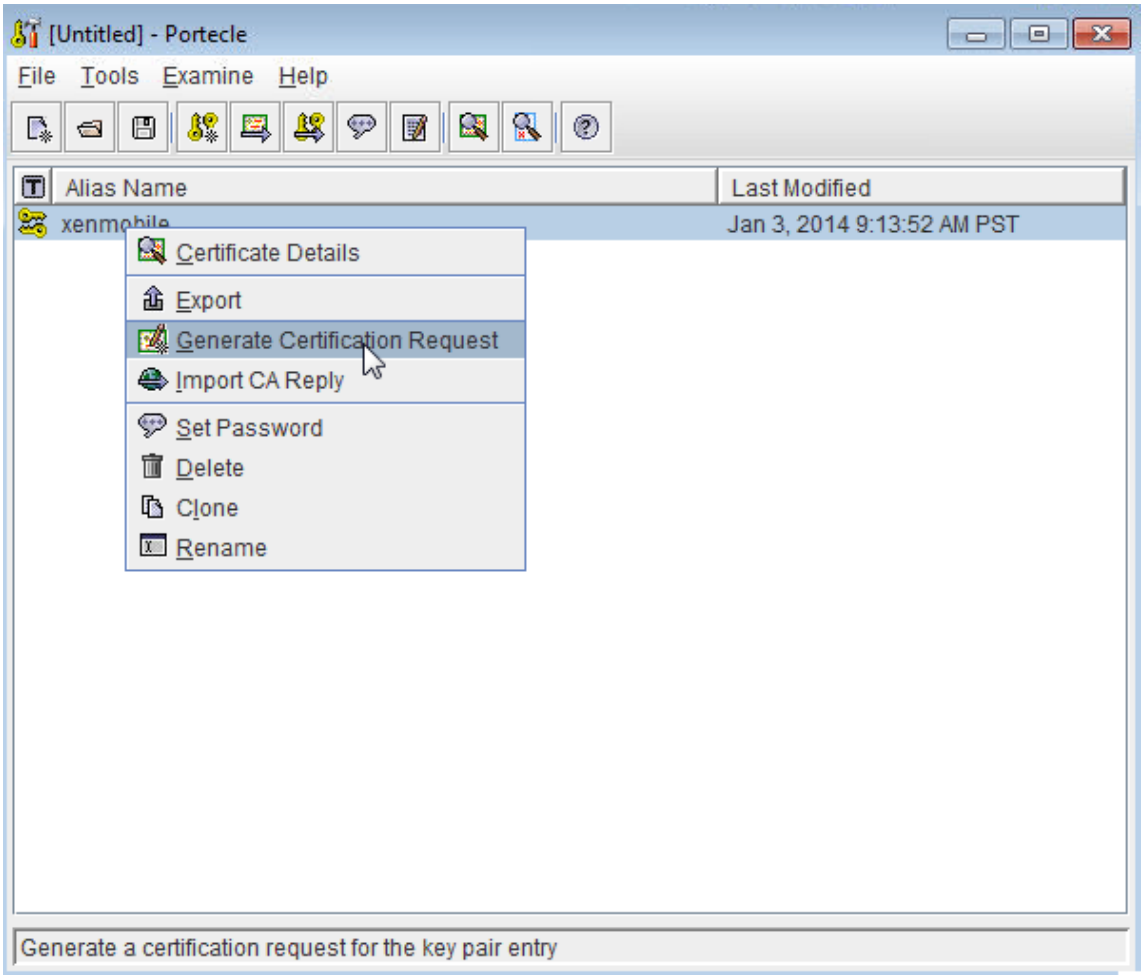
The keystore for client certificate authentication is contained in a registration authority (RA) certificate, named RA.jks. The following steps describe how to generate that certificate by using Portecle. You can also generate the RA certificate by using the Java CLI.

This article also describes how to upload the RA and public certificates.

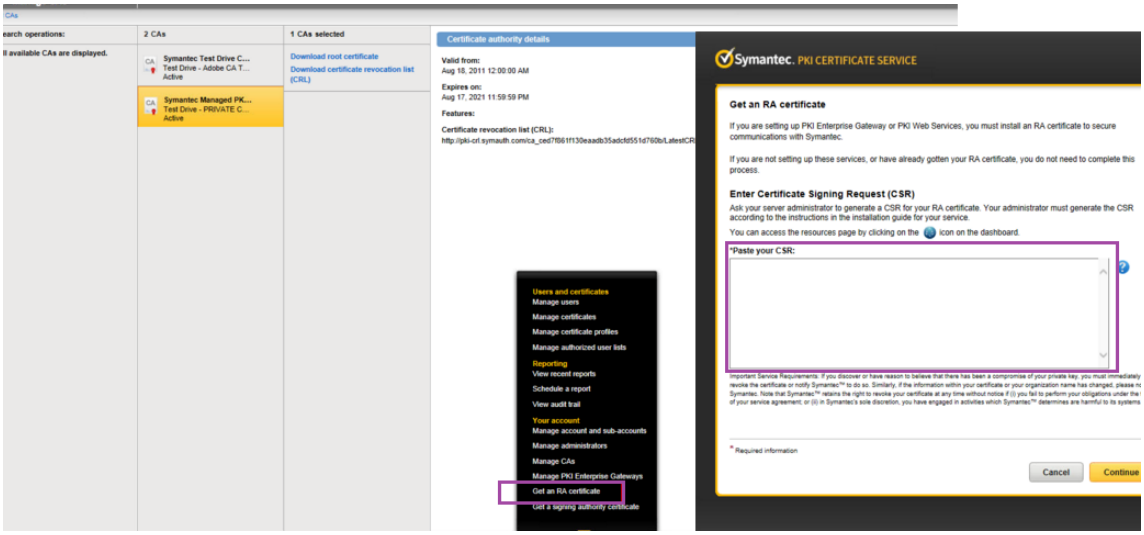
1. In Portecle, go to **Tools > Generate Key Pair**, provide the required information, and generate the key pair.



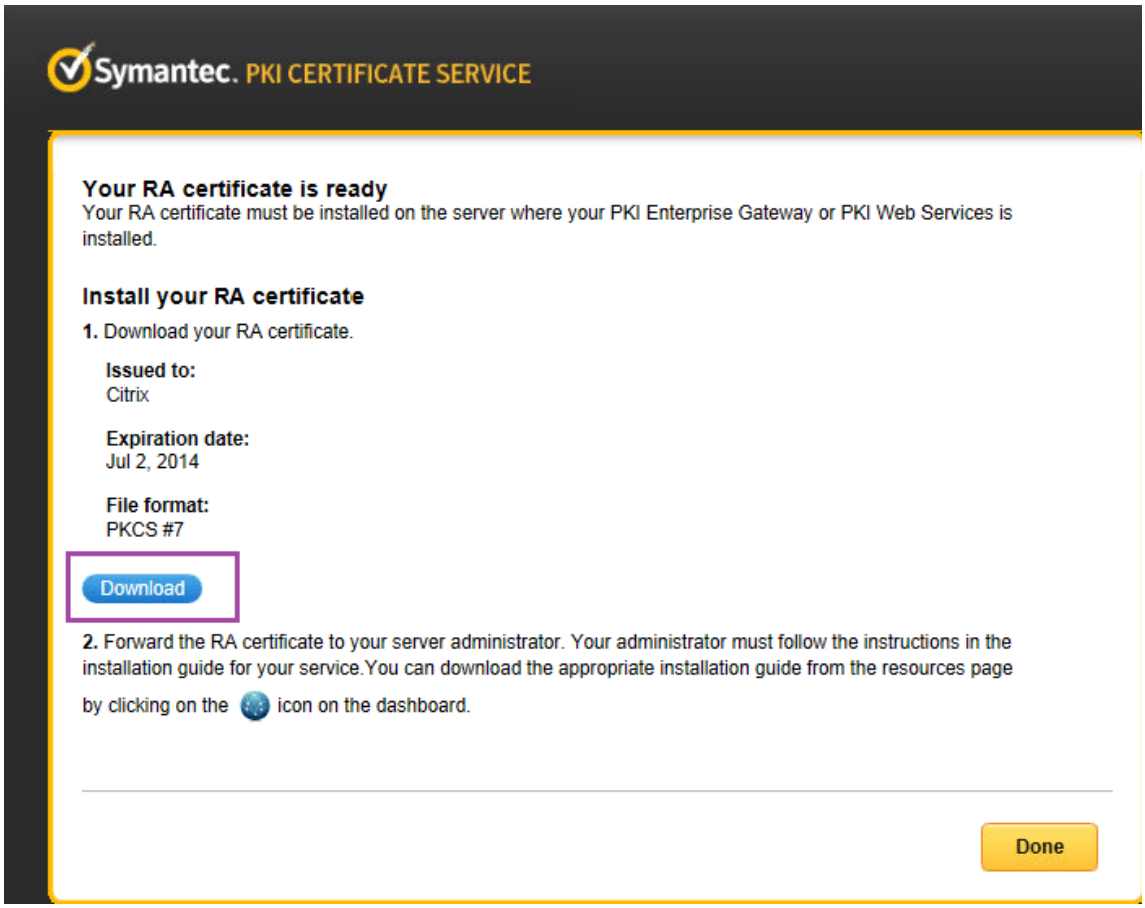
2. Right-click the key pair and then click **Generate Certification Request**.



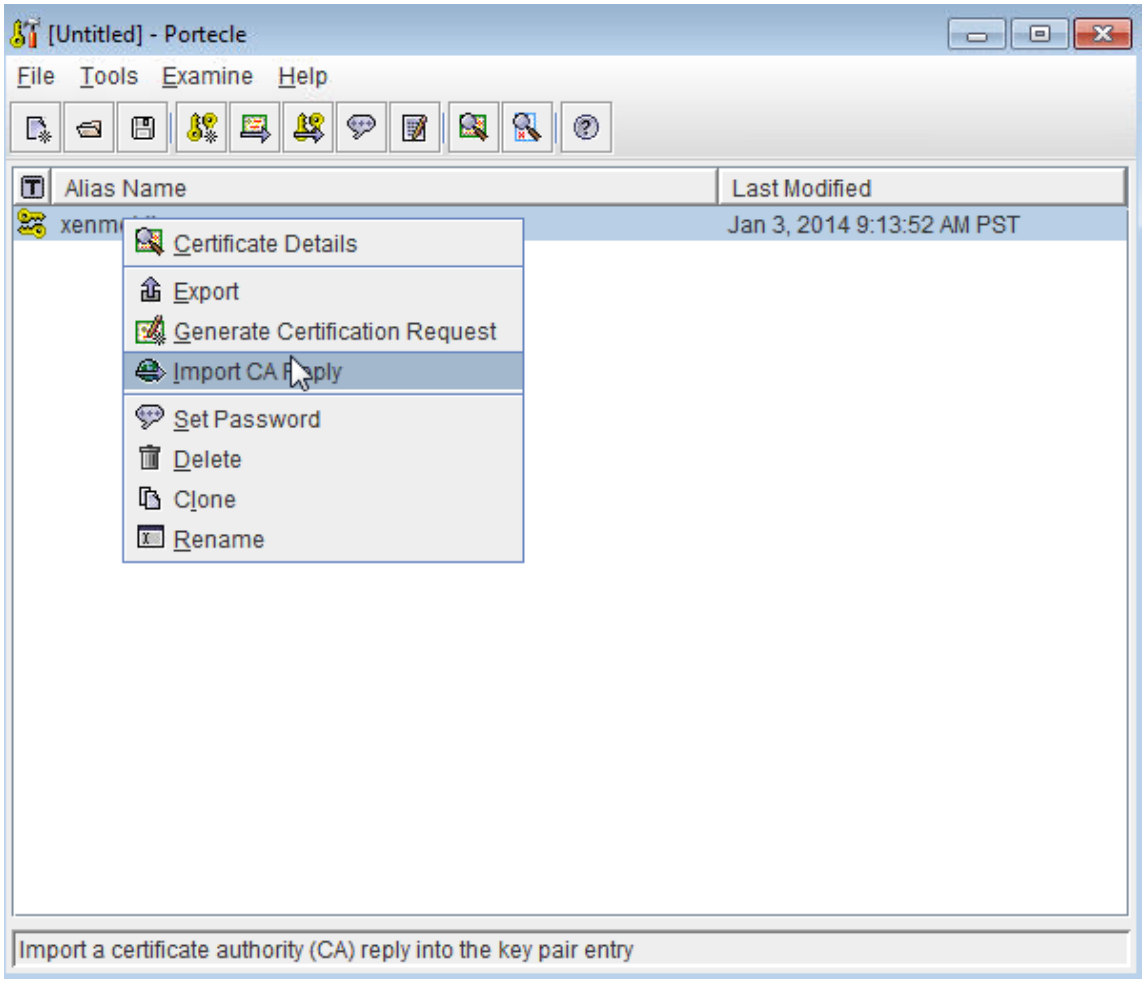
3. Copy the CSR.
4. In DigiCert PKI Manager, generate an RA certificate: Click **Settings,** click **Get a RA Certificate**, paste the CSR, and then click **Continue**.



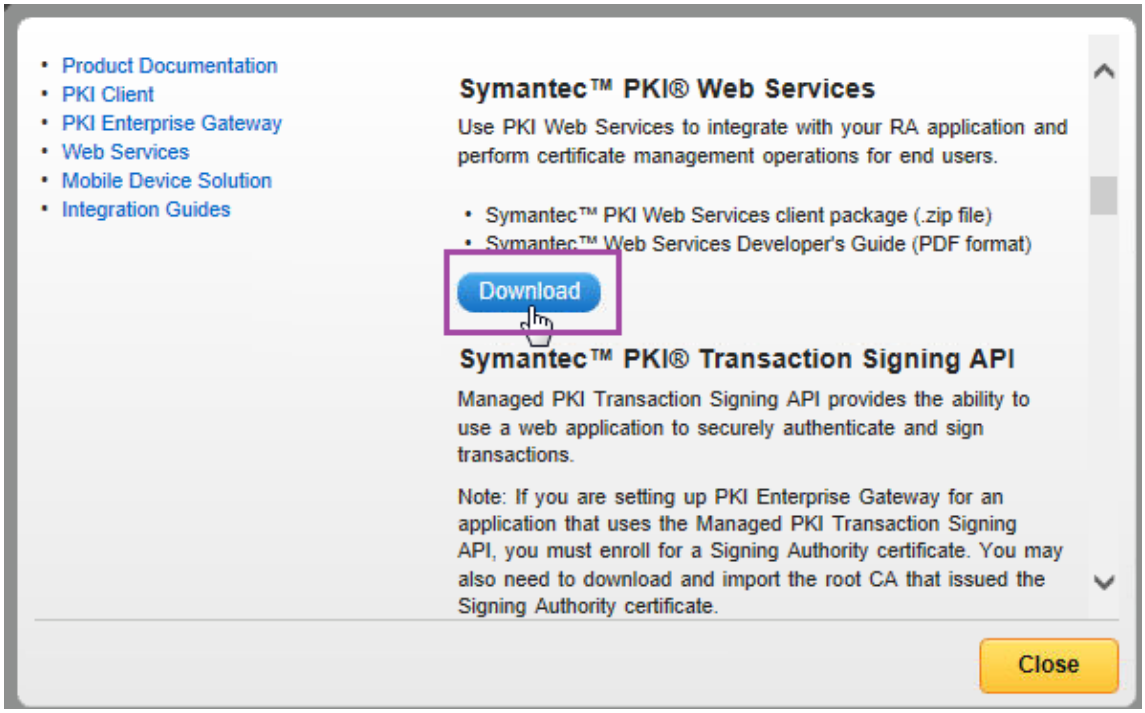
5. Click **Download** to download the generated RA certificate.



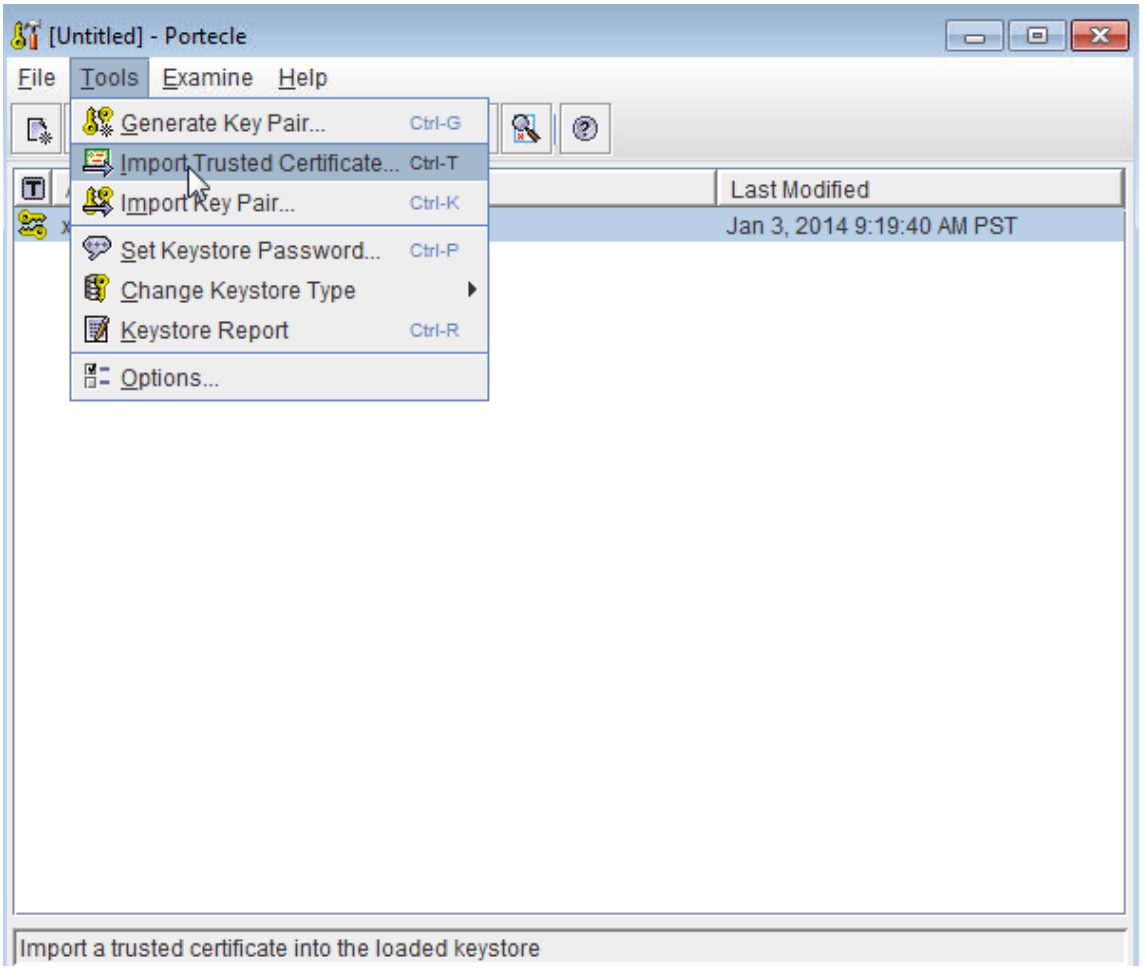
6. In Portecle, import the RA certificate: Right-click the key pair and then click **Import CA Reply**.



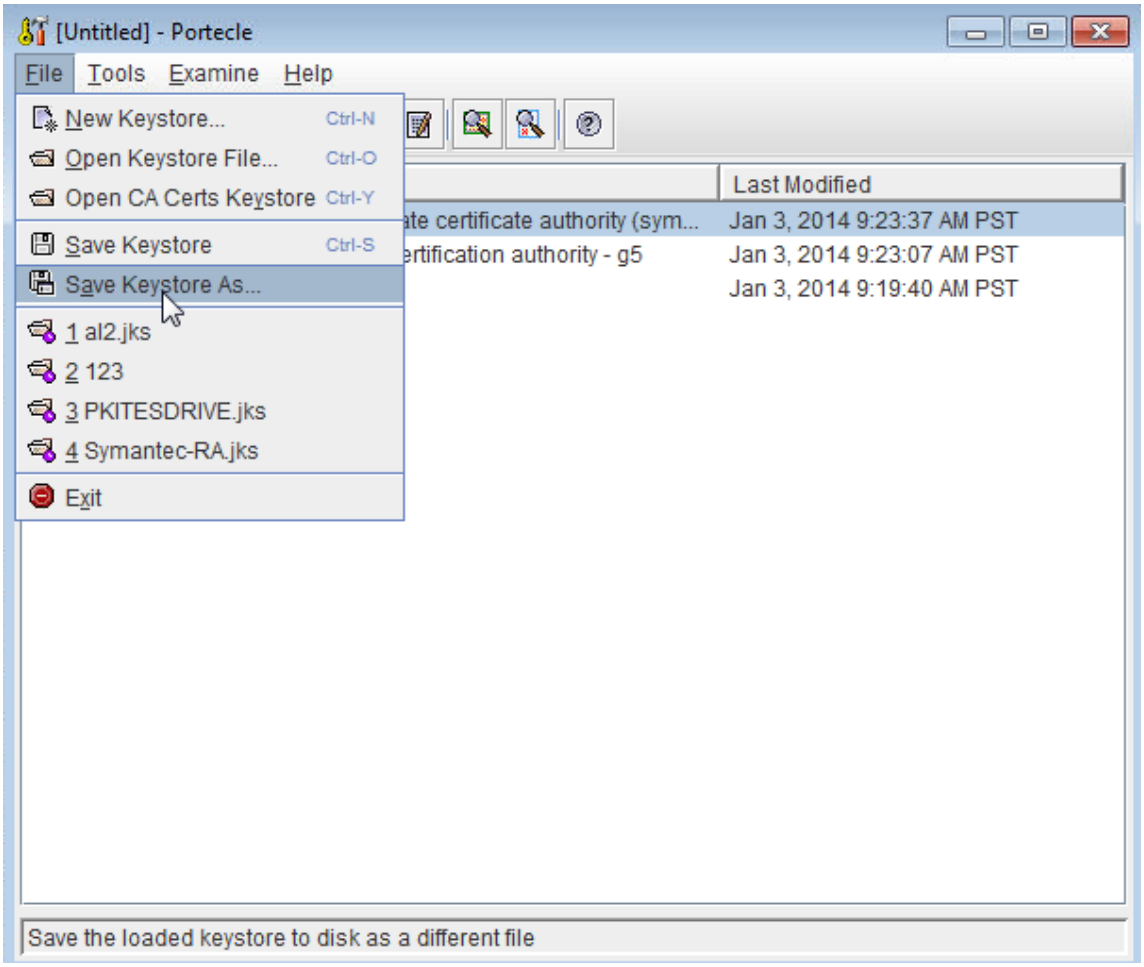
7. In DigiCert PKI Manager: Go to **Resources > Web Services** and then download the CA certificates.



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:\DigiCert folder on the Windows server.



Configure DigiCert 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

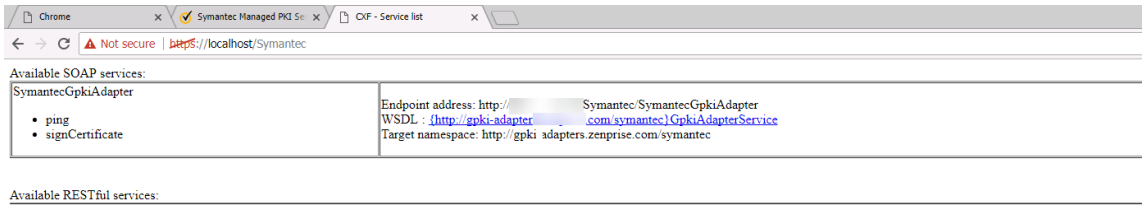
4. Open custom_gpki_adapter.properties in Notepad and edit the following values:

```
Gpki.CaSvc.Url=https://<managed PKI URL>

# keystore for client-cert auth

keyStore=C:\\Symantec\\RA.jks

# truststore for server with self-signed root CA

trustStore=C:\\Symantec\\cacerts.jks
<!--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.
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.

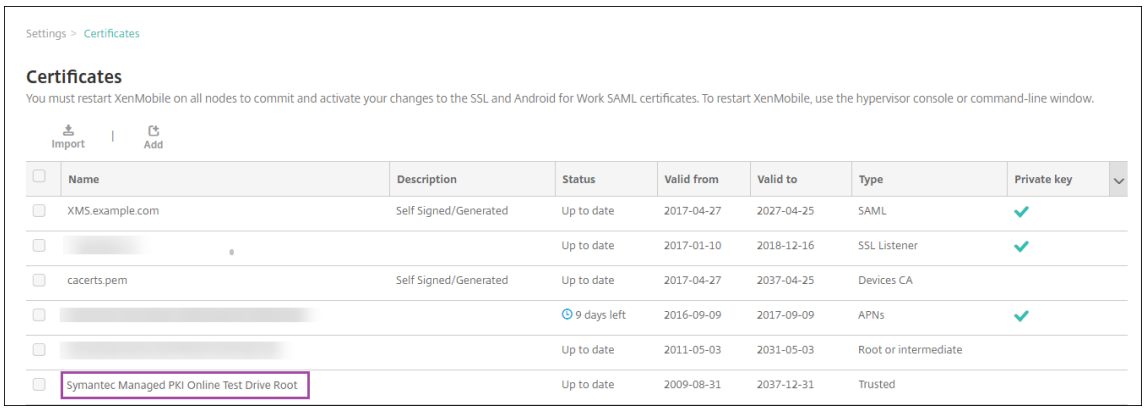


Configure XenMobile Server for DigiCert Managed PKI

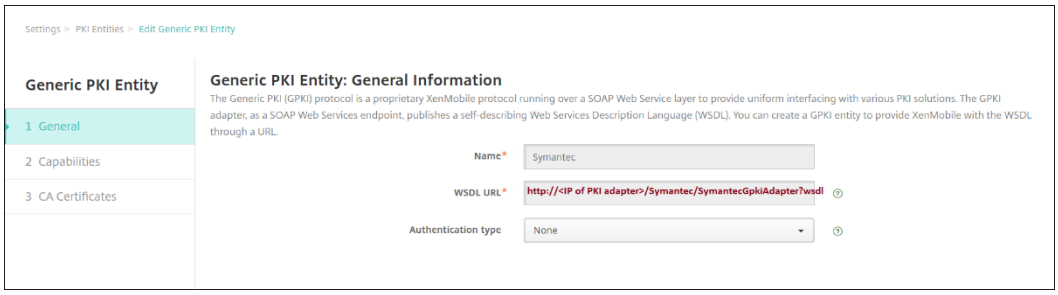
Complete the Windows Server setup before performing the following XenMobile Server configuration.

To import the DigiCert CA certificates and configure the PKI Entity

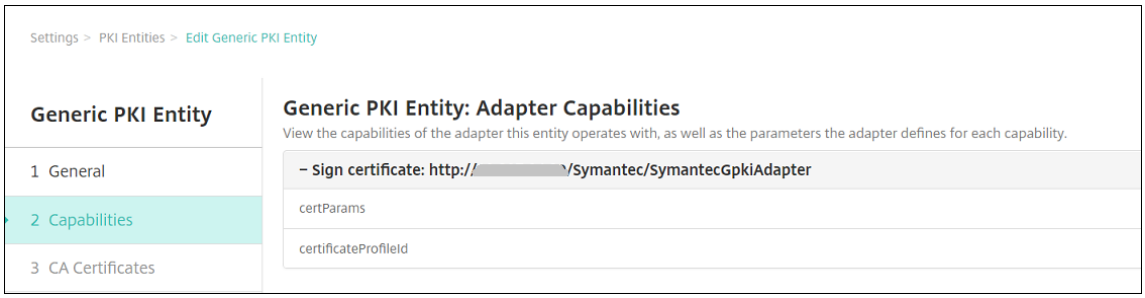
1. Import the DigiCert CA certificates that issue the end-user certificate: In the XenMobile Server console, go to **Settings > Certificates** and click **Import**.



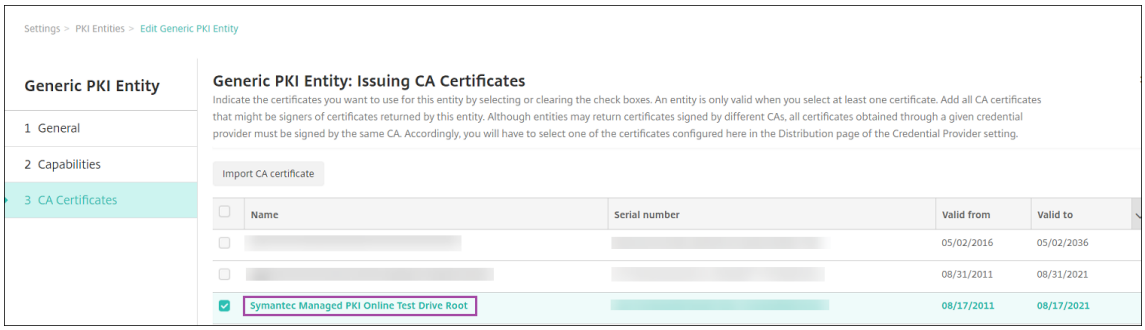
2. Add and configure the PKI Entity: Go to **Settings > PKI Entities**, click **Add**, and then choose **Generic PKI Entity**. In **WSDL URL**, paste the endpoint address that you copied when configuring the PKI adapter in the previous section, and then append `?wsdl` as shown below.



3. Click **Next**. XenMobile populates the parameter names from the WSDL.



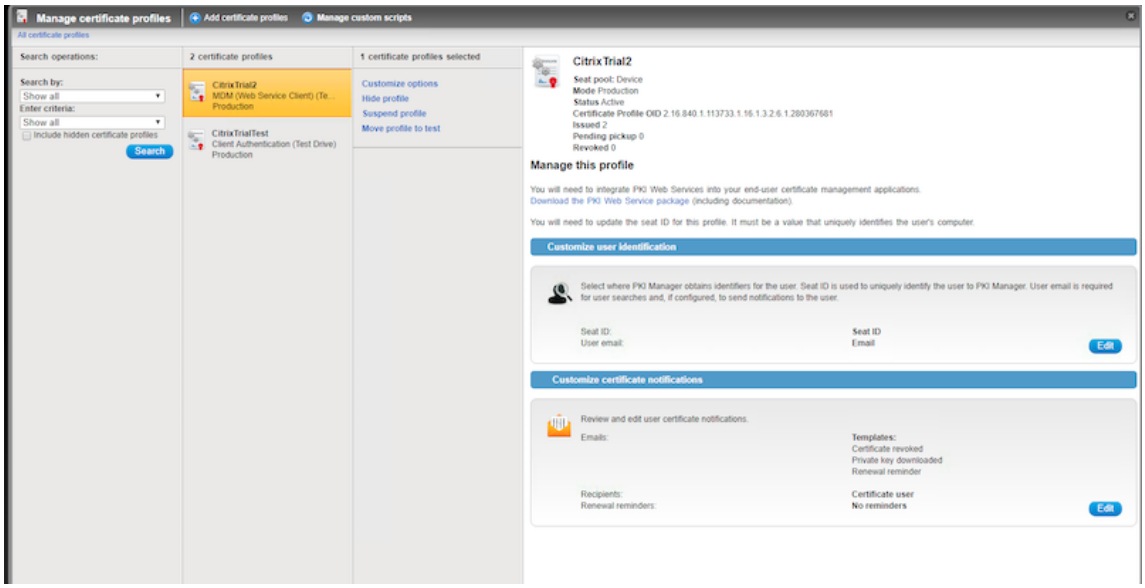
4. Click **Next**, select the correct CA certificate, and then click **Save**.



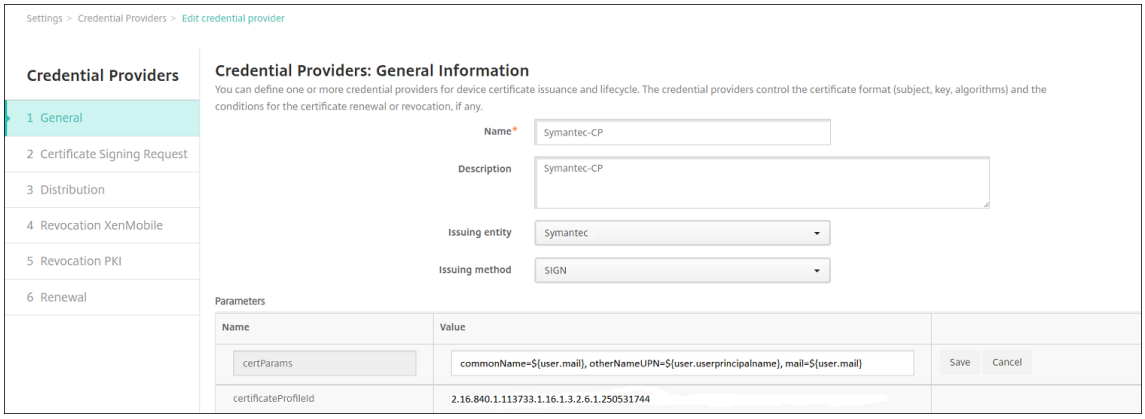
5. On the **Settings > PKI Entities** page, verify that the **State** of the PKI Entity you added is **Valid**.

To create the credential provider for DigiCert Managed PKI

1. In the DigiCert PKI Manager console, copy the **Certificate Profile OID** from the Certificate Template.



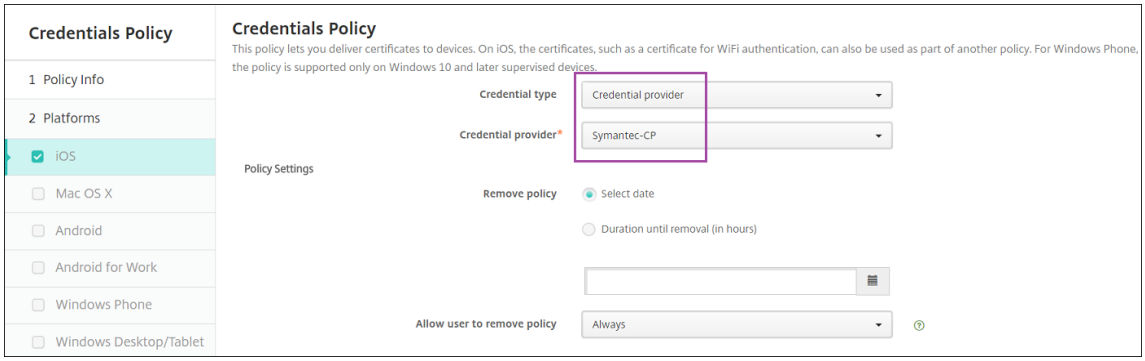
2. In the XenMobile Server console, go to **Settings > Credential Providers**, click **Add**, and then configure the settings as follows.
   - **Name:** Type a unique name for the new provider configuration. This name is used to refer to the configuration in other parts of the XenMobile console.
   - **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.userpri**
   - **certificateProfileid:** Paste the Certificate Profile OID that you copied in Step 1.



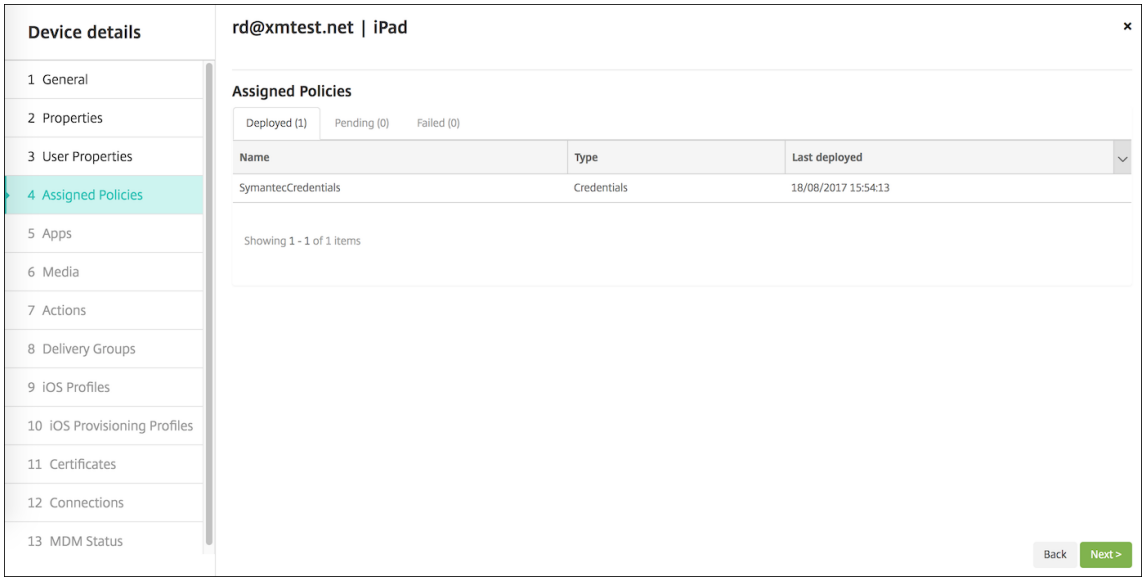
3. Click **Next**. On each of the remaining pages (Certificate Signing Request through Renewal), accept the default settings. When you are finished, click **Save**.

To test and troubleshoot the configuration

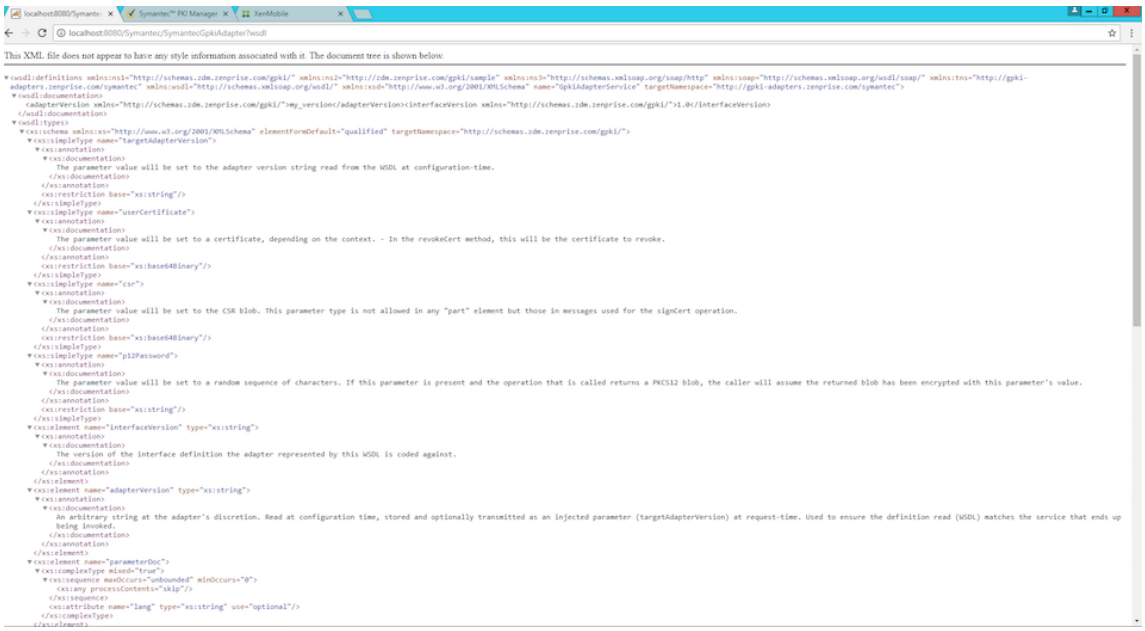
1. Create a Credentials device policy: Go to **Configure > Device Policies**, click **Add**, start typing **Credentials**, and then click **Credentials**.
2. Specify a **Policy Name**.
3. Configure the platform settings as follows:
   - **Credential type:** Choose **Credential Provider**.
   - **Credential provider:** Choose the DigiCert 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.



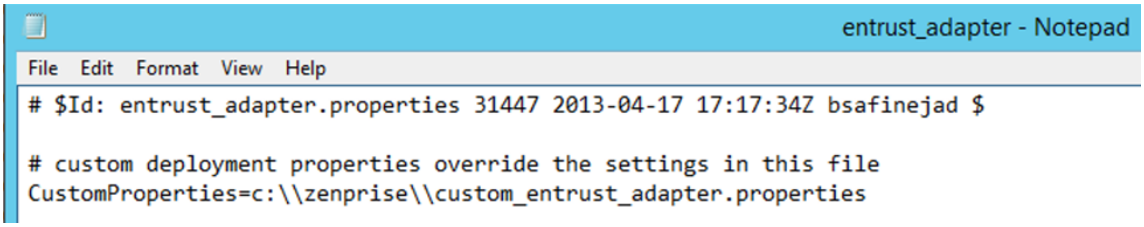
For more troubleshooting information, check the Tomcat logs in `<tomcat dir>\logs\catalina.<current date>`.

Entrust PKI adapter

As an alternative to DigiCert Managed PKI, you can install the Entrust PKI adapter. Prior to installing the adapter, see the steps for installing Java and Apache Tomcat on Windows Server in the DigiCert Managed PKI section of this article.

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 > 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 a zenprise directory and a new file called custom_entrust_adapter.properties.
4. Edit the file with the following content, taking care to replace the Entrust.MdmSvc.URL, AdminUserId, and AdminPassword appropriately.

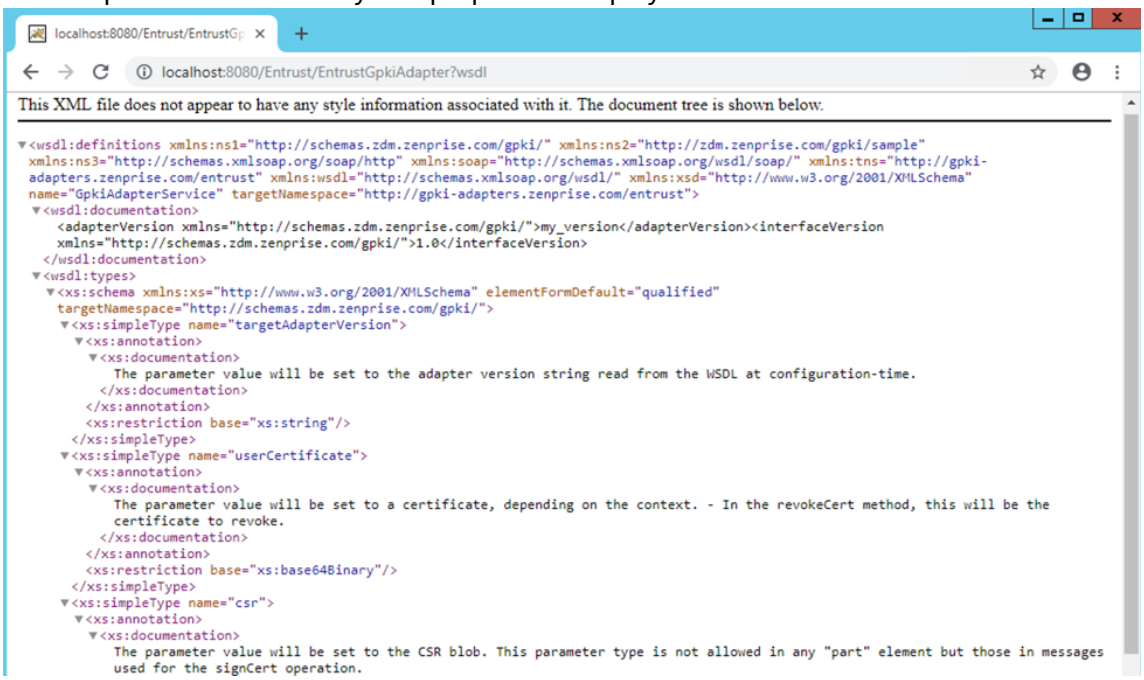
~
# set the following to the proper URL for AS/IG
Entrust.MdmSvc.Url=https://pki.yourcorp.com:19443/mdmws/services/AdminServiceV8

```
# set to 1 or true to force user creation from passed user and
    group parameters if using IG and user does not exist
CreateUser=

# set the credentials for the endpoint
AdminUserId=`[User ID]`
AdminPassword=`[password]`


# keystore for client-cert auth
#keyStore=
#keyStorePassword=
#keyStoreType: JKS, JCEKS and PKCS12  -- not needed for .p12 and .
    jks files

# truststore for server with self-signed root CA
```



```
#trustStore=
#trustStorePassword=
#trustStoreType: JKS, JCEKS and PKCS12  -- not needed for .p12 and
    .jks files
~
```

5. 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`
6. Navigate to `http://localhost:8080/Entrust/EntrustGpkiAdapter?wsdl` or your server's public URL. and verify that proper XML displays.



Configure XenMobile for the Entrust PKI adapter

1. Log in to your XenMobile console and navigate to **Settings > PKI Entities**. Click **Add > Generic PKI Entity**.
2. Enter the following information:
   - **Name:** - Enter a name for the PKI Entity.
   - **WSDL URL:** 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.
    - **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 OSes 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

XenMobile interfaces with Microsoft Certificate Services through its web enrollment interface. XenMobile 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 XenMobile, you must specify the base URL of the Certificate Services web interface. If you choose, use SSL client authentication to secure the connection between XenMobile and the Certificate Services web interface.

Add a Microsoft Certificate Services entity

1. In the XenMobile 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://192.0.2.13/certsrv/`. The URL may 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.

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. XenMobile 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 XenMobile to add to the HTTP request to the 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 XenMobile of the signers of the certificates that the system obtains through this entity. When your CA certificate is renewed, update it in XenMobile. XenMobile 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 ADC Certificate Revocation List (CRL)

XenMobile supports Certificate Revocation List (CRL) only for a third-party Certificate Authority. If you have a Microsoft CA configured, XenMobile uses Citrix ADC to manage revocation.

When you configure client certificate-based authentication, consider whether to configure the Citrix ADC 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.

XenMobile 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 XenMobile with a CA certificate and the associated private key. XenMobile 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, and only 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 XenMobile 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 XenMobile OCSP responder service supports basic OCSP responses and the following hashing algorithms in requests:

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Responses are signed with SHA-256 and the signing certificate key algorithm (DSA, RSA, or ECDSA).

Add discretionary CAs

1. In the XenMobile 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**.

   A menu of PKI entity types appears.
3. Click **Discretionary CA**.

   The **Discretionary CA: General Information** page appears.
4. On the **Discretionary CA: General Information** page, do 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 XenMobile at **Configure > Settings > Certificates**.
5. Click **Next**.

   The **Discretionary CA: Parameters** page appears.
6. On the **Discretionary CA: Parameters** page, do 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 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**.

   The **Discretionary CA: Distribution** page appears.

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**.

   The **Discretionary CA: Online Certificate Status Protocol (OCSP)** page appears.

   On the **Discretionary CA: Online Certificate Status Protocol (OCSP)** page, do 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 OSCP signing CA certificate. This list of certificates is generated from the CA certificates you uploaded to XenMobile.

10. Click **Save**.

    The discretionary CA appears on the PKI Entities table.

Credential providers

March 5, 2021

Credential providers are the actual certificate configurations you use in the various parts of the XenMobile 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, XenMobile does not issue certificates before enrollment, although XenMobile 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 XenMobile 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 XenMobile 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 XenMobile may be sent to the back-end public key infrastructure (PKI). That is, certificate revocation in XenMobile 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. XenMobile 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 XenMobile, is a recovery of an existing key pair. XenMobile 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 XenMobile: 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, XenMobile acts like a delegate (a registrar) to the actual certificate authority. XenMobile 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 XenMobile.

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 XenMobile 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 XenMobile:

Context	SCEP supported	SCEP required
iOS Profile Service	Yes	Yes
iOS mobile device management enrollment	Yes	No
iOS configuration profiles	Yes	No
SHTP enrollment	No	No
SHTP configuration	No	No
Windows Phone and Tablet enrollment	No	No

Context	SCEP supported	SCEP required
Windows Phone and Tablet configuration	No, except for the Wifi device policy, which is supported for Windows Phone 8.1 and the latest Windows 10 release	No

Certificate Revocation

There are three types of revocation.

- **Internal revocation:** Internal revocation affects the certificate status as maintained by XenMobile. XenMobile considers this status when evaluatating 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 XenMobile, this type of revocation applies to certificates obtained from an external PKI. The certificate is revoked on the PKI when XenMobile 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 XenMobile evaluates a given certificate status, XenMobile queries the PKI as to that status. If the certificate is revoked, XenMobile 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.

XenMobile 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, XenMobile 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 XenMobile, is an internal entity. The issuing method for a discretionary entity is always sign. Sign means that with each issuing operation, XenMobile 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 XenMobile 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 XenMobile 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 1024 bits. To avoid false negatives, which depends on the underlying hardware and software, XenMobile 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 XenMobile 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 XenMobile 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 XenMobile** page appears. On this page, you configure the conditions under which XenMobile internally flags certificates, issued through this provider configuration, as revoked.

9. On the **Credential Providers: Revocation XenMobile** page, do the following:

   - In **Revoke issued certificates**, select one of the options indicating when to revoke certificates.
   - To direct XenMobile 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 XenMobile: 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 XenMobile, 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 XenMobile 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 XenMobile 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 XenMobile to do the following:

    - Renew the certificate. You can optionally send a notification 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. XenMobile doesn't renew certificates after they are internally revoked.

    To direct XenMobile to send a notification when the certificate has been renewed: Set **Send notification** to **On**. To direct XenMobile to send a notification when the certification nears ex-

piration: 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 23, 2021

> **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 10.13.0, XenMobile Server 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.

To enroll and manage iOS and macOS devices in XenMobile, you set up an Apple Push Notification service (APNs) certificate from Apple.

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 XenMobile 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 XenMobile
- **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 reenrollment.
> - 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 and 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.

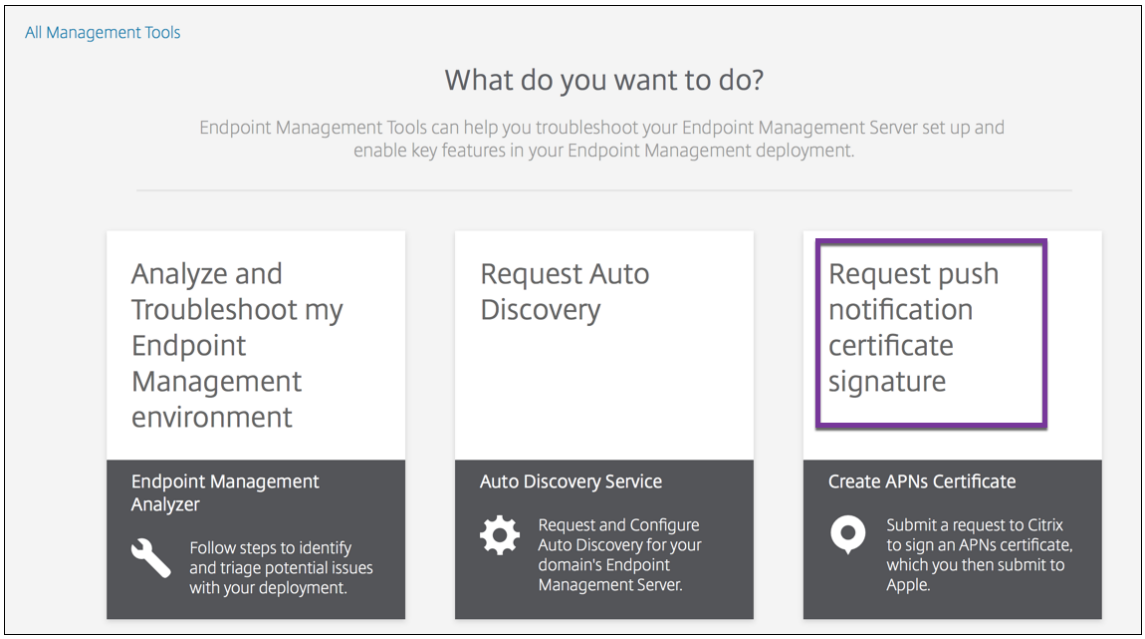
```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
<!--NeedCopy-->
```

4. To continue, sign the CSR as described in the next section.

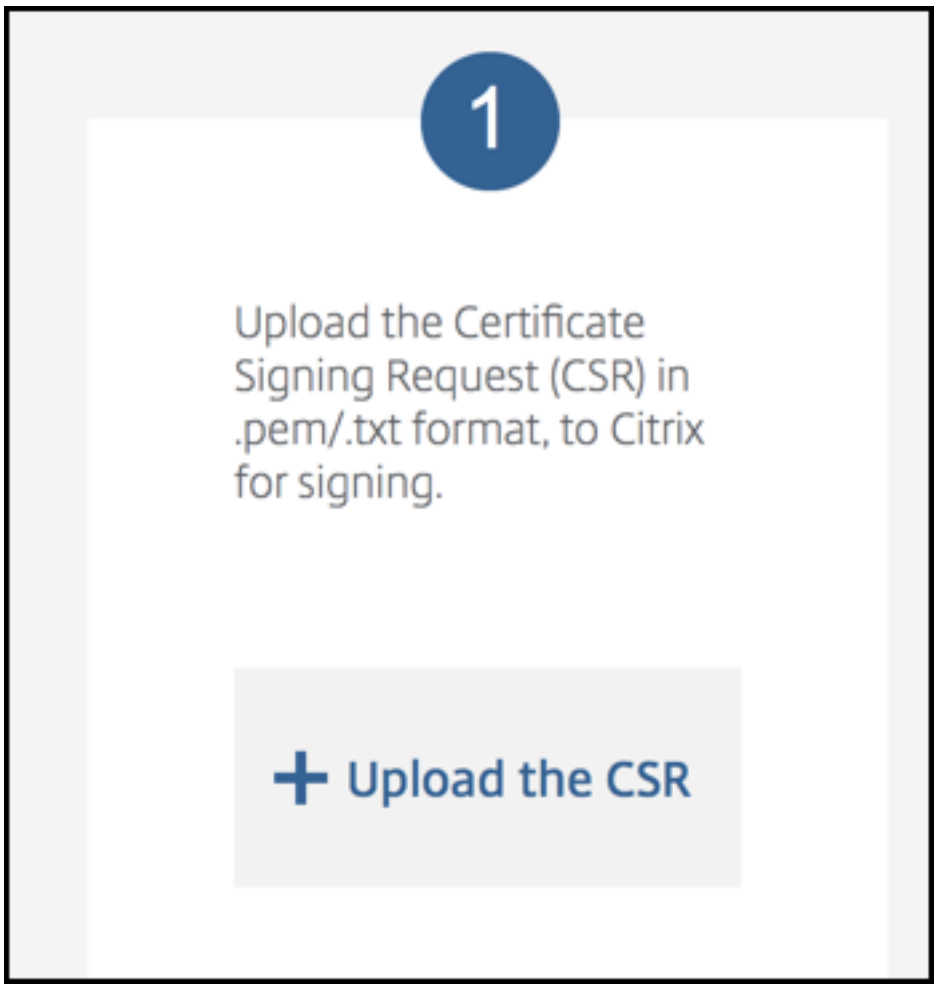
Sign the CSR

To use a certificate with XenMobile, 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 XenMobile.

> **Note:**
>
> Some users have reported problems logging into the Apple Push Portal. As an alternative, log on to the Apple Developer Portal and 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 PCKS #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 PCKS #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 XenMobile. 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 XenMobile server.
8. To continue, see Import an APNs certificate into XenMobile.

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 XenMobile.
7. Copy the .pfx certificate to the server on which you plan to install XenMobile.
8. To continue, see Import an APNs certificate into XenMobile.

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 XenMobile.
3. Note the location for the .pfx certificate file. Then, copy the file to the XenMobile server so you can use the console to upload the file.
4. To continue, import an APNs certificate into XenMobile as described in the next section.

Import an APNs certificate into XenMobile

After you receive the new APNs certificate: Import the APNs certificate into XenMobile to either add the certificate for the first time or to replace a certificate.

1. In the XenMobile 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 XenMobile, 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.

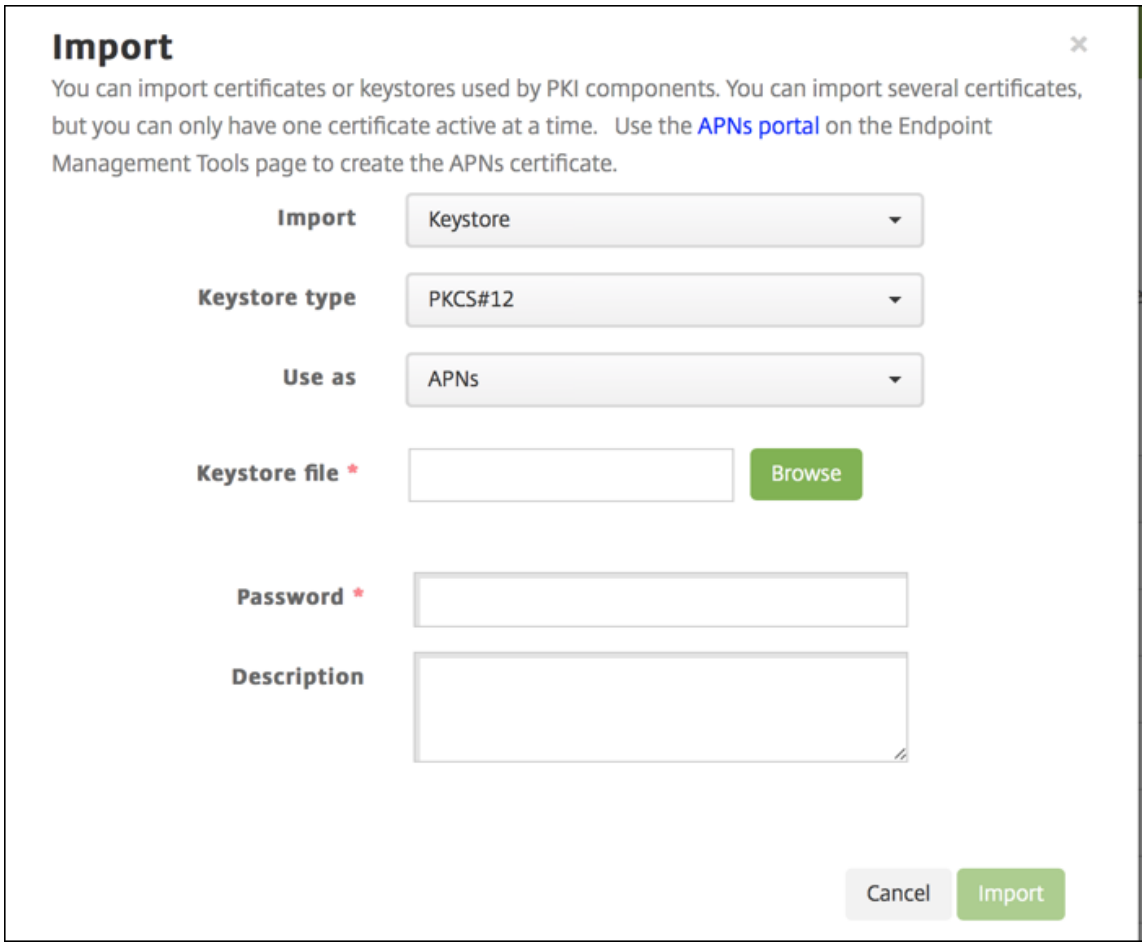
To determine when your APNs certificate expires, in the XenMobile console, go to **Settings > Certificates**. If the certificate expires, do not revoke it.

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 XenMobile 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.

9. Using that .pem file, complete the CSR (according to the method you used to create the CSR in Step 1).
10. Export the certificate as a .pfx file.

In the XenMobile console, import the .pfx file and complete the configuration as follows:

1. Go to **Settings > Certificates > Import**.
2. From the **Import menu**, choose **Keystore**.
3. From the **Keystore type** menu, choose **PKCS #12.**
4. From **Use as**, choose **APNs**.



5. For **Keystore file**, click **Browse** and navigate to the file.
6. In **Password**, type the certificate password.
7. Type an optional **Description**.
8. Click **Import**.

XenMobile 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

February 24, 2021

You can configure XenMobile and Citrix 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 Service or 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 through the Citrix Files mobile app are 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 XenMobile. XenMobile 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 XenMobile as a SAML identity provider (IdP) to Content Collaboration, you must configure XenMobile to use with Enterprise accounts, as described in this article. Alternatively, you can configure XenMobile to work only with storage zone connectors. For more information, see Use Citrix Content Collaboration with XenMobile.

For a detailed reference architecture diagram, see Architecture.

Prerequisites

Complete the following prerequisites before you can configure SSO with XenMobile and Citrix Files apps:

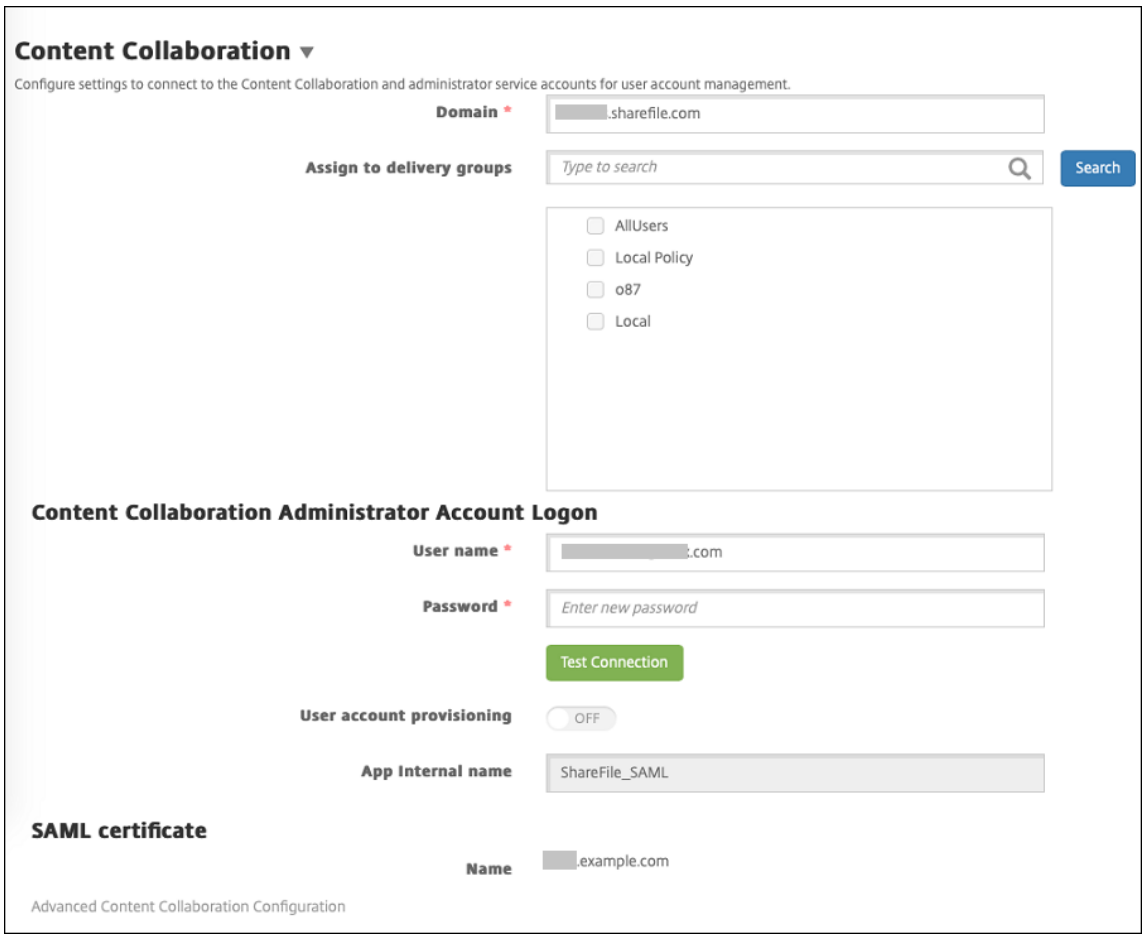
- The MAM SDK, MDX Service, or a compatible version of the MDX Toolkit (for Citrix Files mobile apps).

  For more information, see XenMobile compatibility.
- A compatible version of Citrix Files mobile apps and Secure Hub.
- Content Collaboration administrator account.
- Connectivity verified between XenMobile and Content Collaboration.

Configure Content Collaboration access

Before setting up SAML for Content Collaboration, provide Content Collaboration access information as follows:

1. In the XenMobile web console, click **Configure > ShareFile**. The **ShareFile** configuration page appears. Your console might show the term Content Collaboration instead of ShareFile.



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 Content Collaboration.
   - **ShareFile 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**.
   - XenMobile syncs with Content Collaboration and updates the Content Collaboration settings **ShareFile Issuer/Entity ID** and **Login URL**.
   - The **Configure > ShareFile** 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 wrapped Citrix Files MDX apps. 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.

The following steps apply to iOS and Android apps and devices. To configure SAML for wrapped Citrix Files MDX apps:

1. With the MDX Toolkit, wrap the Citrix Files mobile app. For more information about wrapping apps with the MDX Toolkit, see Wrapping Apps with the MDX Toolkit.
2. In the XenMobile console, upload the wrapped Citrix Files mobile app. For information about uploading MDX apps, see To add an MDX app to XenMobile.
3. Verify the SAML settings: Log on to Content Collaboration with the administrator user name and password you configured earlier.
4. Verify that Content Collaboration and XenMobile are configured for the same time zone. Ensure that XenMobile 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 XenMobile 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 XenMobile Store, download, install, and set up Secure Mail.

3. Open a new email form and then tap **Attach from Citrix Files**. Files available to attach to the email are shown without asking for user name or password.

Configure the Citrix Gateway for Other Citrix Files Clients

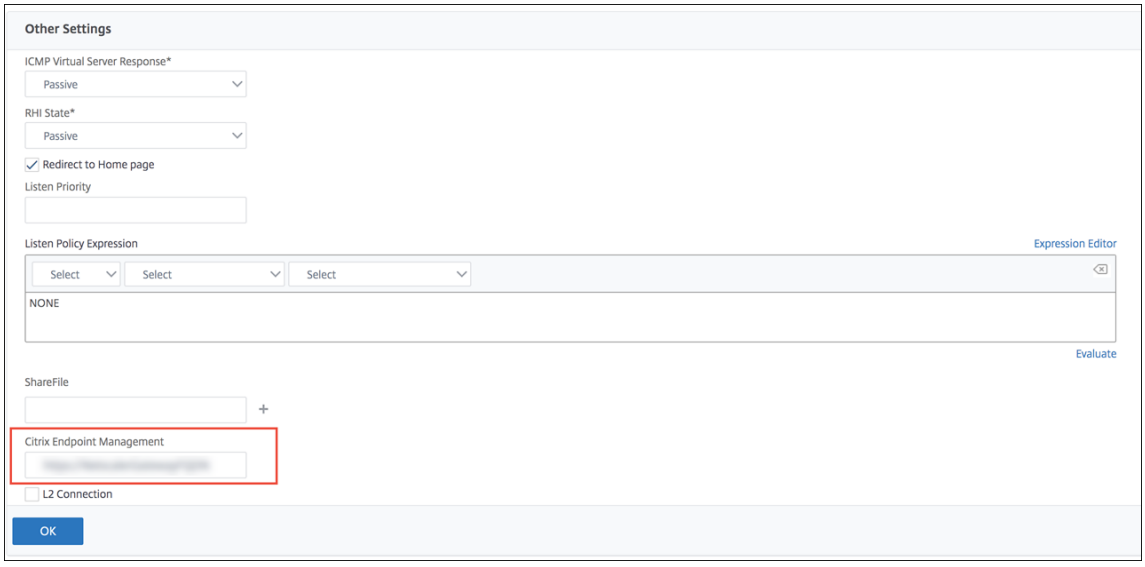
To configure access for non-wrapped Citrix Files clients, such as the website, Outlook plug-in, or the sync clients: Configure Citrix Gateway to support the use of XenMobile as a SAML identity provider as follows.

- 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 XenMobile logons. In Citrix ADC, go to **Other Settings** and then clear the check box labeled **Redirect to Home Page**.



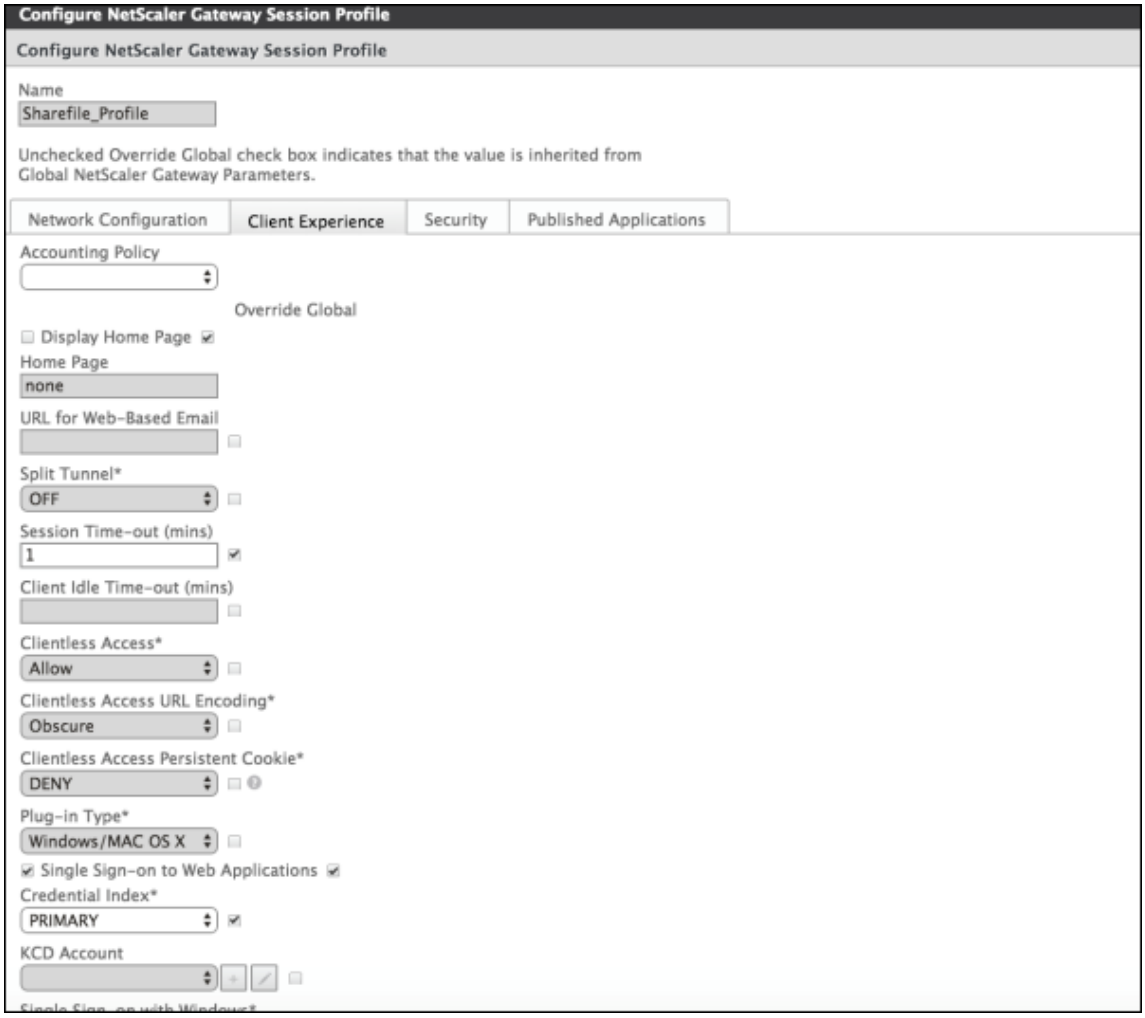
2. Under **ShareFile** (now called Content Collaboration), type your XenMobile internal server name and port number.
3. Under **Citrix Endpoint Management**, type your XenMobile URL. Your version of Citrix Gateway may refer to the older product name **AppController**.

   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:

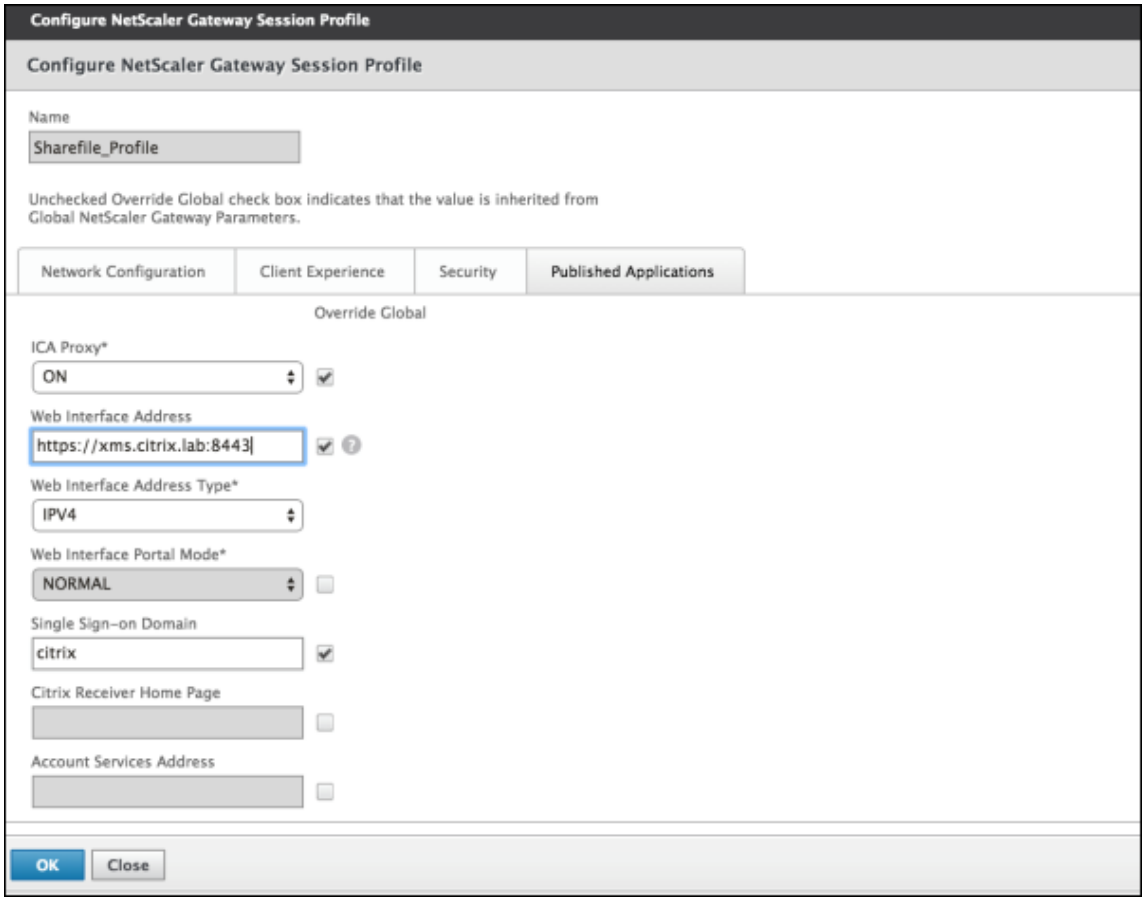
1. In the Citrix Gateway configuration utility, in the left-hand navigation pane, click **Citrix Gateway > Policies > Session**.
2. Create a session policy. On the **Policies** tab, click **Add**.
3. In the **Name** field, type **ShareFile_Policy**.
4. Create an action by clicking the **+** button. The **Create Session Profile** page appears.



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.

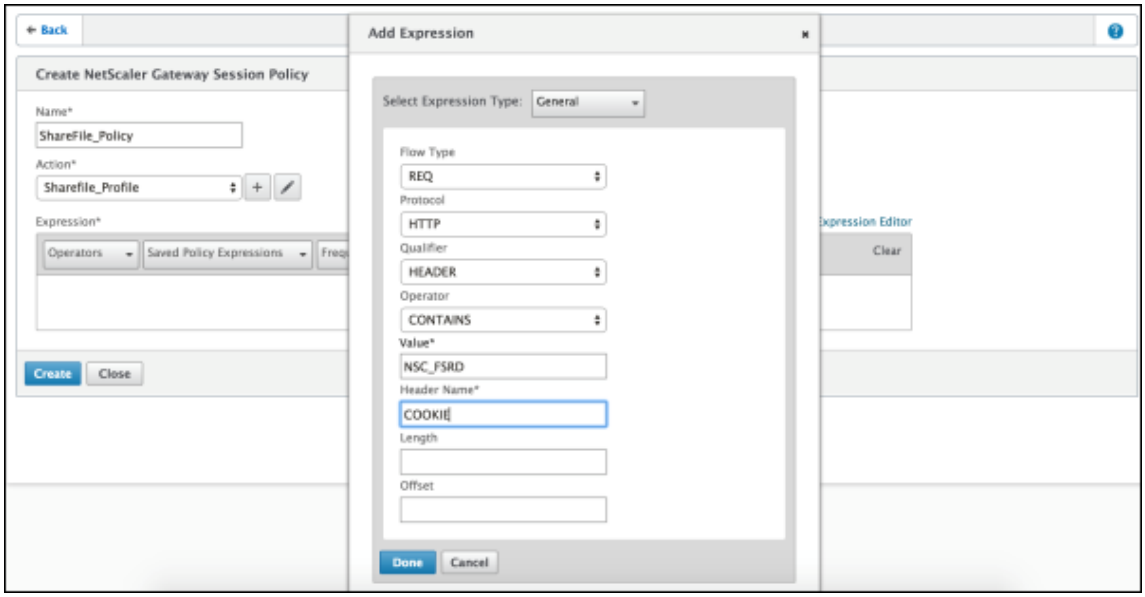


Configure these settings:

- **ICA Proxy:** Click **ON**.
- **Web Interface Address:** Type your XenMobile 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 XenMobile 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**.

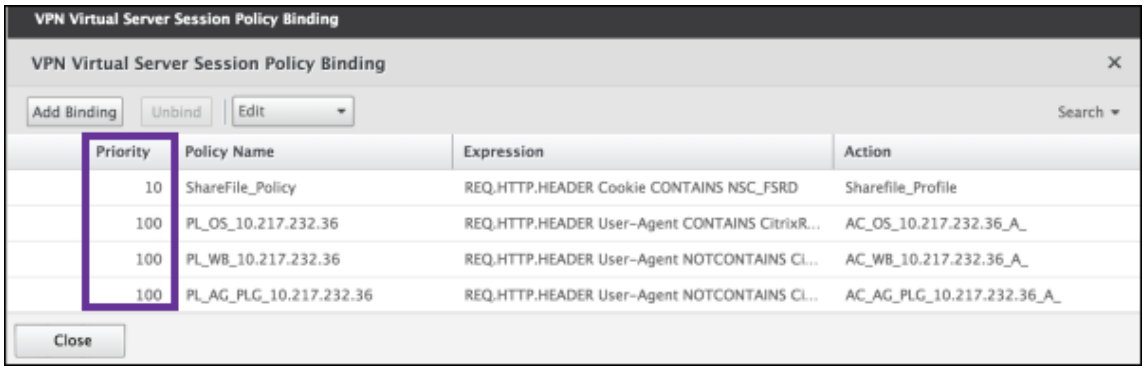
7. Click **Create** and then click **Close**.

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 **Citrix 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:



7. Click **Done** and then save the running Citrix ADC configuration.

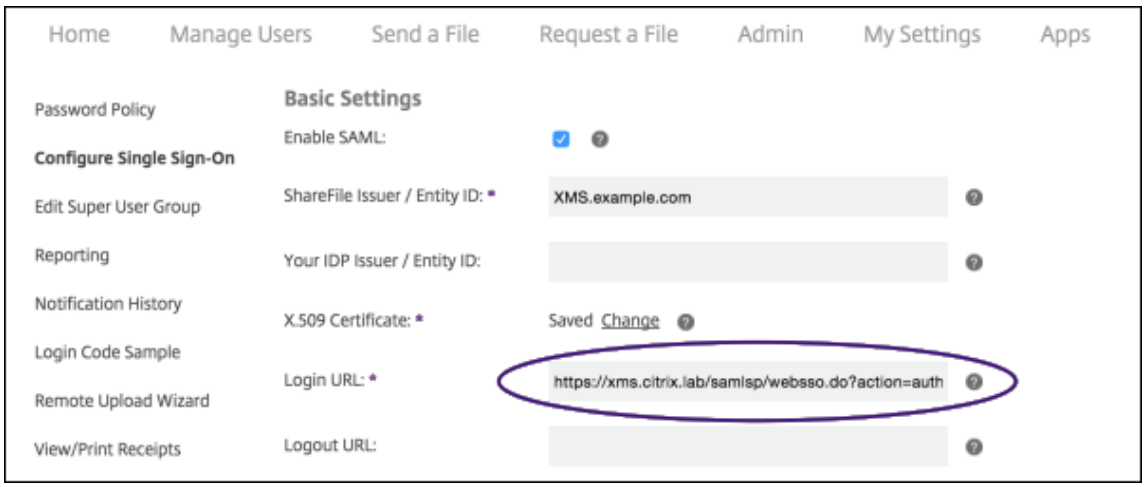
Modify the Citrix Files.com SSO settings

Make the following changes for both MDX and non-MDX Citrix Files apps.

> **Important:**
>
> A new number is appended the internal application name:
>
> - Each time you edit or recreate the Citrix Files app
> - Each time you change the Content Collaboration settings in XenMobile
>
> 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`.



- Insert the Citrix Gateway virtual server external FQDN plus **/cginfra/https/** in front of the XenMobile Server FQDN and then add **8443** after the XenMobile 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`

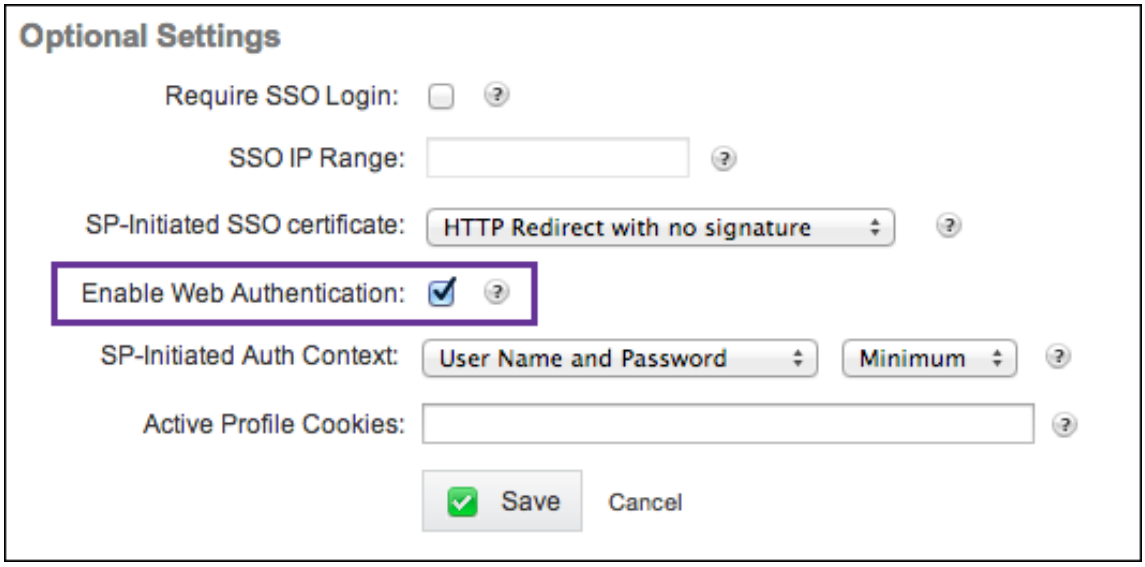
- Change the parameter `&app=ShareFile_SAML_SP` to the internal Citrix Files application name. The internal name is `ShareFile_SAML` by default. However, every time you change your configuration, a number is appended to the internal name (`ShareFile_SAML_2`, `ShareFile_SAML_3`, and so on). You can look up the **App internal name** on the **Configure > ShareFile** 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.



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 XenMobile environment you configured.

   Your Citrix Files folders at `<subdomain>.sharefile.com` appear. If you do not see your Citrix Files folders, ensure that you entered the proper logon credentials.

Azure Active Directory as IdP

May 11, 2021

Configuring Azure Active Directory (AAD) as your identity provider (IdP) lets users enroll in XenMobile using their Azure credentials.

iOS, Android, and Windows 10 devices are supported. iOS and Android devices enroll through Secure Hub. This authentication method is available only to users enrolling in MDM through Citrix Secure Hub. Devices enrolling in MAM can't authenticate using AAD credentials. To use Secure Hub with MDM+MAM, configure XenMobile to use Citrix Gateway for MAM enrollment. For more information, see Citrix Gateway and XenMobile.

You configure Azure as your IdP under **Settings > Authentication > IDP**. The **IDP** page is new to this version of XenMobile. In previous versions of XenMobile, you configured Azure under **Settings > Microsoft Azure**.

Requirements

- Versions and licenses
  - To enroll iOS or Android devices, you need Secure Hub 10.5.5.
  - To enroll Windows 10 devices, you need Microsoft Azure Premium licenses.
- Directory services and authentication
  - XenMobile Server must be configured for certificate-based authentication.
  - If you are using Citrix ADC for authentication, Citrix ADC must be configured for certificate-based authentication.
  - Secure Hub authentication uses Azure AD and honors the authentication mode defined on Azure AD.
  - XenMobile Server must connect to Windows Active Directory (AD) using LDAP. Configure your local LDAP server to sync with Azure AD.

Authentication flow

When device enrolls through Secure Hub and XenMobile is configured to use Azure as its IdP:

1. Users enter their Azure Active Directory user name and password, on their device, in the Azure AD login screen shown in Secure Hub.
2. Azure AD validates the user and sends an ID token.
3. Secure Hub shares the ID token with XenMobile Server.
4. XenMobile validates the ID token and the user information present in the ID token. XenMobile returns a session ID.

Azure account setup

To use Azure AD as your IdP, first log in to your Azure account and make these changes:

1. Register your custom domain and verify the domain. For details, see Add your own domain name to Azure Active Directory.
2. Extend your on-premises directory to Azure Active Directory using directory integration tools. For details, see Directory Integration.

To use Azure AD to enroll Windows 10 devices, make the following changes to your Azure account:

1. Make the MDM a reliable party of Azure AD. To do so, click **Azure Active Directory > Applications** and then click **Add**.
2. Select **Add an application** from the gallery. Go to **MOBILE DEVICE MANAGEMENT** and then select **on-premises MDM application**. Save the settings.

   You choose on-premises application even if you signed up for Citrix XenMobile cloud. In Microsoft terminology, any non-multi-tenant application is an on-premises MDM application.
3. In the application, configure XenMobile Server discovery, terms of use endpoints, and APP ID URI:

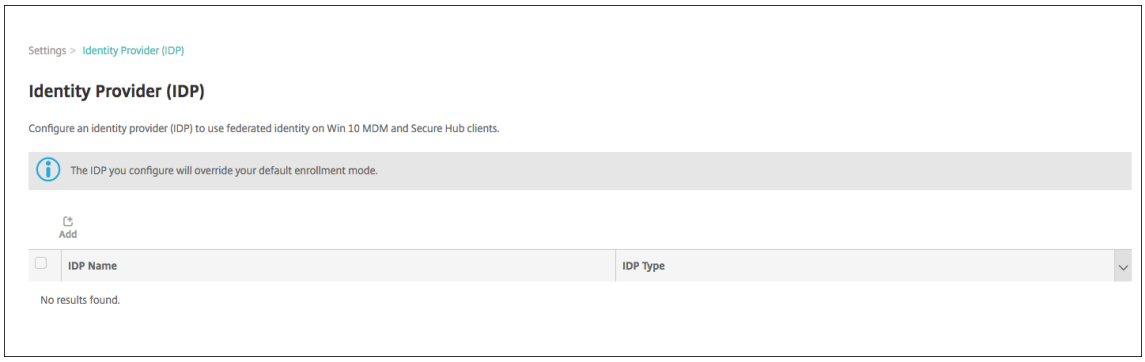
   - **MDM Discovery URL:** `https://<FQDN>:8443/<instanceName>/wpe`
   - **MDM Terms of Use URL:** `https://<FQDN>:8443/<instanceName>/wpe/tou`
   - **APP ID URI:** `https://<FQDN>:8443/`
4. Select the on-premises MDM application that you created in step 2. Enable the option, **Manage devices for these users**, to enable MDM management for all users or any specific user group.

   For more information about using Azure AD with Windows 10 devices, see the Microsoft article Azure Active Directory integration with MDM.

Configure Azure AD as your IdP

1. Locate or make note of the information you need from your Azure account:

   - Tenant ID from the Azure application settings page.
   - If you want to use Azure AD to enroll Windows 10 devices, you also need:
     - **App ID URI:** The URL for the server running XenMobile.
     - **Client ID:** The unique identifier for your app from the Azure Configure page.
     - **Key:** From the Azure application settings page.
2. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.
3. Under **Authentication**, click **Identity Provider (IDP)**. The **Identity Provider** page appears.

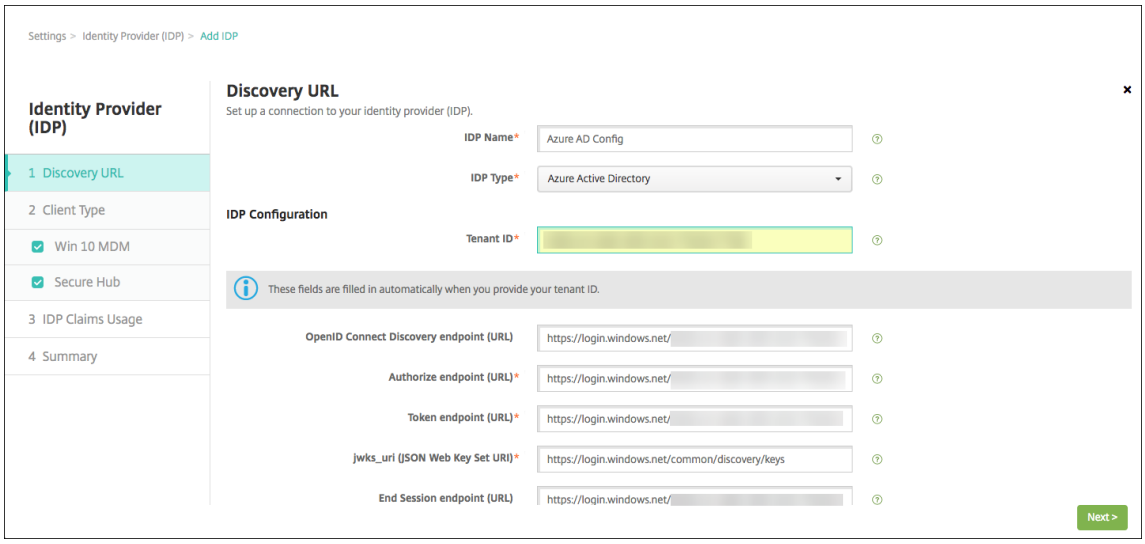


4. Click **Add**. The **IDP configuration** page appears.

5. Configure the following information about your IdP:

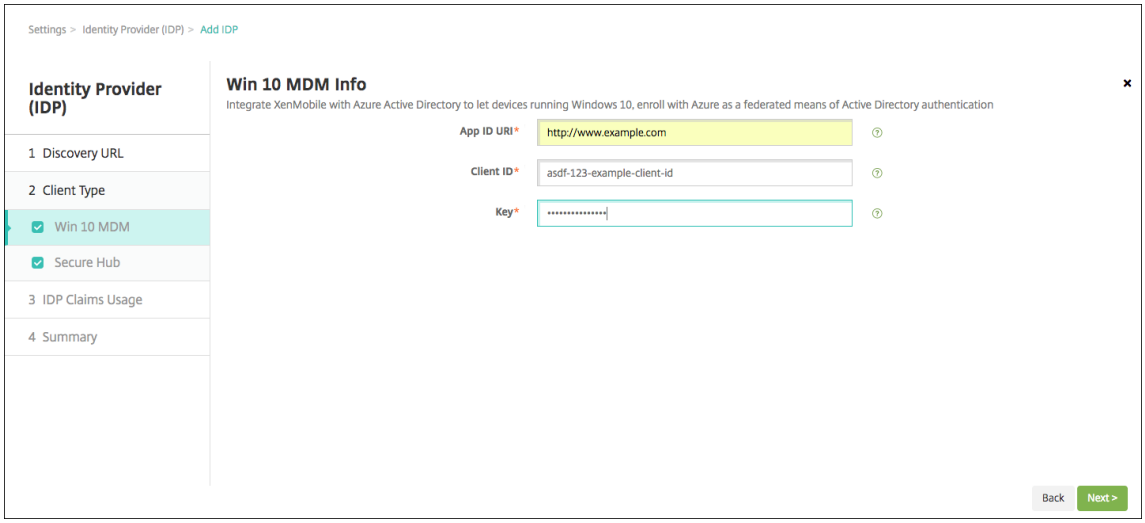
   - **IDP Name:** Type a name for IdP connection you are creating.
   - **IDP Type:** Choose Azure Active Directory as your IdP type.
   - **Tenant ID:** Copy this value from the Azure application settings page. In the browser address bar, copy the section made up of numbers and letters.

   For example, in `https://manage.windowszaure.com/acmew.onmicrosoft.com##workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...`, the tenant ID is: `abc123-abc123-abc123`.



6. The rest of the fields automatically fill. When they are filled, click **Next**.
7. To configure XenMobile to enroll Windows 10 devices using Azure AD for MDM enrollment, configure the following settings. To skip this optional step, clear **Win 10 MDM**.

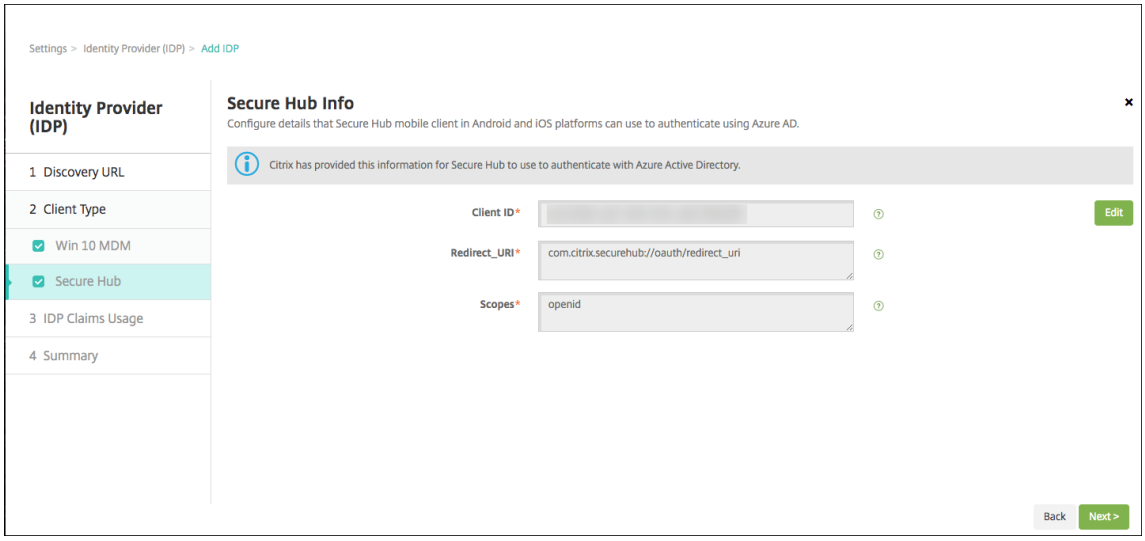
   - **App ID URI:** Type the URL for the XenMobile Server that you entered when you configured your Azure settings.
   - **Client ID:** Copy and paste this value from the Azure Configure page. The client ID is the unique identifier for your app.
   - **Key:** Copy this value from the Azure application settings page. Under keys, select a duration in the list and then save the setting. You can then copy the key and paste it into this field. A key is required when apps read or write data in Microsoft Azure AD.



8. Click **Next**.

   Citrix has registered Secure Hub with Microsoft Azure and maintains the information. This screen shows the details used by Secure Hub to communicate with Azure Active Directory. This page will be used in the future if any of this information needs a change. Edit this page only if Citrix advises you to.

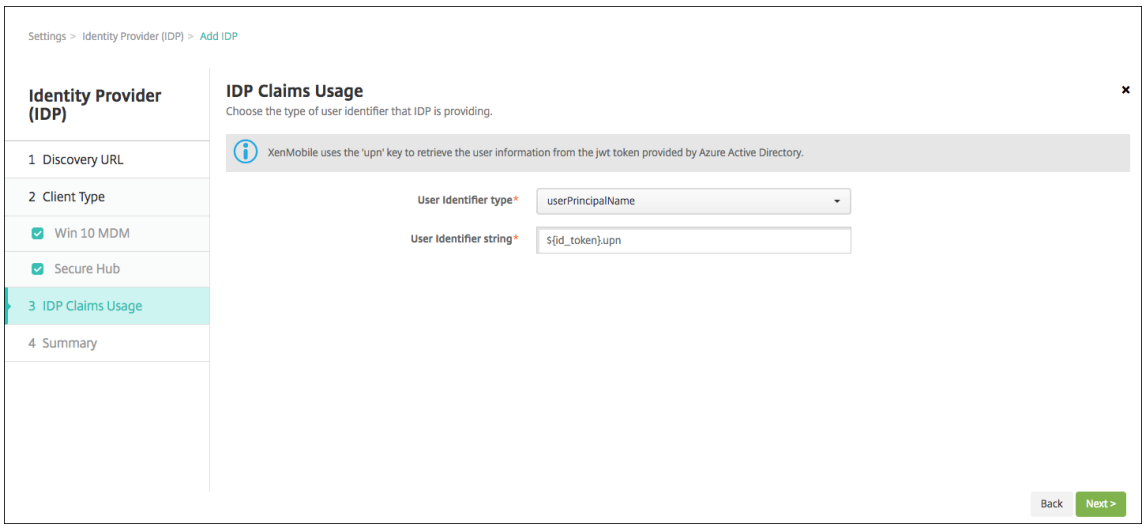
9. Click **Next**.



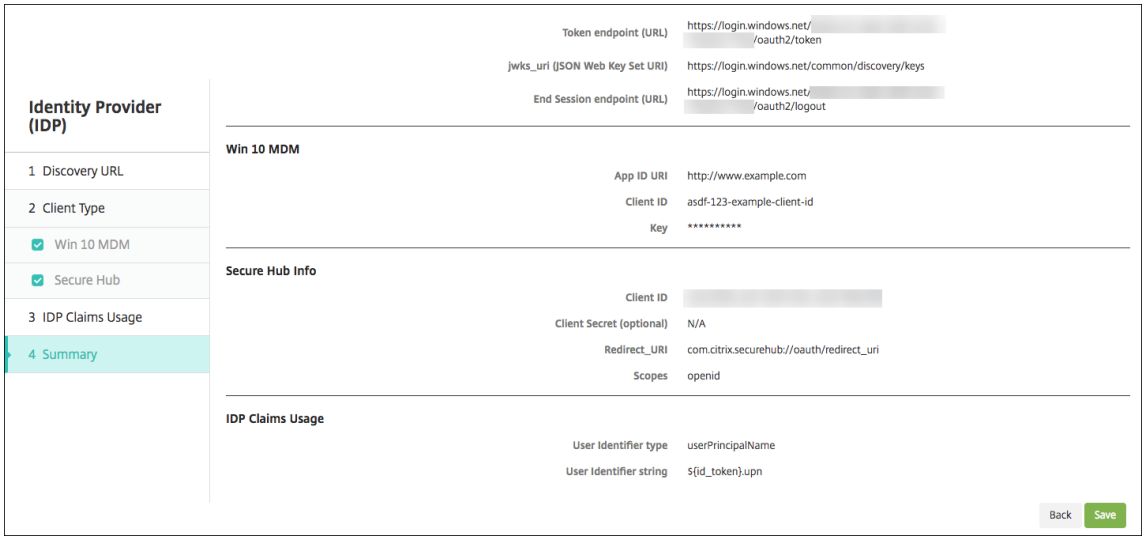
10. Configure the type of user identifier that your IdP provides:

    - **User Identifier type:** Choose **userPrincipalName** from the list.
    - **User Identifier string:** This field is automatically filled.

11. Click **Next**.

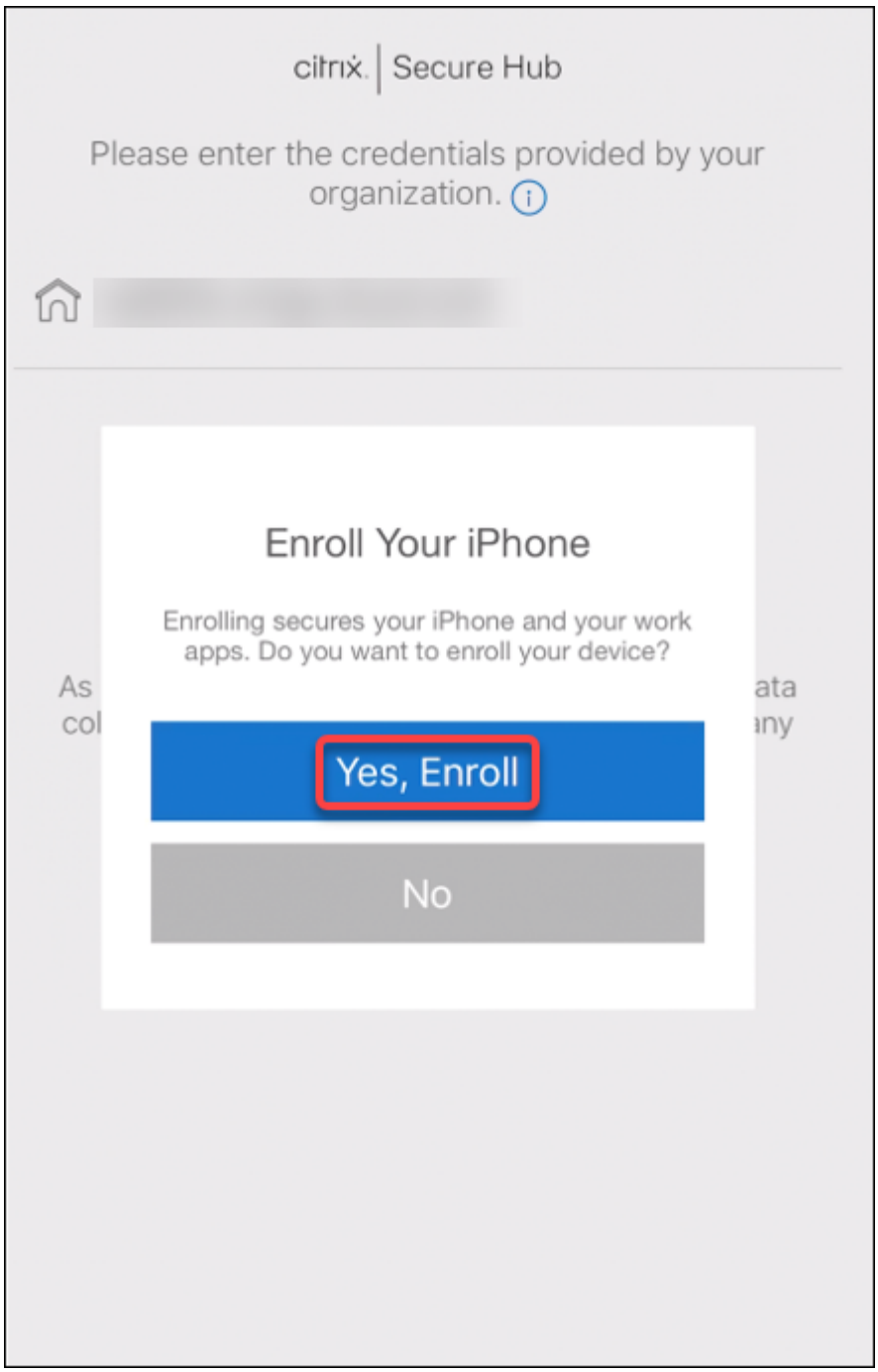


12. Review the **Summary** page and click **Save**.

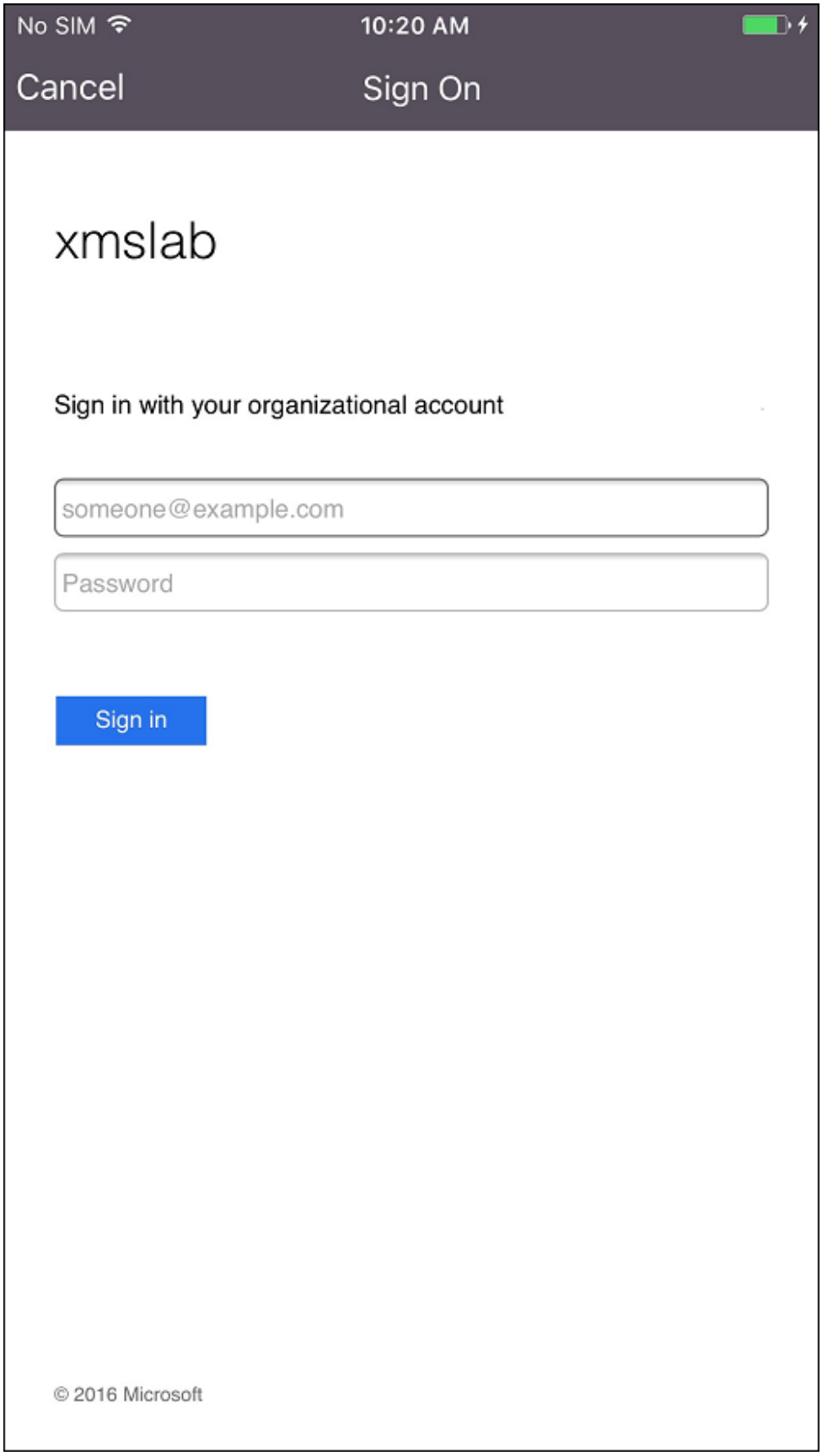


What users experience

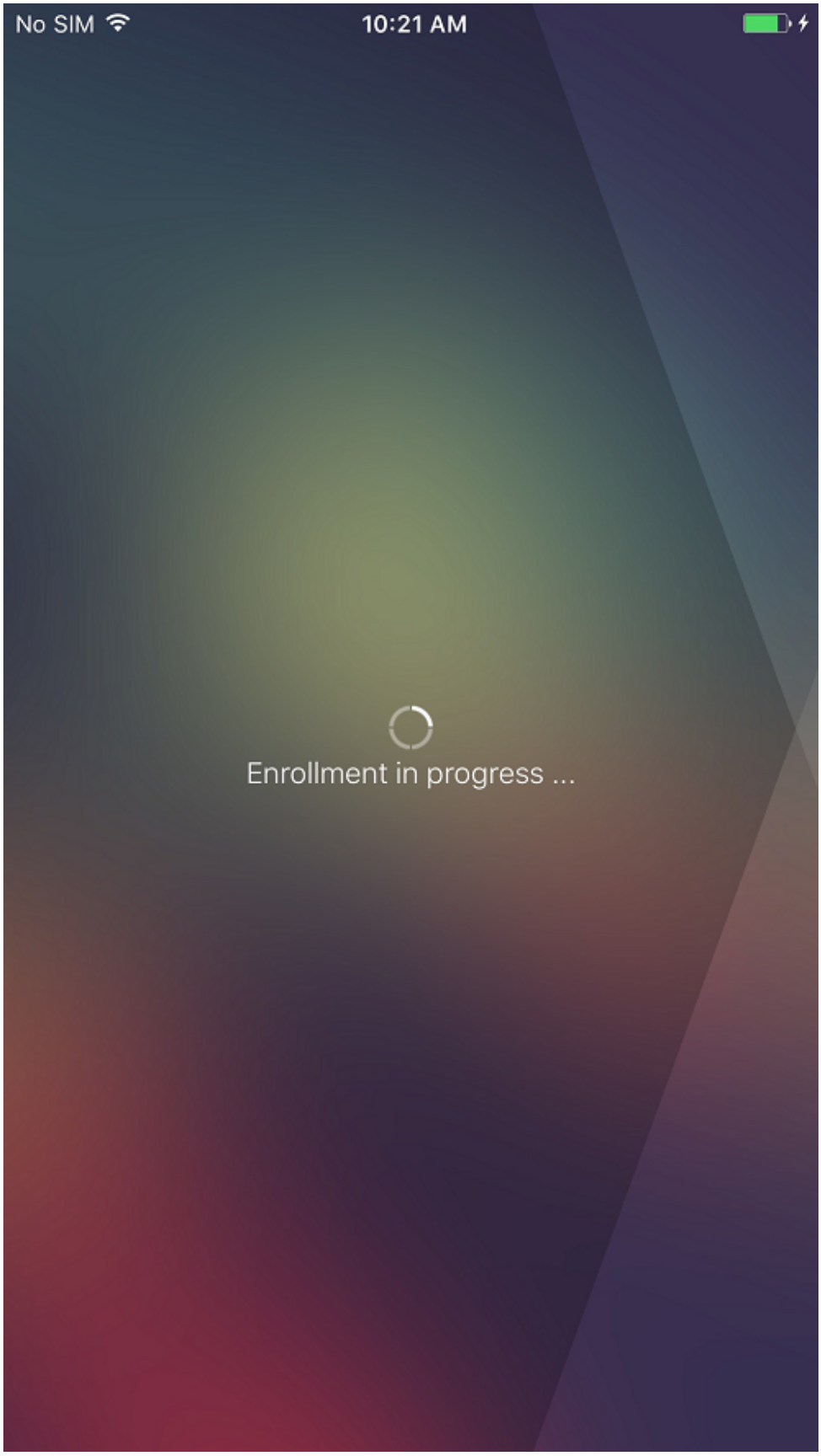
1. Users start Secure Hub. Users then enter the XenMobile Server Fully Qualified Domain Name (FQDN), a User Principle Name (UPN), or email address.

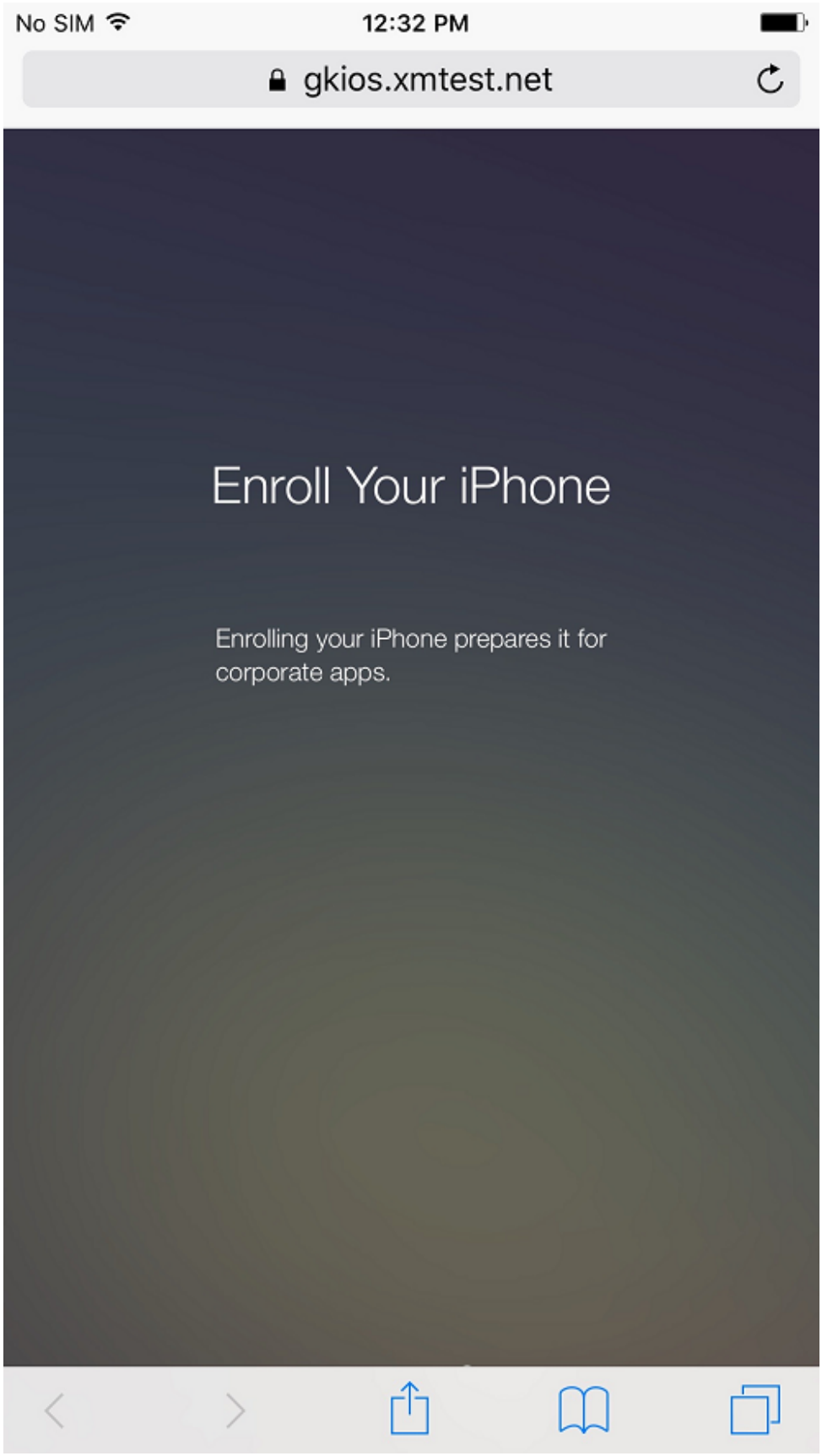


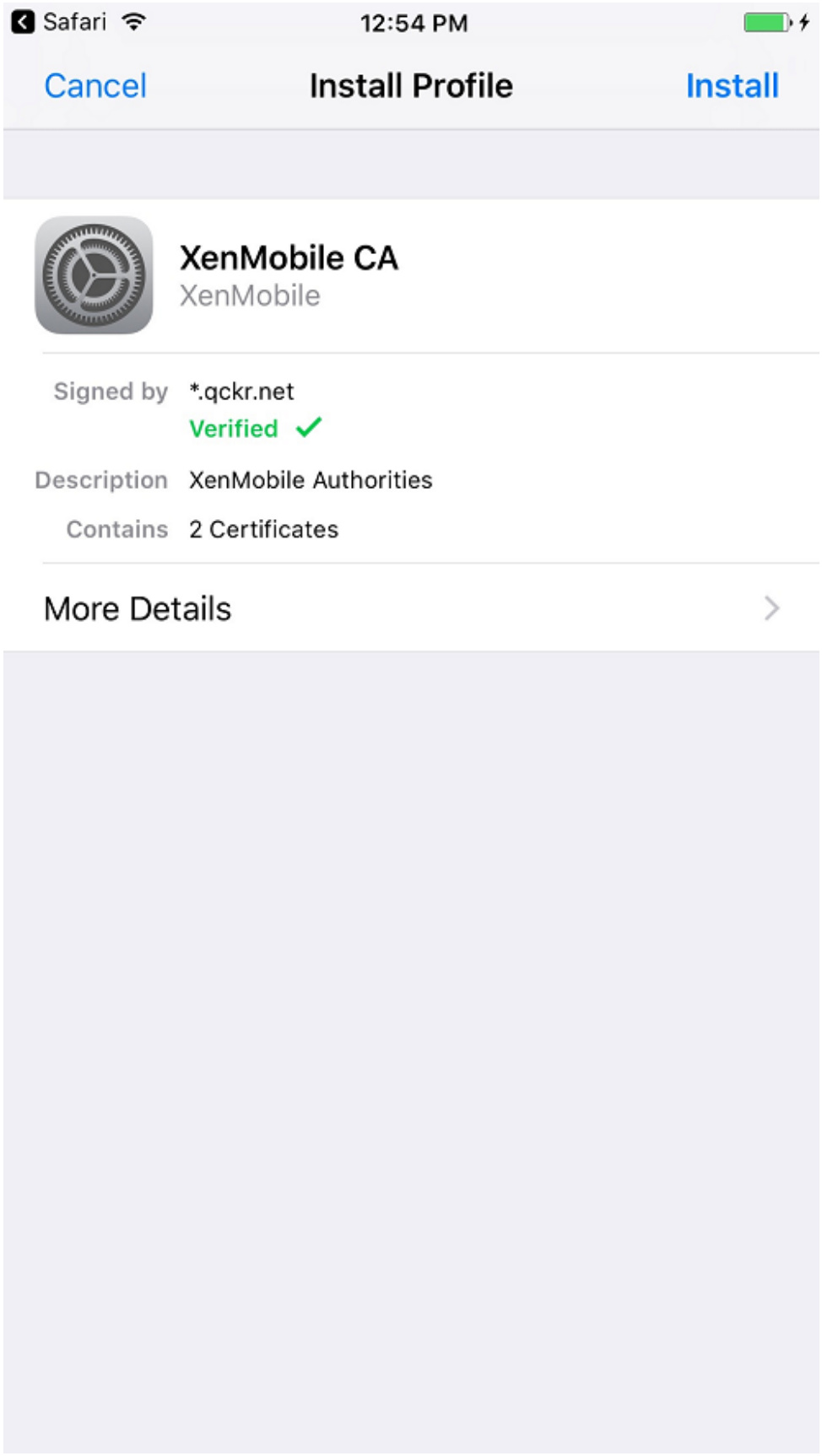
2. Users then click **Yes, Enroll**.



3. Users log on by using their Azure AD credentials.







4. Users complete the enrollment steps in the same way as any other enrollment through Secure Hub.

> **Note:**
>
> XenMobile 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.

Derived credentials

March 18, 2021

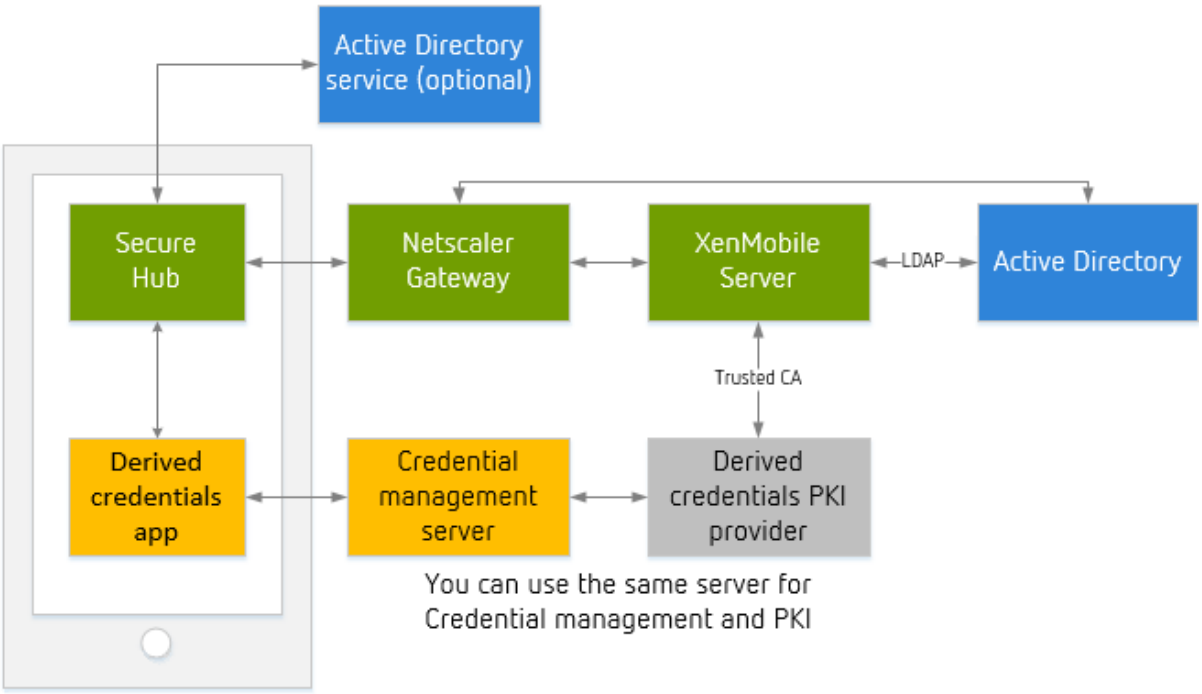
Derived credentials provide strong authentication for mobile devices. A smart card provides the credentials, which reside in a mobile device instead of the card. A smart card is a Personal Identity Verification (PIV) card.

The derived credentials are an enrollment certificate that contains the user identifier, such as UPN. XenMobile saves the credentials obtained from the credential provider in a secure vault on the device.

XenMobile can use derived credentials for device enrollment and authentication. If configured for derived credentials, XenMobile doesn't support enrollment invitations or other enrollment security modes. Citrix supports use of a derived credentials app during enrollment of iOS.

Architecture

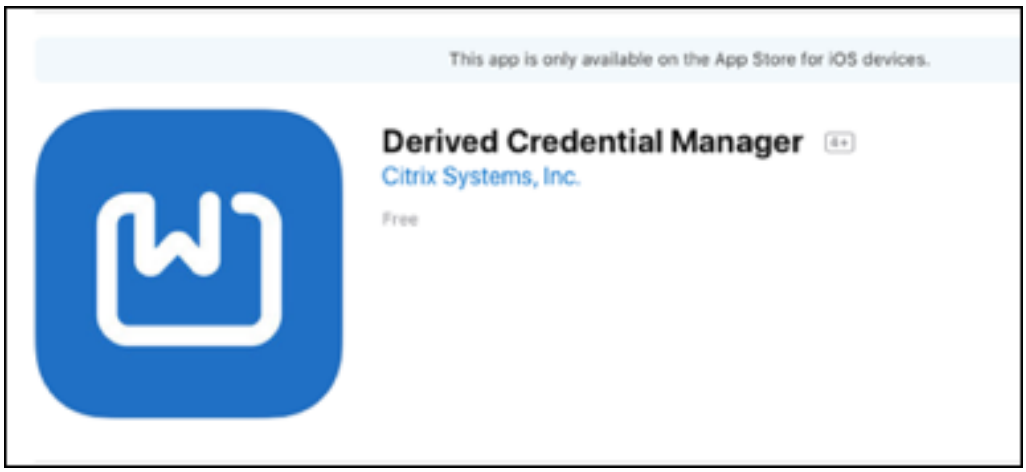
For enrollment, XenMobile Server connects to the components, as shown in the following diagram.



- 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.
- XenMobile Server 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 XenMobile. The Derived Credentials Manager app is the identity provider app for Citrix. The logo for that app follows.



    * The Citrix Derived Credential Manager app supports new enrollments only. Device users must re-enroll.
        - XenMobile Server version 10.8 or later.
        - 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.

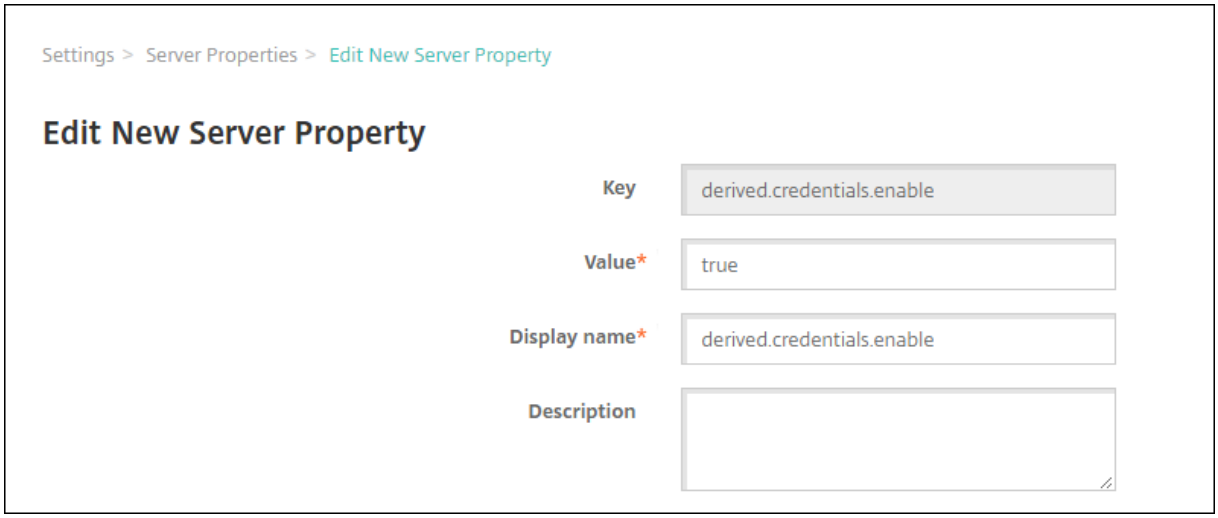
- Must have the root certificate of the authority that issues certificates to the Credentials Provider server. That setup enables XenMobile to accept the digitally signed certificates during enrollment. For information about adding the certificates, see Certificates and authentication.
  - If the user 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`**.
  - XenMobile 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 XenMobile 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**.

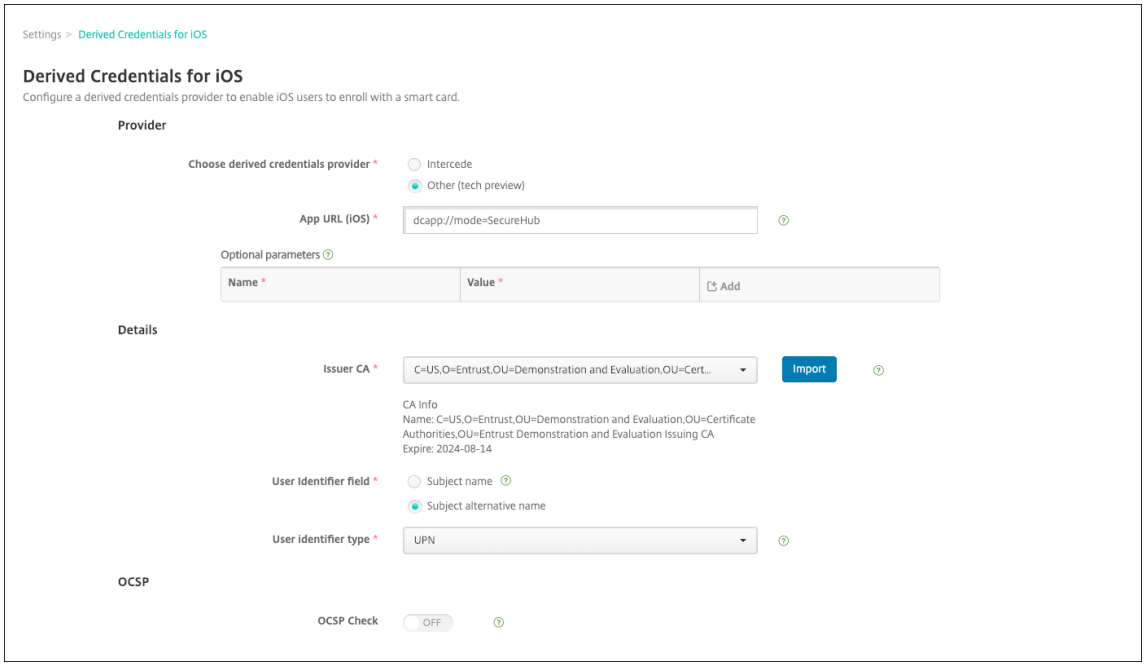


Configure derived credentials

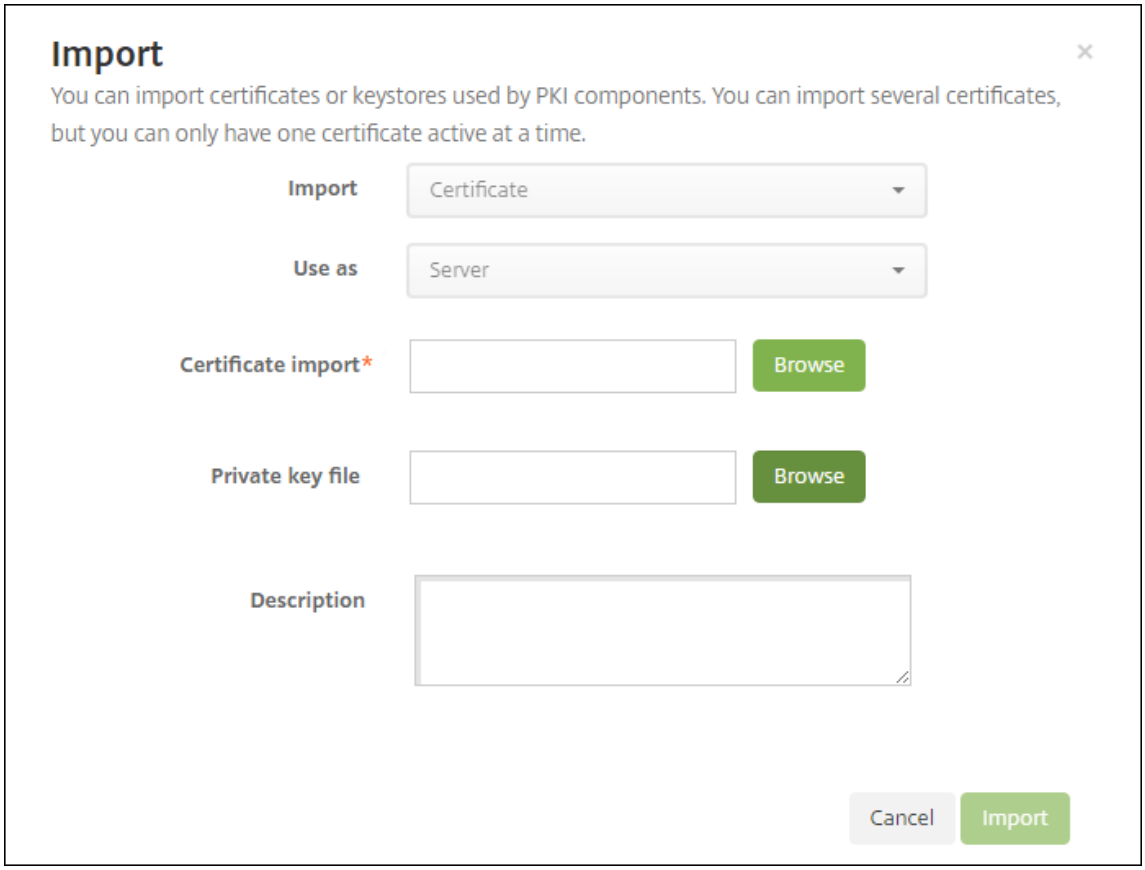
The assumption is that you have a working configuration for the derived credentials provider that you plan to integrate with XenMobile. You can configure XenMobile to communicate with that server. You can also choose a derived credentials CA certificate already added to XenMobile or import the certificate.

You can activate Online Certificate Status Protocol (OCSP) support for that CA certificate. For more information about OCSP, see "Discretionary CAs" in PKI entities.

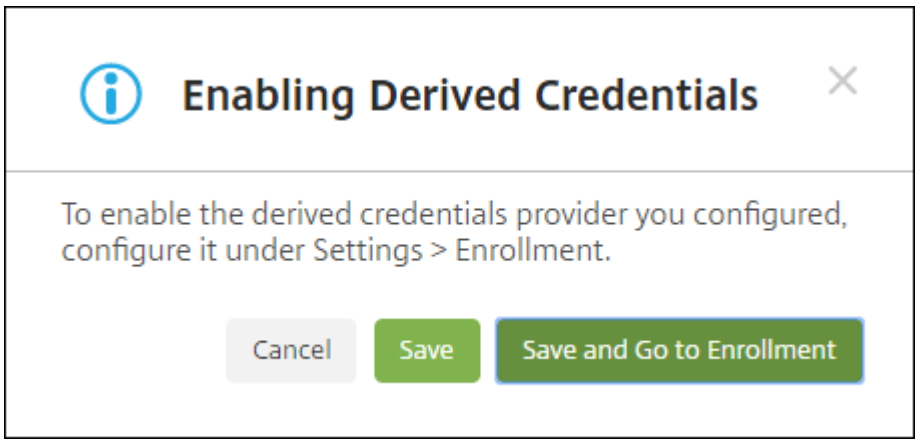
1. In the XenMobile console, go to **Settings > Derived Credentials for iOS**.
2. For **Choose derived credentials provider**, choose **Other** for Entrust Datacard. Type `dcapp://mode=SecureHub` in the **App URL (iOS)**.



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 XenMobile, 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.

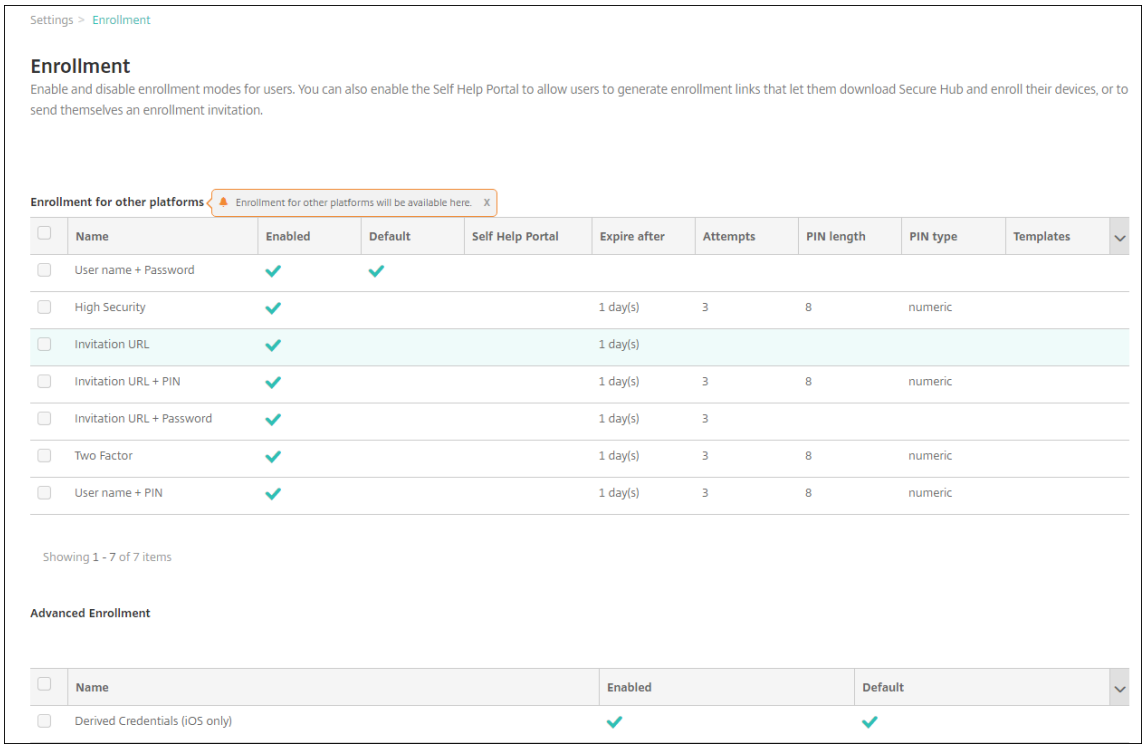


6. Configure the settings.
   - For Citrix Derived Credential Manager app: The **User Identifier field** is **Subject alternative name**, and the **User Identifier type** is **userPrincipalName**.
   - Contact other derived credential providers for their information.
7. You can optionally use an OCSP 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, XenMobile 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.

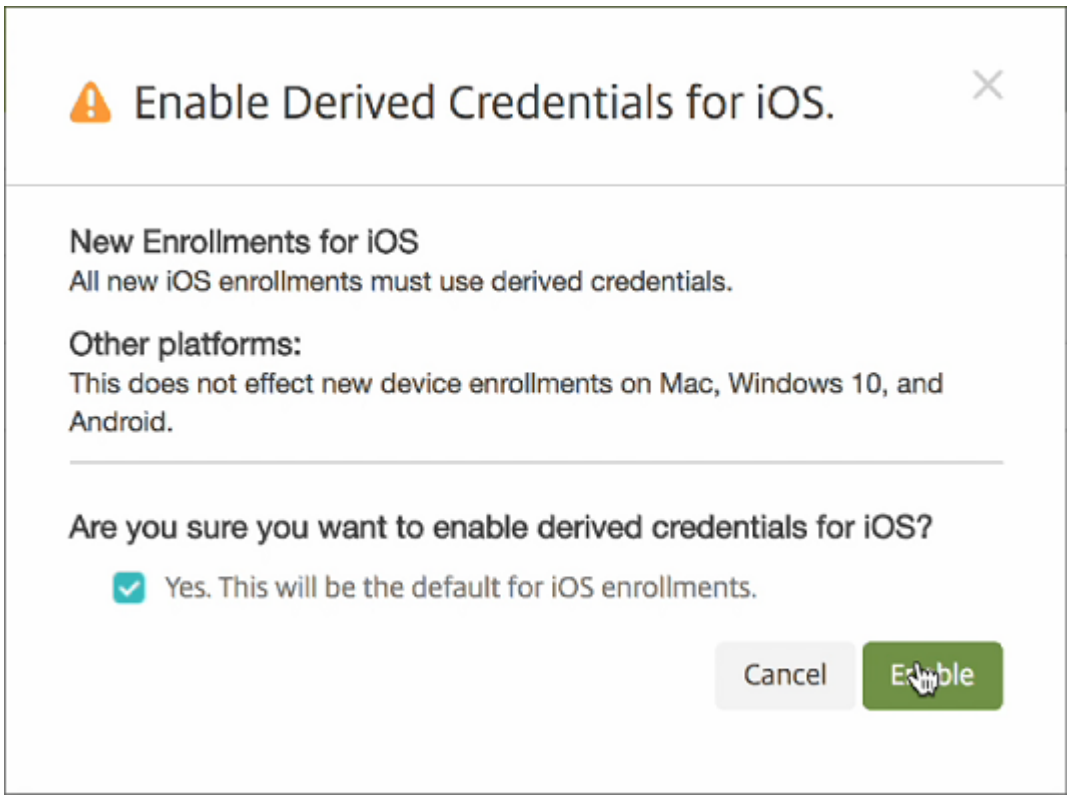


- To enable the derived credentials configuration, click **Save**. To use derived credentials, you must also configure enrollment settings.
- To enable the derived credentials configuration and then go immediately to **Settings > Enrollment**, click **Save and Go to Enrollment**.

9. To enable derived credentials for enrollment: On the **Settings > Enrollment** page, under **Advanced Enrollment**, select **Derived Credentials (iOS only)** and then click **Enable**.



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**.

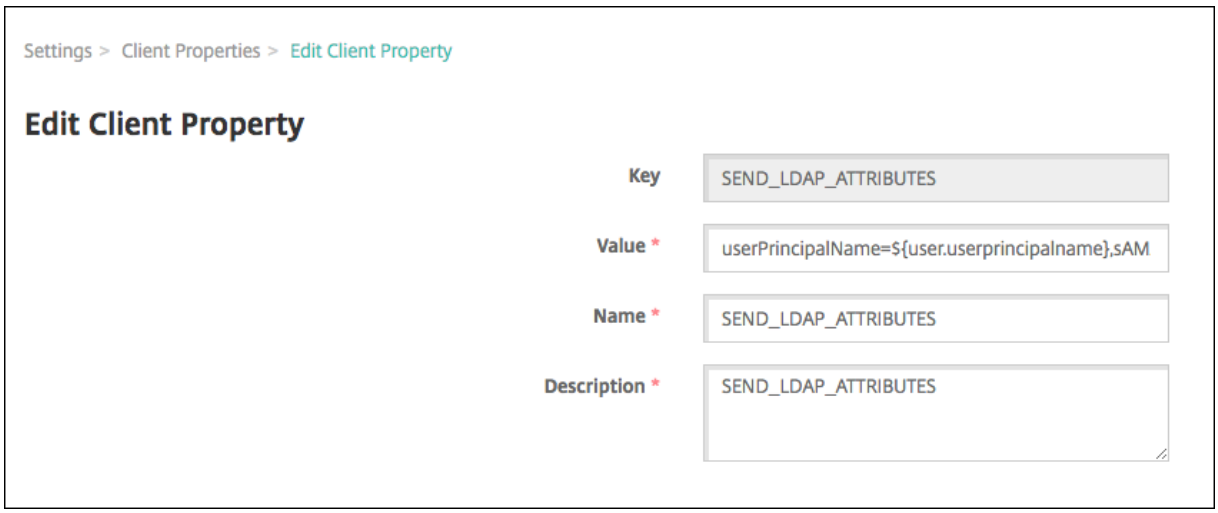
> **Important:**
>
> After adding the derived credentials provider, restart your XenMobile Server.

Configure XenMobile Server for Secure Mail

To enable Secure Mail to support derived credentials, add the `SEND_LDAP_ATTRIBUTES` client property. For information about adding a client property, see Client properties.

Use the following information for the client property:

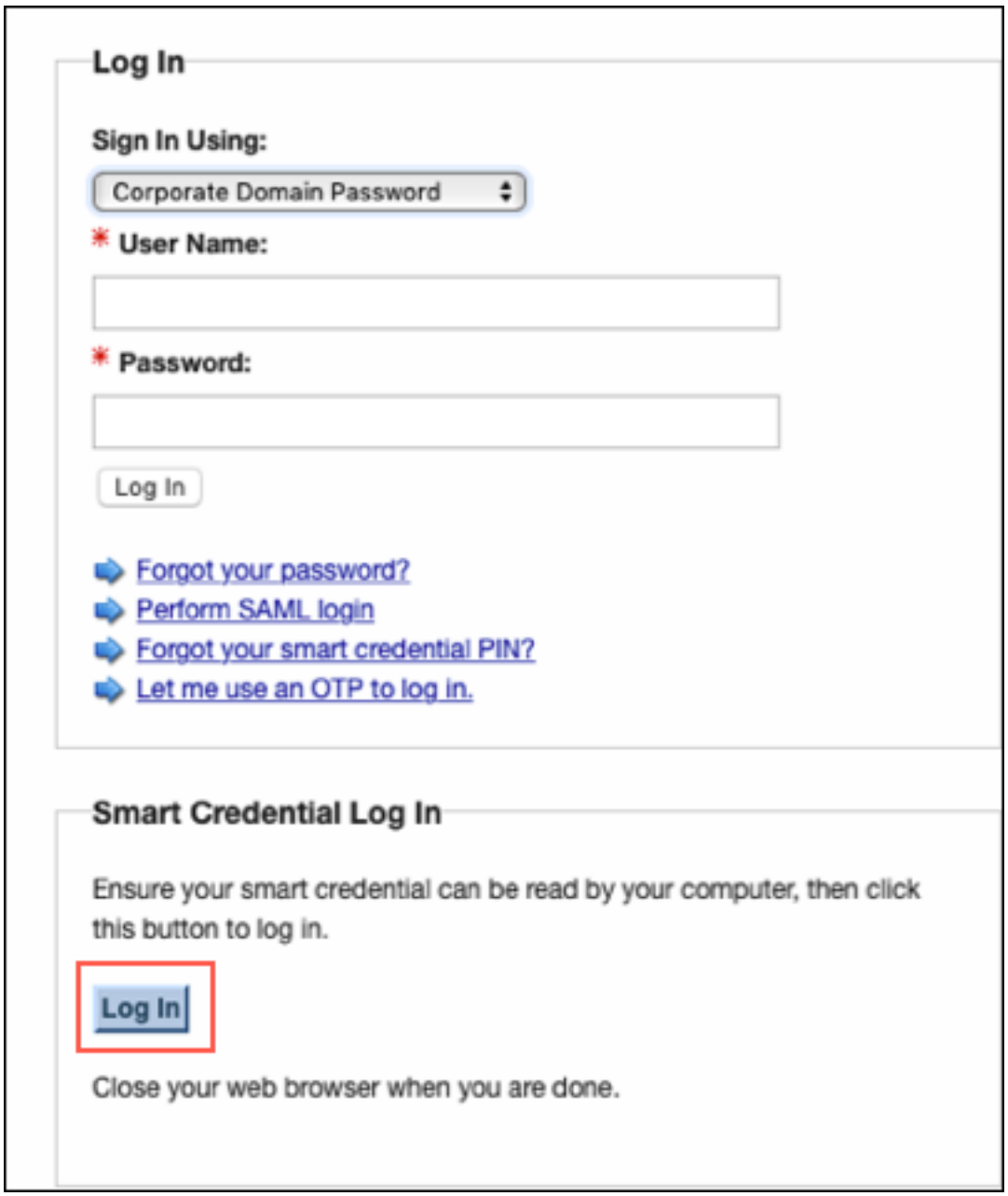
- **Key:** `SEND_LDAP_ATTRIBUTES`
- **Value:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`



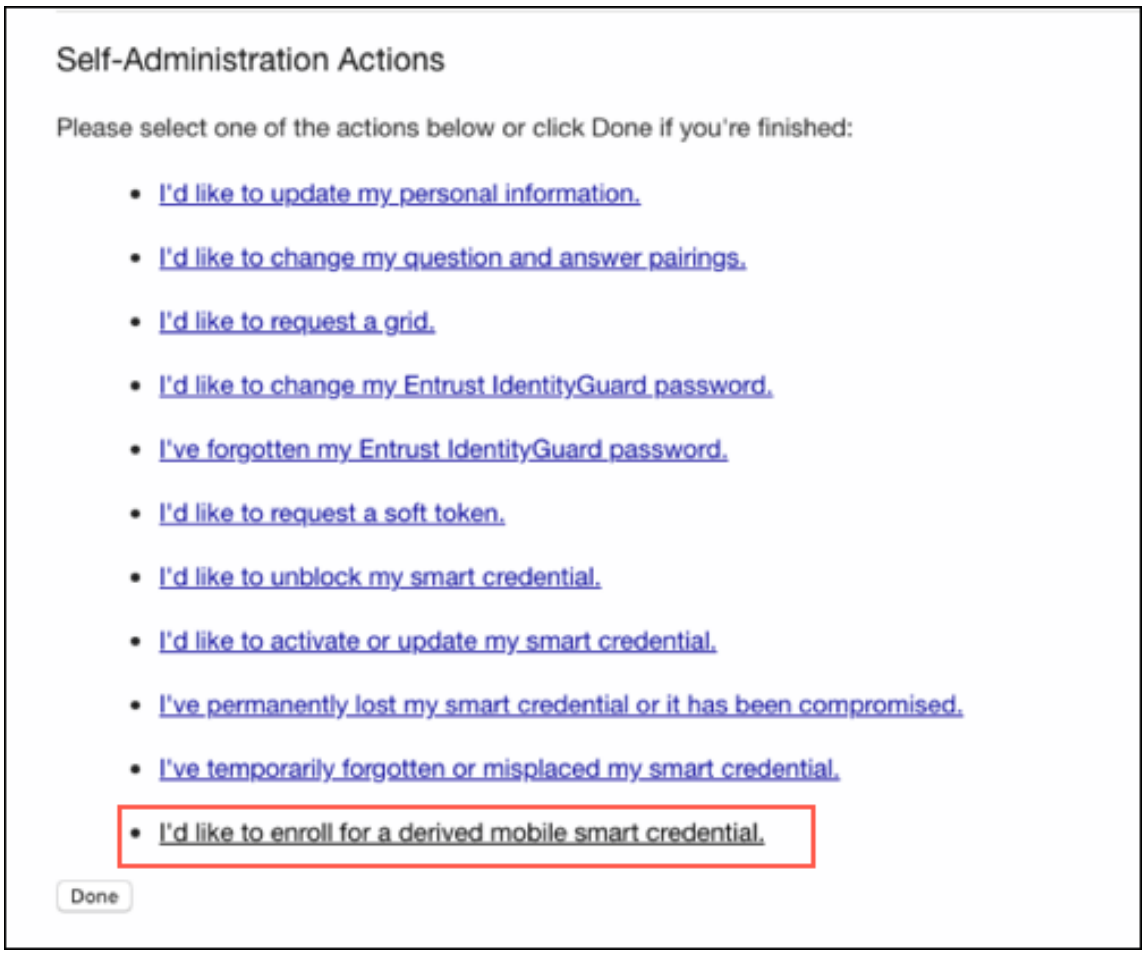
Activating Entrust Datacard derived credentials on iOS devices

> **Note:**
>
> While using the Entrust website, clear the browser cache when changing the PIV card.

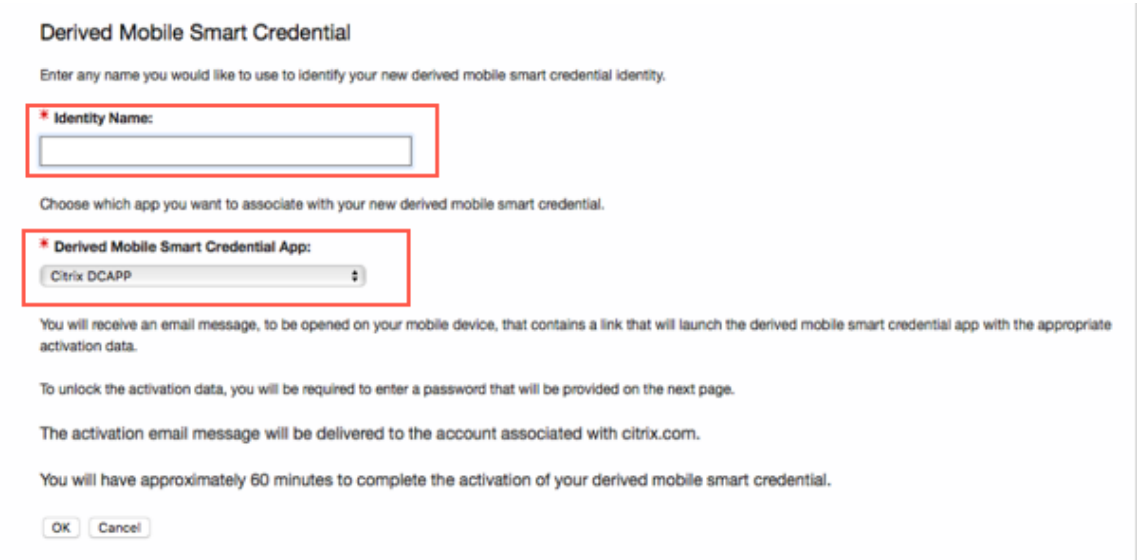
1. To request new smart credentials, use a desktop or any device to log in to the Entrust site. Log in using the **Smart Credential Log In** button at the bottom of the page. Users insert their smart card into a reader attached to their desktop.



2. From the **Self-Administration Actions**, select the **I'd like to enroll for a derived mobile smart credential** and click **Done**.



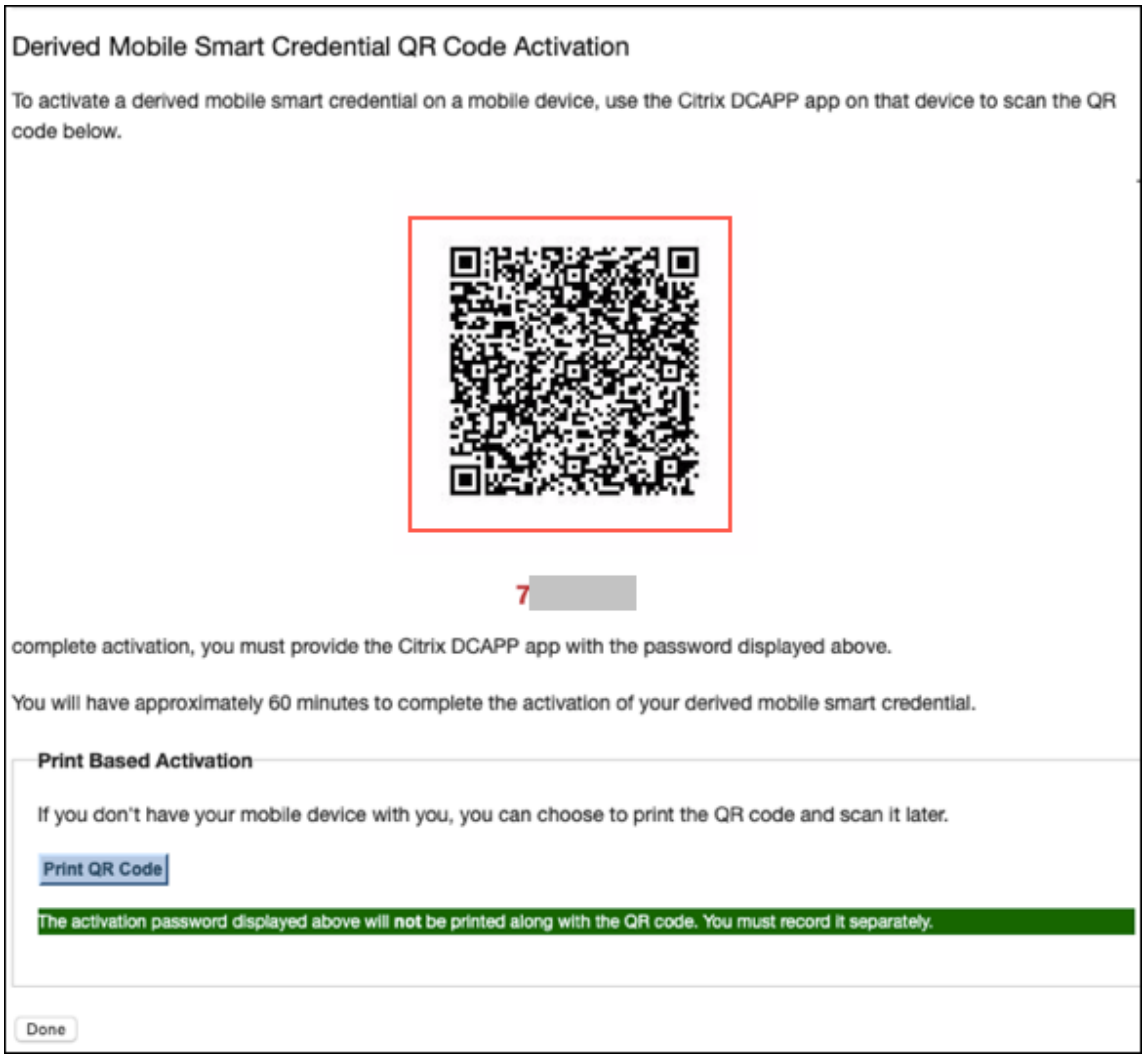
3. In the **Derived Mobile Smart Credential** screen, provide the **Identity Name**. The user can choose a unique name such as a user name or ID numbers.
4. Select the **Citrix DCAPP** from the Derived credential app menu, and click **Ok**.



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.

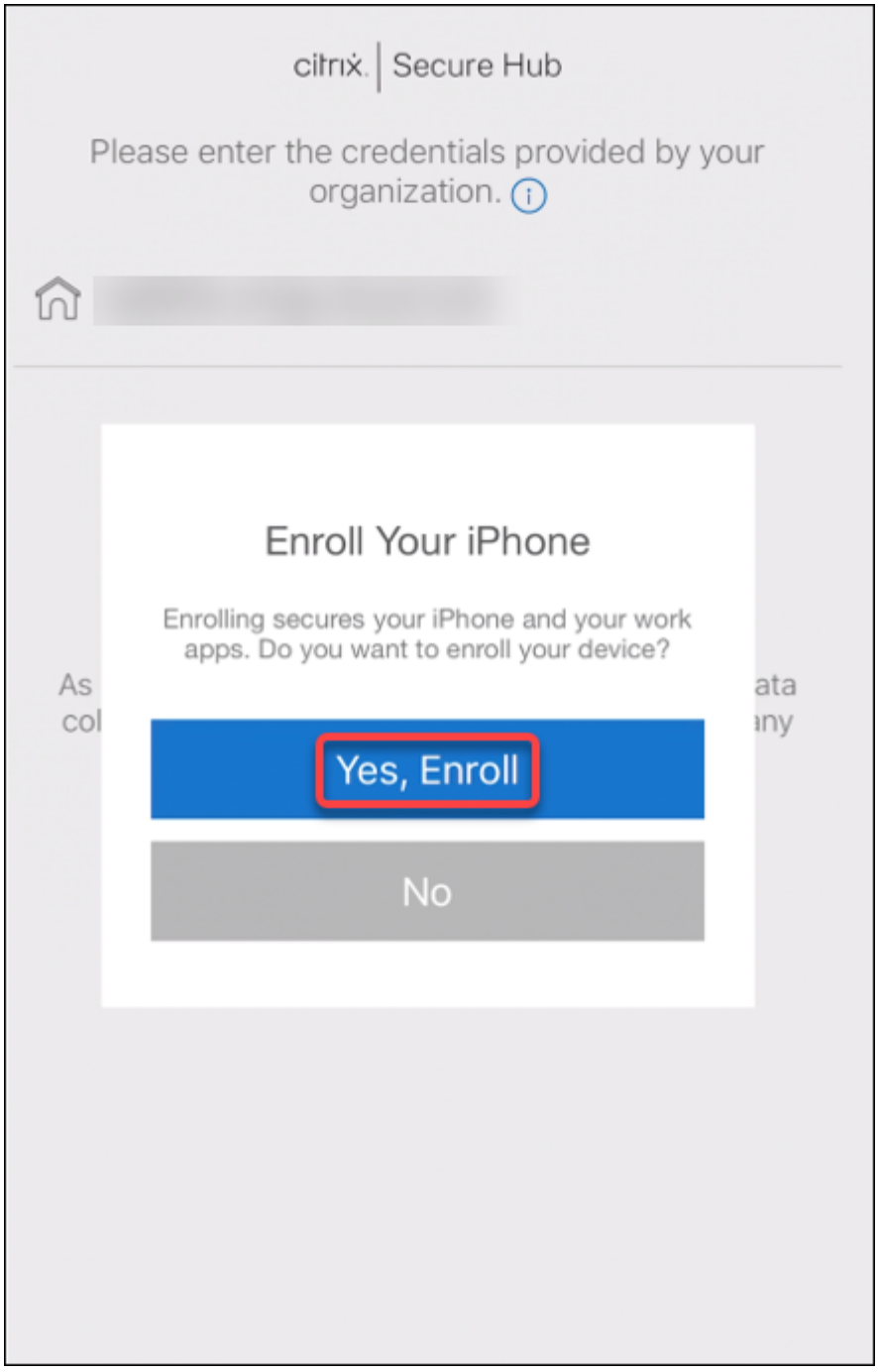


Device enrollment

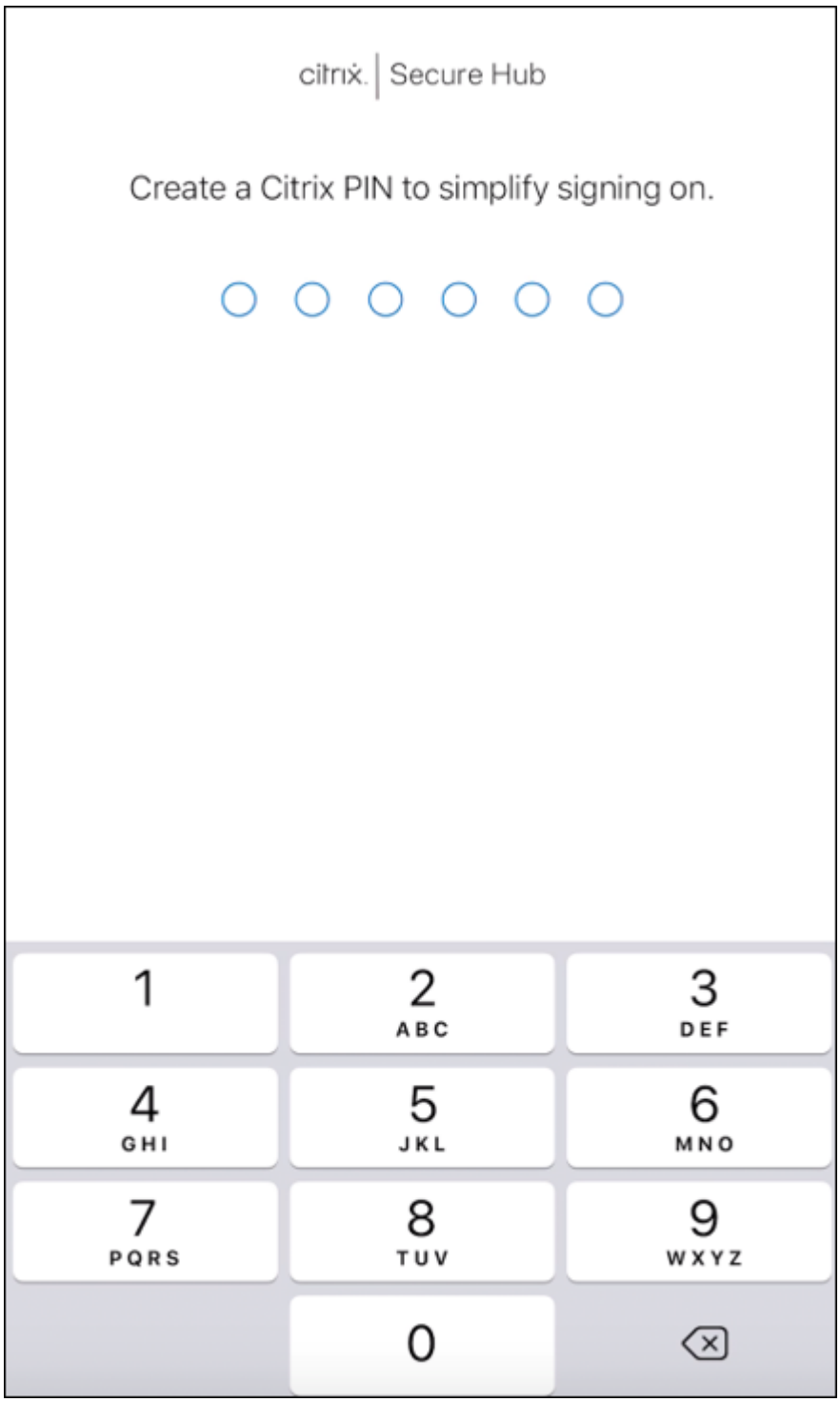
After you complete the setup described earlier in this article, users can enroll their devices by using derived credentials.

> **Note:**
>
> Screenshots in this section use Entrust Datacard as an example.

1. Tap to open **Secure Hub**. When prompted, type XenMobile Server's fully qualified domain name and then click **Next**.
2. Click **Yes, Enroll**. Device enrollment in Secure Hub starts.

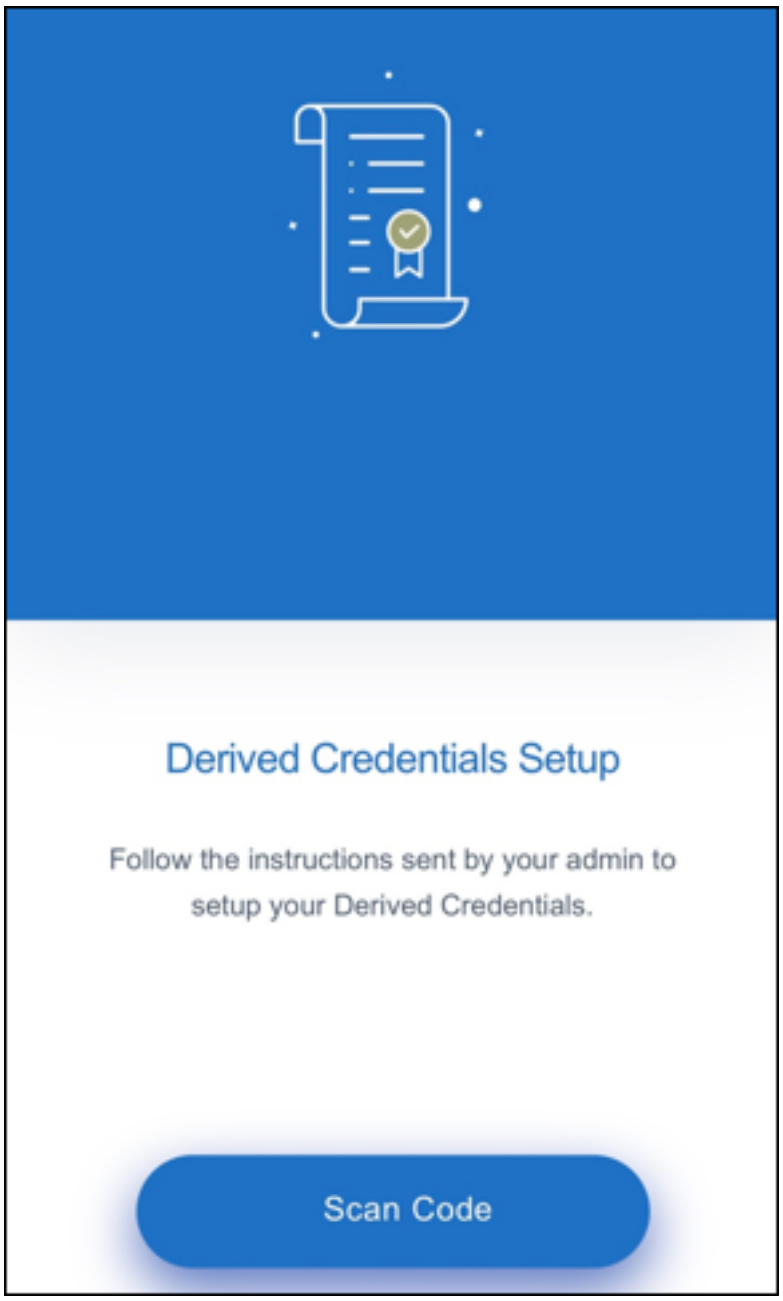


If XenMobile Server supports derived credentials Secure Hub prompts the user to create and confirm the Citrix PIN.



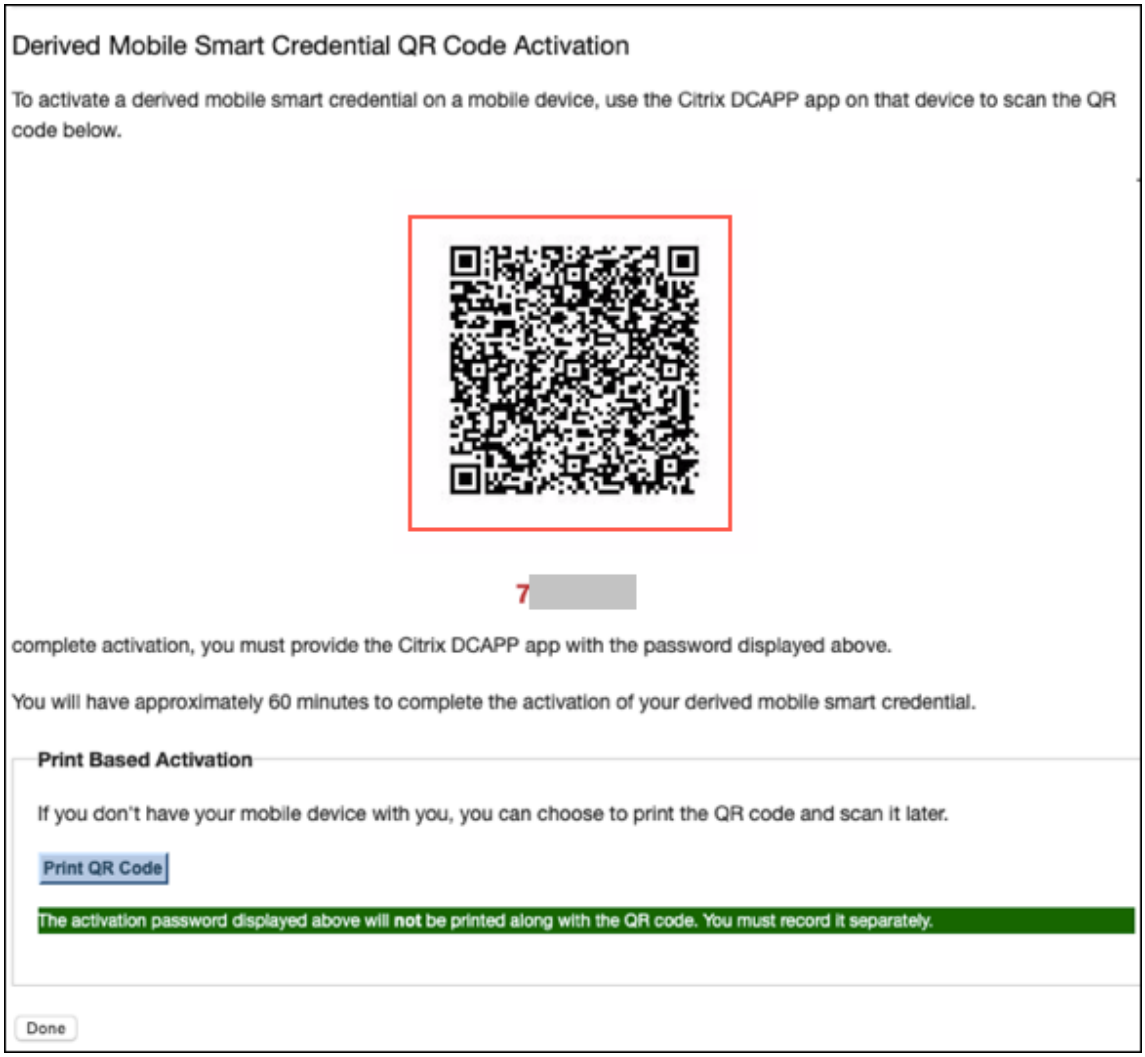
After confirming the Citrix PIN the Derived Credentials setup splash screen appears. Follow the instructions to activate smart credentials.

3. Tap **Scan code**. The mobile phone camera activates.

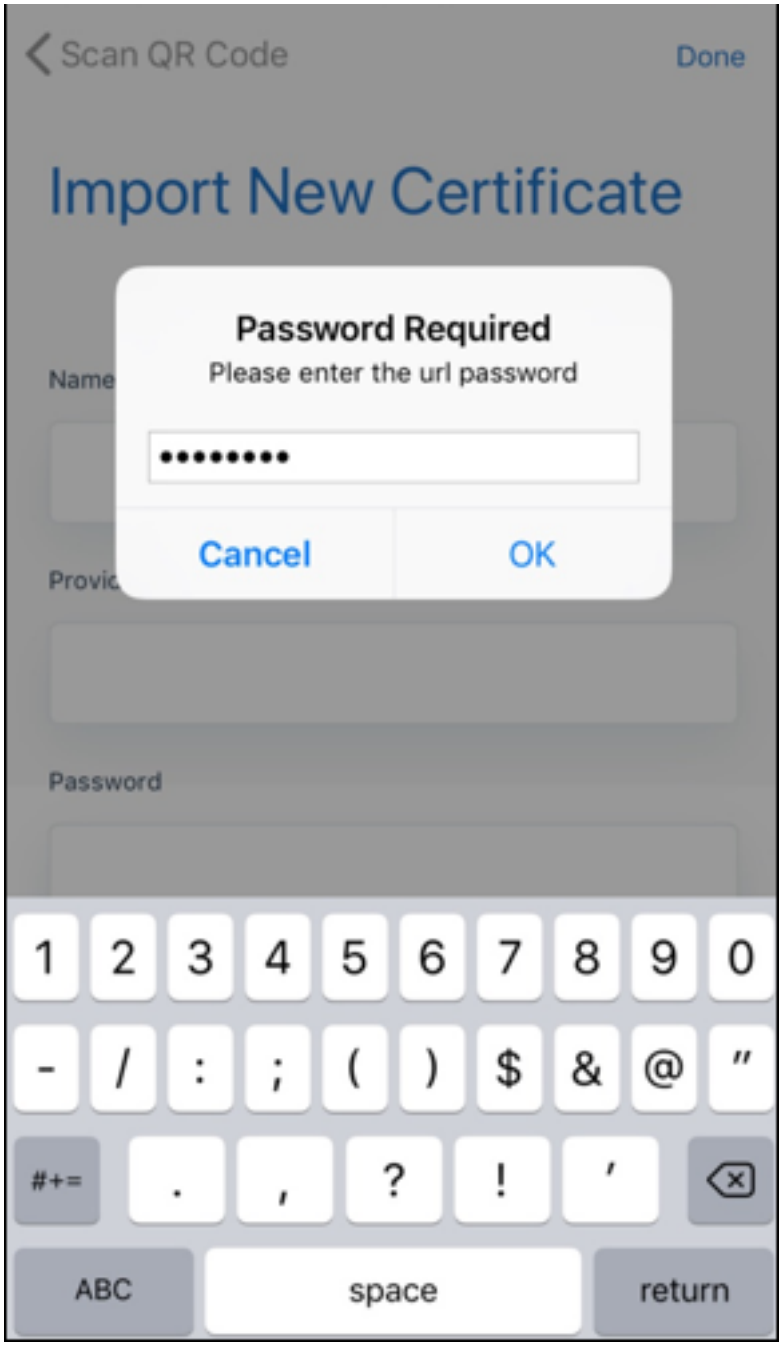


> **Note:**
>
> To scan the QR code, ensure your camera and microphone is enabled and has required access permissions.

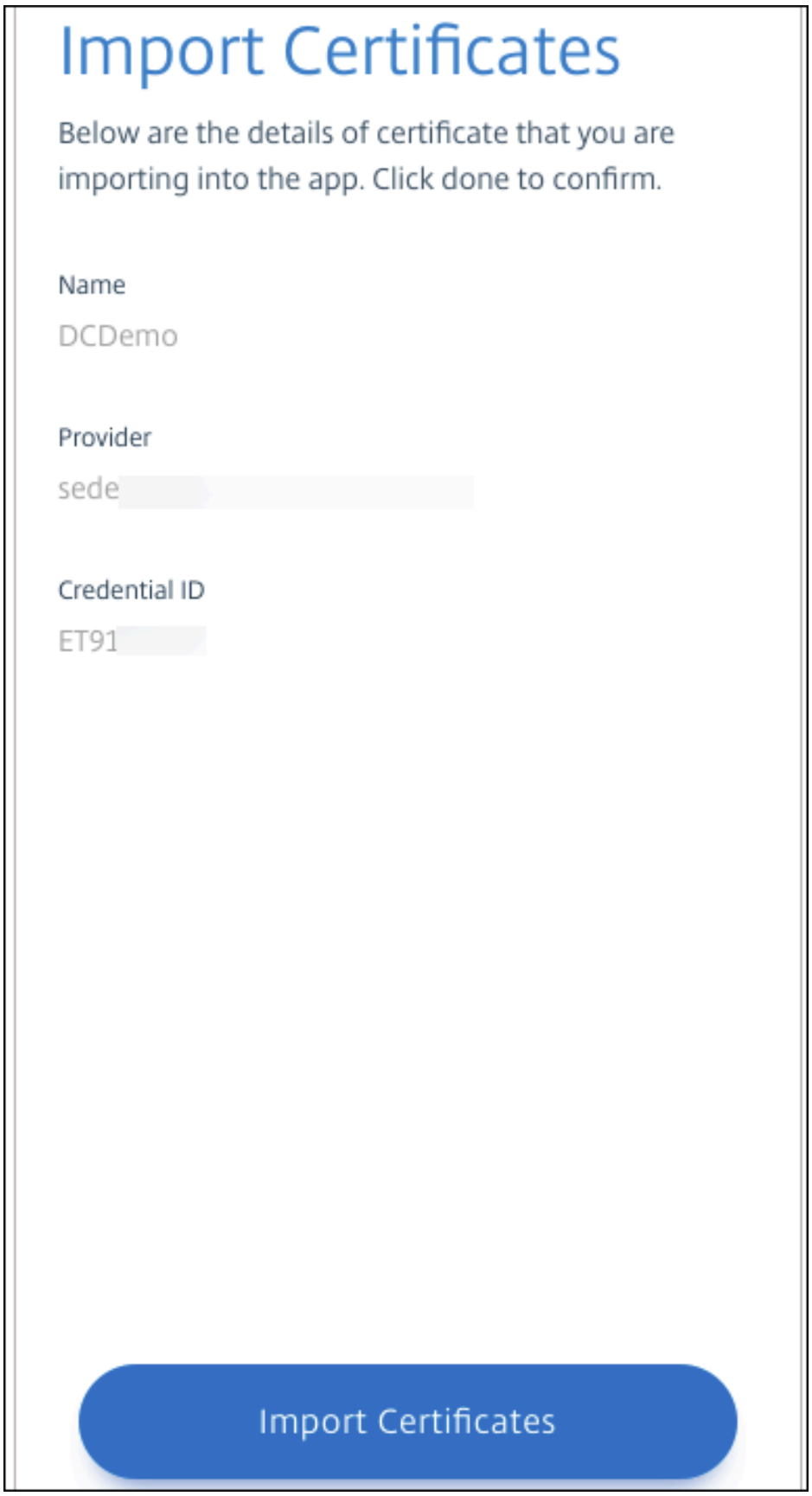
4. In the derived credentials app, scan the QR code that was created in earlier steps.



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.



6. After the certificates are added successfully, in the **Derived Credentials** screen, click **Continue to Secure Hub**.

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 XenMobile console:

- Go to **Manage** > **Devices** and then select a device to display a command box. Click **Show more**.
- Go to **Analyze** > **Dashboard**.

Upgrade

October 13, 2020

> **Tip: XenMobile Migration Service**
>
> If you're using XenMobile Server on premises, our free 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. These blogs discuss the XenMobile Migration Service:
>
> New XenMobile Migration Service
>
> Making the Case for XenMobile in the Cloud

Before you upgrade to XenMobile 10.13

1. Update your Citrix License Server to 11.16 or later before updating to the latest version of XenMobile Server 10.13.

   The latest version of XenMobile requires Citrix License Server 11.16 (minimum version).

   The Customer Success Services date (previously, Subscription Advantage date) in XenMobile 10.13 is September 29, 2020. The Customer Success Services date on your Citrix license must be later than this date. You can view the date next to the license in the License Server. If you connect the latest version of XenMobile to an older License Server environment, the connectivity check fails and you can't configure the License Server.

   To renew the date on your license, download the latest license file from the Citrix Portal and upload the file to the Licensing Server. For more information, see Customer Success Services.

2. For a clustered environment: iOS policy and app deployments to devices running iOS 11 and later have the following requirement. If Citrix Gateway is configured for SSL persistence, you must open port 80 on all XenMobile Server nodes.

3. If the virtual machine running the XenMobile Server to be upgraded has less than 8 GB of RAM, we recommend that you increase the RAM to at least 8 GB.
4. Recommendation: Before you install a XenMobile update, use the functionality in your VM to take a snapshot of your system. Also, back up your system configuration database. If you experience issues during an upgrade, complete backups enable you to recover.

To upgrade

You can directly upgrade to XenMobile 10.13 from XenMobile 10.12.x or 10.11.x. To perform the upgrade, download the latest binary available: Go to https://www.citrix.com/downloads. Navigate to **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. On the tile for the XenMobile Server software for your hypervisor, click **Download File**. To upload the upgrade, use the **Release Management** page in the XenMobile console.

To upgrade using the Release Management page

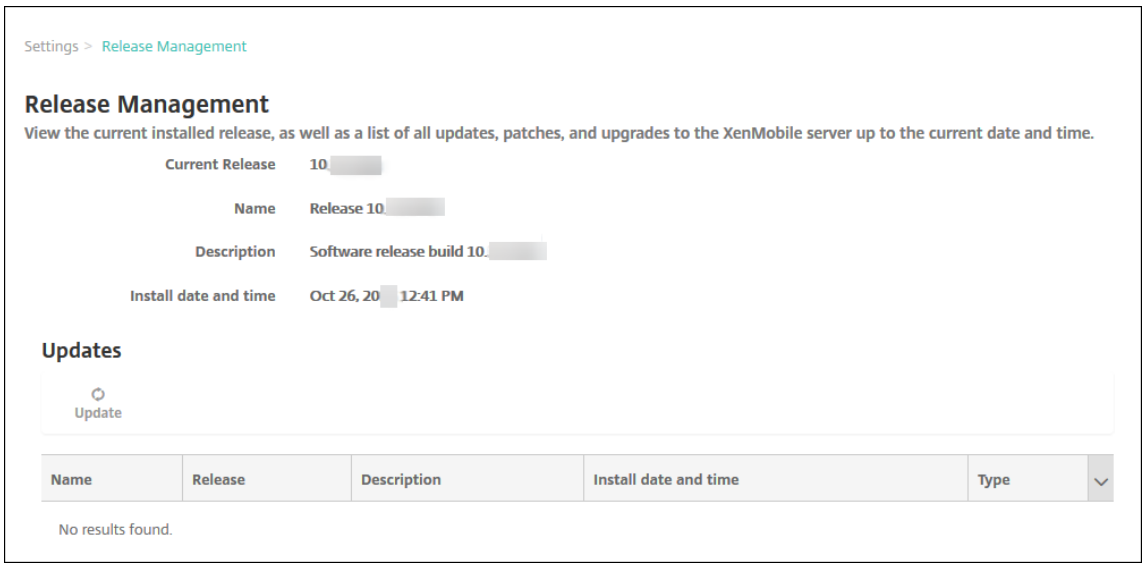
Use the **Release Management** page to upgrade to the latest version of XenMobile Server.

Prerequisites:

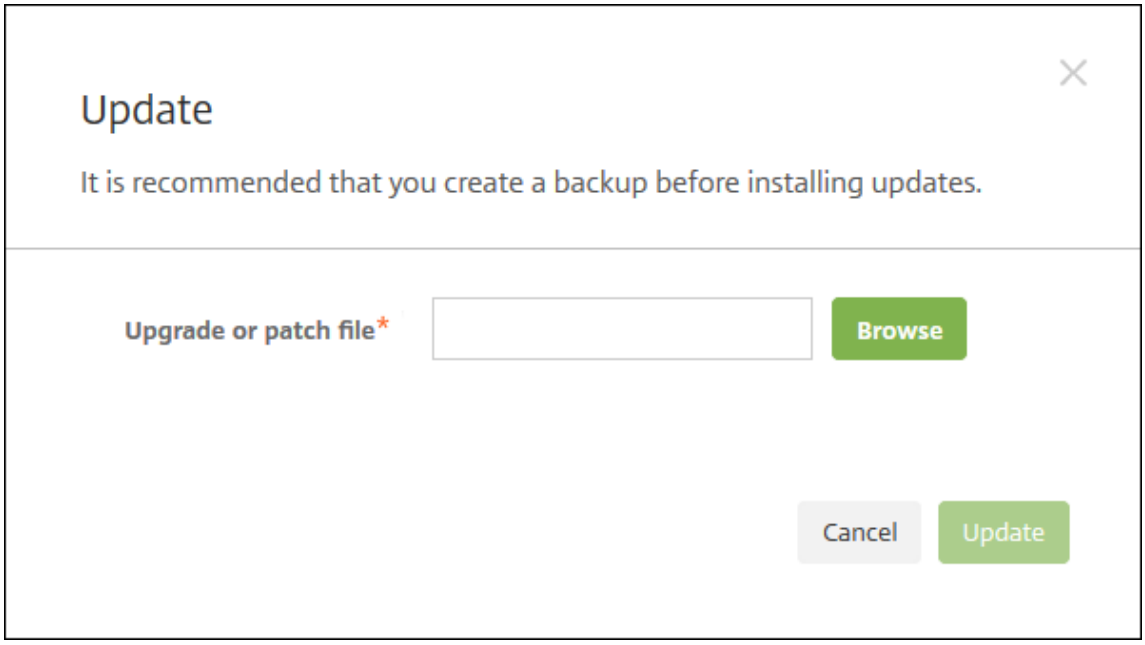
- Review the System Requirements.

If you have a clustered deployment, see the instructions at the end of this article.

1. Download the latest binary available: Go to https://www.citrix.com/downloads. Navigate to **Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10**. On the tile for the XenMobile Server software for your hypervisor, click **Download File**.
2. In the XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
3. Click **Release Management**. The **Release Management** page appears.



4. Under **Updates**, click **Update**. The **Update** dialog box appears.



5. Select the XenMobile upgrade file you downloaded from Citrix.com by clicking **Browse** and navigating to the file location.
6. Click **Update** and then if prompted, restart XenMobile.

   If for some reason the update cannot be completed successfully, an error message appears to indicate the problem. The system is reverted to its state previous to the update attempt.

After you upgrade

After an upgrade, XenMobile requires a restart. Use the XenMobile CLI to restart XenMobile Server. It's important that you clear your browser cache after the system restarts.

If functionality involving outgoing connections stop working, and you haven't changed your connections configuration, check the XenMobile Server log for errors such as the following: "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer"

The certificate validation error indicates that you need to disable host name verification on XenMobile Server. By default, host name verification is enabled on outgoing connections except for the Microsoft PKI server. If host name verification breaks your deployment, change the server property **disable.hostname.verification** to **true**. The default value of this property is **false**.

Citrix publishes new versions or important updates of XenMobile to Citrix.com. At the same time, a notice is sent to the contact on record for each customer.

To upgrade clustered XenMobile deployments

> **Important:**
>
> Before you install a XenMobile update, use the functionality in your virtual machine (VM) to take a snapshot of your system. Also, back up your system configuration database. If you experience issues during an upgrade, complete backups enable you to recover.

If your system is configured in cluster mode, follow these steps to update each node from a XenMobile 10 release:

1. Upload the .bin file on all nodes from **Settings > Release Management**.
2. Shut down all the nodes from the **System Menu** in the CLI.
3. Bring up one node, from the **System Menu** in the CLI, and check that the service is running.
4. Bring up other nodes one after the other.

   If XenMobile can't complete the update successfully, an error message appears to indicate the problem. XenMobile then reverts the system to its state previous to the update attempt.

Upgrade from XenMobile MDM Edition to Enterprise Edition

You can upgrade the XenMobile MDM Edition to the XenMobile Enterprise Edition for iOS and Android devices.

Prerequisites

- The correct Enterprise license.
- Citrix Gateway is configured.

To upgrade

1. Go to **Settings > Licensing** and verify that the correct Enterprise Edition license type is uploaded.
2. Go to **Settings > Server Properties** and change the **Server Mode** property from **MDM** to **ENT**.
3. Go to **Settings > Citrix Gateway** and configure the Citrix Gateway details. Set the authentication mode to the same as the MDM Edition, that is, domain (Active Directory) authentication. XenMobile doesn't support changing the authentication mode after user enrollment.
4. Optional: Go to **Settings > Client Properties** and enable Citrix PIN authentication.

After you complete those steps, users must perform the following steps to switch a device into Enterprise mode.

iOS users

1. Close Secure Hub: Tap the device home button twice (quickly) and slide up the Secure Hub app.
2. Open Secure Hub.

Android users

1. Open Secure Hub.
2. Go to **Preferences > Device Information**.
3. Click **Refresh Policy**.

If you enabled Citrix PIN authentication, Secure Hub prompts users to create a PIN. After a user creates a PIN, XenMobile configures the device in Enterprise mode. In the XenMobile console, the **Manage > Devices** page then shows both MDM and MAM as active for the device.

User accounts, roles, and enrollment

March 18, 2021

You configure user accounts, roles, and enrollment in the XenMobile console on the **Manage** tab and the **Settings** page. Unless otherwise indicated, the steps for the following tasks are provided in this article.

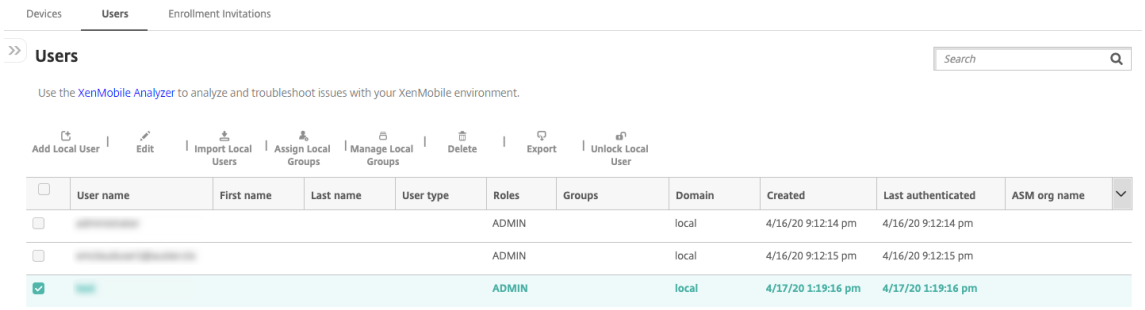
- User accounts and groups:

  - From **Manage > Users**, add user accounts manually or use a .csv provisioning file to import the accounts and to manage local groups.
  - From **Settings > Workflows**, use workflows to manage the creation and removal of user accounts.
- 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: Create and update notification templates.
- 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 steps that users must take to enroll their devices.
  - Enable AutoDiscovery in XenMobile for user enrollment

To add, edit, unlock, or delete local user accounts

You can add local user accounts to XenMobile 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.

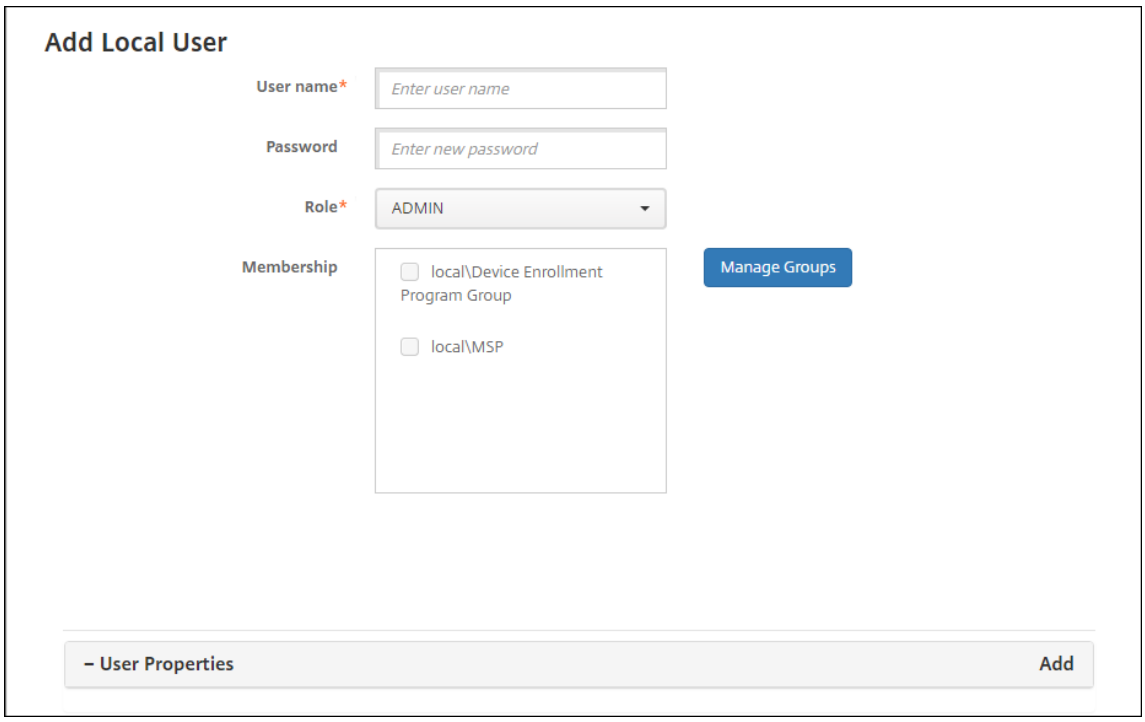
1. In the XenMobile console, click **Manage > Users**. The **Users** page appears.



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 spaces in names, as well as upper 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**.

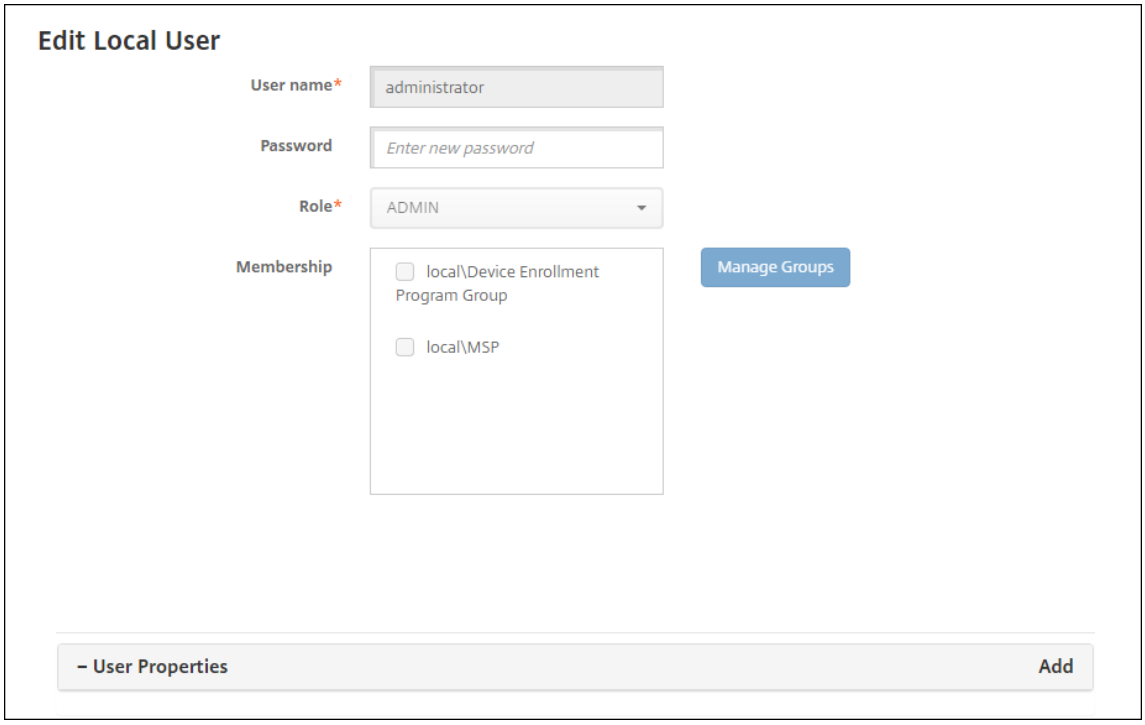
To delete an existing user property, hover over the line containing the property and then click the X on the right side. The property is deleted immediately.

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**.

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.



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

1. On the **Users** page, in the list of user accounts, click to select a user account.
2. Click **Unlock Local User**. A confirmation dialog box appears.
3. Click **Unlock** to unlock the user account or click **Cancel** to leave the user unchanged.

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.

1. Click **Delete**. A confirmation dialog box appears.
2. 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

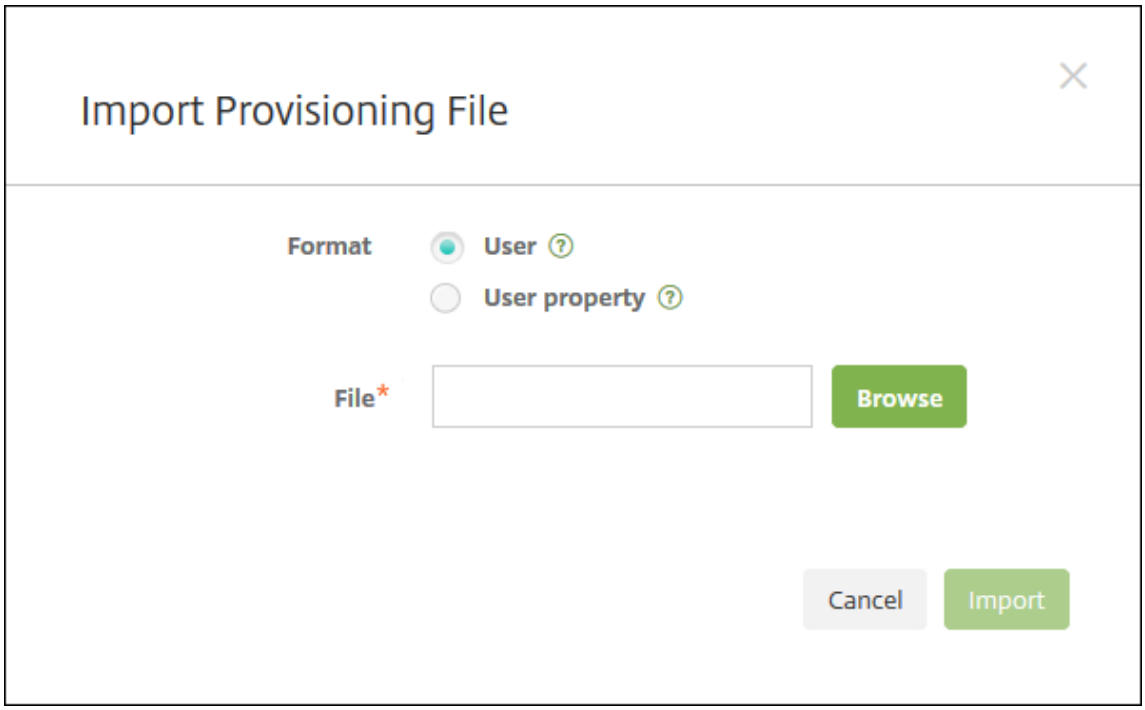
You can import local user accounts and properties from a .csv file called a provisioning file, which you can create manually. For more information about formatting provisioning files, see Provisioning file formats.

> **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 XenMobile, the user cannot enroll by using the corresponding LDAP credentials.
> - If importing user accounts to the XenMobile internal user directory, disable the default domain to speed up the import process. Keep in mind that disabling the domain affects enrollments, so reenable the default domain after the import of internal users completes.
> - 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 XenMobile.

1. In the XenMobile console, click **Manage > Users**. The **Users** page appears.
2. Click **Import Local Users**. The **Import Provisioning File** dialog box appears.



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 manually create a provisioning file to import user accounts and properties to XenMobile. The valid formats are as follows:

- **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 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\\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` means:

- **User:** `user01`
- **Password:** `pwd;01`
- **Role:** `USER`
- **Groups:**
  - `myGroup.users01`
  - `myGroup.users02`
  - `myGroup.users.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`

To configure enrollment security modes

You configure a device enrollment security mode to specify a security level and notification template for device enrollment in XenMobile.

XenMobile offers seven 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 XenMobile Server console from the **Settings > Enrollment** page.

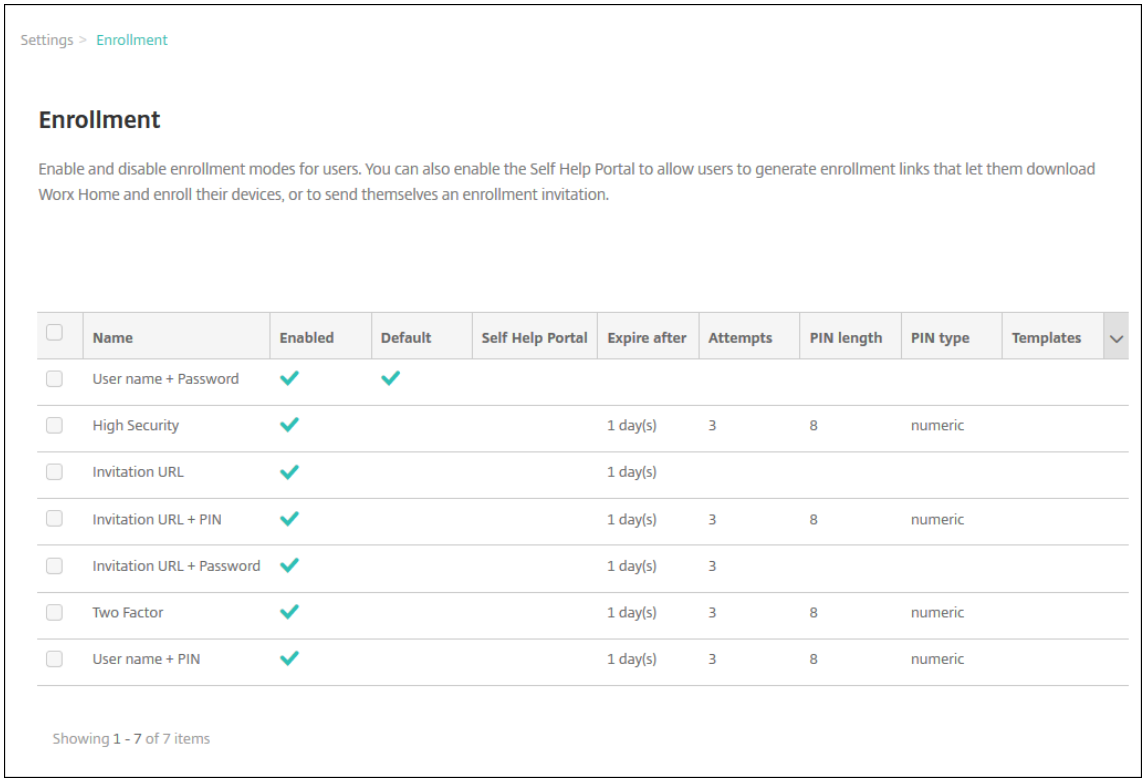
You can make some modes available on the Self-Help Portal. From the portal, users generate enrollment links that allow them to enroll their devices. iOS, iPadOS, macOS, and legacy Android users can choose to send themselves an enrollment invitation from the portal. Enrollment invitations aren't available for Android Enterprise and Windows devices.

You send enrollment invitations from the **Manage > Enrollment Invitations** page. For information, see Send an enrollment invitation.

> **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 XenMobile 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, disable the mode, or allow users access through the Self-Help Portal.

   > **Note:**
   >
   > When you select the check box next to an enrollment security mode, the options menu appears above the enrollment security mode list. When you click anywhere else in the list, the options menu appears on the right side of the listing.



Choose from these enrollment security modes:

- User name + Password
- High Security
- Invitation URL
- Invitation URL + PIN
- Invitation URL + Password
- Two Factor authentication
- User name + PIN

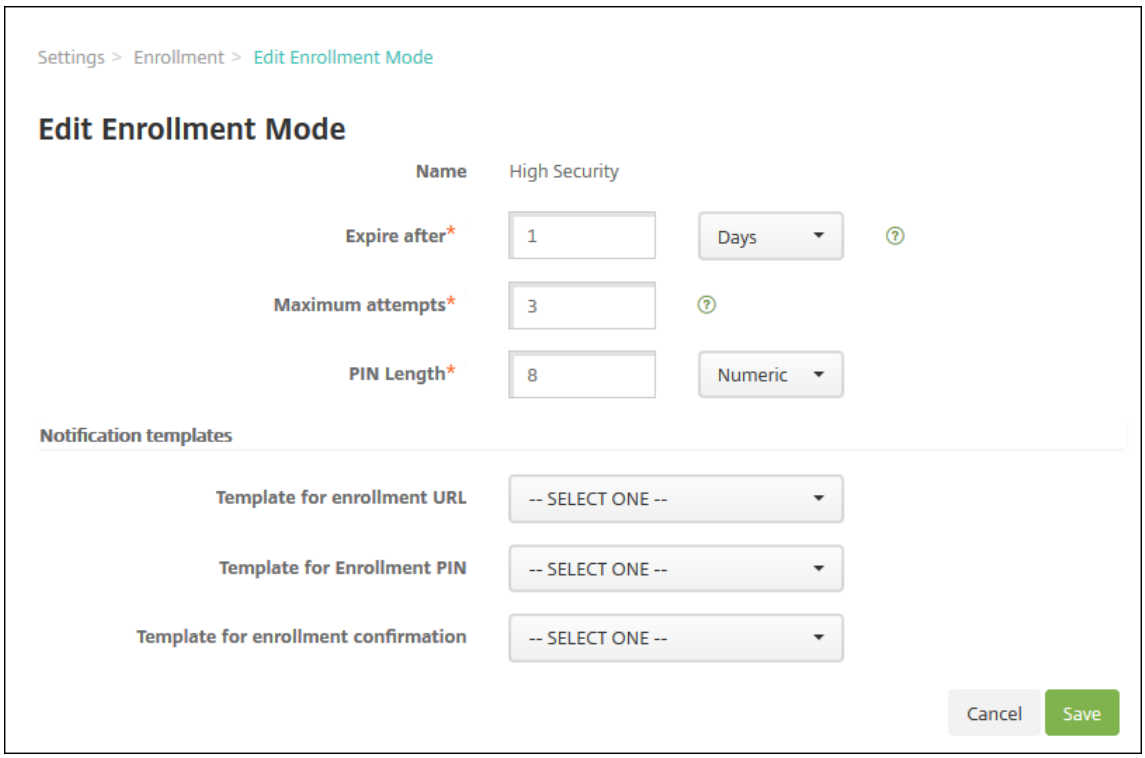
You can use enrollment invitations to restrict enrollment to users with an invitation only.

You can use one-time PIN (OTP) enrollment invitations as a two-factor authentication solution. OTP enrollment invitations control the number of devices a user can enroll.

For environments with the highest security requirements, you can tie enrollment invitations to a device by SN/UDID/EMEI. A two-factor authentication option is also available to require an Active Directory password and OTP.

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. The mode you select determines the options shown.



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 XenMobile. For more information on notification templates, see Creating or updating 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

When you set an enrollment security mode as the default, the 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 a request for enrollment for each device enrollment.

> **Note:**
>
> The only enrollment security modes that you can use as a default are **Only User name + Password**, **Two Factor**, or **User name + PIN**.

1. Select the default enrollment security mode, either **User name + Password**, **Two Factor**, or **User name + PIN**.

   To use a mode as the default, first enable it.

2. 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 can change how users can 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.

To enable an enrollment security mode on the Self-Help Portal

Enabling an enrollment security mode on the Self-Help Portal lets users enroll their devices in XenMobile individually.

> **Note:**
>
> - The enrollment security mode must be enabled and bound to notification templates to be made available on the Self-Help Portal.
> - You can only enable one enrollment security mode on the Self-Help Portal at a time.

1. Select an enrollment security mode.
2. Click **Self Help Portal**. The enrollment security mode you selected is now available to users on the Self-Help Portal. Any mode already enabled on the Self-Help Portal is no longer available to users.

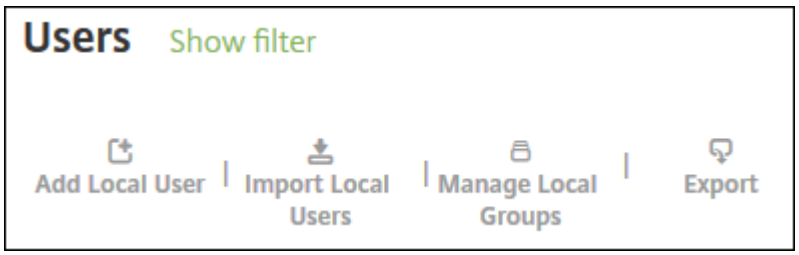
Adding or removing groups

You manage groups in the **Manage Groups** dialog box in the XenMobile console on these pages: **Users**, **Add Local User**, or **Edit Local User**. There is no group edit command.

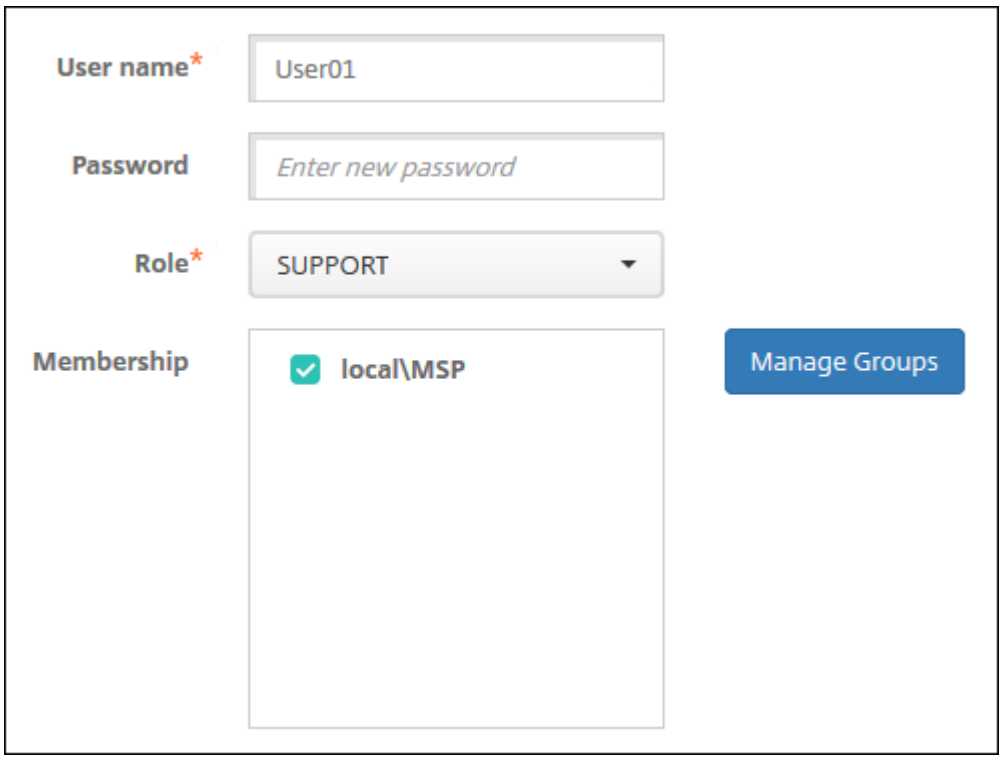
If you remove a group, keep in mind that removing the group has no effect on user accounts. Removing a group simply removes user association with that group. Users also lose access to apps or profiles provided by the Delivery Groups that are associated with that group; any other group associations, however, remain intact. If users are not associated with any other local groups, they are associated at the top level.

To add a local group

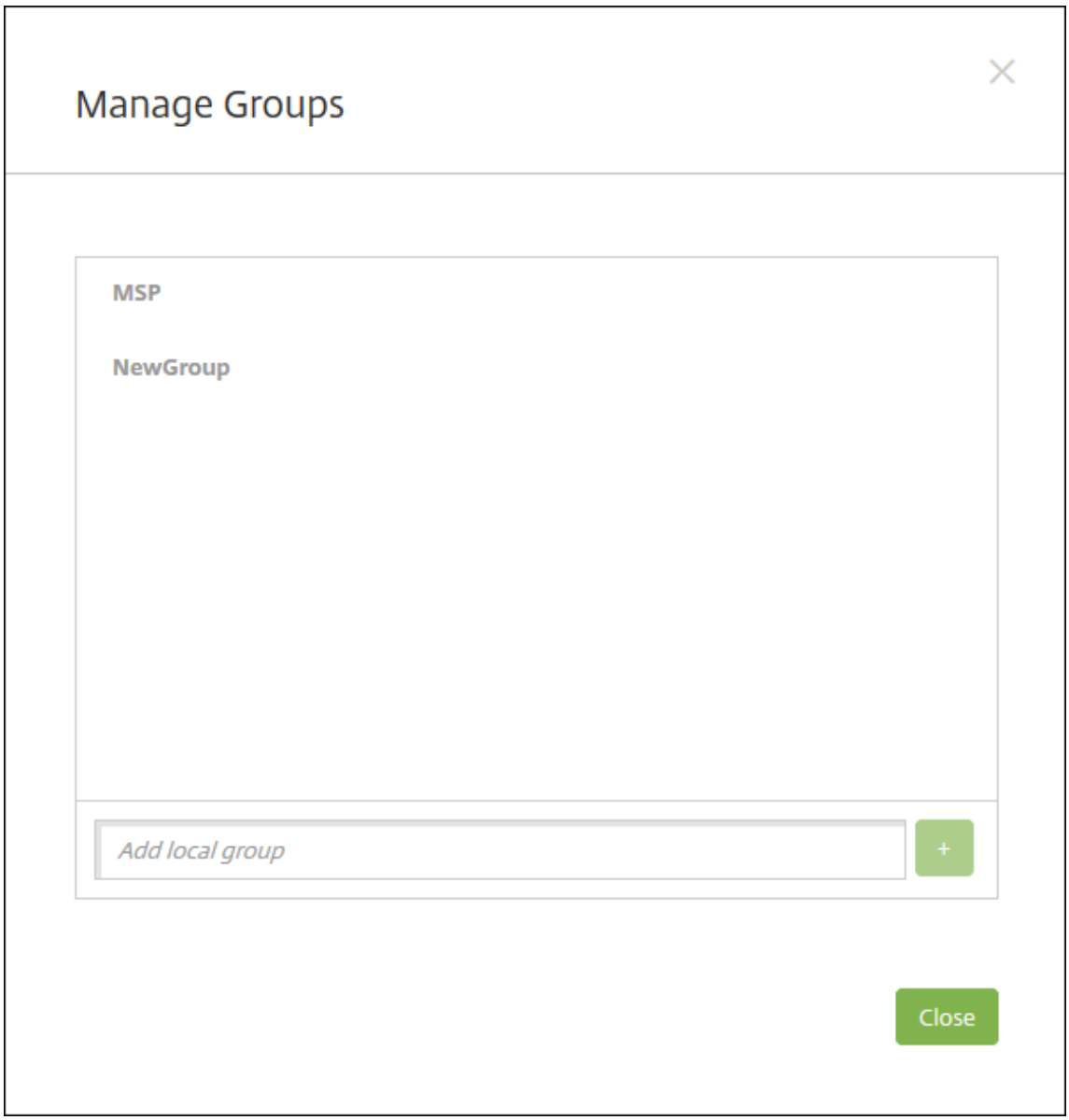
1. Do one of the following:
   - On the **Users** page, click **Manage Local Groups**.



   - On either the **Add Local User** page or the **Edit Local User** page, click **Manage Groups**.



The **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**.

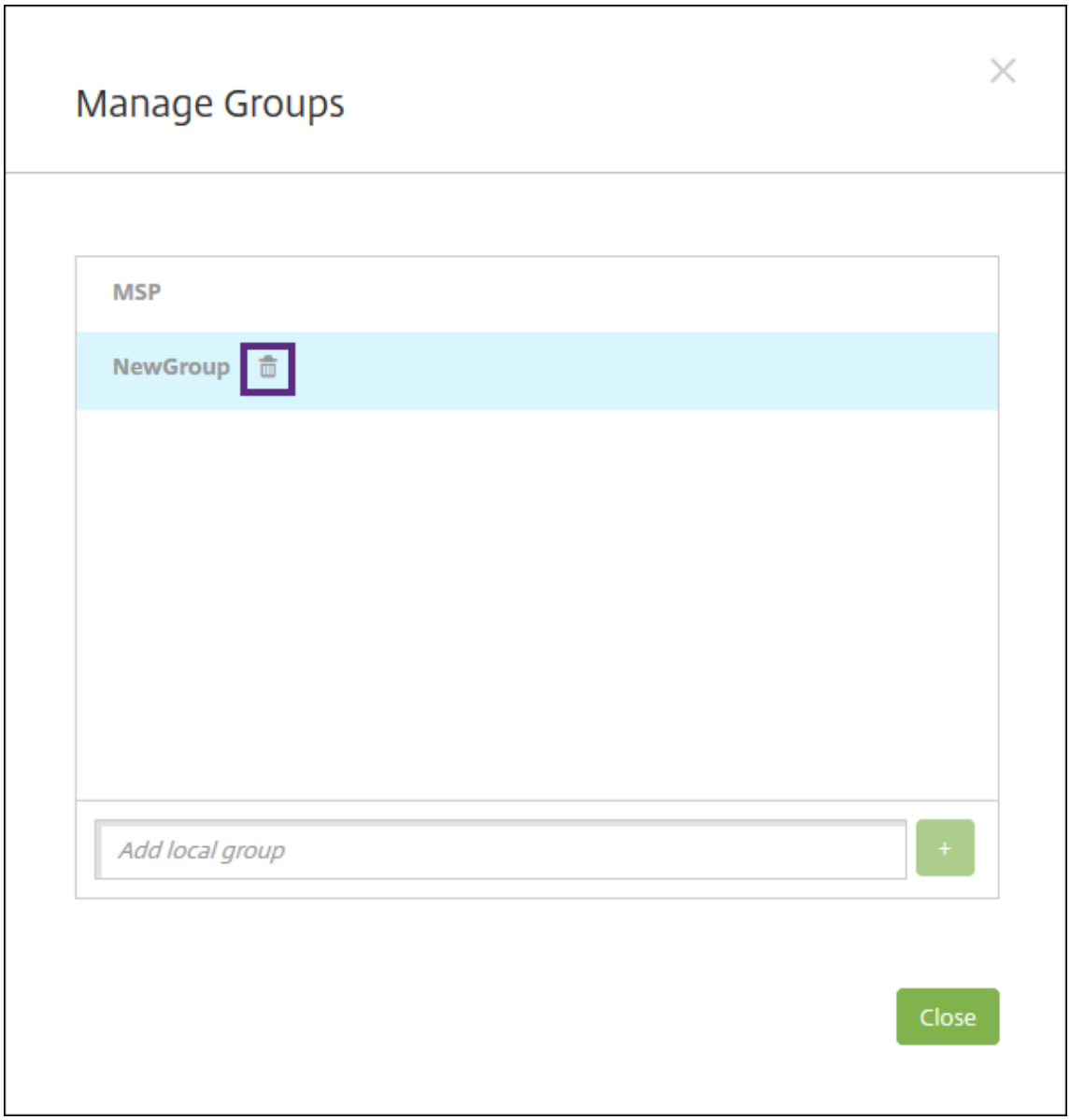
To remove a group

Removing a group has no effect on user accounts. Removing a group simply 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 are not 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 can use a workflow, identify individuals in your organization who have the authority to approve user account requests. Then, you can use the workflow template to create and approve user account requests.

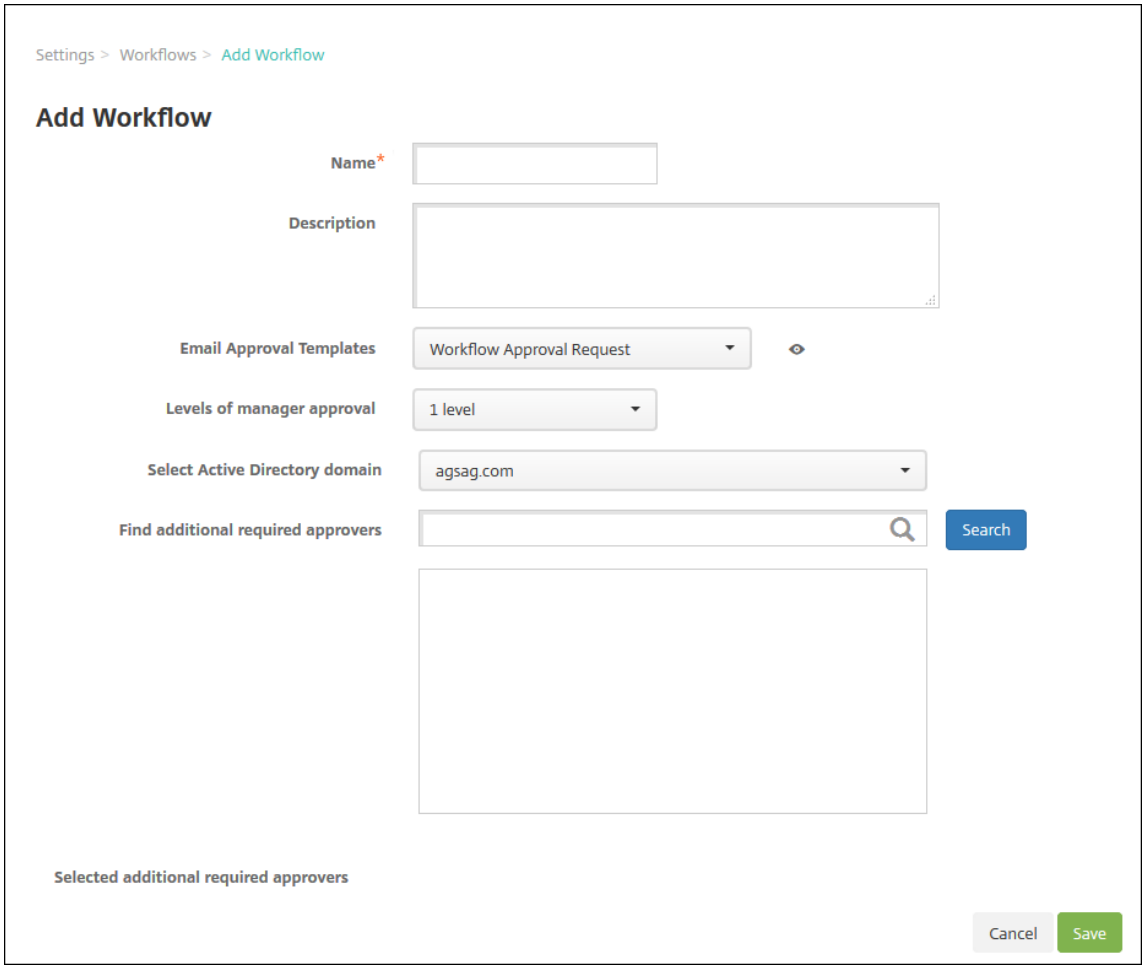
When you set up XenMobile for the first time, you configure workflow email settings, which must be set before you can use workflows. You can change workflow email settings at any time. These settings include the email server, port, email address, and whether the request to create the user account requires approval.

You can configure workflows in two places in XenMobile:

- In the **Workflows** page in the XenMobile 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, you provide a workflow name and then configure the individuals who can approve the user account request. See Adding Apps to XenMobile.

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 XenMobile 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 XenMobile 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.



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 XenMobile 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

May 10, 2021

An enrollment profile specifies the following:

- Device management enrollment options for Android and iOS devices. For Android, the enrollment options available for the MDM+MAM (ENT) server mode differ from the options for MDM mode.
- 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 XenMobile Server 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)

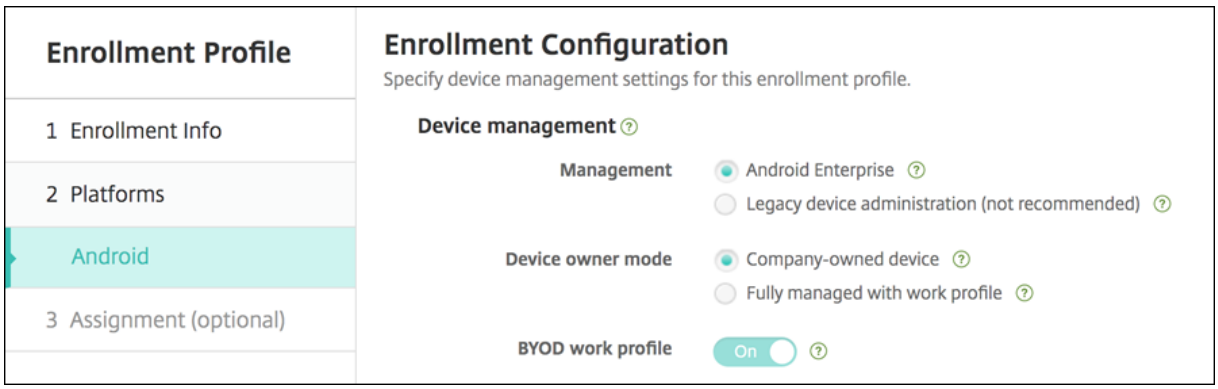
When you create a delivery group, you can use the default enrollment profile named Global or specify a different enrollment profile.

Enrollment profile features by platform include the following.

- **For Android devices:** You specify the device owner mode. For example: Fully managed, fully managed with work profile, and BYOD work profile. The **Dedicated device** option appears only when you have an Enterprise or Advanced license for XenMobile. New devices enroll in Android Enterprise and app management by default. The enrollment security modes **User name + PIN**, **Invitation URL**, **Invitation URL + PIN**, and **Invitation URL + Password** aren't available for Android Enterprise.
- **For iOS devices:** You specify the device enrollment type: Device enrollment or don't manage devices. The iOS settings appear only when you have an Enterprise or Advanced license for XenMobile. New devices enroll in Apple device management and app management by default.

If you don't need to enroll dedicated devices for Android devices or MAM-only enrollment for Android or iOS devices, you can disable the server property `enable.multimode.xms`. However, keeping this property enabled means you need only one XenMobile Server to handle all types of enrollment profiles. See Server properties.

When you disable `enable.multimode.xms`, only the settings in this screenshot are available:

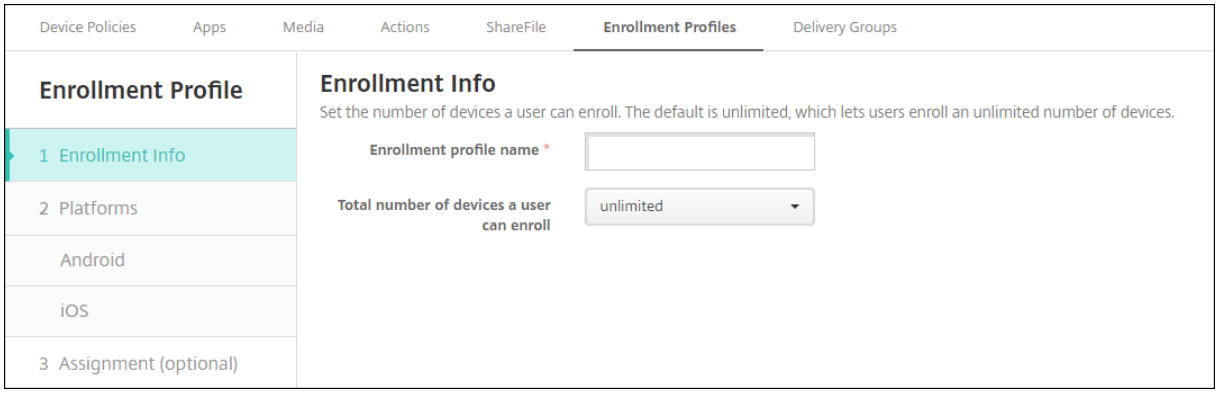


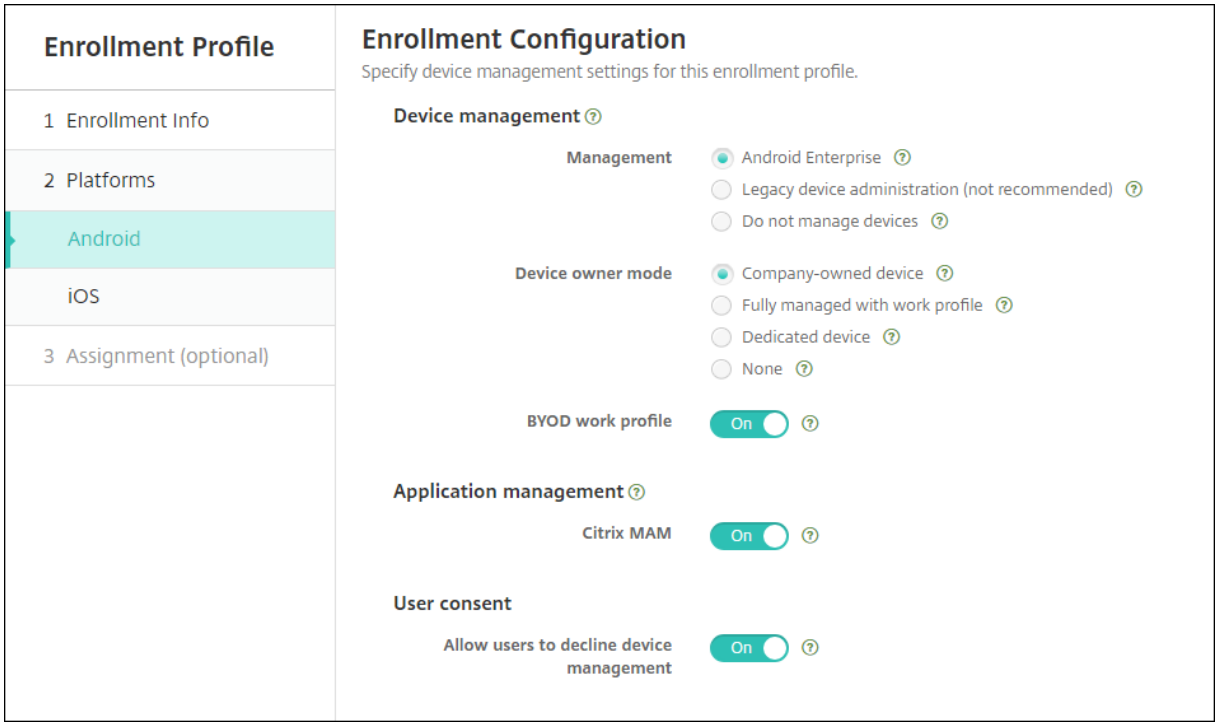
For more details about these settings, see Android Enterprise.

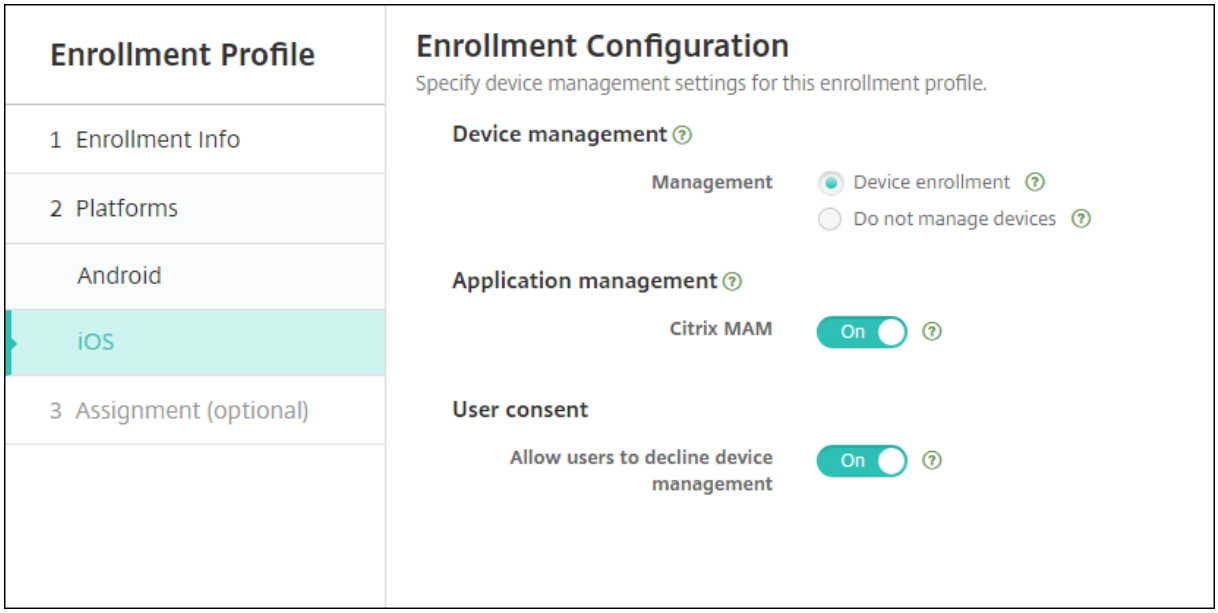
Global enrollment profile

The default enrollment profile is named Global. The Global profile is useful for testing until you have a chance to create enrollment profiles.

The following screenshots show the default settings for the Global enrollment profile.







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. XenMobile Server 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, XenMobile Server 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:
  - Adding MAM to an enrollment profile that’s configured for MDM.
  - Moving a device that’s enrolled in MDM to a delivery group configured for MDM+MAM. That change impacts new device enrollments only. Existing device enrollments aren’t impacted.
  - Adding MDM to an enrollment profile that’s configured for MAM.

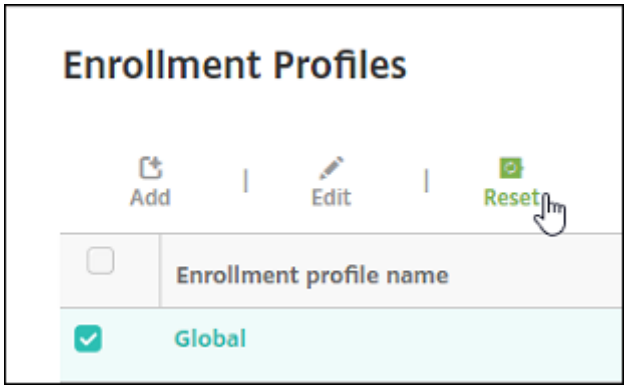
- Switching to a different enrollment profile does not affect existing enrolled devices. However, users must unenroll and then reenroll those devices for the changes to take effect.

To create an enrollment profile

1. In the XenMobile Server 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 and iOS devices that a user enrolls.
3. Complete the platform pages. For information about enrollment settings specific to the platforms, see:
   - Android Enterprise
   - iOS: Supported enrollment methods
4. On the **Assignment** 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. XenMobile 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.



Configure roles with RBAC

July 9, 2021

Each predefined role-based access control (RBAC) role has certain associated access and feature permissions. This article describes what each of those permissions does. For a full list of default permissions for each built-in role, download Role-Based Access Control Defaults.

When you *apply permission*s, you are defining the user groups the RBAC role has the permission to manage. The default administrator cannot change the applied permission settings. By default, the applied permissions apply to all user groups.

When you make an *assignment*, you are assigning the RBAC role to a group, so that the group of users owns the RBAC administrator rights.

> **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.

This article contains the following sections:

Admin Role

Users with the predefined Admin role have access or do not have access to the following features in XenMobile. By default, **Authorized access** (except Self-Help Portal), **Console features**, and **Apply permissions** are enabled.

Authorized access

Admin console access	Administrators have access to all features on the XenMobile console.
Self-Help Portal access	Administrators do not have Self-Help Portal access.
Shared devices enroller	Administrators do not have Shared devices enroller access. This feature is intended for users who need to enroll shared devices.
Remote Support access	Administrators own Remote Support access.*

Public API access	Administrators have access to the public API to perform actions programmatically that are available on the XenMobile console. The actions include administering certificates, apps, devices, delivery groups, and local users.
COSU devices enroller	Provides a way for administrators to enroll dedicated Android Enterprise devices (also known as COSU devices) if this capability is not configured using an enrollment profile.

* Remote support enables your help desk representatives to take remote control of managed Windows CE and Android mobile devices. Screen cast is supported on Samsung Knox devices only. Remote support isn't available for clustered on-premises XenMobile Server deployments. Remote Support is no longer available for new customers as of January 1, 2019. Existing customers can continue to use the product, however Citrix doesn't provide enhancements or fixes.

Console features

Administrators have unrestricted access to the XenMobile console.

Dashboard	The **Dashboard** is the first page that administrators see after logging on to the XenMobile console. The **Dashboard** shows basic information about notifications and devices.
Reporting	The **Analyze > Reporting** page provides pre-defined reports that let you analyze your app and device deployments.

Devices	The **Manage > Devices** 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 **Manage > Users** page is where you can add, edit, or delete local users and local user groups.
Enrollment	The **Manage > Enrollment Invitations** page is where you manage how users are invited to enroll their devices in XenMobile.
Policies	The **Configure > Device Policies** page is where you manage device policies, such as VPN and Wi-Fi.
Apps	The **Configure > Apps** page is where you manage the various apps that users can install on their devices.
Media	The **Configure > Media** page is where you manage the various media that users can install on their devices.
Action	The **Configure > Actions** page is where you manage responses to trigger events.
Enrollment Profiles	The **Configure > Enrollment Profiles** page is where you configure enrollment profiles (modes) to allow users to enroll their devices.

Delivery Groups	The **Configure > Delivery Groups** page is where you manage delivery groups and the resources associated with them.
Settings	The **Settings** page is where you manage system settings, such as client and server properties, certificates, and credential providers. **Important:** 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 **Troubleshooting and Support** page is where you perform troubleshooting activities such as running diagnostics and generating logs.

Devices

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, See the location of a device, Track device, Track a device's location over time.
Lock device	Remotely lock a device so that users cannot 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 DEP/Bypass activation lock	Store a bypass code on a supervised iOS device when Activation Lock is enabled. If you need to erase the device, use this code to clear the Activation Lock automatically.
Rings the device	Remotely ring a Windows device at full volume for 5 minutes.
Reboot the device	Restart Windows devices from the XenMobile console.
Deploy to device	Send apps, notifications, restrictions, and so on 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 XenMobile.
Devices import	Import a group of devices from a file into XenMobile.

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 XenMobile.
App lock	Deny access to all apps on a device. On Android, users can't log into XenMobile. On iOS, users can log in, but they can't access apps.
App wipe	On Android, this action deletes the user's XenMobile account. On iOS, this action deletes the encryption key users need to access XenMobile 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 **Manage > Devices**, you can put a supervised device in lost mode to block a supervised device on the lock screen. Lost mode also enables you to locate the device when the device is lost or stolen.
Disable lost mode	On **Manage > Devices**, you can disable lost mode for a device that is set to lost mode.
OS Update device	You can deploy a Control OS Updates device policy to devices.
Shut down device	Shut down iOS devices from the XenMobile console.
Restart device	Restart iOS devices from the XenMobile console.

Local Users and Groups

Administrators manage local users and local user groups on the **Manage > Users** page in XenMobile.

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 XenMobile.

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 XenMobile.
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 XenMobile.
Add/Delete category	Add or delete a category in which apps can appear in the XenMobile 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 obtained from a public app store or through 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 that is defined by a trigger (event, device or user property, or installed app name) and associated response.
Edit action	Change an action that is defined by a trigger (event, device or user property, or installed app name) and associated response.
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 a 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

Settings

Administrators configure various settings on the **Settings** pages.

RBAC	RBAC Assignment, Assign roles. **Important:** 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.
License	For on-premises XenMobile Server. Administer your Citrix licenses.
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, Certificates SSL Listener

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 Test Connection button on the **Settings > PKI Entities** page to ensure that the server is accessible.
Client Properties	Manage various properties on user devices, such as passcode type, strength, or 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 XenMobile Store. Add a custom logo that appears in a XenMobile Store or Secure Hub.
Carrier SMS Gateway	Set up carrier SMS gateways to configure notifications that XenMobile 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.
Apple Deployment Program	Add an Apple Deployment Program account to XenMobile.

Apple Configurator Device Enrollment	Configure Apple Configurator settings in XenMobile.
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.
Citrix Gateway	For on-premises XenMobile Server. Add a Citrix Gateway. Choose whether to enable authentication and whether to push a user certificate for authentication. Choose a credential provider.
Network Access Control	Set the conditions that determine a device is non-compliant and therefore denied access to the network.
Samsung Knox	Enable or disable XenMobile to query Samsung Knox attestation server REST APIs.
Server Properties	Add or modify server properties. Requires restarting XenMobile on all nodes.
Syslog	For on-premises XenMobile Server. Send log files to a System Log (syslog) server using the server host name or IP address.
XenApp and XenDesktop	Allow users to add Virtual Apps and Desktops through Secure Hub.
Citrix Files	When using XenMobile with Enterprise accounts: Configure settings to connect to the Content Collaboration account and administrator service account to manage user accounts. Requires existing Citrix Files domain and administrator credentials. When using XenMobile with storage zone connectors: Configure XenMobile to point to network shares and SharePoint locations defined in storage zones connectors.

Experience Improvement Program	For on-premises XenMobile Server. Opt into or out of sending anonymous statistics and usage information to Citrix.
Microsoft Azure	For on-premises XenMobile Server. Integrate XenMobile with Microsoft Azure.
Android Enterprise	Configure Android Enterprise server settings.
Identity Provider (IdP)	Configure an identity provider.
XenMobile Tools	Access XenMobile Tools page.
SNMP Configuration	Enable SNMP for XenMobile Server nodes. Edit or add monitoring users, set up the SNMP manager where trap notifications appear, and configure trap intervals and thresholds.

Support

Administrators can perform various support tasks.

Citrix Gateway Connectivity Checks	Perform various connectivity checks for Citrix Gateway by IP address. Requires a user name and password.
XenMobile Connectivity Checks	Perform connectivity checks for selected XenMobile features, such as database, DNS, or Google Plan.
Create Support Bundles	For on-premises XenMobile Server. Create a file to send to Citrix Support for troubleshooting. Contains system information, logs, database information, core information, trace files, and the latest configuration information for XenMobile or Citrix Gateway.
Citrix Product Documentation	Access the public Citrix XenMobile documentation site.
Citrix Knowledge Center	Access the Citrix Support site to search for knowledge base articles.

Logs	Access and analyze log file details for debug, admin audit, and user audit.
Cluster Information	For on-premises XenMobile Server. Access information about each of the nodes in a clustered environment.
Garbage Collection	For on-premises XenMobile Server. Access information about memory objects no longer in use.
Java Memory Properties	For on-premises XenMobile Server. Access a snapshot of Java memory usage, memory details, and memory pool details.
Macros	Populate user or device property data within 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 XenMobile for the status of a device as sent to Citrix Gateway connector for Exchange ActiveSync based on the device ActiveSync ID.
Anonymization and de-anonymization	For on-premises XenMobile Server. When you create support bundles in XenMobile, sensitive user, server, and network data is made anonymous by default. You can change this behavior in **Support > Anonymization and De-anonymization** under **Advanced**.
Log Settings	Customize the log level or add a custom logger.

Restrict Group Access

Admin users can apply permissions to all user groups.

Device Provisioning Role

> **Important:**
>
> The Device Provisioning Role applies only to Windows CE devices.

Users with the predefined Device Provisioning role have limited access to console features. By default, their permission is set to all user groups and they cannot change this setting.

Console features

Device provisioning users have the following restricted access to the XenMobile console. By default, each of the following features is enabled.

Devices

Edit device	Change settings on the device.
Add/Delete device	Add or remove devices from XenMobile.

Settings

Device provisioning users can access the **Settings** page, but do not have the rights to configure the features.

Support Role

Users with the Support role have access to remote support. Their permissions apply to all users by default and they cannot edit this setting.

User Role

Users with the User role have the following limited access to XenMobile.

Authorized access

Self-Help Portal	Users have access only to the Self-Help Portal in XenMobile.

Console features

Users have the following restricted access to the XenMobile console.

Devices

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 DEP/Bypass activation lock	Store a bypass code on a supervised iOS device when Activation Lock is enabled. If you need to erase the device, use this code to clear the Activation Lock automatically.
Rings the device	Remotely ring a Windows device at full volume for 5 minutes.

Reboot the device	Restart a Windows device.
View software inventory	See what software is installed on a device.

Enrollment

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.

Restrict Group Access

For all four default roles, this permission is set by default and can be applied to all user groups. You cannot edit the role.

Configure roles with RBAC

The Role-Based Access Control (RBAC) feature in XenMobile 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.

XenMobile implements four default user roles to logically separate access to system functions:

- **Administrator:** Grants full system access.
- **Device Provisioning:** Grants access to basic device administration for Windows CE devices.
- **Support:** Grants access to remote support.
- **User:** Used by users who can enroll devices and access the Self-Help Portal.

You can also use the default roles as templates that you customize to create user roles. You can assign the roles permissions to access specific system functions beyond the functions defined by the default roles.

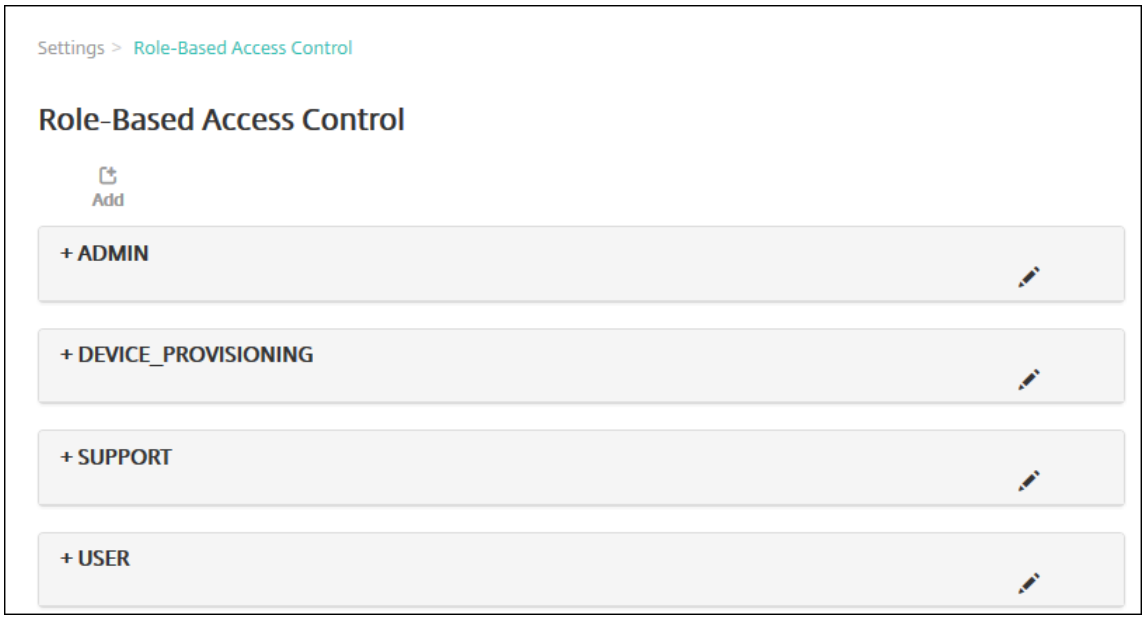
Roles can be assigned to local users (at the user level) or to Active Directory groups (all users in that group have the same permissions). If a user belongs to several Active Directory groups, all the permissions are merged together to define the permissions for that user. For example, suppose that ADGroupA users can locate manager devices and ADGroupB users can wipe employee devices. In that case, a user who belongs to both groups can locate and wipe devices of managers and employees.

> **Note:**
>
> Local users might have only one role assigned to them.

You can use the RBAC feature in XenMobile to do the following:

- Create a role.
- Add groups to a role.
- Associate local users to roles.

1. In the XenMobile console, go to **Settings > Role-Based Access Control**. The **Role-Based Access Control** page appears, which displays the four default user roles, plus any roles you have previously added.



   If you click the plus sign (+) next to a role, the role expands to show all the permissions for that role, as shown in the following figure.

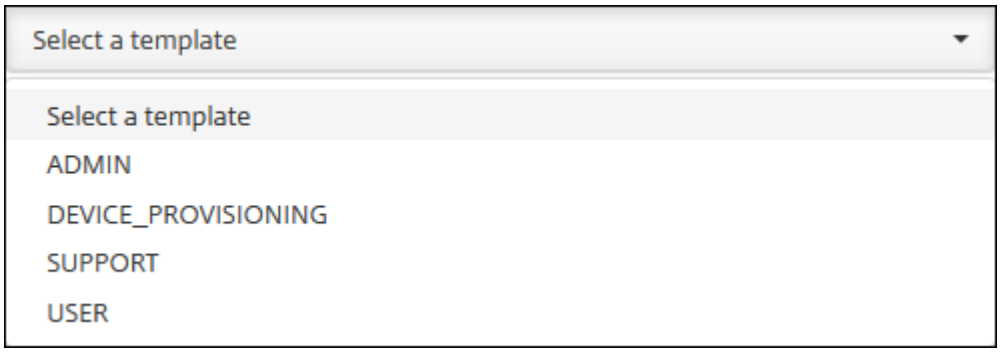
2. Click **Add** to add a new user role. To edit the role, click the pen icon to the right of an existing role. To delete the role, click the trash can icon to the right of a role. You can't delete the default user roles.

- When you click **Add** or the pen icon, the **Add Role** or the **Edit Role** page appears.
- When you click the trash can icon, a confirmation dialog appears. Click **Delete** to remove the selected role.

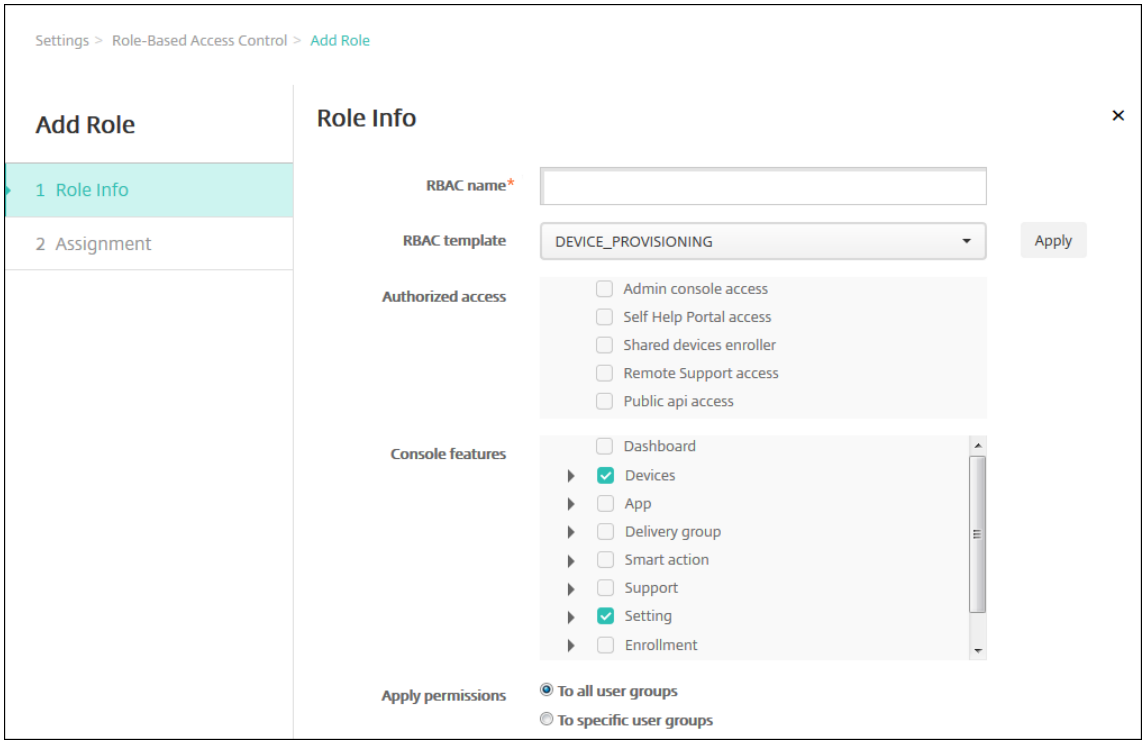
3. Enter the following information to create or edit a user role:

   - **RBAC name:** Enter a descriptive name for the new user role. You cannot change the name of an existing role.
   - **RBAC template:** Optionally, click a template as the starting point for the new role. You cannot select a template if you are editing an existing role.

   RBAC templates are the default user roles. They define the access to system functions that users associated with that role have. After you select an RBAC template, you can see all permissions associated with that role in the **Authorized Access** and **Console Features** fields. Using a template is optional. You can directly select the options you want to assign to a role in the **Authorized Access** and **Console Features** fields.

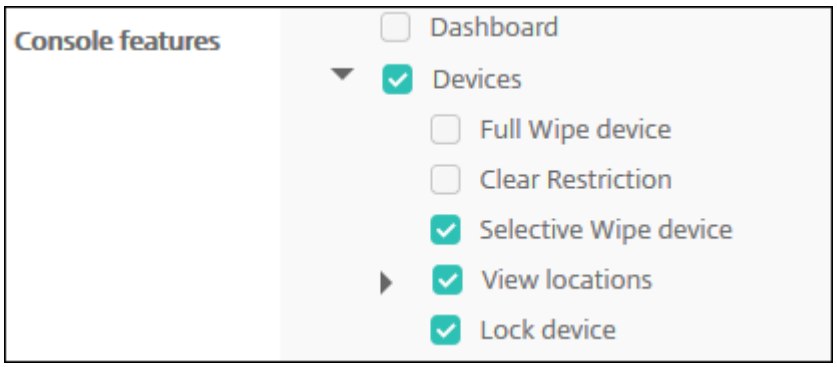


4. Click **Apply** near the selected **RBAC template** field to populate **Authorized access** and **Console features** with the pre-defined access and feature permissions.



5. Select and clear the check boxes in **Authorized access** and **Console features** to customize the role.

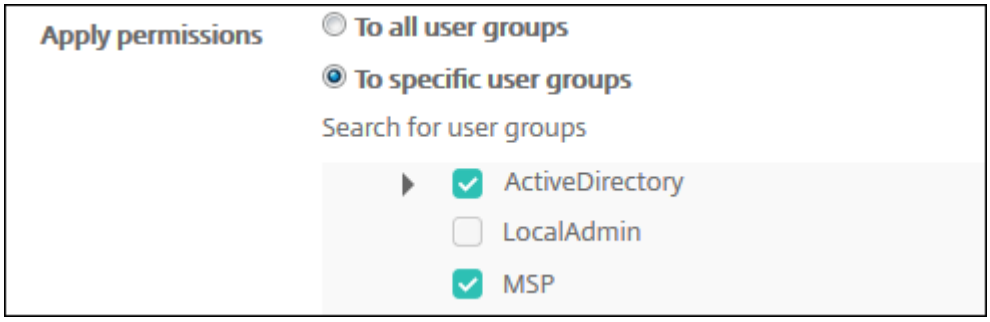
   If you click the triangle next to a Console feature, permissions specific to that feature appear that you can select and clear. Clicking the top-level check box prohibits access to that console area. Select individual options below the top level to enable those options. For example, in the following figure, the **Full Wipe device** and **Clear Restrictions** options don't appear for users assigned to the role. The checked options do appear.



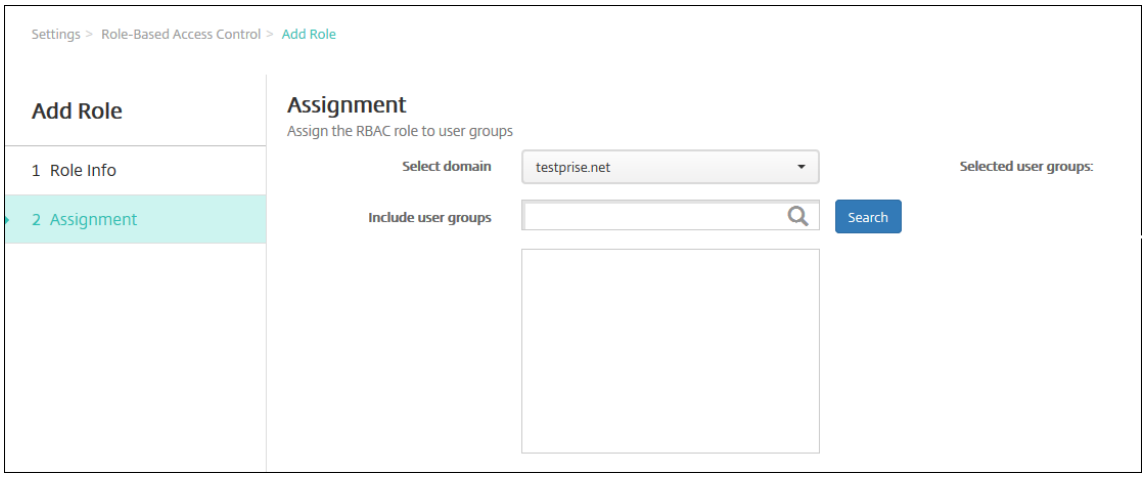
6. **Apply permissions:** Select one or more user groups to limit which groups the administrator can manage. If you click **To specific user groups**, a list of groups appears from which you can select one or more groups.

   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

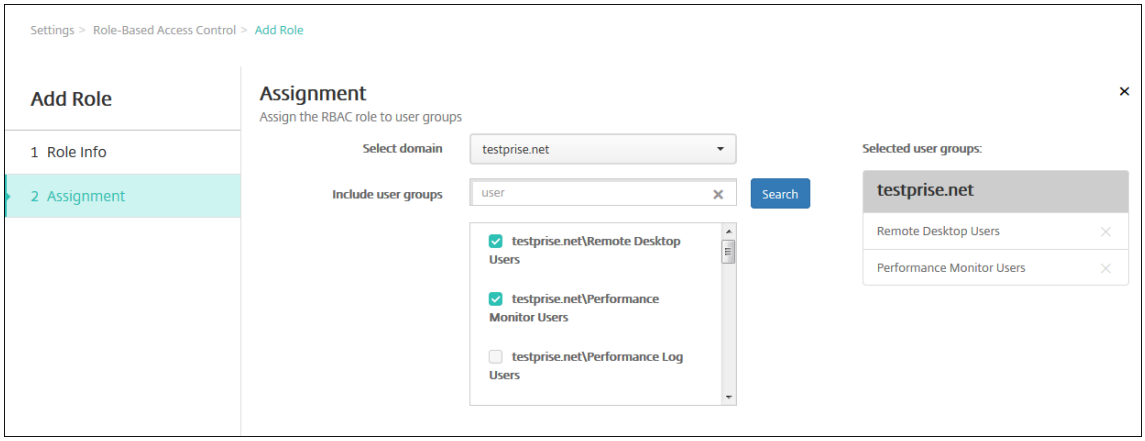


7. Click **Next**. The **Assignment** page appears.



8. Enter the following information to assign the role to user groups.

- **Select domain:** In the list, click a domain.
- **Include user groups:** Click Search to see a list of all available groups, or type a full or partial group name to limit the list to only groups with that name.
- In the list that appears, select the user groups to which you want to assign the role. When you select a user group, the group appears in the **Selected user groups** list.



> **Note:**
>
> To remove a user group from the **Selected user groups** list, click the X next to the user group name.

9. Click **Save**.

Notifications

October 29, 2020

You can use notifications in XenMobile for the following purposes:

- To communicate with select groups of users for a number of 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 XenMobile, you must configure a gateway and a notification server. You can set up a notification server in XenMobile to configure Simple Mail Transfer Protocol (SMTP) and Short Message Service (SMS) gateway servers to 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 by issuing command strings and supplying necessary data, typically over a Trans-

mission Control Protocol (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.

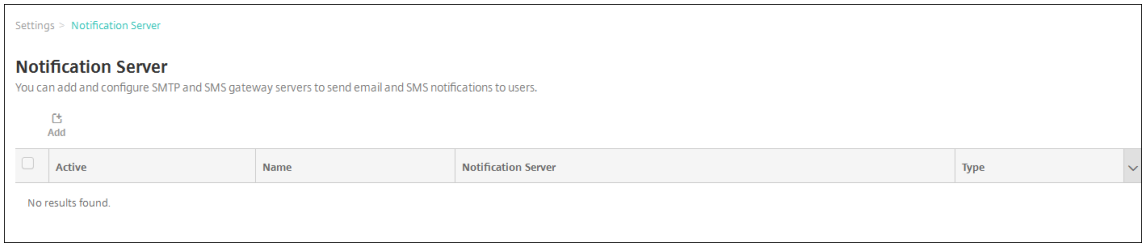
You can also set up a Carrier SMS Gateway in XenMobile to configure notifications that are sent through a SMS gateway of a carrier. Carriers use SMS gateways to send or receive SMS transmissions to or from a telecommunications network. These text-based messages use standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages.

Prerequisites

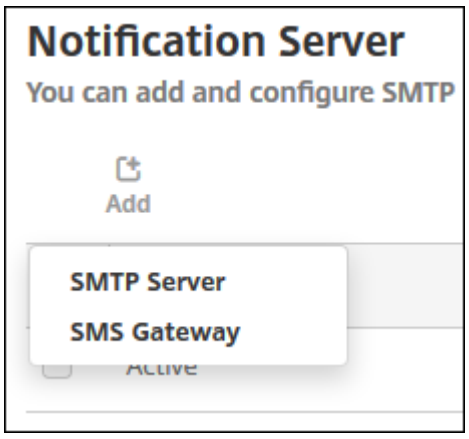
- Before configuring the SMS gateway, consult your system administrator to determine the server information. It's important to know whether the SMS server is hosted on an internal corporate server, or whether the server is part of a hosted email service. In that case, you need information from the website 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 XenMobile located in your network DMZ to point back to the SMTP server on your internal network. That enables XenMobile to send notifications successfully.

Configure an SMTP server and SMS gateway

1. In the XenMobile 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.

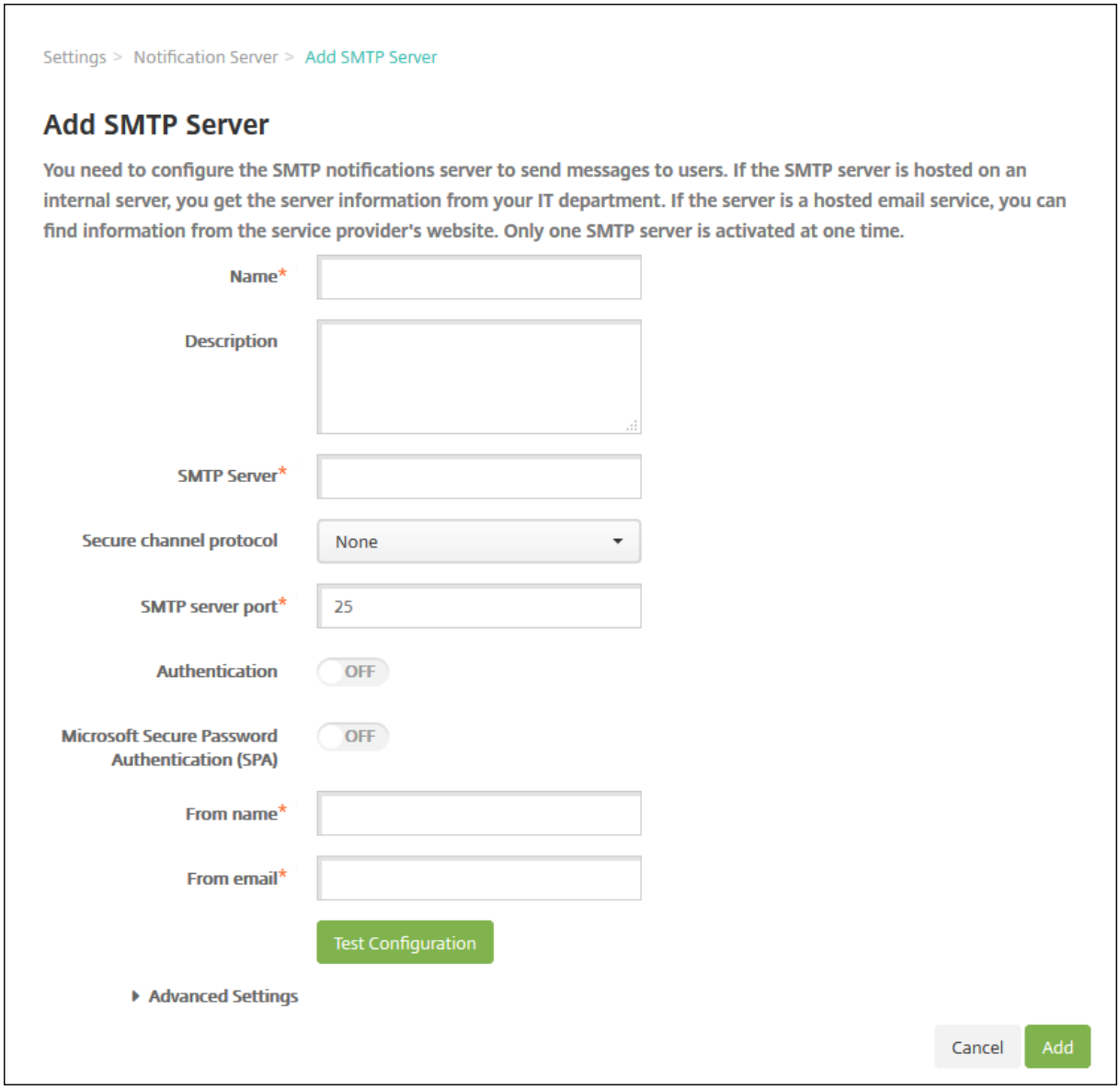


3. Click **Add**. A menu appears with options to configure an SMTP server or an SMS gateway.



- To add an SMTP server, click **SMTP Server** and then see To add an SMTP server for the steps to configure this setting.
- To an SMS gateway, click **SMS Gateway** and then see To add an SMS gateway for the steps to configure this setting.

Add an SMTP server



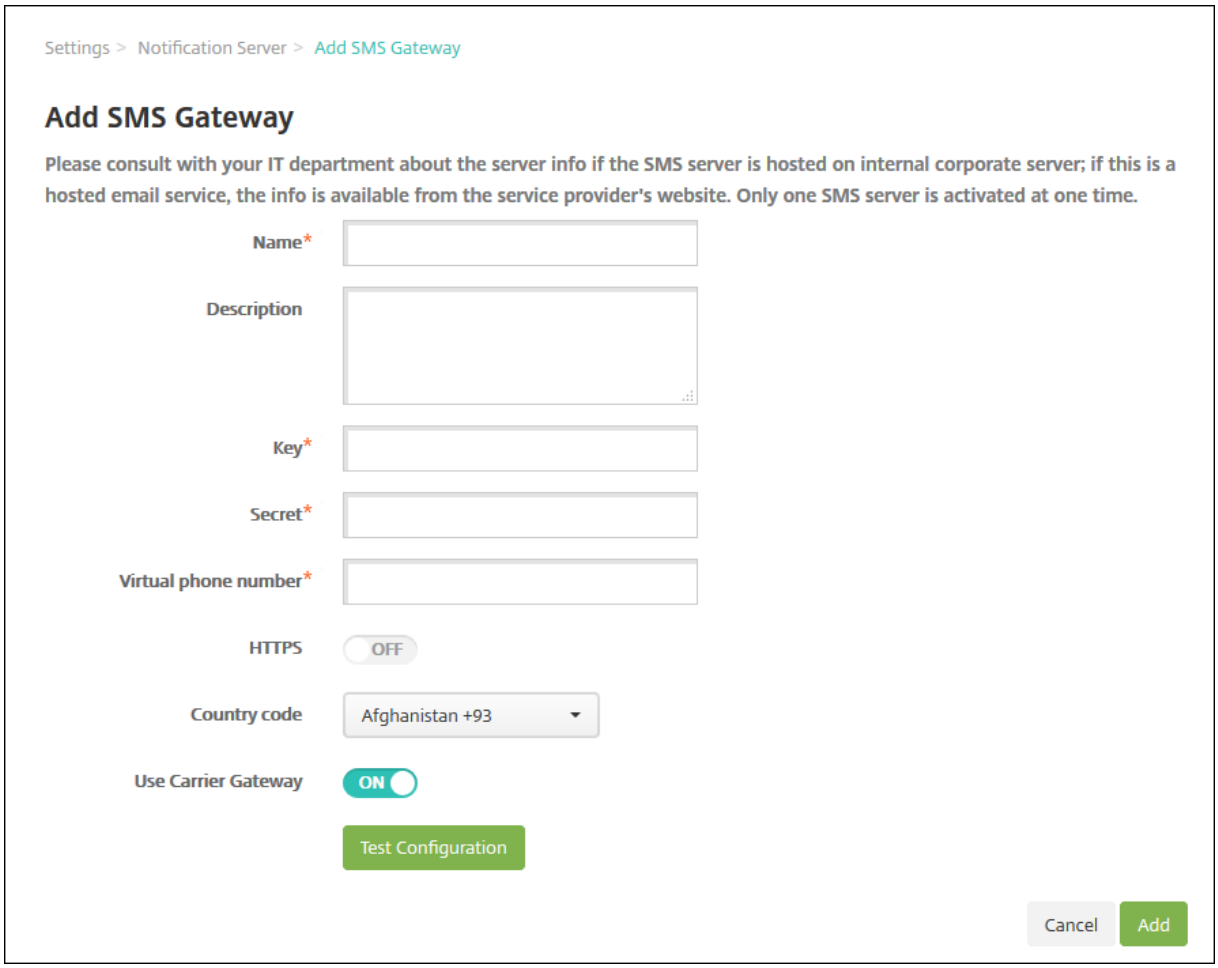
1. Configure these settings:

   - **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. The host name may be 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, the port is set 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 is continuously failing because of timeouts. Use caution when decreasing this value; it could increase 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



Note:

XenMobile 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 in the event that a password is lost or stolen. This field is required.
   - **Virtual Phone Number:** This field is used when sending to North American phone numbers (with the +1 prefix). You must type a Nexmo virtual phone number and you must only use digits in this field. 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**.

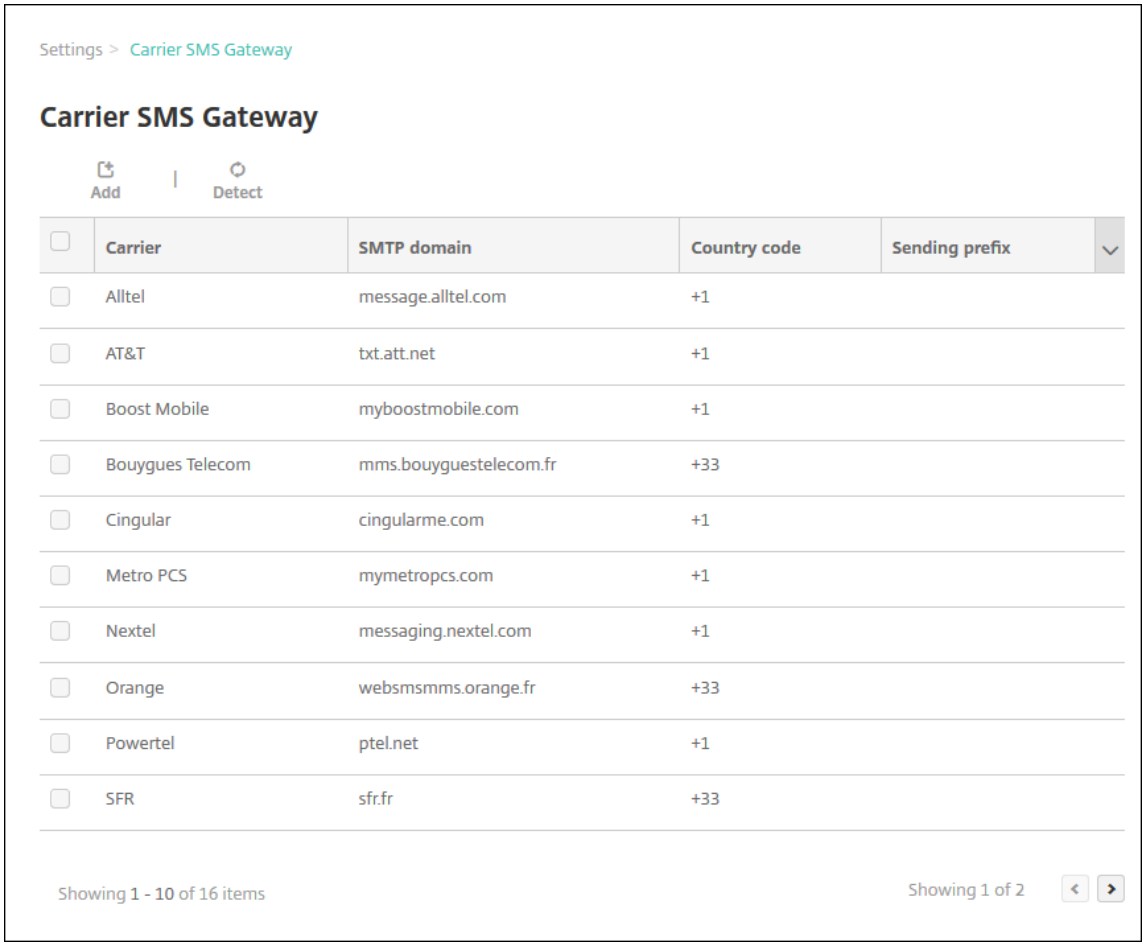
- **Country Code:** In the list, click the default SMS country code prefix for recipients in your organization. This field always starts with a + symbol. The default is **Afghanistan +93**.

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

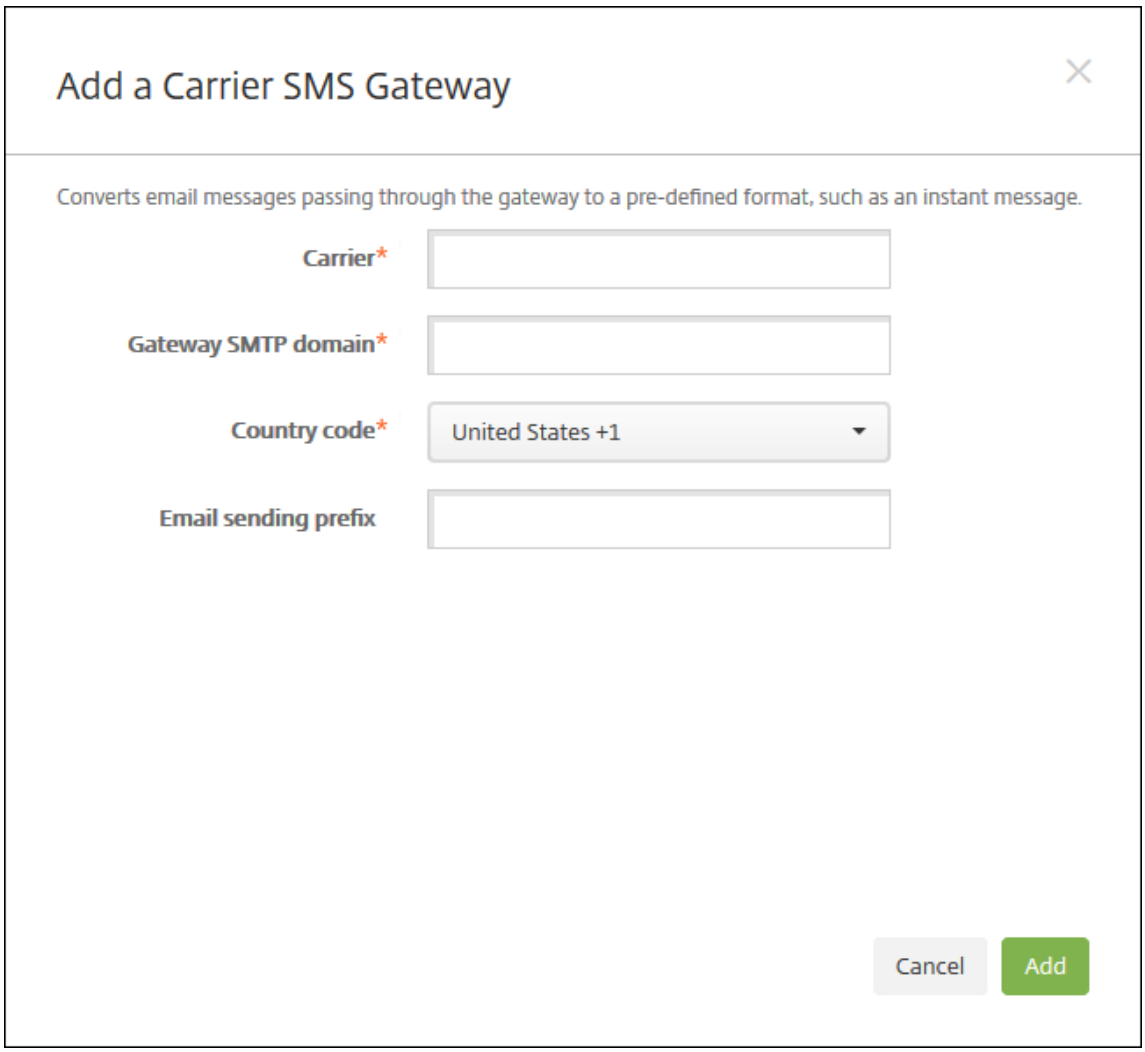
You can set up a Carrier SMS Gateway in XenMobile to configure notifications that are sent through a carrier's SMS gateway. Carriers use Short Message Service (SMS) gateways to send or receive SMS transmissions to or from a telecommunications network. These text-based messages use standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages.

1. In the XenMobile 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.



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.



> **Note:**
>
> XenMobile 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

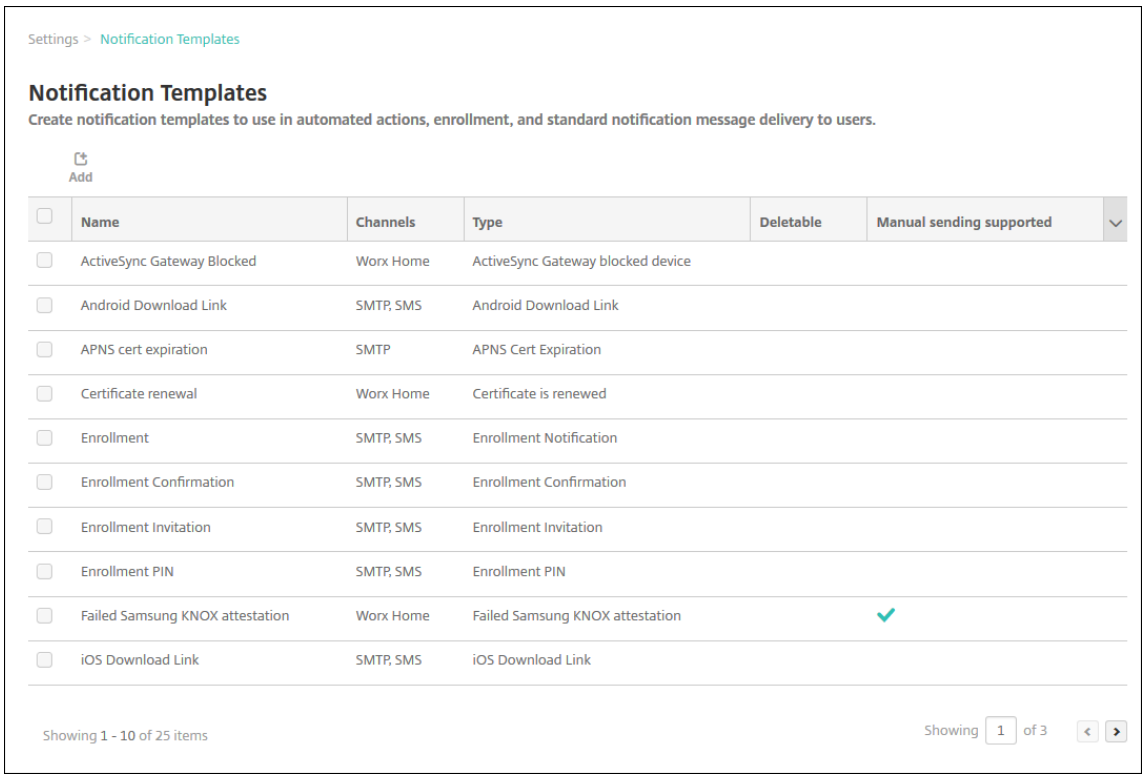
You can create or update notification templates in XenMobile to be used in automated actions, enrollment, and standard notification messages sent to users. You configure the notification templates to

send messages over three different channels: Secure Hub, SMTP, or SMS.

XenMobile includes many predefined notification templates that reflect the distinct types of events that XenMobile 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. XenMobile prompts you to set up the channels when you add notification templates if they are not already set up.

1. In the XenMobile 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.



Add a notification template

1. Click **Add**. If no SMS gateway or SMTP server has been set up, a message appears regarding the use of SMS and SMTP notifications. 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 will not be able to activate those channels when you add or edit a notification template, which means those channels will not be 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. This means you cannot add a new template of this type.

   > **Note:**
   >
   > For some template types, the phrase Manual sending supported appears below the type. This means that the template is available in the **Notifications** list on the **Dashboard** and on the **Devices** page to let you 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)}

     > **Note:**
     >
     > The XenMobile Server console includes the terms “blacklist” and “whitelist”. We are changing those terms in an upcoming release to “block list” and “allow list”.

   - ${outofcompliance.reason(smg_block)}

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’s notification tray.
   - If you choose **SMTP**, most users should receive the message because they will have enrolled with their email addresses.
   - 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 also add recipients (for example, the corporate administrator), in addition to the user by adding their addresses separated by a semi-colon (;). To send Ad Hoc notifications, you can enter specific recipients on this page, 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. For information about using macros in a message, see Macros.

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 where you can make changes to all but the **Type** field, as well as 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.

Devices

January 22, 2021

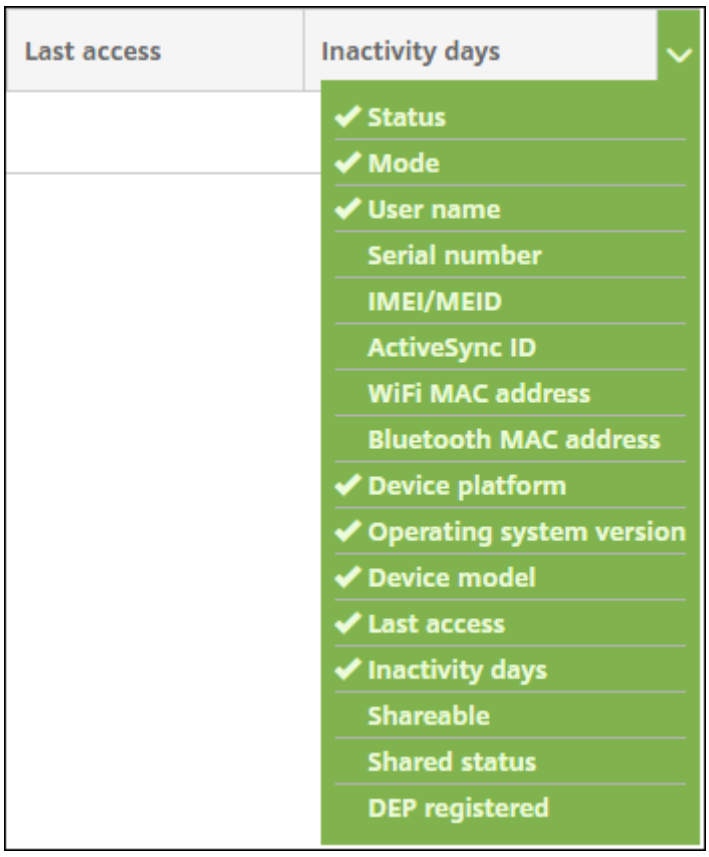
Citrix XenMobile can provision, manage, secure, and inventory a broad range of device types within a single management console.

The XenMobile server database stores a list of mobile devices. A unique serial number or International Mobile Station Equipment Identity (IMEI)/Mobile Equipment Identifier (MEID) uniquely defines each mobile device. To populate the XenMobile 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 **Devices** page in the XenMobile console lists each device and the following information:

- **Status:** Icons indicate whether the device is jailbroken, is managed, whether Active Sync Gateway is available, and the deployment state.
- **Mode:** Whether the device mode is MDM, MAM, or both.
- Other information about the device, such as **User name**, **Device platform**, **Operating system version**, **Device model**, **Last access**, and **Inactivity days**. Those headings are the defaults shown.

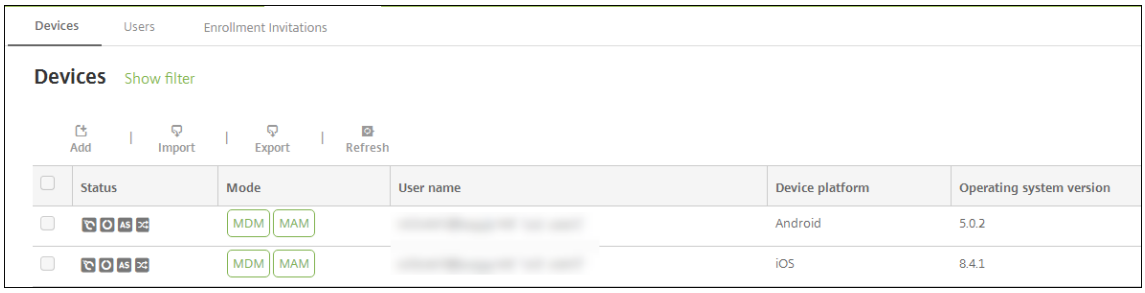
To customize the **Devices** table, click the down arrow on the last heading. Then, select the additional headings you want to see in the table or clear any headings to remove.



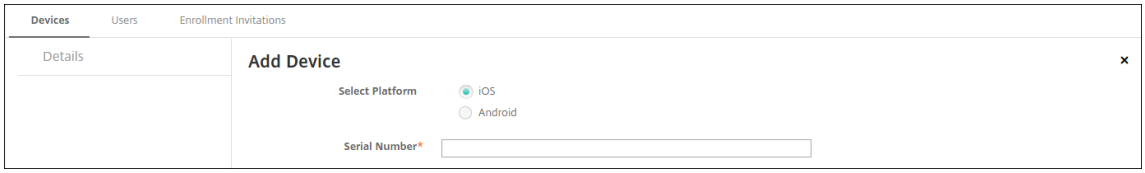
You can add devices manually, import devices from a device provisioning file, edit device details, perform security actions, and send notifications to devices. You can also export all device table data to a .csv file to create a custom report. The server exports all device attributes. If you apply filters, XenMobile uses the filters when creating the .csv file.

Add a device manually

1. In the XenMobile console, click **Manage > Devices**. The **Devices** page appears.



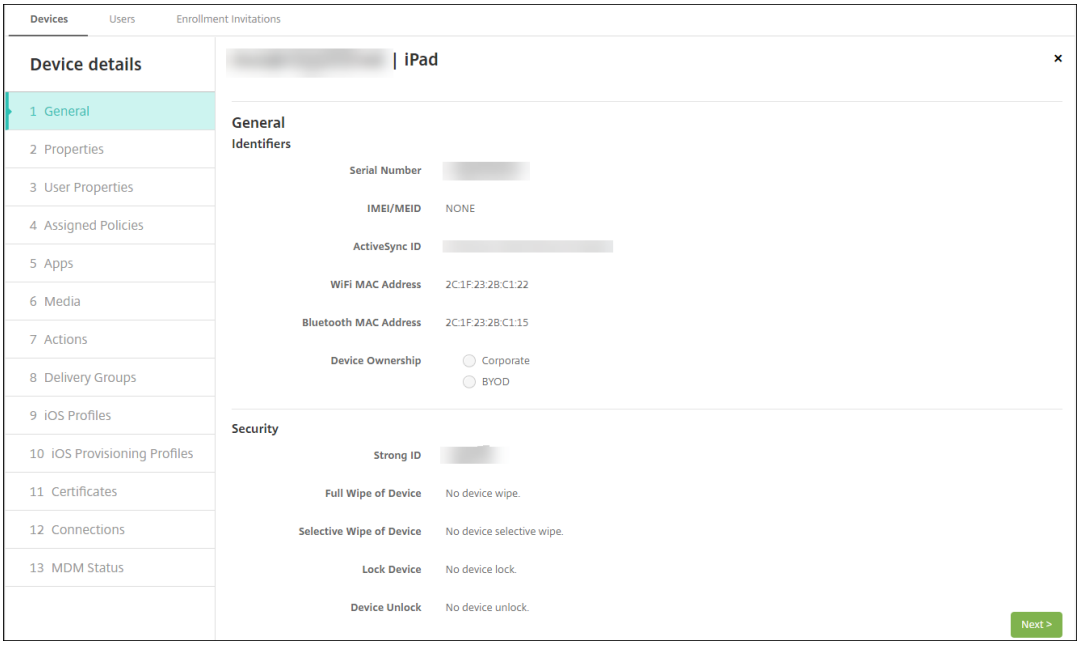
2. Click **Add**. The **Add Device** page appears.



3. Configure these settings:
   - **Select platform:** Click either **iOS** or **Android**.
   - **Serial Number:** Type the device serial number.
   - **IMEI/MEID:** Optionally, for Android devices only, type the device IMEI/MEID information.
4. Click **Add**. The **Devices** table appears with the device added to the bottom of the list. Choose the device you added and then in the menu that appears, click **Edit** to view and confirm the device details.

> **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.

- XenMobile Server configured in Enterprise (XME) or MDM mode
- 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, ActiveSync ID, 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 XenMobile 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. XenMobile deletes the item immediately.

7. The remaining **Device Details** sections contain summary information for the device.

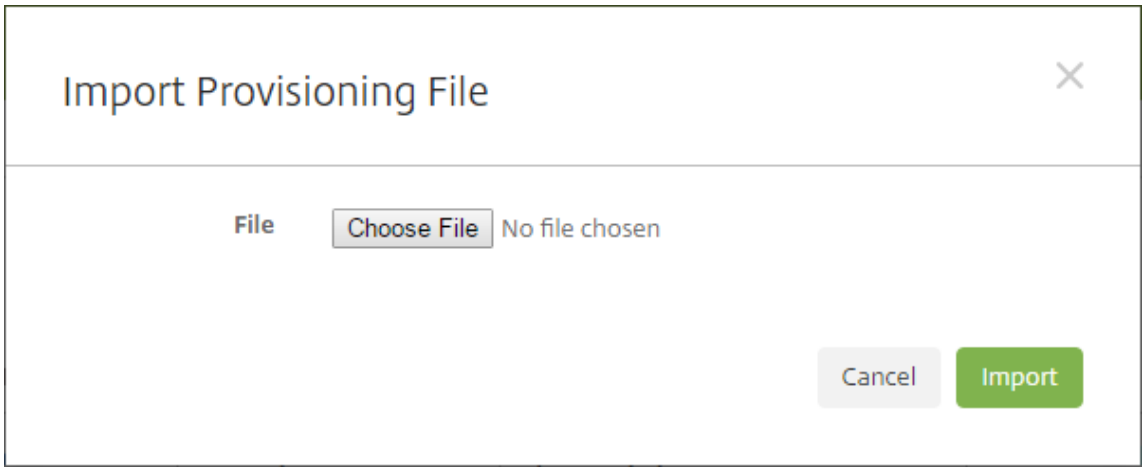
   - **User Properties:** Displays RBAC roles, group memberships, volume purchase accounts, and properties for the user. You can retire a volume purchase account from this page.
   - **Assigned Policies:** Displays the number of assigned policies including the number of deployed, pending, and failed policies. Provides the policy name, type and last deployed information for each policy.
   - **Apps:** Displays, for the last inventory, the number of installed, pending, and failed app deployments. Provides the app name, identifier, type, and other information.

- **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 whether it is managed.
- **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.

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.



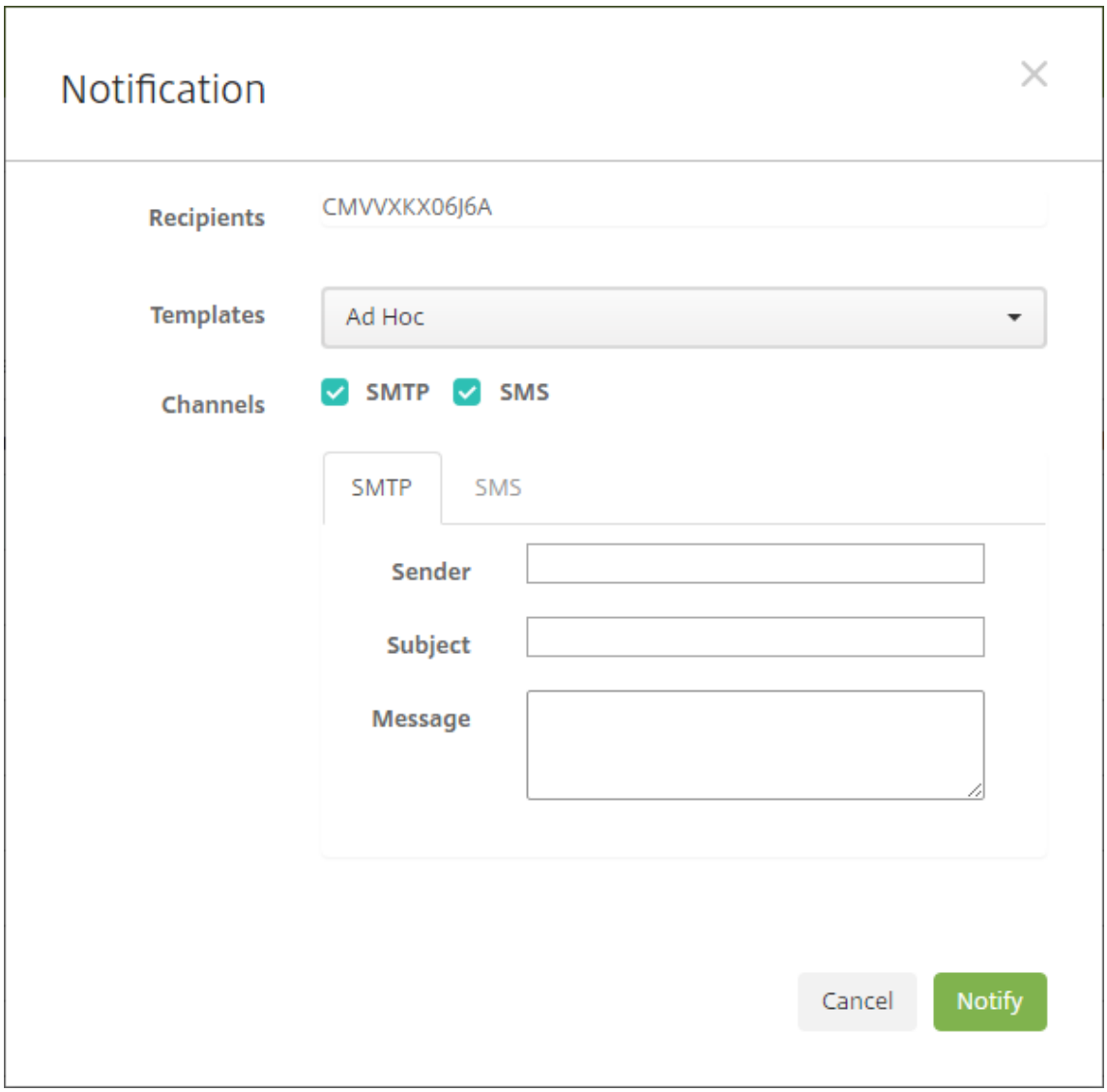
2. Click **Choose File** and then navigate to the file you want to import.
3. Click **Import**. The **Devices** table lists the imported file.

4. To edit the device information, select it and then click **Edit**. For information about the **Device details** pages, see Add a device manually.

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.



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. XenMobile extracts the information in the filtered **Devices** table and converts it to a .csv file.
3. When prompted, open or save the .csv file.

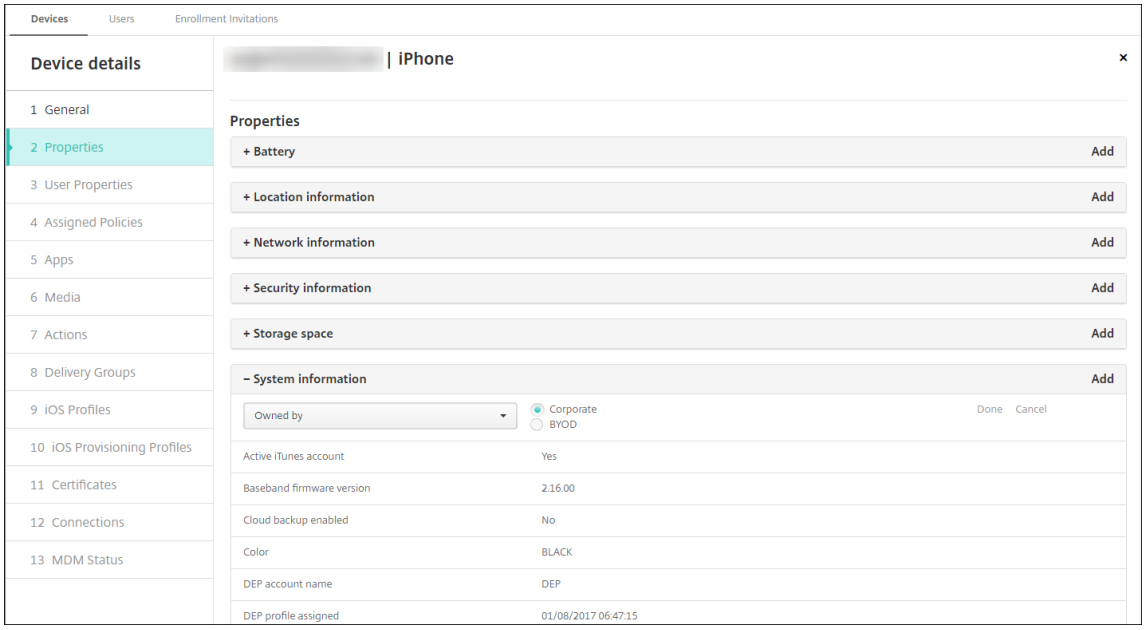
Tag user devices manually

You can manually tag a device in XenMobile 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 XenMobile console.
2. Add the property named **Owned by** and choose either **Corporate** or **BYOD** (employee-owned).



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. XenMobile supports an import file format that is common to all three supported device types: Android, iOS, and Windows.

A provisioning file that you create manually and use to import devices to XenMobile 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:

```
`1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;
   propertyV$*&&éééétest
3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;
4050BF3F5173010816100655105903 93;;iOS;test;
;55244201625379903;ANDROID;test.testé;value;`
```

Each line in the file describes a device. The first entry in the above sample means the following:

- SerialNumber: 1050BF3F5173010816100655105903 91
- IMEI: 15244201625379901
- OperatingSystemFamily: WINDOWS
- PropertyName: propertyN
- PropertyValue: propertyV\;test\;1\;2;prop 2

ActiveSync Gateway

August 27, 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 XenMobile. Based on these rules, you can allow or deny devices access to ActiveSync data. For example, if you activate the rule Missing Required Apps, XenMobile checks the App Access Policy for required apps and denies access to ActiveSync data if the required apps are missing. 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.

XenMobile supports the following rules:

Anonymous Devices: Checks if a device is in anonymous mode. This check is available if XenMobile can't re-authenticate 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 and 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, XenMobile 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 XenMobile 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. That property is usually changed by the automated actions or by a 3rd party leveraging XenMobile APIs.

Revoked Status: Checks whether the device certificate was revoked. A revoked device cannot re-enroll until it is authorized again.

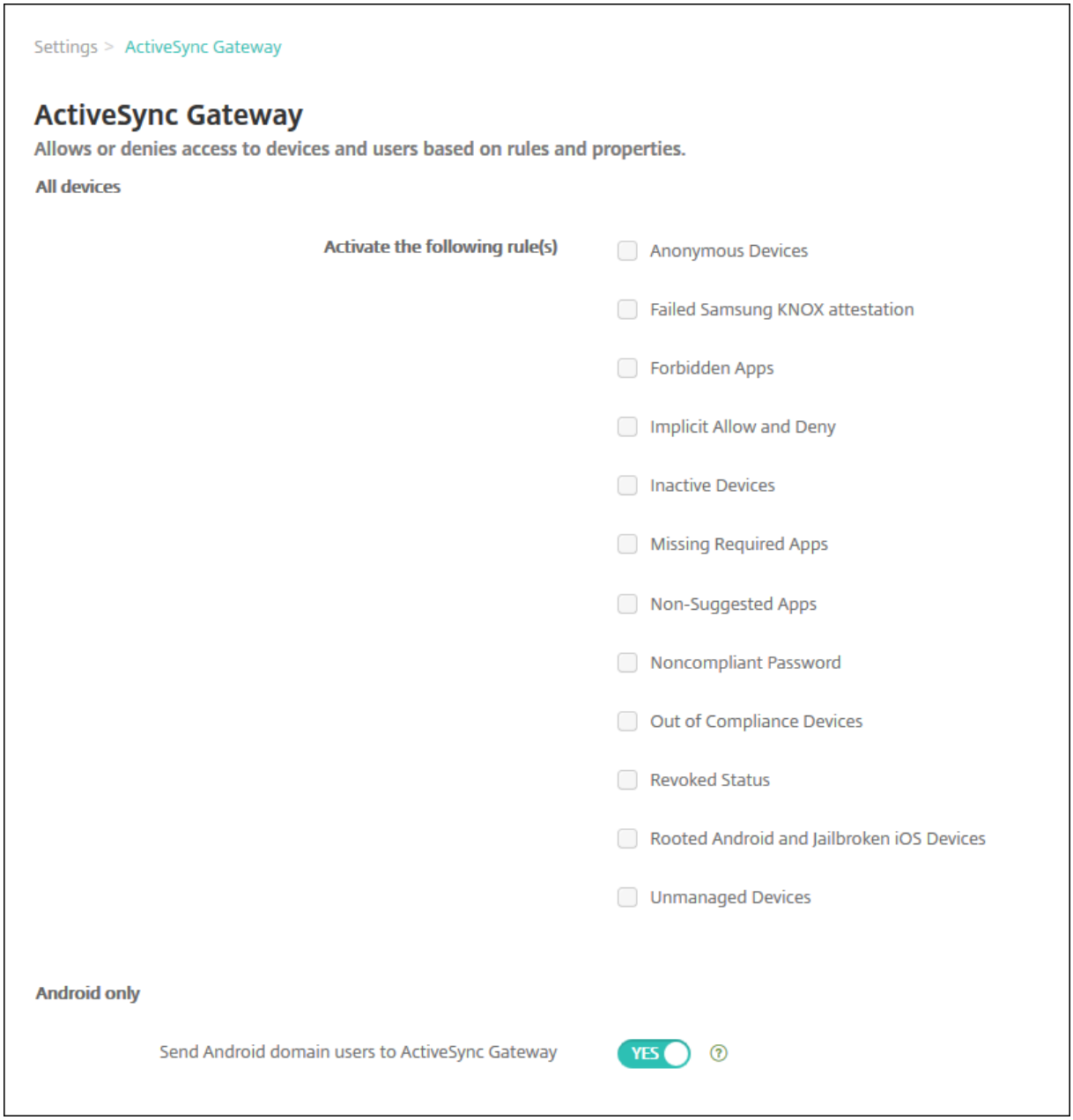
Rooted Android and Jailbroken iOS Devices: Checks whether an Android or iOS device is jailbroken.

Unmanaged Devices: Check whether a device is still in a managed state, under XenMobile control. For example, a device enrolled in MAM or an un-enrolled device is not managed.

Send Android domain users to ActiveSync Gateway: Click **YES** to ensure that XenMobile sends Android device information to the ActiveSync Gateway.

To configure the ActiveSync Gateway settings

1. In the XenMobile 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.



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 XenMobile sends Android device information to the ActiveSync Gateway.
3. Click **Save**.

Migrate from device administration to Android Enterprise

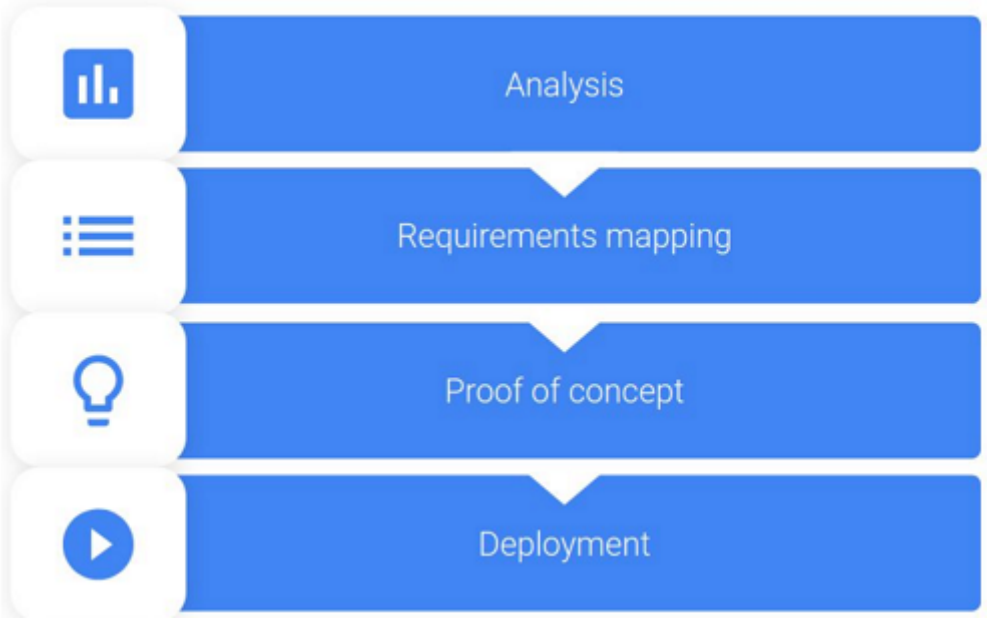
November 14, 2019

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.

XenMobile 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.

That publication also describes the four phases of device administration migration and includes the following diagram. This article includes recommendations specific to XenMobile for the migration phases.



> Diagram from the Android Enterprise Migration Bluebook.
> Republished with the permission of Google.

Impact of device administration deprecation

Google will deprecate the following Device Administration APIs. These APIs won't work on devices running Android Q after you upgrade Secure Hub to target the Android Q API level:

- Disable camera: Controls access to device cameras.

- Expire password: Forces users to change their password after a configurable time period.
- Limit password: Sets restrictive password requirements.

The deprecated APIs have no impact on devices enrolled in Citrix MAM-only mode.

Recommendations

The following recommendations are for devices already enrolled in the Android legacy device administration mode, unenrolled devices, and devices enrolled in Citrix MAM-only mode.

Device enrollment status	Recommended action
Existing device is enrolled in device administration mode and upgradeable to Android Q.	Before upgrading the device to Android Q, migrate from device administration mode to Android Enterprise.
Existing device is enrolled in device administration mode. The device can't upgrade to Android Q.	Device can remain in device administration mode. However, plan to move the device to Android Enterprise on device refresh.
Existing device is enrolled in device administration mode and is upgraded to Android Q.	Migrate from device administration mode to Android Enterprise before Google deprecates the APIs. A warning message for these devices appears in the XenMobile console.
New device delivered with Android Q and enrolled in device administration mode.	Migrate from device administration mode to Android Enterprise before Google deprecates the APIs. A warning message for these devices appears in the XenMobile console.
New device delivered with or upgradeable to Android Q. The device isn't enrolled.	Use Android Enterprise for any new devices.
New or existing device on Android Q gets enrolled in device administration mode after Google deprecates the APIs.	To avoid the impacts of deprecated Google APIs, Citrix recommends migrating to Android Enterprise before Google deprecates the APIs. After that date, enrollments of these devices will fail.
New or existing devices enrolled in Citrix MAM-only mode	No action needed. The deprecated Google APIs have no impact on devices in MAM-only mode.

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 XenMobile: 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 XenMobile 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 G-Suite 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 XenMobile.
  - Option 2: Publish the app from XenMobile as an enterprise app. Publish the APK in XenMobile and select the platform **Android Enterprise** for the MDX file.

Citrix device policy migration

For policies that are available for both the Android and Android Enterprise platforms: Edit the policy and select the platform **Android Enterprise**.

For Android Enterprise, consider the enrollment mode. Some policy options are available only for devices in work profile mode or fully managed mode.

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 XenMobile.
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

June 25, 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 XenMobile to manage company-owned Android devices 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 Android Enterprise terminology in the Google Android Enterprise developers guide. Google updates these terms frequently.
- For Android operating systems supported for XenMobile, see Supported device operating systems.

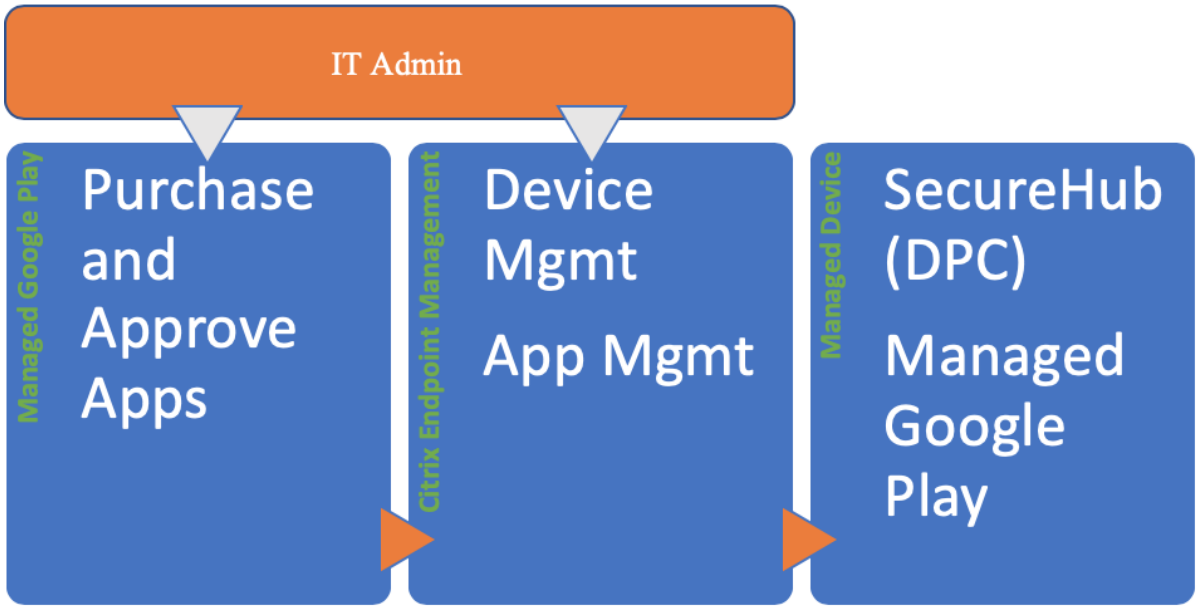
- For information about the outbound connections to consider when setting up network environments for Android Enterprise, see the Google support article, Android Enterprise Network Requirements.

When you integrate XenMobile 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 XenMobile with Android Enterprise, the complete solution has these components:

- **XenMobile:** The Citrix EMM. XenMobile is the unified XenMobile solution for a secure digital workspace. XenMobile 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 XenMobile. Secure Hub enforces policies on the device.
- **Managed Google Play:** A Google enterprise app platform that integrates with XenMobile. The Google Play EMM API sets app policies and distributes app.

This illustration shows how administrators interact with these components and how the components interact with each other:



Using managed Google Play with XenMobile

> **Note:**
>
> You can use either managed Google Play or Google Workspace 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 (formerly G-Suite) customers.

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 to manage separate sets of devices and apps.

For XenMobile 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 modes of operation

Device deployment scenario 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. 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 will migrate devices managed as “fully managed with a work profile” to a new security-enhanced work profile experience. For more information, see Changes ahead for Android Enterprise’s Fully Managed with 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	Yes. The DPC can perform device-wide actions, such as configure device-wide connectivity, configure global settings, and perform a factory reset.	For new or factory reset devices only.
Fully managed with a work profile	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.	Formerly known as corporate-owned personally enabled (COPE) devices.
Dedicated devices*	Company-owned devices configured for a single use case, such as digital signage or ticket printing	No	Yes. You provide only the required apps and prevent users from adding other apps.	Formerly known as corporate owned single use (COSU) devices.

Device management	Use cases	Work profile	Personal profile	Notes
BYOD work profile**	Personal devices enrolled in work profile mode (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.

* 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.

** XenMobile does not support Zebra devices as in BYOD work profile mode. XenMobile supports Zebra devices as fully managed devices and in device legacy mode (also called device admin mode).

For information on migrating from legacy mode to device owner or profile owner mode, see Migrate from device administration to Android Enterprise.

Authentication methods

Enrollment profiles determine whether Android devices enroll in MAM, MDM, or MDM+MAM, with the option for users to opt out of MDM.

The enrollment security modes **User name + PIN**, **Invitation URL**, **Invitation URL + PIN**, and **Invitation URL + Password** aren't available for Android Enterprise. For information about specifying the level of security and required enrollment steps, see To configure enrollment security modes.

XenMobile supports the following authentication methods for Android devices enrolled in MDM+MAM. For information, see the articles under Certificates and authentication.

- Domain
- Domain plus security token
- Client certificate
- Client certificate plus domain
- Identity providers:
  - Azure Active Directory
  - Citrix Identity provider

Another 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:

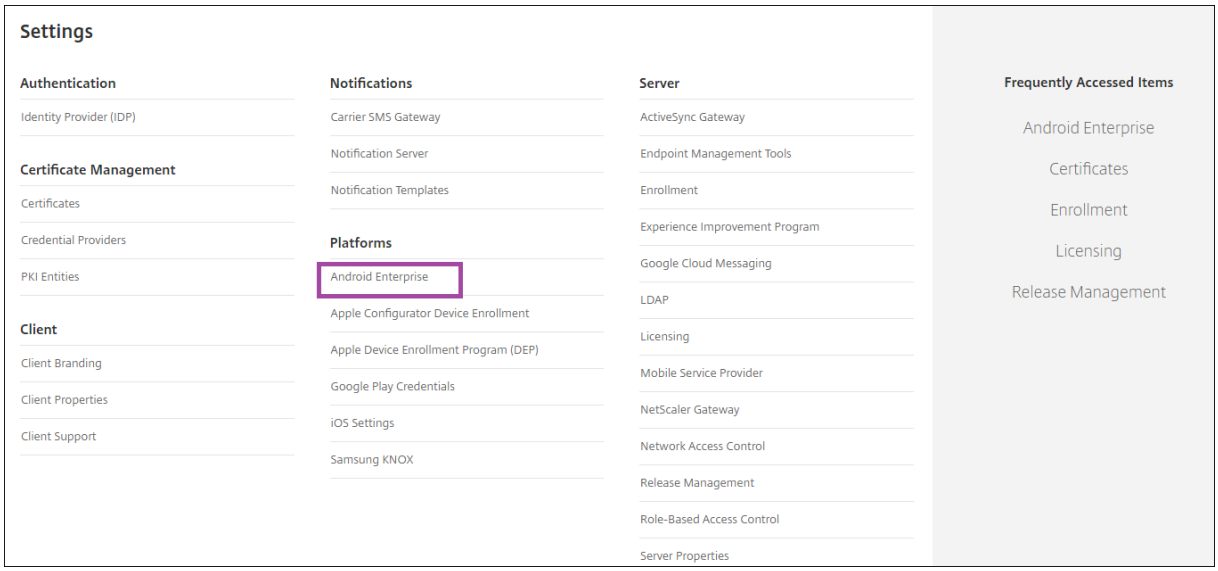
- Accounts and credentials:
  - To set up Android Enterprise with managed Google Play, a corporate Google account
  - To download the latest MDX files, a Citrix customer account
  - To deploy private apps (optional), a Google developer account
- Firebase Cloud Messaging (FCM) configured for XenMobile. See Firebase Cloud Messaging for instructions.
- For Samsung Knox Mobile Enrollment (optional), Knox premium licenses.

Connecting XenMobile to Google Play

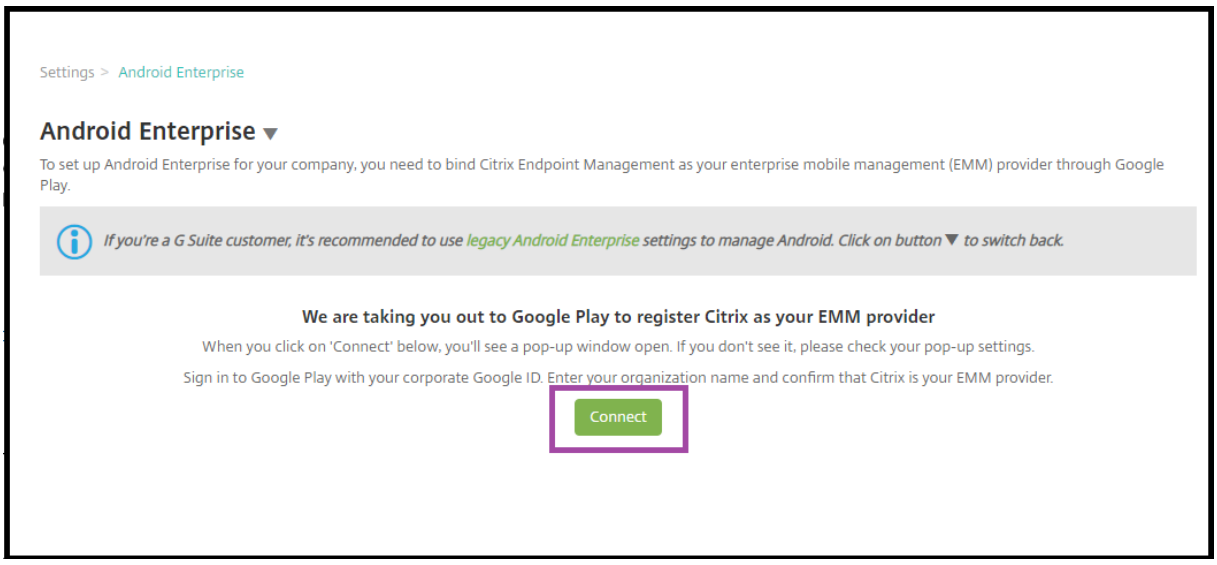
To set up Android Enterprise for your organization, register Citrix as your EMM provider through managed Google Play. That setup connects managed Google Play to XenMobile and creates an enterprise for Android Enterprise in XenMobile.

You need a corporate Google account to sign in to Google Play.

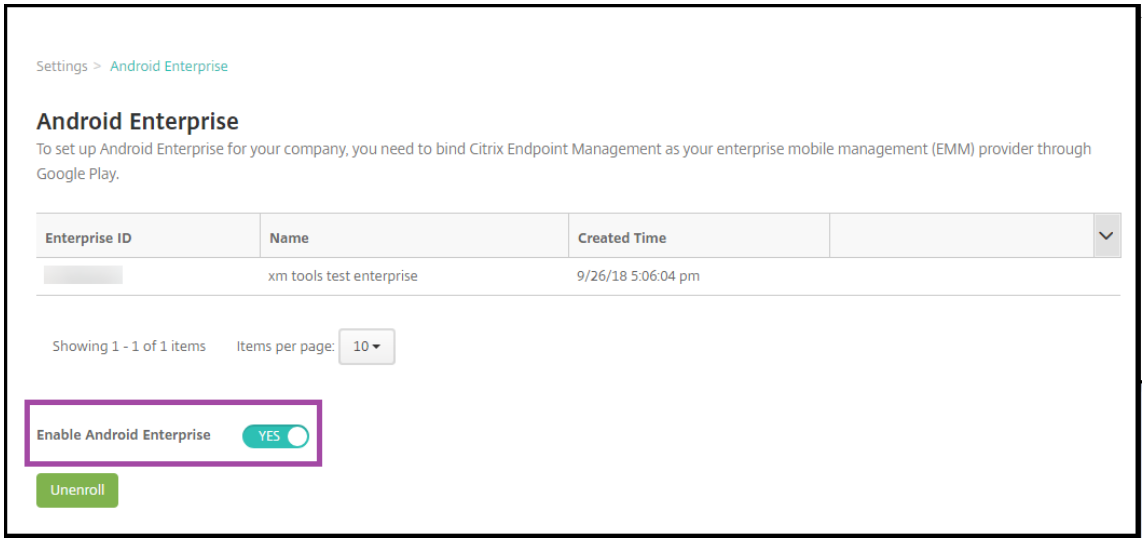
1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Go to **Settings > Android Enterprise**.



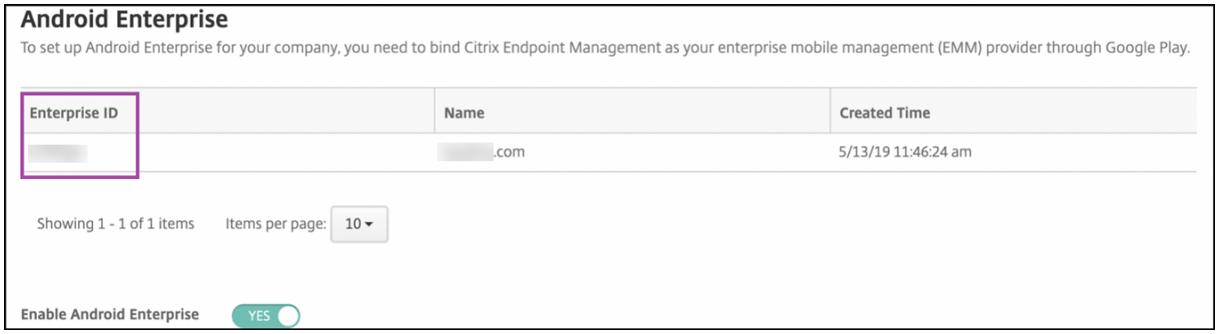
1. Click **Connect**. Google Play opens.



1. Sign in to Google Play with your corporate Google account credentials. Enter your organization name and confirm Citrix is your EMM provider.
2. An enterprise ID is added for Android Enterprise. To enable Android Enterprise, slide **Enable Android Enterprise** to **Yes**.



Your Enterprise ID appears in the XenMobile console.



Your environment is connected to Google and is ready to manage devices. You can now provide apps for users.

XenMobile can be used to 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.

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.

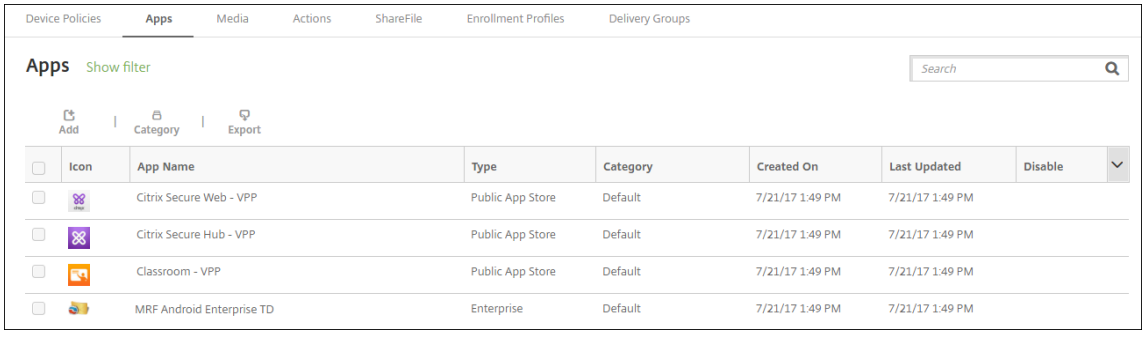
The apps you publish are available to devices enrolled in your Android Enterprise enterprise.

> **Note:**
>
> When you deploy an Android Enterprise public app store app to an Android user, that user is automatically enrolled in Android Enterprise.

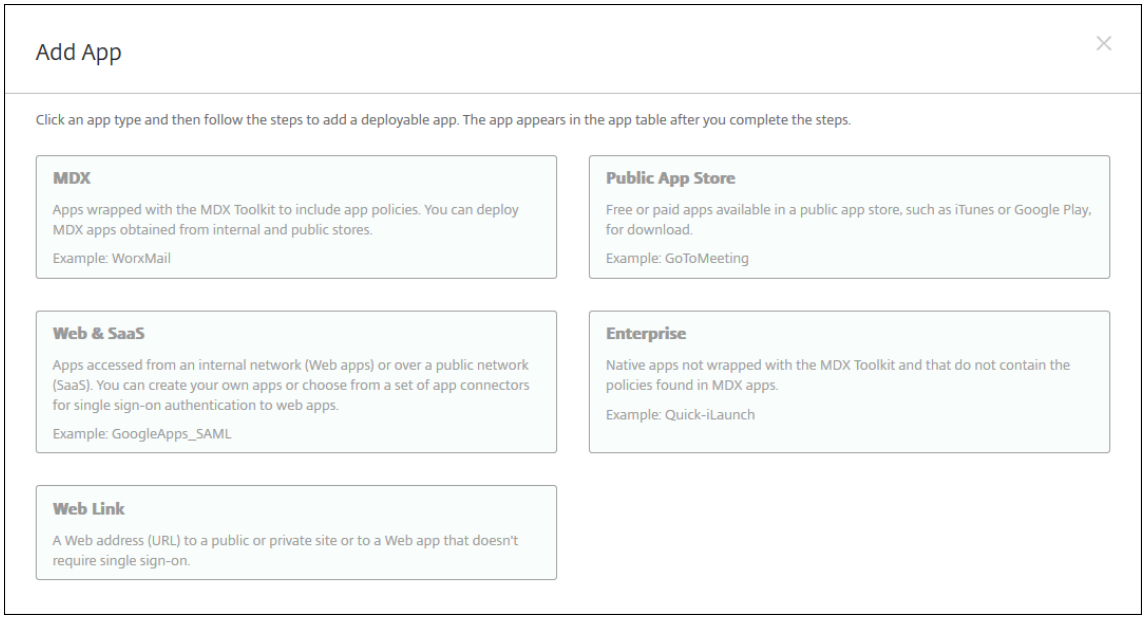
Configure apps as MDX apps

To configure a Citrix productivity app as an MDX app for Android Enterprise:

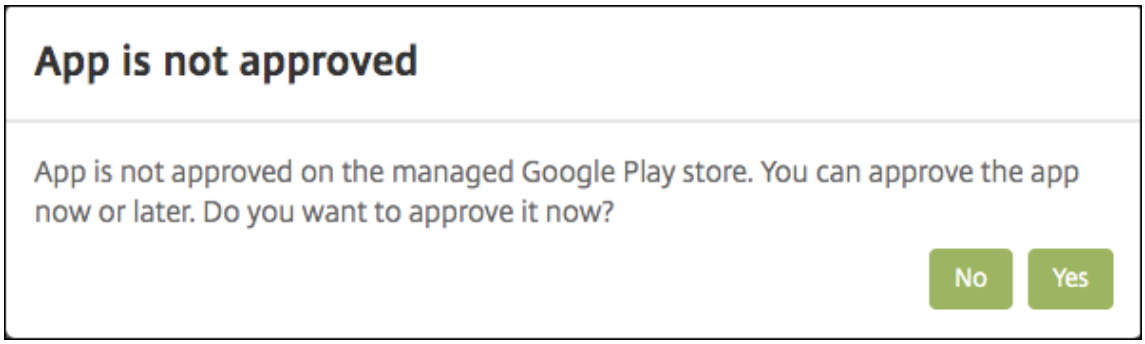
1. In the XenMobile console, click **Configure > Apps**. The **Apps** page appears.



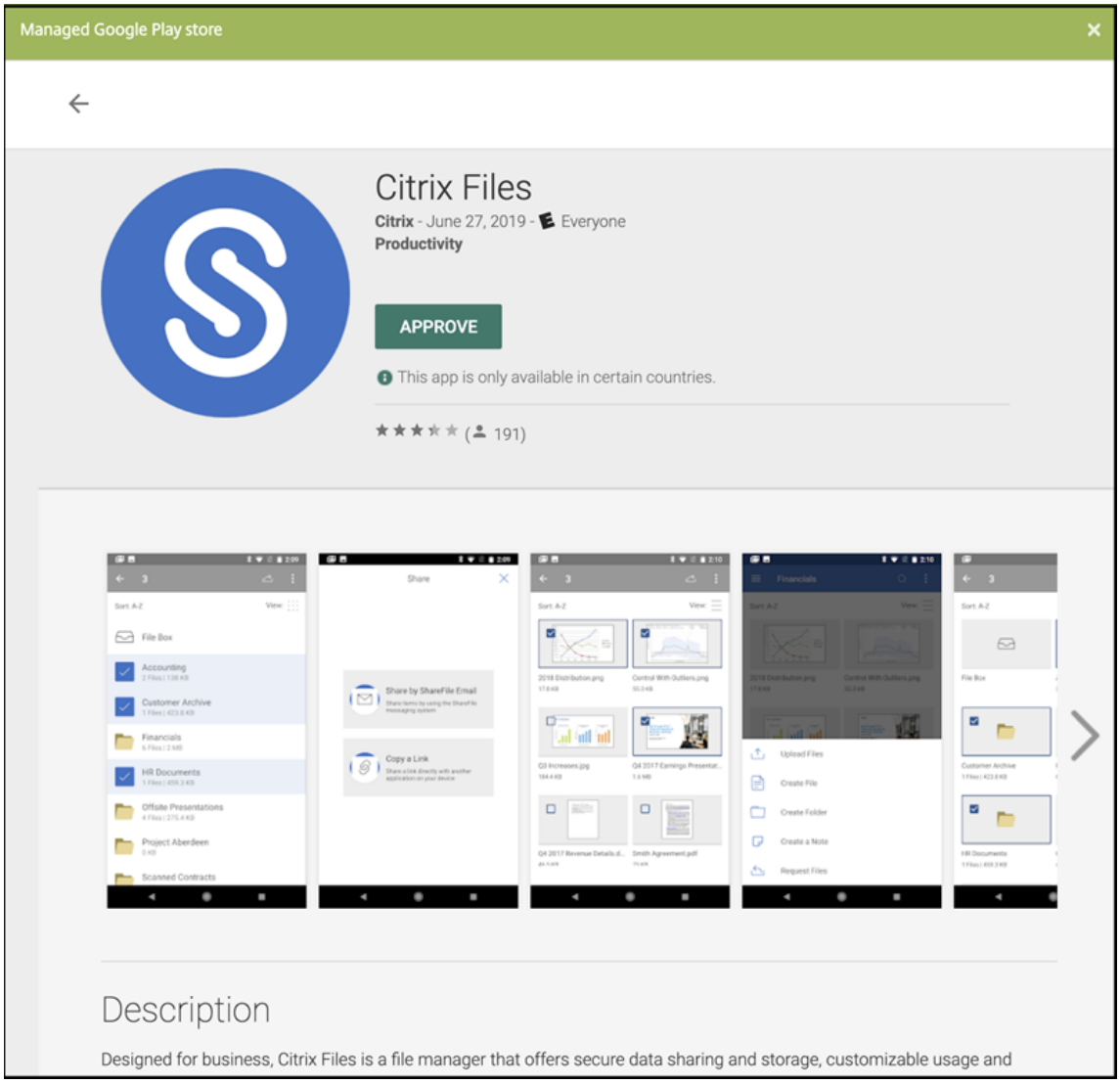
2. Click **Add**. The **Add App** dialog box appears.



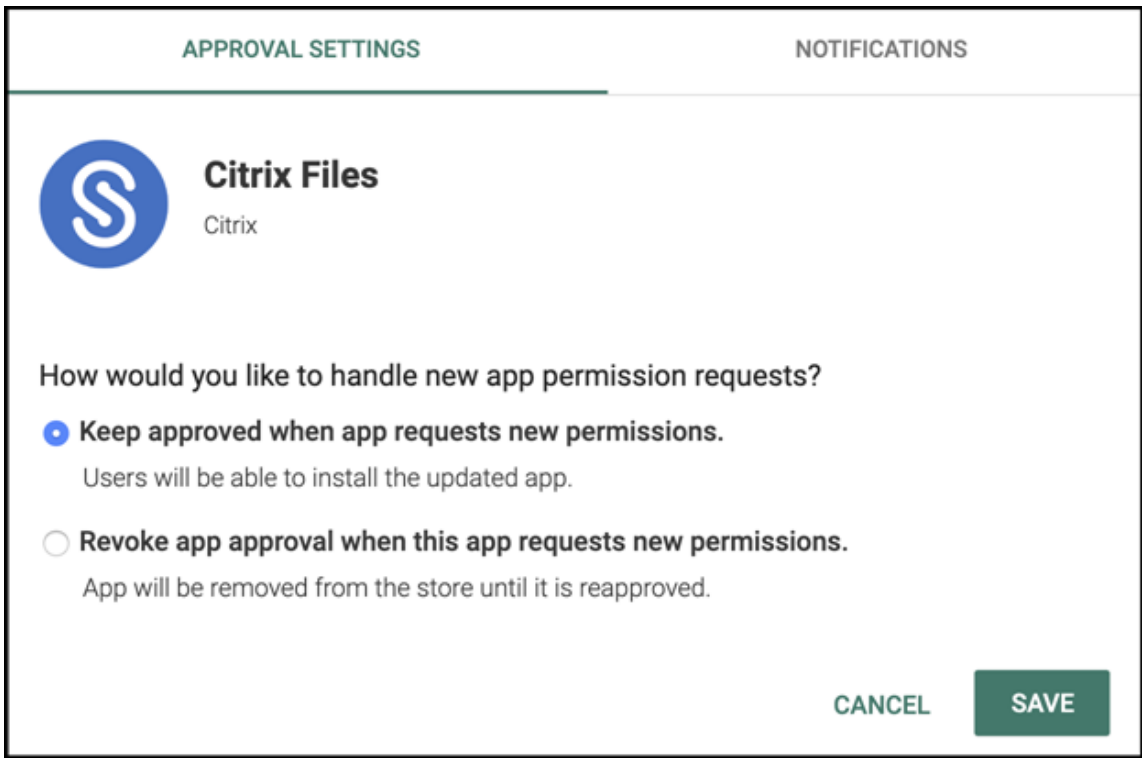
3. Click **MDX**. The **App Information** page appears.
4. On the left side of the page, select **Android Enterprise** as the platform.
5. On the **App Information** page, type the following information:
   - **Name:** Type a descriptive name for the app. This name appears under **App Name** on the **Apps** 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 XenMobile console, click **Yes**.



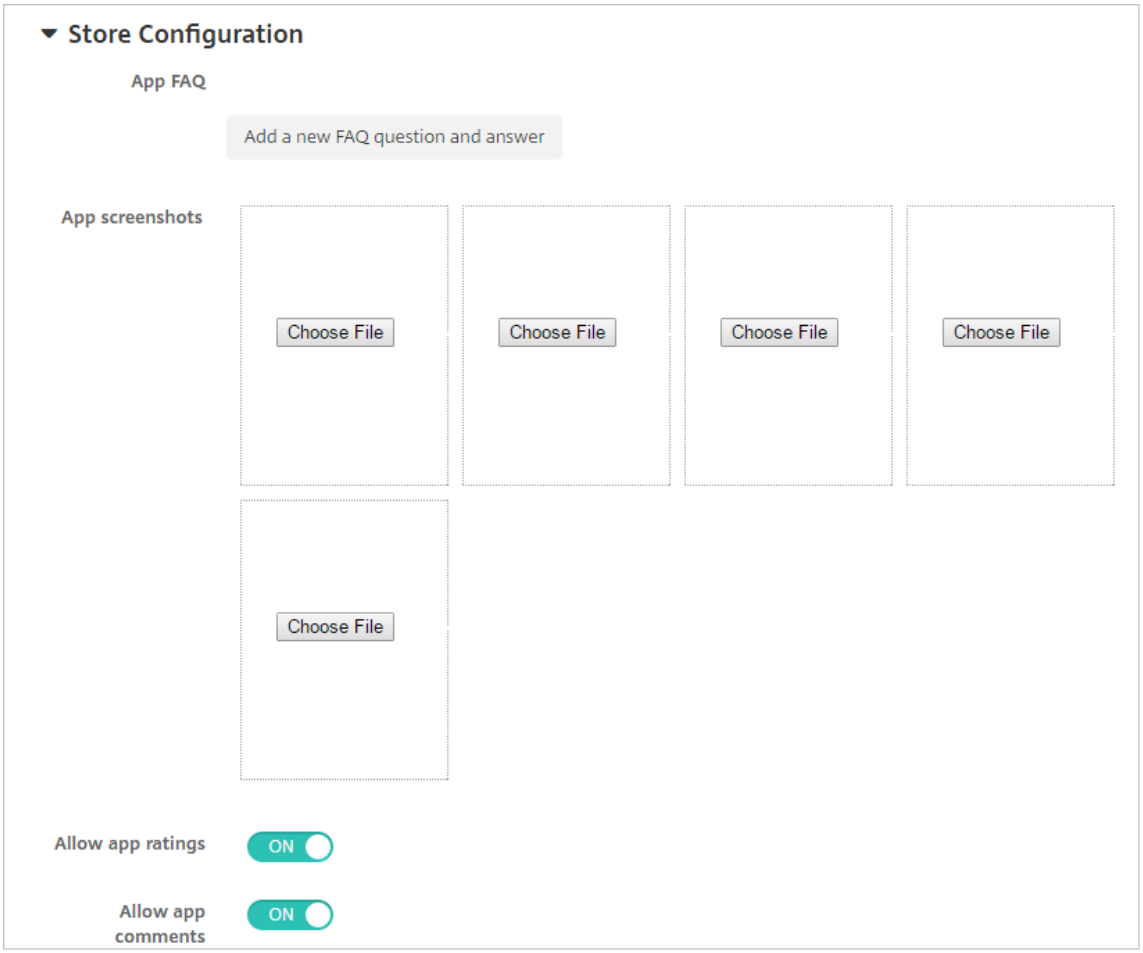
9. When the managed Google Play store page opens, click **Approve**.



10. Click **Approve** again.
11. Select **Keep approved when app requests new permissions**. Click **Save**.



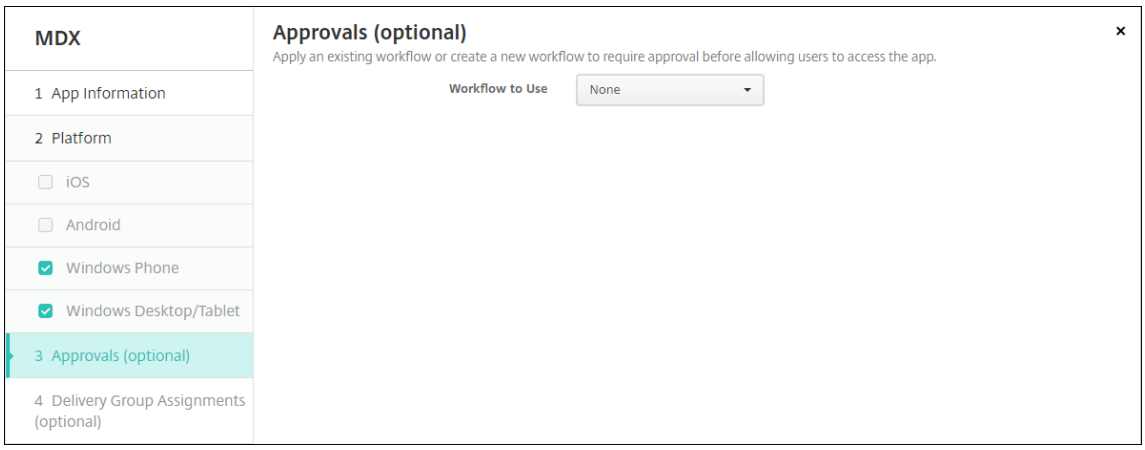
12. When the app is approved and saved, more settings appear on the page. Configure these settings:
    - **File name:** Type the file name associated with the app.
    - **App Description:** Type a description for the app.
    - **Product track:** Specify which product track you want to push to user 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.



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.



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.

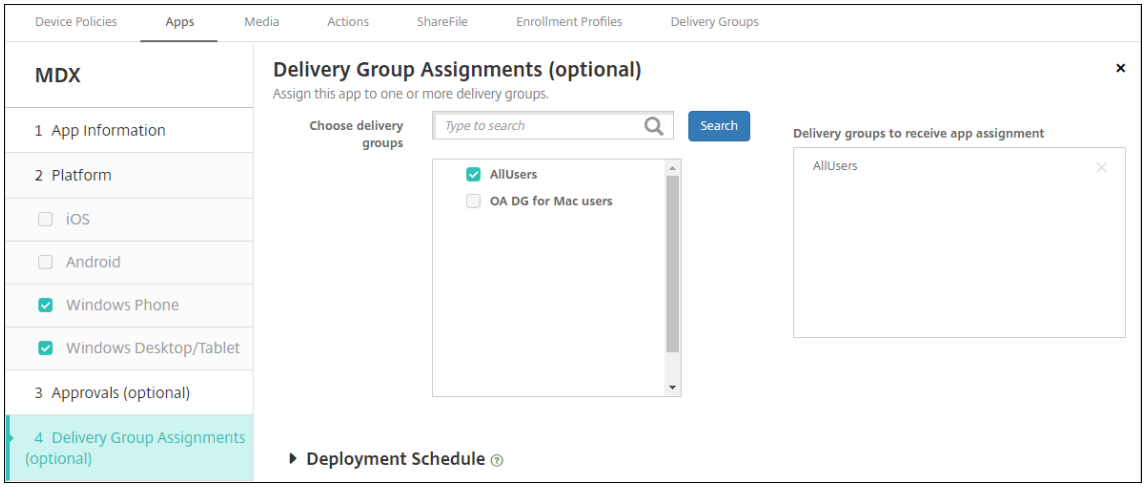
Configure these settings to assign or create a workflow:

- **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 Apply 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 if you began using XenMobile with version 10.18.19 or later. We don't recommend the connections for customers who began using XenMobile 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 to configure an MDX app for each mobile productivity app.

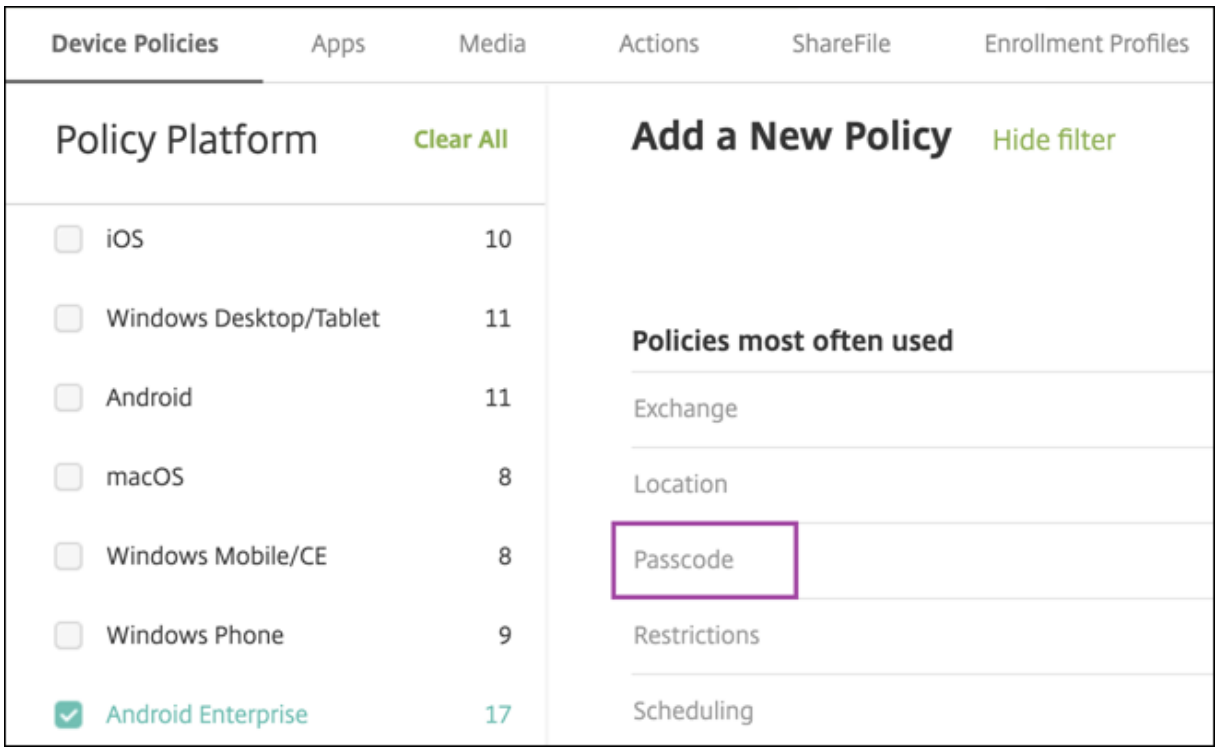
Configure security challenge policy

The XenMobile Passcode device policy configures the set of rules for the security challenges users to 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.

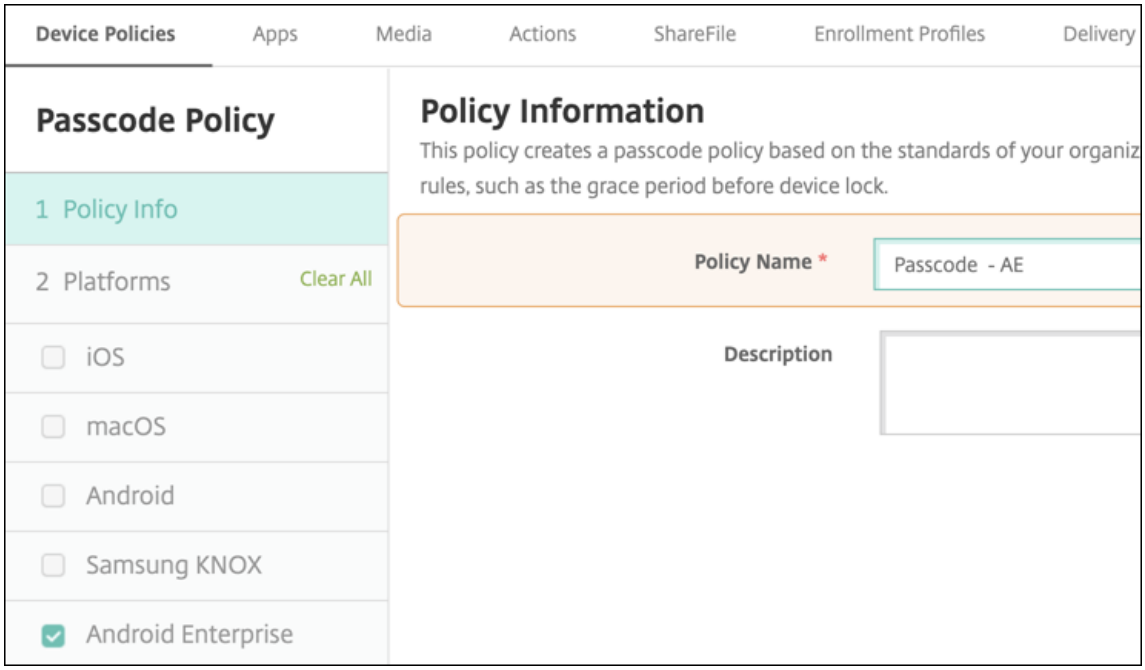
- If your Android Enterprise deployment includes BYOD devices, configure the passcode policy for the work profile.
- If your deployment includes, company-owned, fully managed devices, configure the passcode policy for the device itself.
- If your deployment includes both types of devices, configure both types of passcode policy.

To configure the passcode policy:

1. In the XenMobile 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.



1. Enter a **Policy Name**. Click **Next**.



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 in enabled for your XenMobile 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 (COSU devices)
- Fully managed devices with a work profile (COPE 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 XenMobile deployment, all newly enrolled or re-enrolled 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 devices.

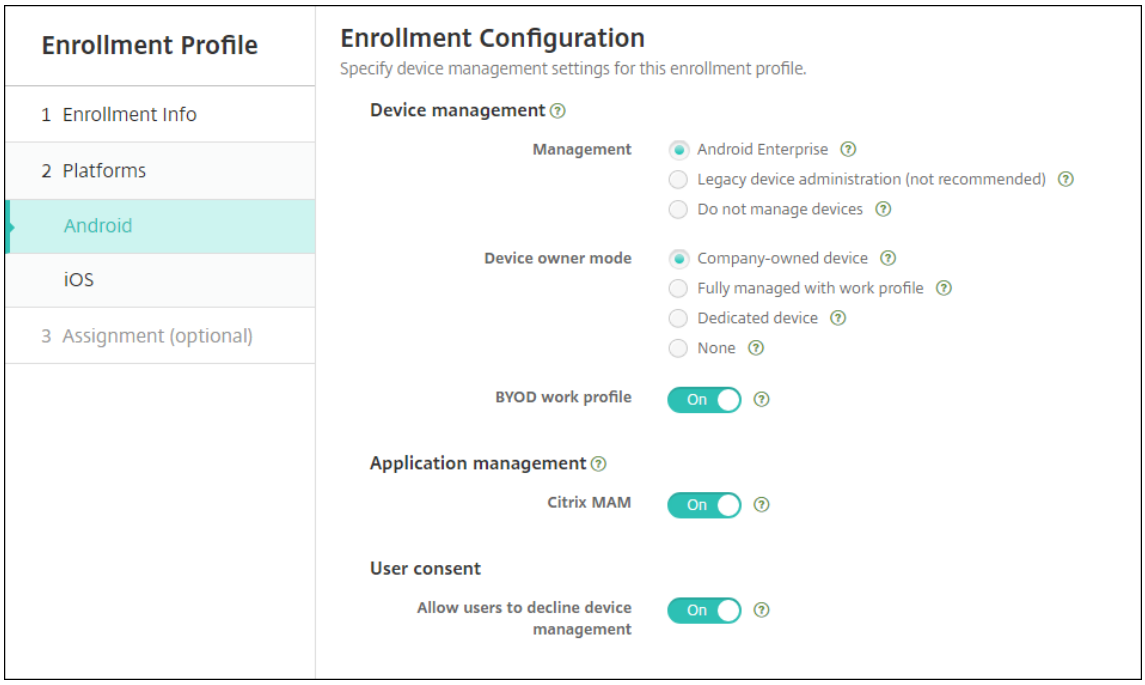
When you create enrollment profiles, you assign delivery groups to them. If a user belongs to multiple delivery groups that have different enrollment profiles, the name of the delivery group determines the enrollment profile used. XenMobile selects the delivery group that appears last in an alphabetized list of delivery groups. For more information, see Enrollment profiles.

You can use enrollment profiles to combine multiple use cases such as MDM only, MDM+MAM, and MAM only. Your XenMobile Server license type, reflected in the server property, `xms.server.mode`, determines the settings available in **Configure > 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.

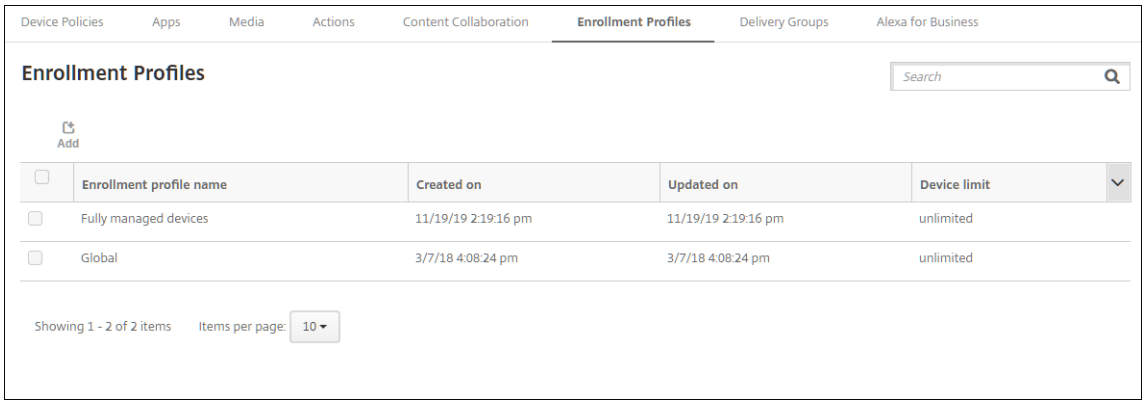
1. In the XenMobile console, go to **Configure > Enrollment Profiles**.
2. To add an enrollment profile, click **Add**. In the Enrollment Info page, type a name for the enrollment profile.
3. Set the number of devices that members with this profile can enroll.
4. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
5. Set **Management** to **Android Enterprise**.
6. Set **Device owner mode** to **Company owned device**.



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. The default is **On**.
   - Set **BYOD work profile** to **Off** to restrict enrollment to fully managed devices.
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.

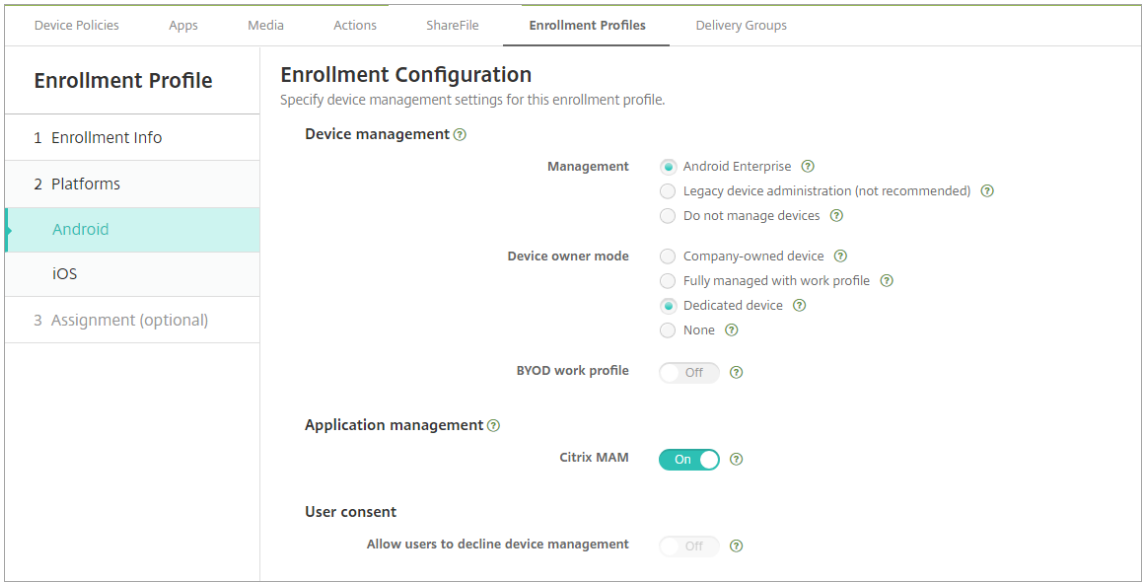


Add a dedicated device enrollment profile

When your XenMobile deployment includes dedicated devices, a single XenMobile 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 XenMobile 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. Ensure that the number of devices that members with this profile can enroll is set to unlimited.

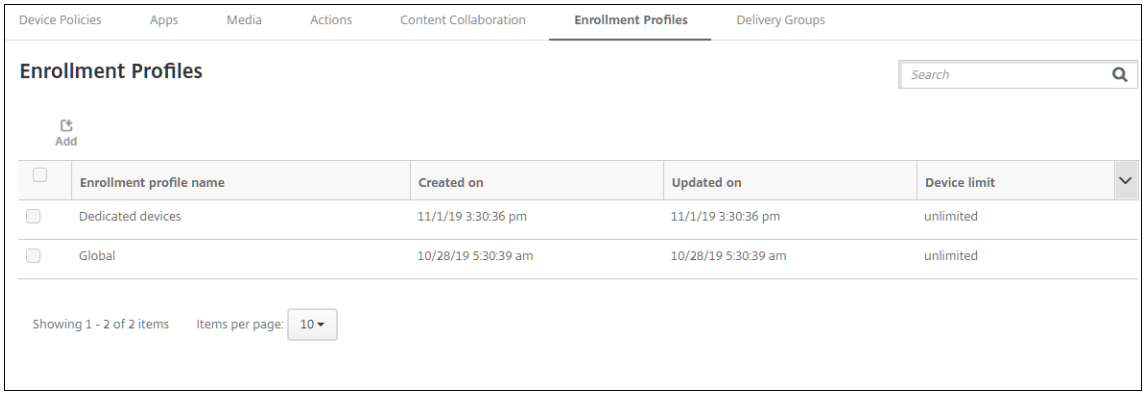
3. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
4. Set **Management** to **Android Enterprise**.
5. Set **Device owner mode** to **Dedicated device**.



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**.

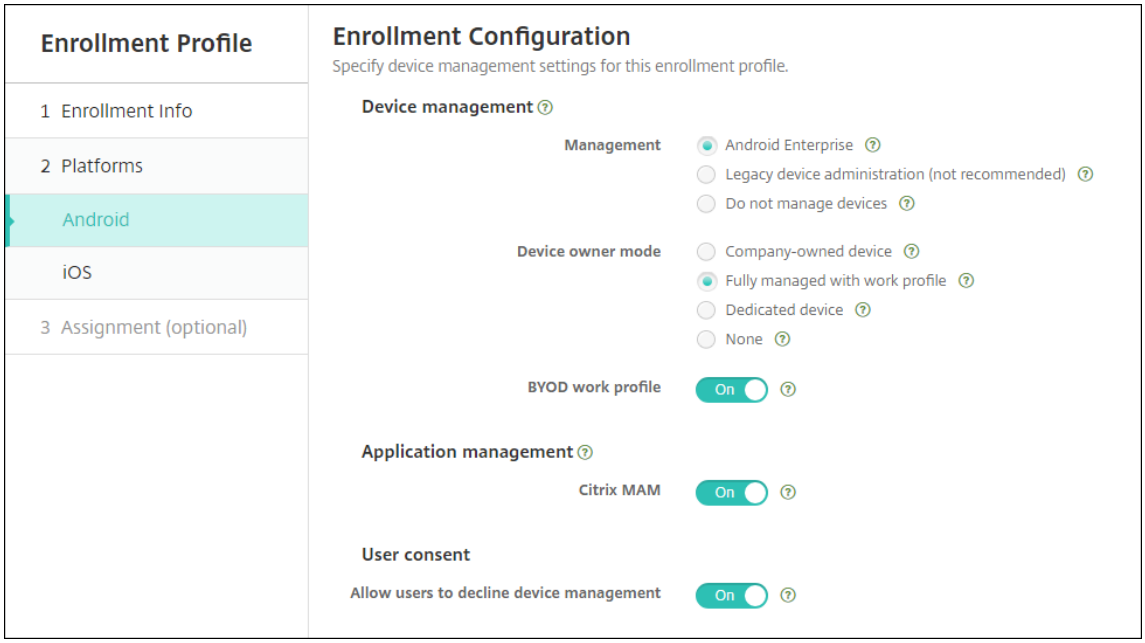
   If **BYOD work profile** is set to **On**, the default value of **Allow users to decline device management** is **On**. If **BYOD work profile** is set to **Off**, then **Allow users to decline device management** is disabled.
9. Select **Assignment (options)**. The Delivery Group Assignment screen appears.
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

1. In the XenMobile 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**.



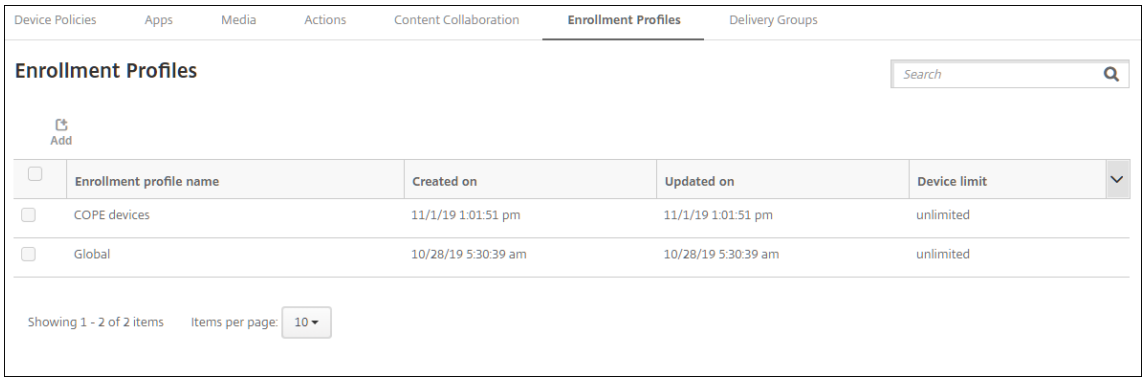
6. **BYOD work profile** allows you to configure the enrollment profile to enroll BYOD devices as work profile devices. New and factory reset devices are enrolled as fully managed devices with a work profile. Set **BYOD work profile** to **On** to allow enrollment of BYOD devices as work profile

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 is deprecating 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:

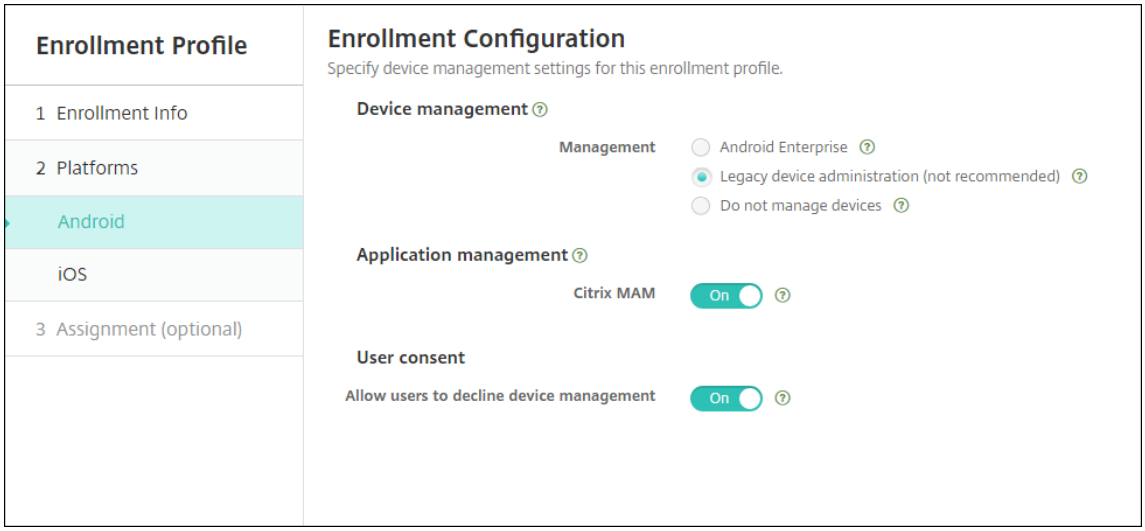
- Citrix makes Android Enterprise the default enrollment option for Android devices.
- If Android Enterprise is enabled for your XenMobile deployment, all newly enrolled or re-enrolled Android devices are enrolled as Android Enterprise devices.

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, XenMobile 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.

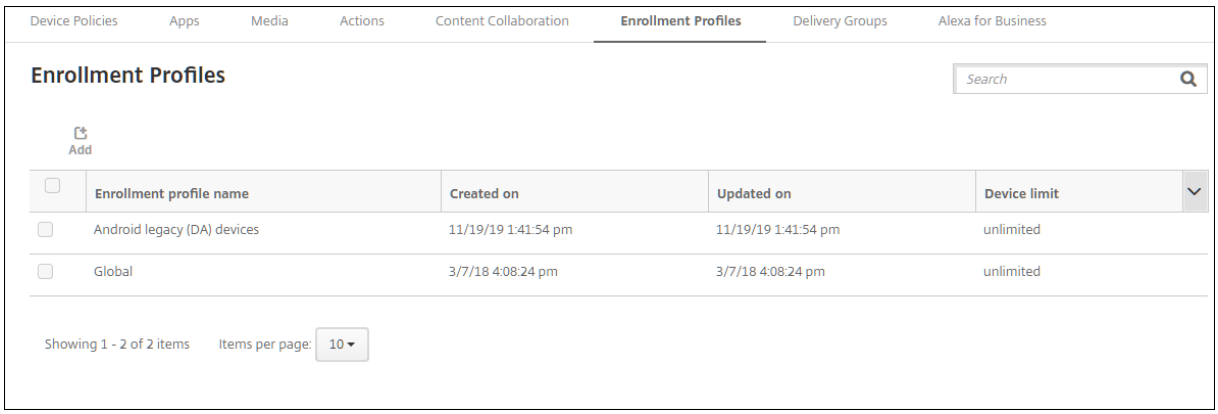
To create an enrollment profile for legacy devices:

1. In the XenMobile 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**.



6. Choose whether to enroll devices in Citrix MAM.
7. To allow users to decline device management when they enroll their devices, set **Allow users to decline device management** to **On**. Default is **On**.
8. Select **Assignment (options)**. The Delivery Group Assignment screen appears.
9. 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 a legacy device 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 XenMobile. 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.

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 XenMobile 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.

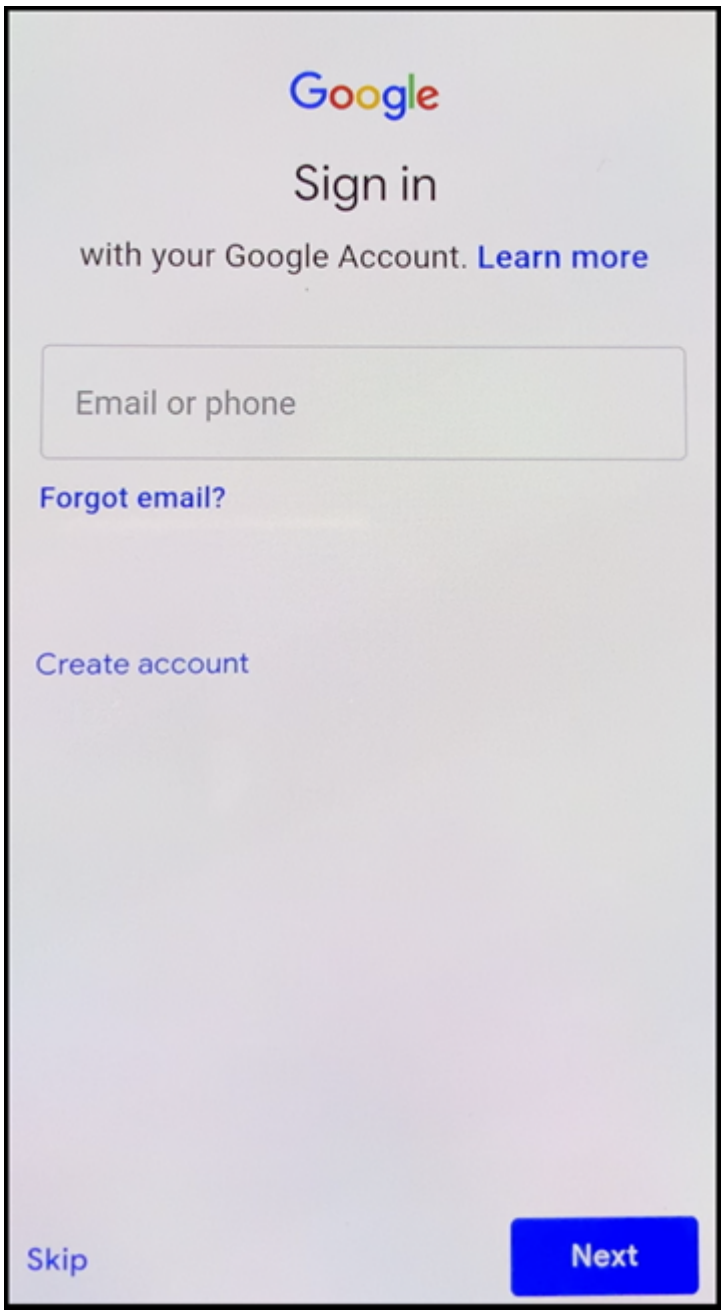
In this enrollment method is recommended for most customers because the latest version of Secure Hub is downloaded from the Google Play store. Unlike with other enrollment methods, you do not provide Secure Hub for download from the XenMobile Server.

System requirements

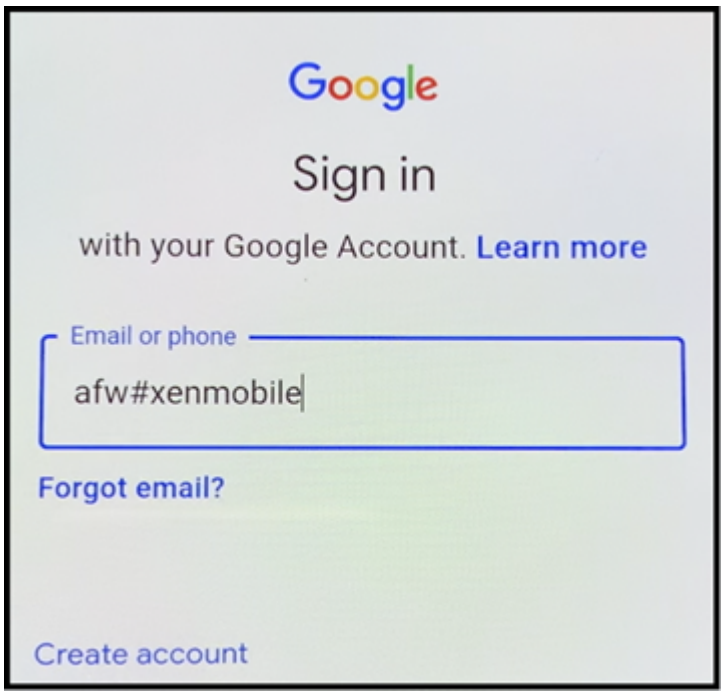
- Supported on all Android devices running the Android OS.

To enroll the device

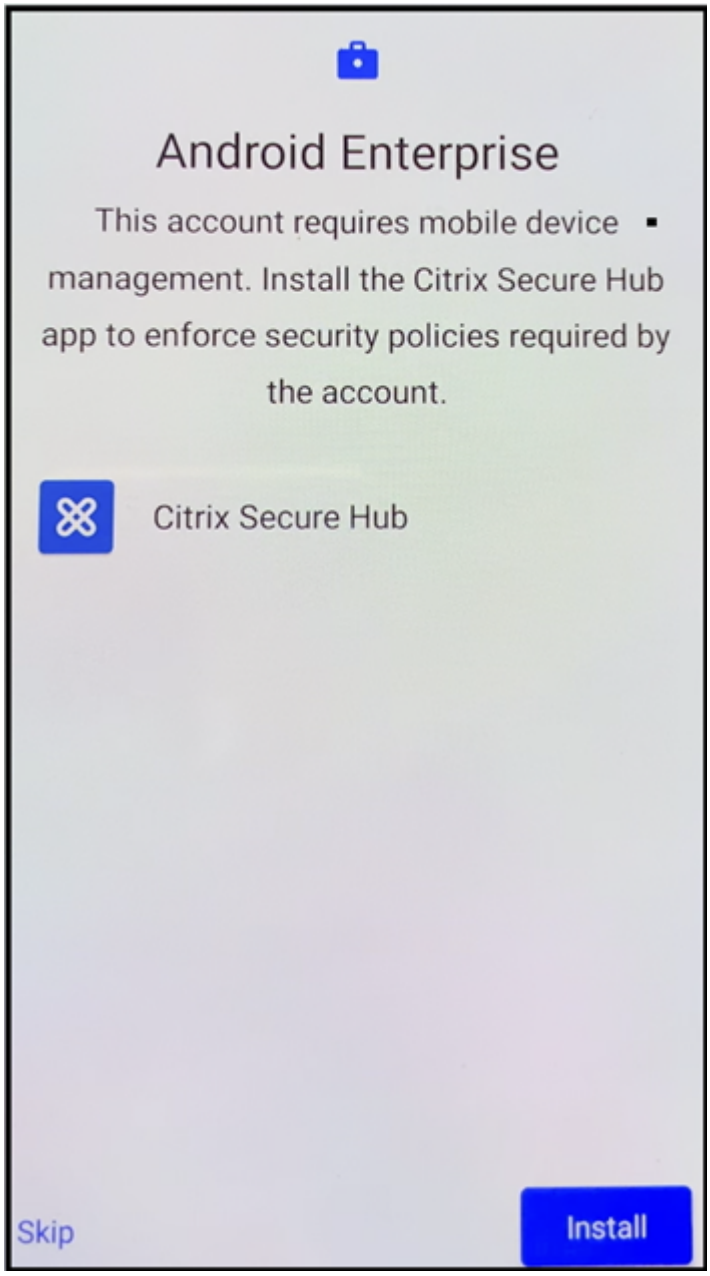
1. Power on a new or factory reset device.
2. The initial device setup loads and prompts for a Google account. If the device loads the home screen of the device, check the notification bar for a **Finish Setup** notification.



3. Enter `afw##xenmobile` in the **Email or phone** field.

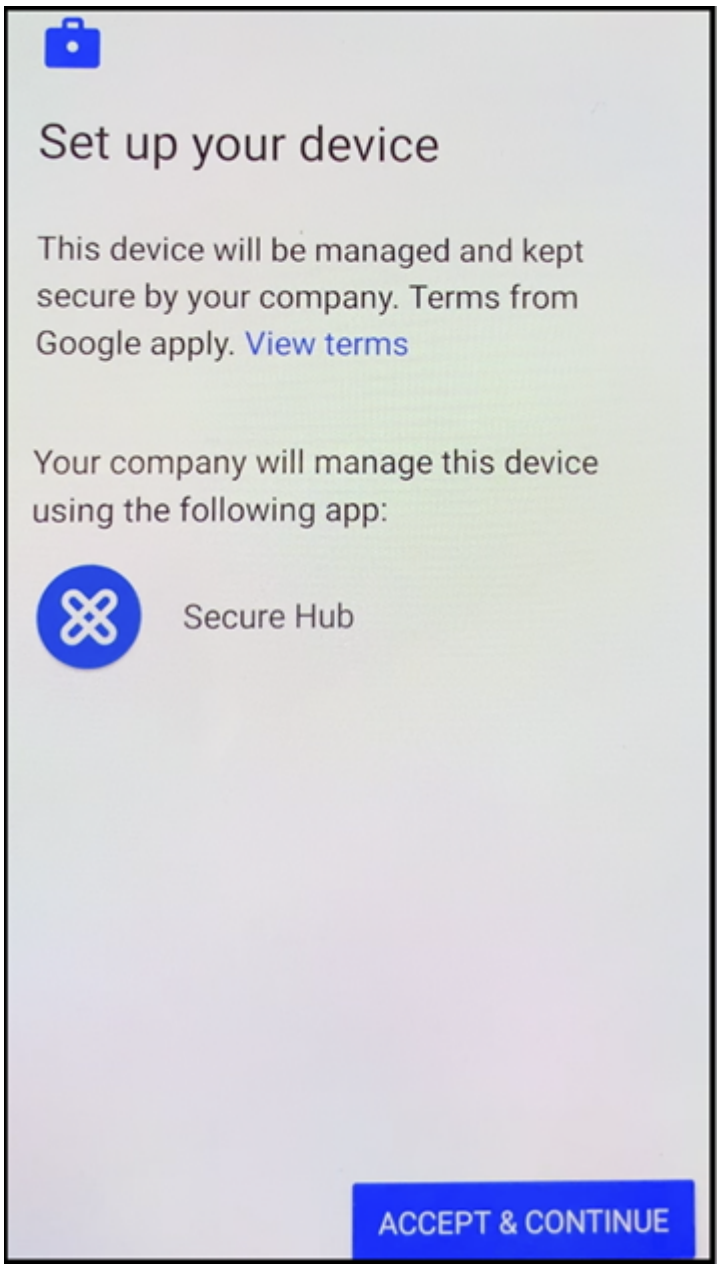


4. Tap **Install** on the Android Enterprise screen prompting to install Secure Hub.

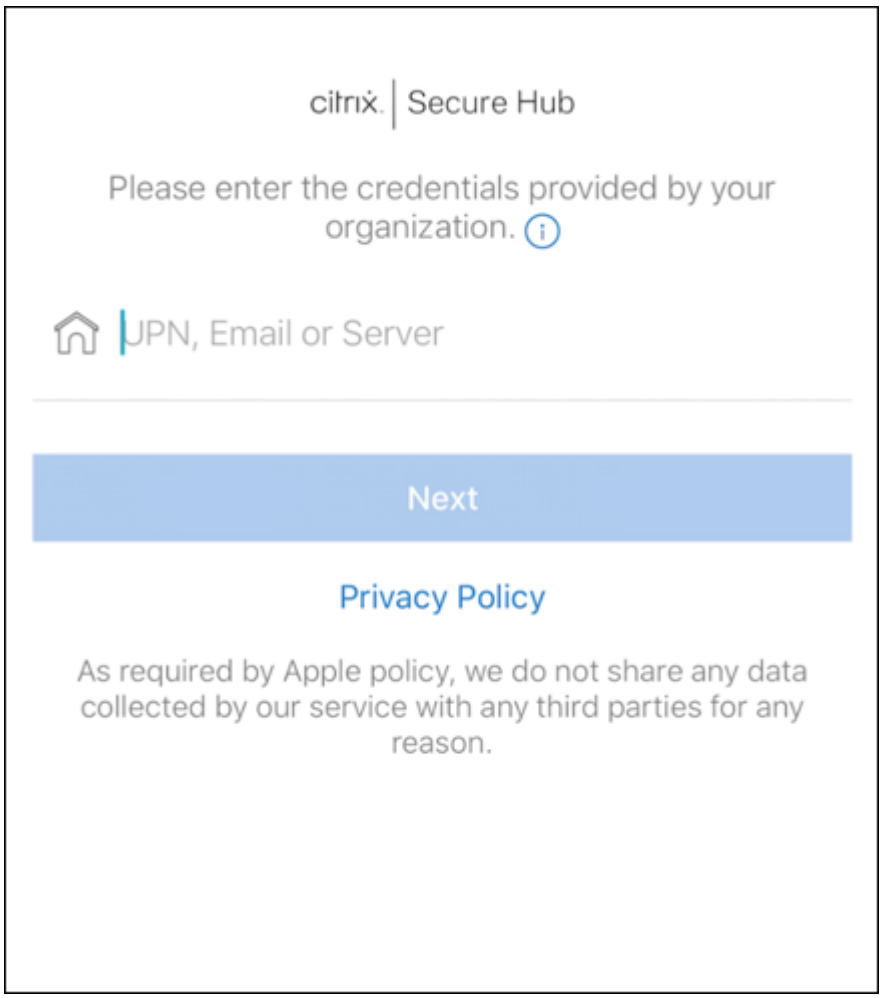


5. Tap **Install** on the Secure Hub installer screen.

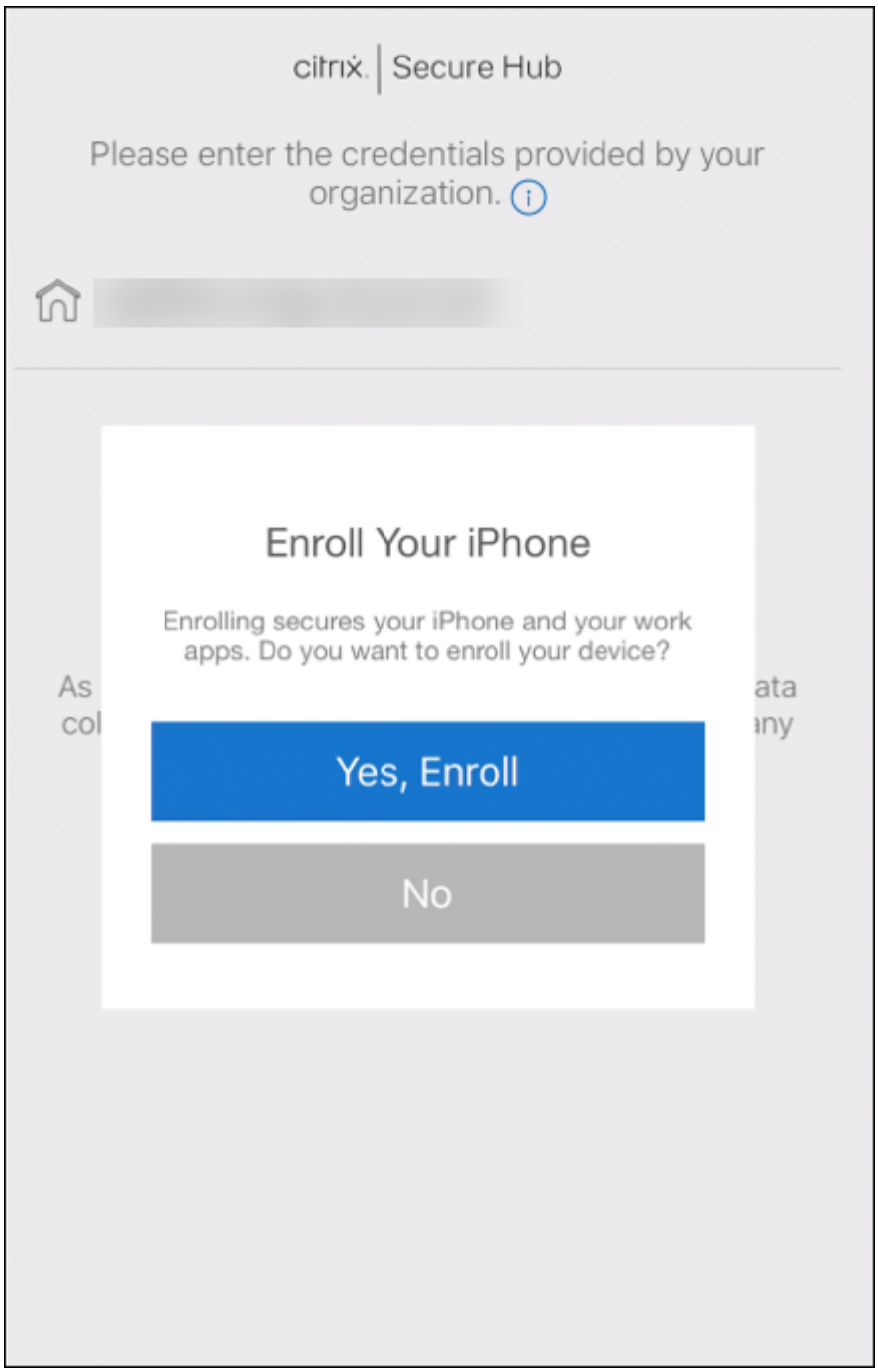
6. Tap **Allow** for all app permission requests.
7. Tap **Accept & Continue** to install Secure Hub and allow it to manage the device.



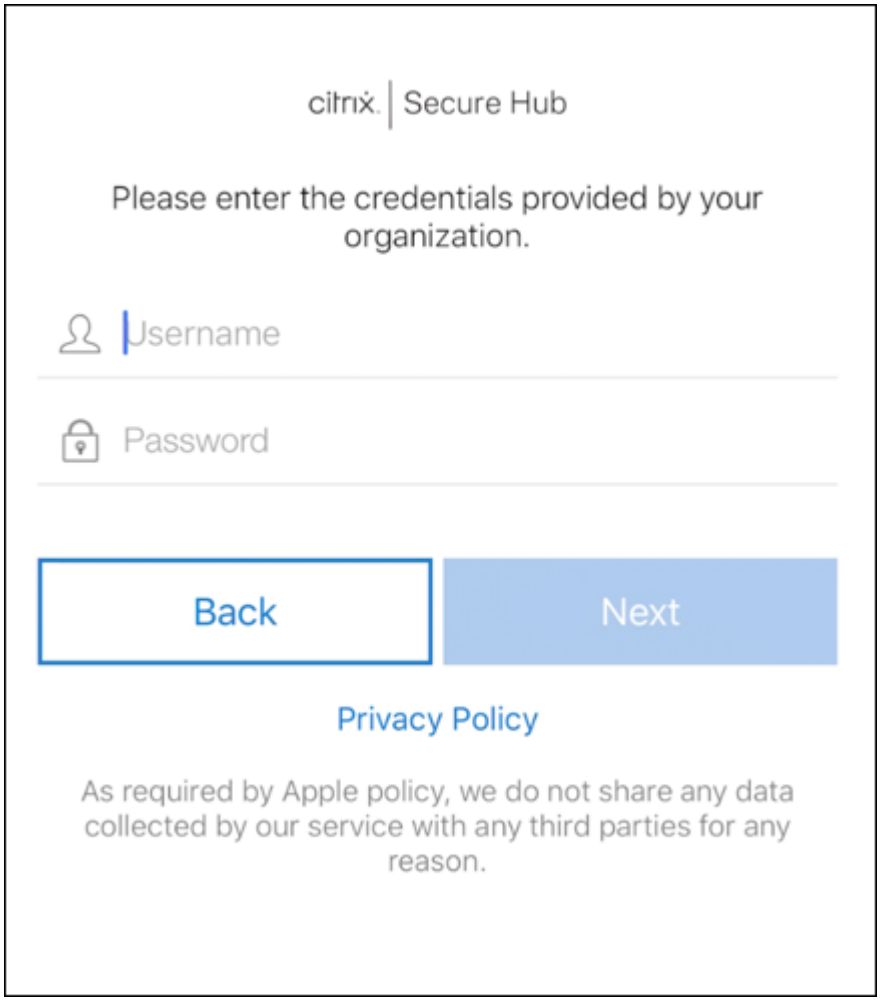
8. Secure Hub is now installed and on the default enrollment screen. In this example, AutoDiscovery is not set up. If it was, the user can enter their username/email and a server would be found for them. Instead, enter the enrollment URL for the environment and tap **Next**.



9. The default configuration for XenMobile allows users to choose if they use MAM or MDM+MAM. If prompted in this way, tap **Yes, Enroll** to choose MDM+MAM.

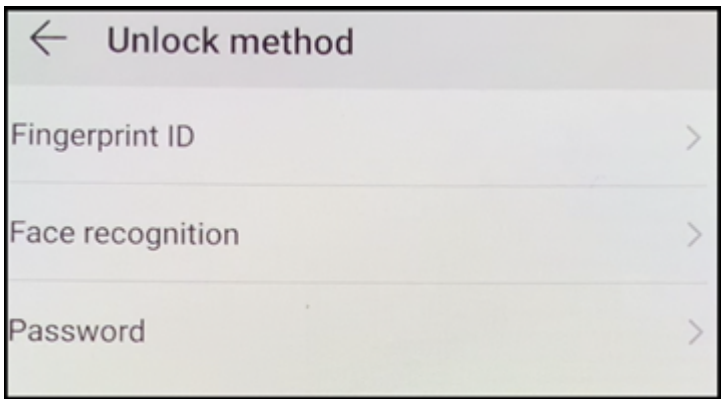


10. Enter the user name and password, then tap **Next**.

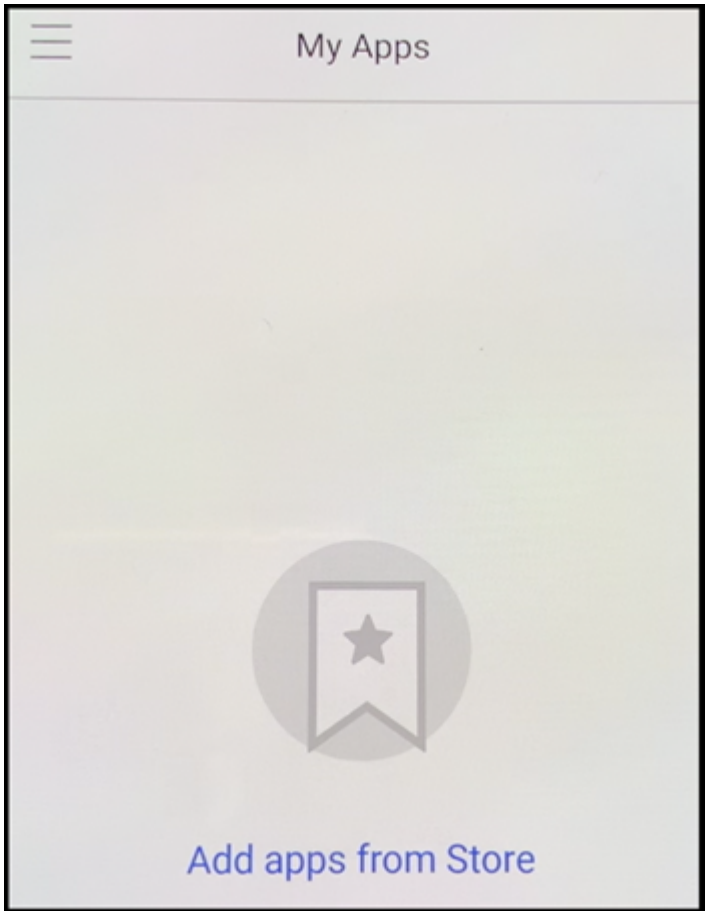


11. The user is prompted to configure a device passcode. Tap **Set** and enter a passcode.

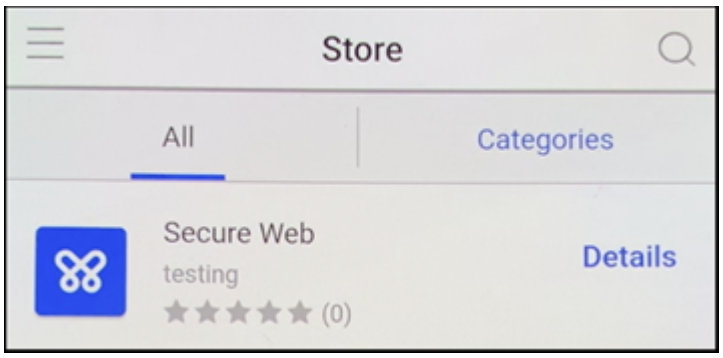
12. The user is prompted to configure a work profile unlock method. For this example, tap **Password**, tap **PIN**, and enter a PIN.



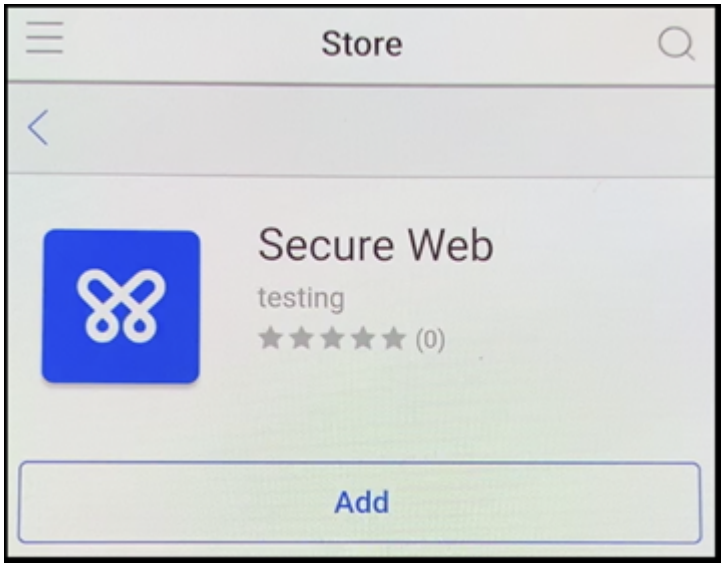
13. The device is now on the Secure Hub **My Apps** landing screen. Tap **Add apps from Store**.



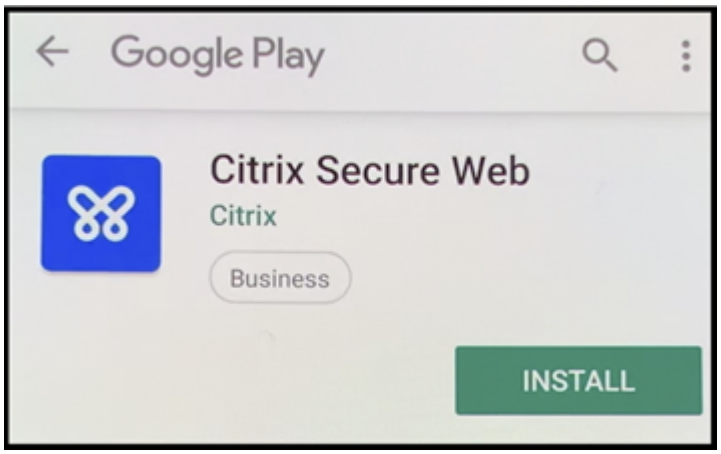
14. To add Secure Web, tap **Secure Web**.



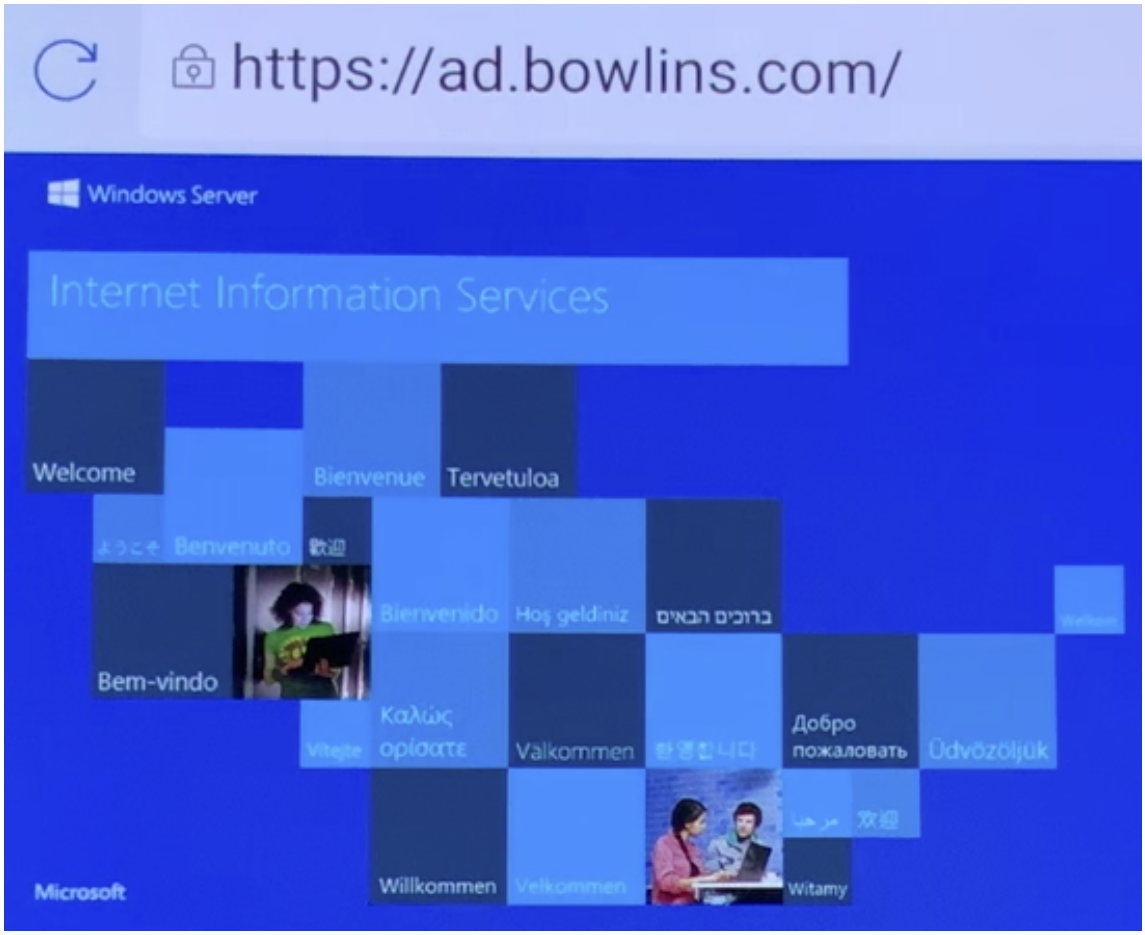
15. Tap **Add**.



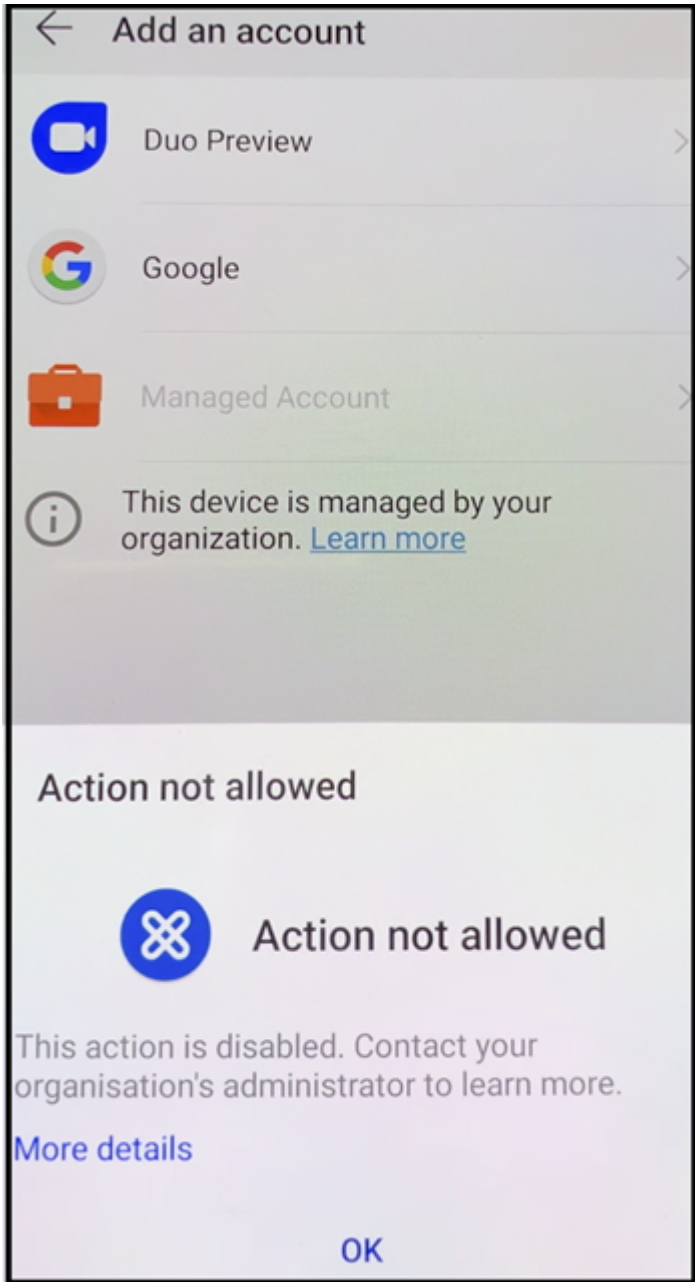
16. Secure Hub directs the user to the Google Play store to install Secure Web. Tap **Install**.



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 XenMobile Provisioning Tool.

System requirements and prerequisites

- Supported Android devices.

- 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 Secure Hub. Only one profile is allowed on each device. Attempting to add a second DPC app removes the installed Secure Hub.

Data transferred through the NFC bump

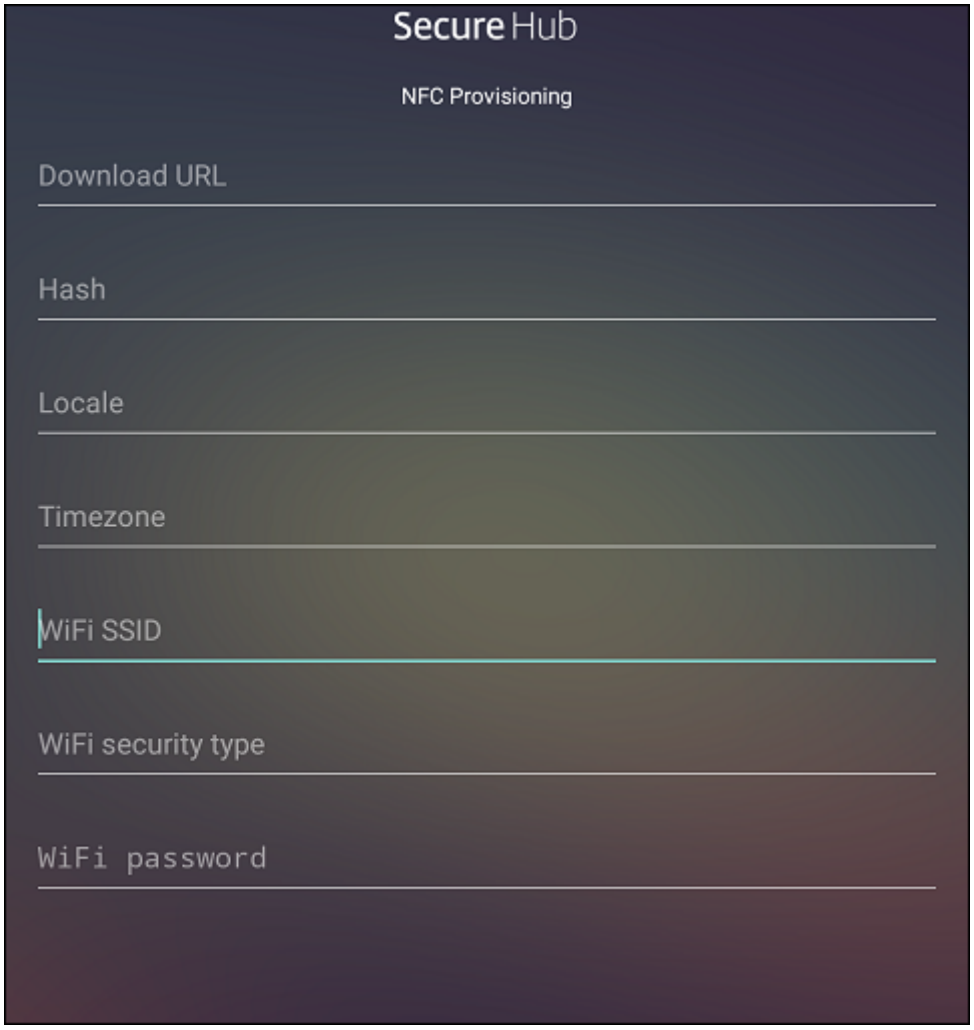
Provisioning a factory-reset device requires you to send the following data through an NFC bump to initialize Android Enterprise:

- 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.
- SHA1 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 XenMobile 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.



You can type data into the required fields or populate them using a 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=<SHA1 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 an Olson name of the form area/location. For example, America/Los_Angeles for Pacific time. If you don't enter a name, the time zone is automatically populated.

`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=ga50TwdCmfdJ72LGRFkke4Crb
\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=ga50TwdCmfdJ72LGRFkke4Cr
\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: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-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:

Download the app's APK file from the Google Play store.

In the OpenSSL command line, navigate to the **apksigner** tool: `android-sdk/build-tools/<version>/apksigner` and type the following:

```
apksigner verify -print-certs <apk_path> | perl -nle 'print
```


This content has been machine translated dynamically.

Give feedback here


```
60
61
62
63
64          Thank you for the feedback
65
66
67
68
69
70
71
72
73
74              XenMobile
75              XenMobile Server Current Release
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90                  This content has been machine translated dynamically.
91                  Dieser Inhalt ist eine maschinelle Übersetzung, die
                        dynamisch erstellt wurde. (Haftungsausschluss)
92                  Cet article a été traduit automatiquement de maniére
                        dynamique. (Clause de non responsabilité)
93                  Este artículo lo ha traducido una máquina de forma diná
                        mica. (Aviso legal)
94                  此内容已动态机器翻译。  放弃
95                  このコンテンツは動的に機械翻訳されています。免責事項
96                  This content has been machine translated dynamically.
97                  This content has been machine translated dynamically.
98                  This content has been machine translated dynamically.
99
100                 This article has been machine translated.
101                 Dieser Artikel wurde maschinell übersetzt. (
```



```
                    Haftungsausschluss)
102                 Ce article a été traduit automatiquement. (Clause de
                    non responsabilité)
103                 Este artículo ha sido traducido automáticamente. (Aviso
                     legal)
104                 この記事は機械翻訳されています.免責事項
105                 이 기사는 기계 번역되었습니다.
106                 Este artigo foi traduzido automaticamente.
107                 这篇文章已经过机器翻译.放弃
108
109
110
111
112
113
114                             Switch to english
115                             Auf Englisch anzeigen
116                             Lire en anglais
117                             Leer en inglés
118                             英語に切り替え
119                             영어로 전환
120                             Mudar para ingles
121                             切换到英文
122
123
124
125
126
127
128
129
130         Translation failed!
131
132
133
134
135
136
137
138
139                                     Android Enterprise
140
141
142
143
```



```
144
145
146                 June 25, 2021
147
148                                 Contributed by:
149
150
151
152
153                                                                 C
154
155
156
157
158
159
160                         Android Enterprise is a set of tools and
                               services provided by Google as an enterprise
                                management solution for Android devices.
                               With Android Enterprise:
161
162
163
164     You use XenMobile to manage company-owned Android devices and bring
            your own device (BYOD) Android devices.
165
166
167     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.
168
169
170     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.
171
172
173
174 Resources:
175
176
177
178     For a list of terms and definitions related to Android Enterprise,
           see Android Enterprise terminology in the Google Android
           Enterprise developers guide. Google updates these terms
```



```
          frequently.
179
180
181     For Android operating systems supported for XenMobile, see
          Supported device operating systems.
182
183
184     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.
185
186
187
188 When you integrate XenMobile 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.
189
190 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 XenMobile with Android
      Enterprise, the complete solution has these components:
191
192
193
194 XenMobile:  The Citrix EMM. XenMobile is the unified XenMobile solution
      for a secure digital workspace. XenMobile provides the means for IT
      administrators to manage devices and apps for their organizations.
195
196 Citrix Secure Hub:  The Citrix DPC app. Secure Hub is the launchpad for
      XenMobile. Secure Hub enforces policies on the device.
197
198 Managed Google Play:  A Google enterprise app platform that integrates
      with XenMobile. The Google Play EMM API sets app policies and
      distributes app.
199
200
201 This illustration shows how administrators interact with these
      components and how the components interact with each other:
202
203
204
205
206 Using managed Google Play with XenMobile
```



```
207
208
209   Note:
210
211   You can use either managed Google Play or Google Workspace 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 (formerly G-Suite) customers.
212
213
214 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.
215
216 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 to manage separate sets of devices and apps.
217
218 For XenMobile 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.
219
220 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.
221
222
223 Device deployment scenarios and modes of operation
224
225 Device deployment scenario 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.
226
227 A work profile isolates business accounts, apps, and data from personal
        accounts, apps, and data. For more details about work profiles, see
```



```
        the Google Android Enterprise help topic, What is a work profile.
228
229
230    Important:
231
232    When Android Enterprise devices update to Android 11, Google will
          migrate devices managed as  “fully managed with a work profile”
          to a new security-enhanced work profile experience. For more
          information, see Changes ahead for Android Enterprise’ s Fully
          Managed with Work Profile.
233
234
235
236
237
238        Device management
```

Use cases

Work profile

Personal profile

Notes

Company-owned devices (fully managed)

Company-owned devices intended only for work use

No

Yes. The DPC can perform device-wide actions, such as configure device-wide connectivity, configure global settings, and perform a factory reset.

For new or factory reset devices only.

Fully managed with a work profile

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.

Formerly known as corporate-owned personally enabled (COPE) devices.

Dedicated devices*

Company-owned devices configured for a single use case, such as digital signage or ticket printing

No

Yes. You provide only the required apps and prevent users from adding other apps.

Formerly known as corporate owned single use (COSU) devices.

BYOD work profile**

Personal devices enrolled in work profile mode (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.

* 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.

** XenMobile does not support Zebra devices as in BYOD work profile mode. XenMobile supports Zebra devices as fully managed devices and in device legacy mode (also called device admin mode).

For information on migrating from legacy mode to device owner or profile owner mode, see Migrate from device administration to Android Enterprise.

Authentication methods

Enrollment profiles determine whether Android devices enroll in MAM, MDM, or MDM+MAM, with the option for users to opt out of MDM.

The enrollment security modes **User name + PIN**, **Invitation URL**, **Invitation URL + PIN**, and **Invitation URL + Password** aren't available for Android Enterprise. For information about specifying the level of security and required enrollment steps, see To configure enrollment security modes.

XenMobile supports the following authentication methods for Android devices enrolled in MDM+MAM. For information, see the articles under Certificates and authentication.

- Domain
- Domain plus security token
- Client certificate
- Client certificate plus domain
- Identity providers:
  - Azure Active Directory
  - Citrix Identity provider

Another 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:

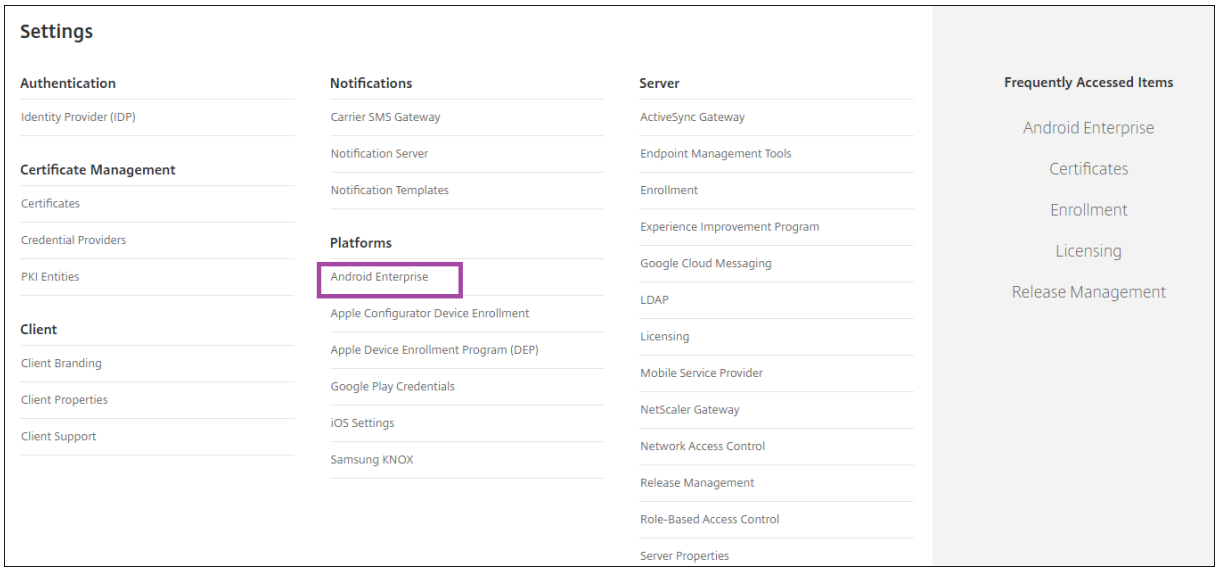
- Accounts and credentials:
  - To set up Android Enterprise with managed Google Play, a corporate Google account
  - To download the latest MDX files, a Citrix customer account
  - To deploy private apps (optional), a Google developer account
- Firebase Cloud Messaging (FCM) configured for XenMobile. See Firebase Cloud Messaging for instructions.
- For Samsung Knox Mobile Enrollment (optional), Knox premium licenses.

Connecting XenMobile to Google Play

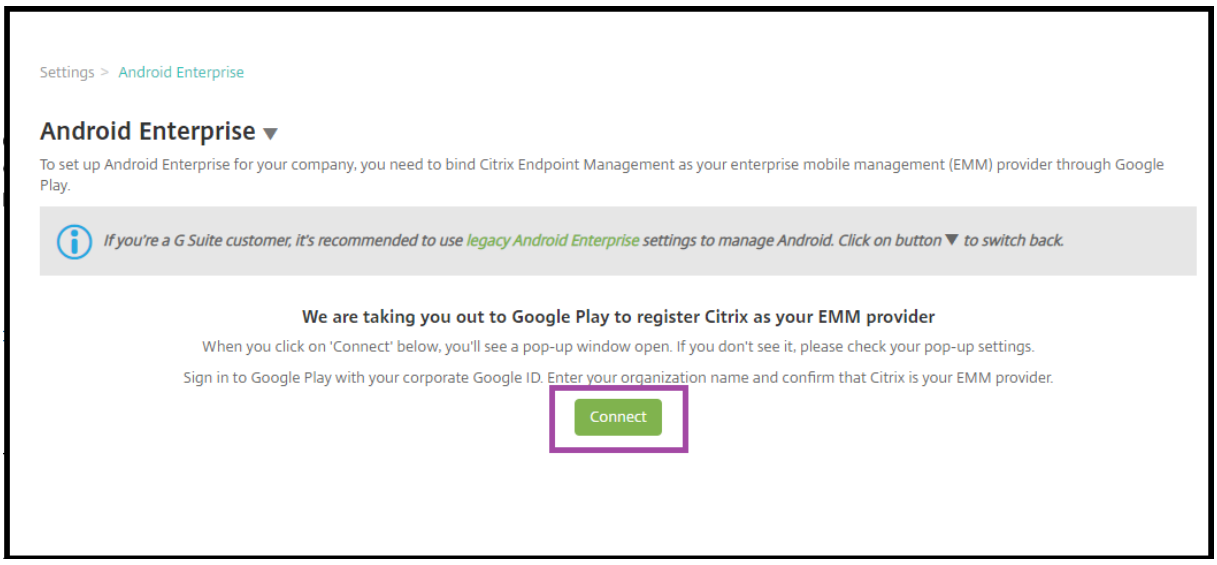
To set up Android Enterprise for your organization, register Citrix as your EMM provider through managed Google Play. That setup connects managed Google Play to XenMobile and creates an enterprise for Android Enterprise in XenMobile.

You need a corporate Google account to sign in to Google Play.

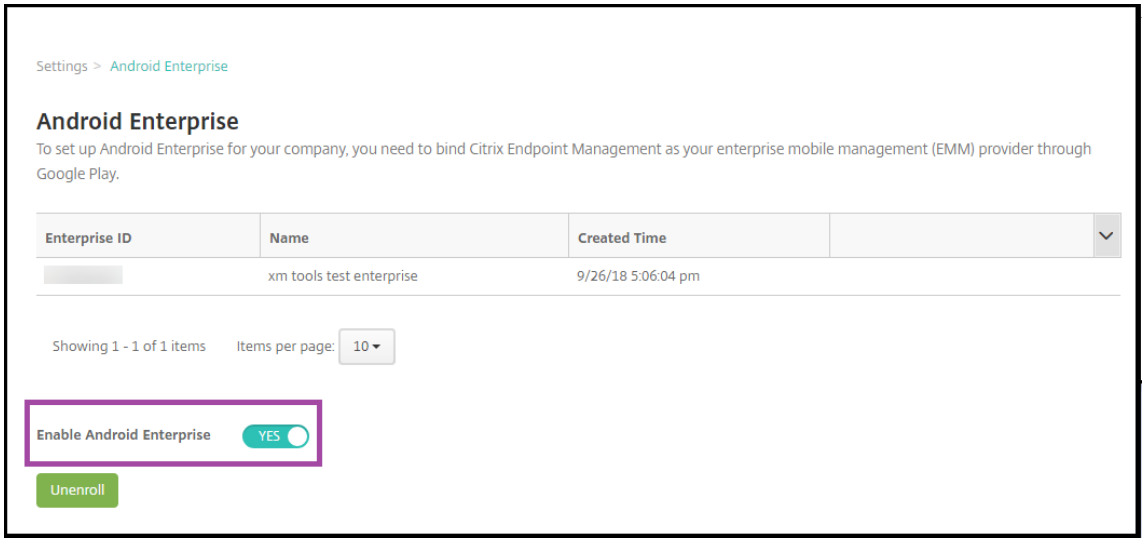
1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Go to **Settings > Android Enterprise**.



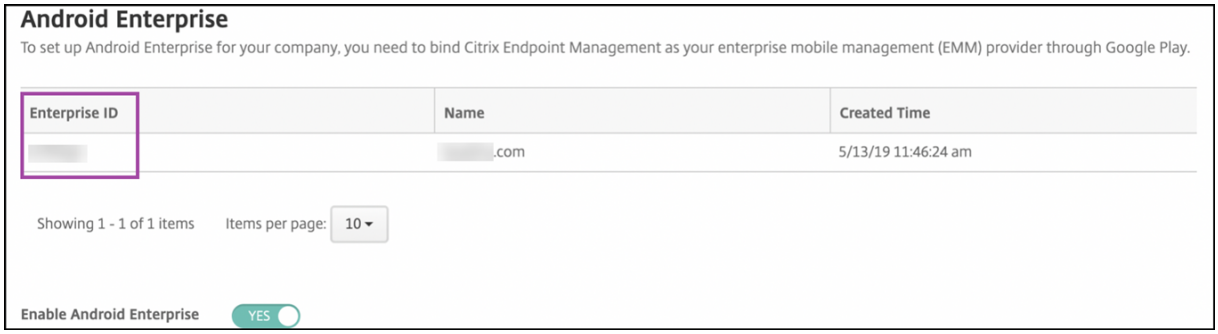
1. Click **Connect**. Google Play opens.



1. Sign in to Google Play with your corporate Google account credentials. Enter your organization name and confirm Citrix is your EMM provider.
2. An enterprise ID is added for Android Enterprise. To enable Android Enterprise, slide **Enable Android Enterprise** to **Yes**.



Your Enterprise ID appears in the XenMobile console.



Your environment is connected to Google and is ready to manage devices. You can now provide apps for users.

XenMobile can be used to 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.

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.

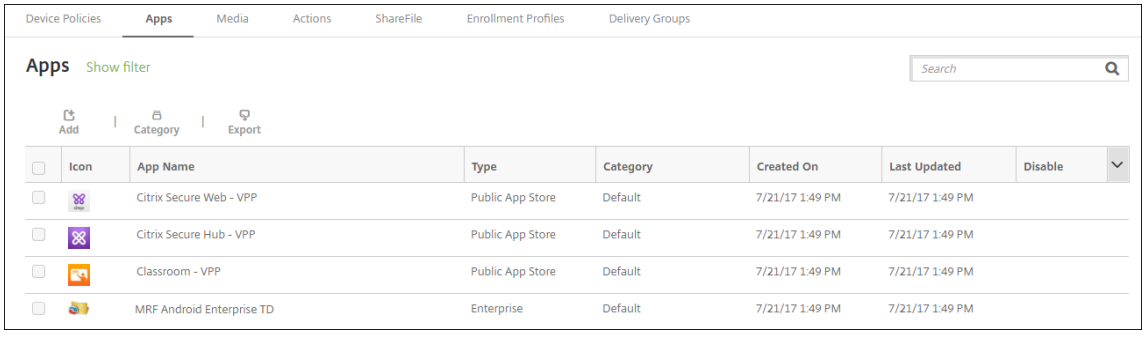
The apps you publish are available to devices enrolled in your Android Enterprise enterprise.

> **Note:**
>
> When you deploy an Android Enterprise public app store app to an Android user, that user is automatically enrolled in Android Enterprise.

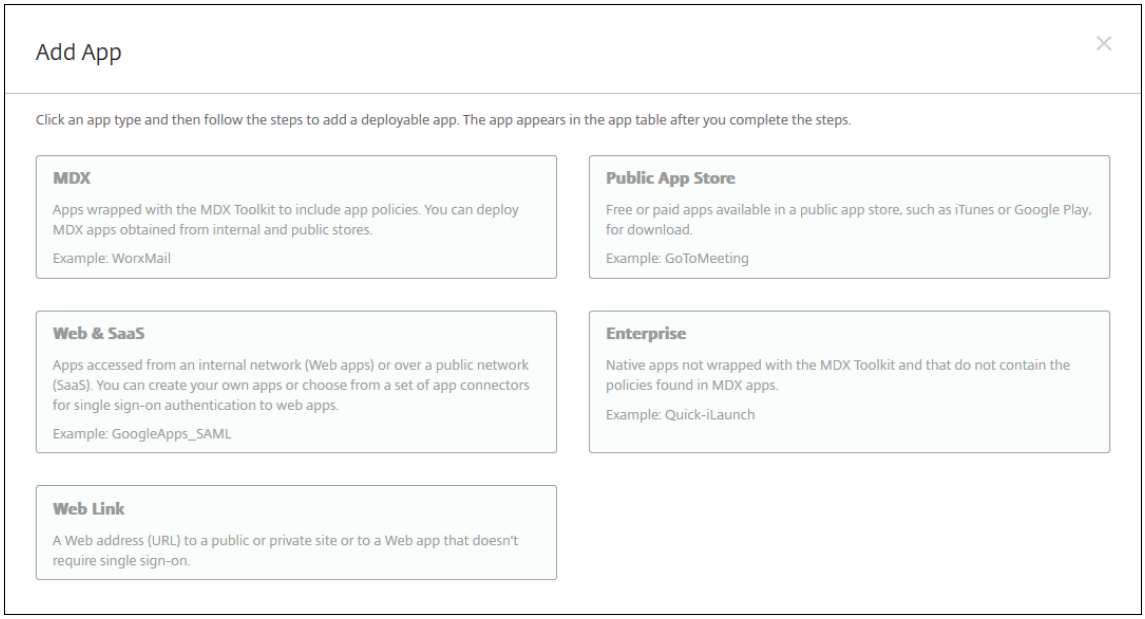
Configure apps as MDX apps

To configure a Citrix productivity app as an MDX app for Android Enterprise:

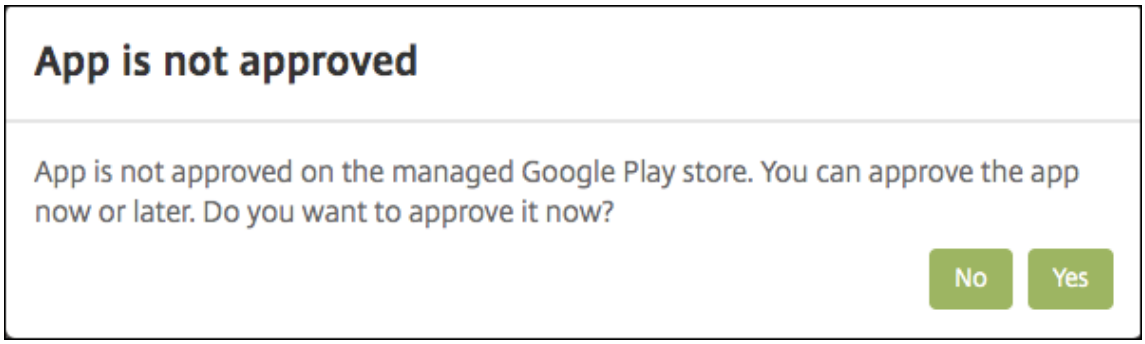
1. In the XenMobile console, click **Configure > Apps**. The **Apps** page appears.



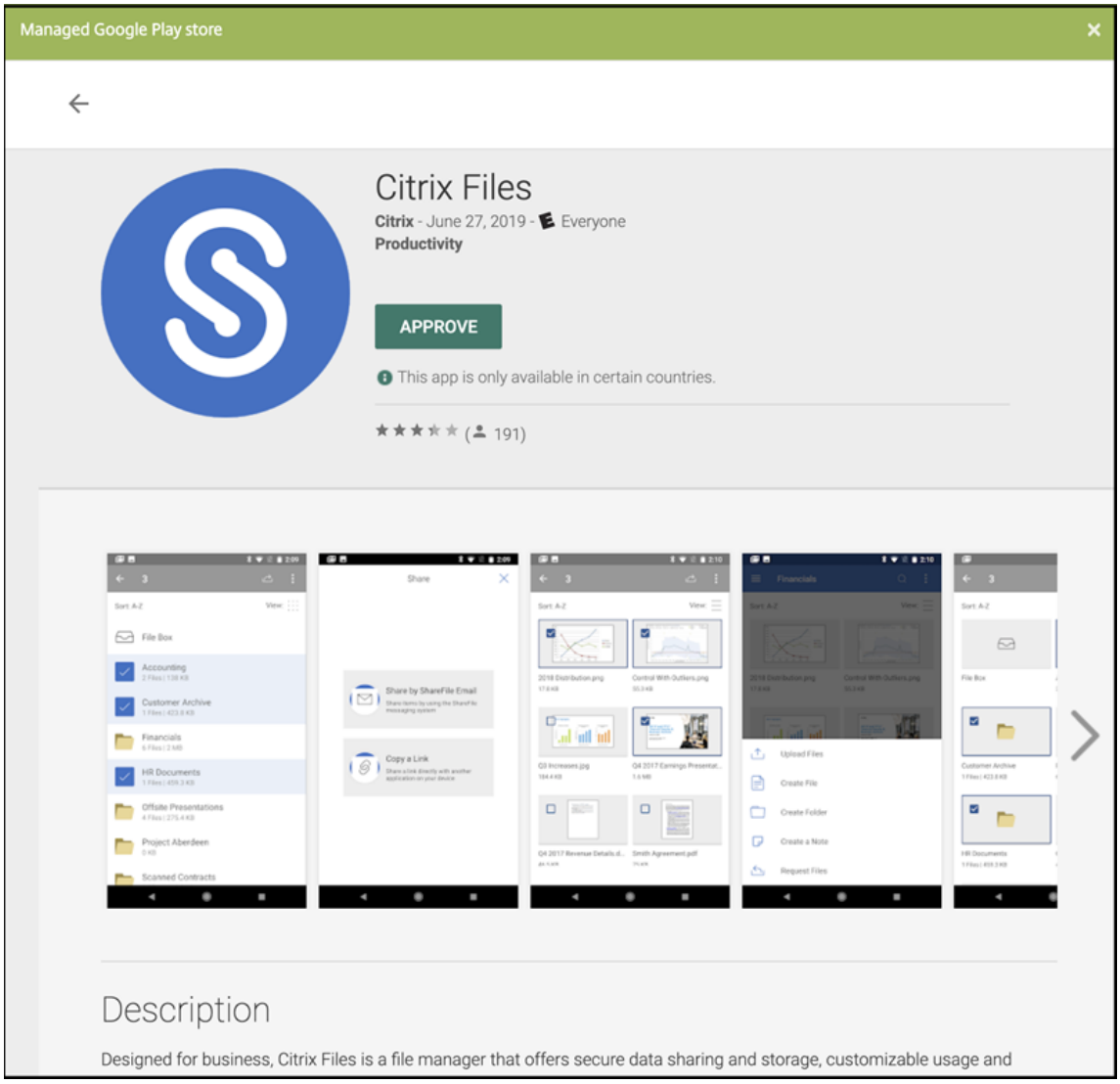
2. Click **Add**. The **Add App** dialog box appears.



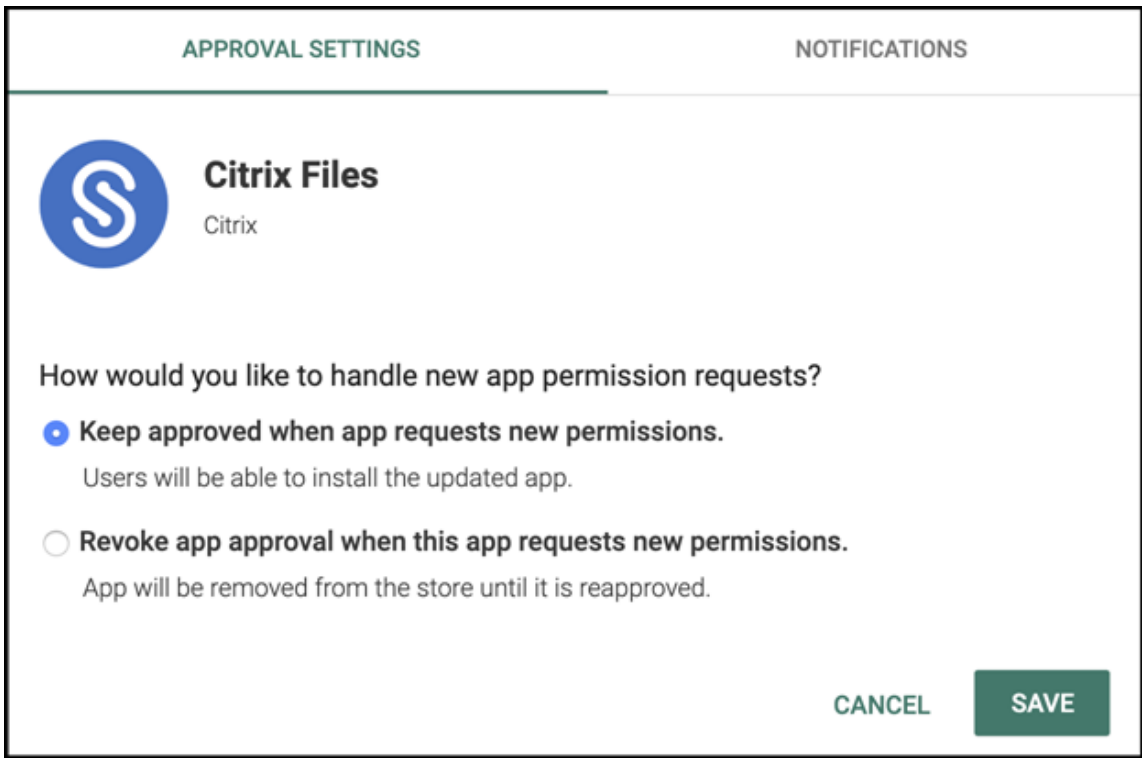
3. Click **MDX**. The **App Information** page appears.
4. On the left side of the page, select **Android Enterprise** as the platform.
5. On the **App Information** page, type the following information:
   - **Name:** Type a descriptive name for the app. This name appears under **App Name** on the **Apps** 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 XenMobile console, click **Yes**.



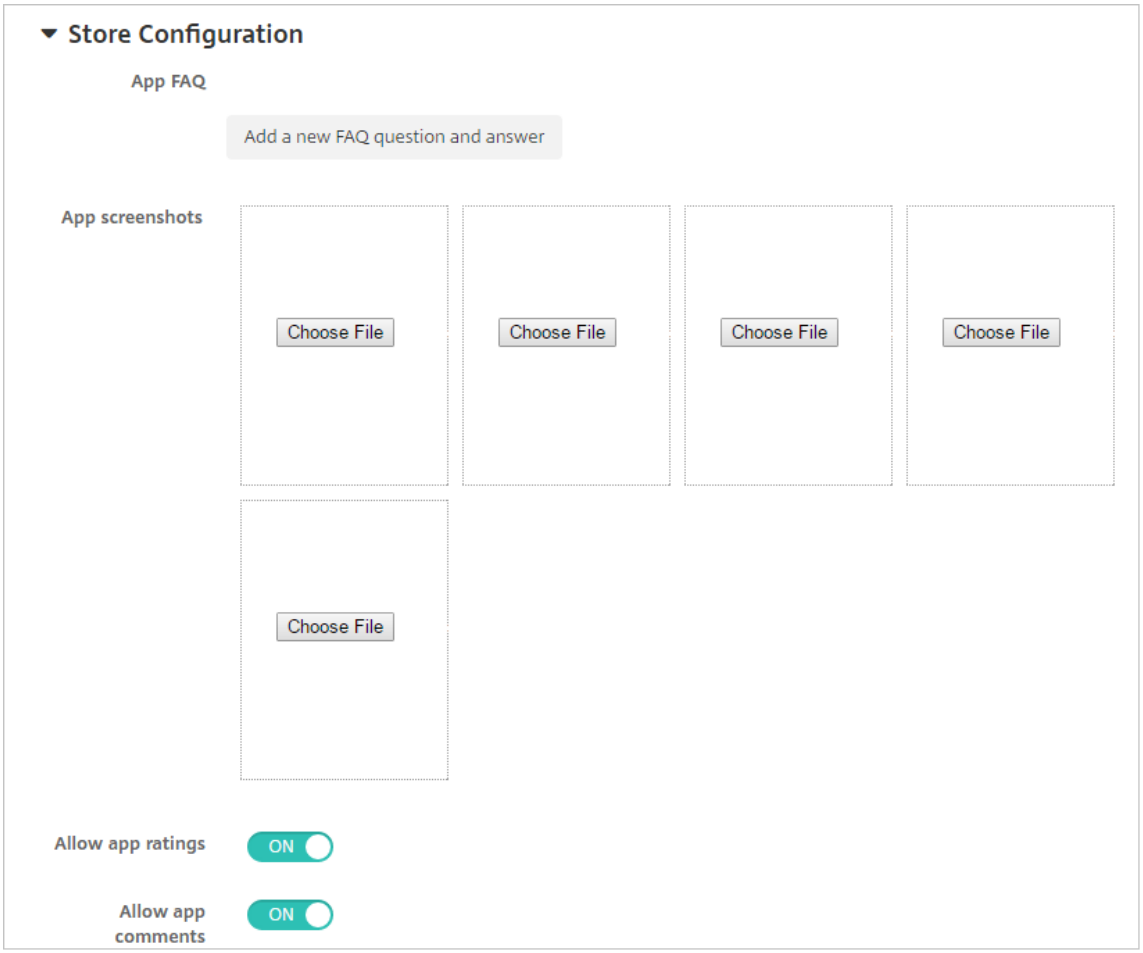
9. When the managed Google Play store page opens, click **Approve**.



10. Click **Approve** again.
11. Select **Keep approved when app requests new permissions**. Click **Save**.



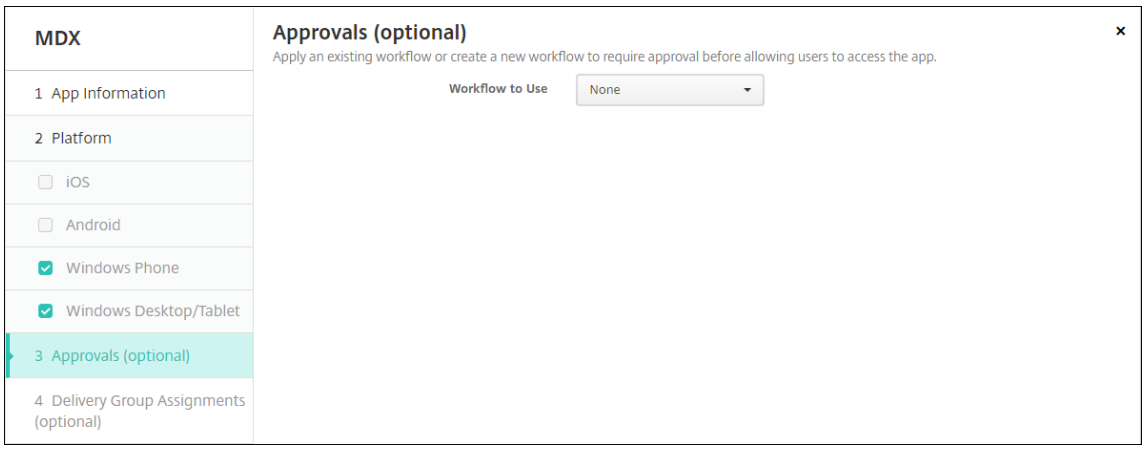
12. When the app is approved and saved, more settings appear on the page. Configure these settings:
    - **File name:** Type the file name associated with the app.
    - **App Description:** Type a description for the app.
    - **Product track:** Specify which product track you want to push to user 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.



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.



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.

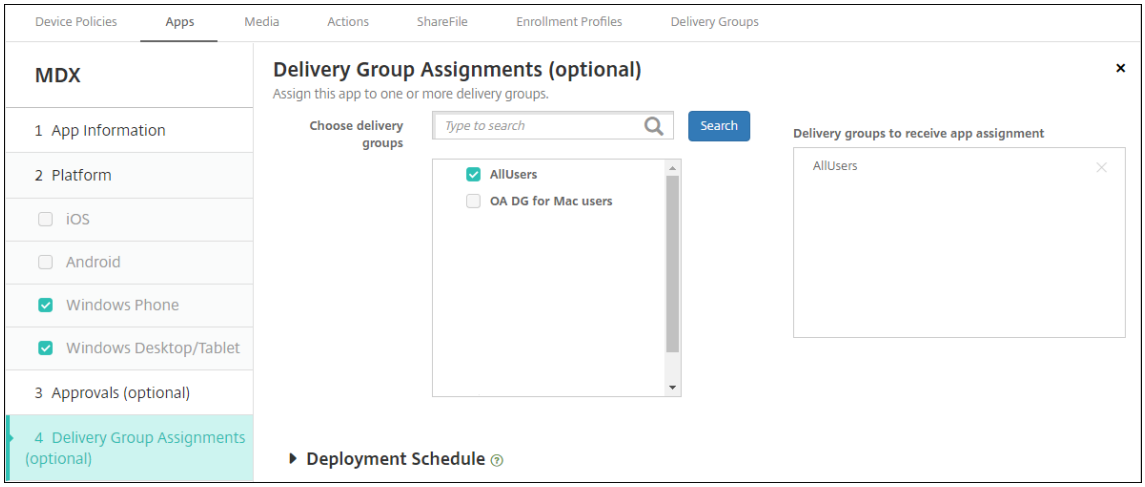
Configure these settings to assign or create a workflow:

- **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 Apply 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 if you began using XenMobile with version 10.18.19 or later. We don't recommend the connections for customers who began using XenMobile 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 to configure an MDX app for each mobile productivity app.

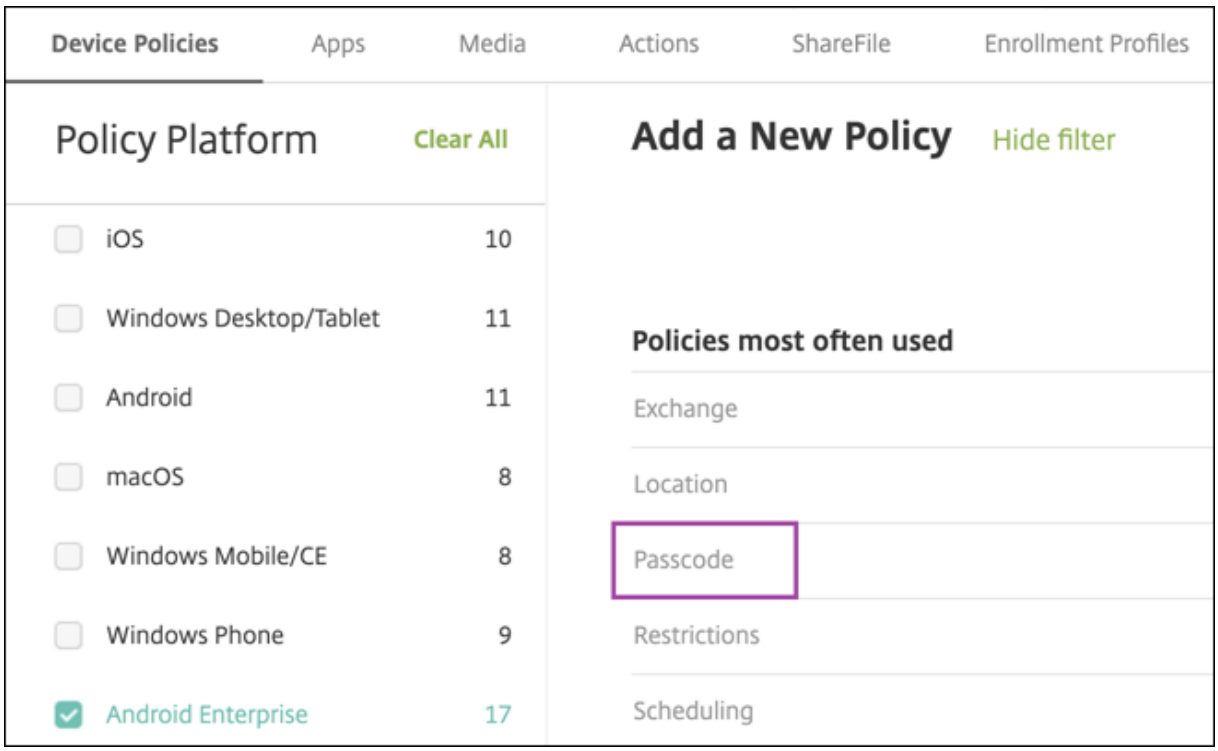
Configure security challenge policy

The XenMobile Passcode device policy configures the set of rules for the security challenges users to 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.

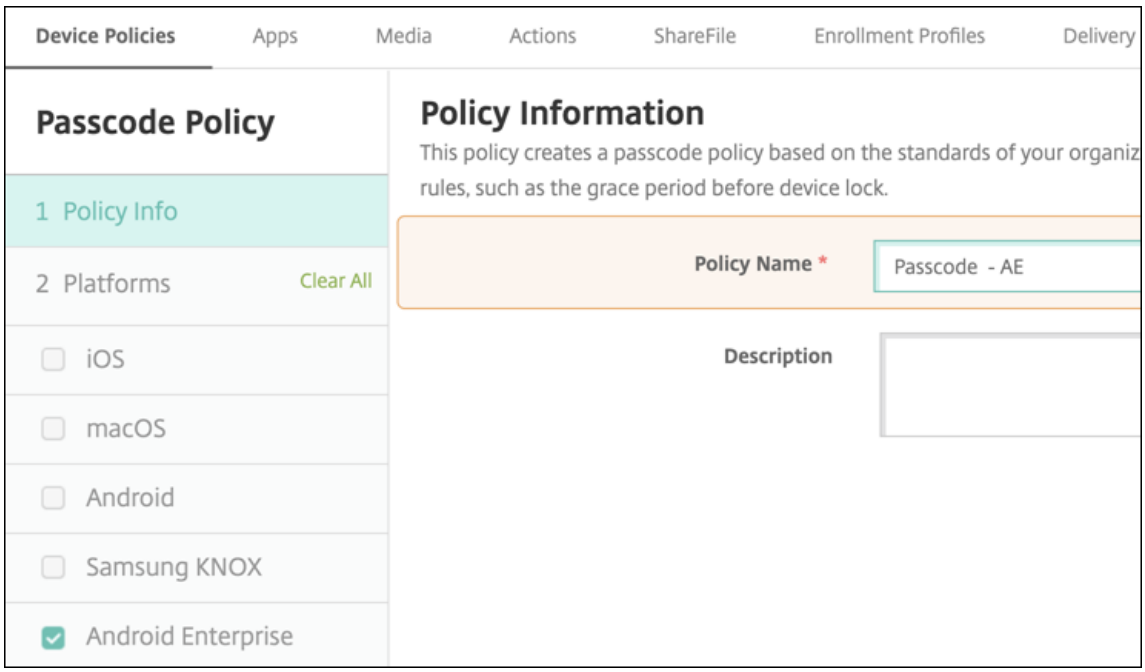
- If your Android Enterprise deployment includes BYOD devices, configure the passcode policy for the work profile.
- If your deployment includes, company-owned, fully managed devices, configure the passcode policy for the device itself.
- If your deployment includes both types of devices, configure both types of passcode policy.

To configure the passcode policy:

1. In the XenMobile 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.



1. Enter a **Policy Name**. Click **Next**.



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 in enabled for your XenMobile 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 (COSU devices)
- Fully managed devices with a work profile (COPE 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 XenMobile deployment, all newly enrolled or re-enrolled 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 devices.

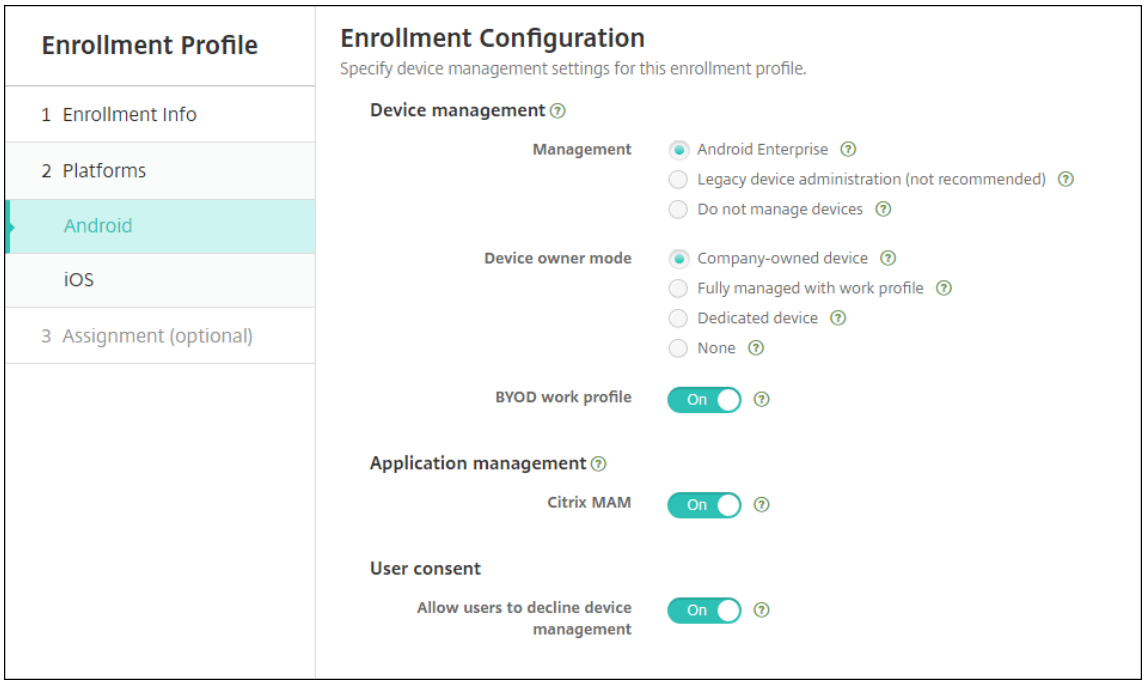
When you create enrollment profiles, you assign delivery groups to them. If a user belongs to multiple delivery groups that have different enrollment profiles, the name of the delivery group determines the enrollment profile used. XenMobile selects the delivery group that appears last in an alphabetized list of delivery groups. For more information, see Enrollment profiles.

You can use enrollment profiles to combine multiple use cases such as MDM only, MDM+MAM, and MAM only. Your XenMobile Server license type, reflected in the server property, `xms.server.mode`, determines the settings available in **Configure > 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.

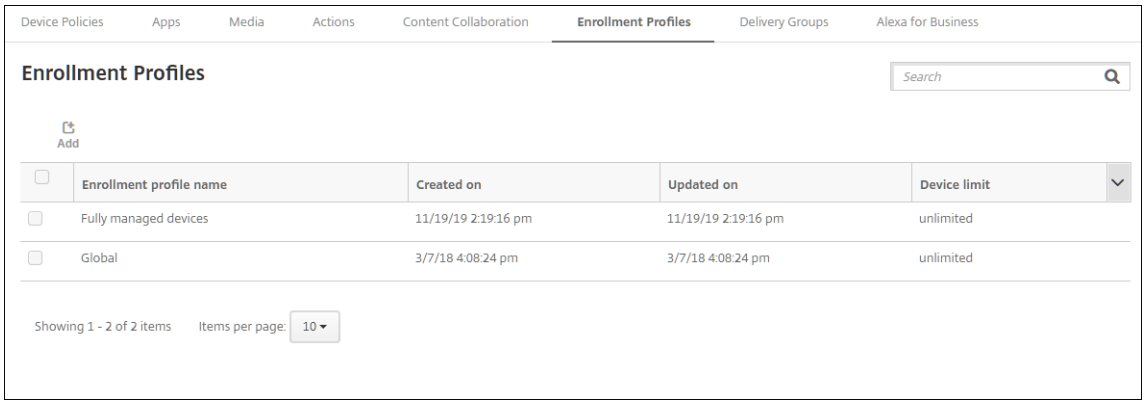
1. In the XenMobile console, go to **Configure > Enrollment Profiles**.
2. To add an enrollment profile, click **Add**. In the Enrollment Info page, type a name for the enrollment profile.
3. Set the number of devices that members with this profile can enroll.
4. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
5. Set **Management** to **Android Enterprise**.
6. Set **Device owner mode** to **Company owned device**.



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. The default is **On**.
   - Set **BYOD work profile** to **Off** to restrict enrollment to fully managed devices.
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.

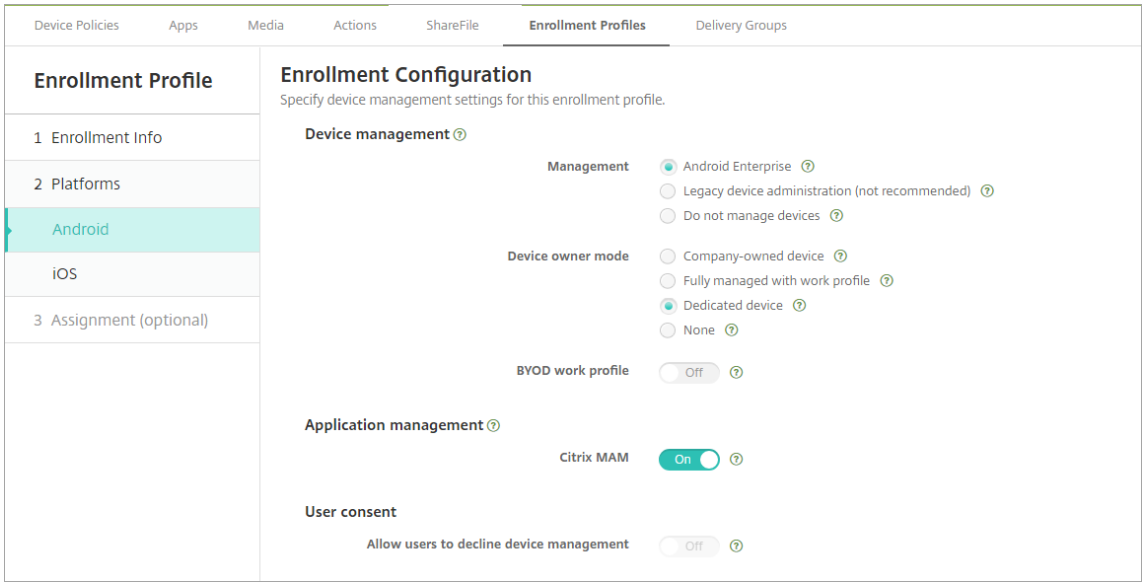


Add a dedicated device enrollment profile

When your XenMobile deployment includes dedicated devices, a single XenMobile 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 XenMobile 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. Ensure that the number of devices that members with this profile can enroll is set to unlimited.

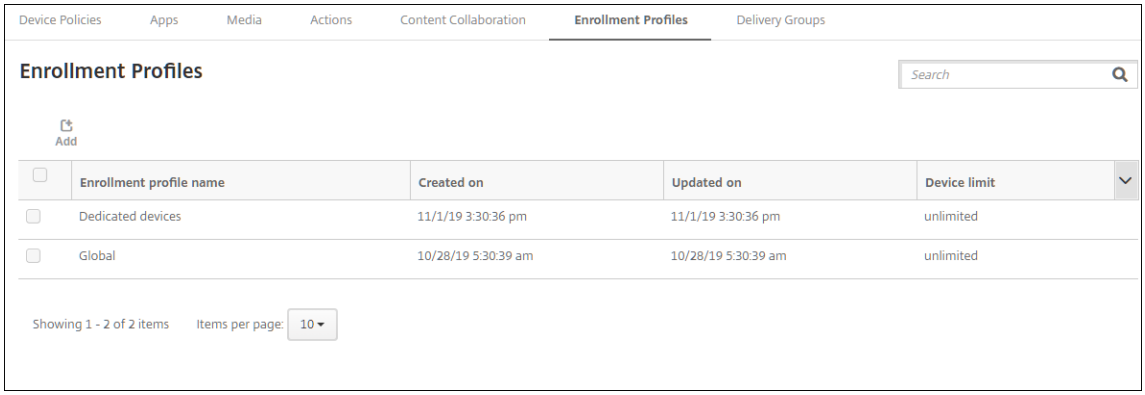
3. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
4. Set **Management** to **Android Enterprise**.
5. Set **Device owner mode** to **Dedicated device**.



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**.

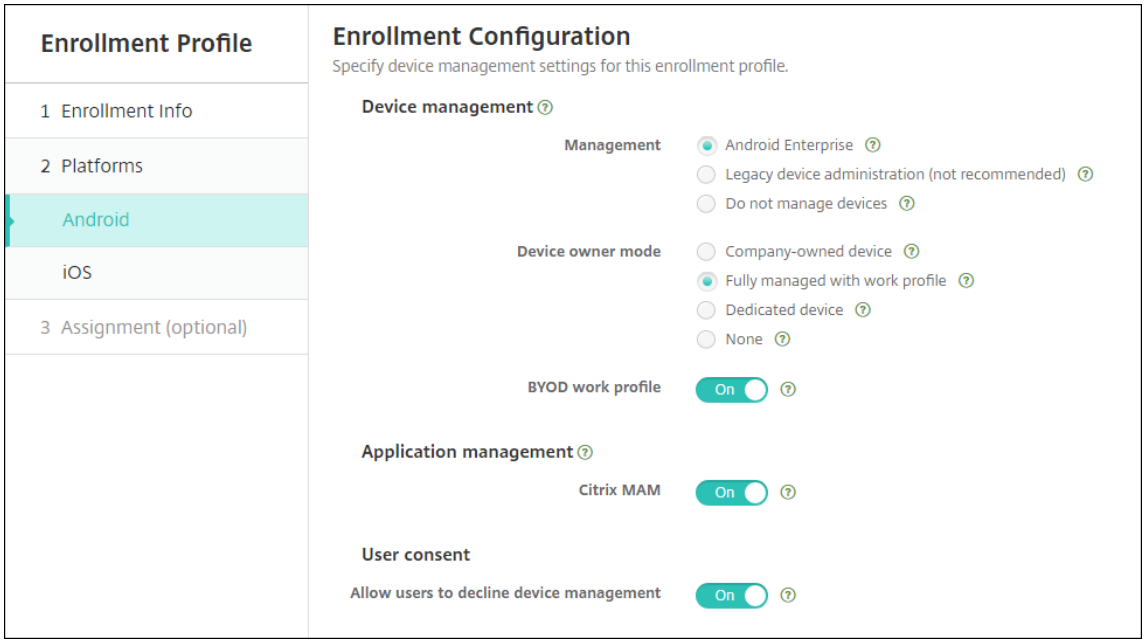
   If **BYOD work profile** is set to **On**, the default value of **Allow users to decline device management** is **On**. If **BYOD work profile** is set to **Off**, then **Allow users to decline device management** is disabled.
9. Select **Assignment (options)**. The Delivery Group Assignment screen appears.
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

1. In the XenMobile 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**.



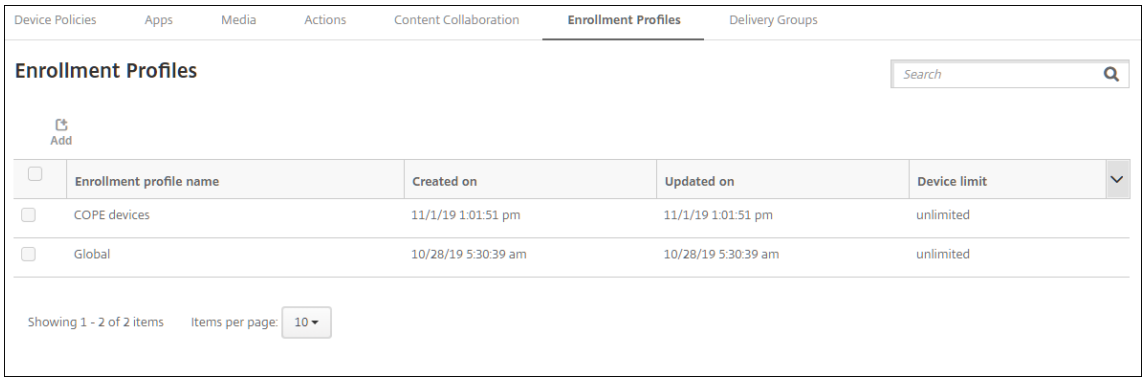
6. **BYOD work profile** allows you to configure the enrollment profile to enroll BYOD devices as work profile devices. New and factory reset devices are enrolled as fully managed devices with a work profile. Set **BYOD work profile** to **On** to allow enrollment of BYOD devices as work profile

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 is deprecating 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:

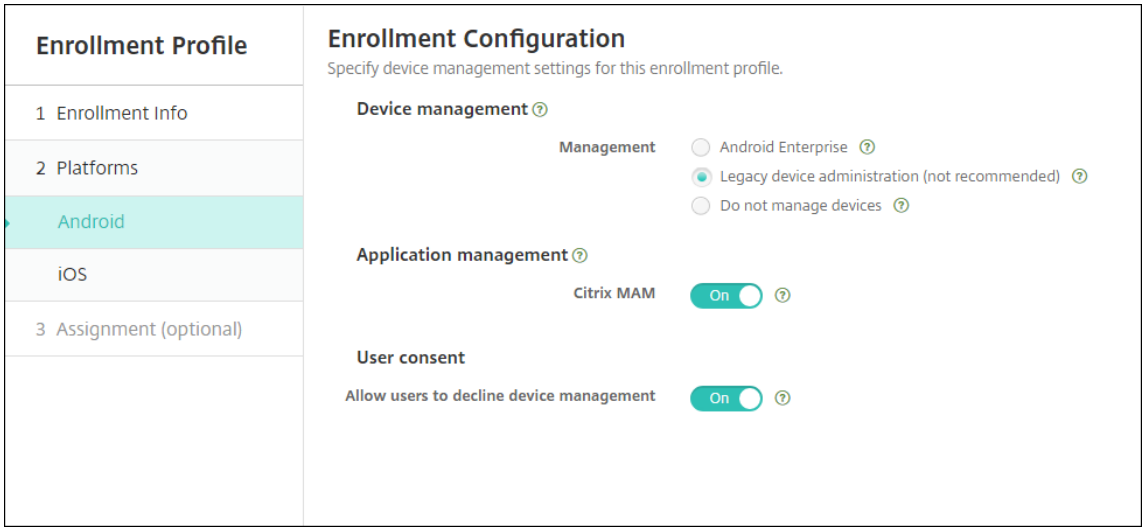
- Citrix makes Android Enterprise the default enrollment option for Android devices.
- If Android Enterprise is enabled for your XenMobile deployment, all newly enrolled or re-enrolled Android devices are enrolled as Android Enterprise devices.

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, XenMobile 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.

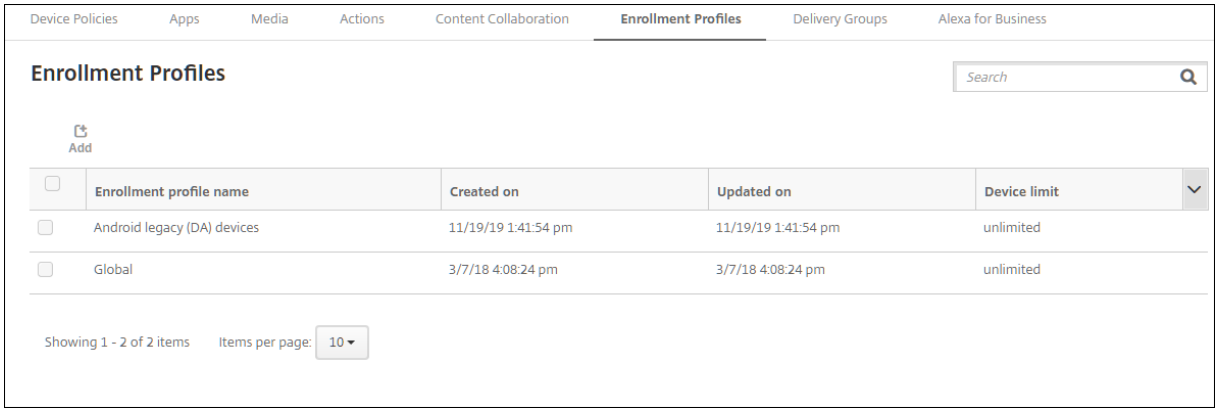
To create an enrollment profile for legacy devices:

1. In the XenMobile 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**.



6. Choose whether to enroll devices in Citrix MAM.
7. To allow users to decline device management when they enroll their devices, set **Allow users to decline device management** to **On**. Default is **On**.
8. Select **Assignment (options)**. The Delivery Group Assignment screen appears.
9. 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 a legacy device 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 XenMobile. 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.

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 XenMobile 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.

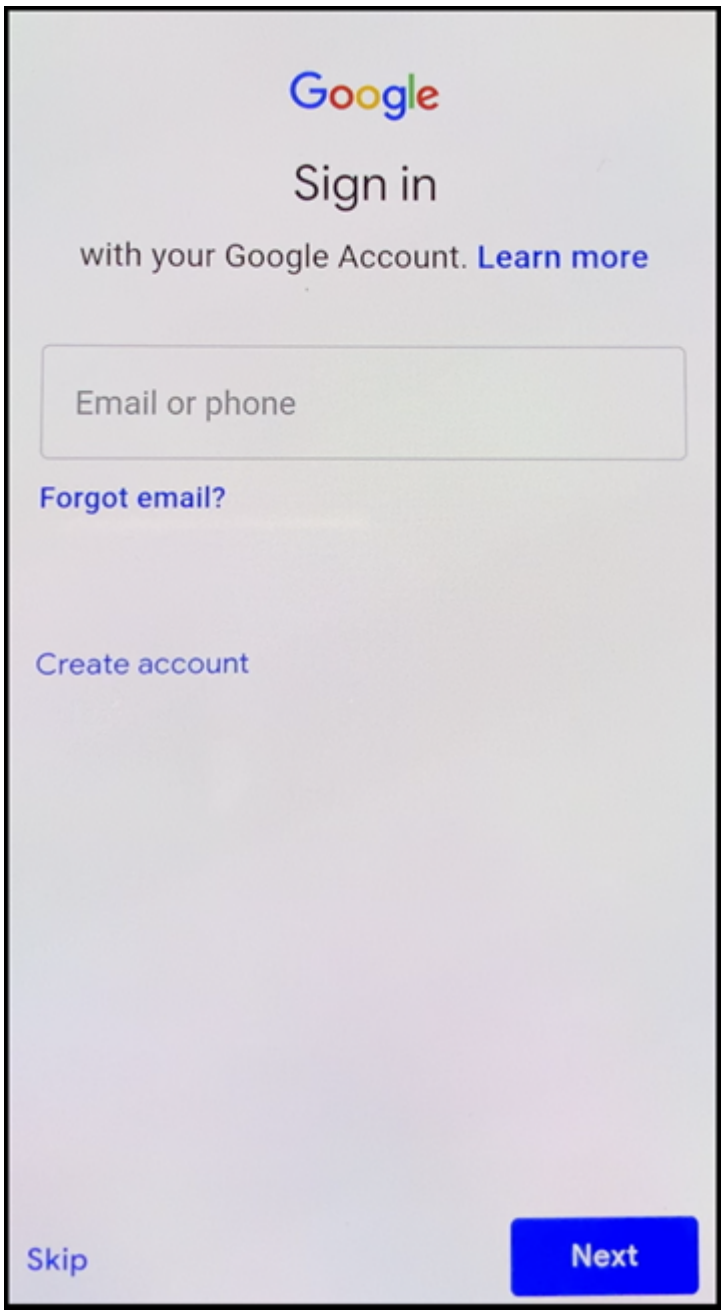
In this enrollment method is recommended for most customers because the latest version of Secure Hub is downloaded from the Google Play store. Unlike with other enrollment methods, you do not provide Secure Hub for download from the XenMobile Server.

System requirements

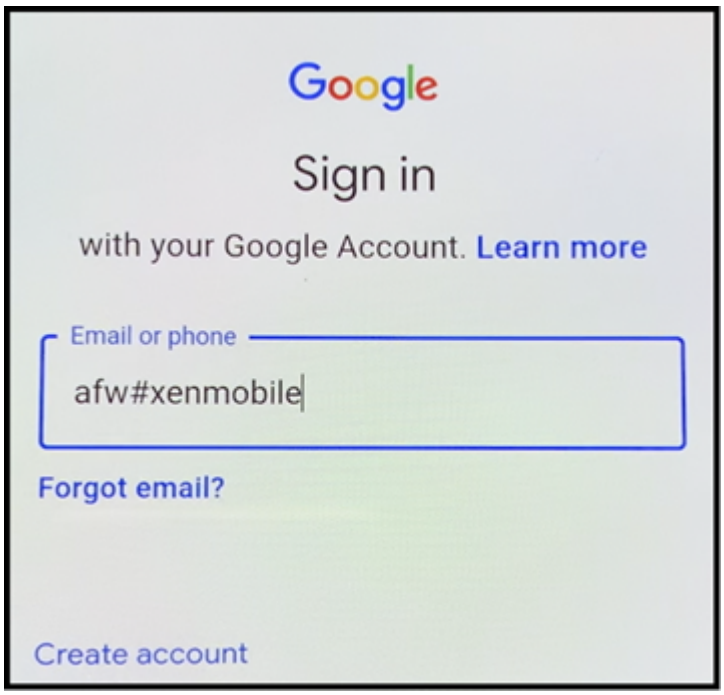
- Supported on all Android devices running the Android OS.

To enroll the device

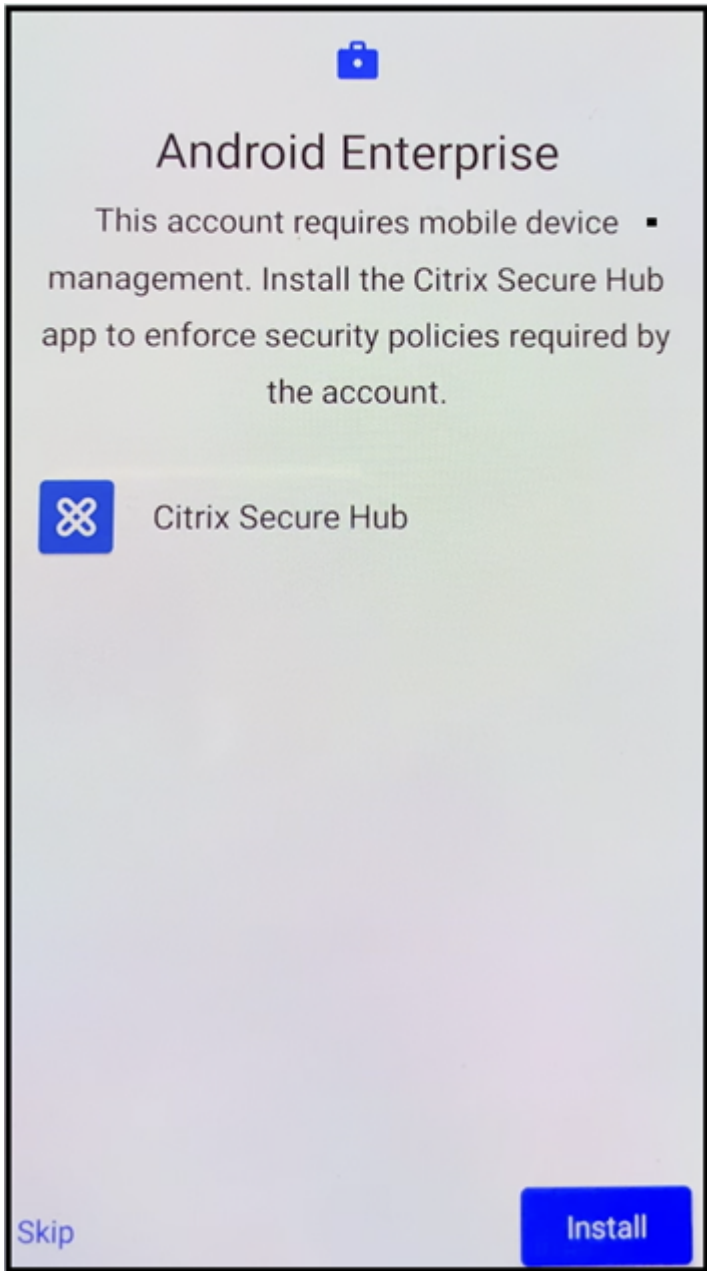
1. Power on a new or factory reset device.
2. The initial device setup loads and prompts for a Google account. If the device loads the home screen of the device, check the notification bar for a **Finish Setup** notification.



3. Enter `afw##xenmobile` in the **Email or phone** field.

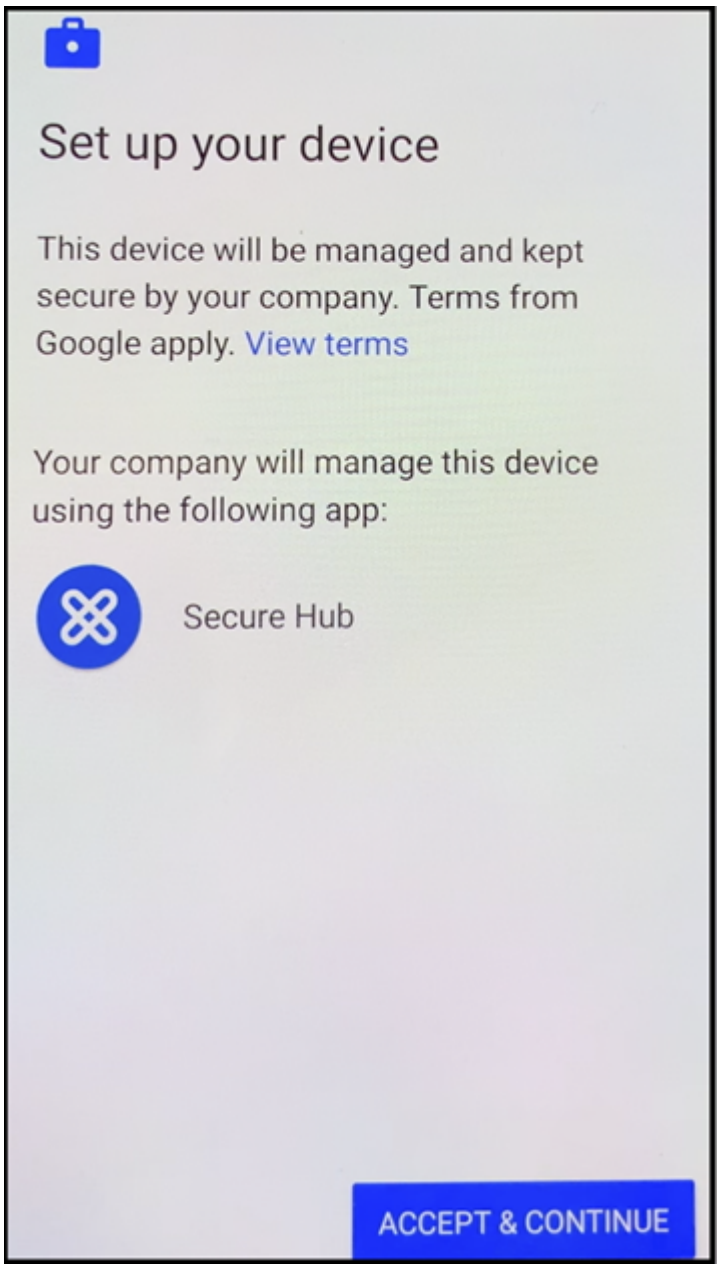


4. Tap **Install** on the Android Enterprise screen prompting to install Secure Hub.

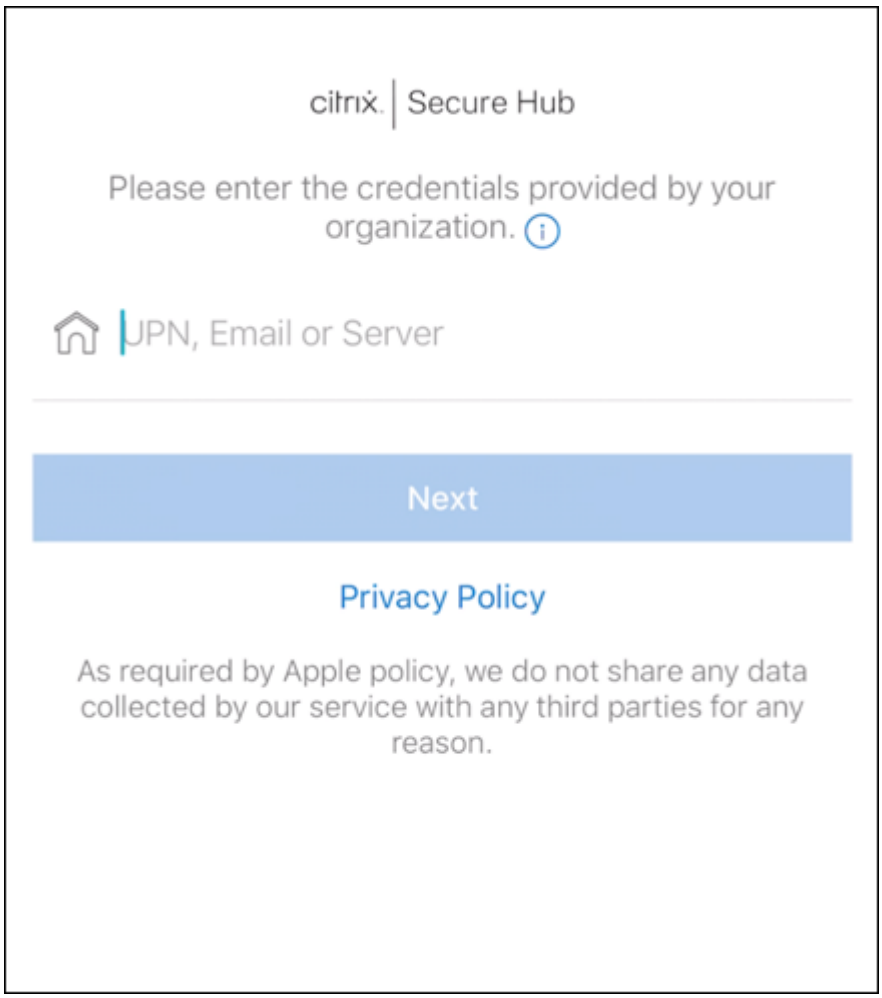


5. Tap **Install** on the Secure Hub installer screen.

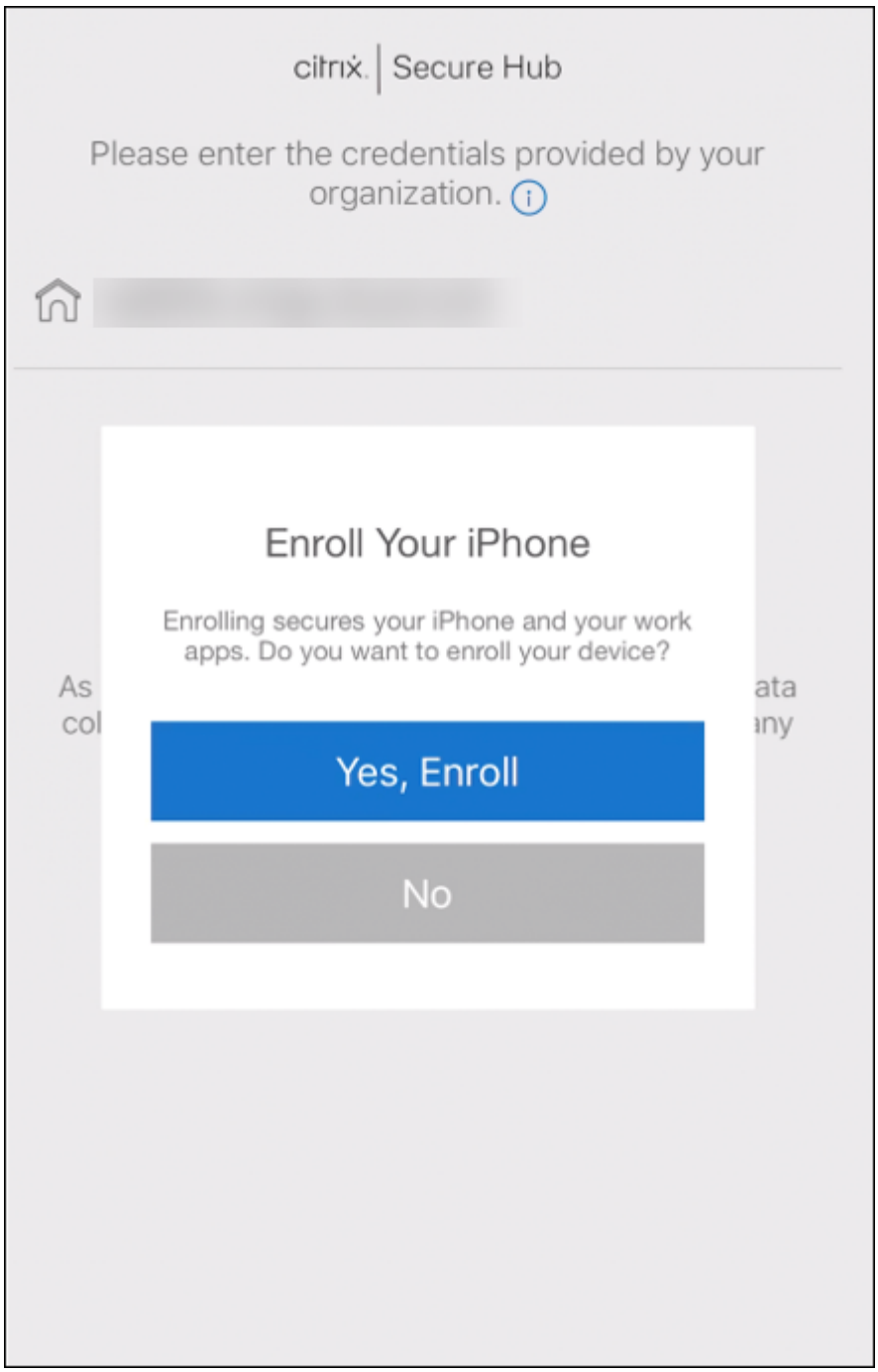
6. Tap **Allow** for all app permission requests.
7. Tap **Accept & Continue** to install Secure Hub and allow it to manage the device.



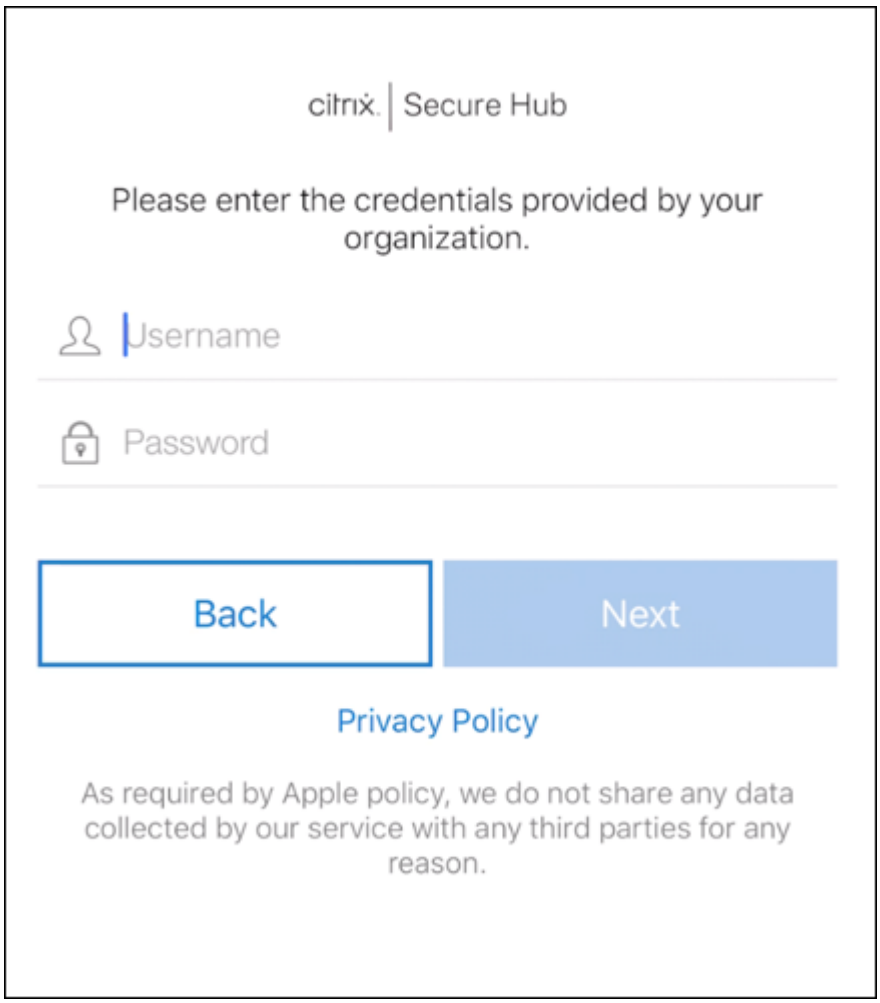
8. Secure Hub is now installed and on the default enrollment screen. In this example, AutoDiscovery is not set up. If it was, the user can enter their username/email and a server would be found for them. Instead, enter the enrollment URL for the environment and tap **Next**.



9. The default configuration for XenMobile allows users to choose if they use MAM or MDM+MAM. If prompted in this way, tap **Yes, Enroll** to choose MDM+MAM.

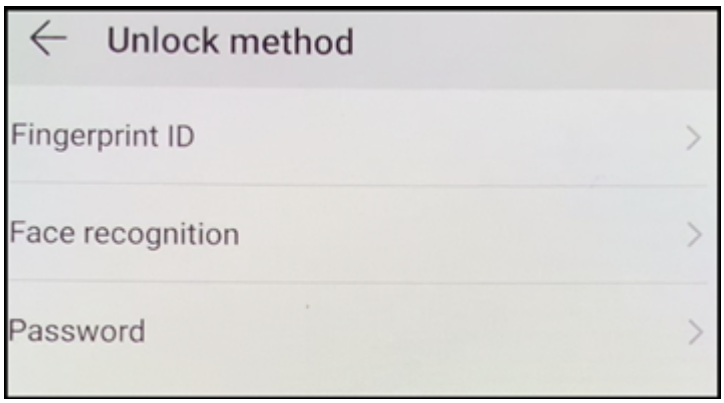


10. Enter the user name and password, then tap **Next**.

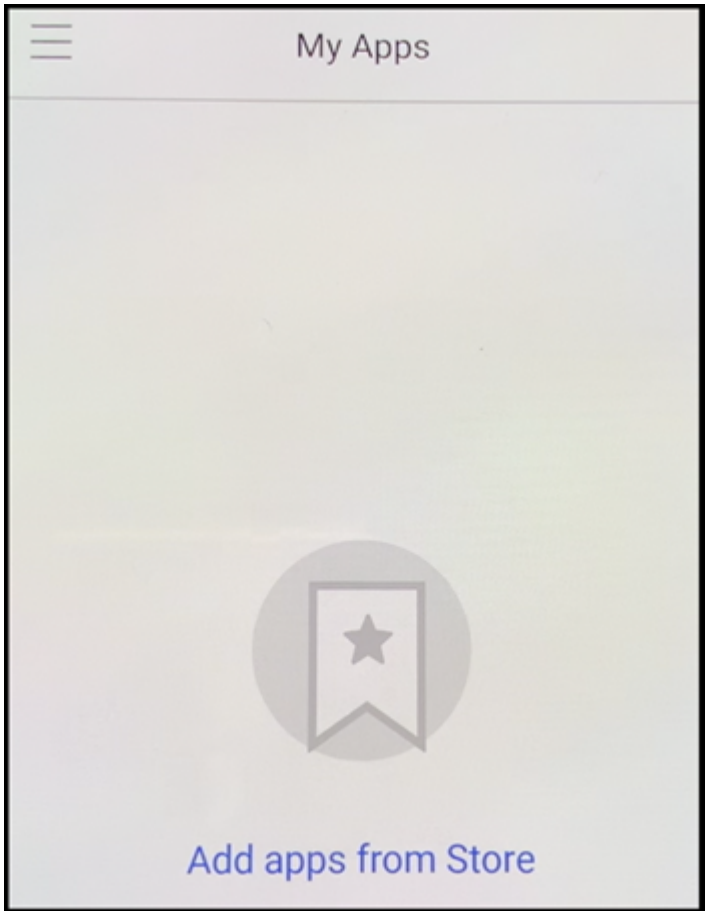


11. The user is prompted to configure a device passcode. Tap **Set** and enter a passcode.

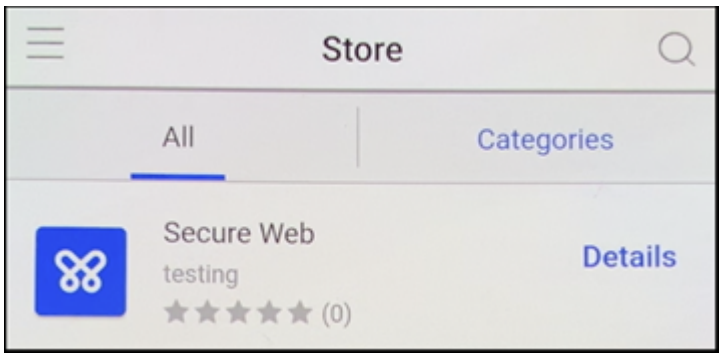
12. The user is prompted to configure a work profile unlock method. For this example, tap **Password**, tap **PIN**, and enter a PIN.



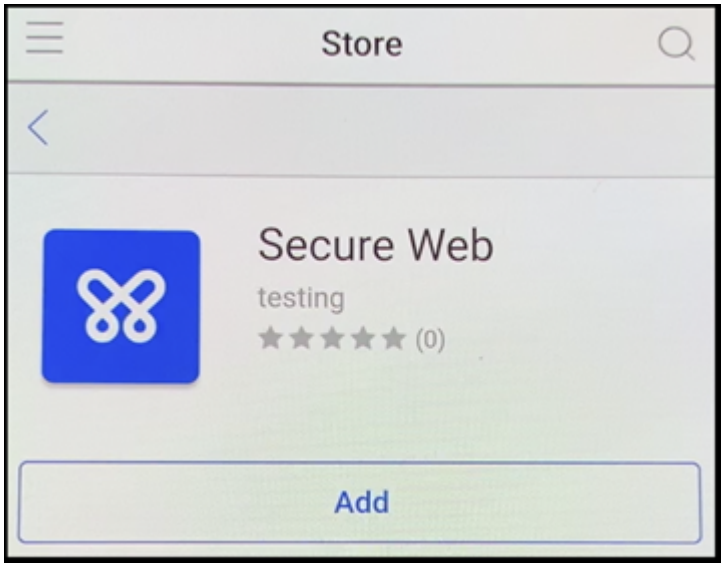
13. The device is now on the Secure Hub **My Apps** landing screen. Tap **Add apps from Store**.



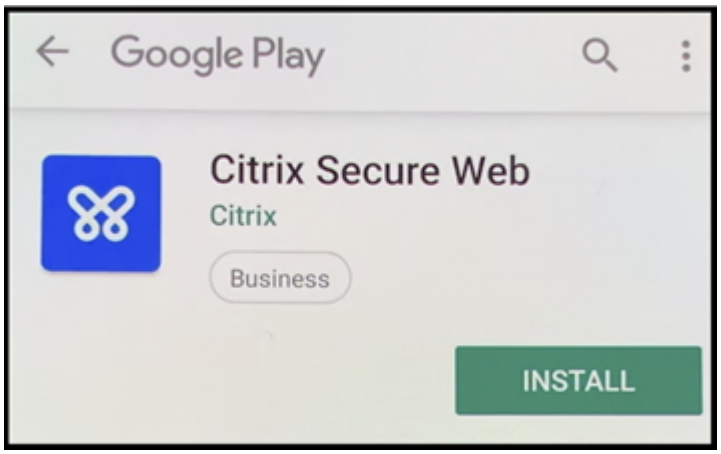
14. To add Secure Web, tap **Secure Web**.



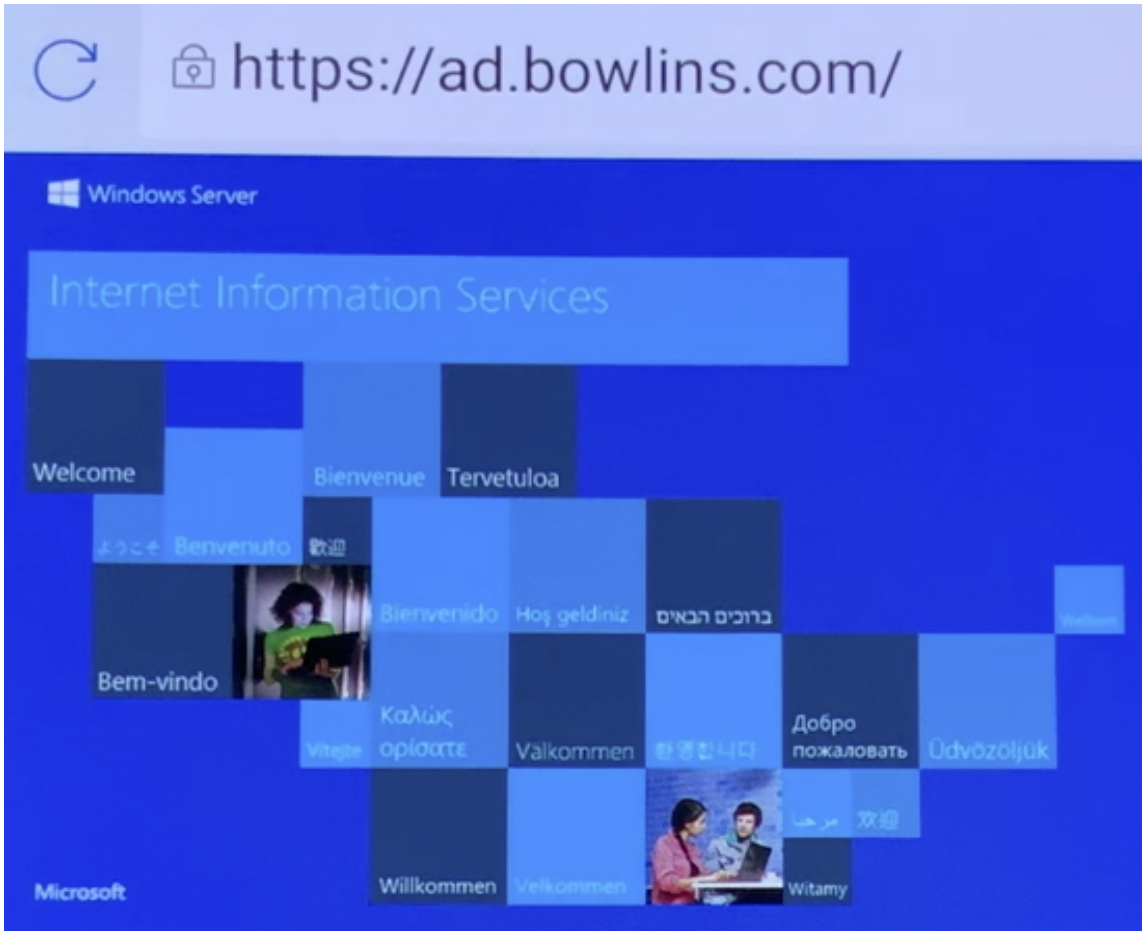
15. Tap **Add**.



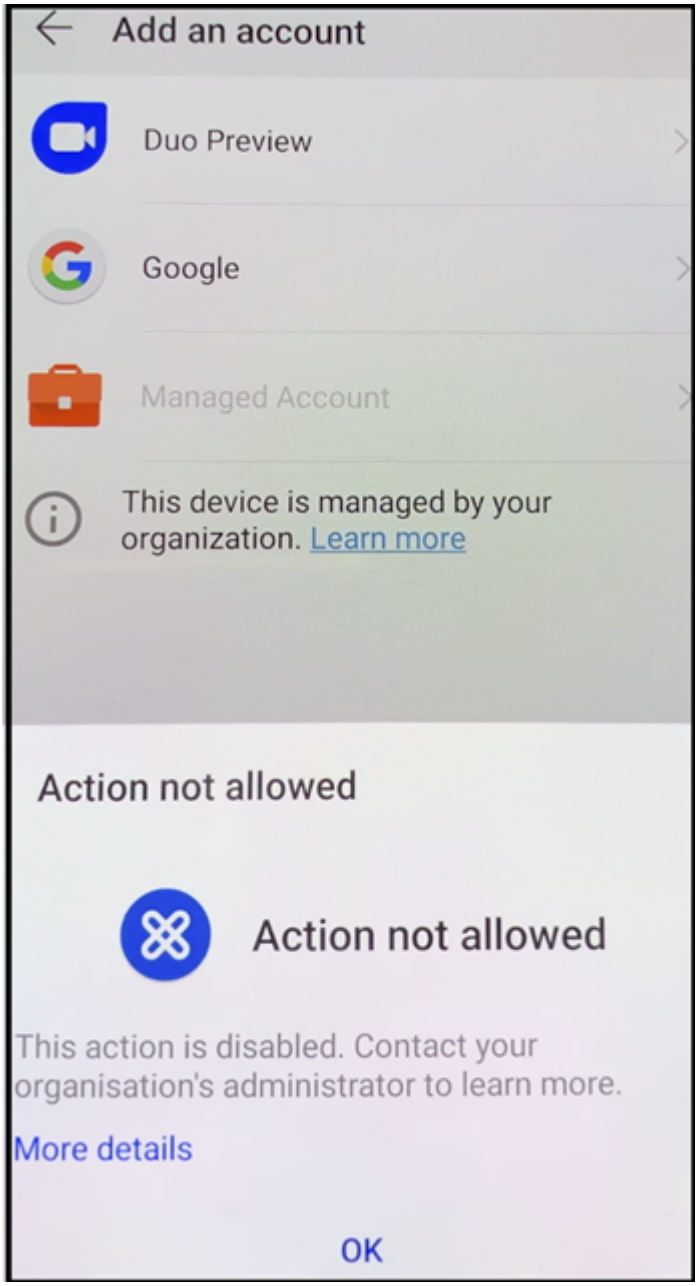
16. Secure Hub directs the user to the Google Play store to install Secure Web. Tap **Install**.



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 XenMobile Provisioning Tool.

System requirements and prerequisites

- Supported Android devices.

- 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 Secure Hub. Only one profile is allowed on each device. Attempting to add a second DPC app removes the installed Secure Hub.

Data transferred through the NFC bump

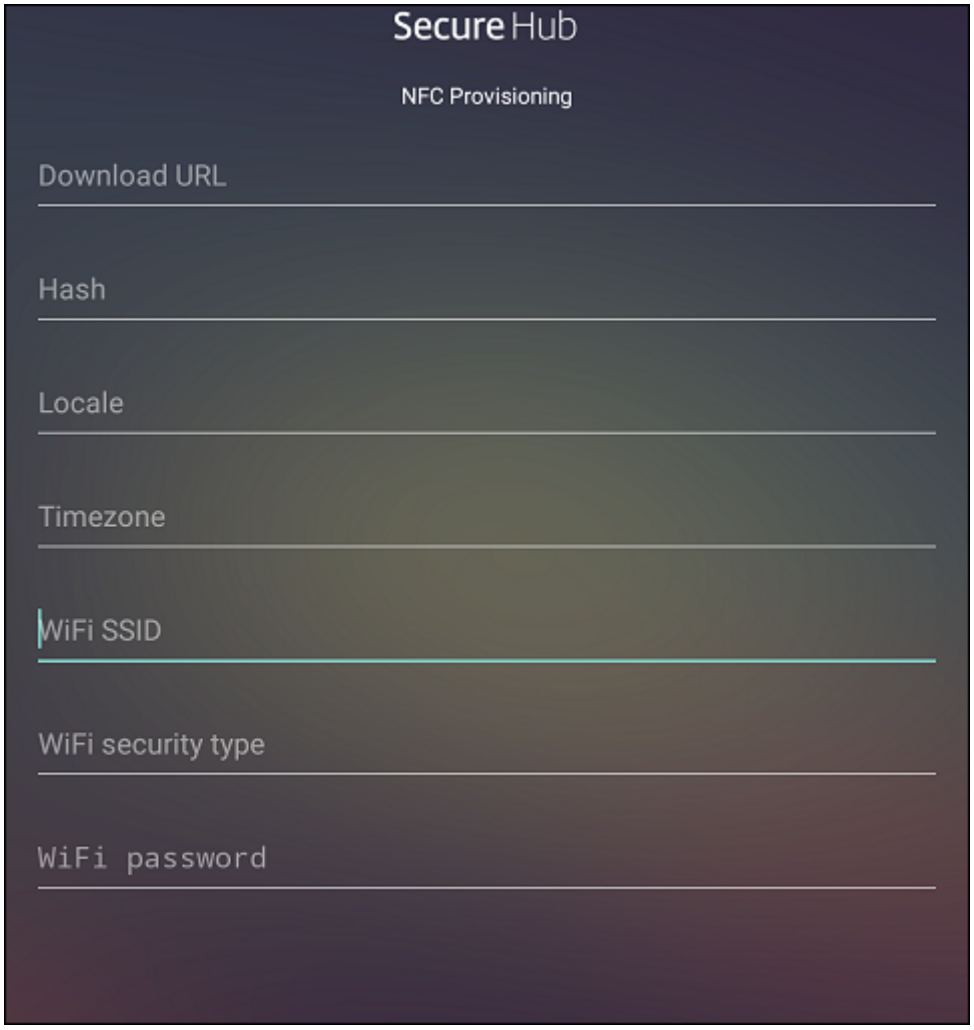
Provisioning a factory-reset device requires you to send the following data through an NFC bump to initialize Android Enterprise:

- 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.
- SHA1 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 XenMobile 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.



You can type data into the required fields or populate them using a 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=<SHA1 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 an Olson name of the form area/location. For example, America/Los_Angeles for Pacific time. If you don't enter a name, the time zone is automatically populated.

`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=ga50TwdCmfdJ72LGRFkke4Crb
\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=ga50TwdCmfdJ72LGRFkke4Crb
\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: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-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:

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if
    m{
 (?<=SHA-256 digest:) .* }
 '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->
```

   The command returns a valid checksum.

3. To generate the QR code, enter the checksum in the `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSU` field. For example:

```
{

  "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_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"
    }

 }

<!--NeedCopy-->
```

Libraries used

The Provisioning Tool uses the following libraries in its source code:

- v7 `appcompat` library, Design support library, and v7 Palette 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

To enroll a fully managed device 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.

System requirements

- Supported on all Android devices running Android 8.0 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 an Olson name of the form area/location. For example, America/Los_Angeles for Pacific time. If you don't enter one, the time zone is automatically populated.

- **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": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "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, such as https://www.qr-code-generator.com.

This QR code gets scanned by a factory-reset device to enroll the device 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 (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 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.

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 XenMobile. 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.

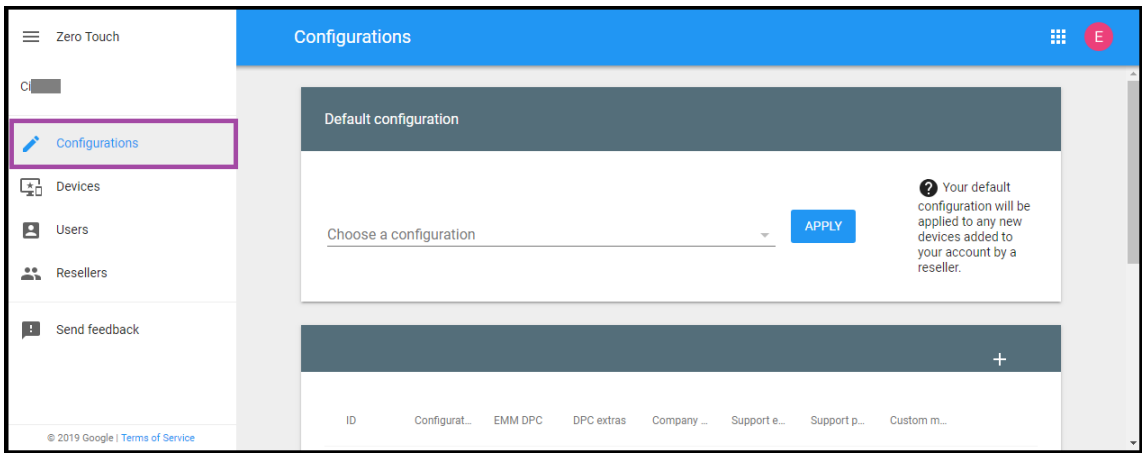
Use this JSON to configure the device to enroll on the XenMobile Server you specify. Substitute the URL of your server for 'URL' in this example.


```
1        {
2
3            "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6                "serverURL":"URL",
7            }
8
9         }
10
11 <!--NeedCopy-->
```

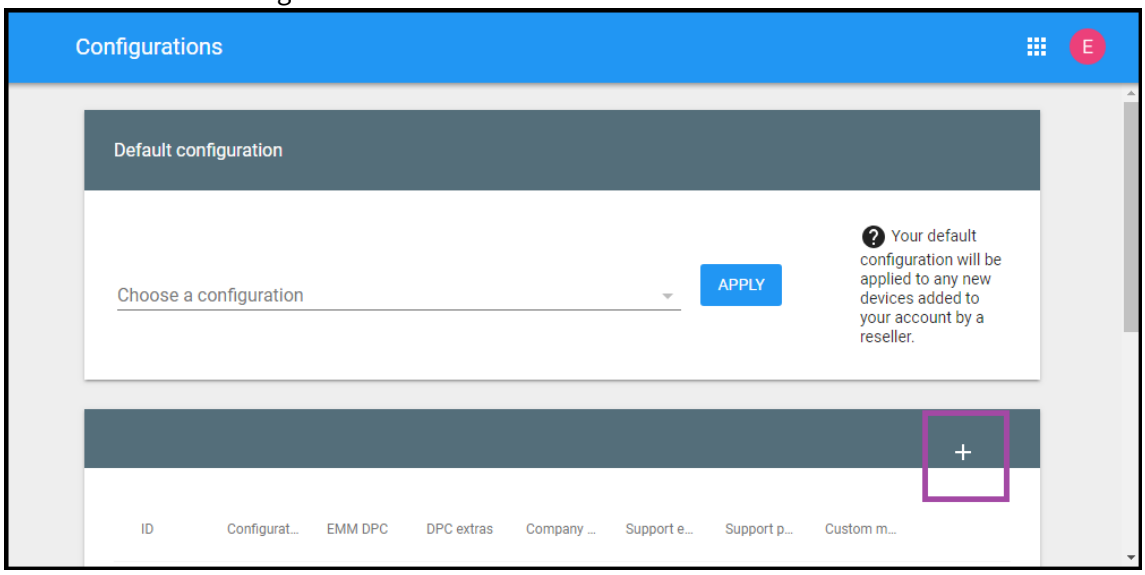
You can use an optional JSON with more parameters to further customize your configuration. This example specifies the XenMobile Server and the user name and password that devices using this configuration use to log on to the server.

```
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-->
```

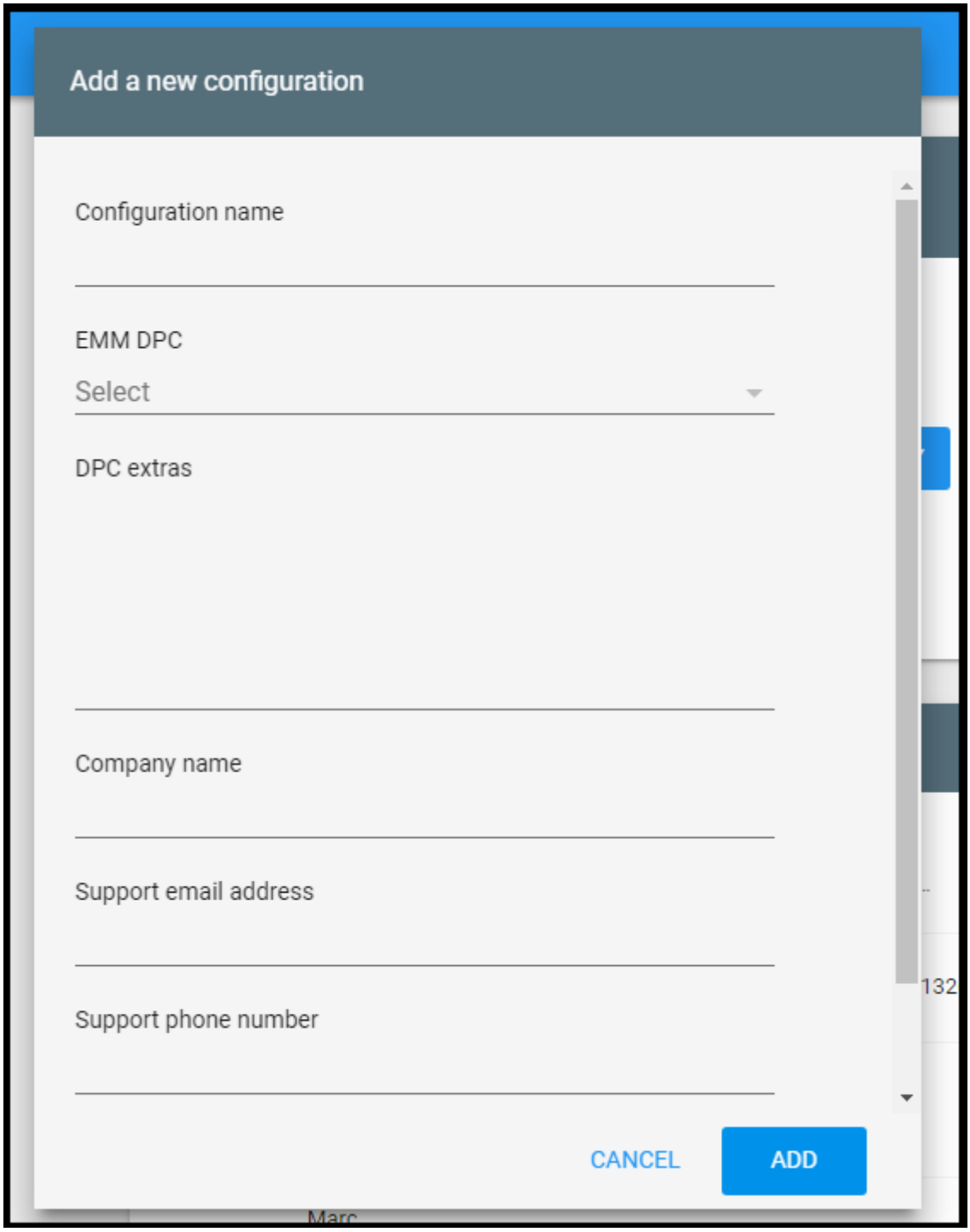
1. Go to the Android zero-touch portal at https://partner.android.com/zerotouch. Log in with the account information from your zero-touch device reseller.
2. Click **Configuration**.



3. Click **+** above the configuration table.



4. Enter your configuration information in the configuration window that appears.

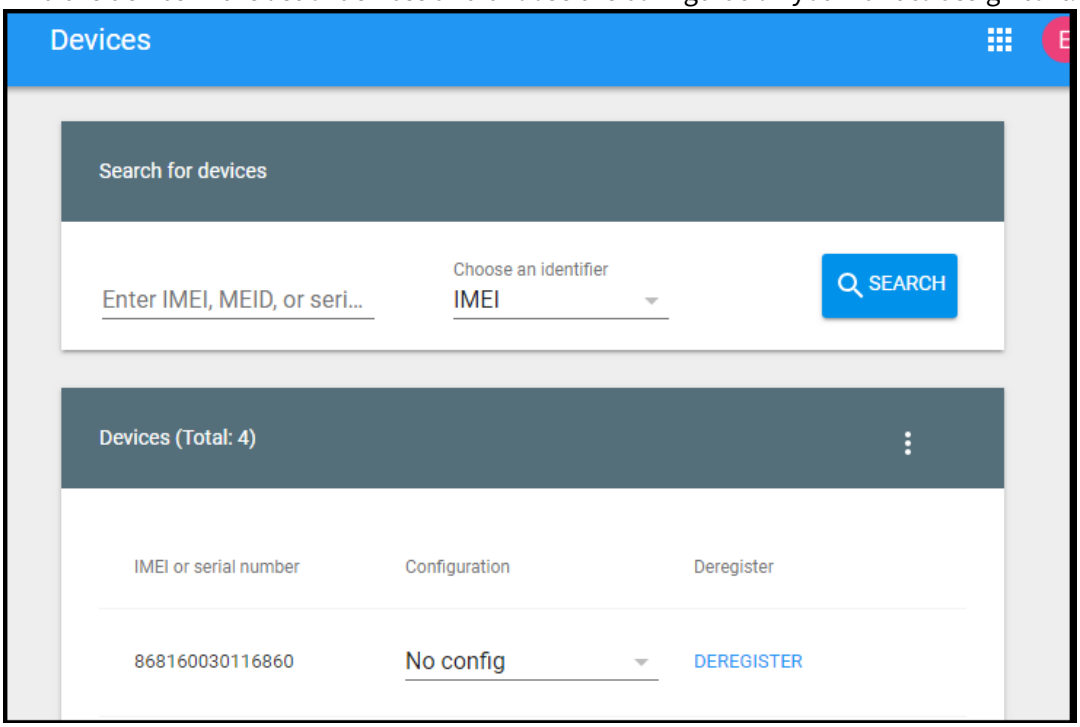


- **Configuration name:** Type the name you choose for this configuration.
- **EMM DPC:** Choose **Citrix Secure Hub**.
- **DPC extras:** Paste your custom JSON text in this field.
- **Company name:** Type the name you want to appear on your Android Enterprise zero-touch devices during device provisioning.
- **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:
   a) In the Android zero-touch portal, click **Devices**.
   b) 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. Dedicated devices are also known as corporate owned single use (COSU) devices. You restrict these devices to one app or 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 XenMobile administrators that you allow to enroll dedicated devices to your XenMobile deployment. See Creating enrollment profiles.
- Allow the apps you want the dedicated device to access.
- 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

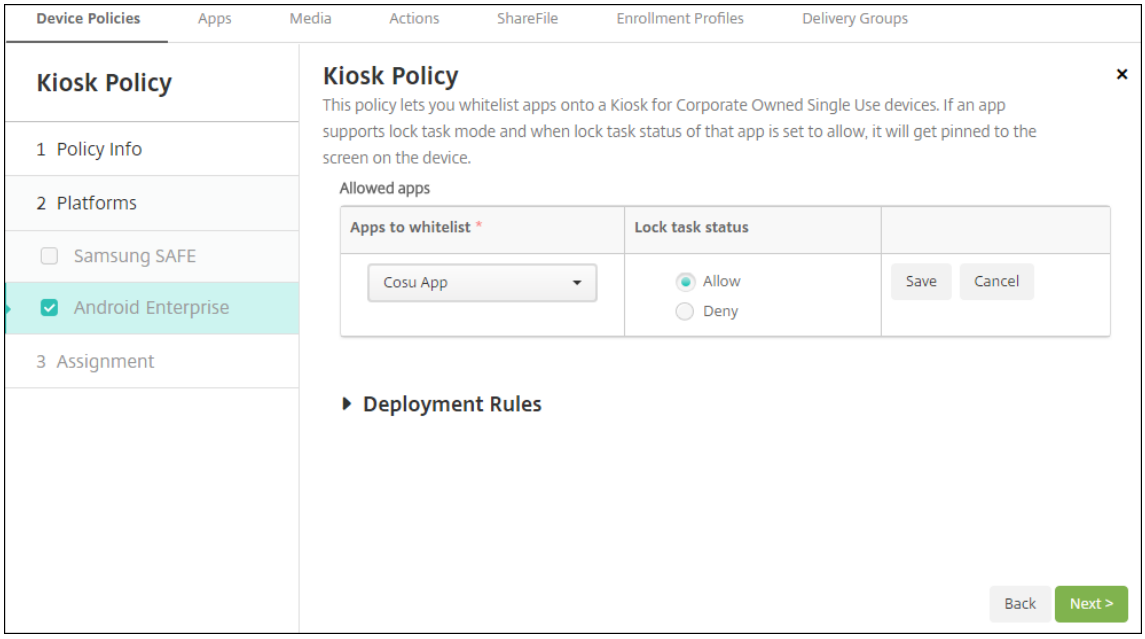
The Kiosk device policy lets you allow apps and set lock task mode. By default, Secure Hub and Google Play services are allowed.

To add the Kiosk policy:

1. In the XenMobile 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.

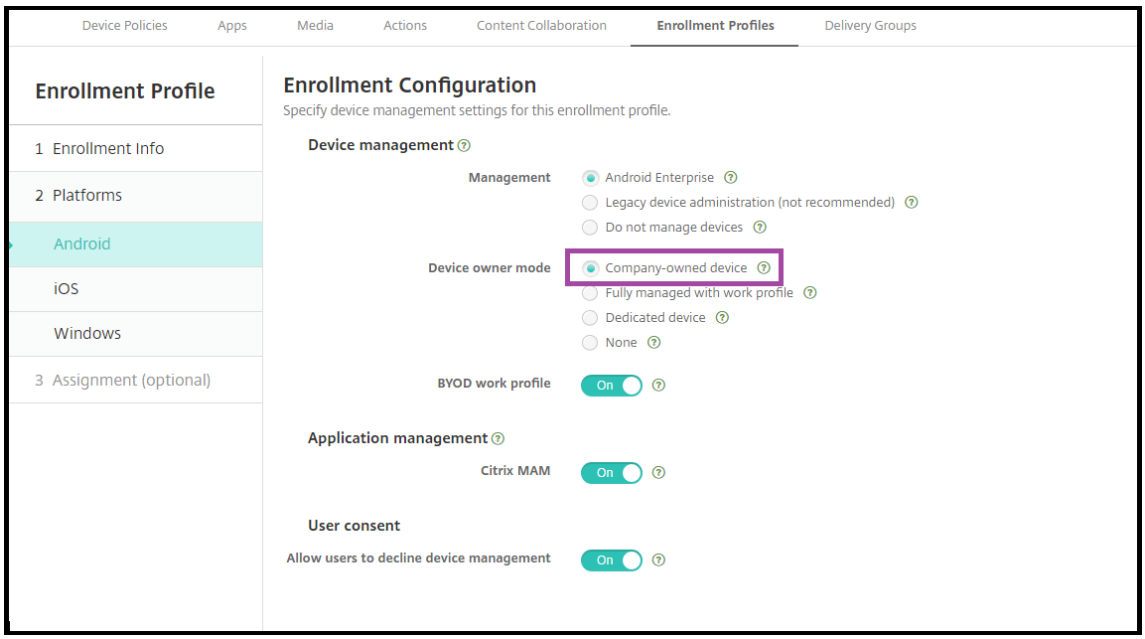
Choose **Allow** to set the app to be pinned to the device screen when the user starts the app. Choose **Deny** to set the app not to be pinned. Default is **Allow**.



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.

To enroll the device

1. Click **Next** or select **Android** under **Platforms**. The Enrollment Configuration page appears.
2. Set **Management** to **Android Enterprise**.
3. Set **Device owner mode** to **Company-owned device**.



4. Select **Assignment (options)**. The Delivery Group Assignment screen appears.
5. Choose the delivery group or delivery groups containing the administrators who enroll dedicated devices. Then click **Save**.

If you enabled **BYOD work profile** in the enrollment profile, devices that are not new or factory reset are enrolled as work profile devices. See Provisioning Android Enterprise work profile devices.

Provision Android Enterprise fully managed devices with a work profile (COPE devices)

Fully managed devices with a work profile, formerly called COPE devices, are company-owned devices that are used for both work and personal purposes. Your organization manages the entire devices. You can apply one set of policies to the device and a separate set of policies to the work profile.

In the XenMobile 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”.

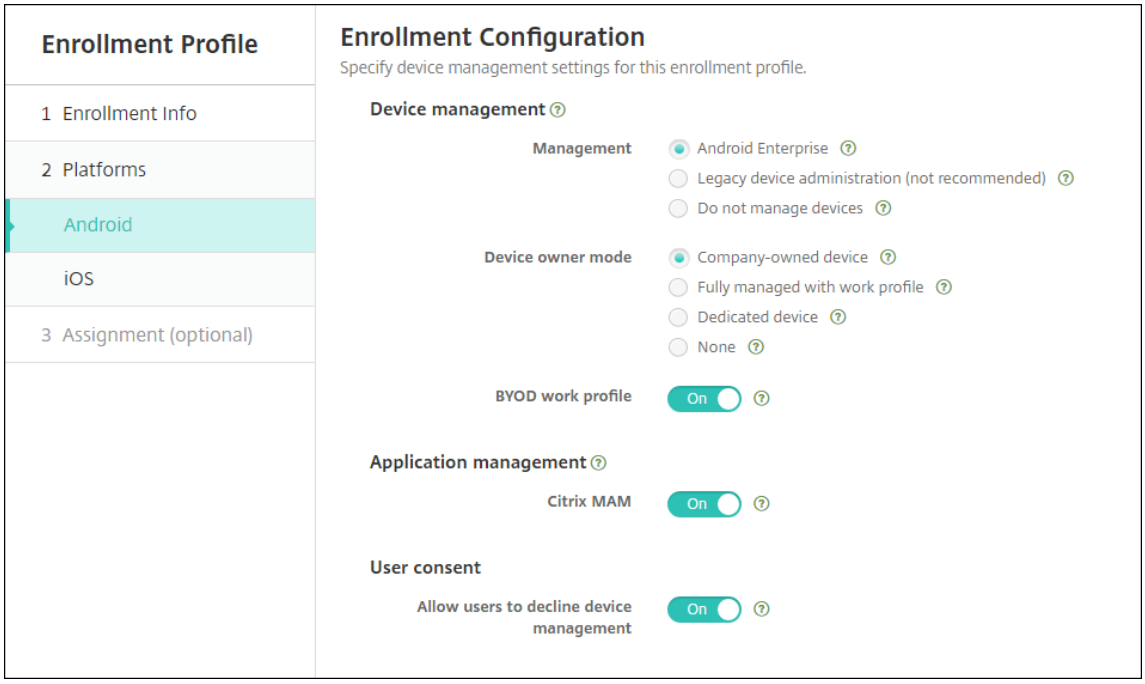
System requirements

- Support for enrolling fully managed devices with work profiles begins with Android 8.0.

Add an enrollment profile for fully managed devices with work profiles

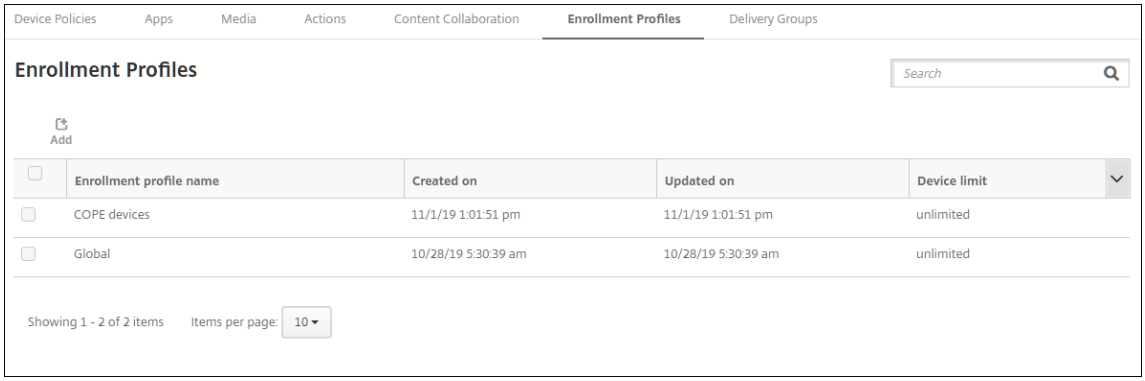
Create an enrollment profile for enrolling fully managed devices with work profiles. The administrators in the delivery groups assigned to this enrollment profile can enroll fully managed devices with work profiles. To ensure that these administrators can enroll all the devices required, create an enrollment profile for them with unlimited devices allowed per user. Assign this profile to a delivery group containing the administrators who enroll fully managed devices with work profiles.

1. In the XenMobile 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. Ensure that the number of devices that members with this profile can enroll is set to unlimited.
3. Click **Next** or select **Android Enterprise** under **Platforms**. The Enrollment Configuration page appears.
4. Set **Enrollment Type** to one of the following:
   - **Fully managed/Work profile:** New devices or factory reset devices enroll fully managed. BYOD devices enroll with only a work profile managed by you.
   - **COPE/Work profile:** New devices or factory reset devices enroll fully managed with a work profile. BYOD devices enroll with only a work profile managed by you.



5. Select **Assignment (optional)** or click **Next**. The Delivery Group Assignment screen appears.
6. 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.



If a user belongs to multiple delivery groups that have different enrollment profiles, the name of the delivery group determines the enrollment profile used. XenMobile selects the delivery group that appears last in an alphabetized list of delivery groups.

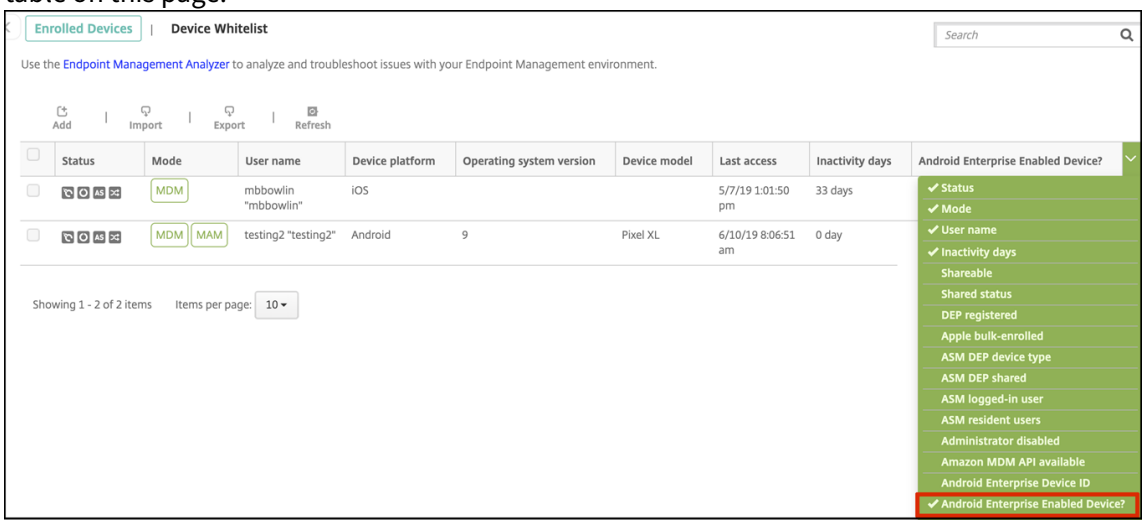
To enroll the device

New and factory reset devices enroll as fully managed devices with a work profile using the DPC identifier token, near field communication (NFC) bump, or QC code methods. See Enrolling devices using the Citrix DPC identifier token, Enrolling devices with NFC bump, or Enrolling devices using a QR code.

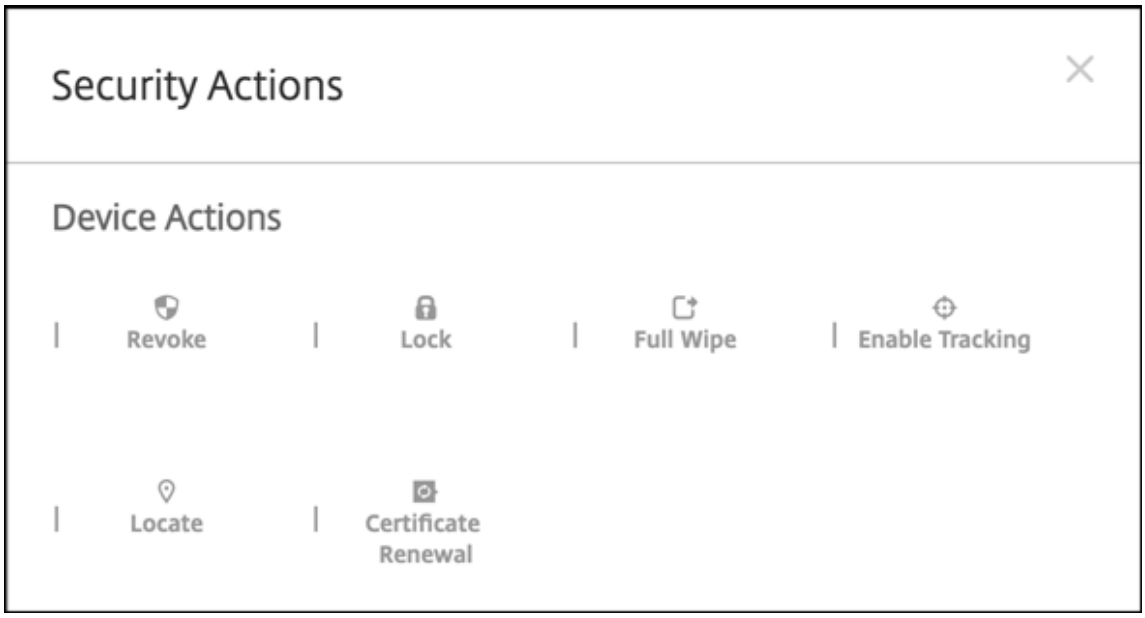
Devices that are not new or factory reset enroll as work profile devices as described in Provisioning Android Enterprise work profile devices.

Viewing Android Enterprise devices in the XenMobile console

1. In the XenMobile console, go to **Manage > Devices**.
2. Add the **Android enterprise Enabled Device?** column by clicking the menu on the right of the table on this page.



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 managed 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:

- **Data loss protection:** The XenMobile MAM container technology secures apps with encryption and other mobile Data Loss Prevention (DLP) technologies. Use the Citrix MAM SDK, MDX Service, or MDX Toolkit to MDX-enable apps.
- **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.

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.

Android Enterprise app permissions	Android Enterprise managed configurations	App Inventory
App Uninstall	Automatically update managed apps	Control OS Update
Credentials	Custom XML	Exchange
Files	Keyguard management	Kiosk
Location	Passcode	Restrictions
Samsung MDM license key	Scheduling	Wi-Fi
XenMobile options		

Device policies for fully managed devices with work profile (COPE devices)

For fully managed devices with work profiles (COPE devices), some device policies can be used 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.

Policy	Applies to
Android Enterprise app permissions	Work profile
Android Enterprise managed configurations	Work profile
App inventory	Work profile
App uninstall	Work profile
Automatically update managed apps	Work profile
Control OS update	N/A
Credentials	Work profile
Custom XML	N/A
Exchange	N/A

Policy	Applies to
Files	Work profile
Keyguard management	Device and work profile
Kiosk	N/A
Location	Device (location mode only)
Passcode	Device and work profile
Restrictions	Device and work profile (create separate policies for the device and the work profile)
Samsung MDM license key	N/A
Scheduling	Work profile
Wi-Fi	Device
XenMobile options	Work profile

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	No	Yes
Locate	Yes	Yes
Lock	Yes	Yes
Lock and Reset Password	No	Yes
Notify (Ring)	Yes	Yes
Revoke	Yes	Yes
Selective Wipe	Yes	No

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.
- On fully managed devices with work profiles (COPE devices):
  - You can apply the Lock security action separately to the device or the work profile

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 XenMobile console.

After the Android Enterprise enterprise is unenrolled:

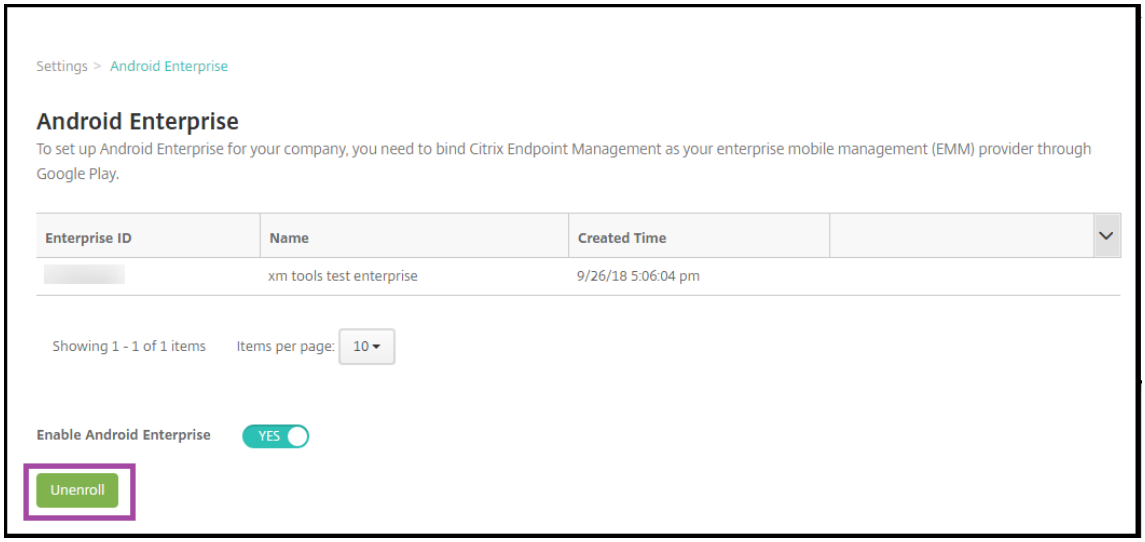
- Devices and users enrolled through the enterprise have the Android Enterprise apps reset to their default state. Android Enterprise Managed Configurations policies previously applied no longer affect operations.
- XenMobile manages devices enrolled through the enterprise. From the perspective of Google, those devices are unmanaged. You can't add new Android Enterprise apps. You can't apply Android Enterprise 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 XenMobile Server console and XenMobile Tools.

When you perform this task, XenMobile opens a popup window for XenMobile Tools. Before you begin, ensure that XenMobile 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 XenMobile site to the popup block allow list.

To unenroll an Android Enterprise enterprise:

1. In the XenMobile 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**.



amp; if m{(?<=SHA-256 digest:) .*}' | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->

The command returns a valid checksum.

To generate the QR code, enter the checksum in the `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM` field. For example:

```
{

  "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_ADMIN_EXTRAS_BUNDLE": {

```



```
        "serverURL": "https://supportablility.xm.cloud.com"
      }

  }

<!--NeedCopy-->
```

Libraries used

The Provisioning Tool uses the following libraries in its source code:

- v7 `appcompat` library, Design support library, and v7 Palette 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

To enroll a fully managed device 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.

System requirements

- Supported on all Android devices running Android 8.0 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 an Olson name of the form area/location. For example, America/Los_Angeles for Pacific time. If you don't enter one, the time zone is automatically populated.

- **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": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "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, such as https://www.qr-code-generator.com.

This QR code gets scanned by a factory-reset device to enroll the device 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 (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 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.

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 XenMobile. 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 XenMobile Server you specify. Substitute the URL of your server for 'URL' in this example.

```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
  {

        "serverURL":"URL",
    }

 }
```

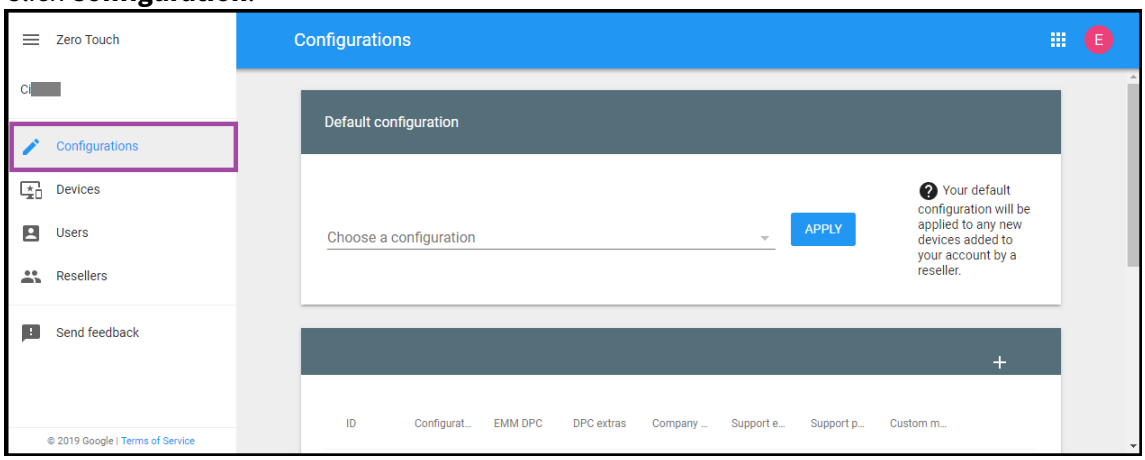


```
10
11  <!--NeedCopy-->
```

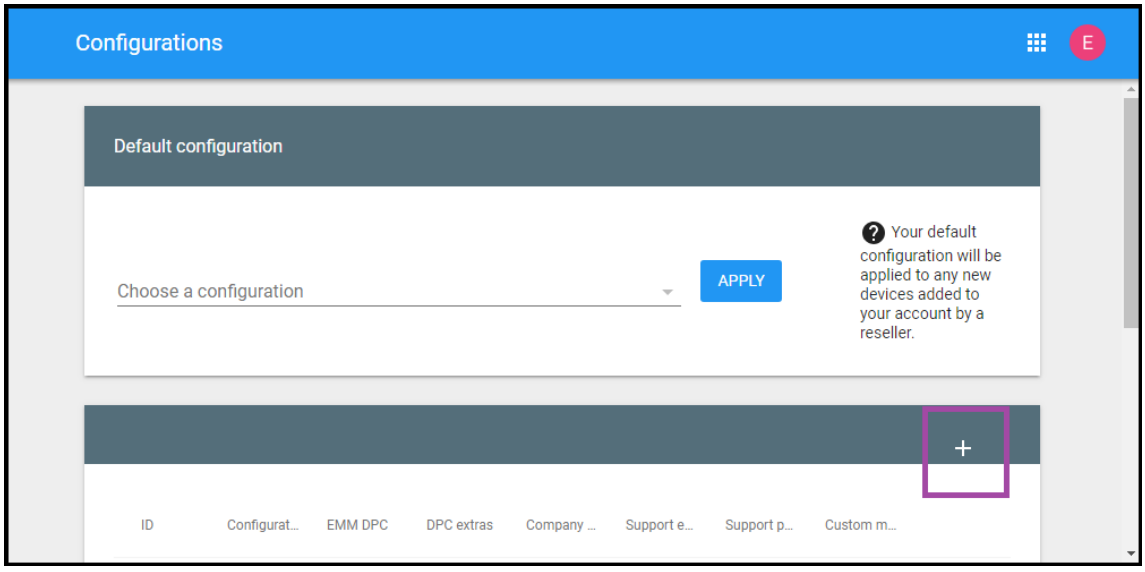
You can use an optional JSON with more parameters to further customize your configuration. This example specifies the XenMobile Server and the user name and password that devices using this configuration use to log on to the server.

```
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-->
```

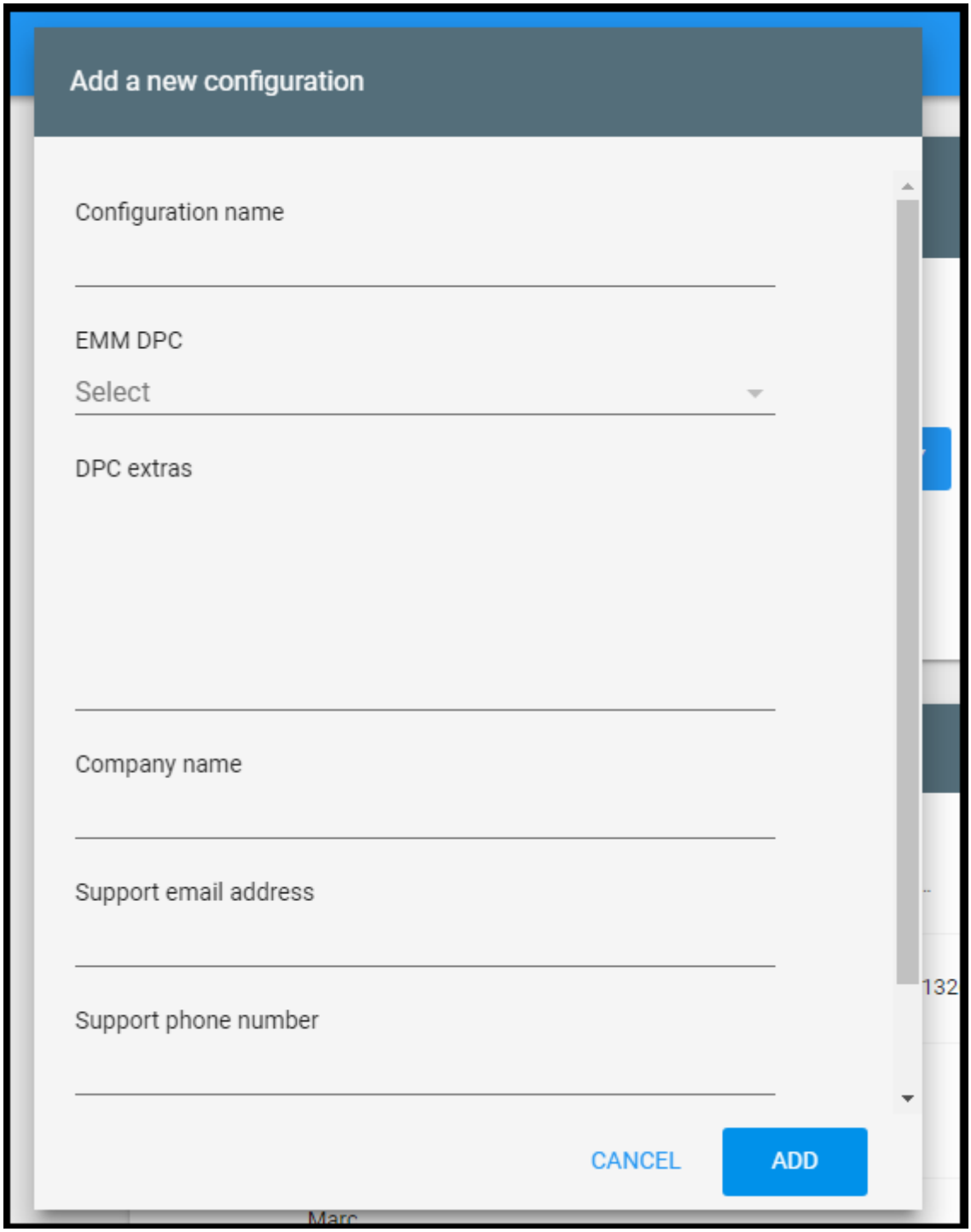
1. Go to the Android zero-touch portal at https://partner.android.com/zerotouch. Log in with the account information from your zero-touch device reseller.
2. Click **Configuration**.



3. Click **+** above the configuration table.



4. Enter your configuration information in the configuration window that appears.

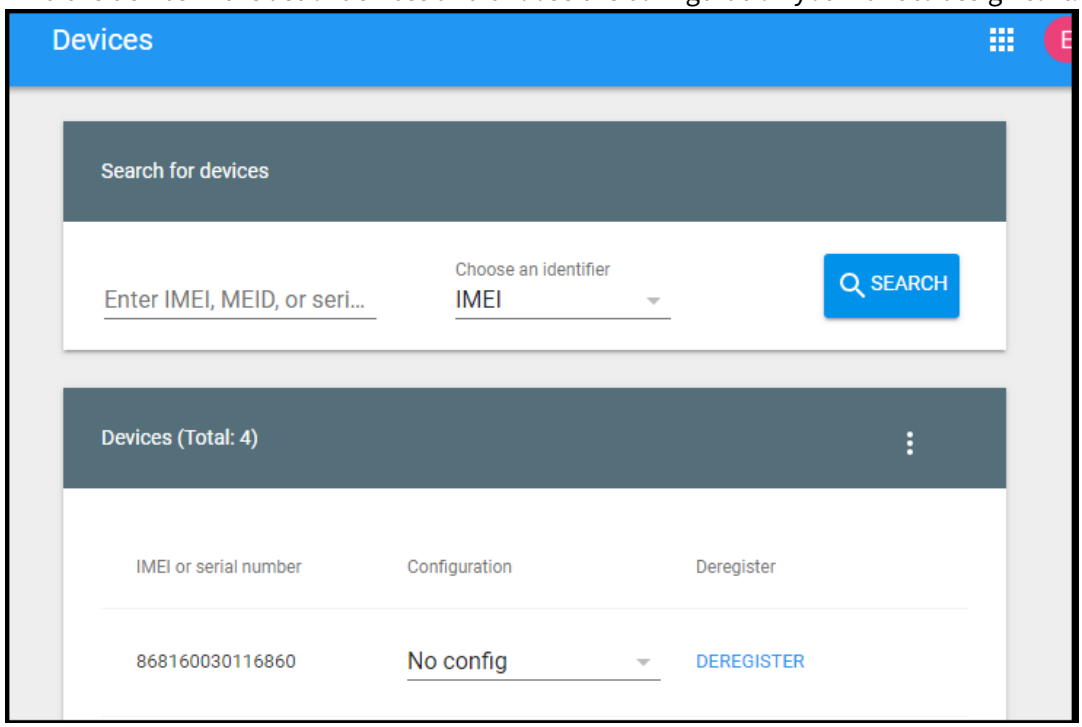


- **Configuration name:** Type the name you choose for this configuration.
- **EMM DPC:** Choose **Citrix Secure Hub**.
- **DPC extras:** Paste your custom JSON text in this field.
- **Company name:** Type the name you want to appear on your Android Enterprise zero-touch devices during device provisioning.
- **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:
   a) In the Android zero-touch portal, click **Devices**.
   b) 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. Dedicated devices are also known as corporate owned single use (COSU) devices. You restrict these devices to one app or 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 XenMobile administrators that you allow to enroll dedicated devices to your XenMobile deployment. See Creating enrollment profiles.
- Allow the apps you want the dedicated device to access.
- 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

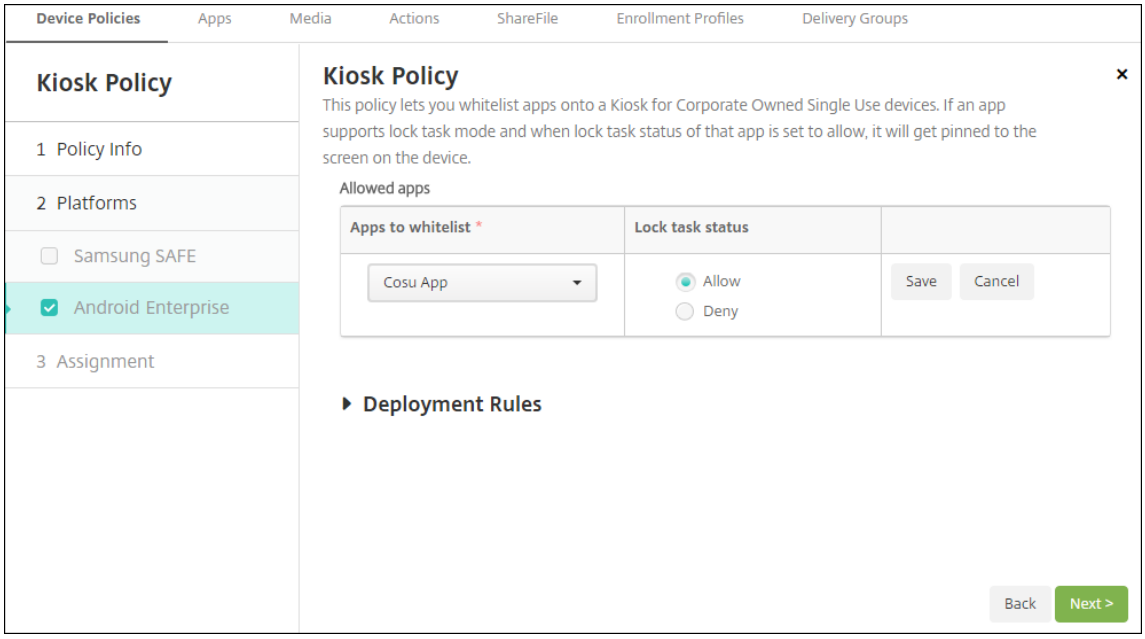
The Kiosk device policy lets you allow apps and set lock task mode. By default, Secure Hub and Google Play services are allowed.

To add the Kiosk policy:

1. In the XenMobile 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.

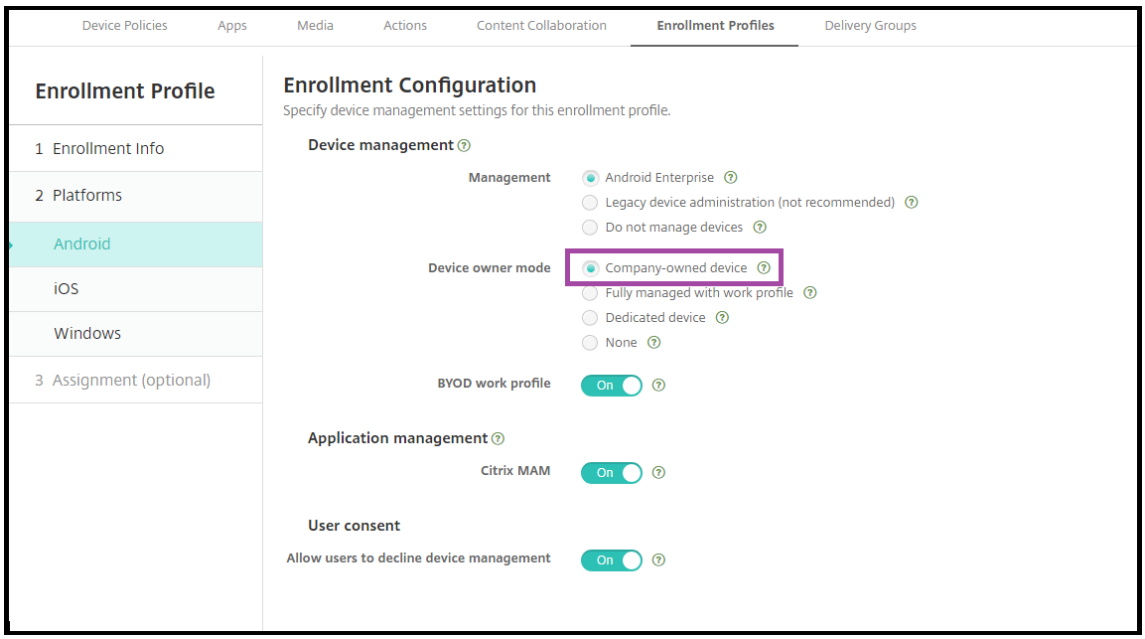
Choose **Allow** to set the app to be pinned to the device screen when the user starts the app. Choose **Deny** to set the app not to be pinned. Default is **Allow**.



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.

To enroll the device

1. Click **Next** or select **Android** under **Platforms**. The Enrollment Configuration page appears.
2. Set **Management** to **Android Enterprise**.
3. Set **Device owner mode** to **Company-owned device**.



4. Select **Assignment (options)**. The Delivery Group Assignment screen appears.
5. Choose the delivery group or delivery groups containing the administrators who enroll dedicated devices. Then click **Save**.

If you enabled **BYOD work profile** in the enrollment profile, devices that are not new or factory reset are enrolled as work profile devices. See Provisioning Android Enterprise work profile devices.

Provision Android Enterprise fully managed devices with a work profile (COPE devices)

Fully managed devices with a work profile, formerly called COPE devices, are company-owned devices that are used for both work and personal purposes. Your organization manages the entire devices. You can apply one set of policies to the device and a separate set of policies to the work profile.

In the XenMobile 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”.

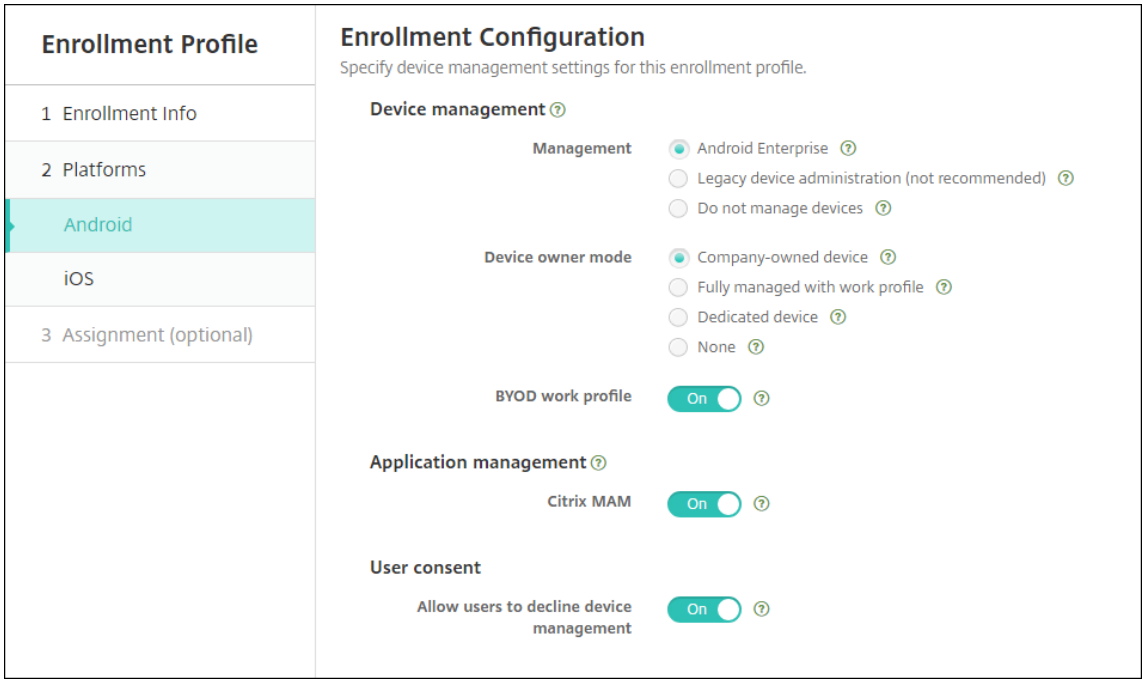
System requirements

- Support for enrolling fully managed devices with work profiles begins with Android 8.0.

Add an enrollment profile for fully managed devices with work profiles

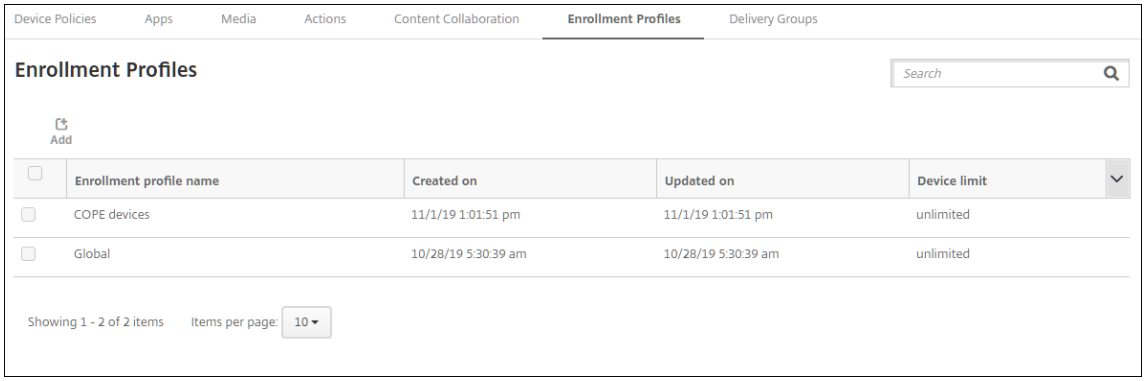
Create an enrollment profile for enrolling fully managed devices with work profiles. The administrators in the delivery groups assigned to this enrollment profile can enroll fully managed devices with work profiles. To ensure that these administrators can enroll all the devices required, create an enrollment profile for them with unlimited devices allowed per user. Assign this profile to a delivery group containing the administrators who enroll fully managed devices with work profiles.

1. In the XenMobile 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. Ensure that the number of devices that members with this profile can enroll is set to unlimited.
3. Click **Next** or select **Android Enterprise** under **Platforms**. The Enrollment Configuration page appears.
4. Set **Enrollment Type** to one of the following:
   - **Fully managed/Work profile:** New devices or factory reset devices enroll fully managed. BYOD devices enroll with only a work profile managed by you.
   - **COPE/Work profile:** New devices or factory reset devices enroll fully managed with a work profile. BYOD devices enroll with only a work profile managed by you.



5. Select **Assignment (optional)** or click **Next**. The Delivery Group Assignment screen appears.
6. 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.



If a user belongs to multiple delivery groups that have different enrollment profiles, the name of the delivery group determines the enrollment profile used. XenMobile selects the delivery group that appears last in an alphabetized list of delivery groups.

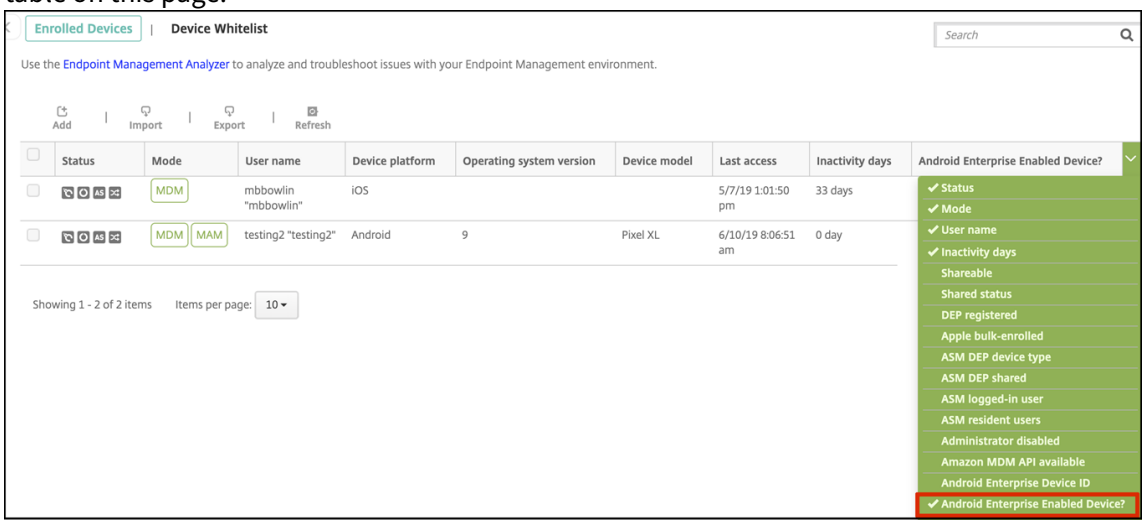
To enroll the device

New and factory reset devices enroll as fully managed devices with a work profile using the DPC identifier token, near field communication (NFC) bump, or QC code methods. See Enrolling devices using the Citrix DPC identifier token, Enrolling devices with NFC bump, or Enrolling devices using a QR code.

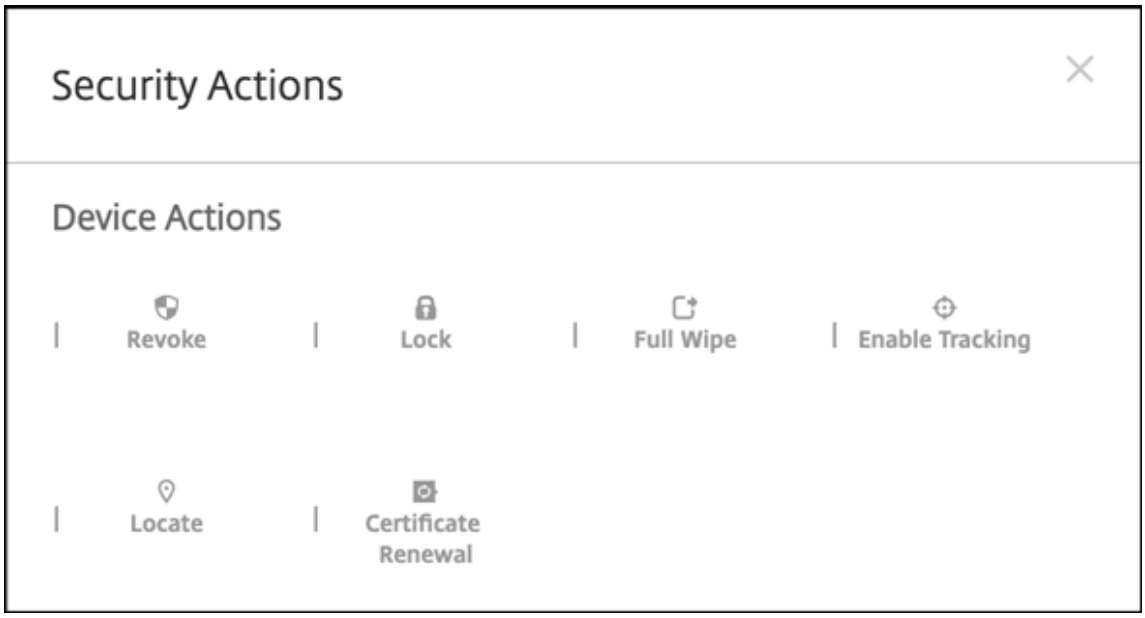
Devices that are not new or factory reset enroll as work profile devices as described in Provisioning Android Enterprise work profile devices.

Viewing Android Enterprise devices in the XenMobile console

1. In the XenMobile console, go to **Manage > Devices**.
2. Add the **Android enterprise Enabled Device?** column by clicking the menu on the right of the table on this page.



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 managed 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:

- **Data loss protection:** The XenMobile MAM container technology secures apps with encryption and other mobile Data Loss Prevention (DLP) technologies. Use the Citrix MAM SDK, MDX Service, or MDX Toolkit to MDX-enable apps.
- **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.

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.

Android Enterprise app permissions	Android Enterprise managed configurations	App Inventory
App Uninstall	Automatically update managed apps	Control OS Update
Credentials	Custom XML	Exchange
Files	Keyguard management	Kiosk
Location	Passcode	Restrictions
Samsung MDM license key	Scheduling	Wi-Fi
XenMobile options		

Device policies for fully managed devices with work profile (COPE devices)

For fully managed devices with work profiles (COPE devices), some device policies can be used 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.

Policy	Applies to
Android Enterprise app permissions	Work profile
Android Enterprise managed configurations	Work profile
App inventory	Work profile
App uninstall	Work profile
Automatically update managed apps	Work profile
Control OS update	N/A
Credentials	Work profile
Custom XML	N/A
Exchange	N/A

Policy	Applies to
Files	Work profile
Keyguard management	Device and work profile
Kiosk	N/A
Location	Device (location mode only)
Passcode	Device and work profile
Restrictions	Device and work profile (create separate policies for the device and the work profile)
Samsung MDM license key	N/A
Scheduling	Work profile
Wi-Fi	Device
XenMobile options	Work profile

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	No	Yes
Locate	Yes	Yes
Lock	Yes	Yes
Lock and Reset Password	No	Yes
Notify (Ring)	Yes	Yes
Revoke	Yes	Yes
Selective Wipe	Yes	No

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.
- On fully managed devices with work profiles (COPE devices):
  - You can apply the Lock security action separately to the device or the work profile

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 XenMobile console.

After the Android Enterprise enterprise is unenrolled:

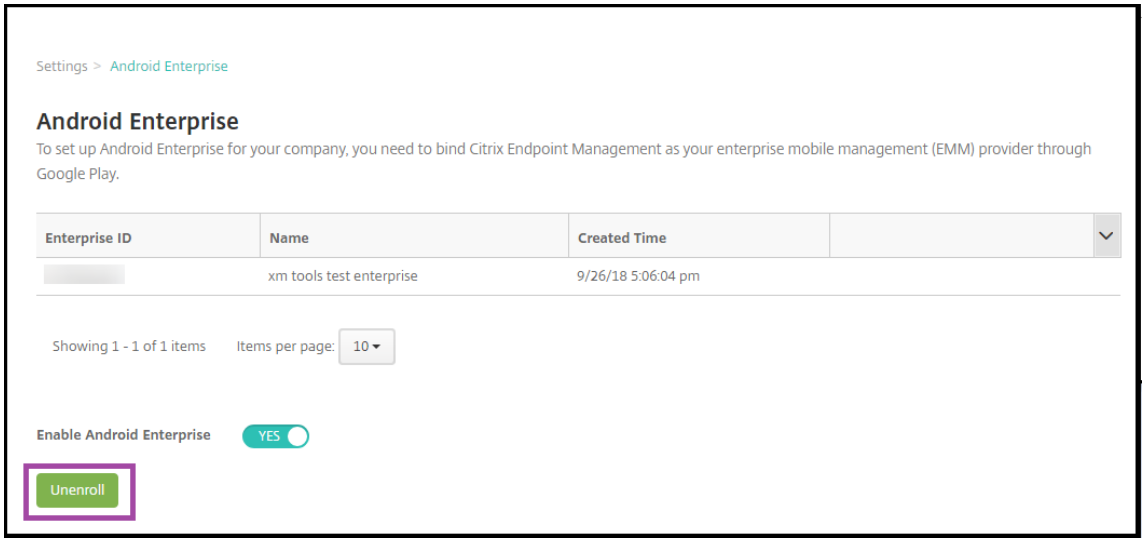
- Devices and users enrolled through the enterprise have the Android Enterprise apps reset to their default state. Android Enterprise Managed Configurations policies previously applied no longer affect operations.
- XenMobile manages devices enrolled through the enterprise. From the perspective of Google, those devices are unmanaged. You can't add new Android Enterprise apps. You can't apply Android Enterprise 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 XenMobile Server console and XenMobile Tools.

When you perform this task, XenMobile opens a popup window for XenMobile Tools. Before you begin, ensure that XenMobile 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 XenMobile site to the popup block allow list.

To unenroll an Android Enterprise enterprise:

1. In the XenMobile 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**.



Distribute Android Enterprise apps

April 1, 2021

XenMobile manages apps deployed to devices. You can organize and deploy the following types of Android Enterprise 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 XenMobile console as enterprise apps, as described in the 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 XenMobile 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 XenMobile console, the ownership of the apps differs. 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 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

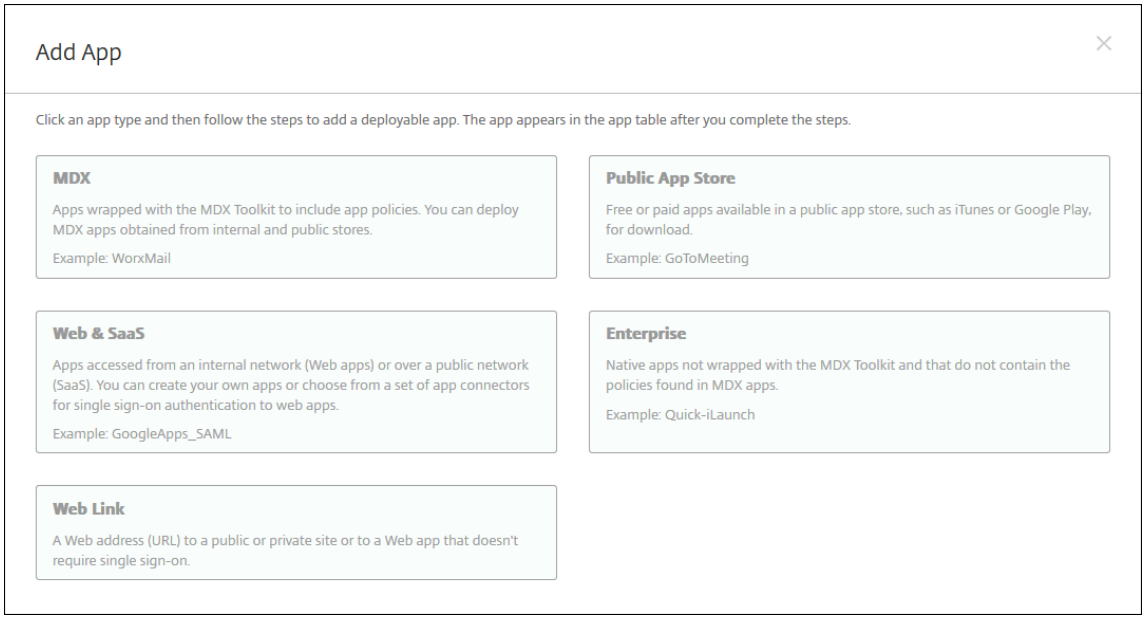
Managed app store apps

You can add free and paid apps available on the managed Google Play Store to XenMobile.

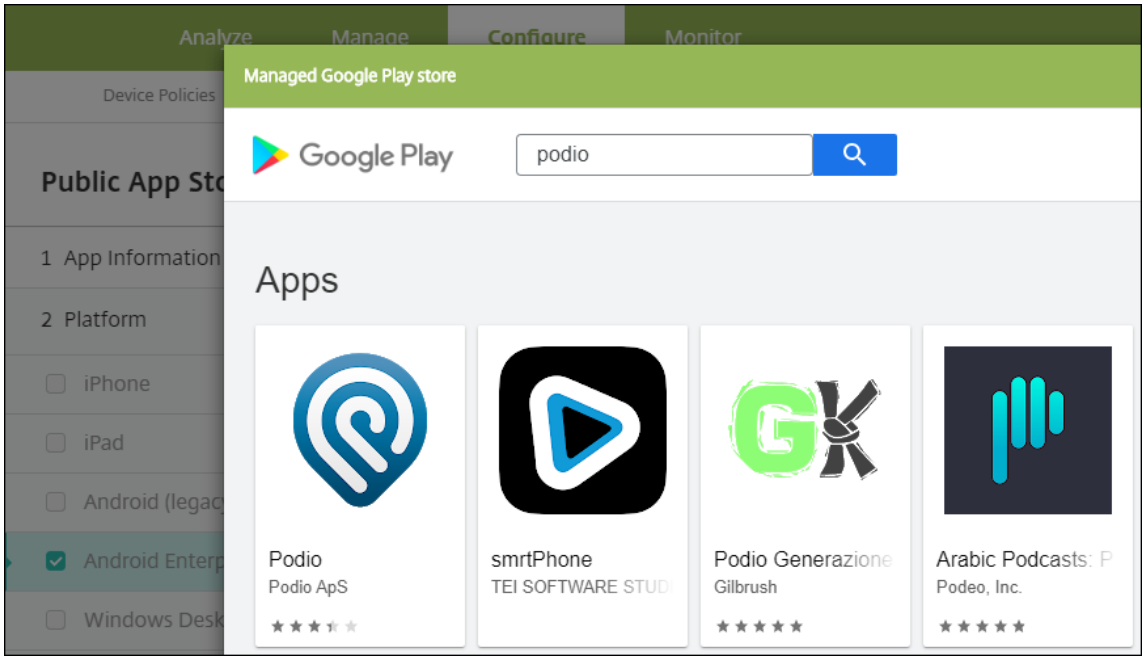
> **Note:**
>
> To make all apps in the Google Play store accessible from managed Google Play, use the **Access all apps in the managed Google Play store** server property. See Server properties. Setting this property to **true** allows all Android Enterprise users to access public Google Play store apps. You can then use the Restrictions device policy to control access to these apps.

Step 1: Add and configure apps

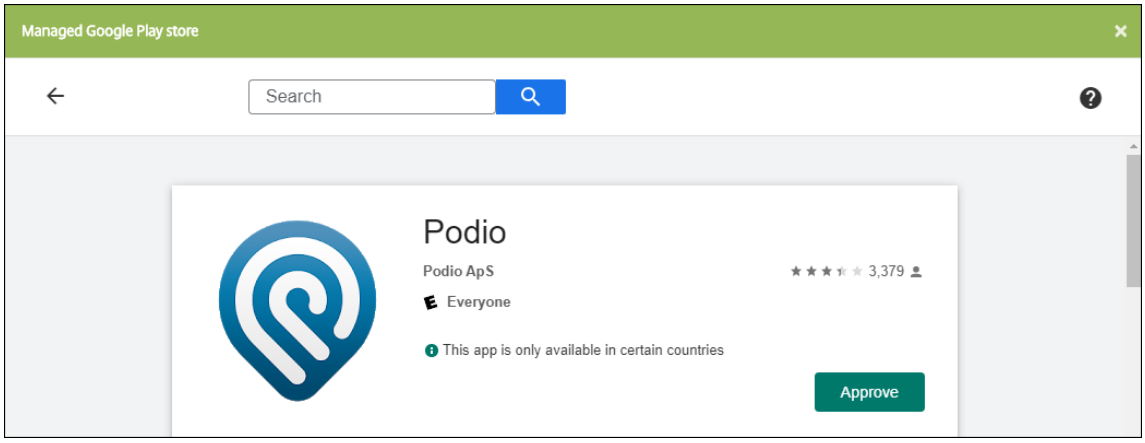
1. In the XenMobile console, navigate to **Configure > Apps**. Click **Add**.
2. Click **Public App Store**.



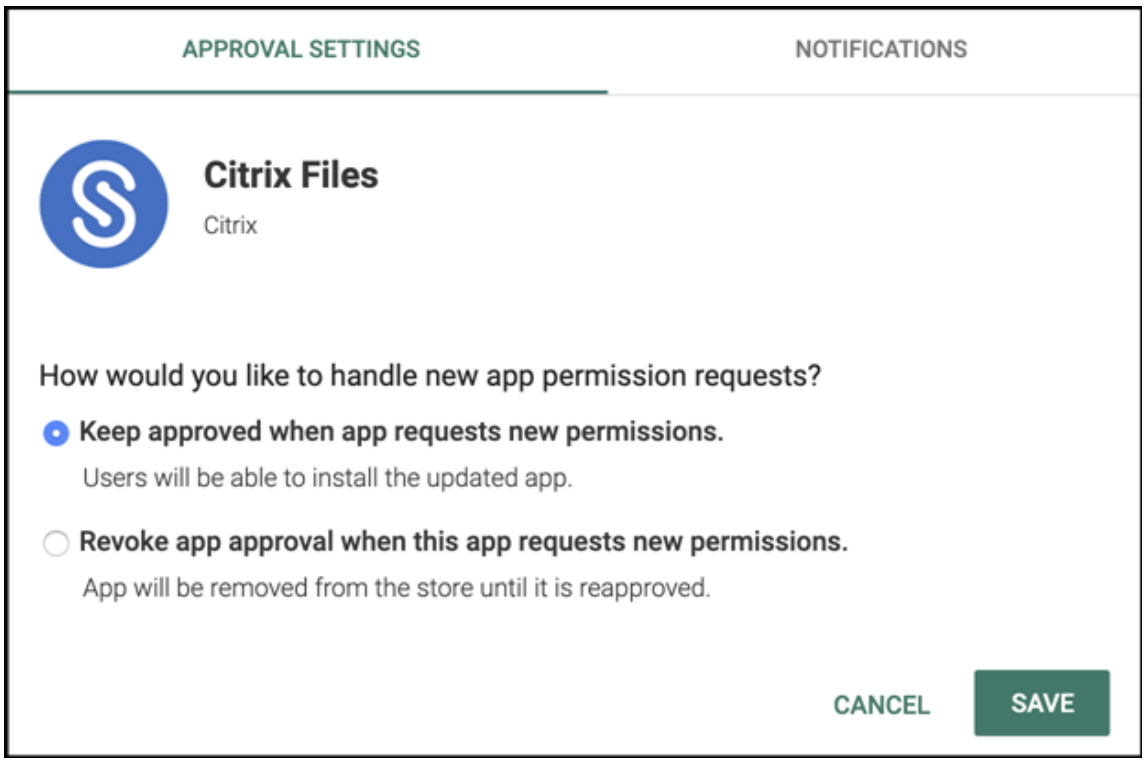
3. In the **App Information** pane, type the following information:
   - **Name:** Type a descriptive name for the app. The name appears under **App Name** on the **Apps** table.
   - **Description:** Type an optional description of the app.
   - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see About app categories.
4. Select **Android Enterprise** 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`.



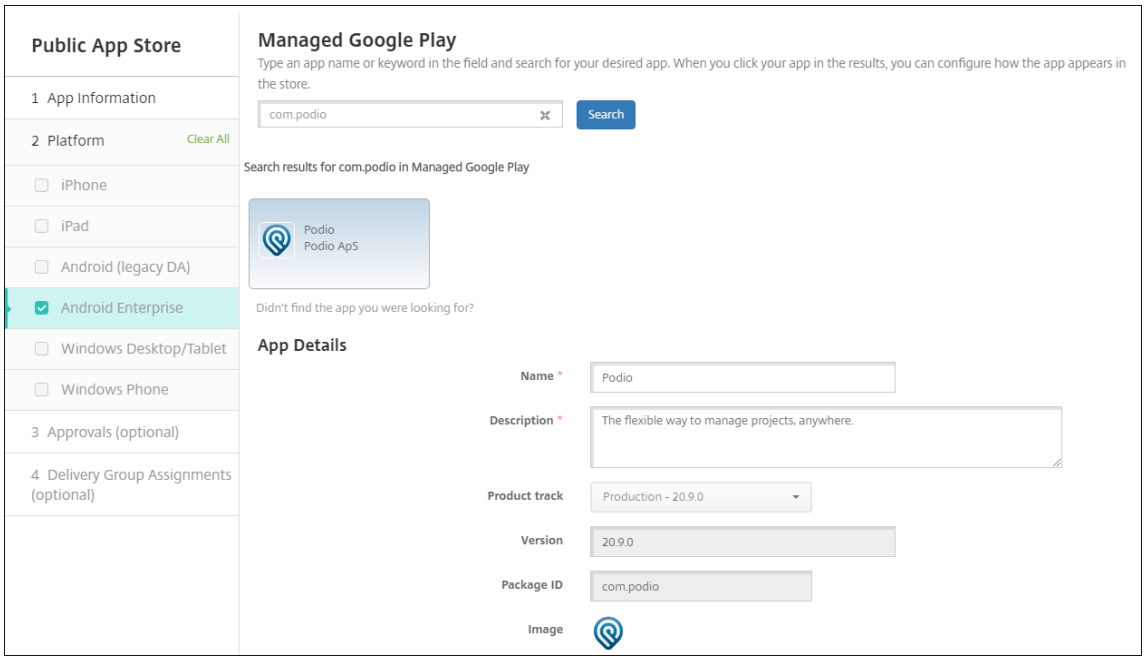
6. Apps matching the search criteria appear. Click the desired app then click **Approve**.



7. Click **Approve** again.
8. Select **Keep approved when app requests new permissions**. Click **Save**.



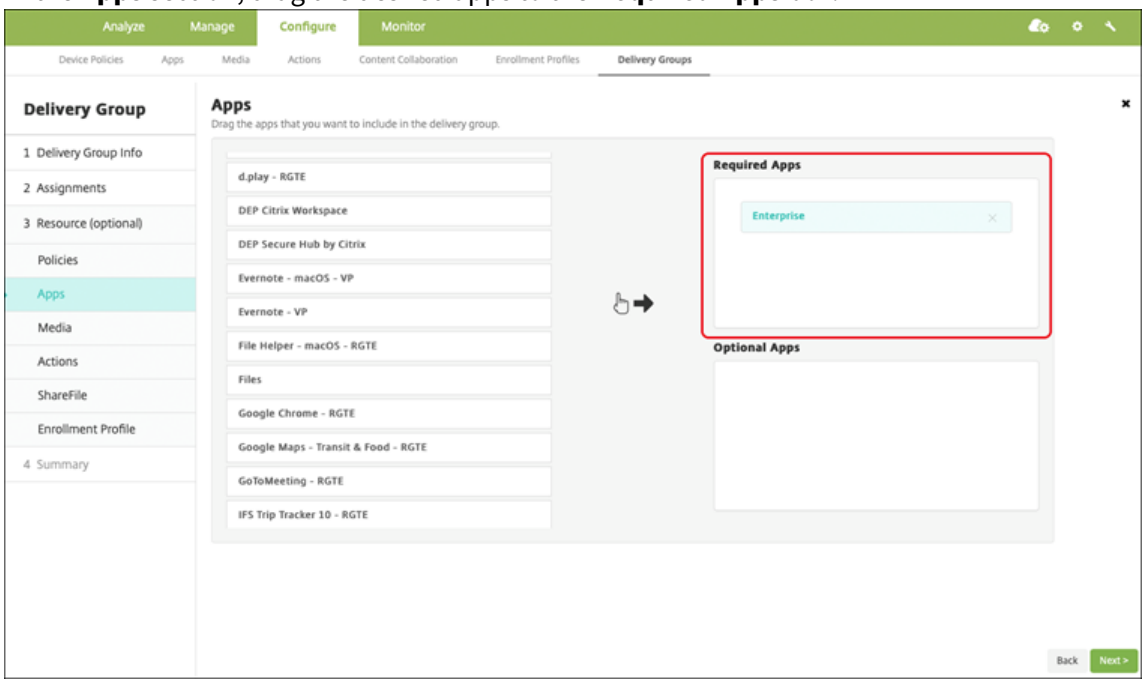
9. Click the app icon and configure the app **Name** and **Description**.



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 XenMobile 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:

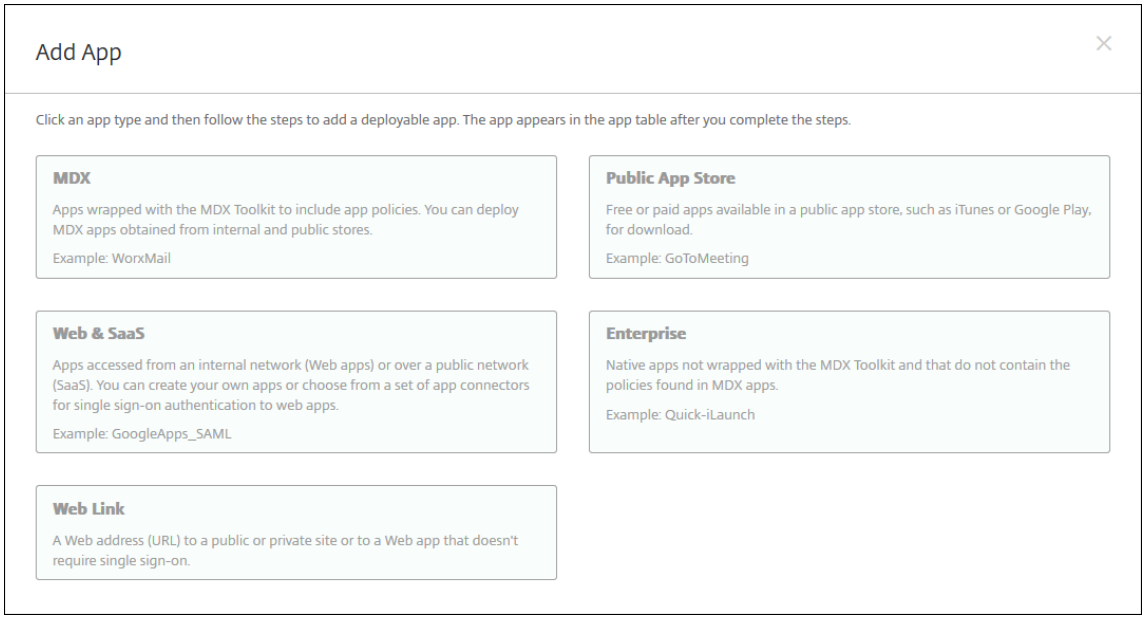
- MAM SDK Overview
- MDX Policies at a Glance

Step 1: Add and configure apps

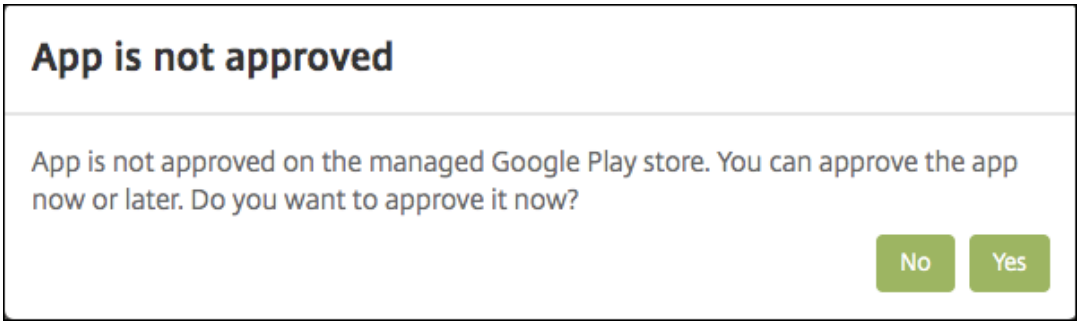
1. For Citrix mobile productivity apps, download the public-store MDX files: Go to https://www.citrix.com/downloads. Navigate to **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.

   For other types of MDX apps, obtain the MDX file.

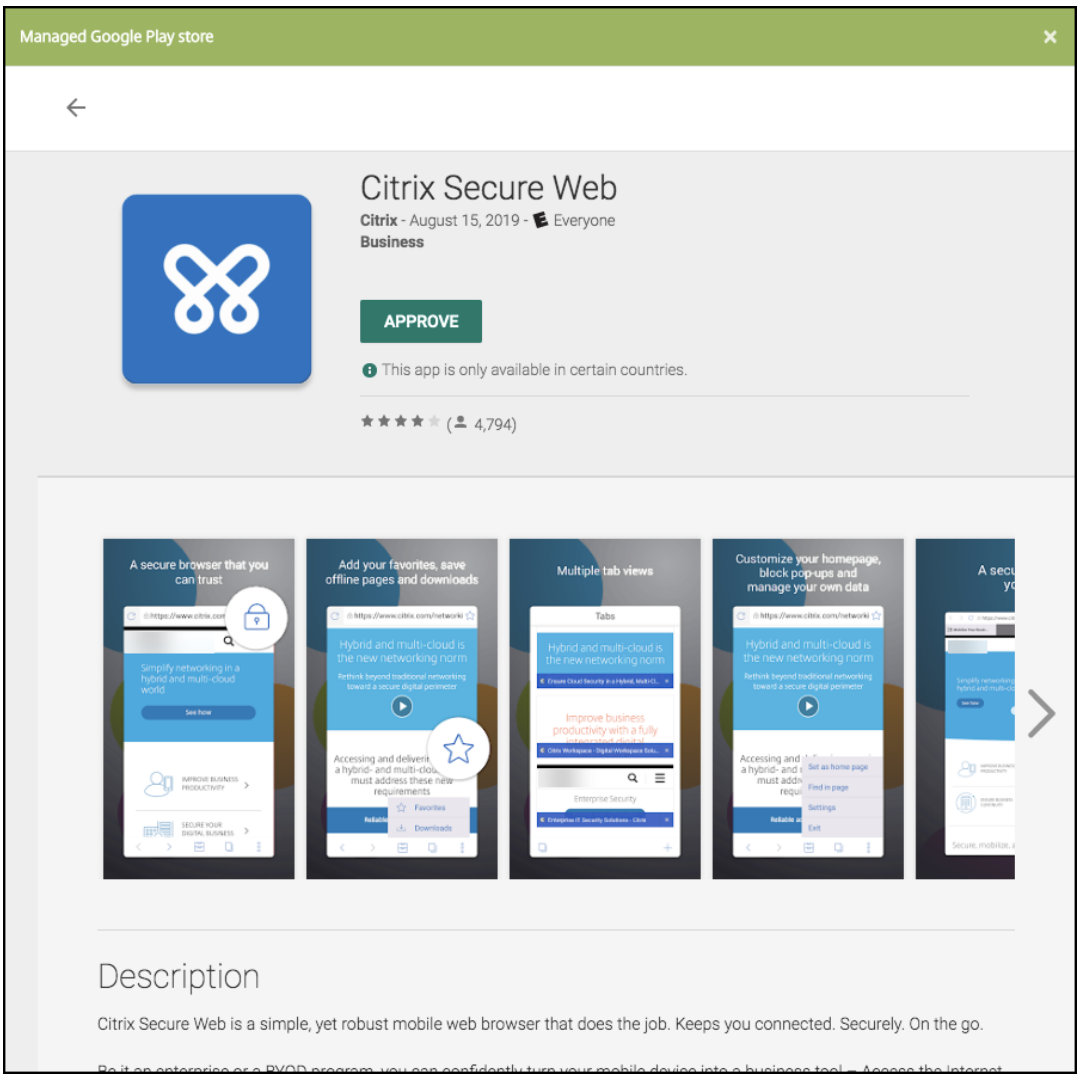
2. In the XenMobile console, click **Configure > Apps**. Click **Add**. The **Add App** dialog box appears.



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** as the platform.
5. Click **Upload** and navigate to the MDX file. Android Enterprise only supports apps prepared with the MAM SDK or MDX Toolkit. Do not wrap apps using the MDX Service.
   - The UI notifies you if the attached application requires approval from the managed Google Play Store. To approve the application without leaving the XenMobile 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.

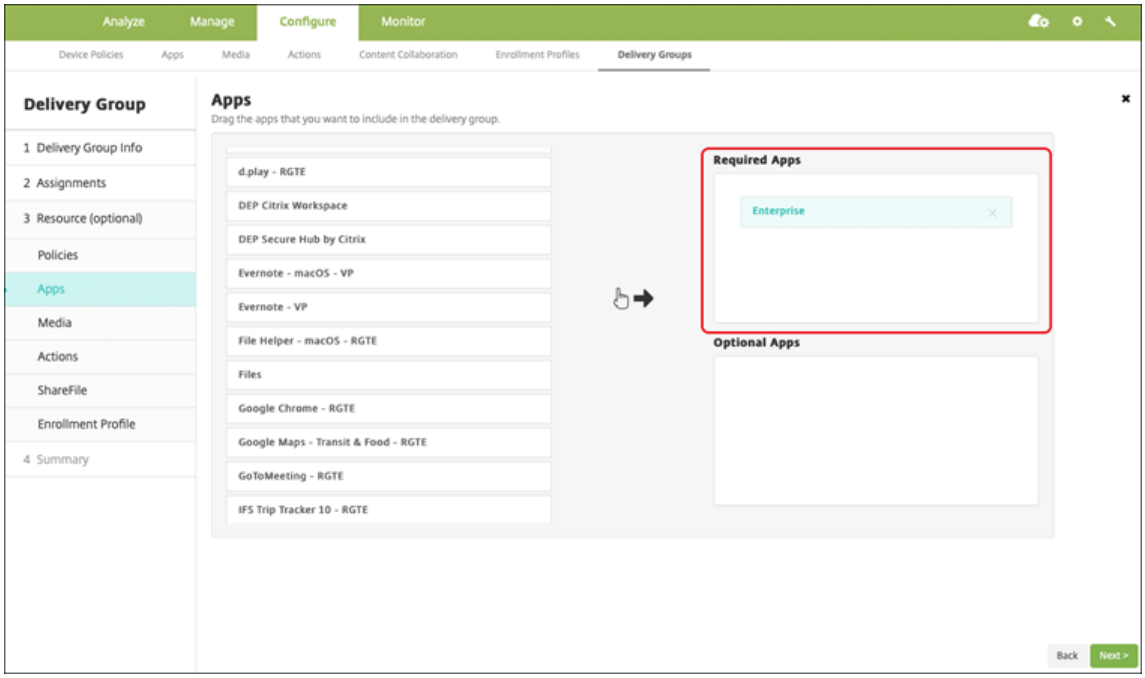
6. Configure these settings:

- **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

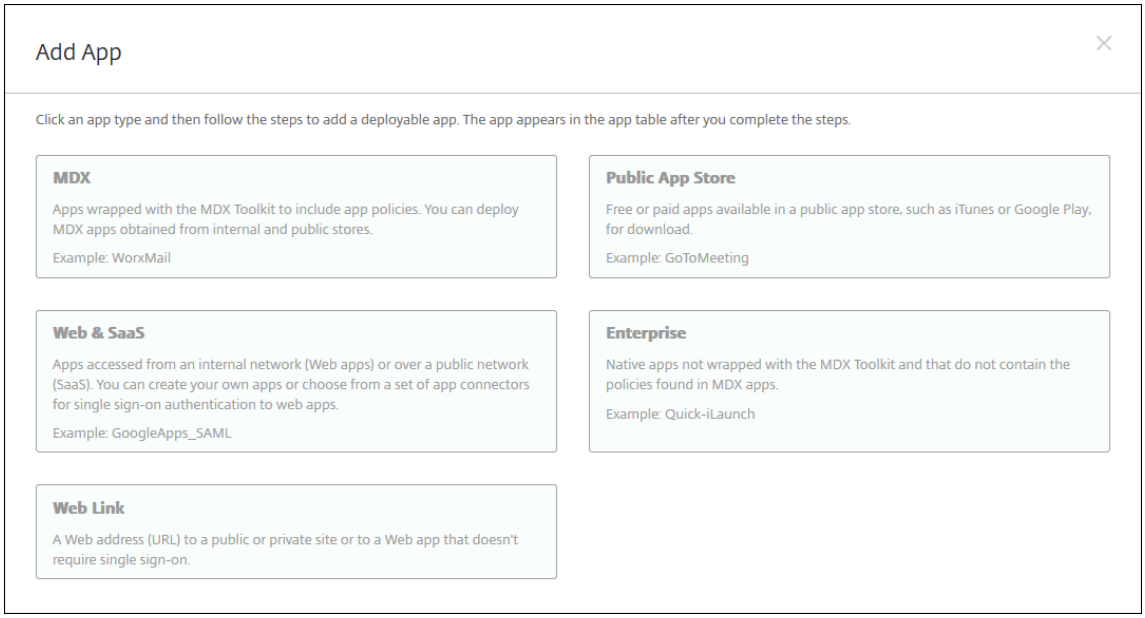
need the APK file associated with the app. Ensure that you follow Google Best practices for private apps.

Step 1: Add and configure apps

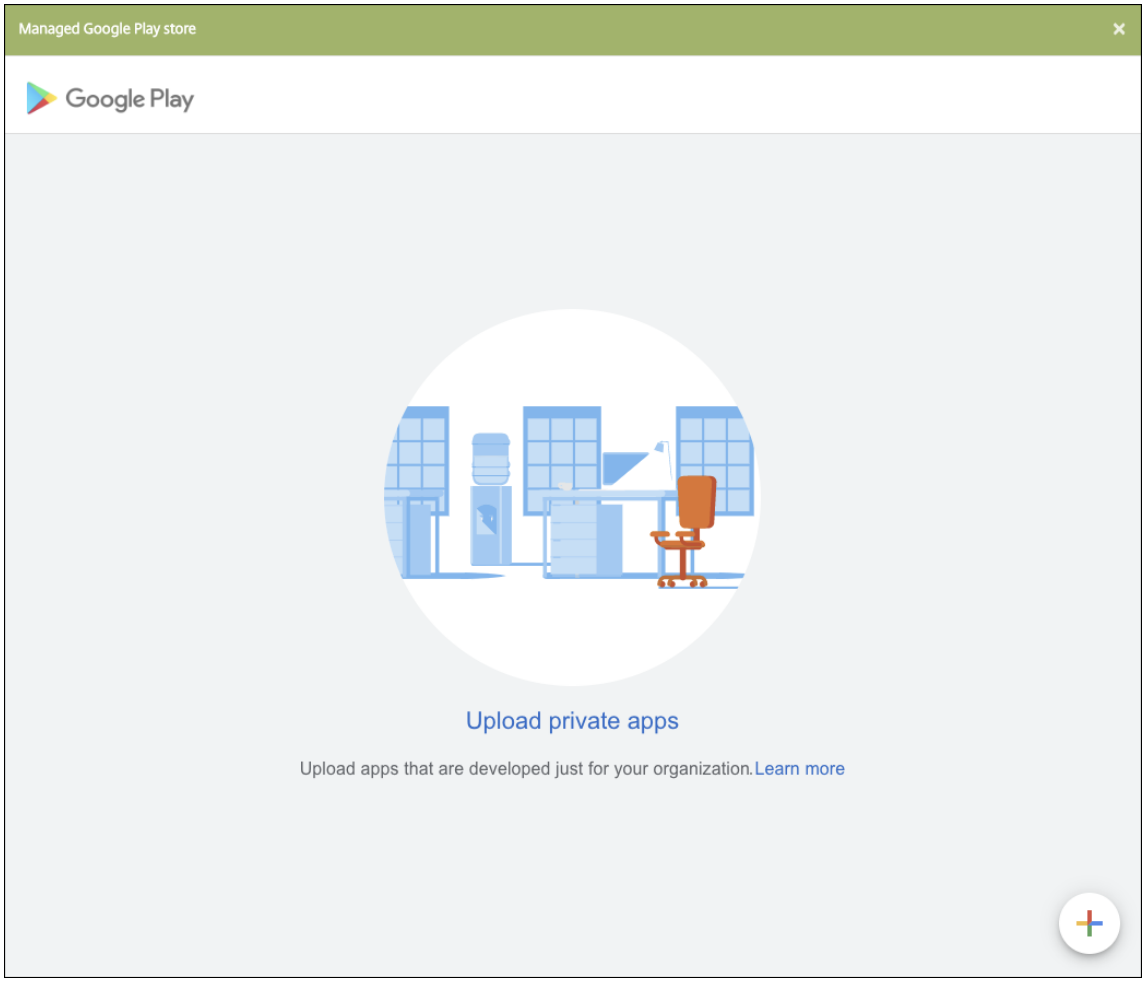
Add the app one of two ways:

- Publish the app directly to the managed Google Play Store and add it to the XenMobile 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 XenMobile console as an enterprise app. Perform the following steps:

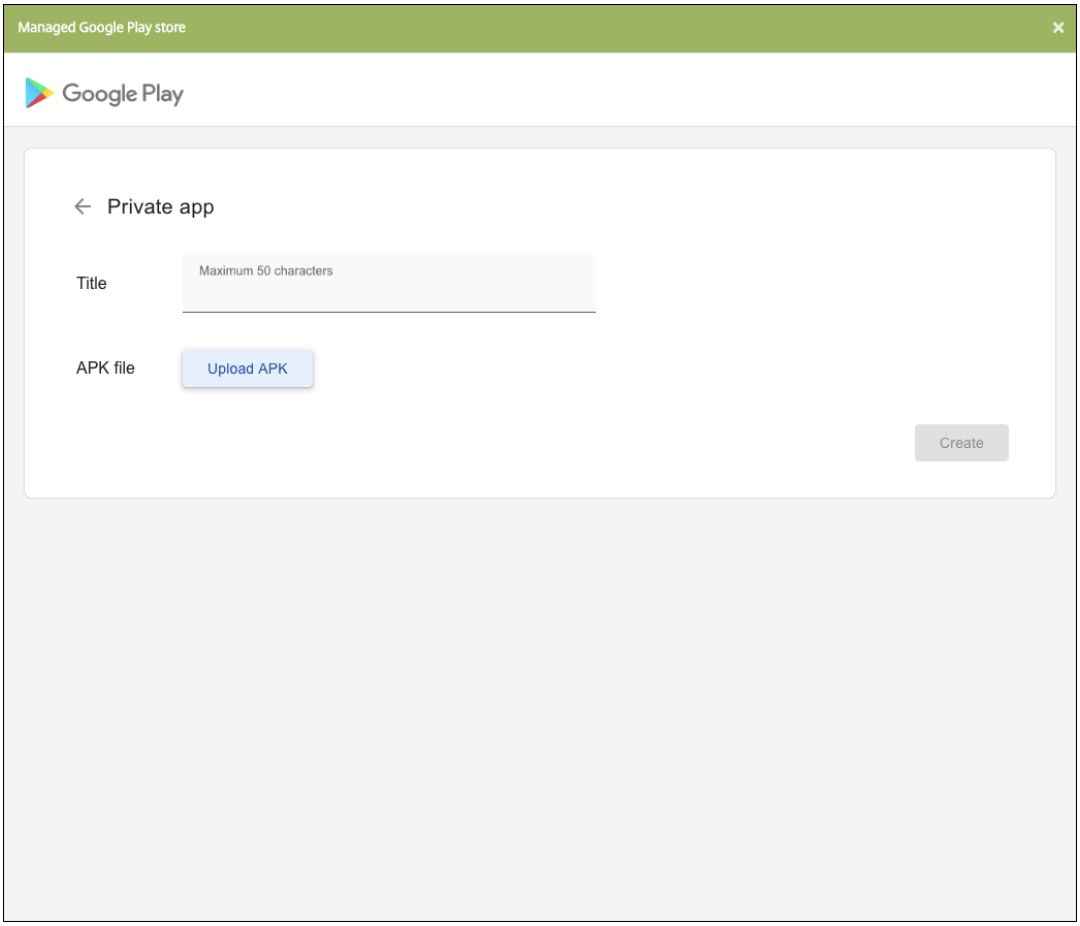
1. In the XenMobile console, click **Configure > Apps**. Click **Add**. The **Add App** dialog box appears.



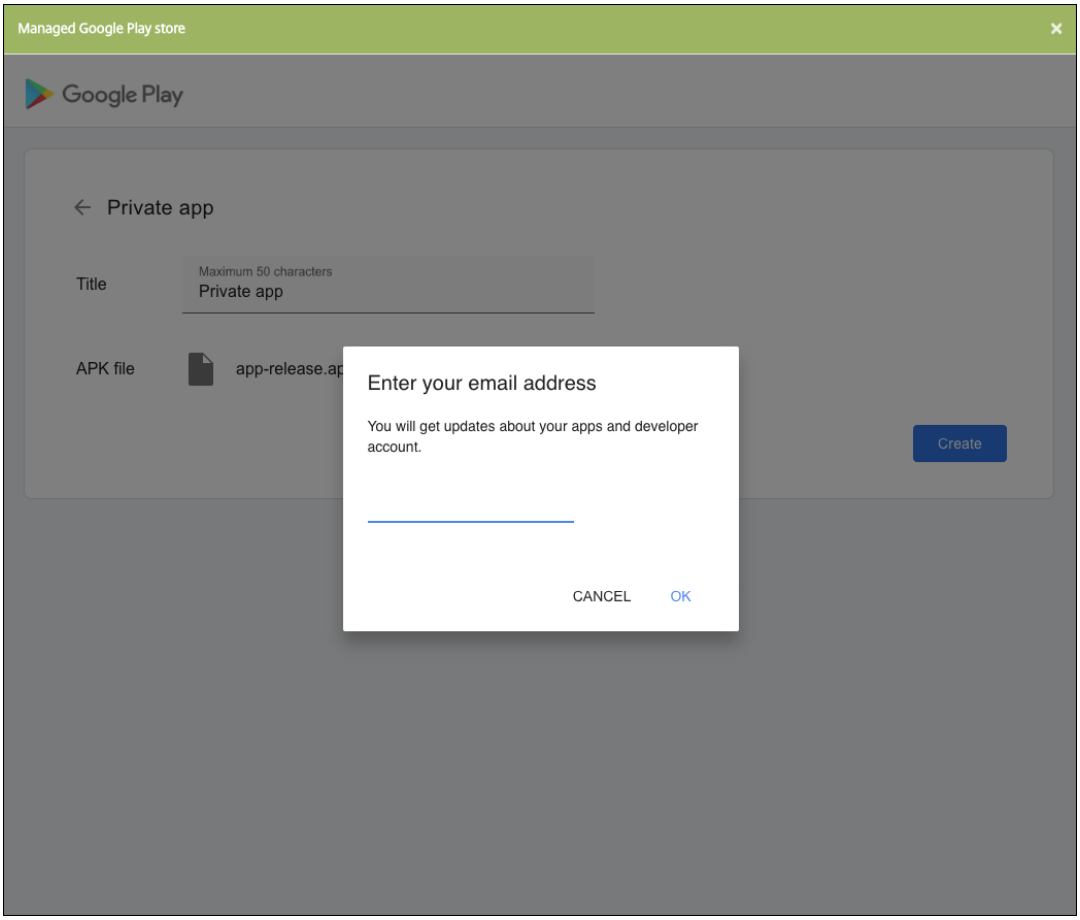
2. Click **Enterprise**. In the **App Information** pane, type the following information:
   - **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
   - **Description:** Type an optional description of the app.
   - **App category:** Optionally, in the 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** 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.



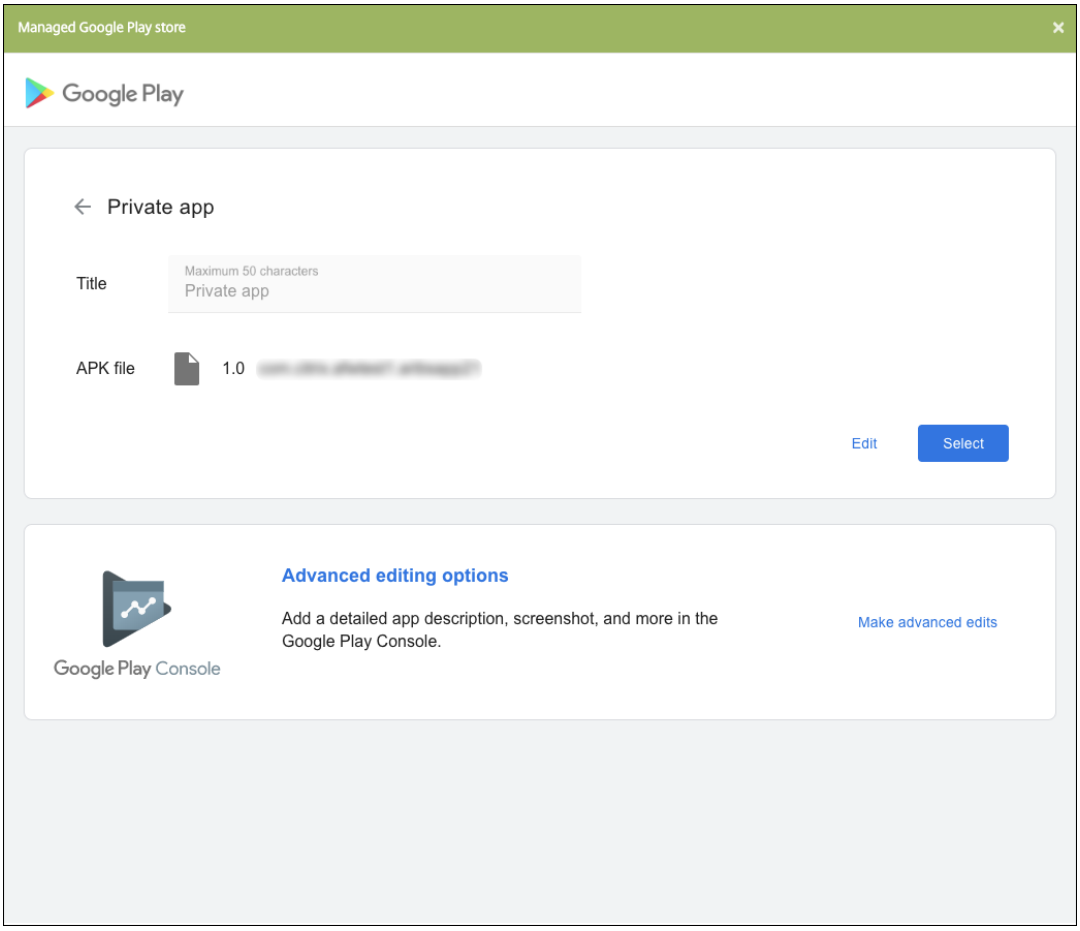
a) Type the name for your app and upload the .apk file. When finished, click **Create**. It might take up to 10 minutes for your private app to publish.



b) Enter an email address to get updates about your apps.



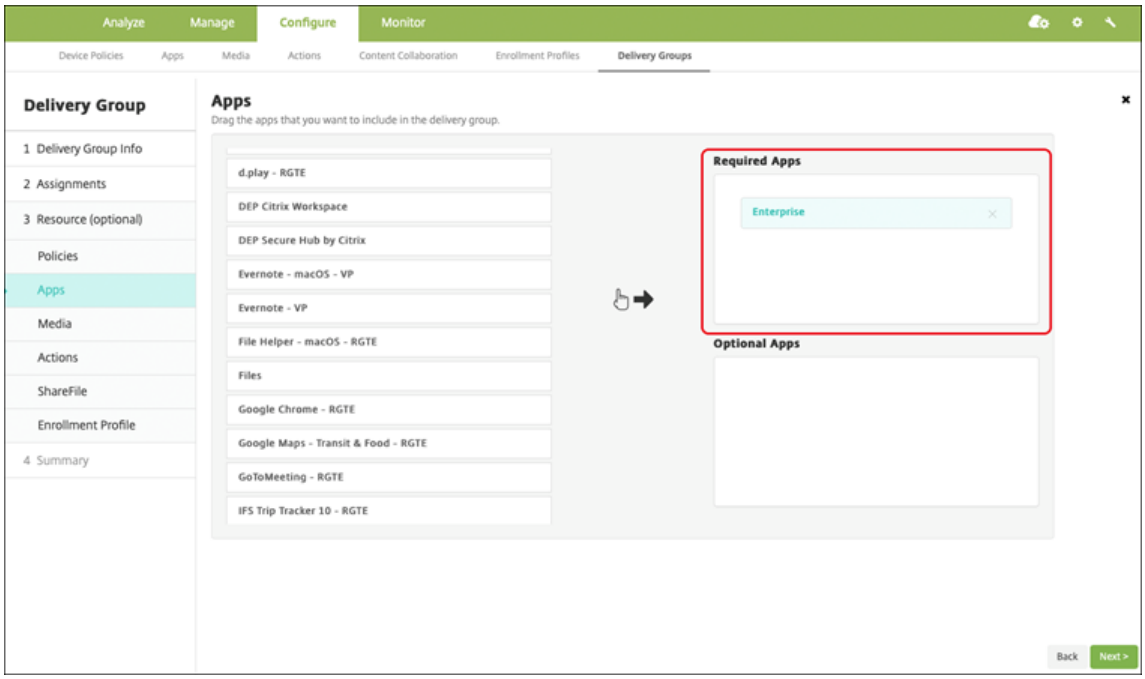
c) After your application is published, click the icon for the private app. If you want to add an app description, change the app icon, and other actions, click **Make advanced edits**. Otherwise, click **Select** to open the app information page.



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 apps as MDX-enabled enterprise apps:

1. Create a private Android Enterprise app and MDX-enable the app.
2. Add the app to the XenMobile console.
   - Host and publish the app on the managed Google Play Store.
   - Add the app to the XenMobile console as an Enterprise app.
3. Add the MDX file to XenMobile.

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 XenMobile, see the following sections.

Prepare a private Android Enterprise app

When you create a private Android Enterprise app, ensure that you follow Google Best practices for private apps.

After you create a private Android Enterprise app, integrate the MAM SDK with the app or wrap the app by using the MDX Toolkit. Android Enterprise doesn't support apps wrapped using the MDX Service. 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 private Android Enterprise app and generate a signed .apk file.
2. The following sample file contains all known policies, some of which might not be applicable for your environment. Any unusable settings are ignored. Create an XML file with the following parameters:

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileAppPolicies>
    <PolicySchemaVersion>
        1.0
    </PolicySchemaVersion>
    <Policies>
        <DevicePasscode>false</DevicePasscode>
        <AppPasscode>false</AppPasscode>
        <MaxOfflinePeriod>72</MaxOfflinePeriod>
        <StepupAuthAddress/>
        <RequireUserEntropy>false</RequireUserEntropy>
        <BlockRootedDevices>true</BlockRootedDevices>
        <BlockDebuggerAccess>false</BlockDebuggerAccess>
        <RequireDeviceLock>false</RequireDeviceLock>
        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
           NonCompliantDeviceBehavior>
        <WifiOnly>false</WifiOnly>
        <RequireInternalNetwork>false</RequireInternalNetwork>
        <InternalWifiNetworks/>
        <AllowedWifiNetworks/>
        <UpgradeGracePeriod>168</UpgradeGracePeriod>
        <WipeDataOnAppLock>false</WipeDataOnAppLock>
        <ActivePollPeriod>60</ActivePollPeriod>
        <PublicFileAccessLimitsList/>
        <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-->
```

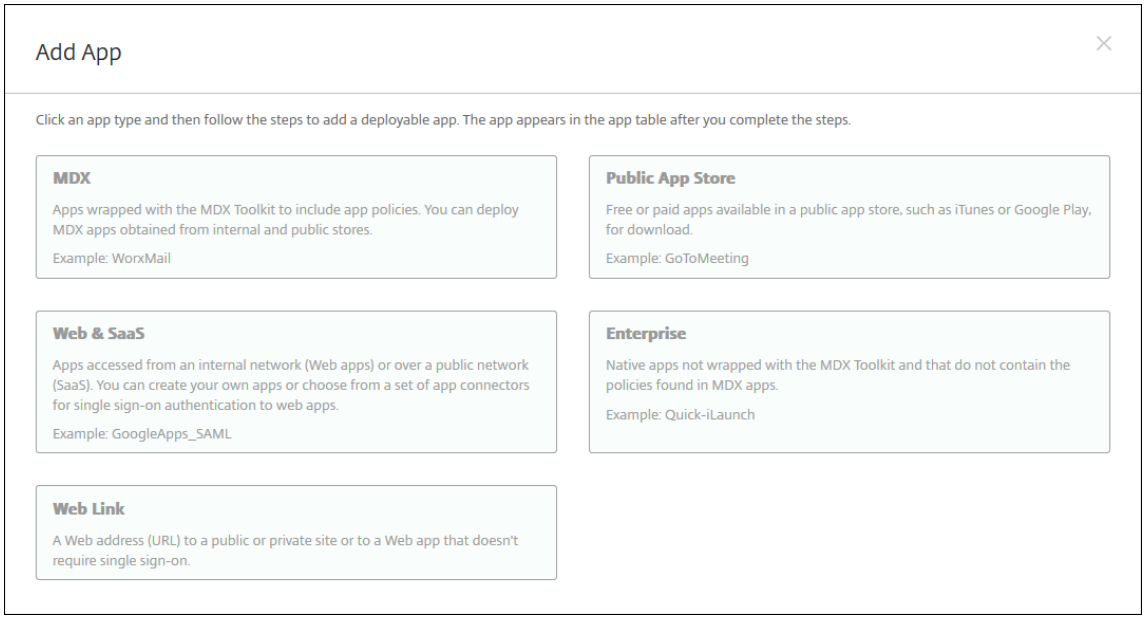
3. Wrap the app using the MDX Toolkit. For information about using the MDX Toolkit, see Wrapping Android mobile apps.

   Set the **apptype** parameter to **Premium**. Use the XML file from the previous step in the command described next.

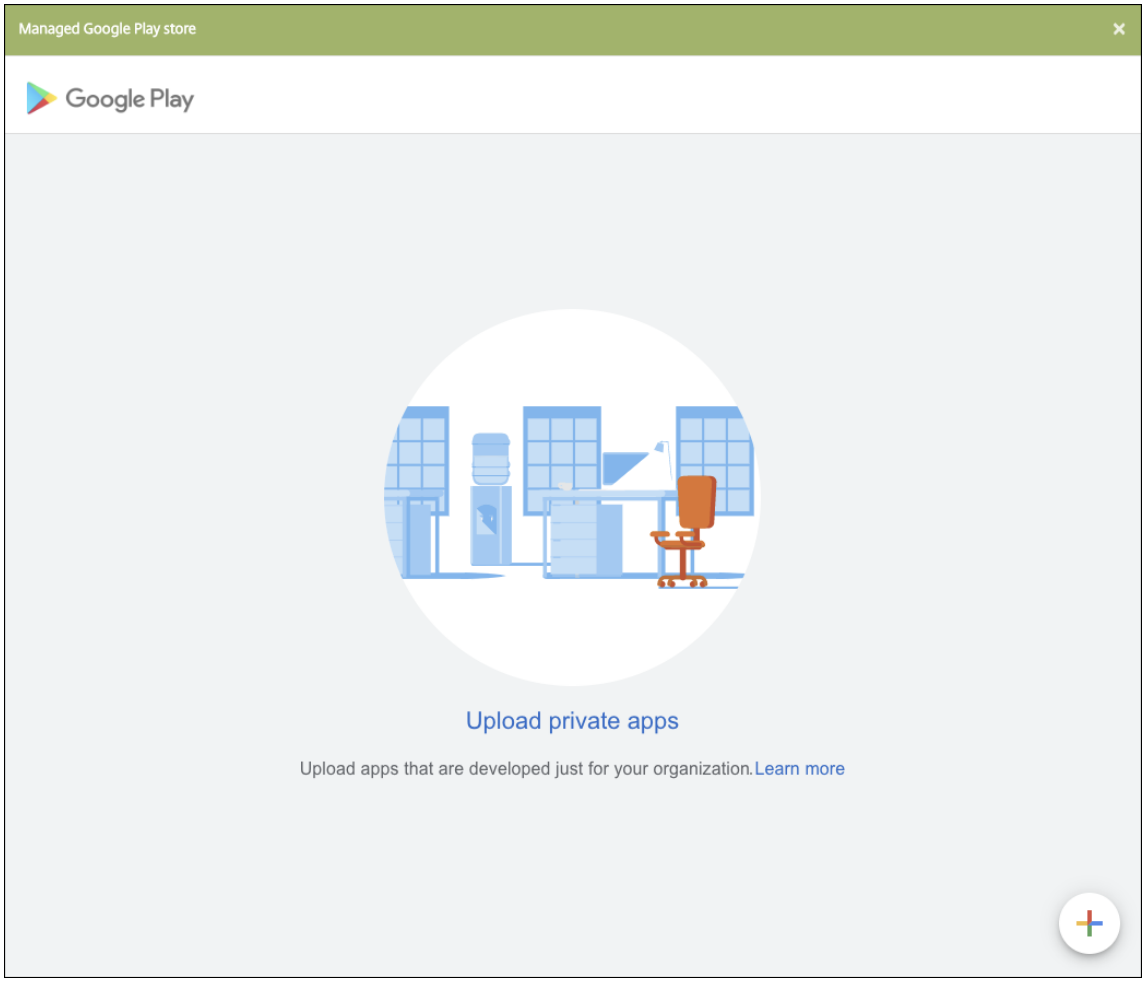
If you know the store URL for the app, set the **storeURL** parameter to the store URL. Users download the app from the store URL after you publish the app.

Here is an example of an MDX Toolkit command used to wrap an app called SampleAEapp:

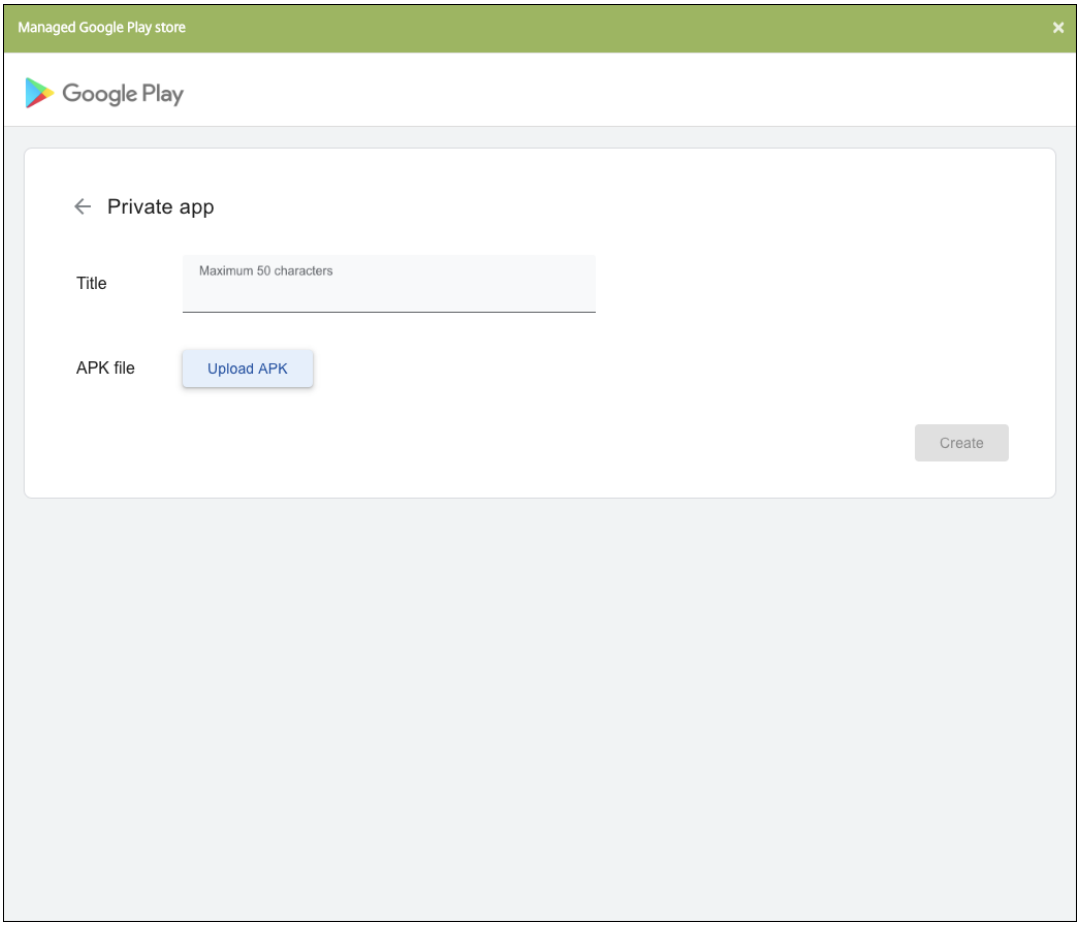
```
```
 java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -
    Duser.variant
 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
 -MinPlatform 5.0
 -keystore /MyKeystore
 -storepass mystorepwd123
 -keyalias key0
 -keypass mykeypwd123
 -storeURL "https://play.google.com/store/apps/details?id=
    SampleAEappPackage"
 -appType Premium
 -premiumMdxPolicies <Path to Premium policy XML>
<!--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 XenMobile 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 XenMobile console as an enterprise app. Perform the following steps:

1. In the XenMobile console, click **Configure > Apps**. The **Apps** page opens.
2. Click **Add**. The **Add App** dialog box appears.

 
```



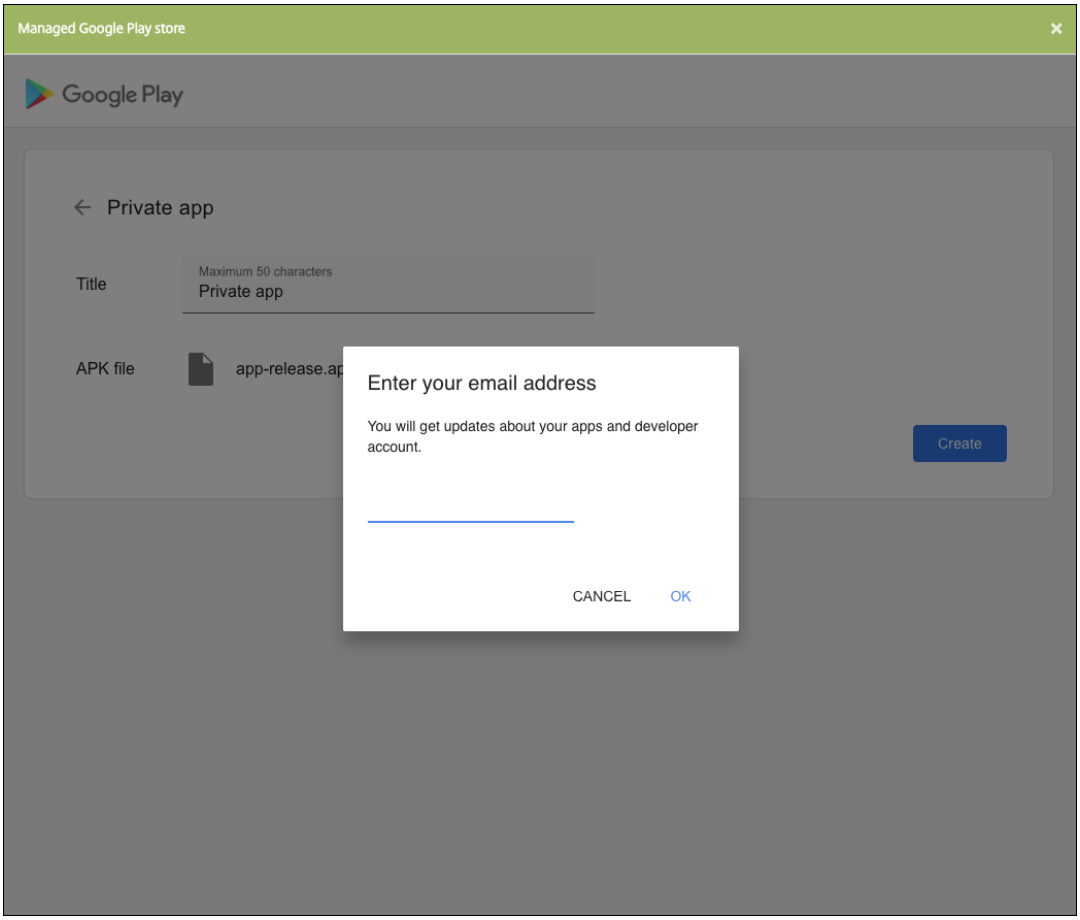
3. Click **Enterprise**. In the **App Information** pane, type the following information:
   - **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
   - **Description:** Type an optional description of the app.
   - **App category:** Optionally, in the 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** 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.



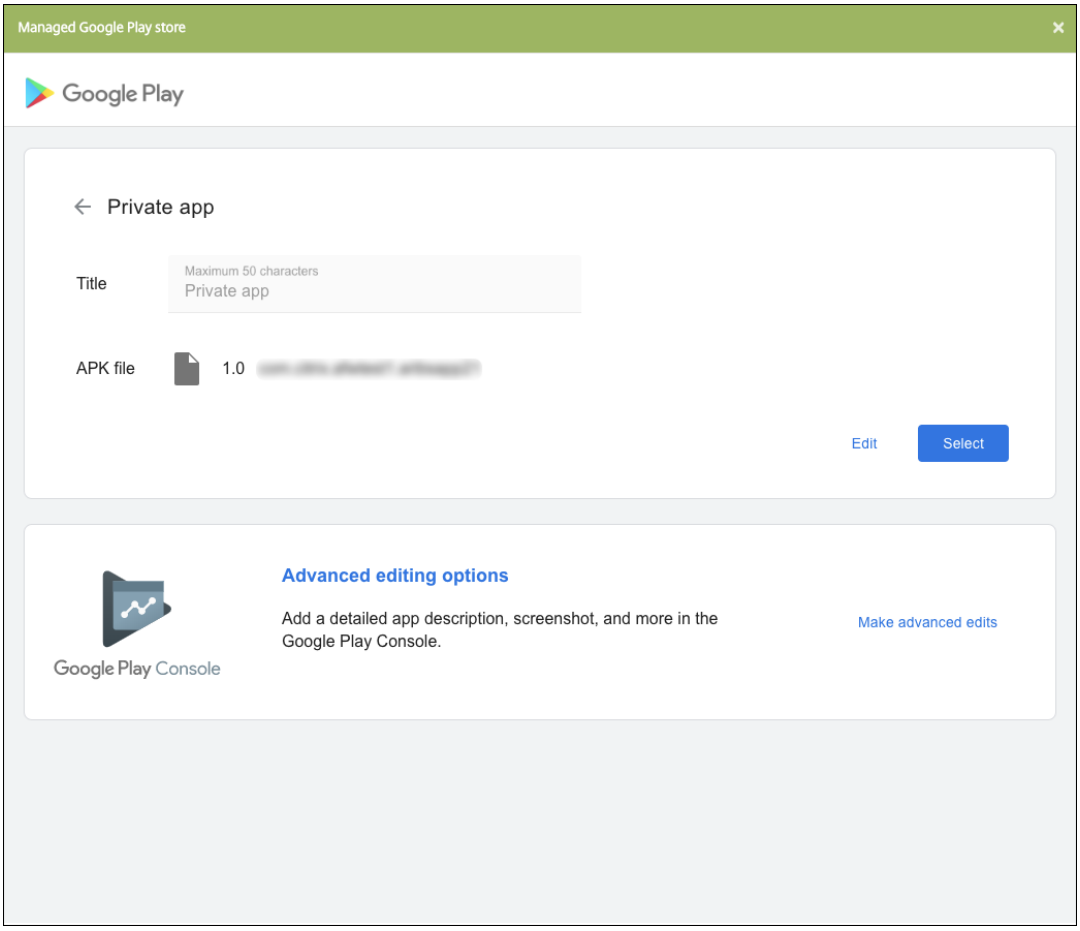
a) Type the name for your app and upload the .apk file. When finished, click **Create**. It might take up to 10 minutes for your private app to publish.



b) Enter an email address to get updates about your apps.



c) After your application is published, click a private app's icon 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 **Android Enterprise 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

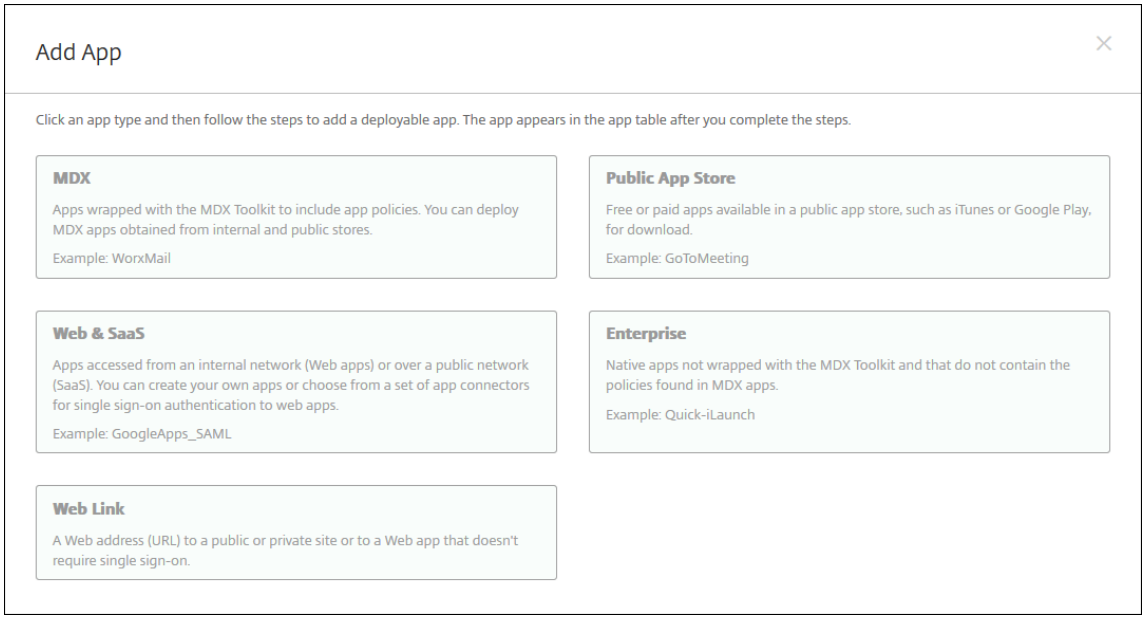
If you didn't know the store URL when you wrapped the app, add the store URL now.

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 might 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:

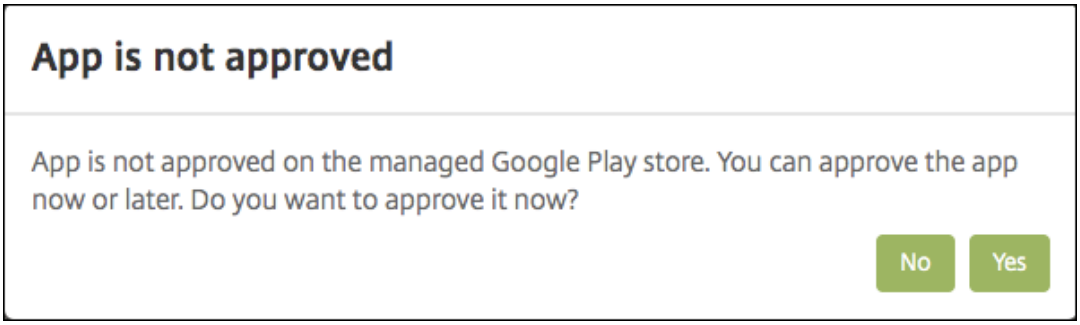
```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \
setinfo \
-in ~/Desktop/SampleApps/Sample.mdx \
-out ~/Desktop/SampleApps/wrapped/Sample.mdx \
-storeURL "https://play.google.com/store/apps/details?id=
   SampleAEappPackage"
<!--NeedCopy-->
```

Add the .mdx file

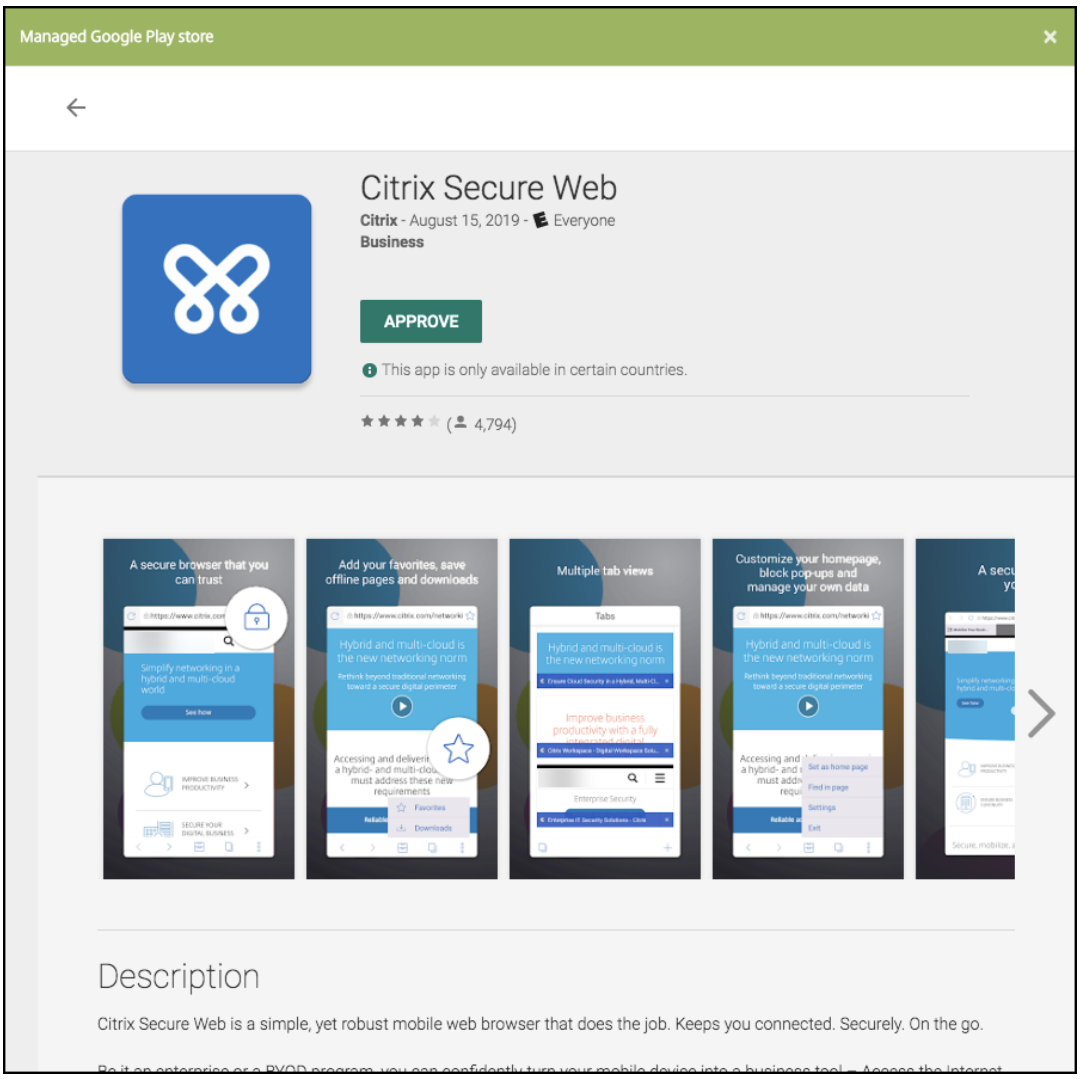
1. In the XenMobile console, click **Configure > Apps**. Click **Add**. The **Add App** dialog box appears.



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** as the platform.
4. Click **Upload** and navigate to the MDX file. Android Enterprise only supports apps wrapped with the MDX Toolkit. Do not wrap apps using the MDX Service.
   - The UI notifies you if the attached application requires approval from the managed Google Play Store. To approve the application without leaving the XenMobile 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:

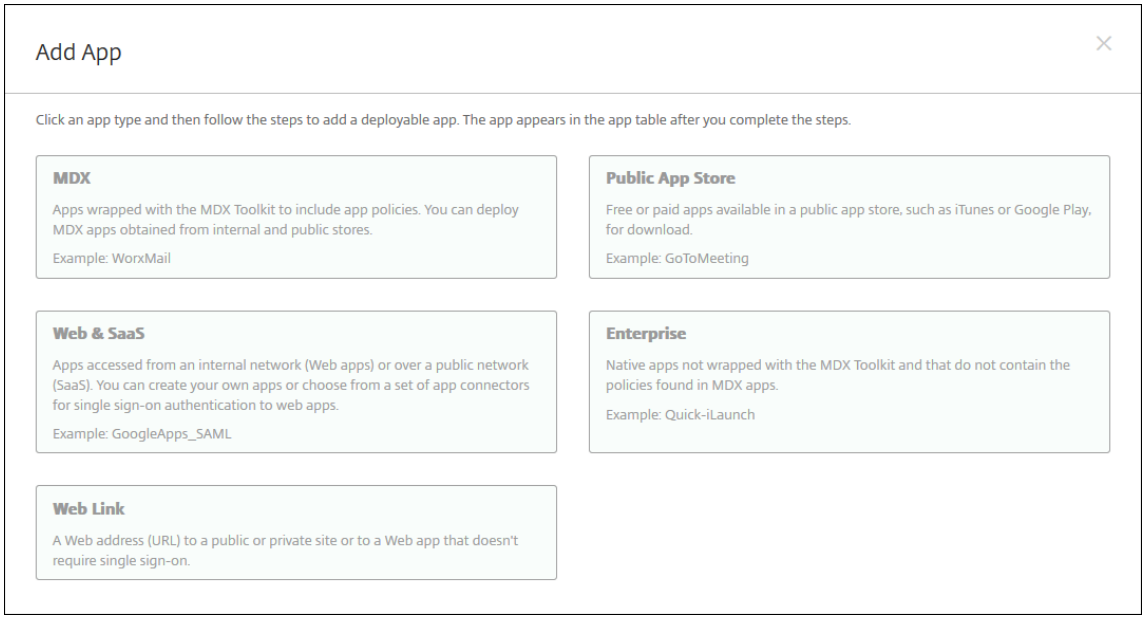
   - Is not available Android Enterprise customers who began using Endpoint Management with version 10.18.19 or later
   - Is not recommended for Android Enterprise customers who began using Endpoint Management before version 10.18.19

   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.

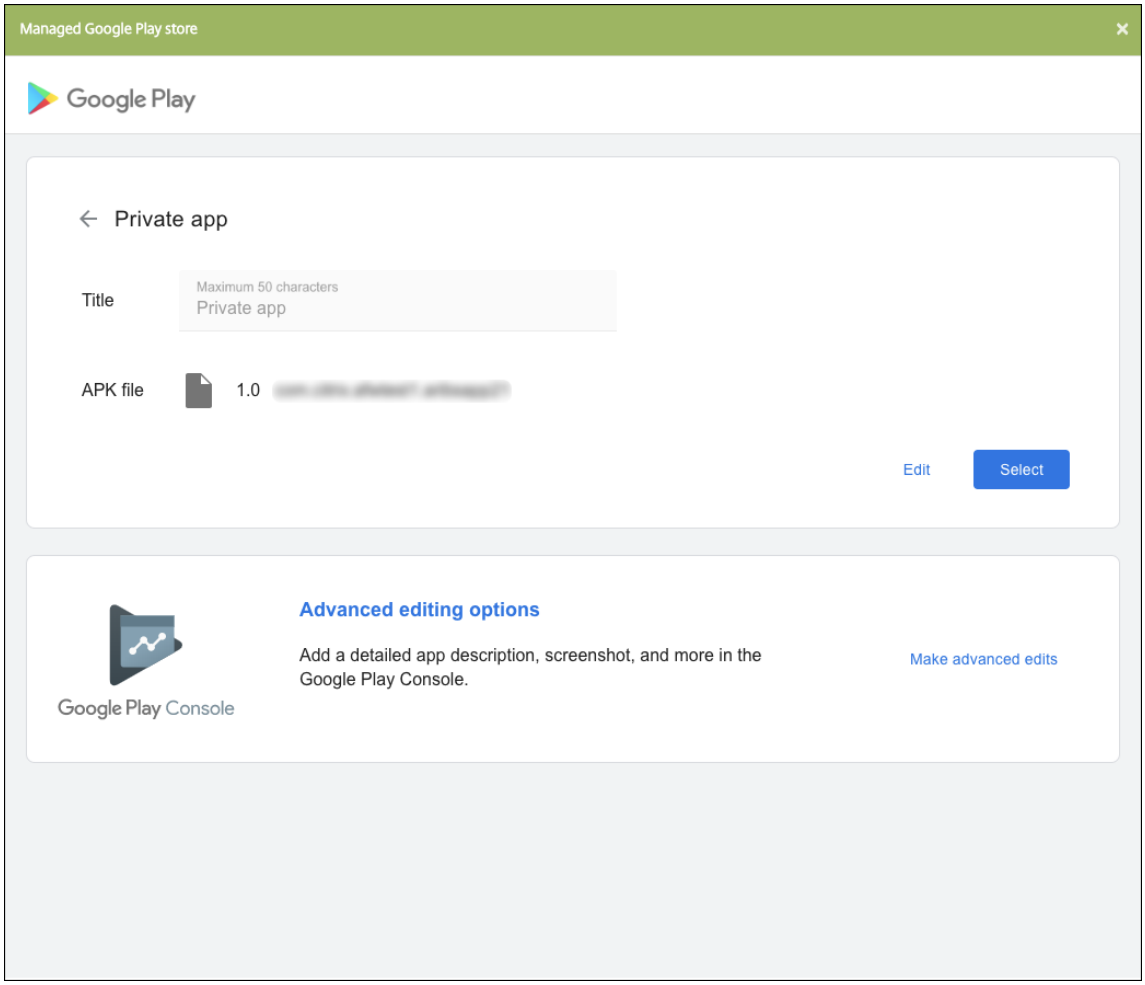
Update the app

To update the Android Enterprise 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 XenMobile 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** as the platform.
6. Click **Next**. The **Android Enterprise 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

June 25, 2021

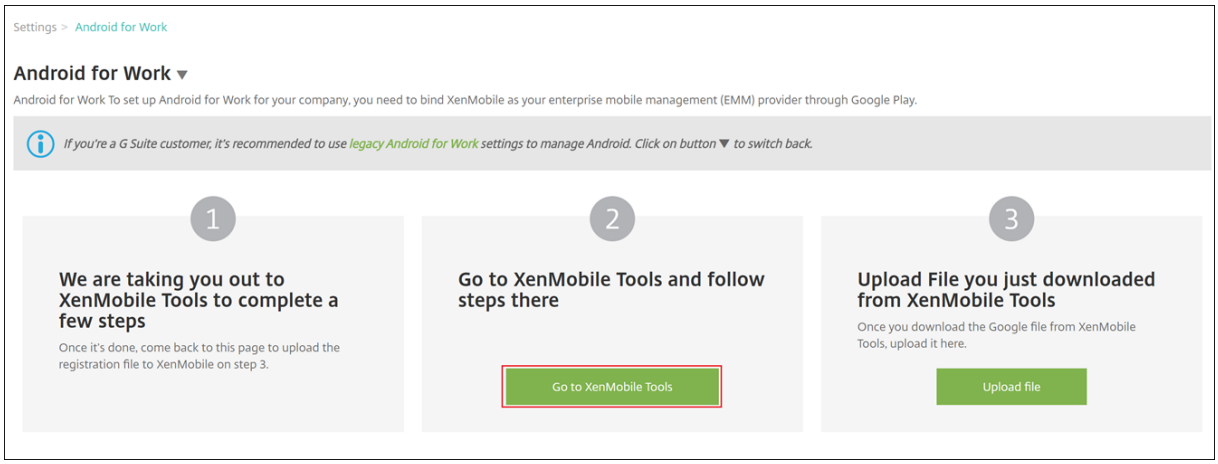
Google Workspace (formerly G Suite) customers must use the legacy Android Enterprise settings to configure legacy Android Enterprise.

Requirements for legacy Android Enterprise:

- A publicly accessible domain
- A Google administrator account
- Devices that have managed profile support and that are running Android 5.0+ Lollipop

- 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 XenMobile Settings.



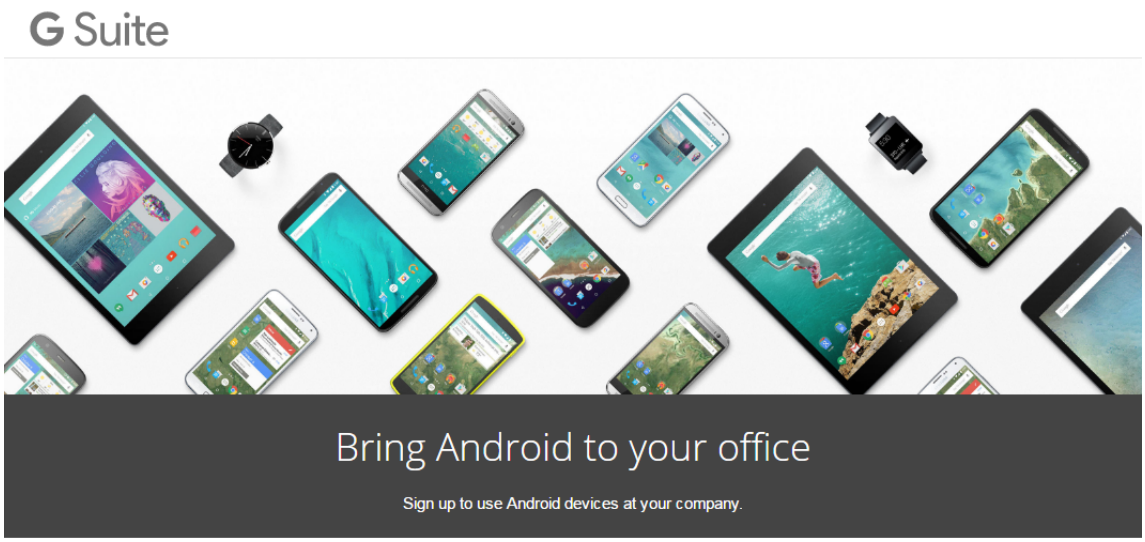
Create an Android Enterprise Account

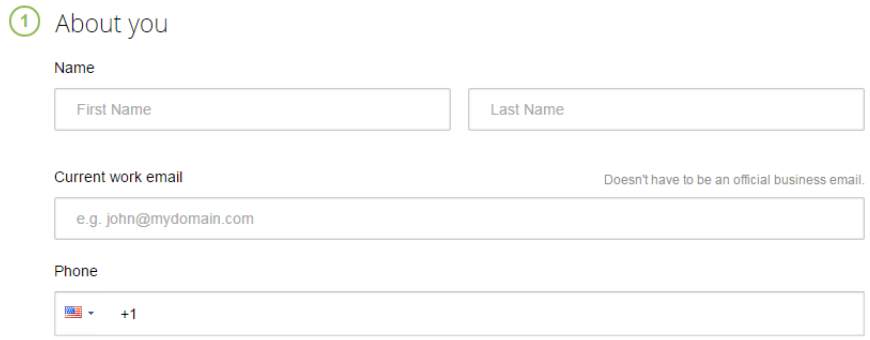
Before you can set up an Android Enterprise account, you must verify your domain name with Google.

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.

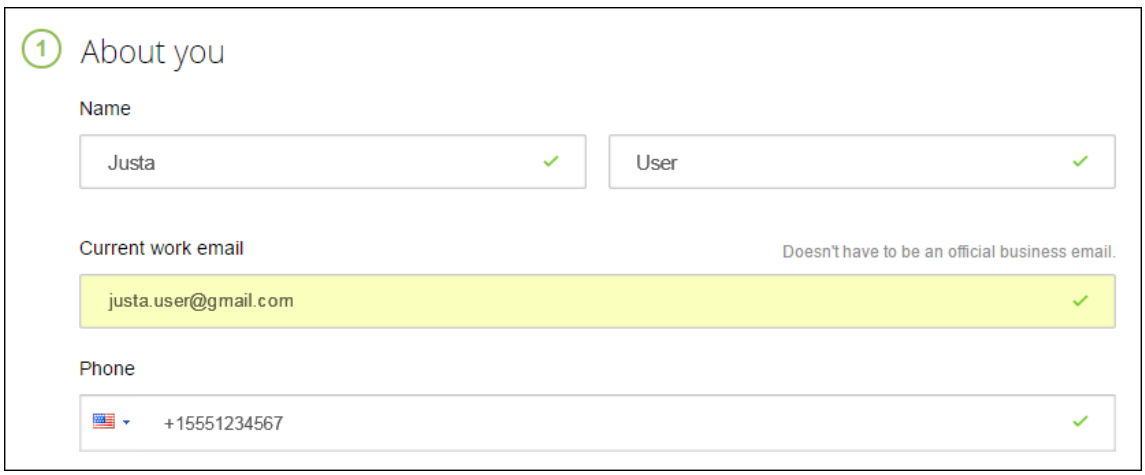
1. Navigate to https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

   The following page displays where you type your administrator and company information.

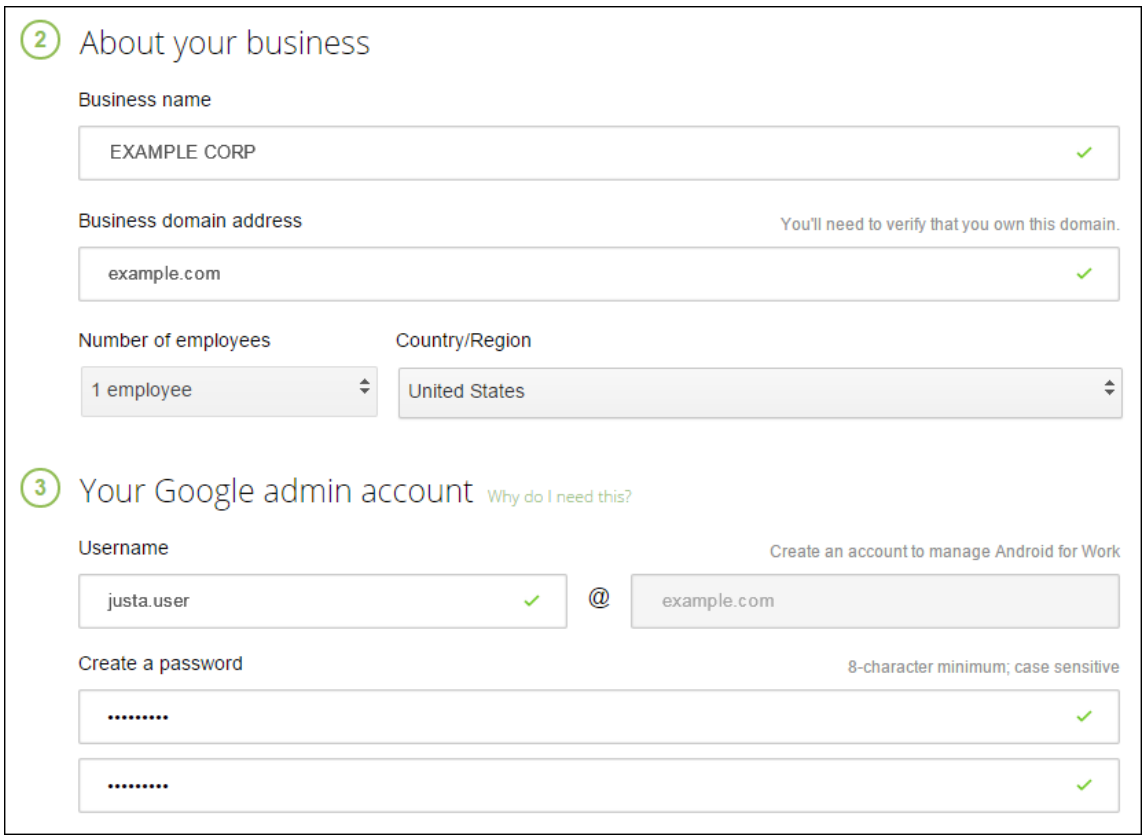




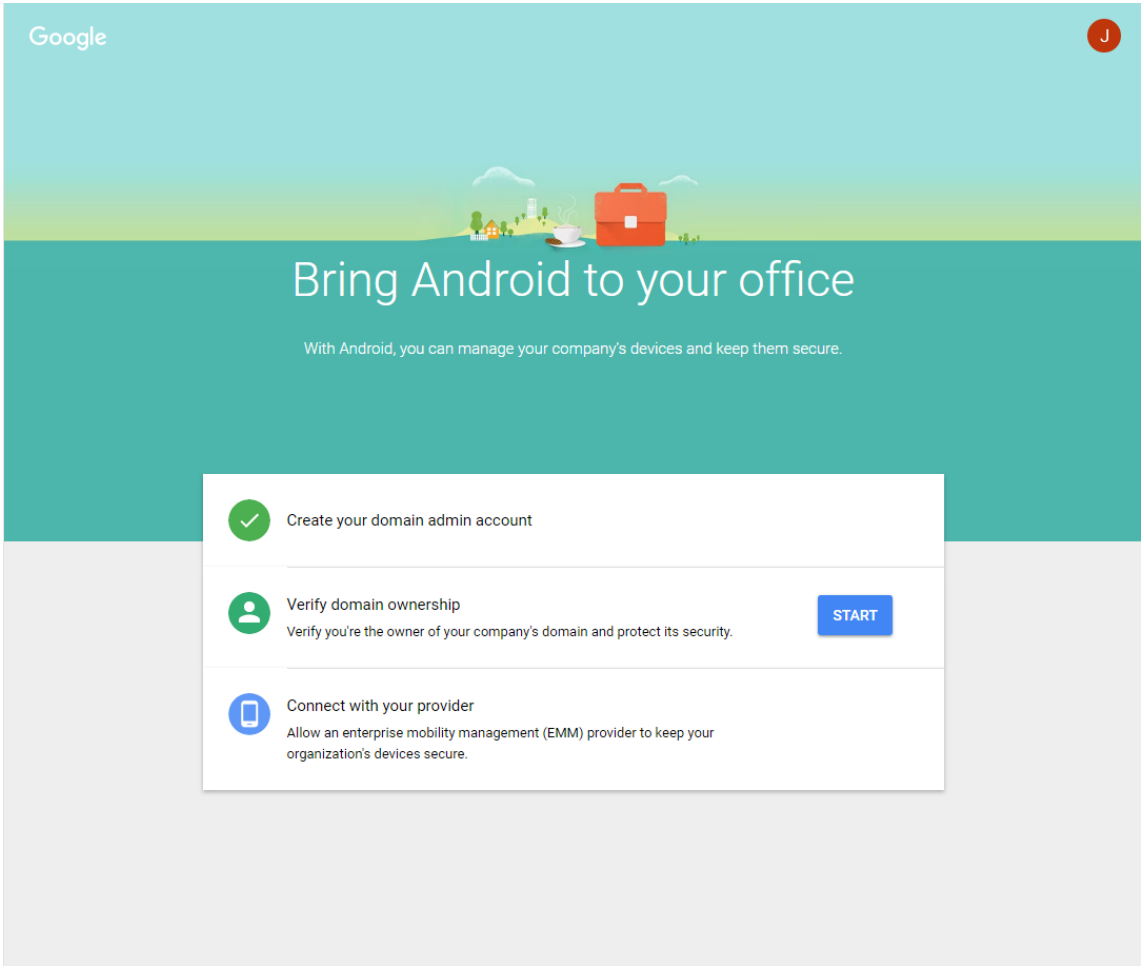
2. Type your administrator user information.



3. Type your company information, in addition to your administrator account information.



The first step in the process is complete and you see the following page.



Verify domain ownership

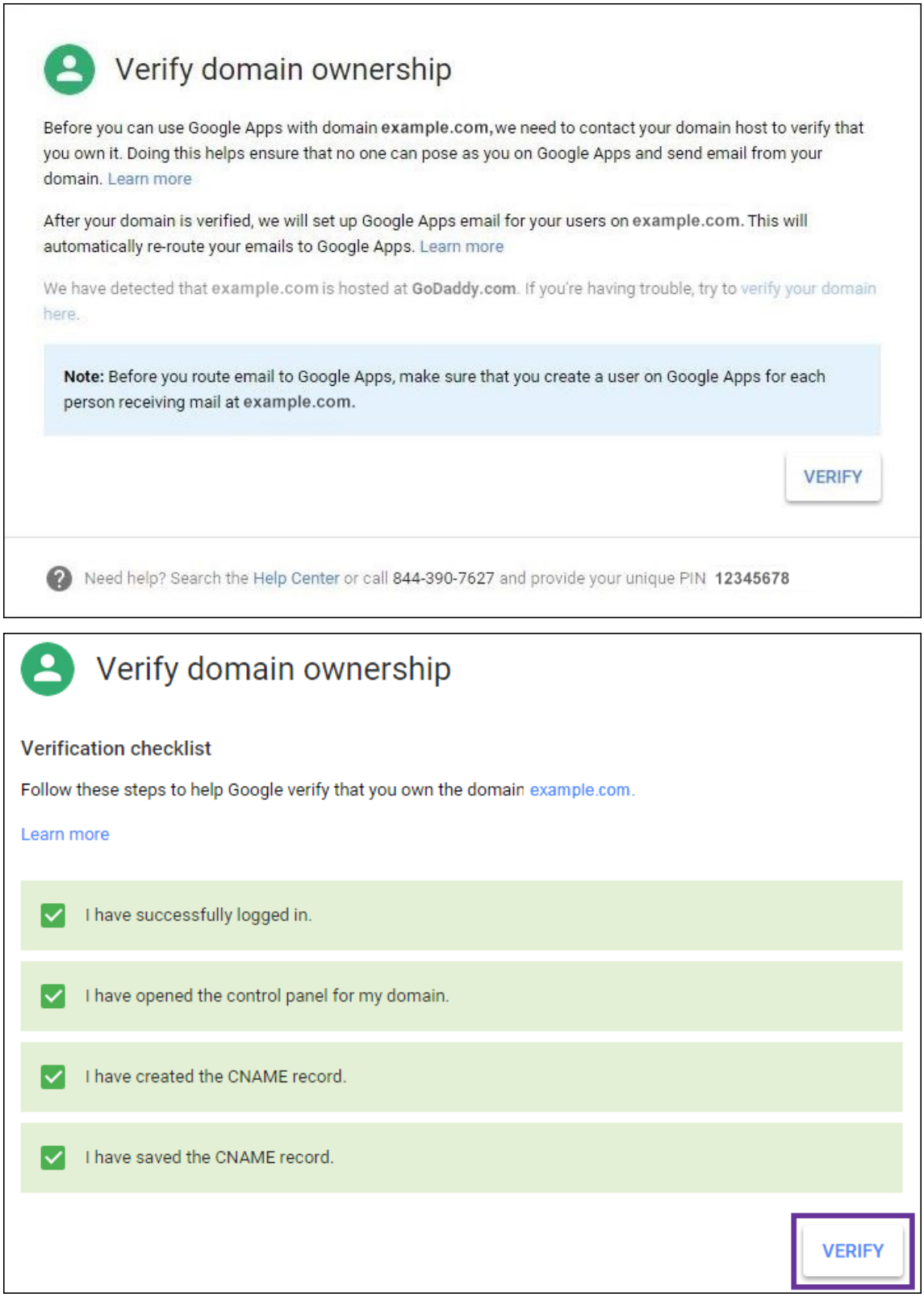
Allow Google to verify your domain in one of the following ways:

- 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.

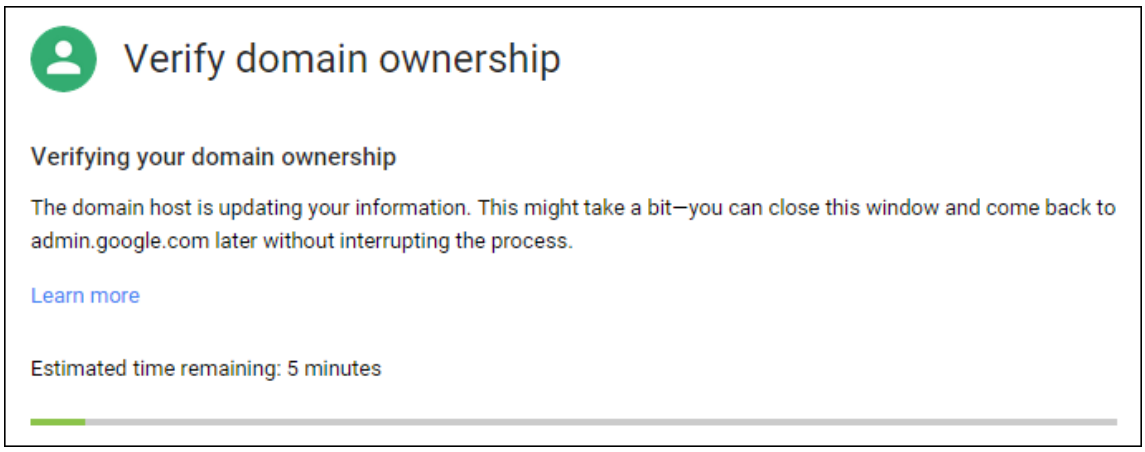
1. Click **Start** to begin the verification of your domain.

   The **Verify domain ownership** page appears. Follow the instructions on the page to verify your domain.

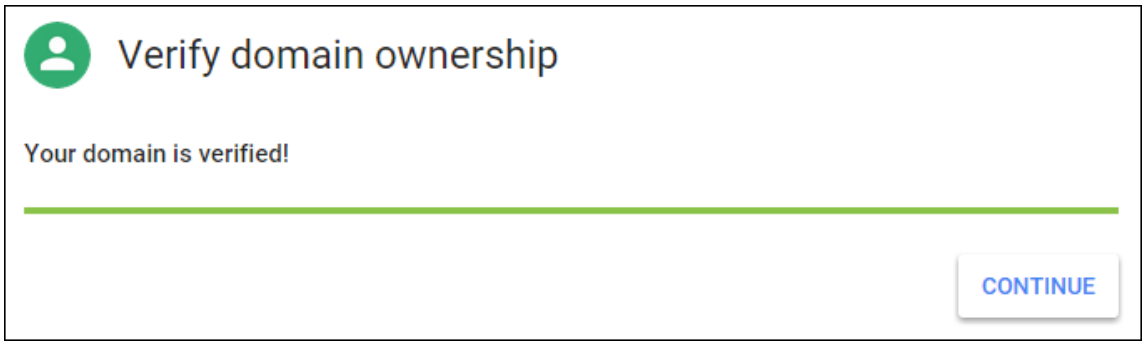
2. Click **Verify**.



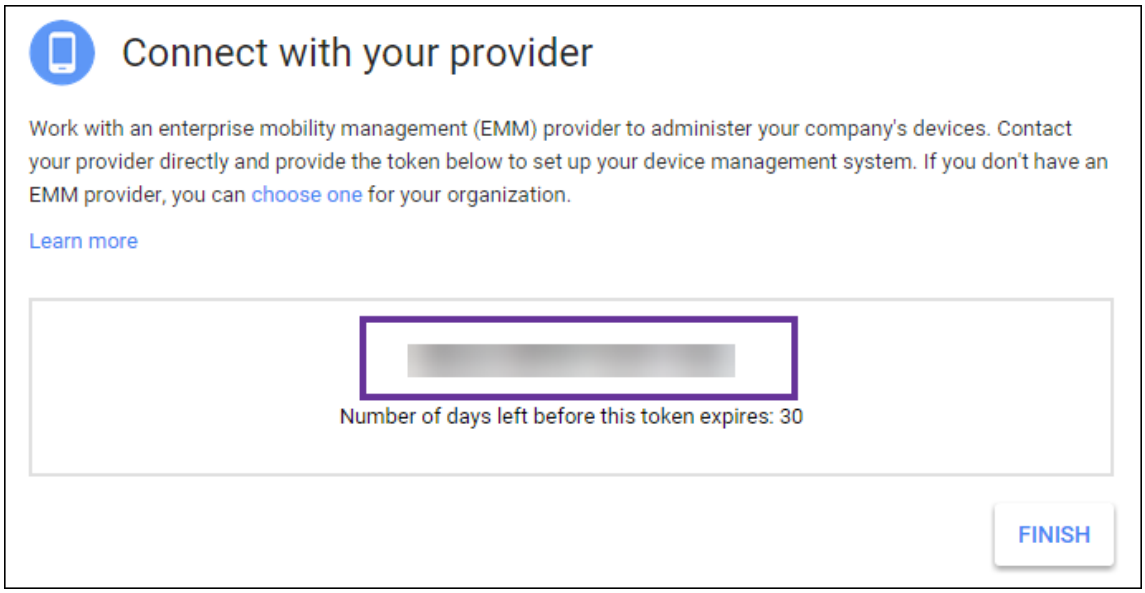
3. Google verifies your domain ownership.



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.



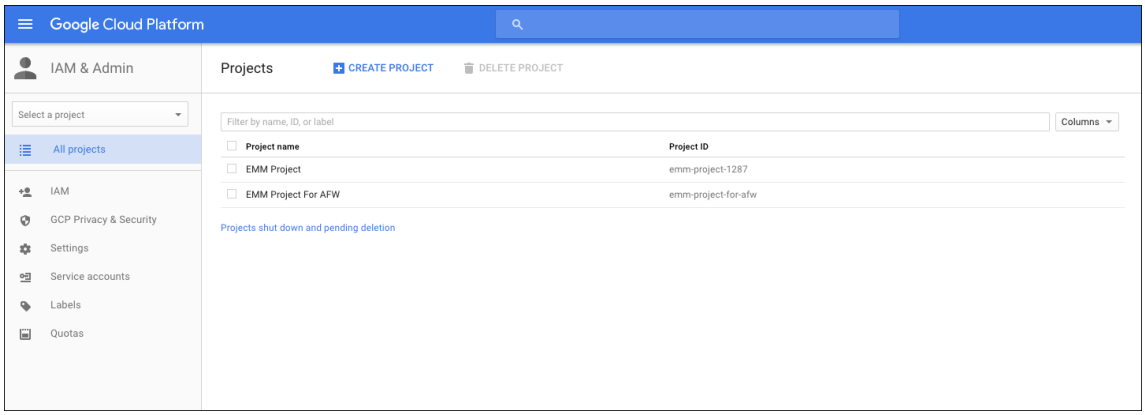
6. Click **Finish** to complete setting up Android Enterprise. A page appears, indicating that you've successfully verified your domain.

After you create an Android Enterprise service account, you can sign in to the Google Admin console to manage your mobility management settings.

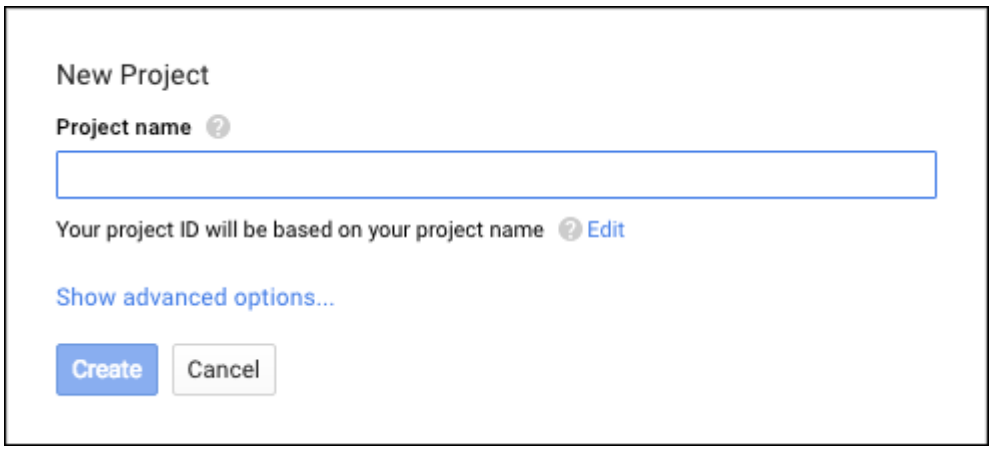
Set up an Android Enterprise service account and download an Android Enterprise certificate

To allow XenMobile 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 XenMobile and Google services for Android. For more information about the authentication protocol being used, go to https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

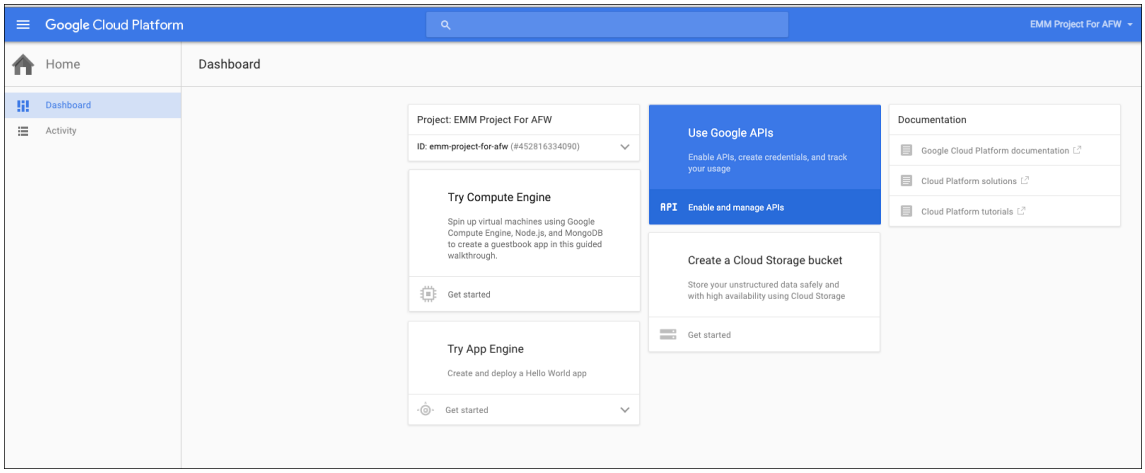
1. In a web browser, go to https://console.cloud.google.com/project and sign in with your Google administrator credentials
2. In the **Projects** list, click **Create Project.**



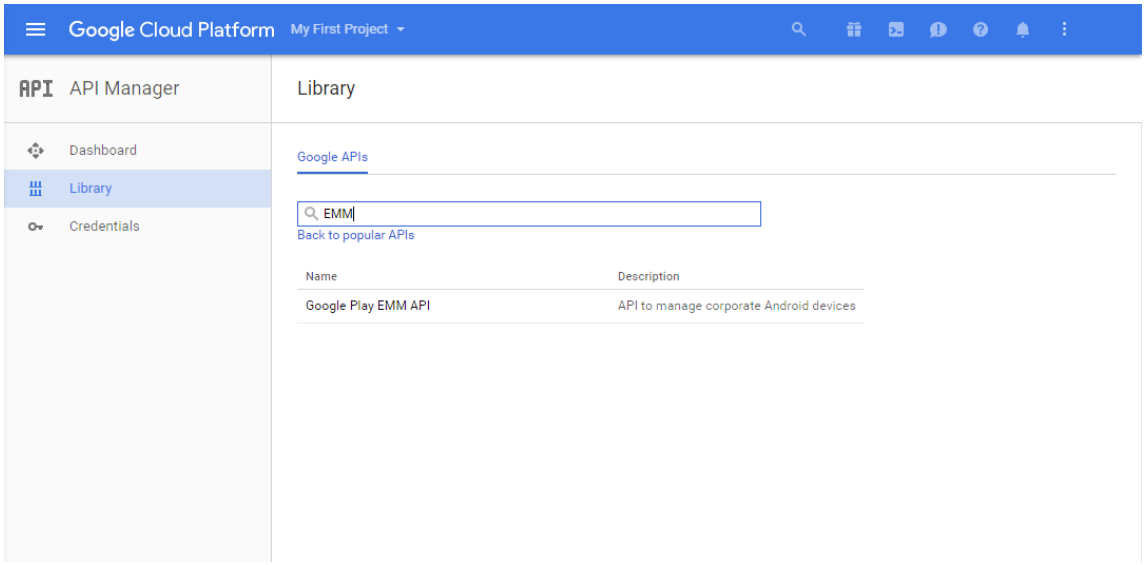
3. In **Project name**, type a name for the project.



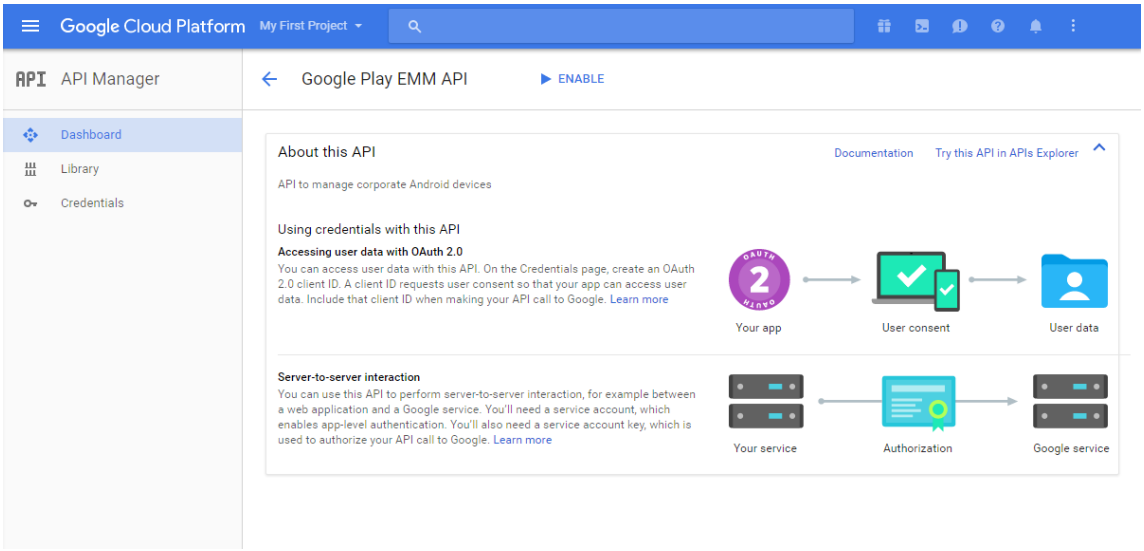
4. On the Dashboard, click **Use Google APIs**.



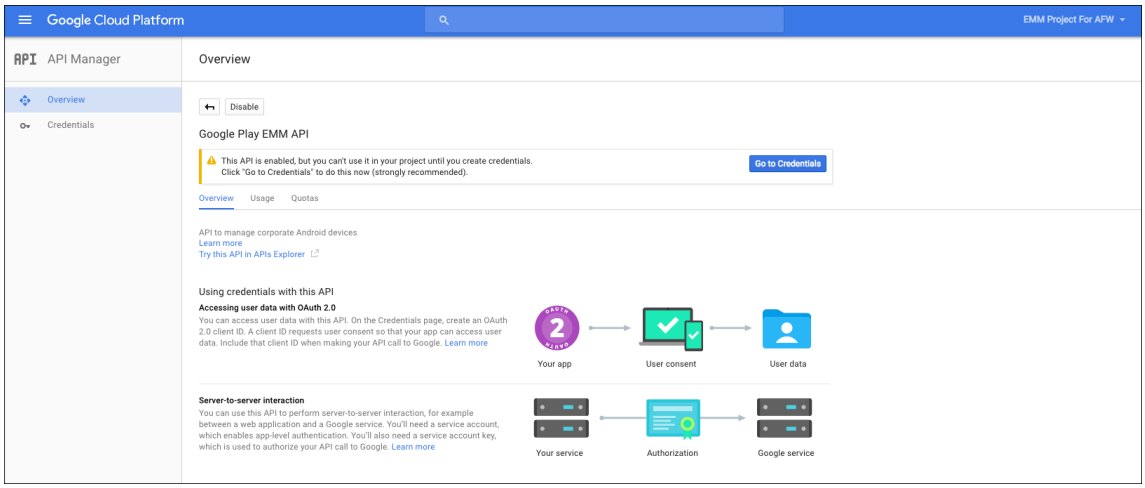
5. Click **Library**, in **Search**, type **EMM** and then click the search result.



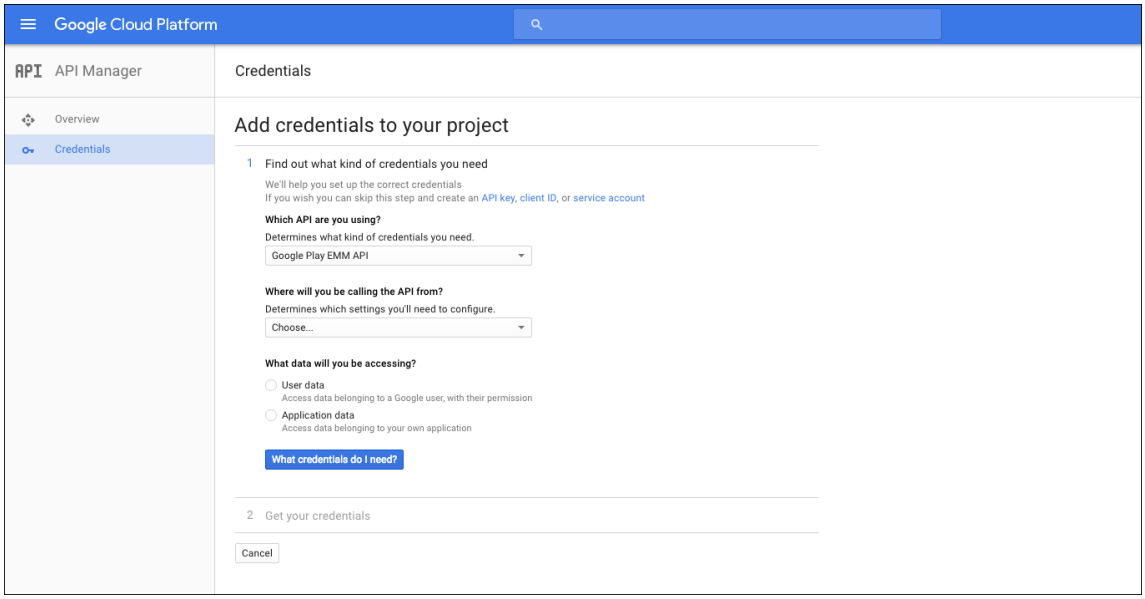
6. On the **Overview** page, click **Enable**.



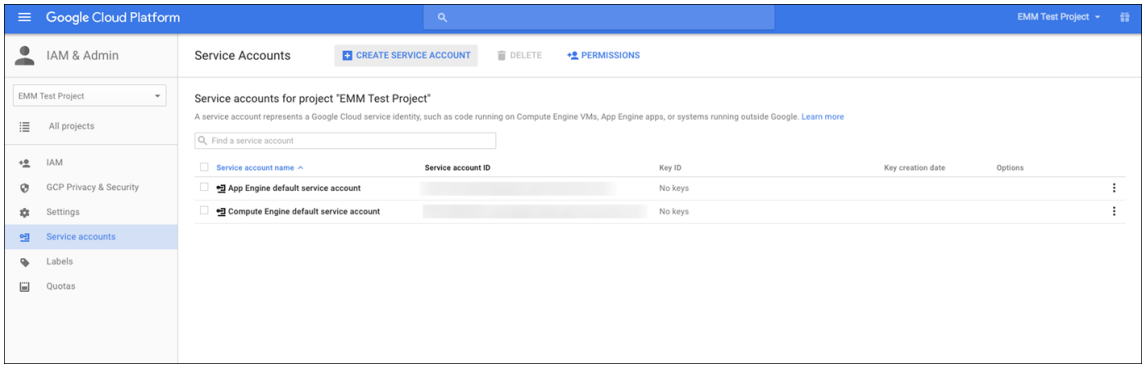
7. Next to **Google Play EMM API**, click **Go to Credentials**.



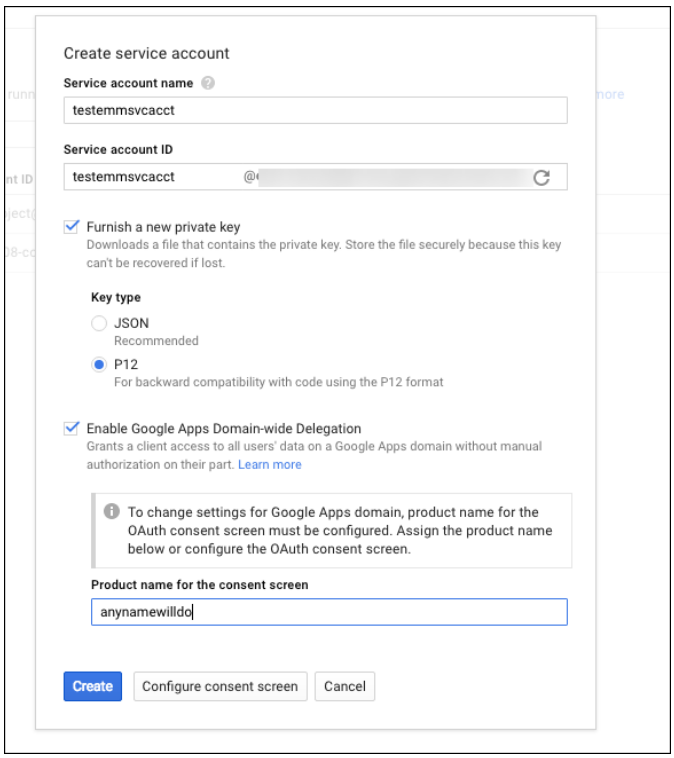
8. In the **Add credentials to our project** list, in step 1, click **service account**.



9. On the **Service Accounts** page, click **Create Service Account**.

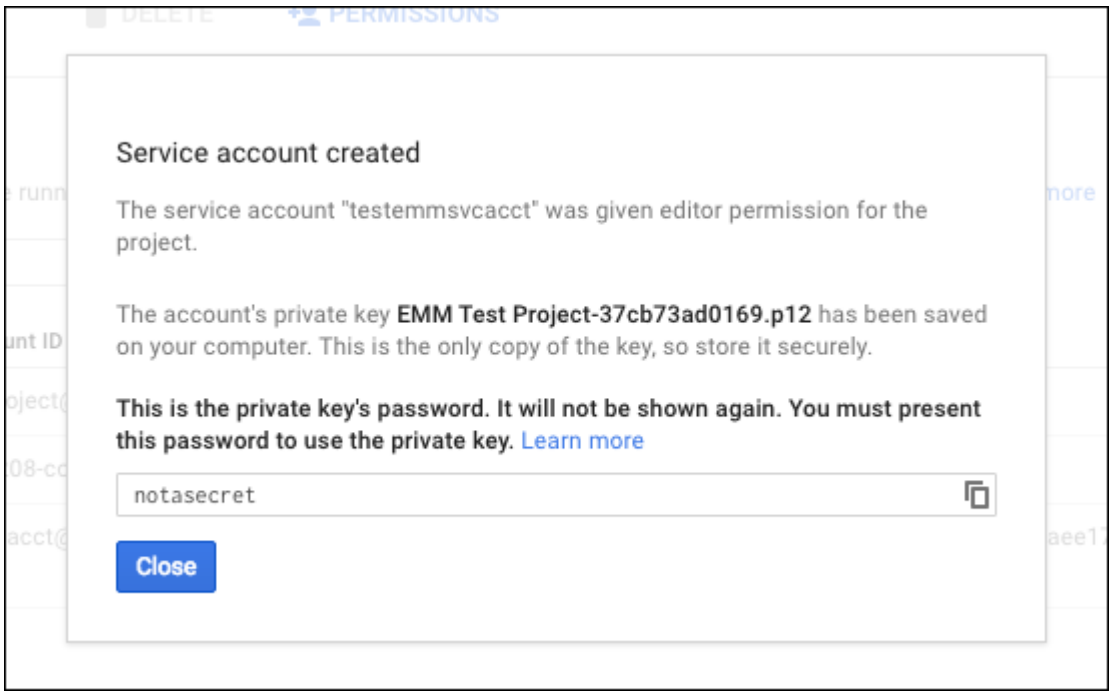


10. In **Create service account**, name the account, and select the **Furnish a new private key** check box. Click **P12**, select the **Enable Google Apps Domain-wide Delegation** check box and then click **Create.**

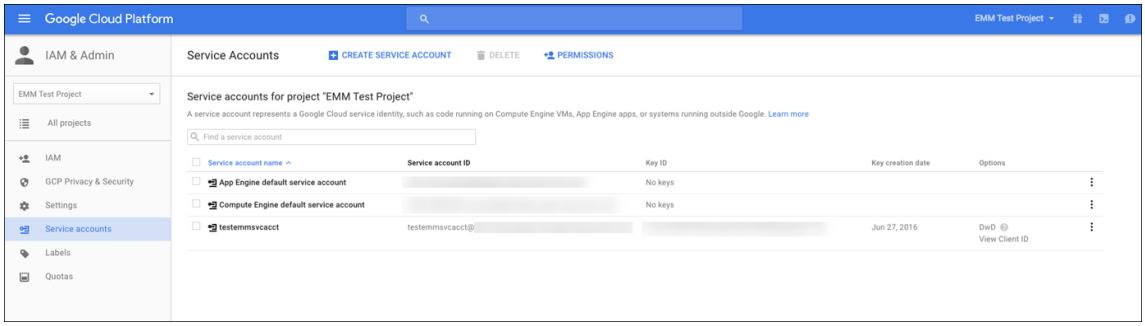


The certificate (P12 file) is downloaded to your computer. Be sure to save the certificate in a secure location.

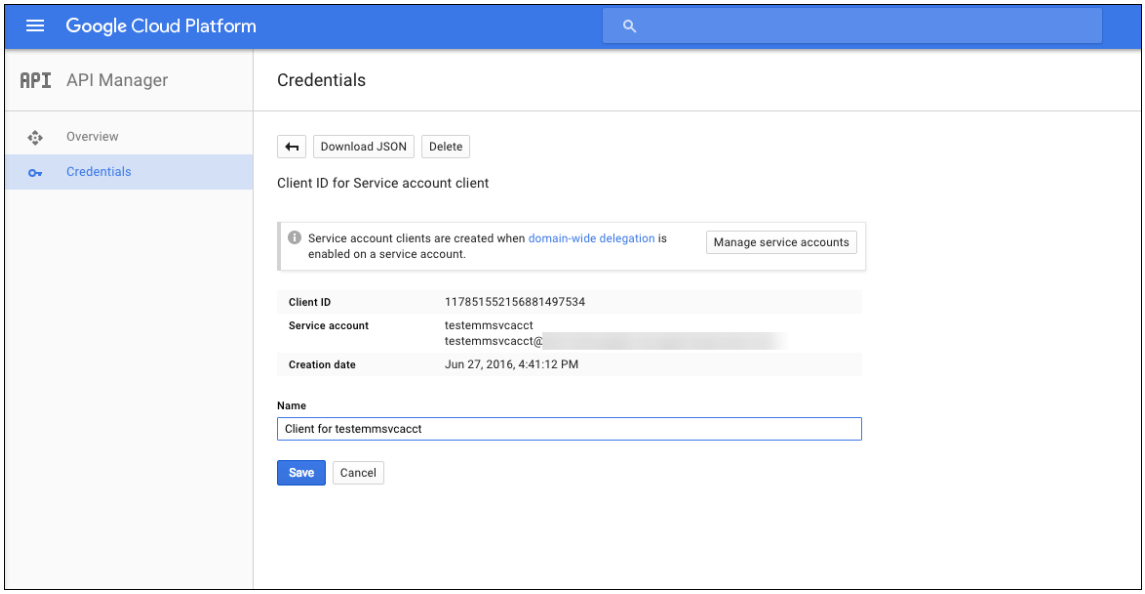
11. On the **Service account created** confirmation page, click **Close**.



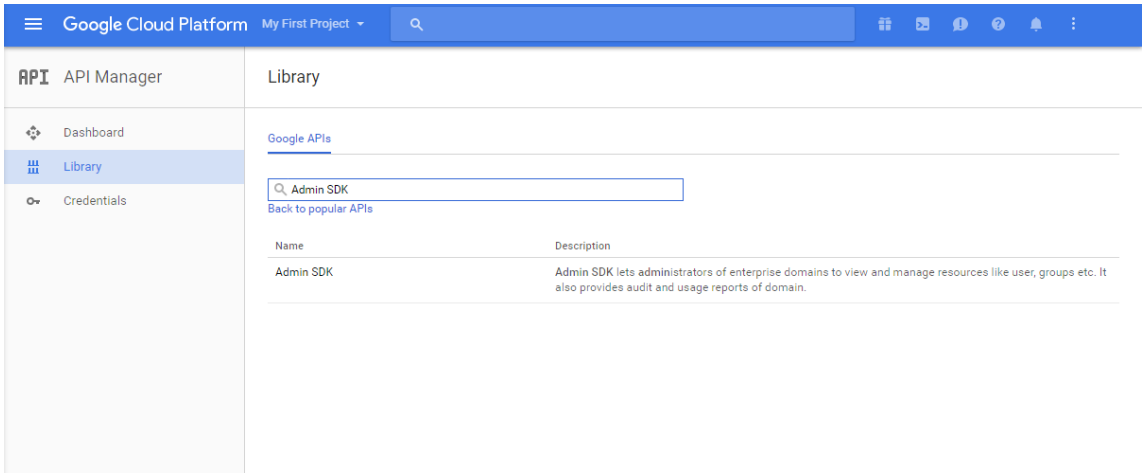
12. In **Permissions**, click **Service accounts** and then under **Options** for your service account, click **View Client ID**.



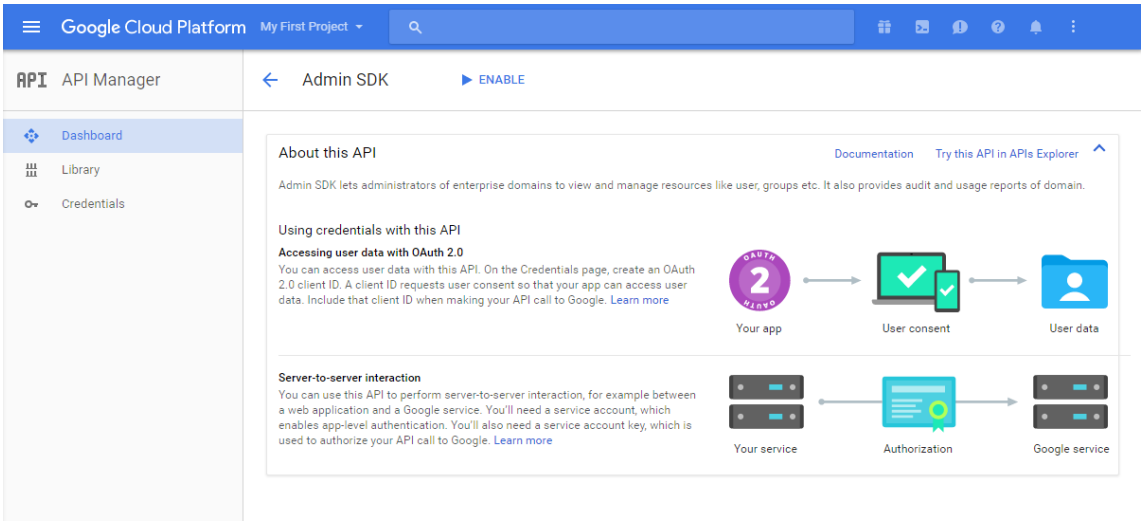
13. The details required for account authorization on the Google admin console display. Copy the **Client ID** and **Service account ID** to a location where you can retrieve the information later. You need this information, along with the domain name to send to Citrix support for allowing.



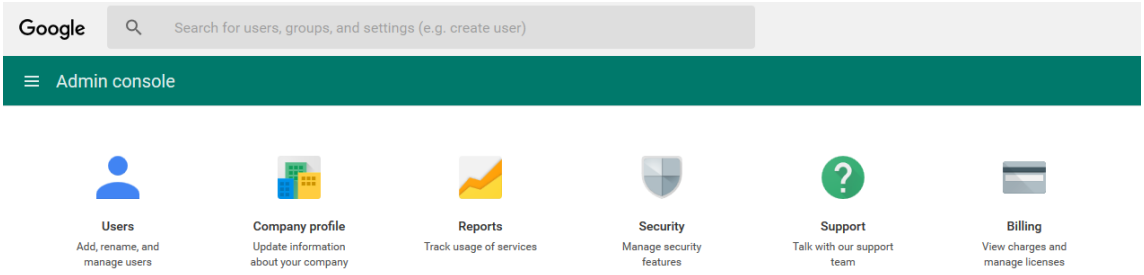
14. On the **Library** page, search for **Admin SDK** and then click the search result.



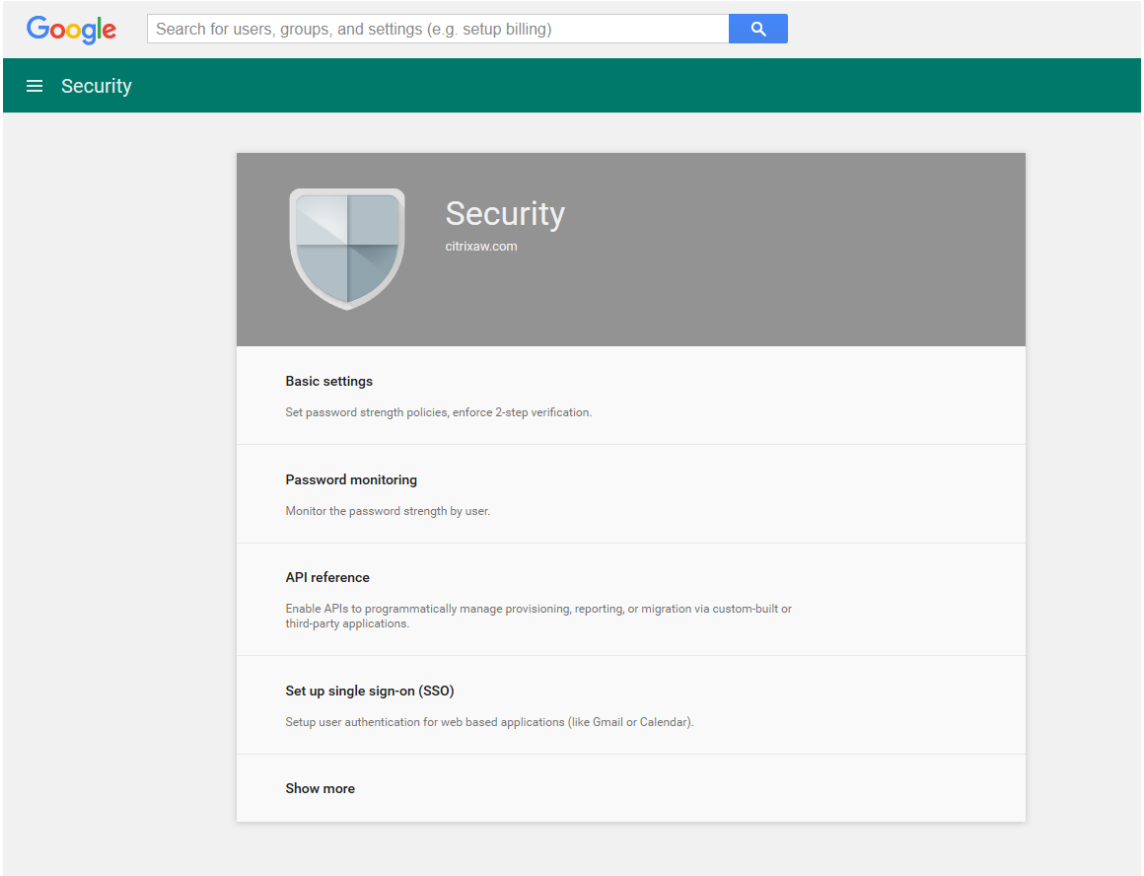
15. On the **Overview** page, click **Enable**.

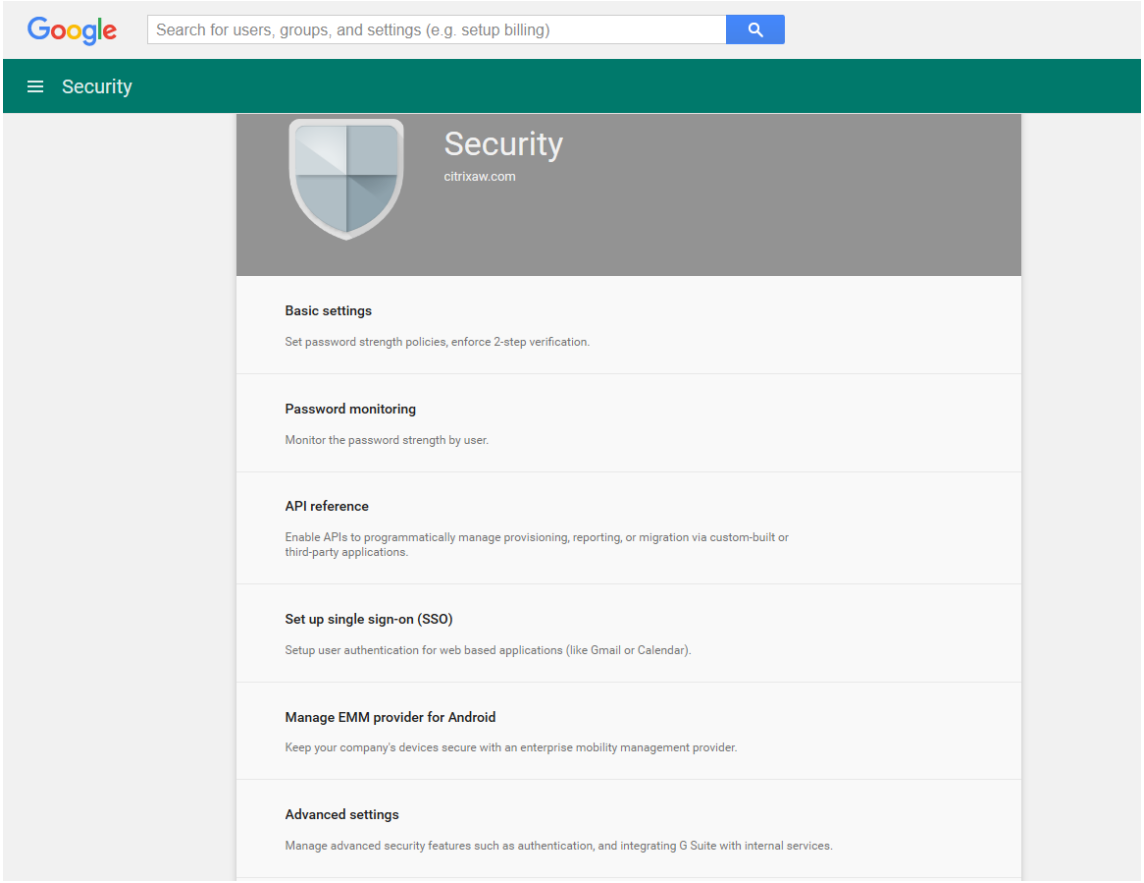


16. Open the Google admin console for your domain and then click **Security**.

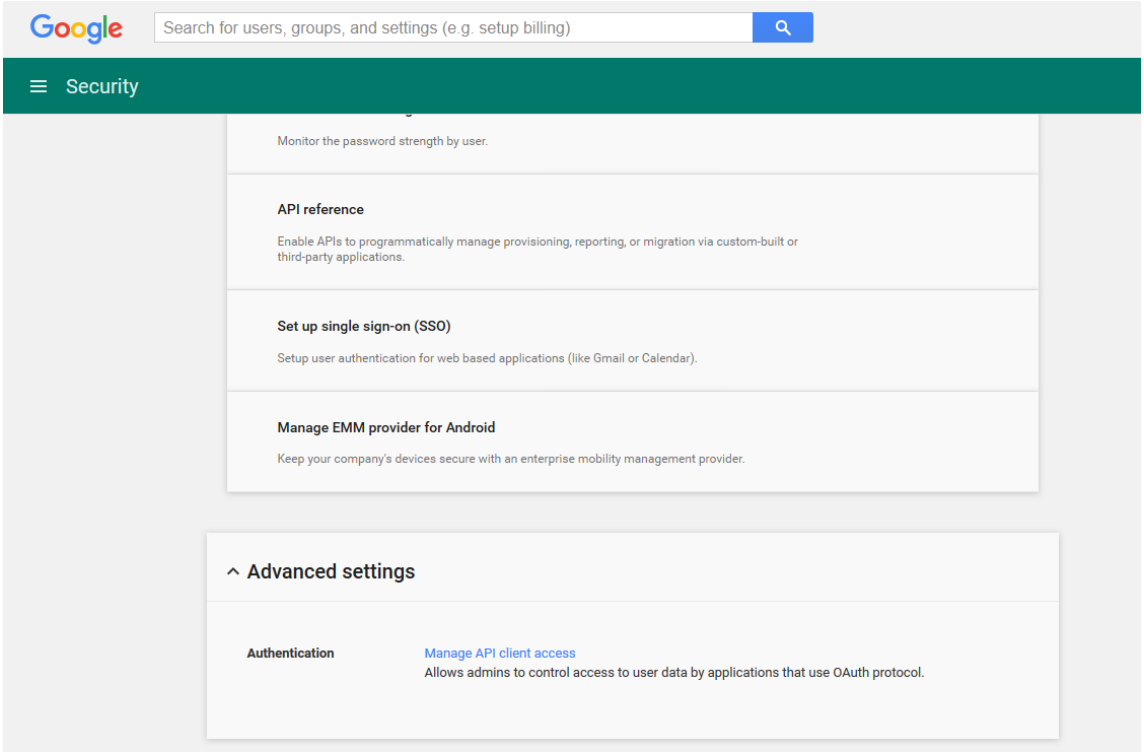


17. On the **Settings** page, click **Show more** and then click **Advanced settings**.

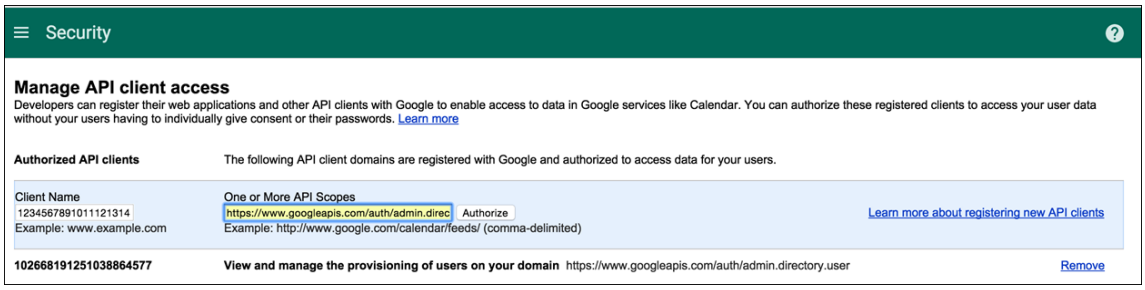




18. Click **Manage API client access**.



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**.



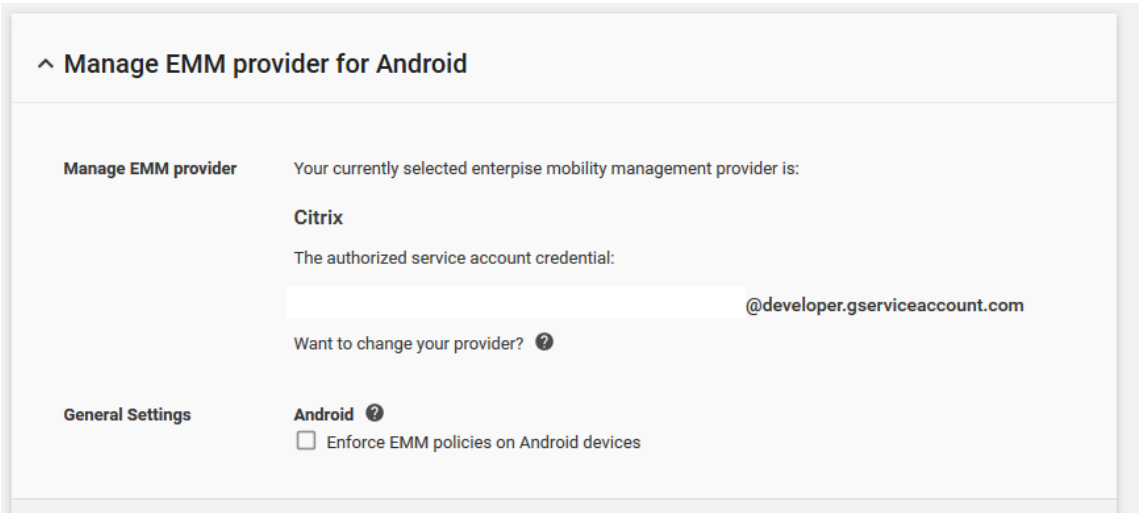
Binding to EMM

Before you can use XenMobile 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 XenMobile 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.

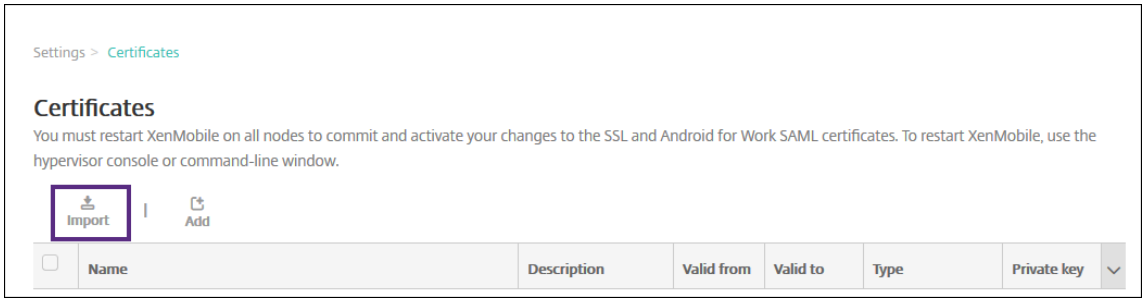
   After you confirm the token binding, you can start using the XenMobile console to manage your Android devices. Import the P12 certificate you generated in step 14. Set up Android Enterprise server settings, enable SAML-based single-sign-on (SSO), and define at least one Android Enterprise device policy.



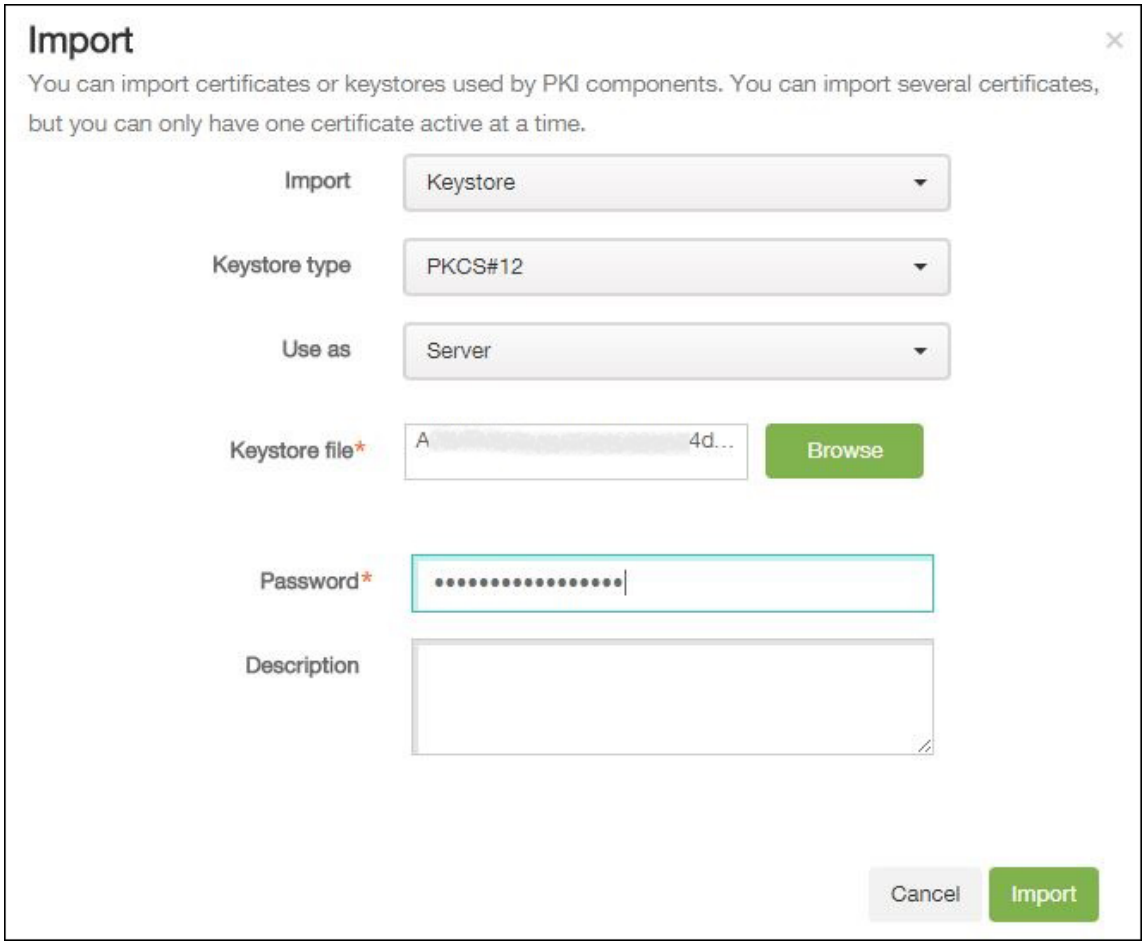
Import the P12 certificate

Follow these steps to import your Android Enterprise P12 certificate:

1. Sign in to the XenMobile console.
2. 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.



3. Click **Import**. The **Import** dialog box appears.



Configure the following settings:

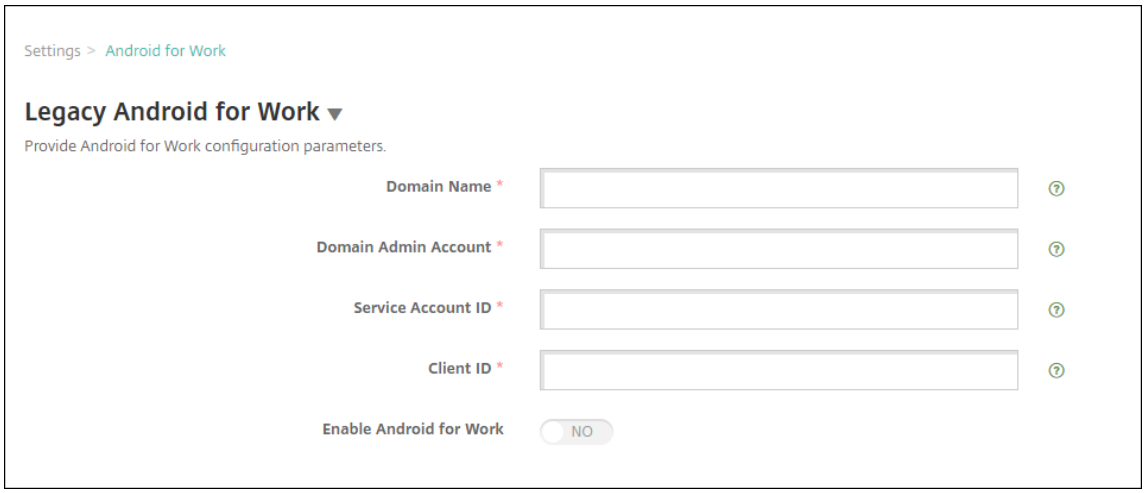
- **Import:** In the list, click **Keystore**.

- **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 keystore password.
- **Description:** Optionally, type a description of the certificate.

4. Click **Import**.

Set up Android Enterprise server settings

1. In the XenMobile console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Under **Server**, click **Android Enterprise**. The **Android Enterprise** page appears.



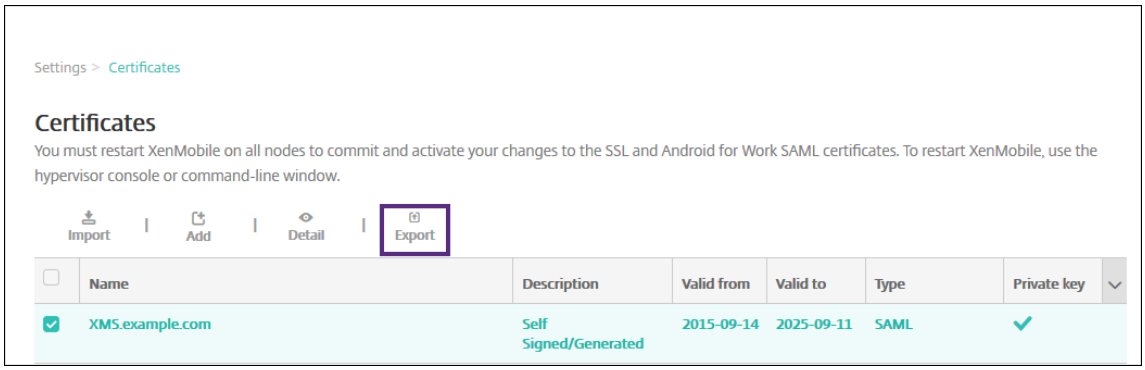
Configure the following settings and then click **Save.**

- **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.

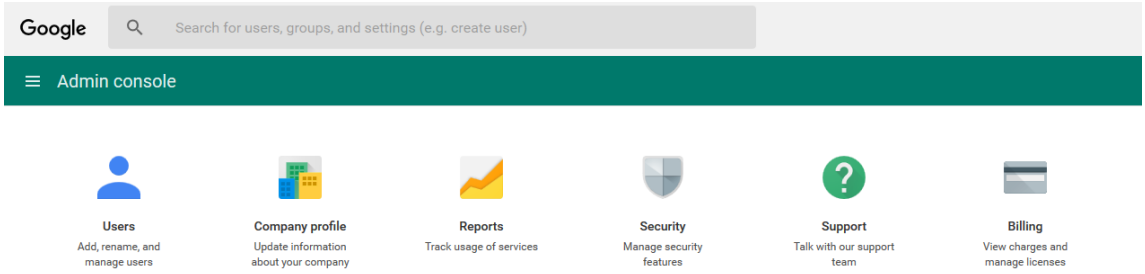
Enable SAML-based single-sign-on

1. Sign in to the XenMobile console.
2. Click the gear icon in the upper-right corner of the console. The **Settings** page appears.

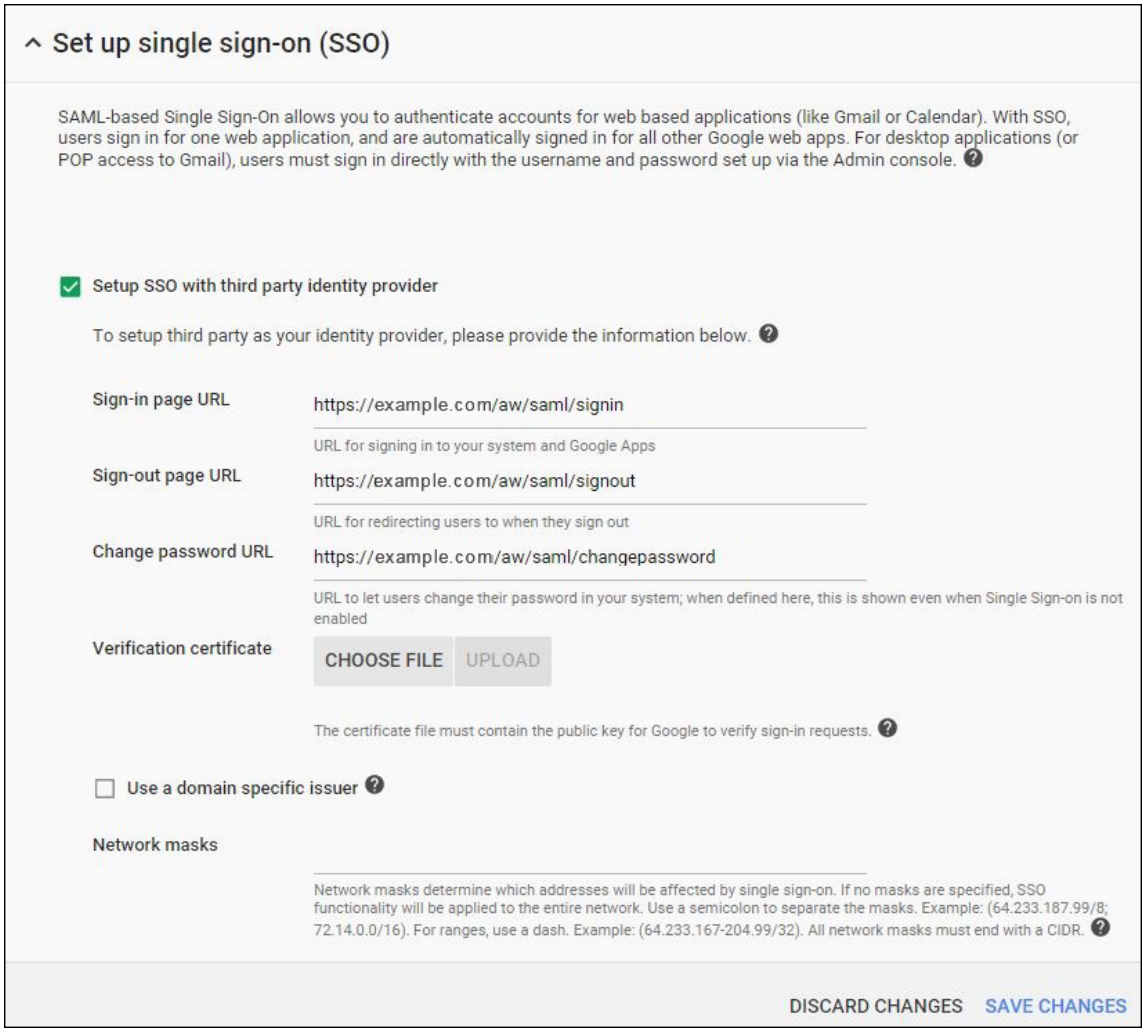
3. Click **Certificates**. The **Certificates** page appears.



4. In the list of certificates, click the SAML certificate.
5. Click **Export** and save the certificate to your computer.
6. Sign in to the Google Admin portal by using your Android Enterprise administrator credentials. For access to the portal, see Google Admin portal.
7. Click **Security**.



8. Under **Security**, click **Set up single sign-on (SSO)** and then configure the following settings.

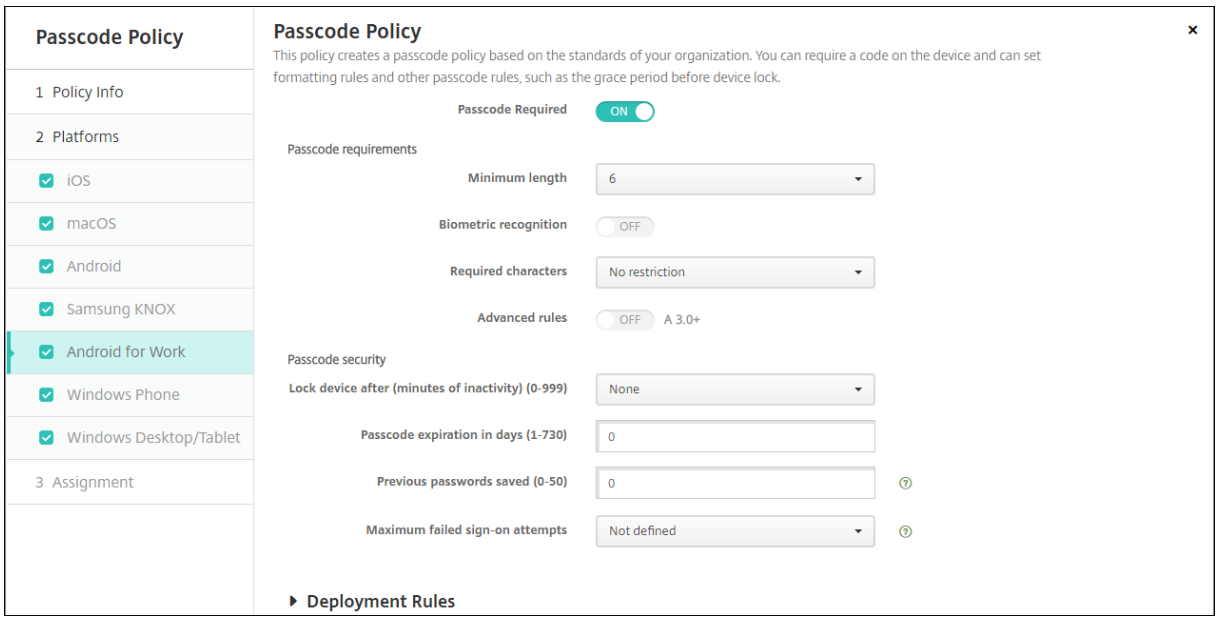


- **Sign-in page URL:** Type the URL for users signing in to your system and Google Apps. For example: `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **Sign out page URL:** Type the URL to which users are redirected when they sign out. For example: `https://<Xenmobile-FQDN>/aw/saml/signout`.
- **Change 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 XenMobile.

9. 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.



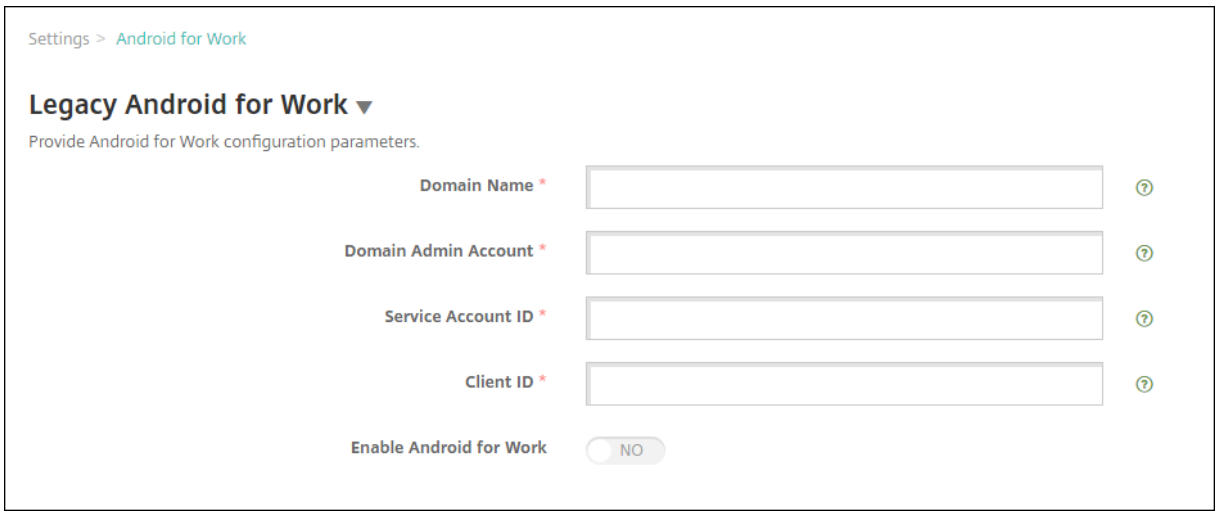
The basic steps to setting up any device policy are as follows.

1. Sign on to the XenMobile console.
2. Click **Configure**, and then click **Device Policies**.
3. 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**.
4. Complete the **Policy Information** page.
5. Click **Android Enterprise** and then configure the settings for the policy.
6. 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 XenMobile. 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 XenMobile web console, click the gear icon in the upper-right corner. The **Settings** page displays.
2. Under **Server**, click **Android Enterprise**. The **Android Enterprise** configuration page appears.



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 XenMobile

Some end-point management features for Chrome use Google partner APIs to communicate between XenMobile and your Google Workspace domain. For example, XenMobile 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 XenMobile console and then configure your Google Workspace account.

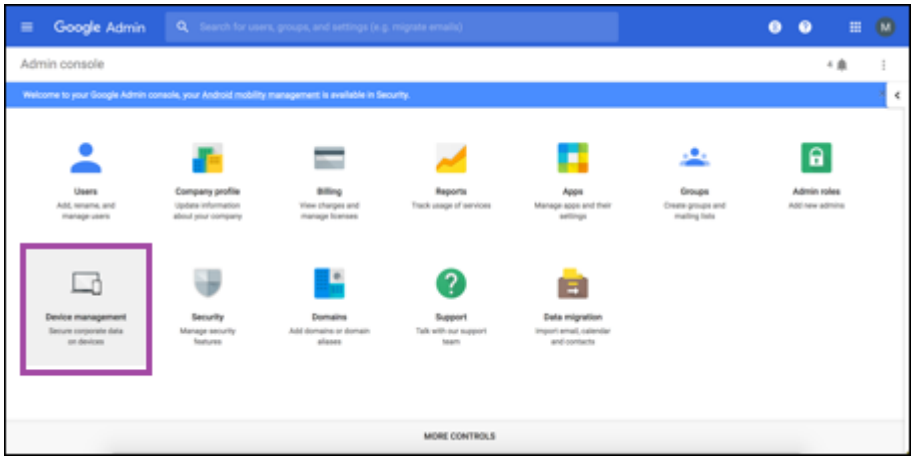
Set up your Google Workspace (formerly G Suite) domain in XenMobile

To enable XenMobile to communicate with the APIs in your Google Workspace domain, go to **Settings > Google Chrome Configuration** and configure the settings.

- **G Suite domain:** The Google Workspace domain that hosts the APIs needed by XenMobile.
- **G Suite admin account:** The administator account for your G Suite domain.
- **G Suite client ID:** The client ID for Citrix. Use this value to configure partner access for your Google Workspace domain.
- **G Suite enterprise ID:** The enterprise ID for your account, filled in from your Google enterprise account.

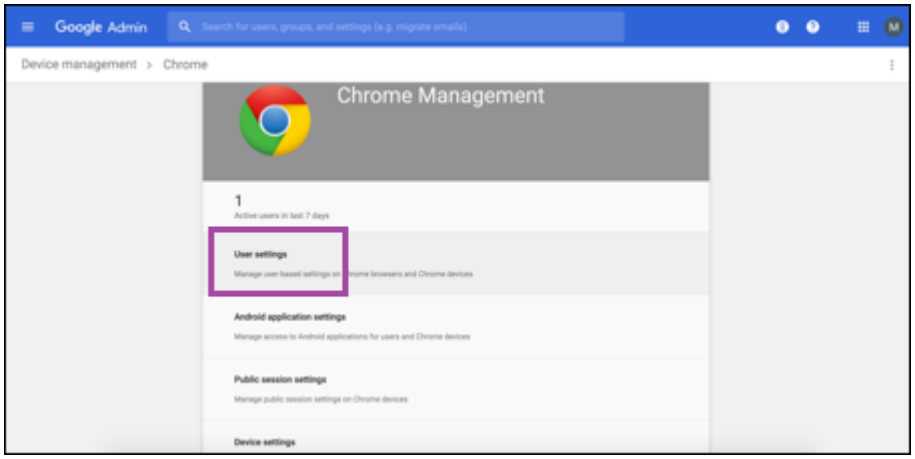
Enable partner access for devices and users in your Google Workspace domain

1. Log in into the Google admin console: https://admin.google.com
2. Click **Device Management**.



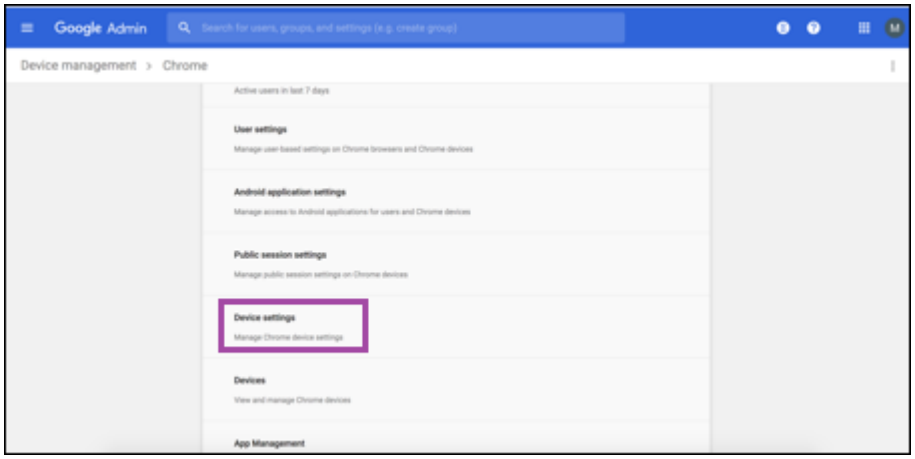
3. Click **Chrome management**.

4. Click **User settings**.

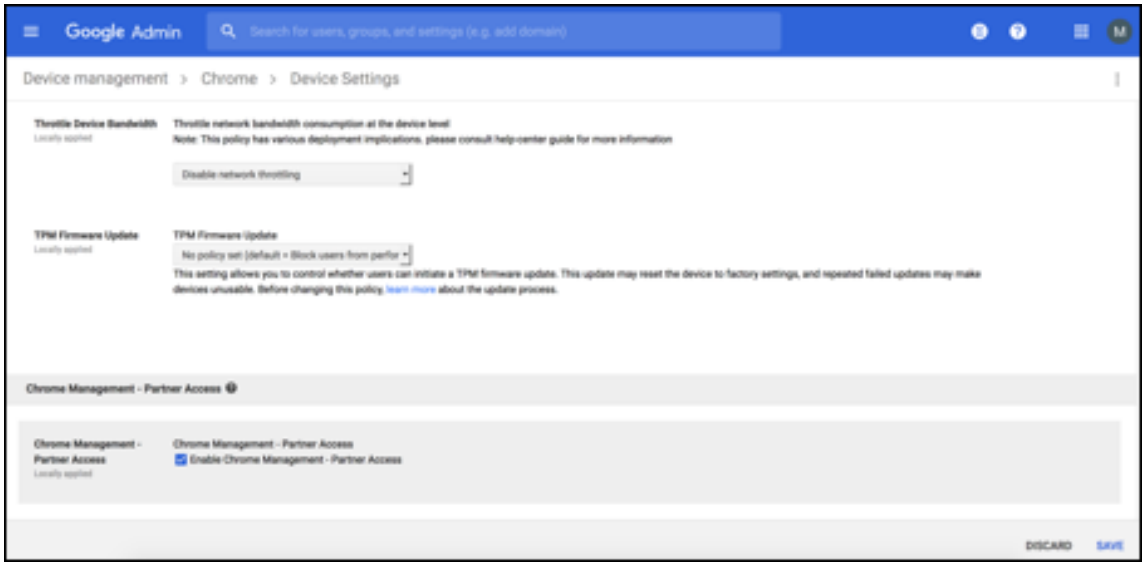


5. Search for **Chrome Management - Partner Access**.

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**.

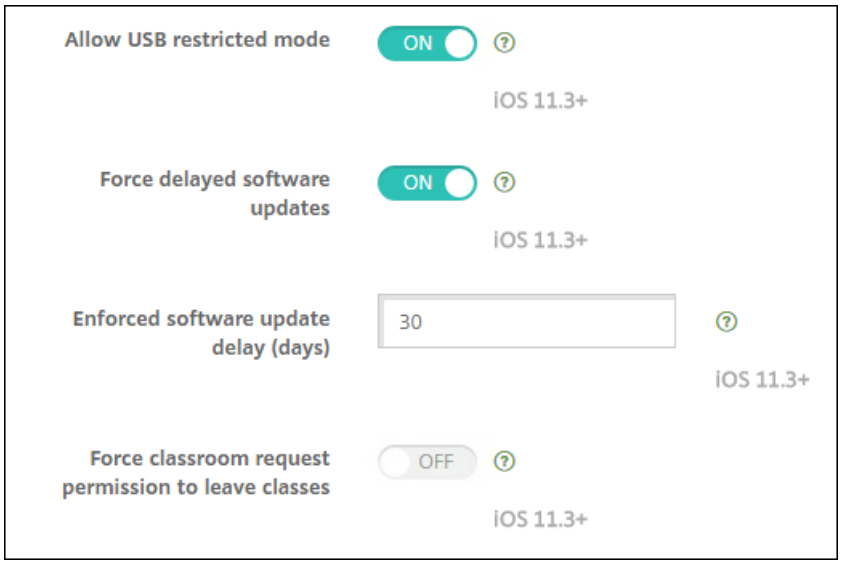


10. Select the **Enable Chrome Management - Partner Access** check box.
11. Agree that you understand and want to enable partner access. Click **Save**.
12. Go to the **Security** page and then click **Advanced Settings**.

13. Click **Manage API client Access**.
14. In the XenMobile console, go to **Settings > Google Chrome Configuration** and copy the value of Google Workspace 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 username or user ID, the format accepted depends on how the XenMobile server is configured to search for users by User Principal Name (UPN) or SAM account name.

If the XenMobile server is configured to search for users by UPN, users must enter a UPN in the format:

- *username@domain*

If the XenMobile 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 XenMobile server is configured for:

1. In the XenMobile 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**, XenMobile server is set for UPN.
    - If it is set to **sAMAccountName**, XenMobile server is set for SAM.

Unenrolling an Android Enterprise enterprise

You can unenroll an Android Enterprise enterprise using the XenMobile Server console and XenMobile Tools.

When you perform this task, the XenMobile Server opens a popup window for XenMobile Tools. Before you begin, ensure that the XenMobile 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 XenMobile site to the popup block 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.

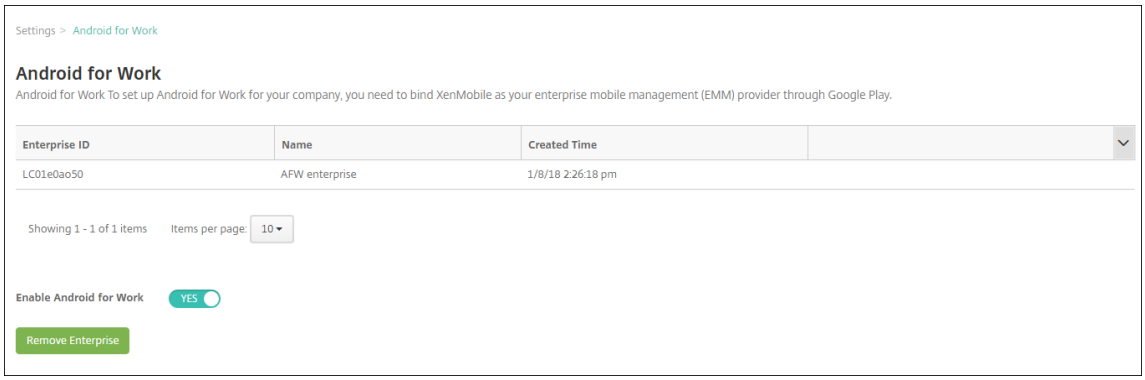
After the Android Enterprise enterprise is unenrolled:

- Devices and users enrolled through the enterprise have the Android Enterprise apps reset to their default state. Android Enterprise App Permissions and Android Enterprise App Restrictions policies previously applied no longer have an effect.
- Devices enrolled through the enterprise are managed by XenMobile, but are unmanaged from Google perspective. No new Android Enterprise apps can be added. No Android Enterprise App Permissions or Android Enterprise App Restrictions 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.

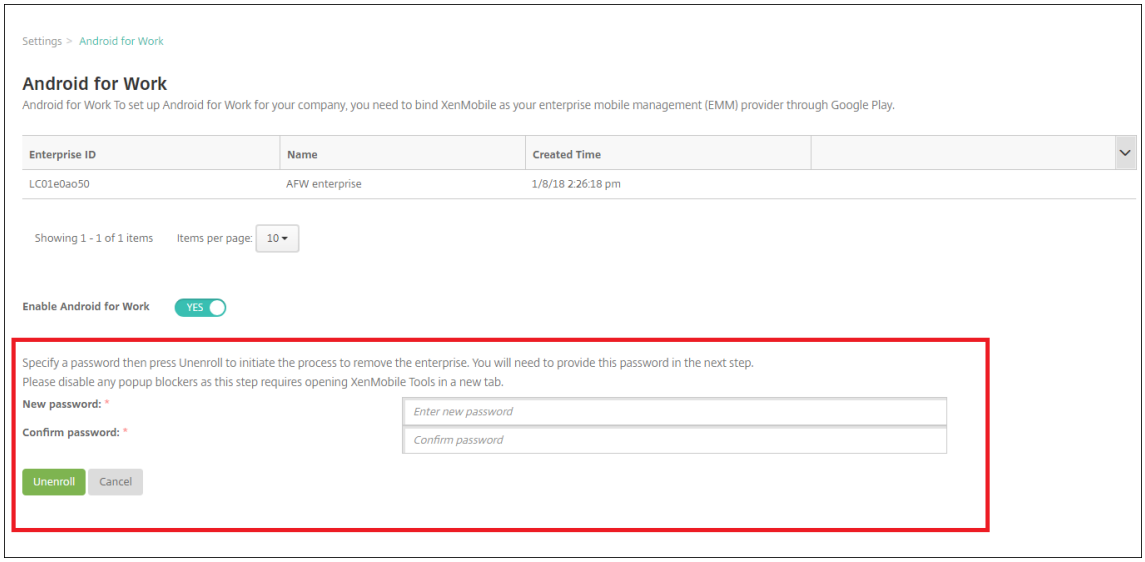
To unenroll an Android Enterprise enterprise:

1. In the XenMobile console, click the gear icon in the upper-right corner. The Settings page appears.
2. On the Settings page, click **Android Enterprise**.

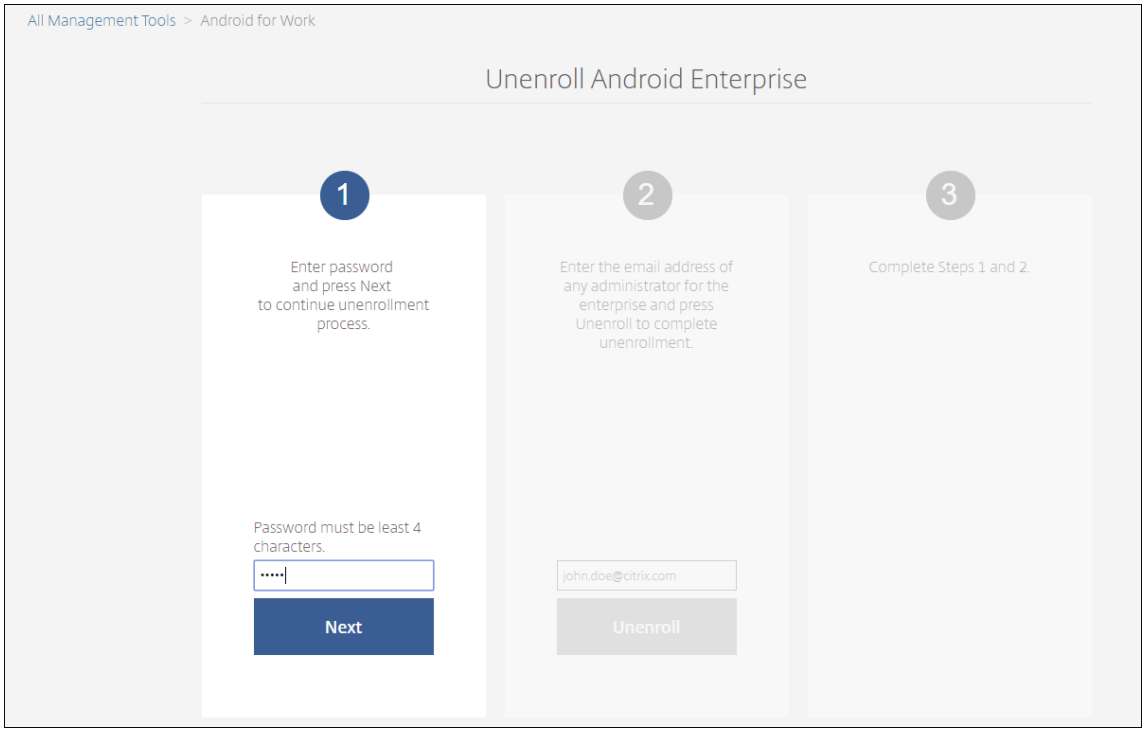
3. Click **Remove Enterprise**.



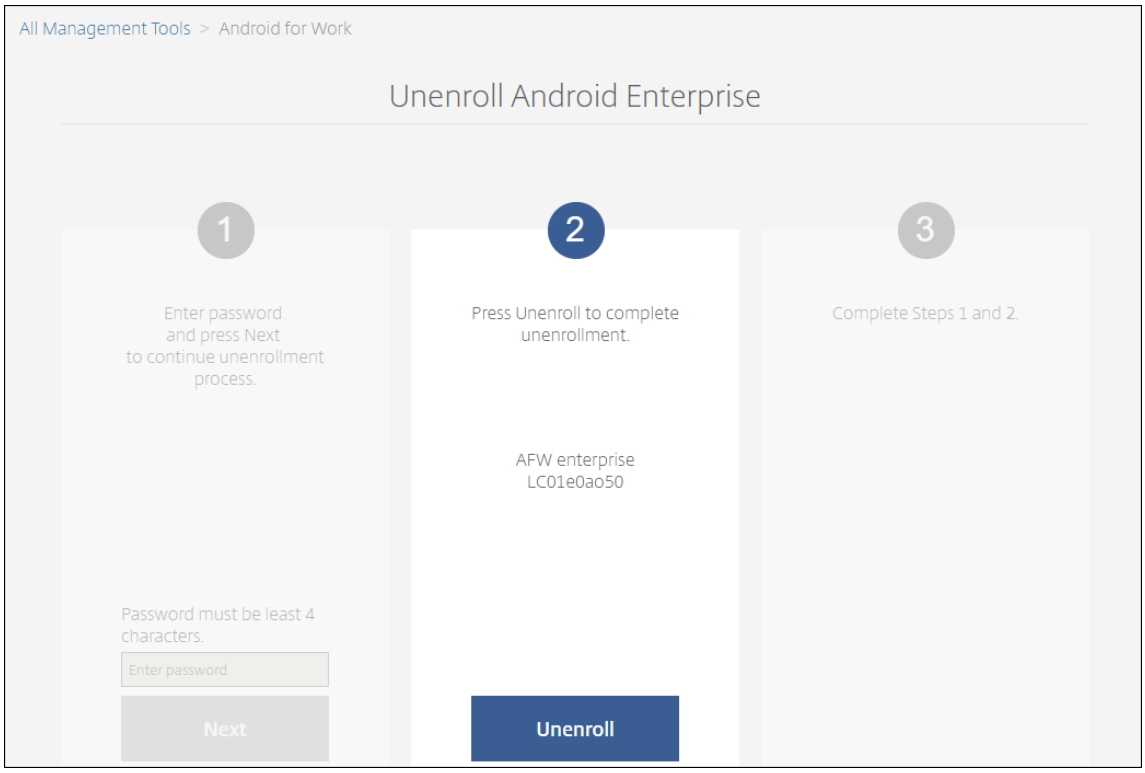
4. Specify a password. You'll need this for the next step to complete the unenrollment. Then click **Unenroll**.



5. When the XenMobile 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 fulll managed devices for 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.

XenMobile 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 XenMobile 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.

In 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 XenMobile server.

Prerequisites:

- Supported on all Android devices running Android 5.0 and above..

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://path/to/securehub.apk`

> **Note:**
>
> If Secure Hub is uploaded onto Citrix XenMobile server as an enterprise app, it can be downloaded from `https://<fqdn>:4443/*instanceName*/worxhome.apk`. The path to the Secure Hub APK must be accessible over the Wi-Fi connection that the device connects to during provisioning.

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.

  Enter an Olson name of the form area/location. For example, America/Los_Angeles for Pacific time. If you don't enter one, the time zone is automatically populated.

- **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": "                                                ",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "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, such as https://goqr.me.

This QR code gets scanned by a factory-reset device to enroll the device in work-managed device mode.

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, see this Google guide for Android EMM developers: https://developers.google.com/android/work/prov-devices#qr_code_method.

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 XenMobile Provisioning Tool.

Prerequisites:

- Supported on all Android devices running Android 5.0, Android 5.1, Android 6.0 and above.
- A XenMobile Server version 10.4 that is 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 10.4 or on the Citrix downloads page.

Each device can have only one Android Enterprise profile, managed by an enterprise mobility management (EMM) app. In XenMobile, 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

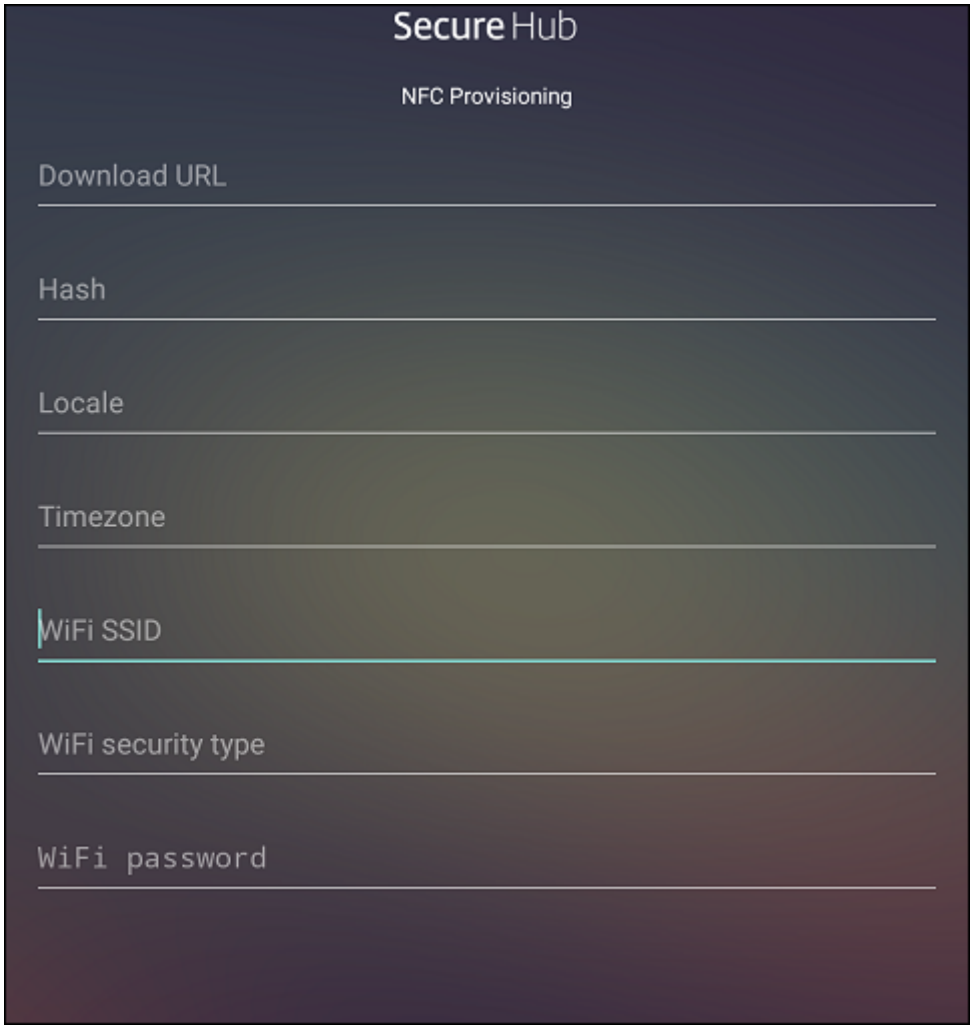
Provisioning a factory-reset device requires you to send the following data through an NFC bump to initialize Android Enterprise:

- 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.
- SHA1 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 XenMobile 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.



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=<SHA1 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 an Olson name of the form area/location. For example, America/Los_Angeles for Pacific time. If you don't enter a name, the time zone is automatically populated.

`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=ga50TwdCmfdJ72LGRFkke4Crb
\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=ga50TwdCmfdJ72LGRFkke4Cr
\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 Secure Hub checksum

To get the checksum of any app, add the app as an enterprise app.

1. In the XenMobile console, go to **Configure > Apps** and then click **Add**.

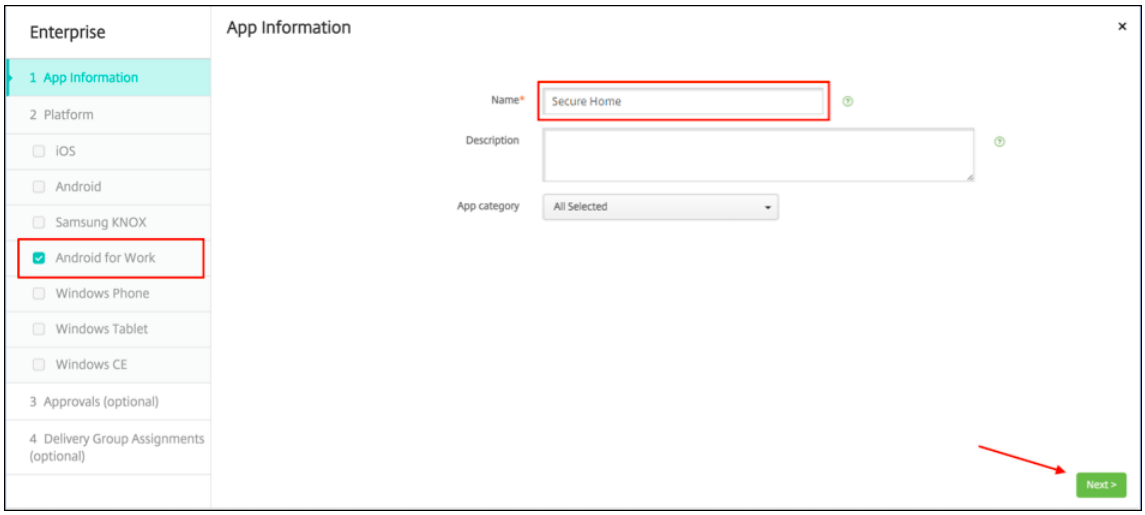
   The **Add Apps** window appears.

2. Click **Enterprise**.

   The **App information** page displays.

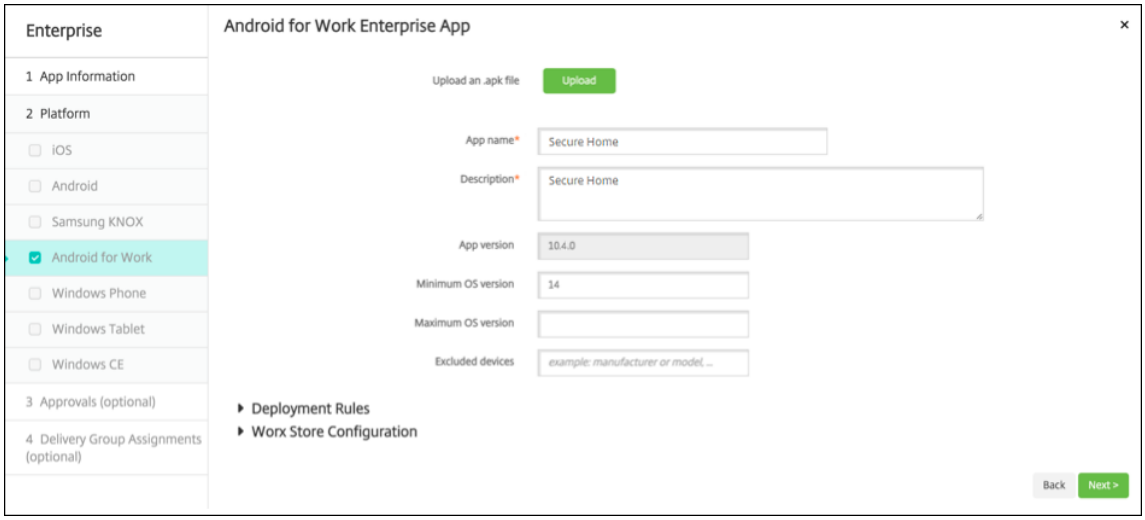
3. Select the following configuration and then click **Next**.

   The **Android Enterprise Enterprise App** page appears.



4. Provide the path to the .apk and then click **Next** to upload the file.

   Once the upload is complete, the details of the uploaded package appear.



5. Click **Next** to open page to download the JSON file, which you then use to upload to Google Play. For Secure Hub, uploading to Google Play is not required, but you need the JSON file to read the SHA1 value from it.

   A typical JSON file looks like the following:

6. Copy the **file_sha1_base64 value** and use it in the **Hash** field in the Provisioning Tool.

   > **Note:**
   >
   > The hash must be URL safe.

   - Convert any **+** symbols to **-**
   - Convert any **/** symbols to **_**
   - Replace the trailing **\u003d** with **=**

   If you store the hash in the nfcprovisioning.txt file on the SD card of the device, the app does the safety conversion. However, if you opt to type the hash manually, it's your responsibility to ensure its URL safety.

Libraries used

The Provisioning Tool uses the following libraries in its source code:

- v7 appcompat library, Design support library, and v7 Palette 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

Provision work profile device in Android Enterprise

On work profile devices in Android Enterprise, 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 XenMobile. 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.

iOS

April 14, 2021

To manage iOS devices in XenMobile Server, 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 MDM. XenMobile Server supports the following authentication types for iOS devices in MDM+MAM. For information, see the articles under Certificates and authentication.

- Domain
- Domain plus security token
- Client certificate
- Client certificate plus domain

> **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 Uploading certificates in XenMobile Server.

For supported operating systems, see Supported device operating systems.

iOS 14 compatibility

XenMobile Server 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 delay software upgrades for up to 90 days. In the Restrictions device policy for iOS, use these settings:

- **Force delayed software updates**
- **Enforced software update delay**

See iOS settings. Those settings aren't available for devices in user enrollment mode or unsupervised (full MDM) mode.

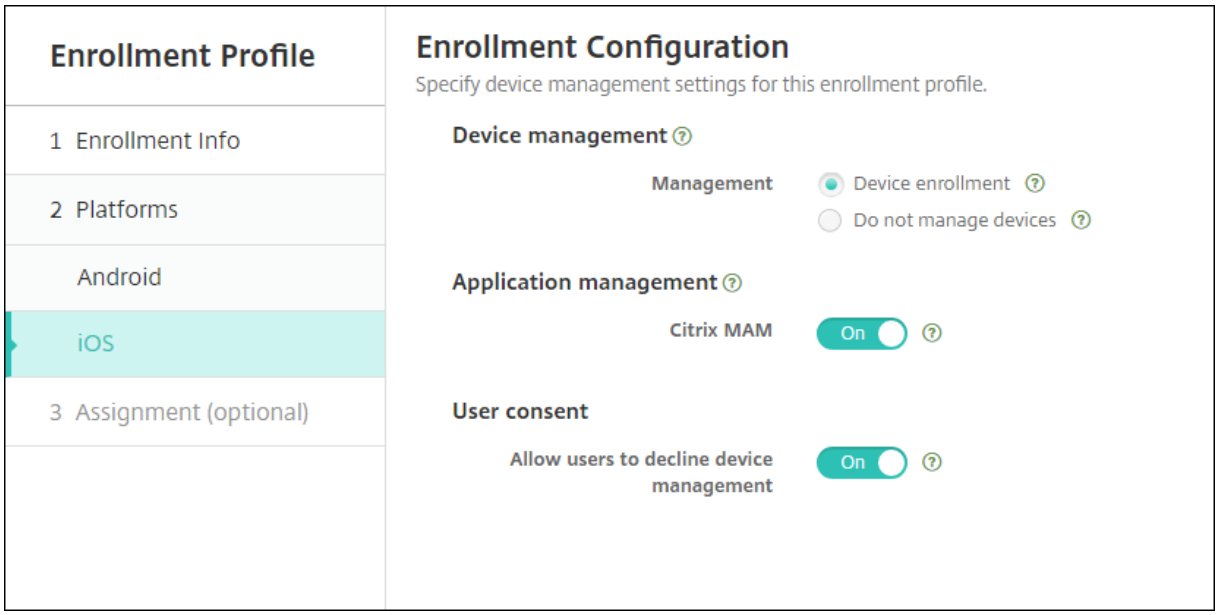
Apple host names that must remain open

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 device enrollment or no MDM enrollment.

To configure enrollment settings for iOS devices, go to **Configure > Enrollment Profiles > iOS**.



The following table lists which enrollment methods XenMobile Server supports for iOS devices:

Method	Supported
Apple Deployment Program	Yes
Apple School Manager	Yes
Apple Configurator	Yes
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 XenMobile Server. That program is for iOS and macOS devices. See Deploy devices through Apple Deployment Program.

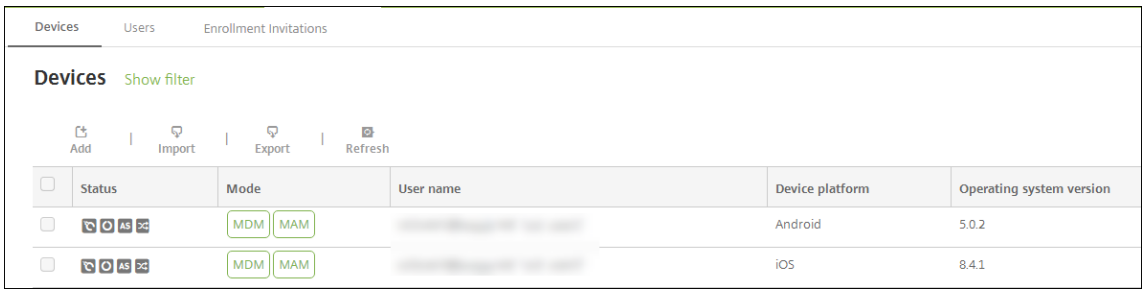
For education accounts, you create an Apple School Manager account. Apple School Manager unifies the Deployment Program and volume purchase. Apple School Manager is a type of Education Apple Deployment Program. See Integrate with Apple Education features.

You can use the Apple Deployment Program to bulk enroll iOS and macOS devices. You can purchase 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 Bulk enrollment of Apple devices.

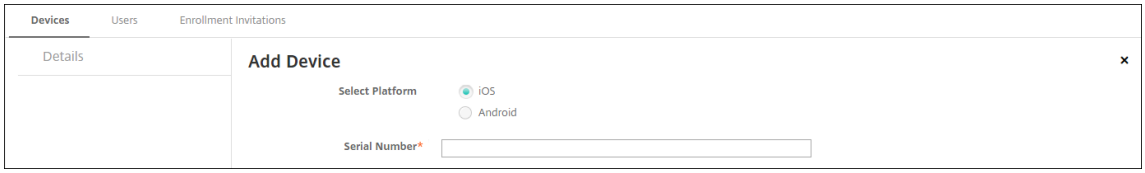
Add an iOS device manually

If you want to add an iOS device manually, such as for testing purposes, follow these steps.

1. In the XenMobile Server console, click **Manage > Devices**. The **Devices** page appears.



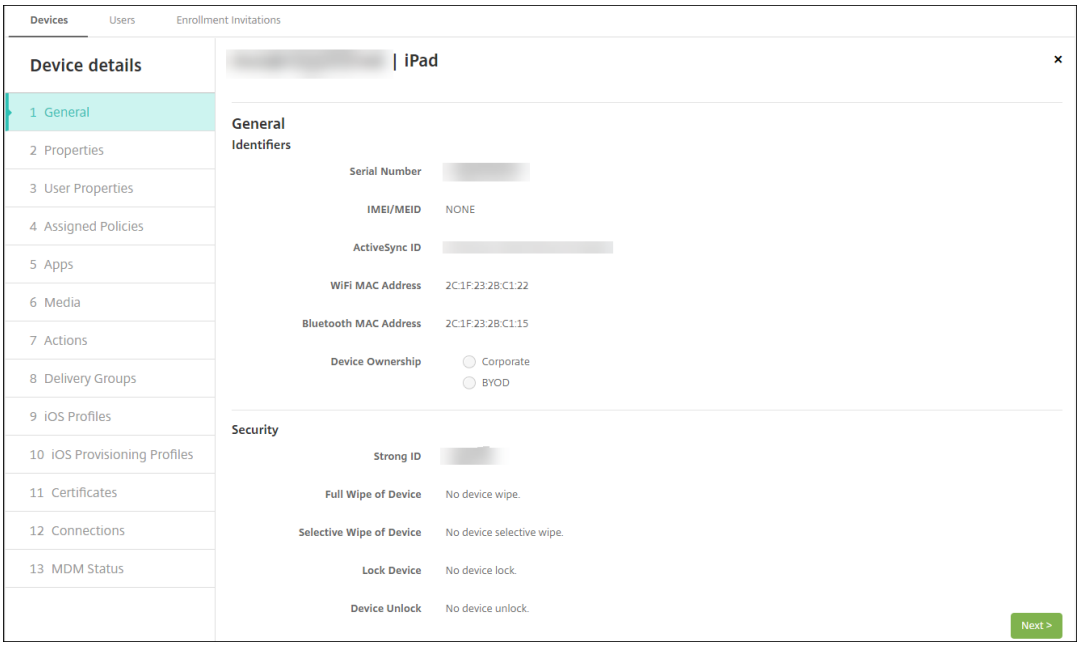
2. Click **Add**. The **Add Device** page appears.



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. 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 XenMobile Server 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. XenMobile Server deletes the item immediately.

7. The remaining **Device Details** sections contain summary information 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 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, 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.

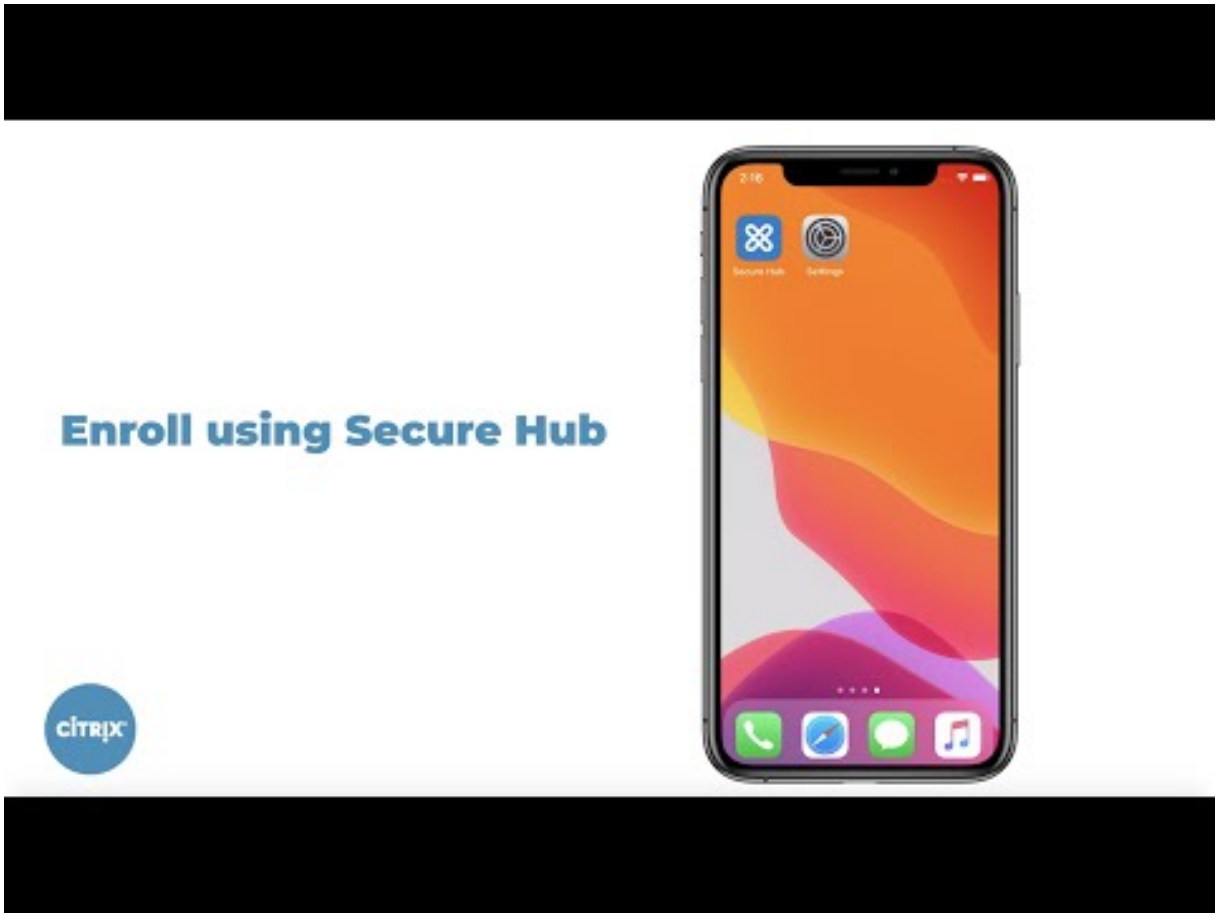
Configure iOS device policies

Use these policies to configure how XenMobile Server interacts with devices running iOS. This table lists all device policies available for iOS devices.

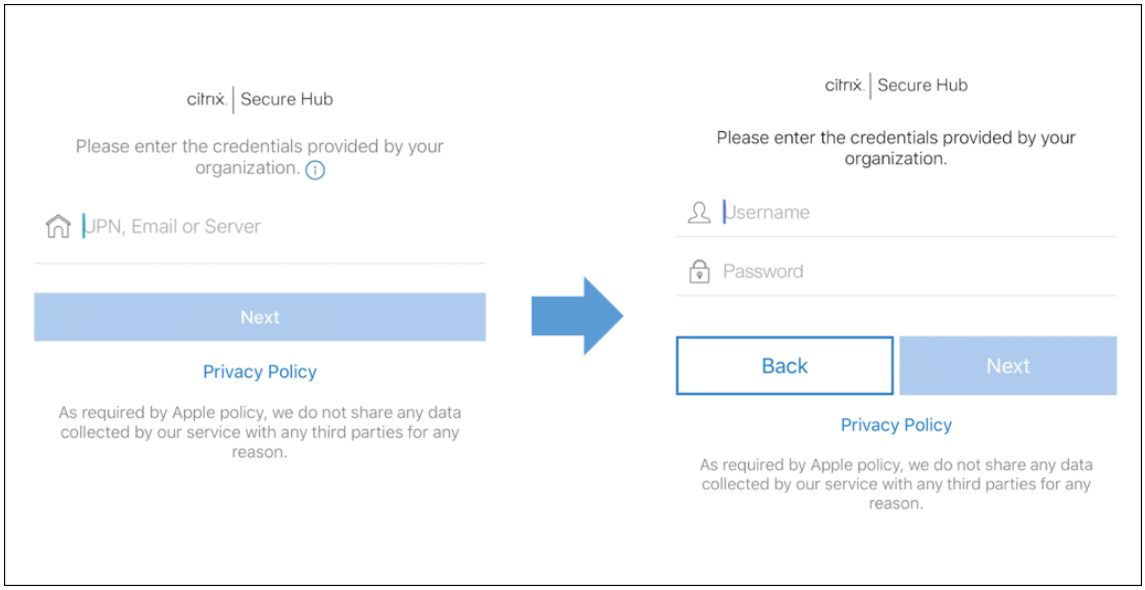
AirPlay Mirroring	AirPrint	APN
App Access	App Attributes	App Configuration
App Inventory	App Lock	App Network Usage
App Uninstall	Apps Notifications	Calendar (CalDAV)
Cellular	Contacts (CardDAV)	Control OS Update
Credentials	Device Name	Education Configuration
Exchange	Font	Home Screen Layout
Import iOS & macOS Profile	LDAP	Location
Mail	Managed Domains	MDM Options
Organization Info	Passcode	Personal Hotspot
Profile Removal	Provisioning Profile	Provisioning Profile Removal
Proxy	Restrictions	Roaming
SCEP	Shared iPad - Maximum Resident Users	Shared iPad - Passcode Lock Grace Period
SSO Account	Store	Subscribed Calendars
Terms & Conditions	VPN	Wallpaper
Web Content Filter	Webclip	WiFi

Enroll iOS devices

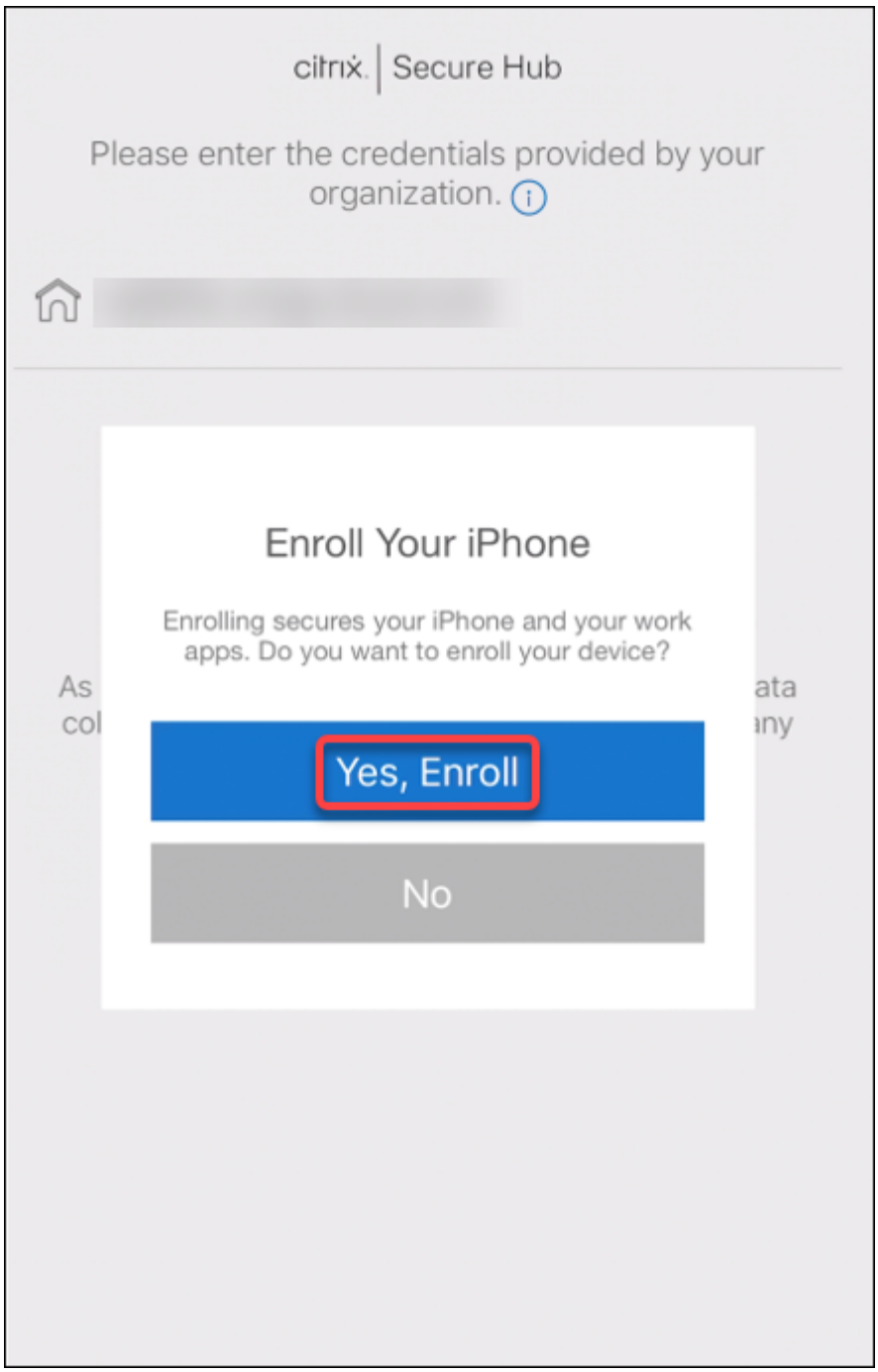
This section shows how users enroll iOS devices (12.2 or later) into XenMobile Server. For more information about the iOS enrollment, open the following video:



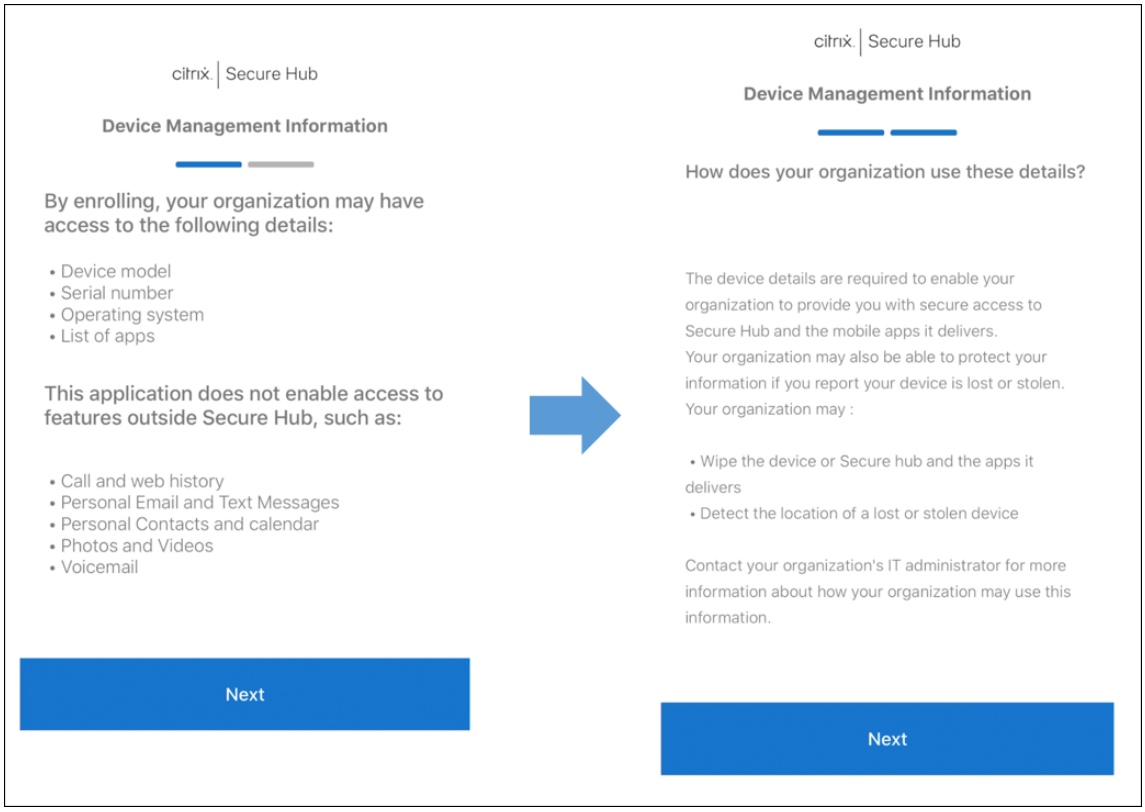
1. Go to the Apple store on your iOS device, download the Citrix Secure Hub app, and then tap the app.
2. When prompted to install the app, tap **Next** and then tap **Install**.
3. After Secure Hub installs, tap **Open**.
4. Enter your corporate credentials, such as your XenMobile Server server name, User Principal Name (UPN), or email address. Then, click **Next**.



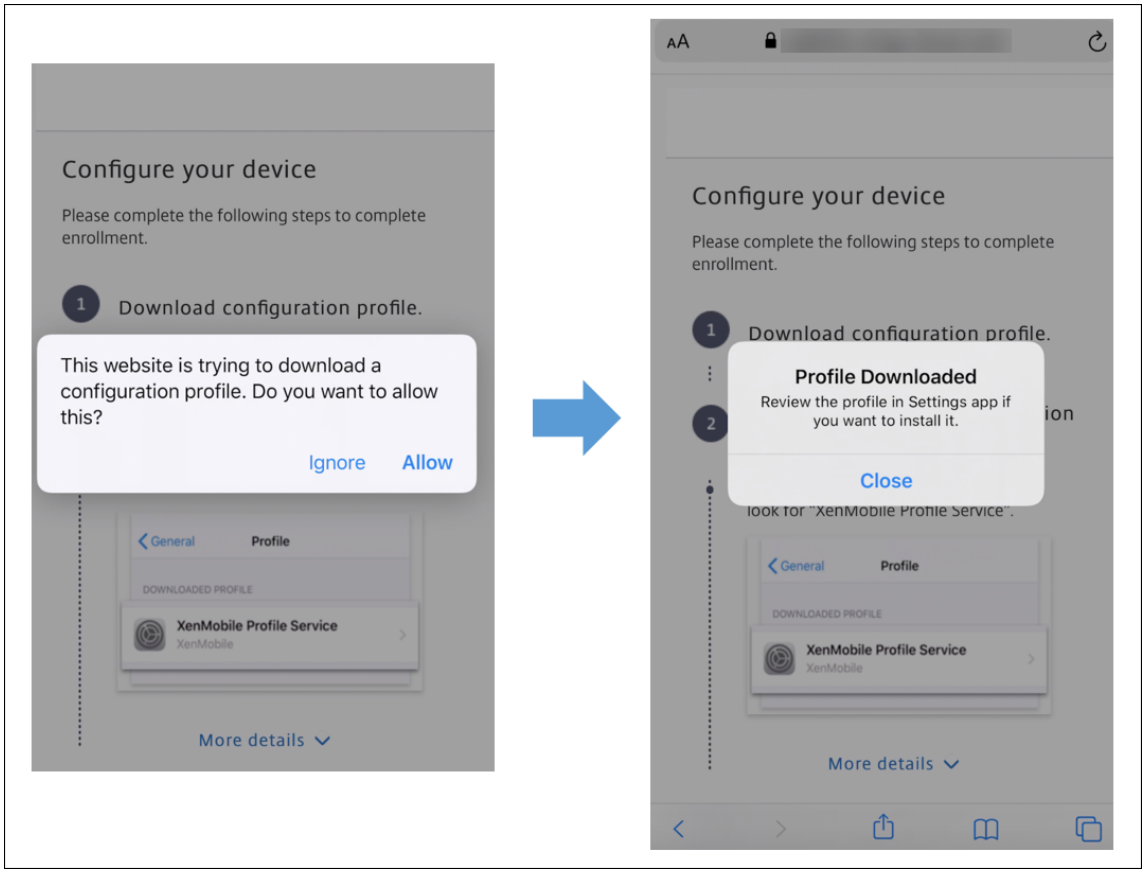
5. Tap **Yes, Enroll** to enroll your iOS device.



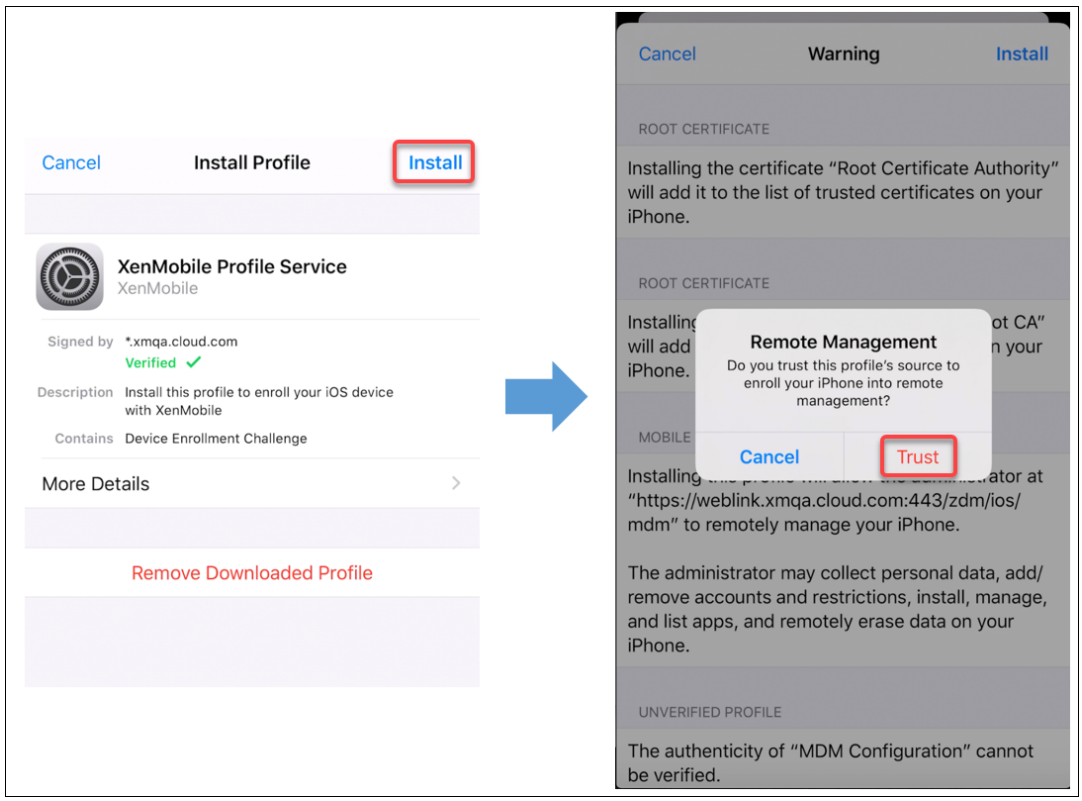
6. A list of the data XenMobile Server collects appears. Click **Next**. An explanation of how an organization uses that data appears. Click **Next**.



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 iOS certificate and add the device to the trusted list.
   - 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

iOS supports the following security actions. For a description of each security action, see Security actions.

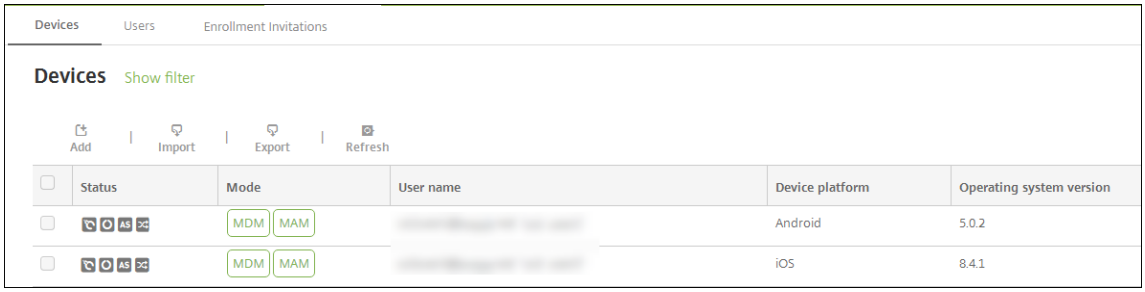
Activation Lock Bypass	App Lock	App Wipe
ASM Activation Lock	Certificate Renewal	Clear Restrictions
Enable/Disable Lost Mode	Enable/Disable Tracking	Full Wipe
Locate	Lock	Ring
Request/Stop AirPlay Mirroring	Restart/Shut Down	Revoke/Authorize
Selective Wipe	Unlock	

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.

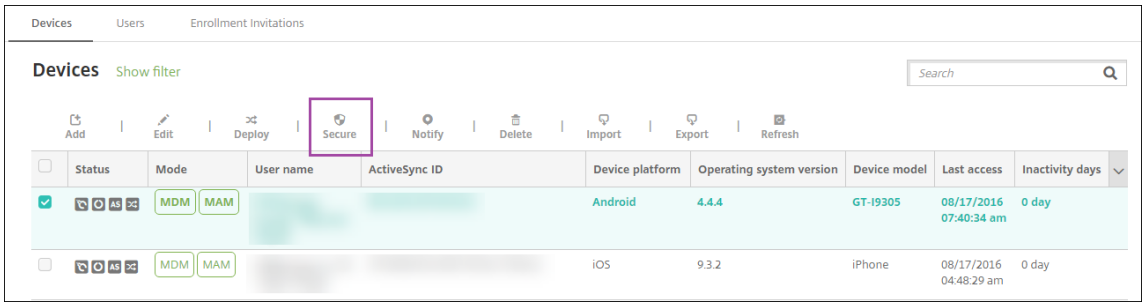
To display a message and phone number on a locked device, set the Passcode policy to **true** in the XenMobile Server console. Alternatively, users can enable the passcode on the device manually.

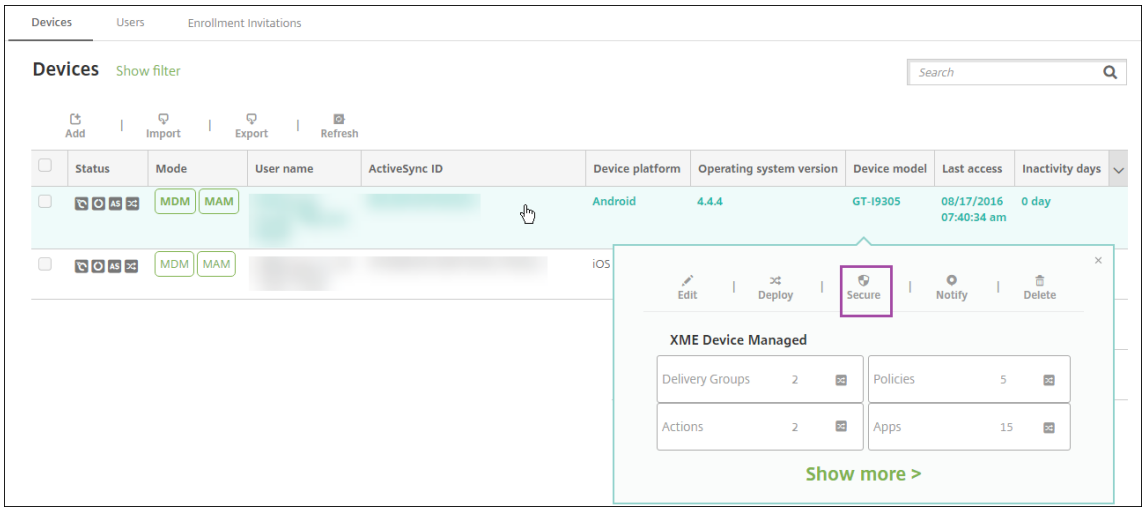
1. Click **Manage > Devices**. The **Devices** page appears.



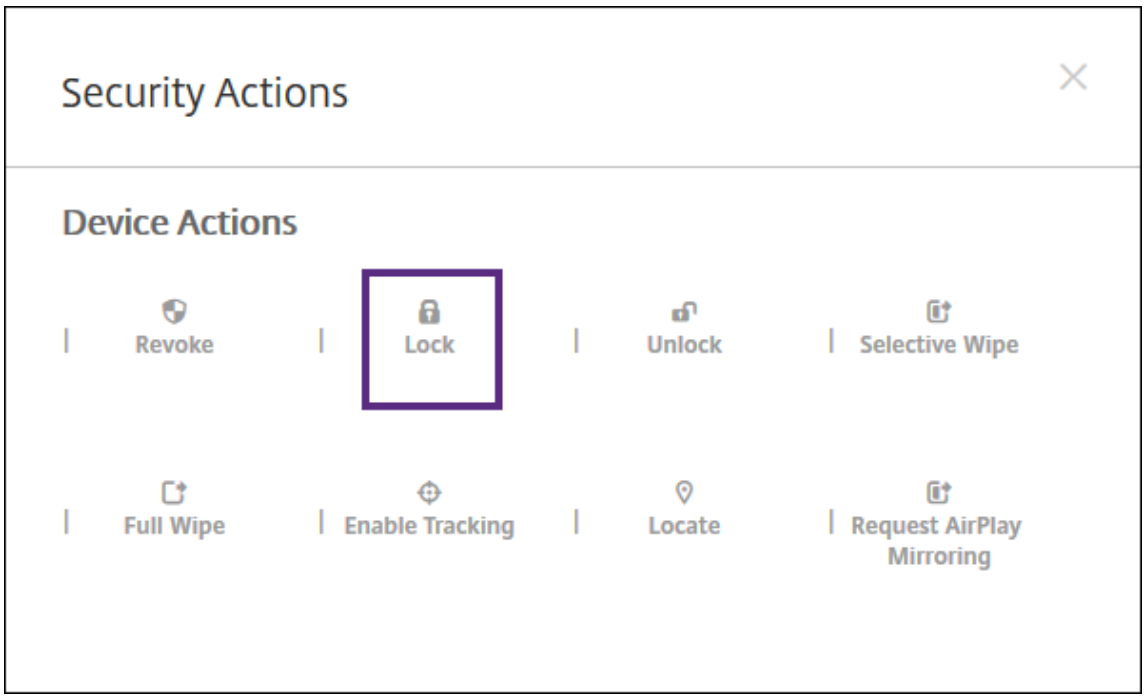
2. Select the iOS device you want to lock.

   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.

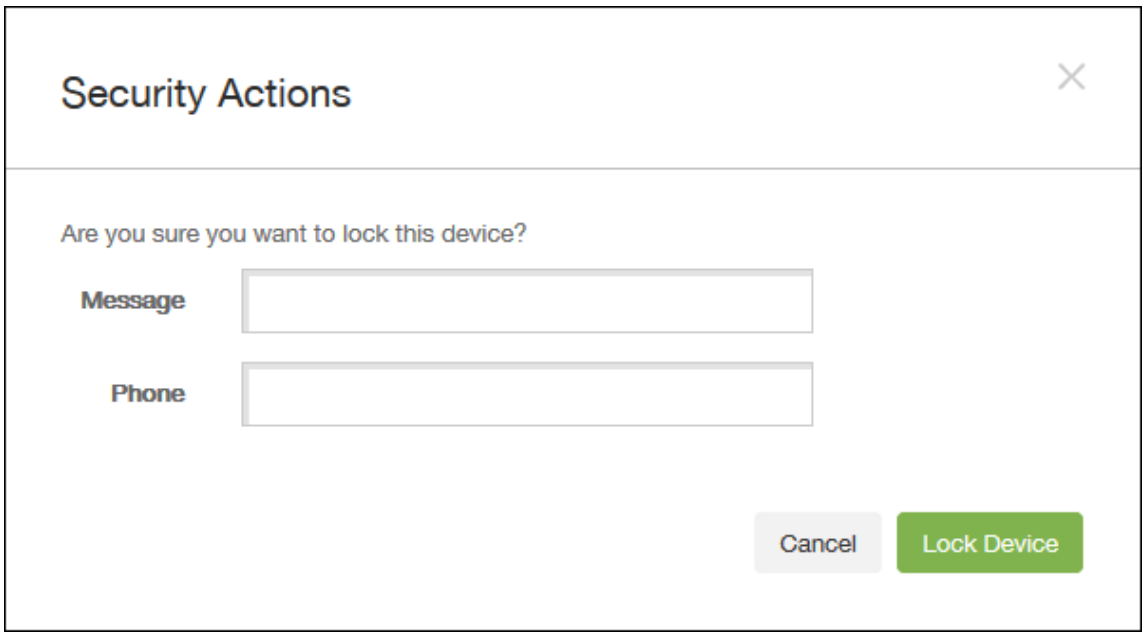




3. In the options menu, click **Secure**. The **Security Actions** dialog box appears.



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.

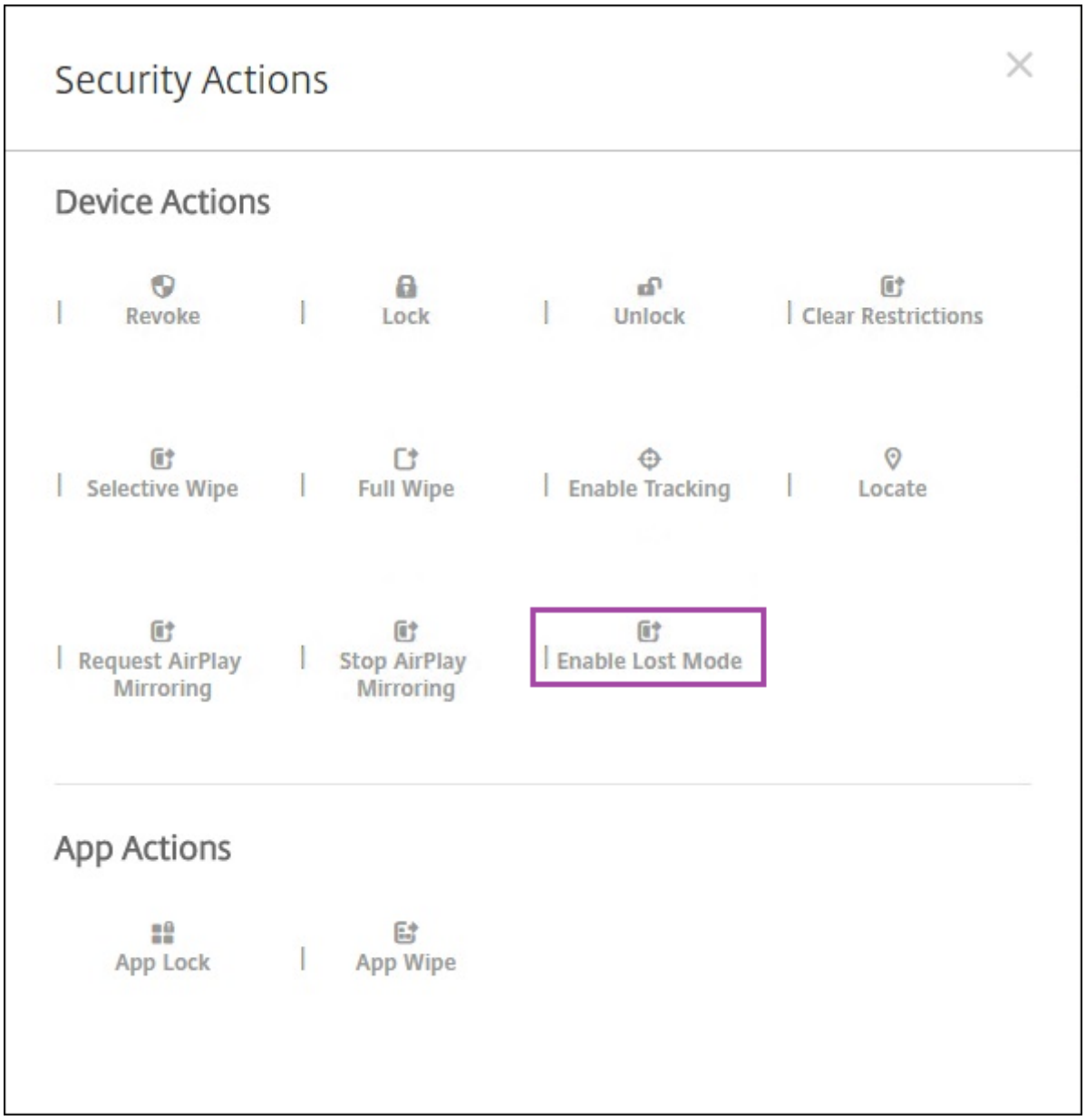
6. Click **Lock Device**.

Put iOS devices in Lost Mode

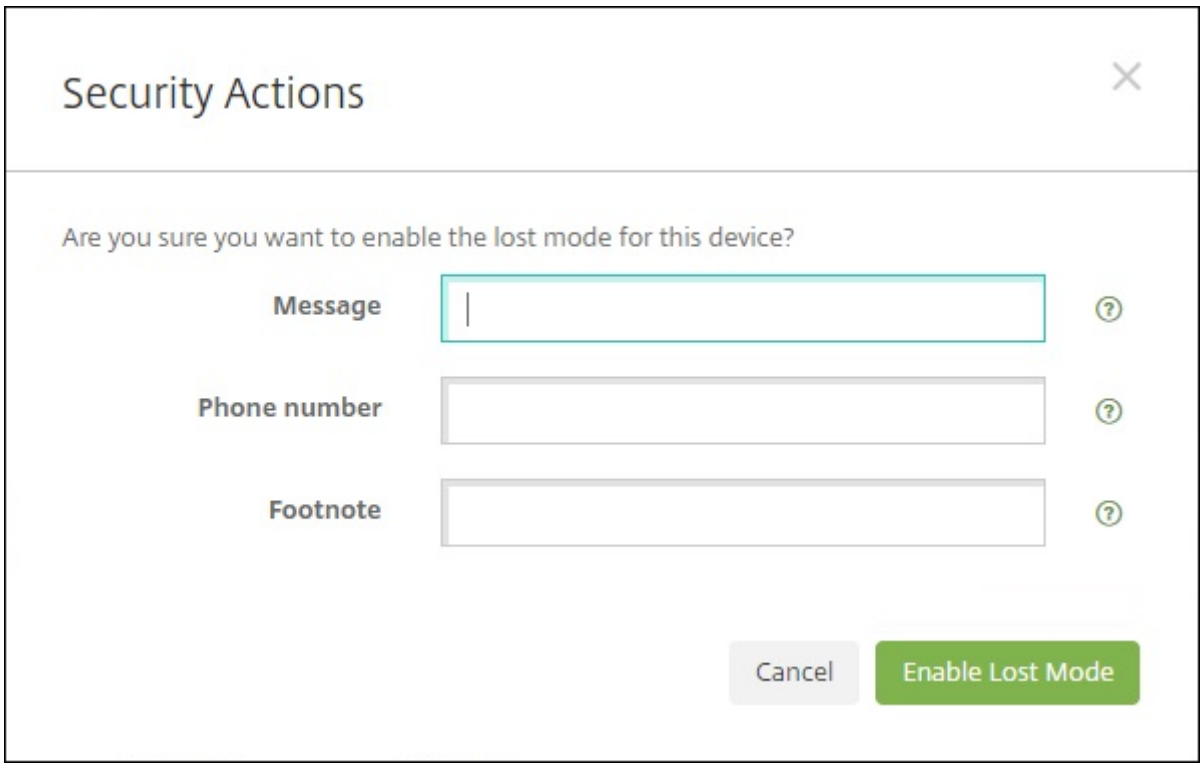
The XenMobile Server Lost Mode device property puts an iOS device in Lost Mode. Unlike Apple Managed Lost Mode, XenMobile Server Lost Mode doesn't require a user to perform either of the following actions to enable locating their device: Configure the **Find My iPhone/iPad** setting or enable the Location Services for Citrix Secure Hub.

In XenMobile Server Lost Mode, only XenMobile Server can unlock the device. (In contrast, if you use the XenMobile Server 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**.

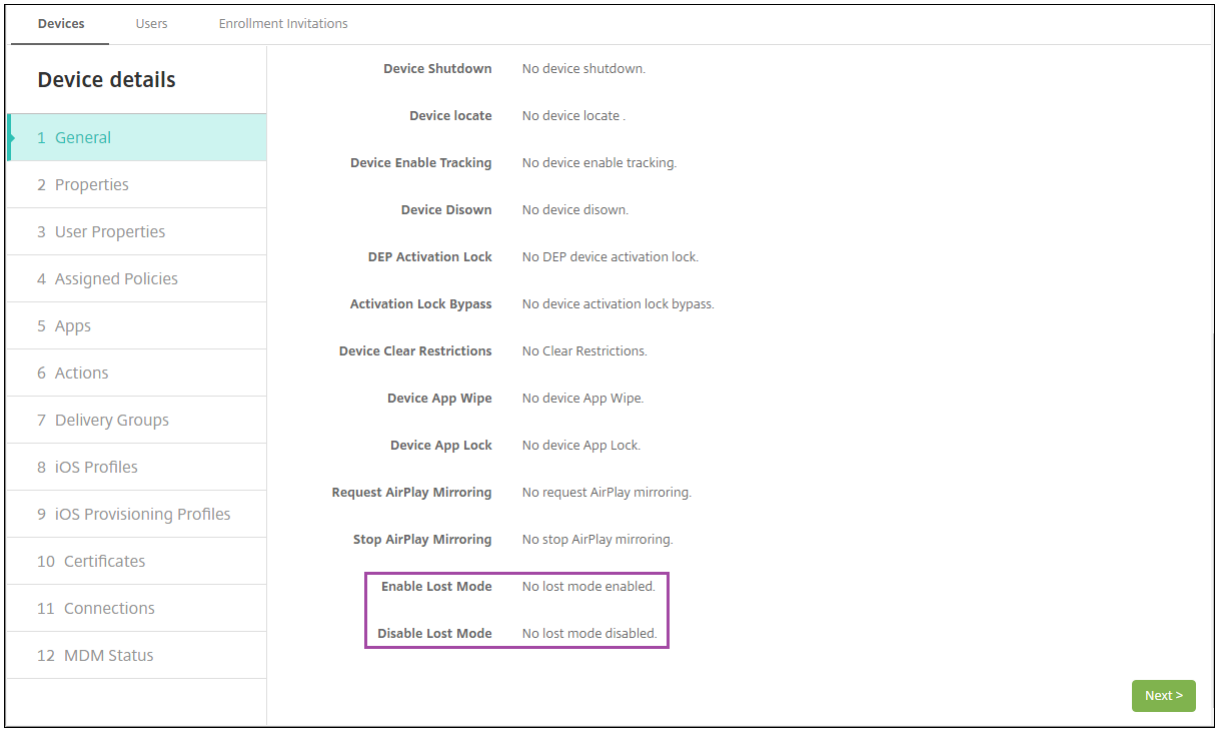


If you click **Enable Lost Mode**, type information to appear on the device when it's in lost mode.

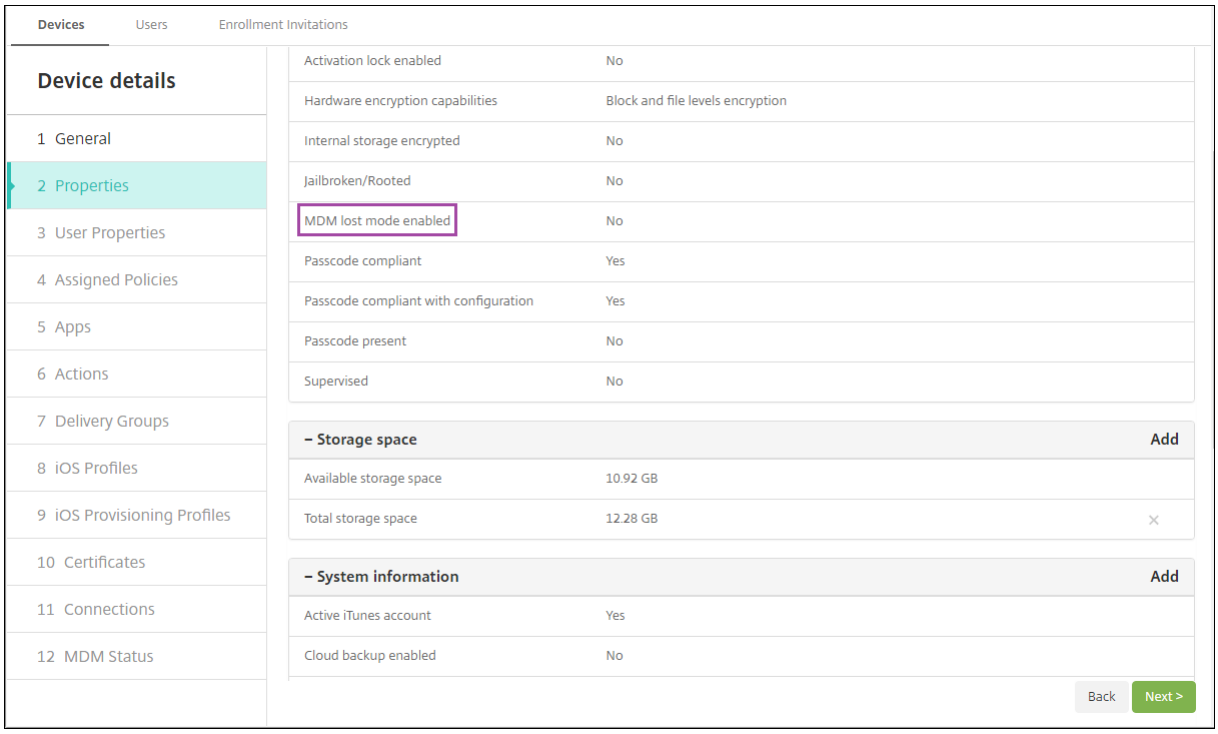


Use any of the following methods to check Lost Mode status:

- 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.



- From **Manage > Devices**, on the **Properties** tab, verify that the value of the **MDM lost mode enabled** setting is correct.



If you enable XenMobile Server Lost Mode on an iOS device, the XenMobile Server 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 XenMobile Server MDM Options device policy. You can then manage a device from the XenMobile Server 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 XenMobile Server 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 XenMobile Server console.

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 XenMobile Server
- 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 with a generated Activation lock bypass code and with the Activation lock enabled: If you can't bypass the Activate iPhone/iPad page after a Full Wipe, there is no need to delete the device from XenMobile Server. Either you or the user can contact Apple support to unblock the device directly.
- During a hardware inventory, XenMobile Server queries a device for an Activation lock bypass code. If a bypass code is available, the device sends it to XenMobile Server. Then, to remove the bypass code from the device, send the Activation Lock Bypass security action from the XenMobile Server console. At that point, XenMobile Server 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 as follows. On the device, manually enter the credentials of the iCloud account. Or, 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

April 14, 2021

To manage macOS devices in XenMobile, you set up an Apple Push Notification service (APNs) certificate from Apple. For information, see APNs certificates.

XenMobile enrolls macOS devices into MDM. XenMobile 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 Uploading certificates in XenMobile.

A general workflow for starting macOS device management is as follows:

1. Configure macOS device policies.
2. Enroll macOS devices.
3. 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 XenMobile 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 XenMobile. That program is for iOS and macOS 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 and macOS 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 XenMobile interacts with devices running macOS. This table lists all device policies available for macOS devices.

AirPlay Mirroring	App Inventory	Calendar (CalDAV)
Contacts (CardDAV)	Control OS Update	Credentials
Device Name	Exchange	FileVault
Firewall	Font	Import iOS & macOS Profile
LDAP	Mail	Passcode
Profile Removal	Restrictions	SCEP
VPN	Web clip	Wi-Fi

Enroll macOS devices

XenMobile 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

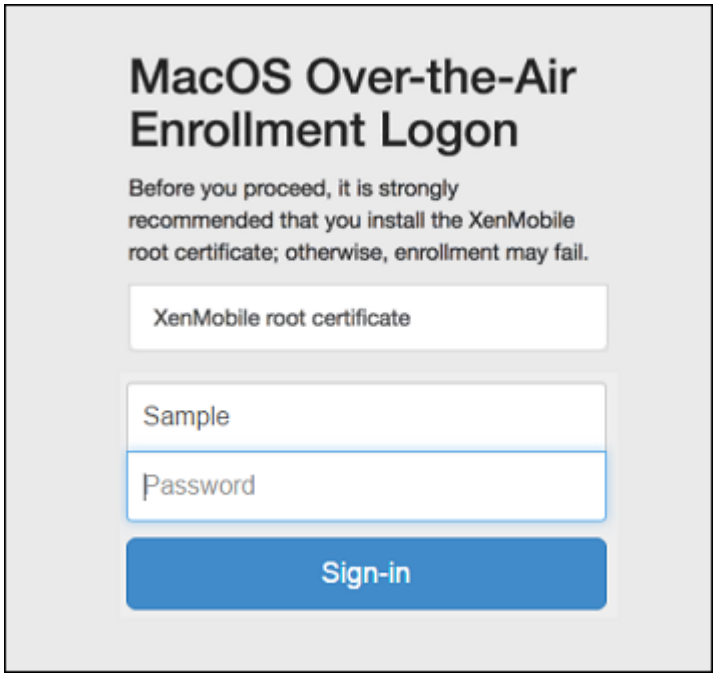
  When the user follows the instructions in the enrollment invitation, a sign-on screen with the user name filled in appears.
- **Send users an enrollment link:** This enrollment method for macOS devices sends users an enrollment link, which they can open in Safari or Chrome browsers. A user then enrolls 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 Create an enrollment invitation.

2. After users receive the invitation and click the link, the following screen appears in the Safari browser. XenMobile 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 XenMobile 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 XenMobile.
   - 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 Send an enrollment invitation.

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 XenMobile just as you manage mobile devices.

Security actions

macOS supports the following security actions. For a description of each security action, see Security actions.

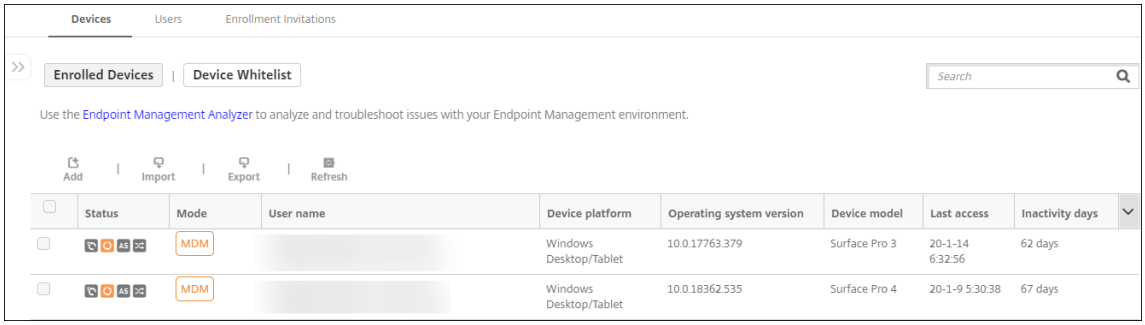
Revoke	Lock	Selective Wipe
Full Wipe	Certificate renewal	

Lock macOS devices

You can remotely lock a lost macOS device. XenMobile 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 XenMobile console.

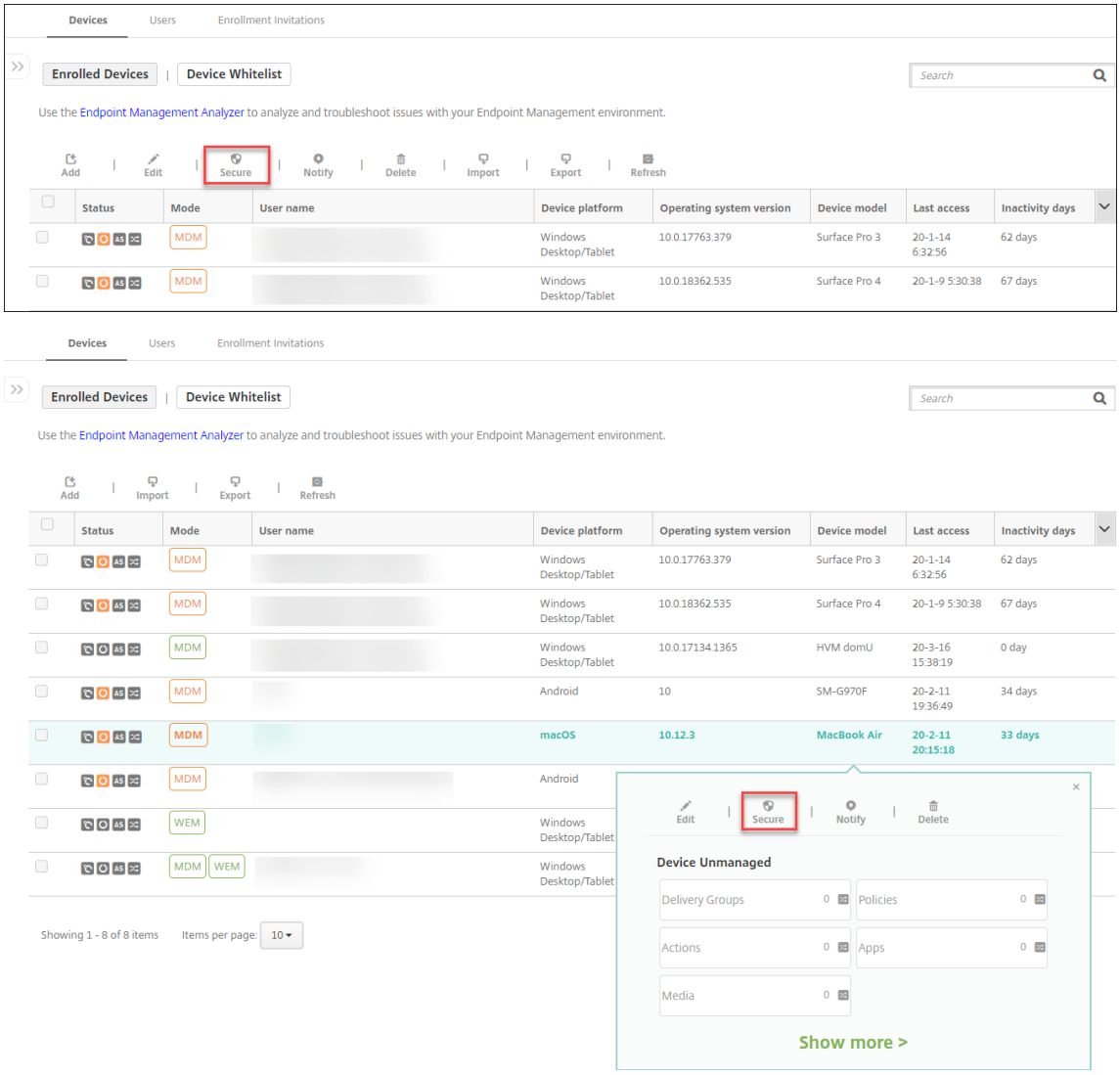
You can use the Passcode device policy to configure more settings associated with the PIN code. For more information, see macOS settings.

1. Click **Manage > Devices**. The **Devices** page appears.



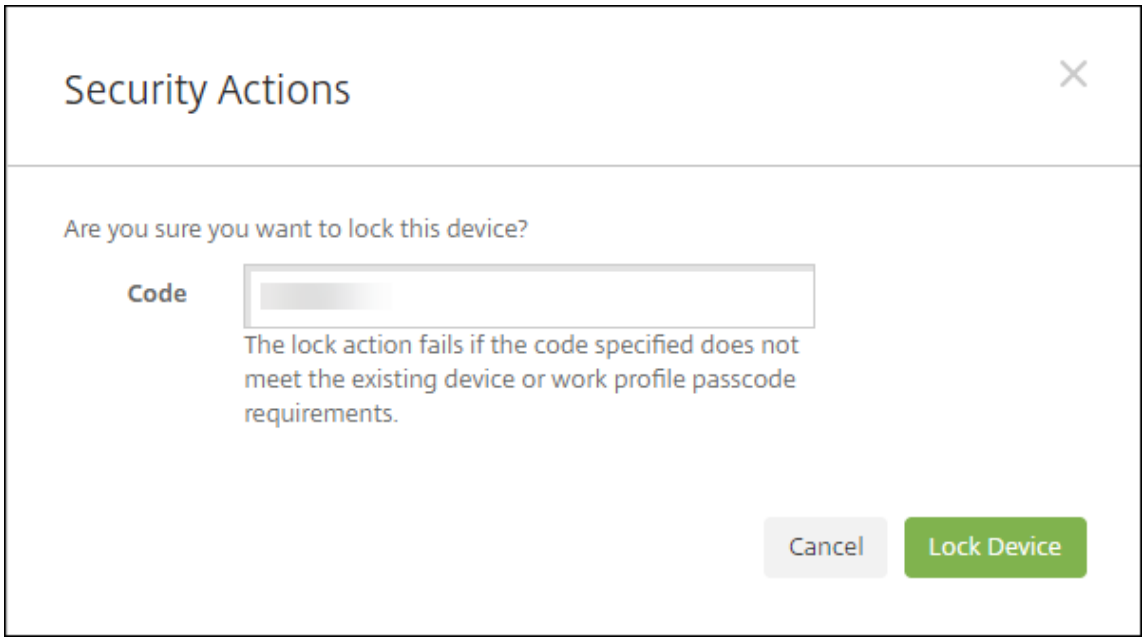
2. Select the macOS device you want to lock.

   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.



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 XenMobile generates. The lock action fails if the code specified does not meet the code requirements of the device or existing work profile.

Bulk enrollment of Apple devices

April 21, 2021

You can enroll large numbers of iOS, iPadOS, and macOS devices in XenMobile in two ways.

- Use the Apple Deployment Program to enroll the iOS, iPadOS, and macOS devices that you buy directly from Apple, a participating Apple Authorized Reseller, or a carrier. That support includes Shared iPads. XenMobile supports the Apple Deployment Program for Apple Business Manager (ABM) and Apple School Manager (ASM) for Education. This article describes how to integrate multiple devices with your ABM account. For information on enrolling in ABM and connecting your ABM account with XenMobile, see Deploy devices through Apple Deployment Program. For information about Apple School Manager accounts, see Integrate with Apple Education features.

  For enrollment of macOS devices, XenMobile requires that the devices run macOS 10.10 or later.

- You can also use Apple Configurator 2 to enroll iOS devices whether you purchased them directly from Apple or not.

With ABM:

- You do not have to touch or prepare the devices. Instead, you submit device serial numbers or purchase order numbers through ABM to configure and enroll the devices.
- After XenMobile enrolls the devices, you can give them to users who can start using them right away. When you set up devices with ABM, you can eliminate some of the Setup Assistant steps that users would have to complete when they first start their devices.
- For more information on setting up ABM, see the documentation available from Apple Business Manager.

With Apple Configurator 2:

- You attach iOS devices to an Apple computer 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.
- After you provision the devices with the required policies, the first time the devices connect to XenMobile, the devices receive policies from XenMobile. You can then start managing the devices.
- For more information about using Apple Configurator 2, see the Apple Configurator Help.

Prerequisites

Open required ports for connectivity between XenMobile and Apple. For more information, see Port requirements.

Integrate your Apple Business Manager account with XenMobile

If you do not have an ABM account set up with XenMobile, complete the following steps in Deploy devices through Apple Deployment Program.

- Enroll in Apple Business Manager.
- Connect your Apple Business Manager account with XenMobile.
- Order Deployment Program enabled devices.
- Manage Deployment Program enabled devices.

Set a default server for bulk enrollment

To assign large orders of iOS, iPadOS, and macOS devices to an MDM server, you can set XenMobile as the default server.

1. Sign in to Apple Business Manager using an administrator or device enrollment manager account.
2. In the sidebar, click **Settings > Device Management Settings**.
3. Choose an existing MDM server. Under **Default Device Assignment**, click **Change**. Select the default XenMobile server for each device type. Click **Done**.

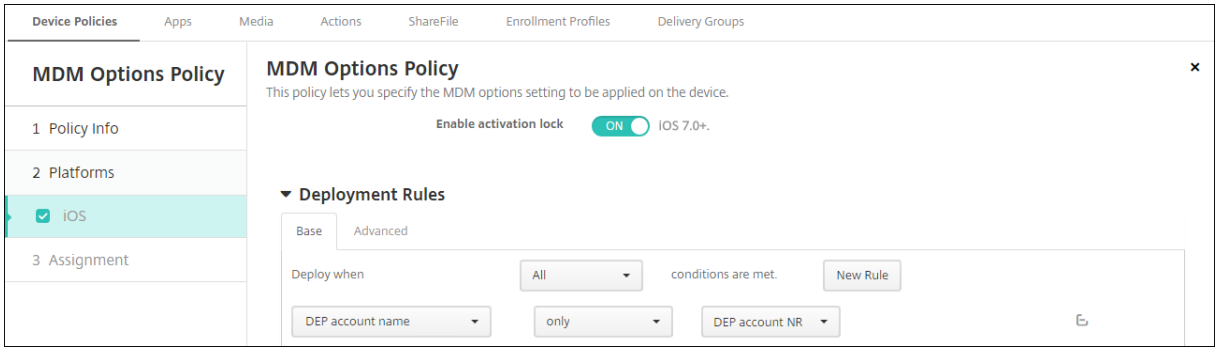
Configure deployment rules of device policies and apps for ABM accounts

You can associate ABM accounts with different device policies and apps by using the **Deployment Rules** section under **Configure > Device Policies** and **Configure > Apps**. You can specify that a policy or app either:

- Deploys only for a particular ABM account.
- Deploys 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, XenMobile 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".

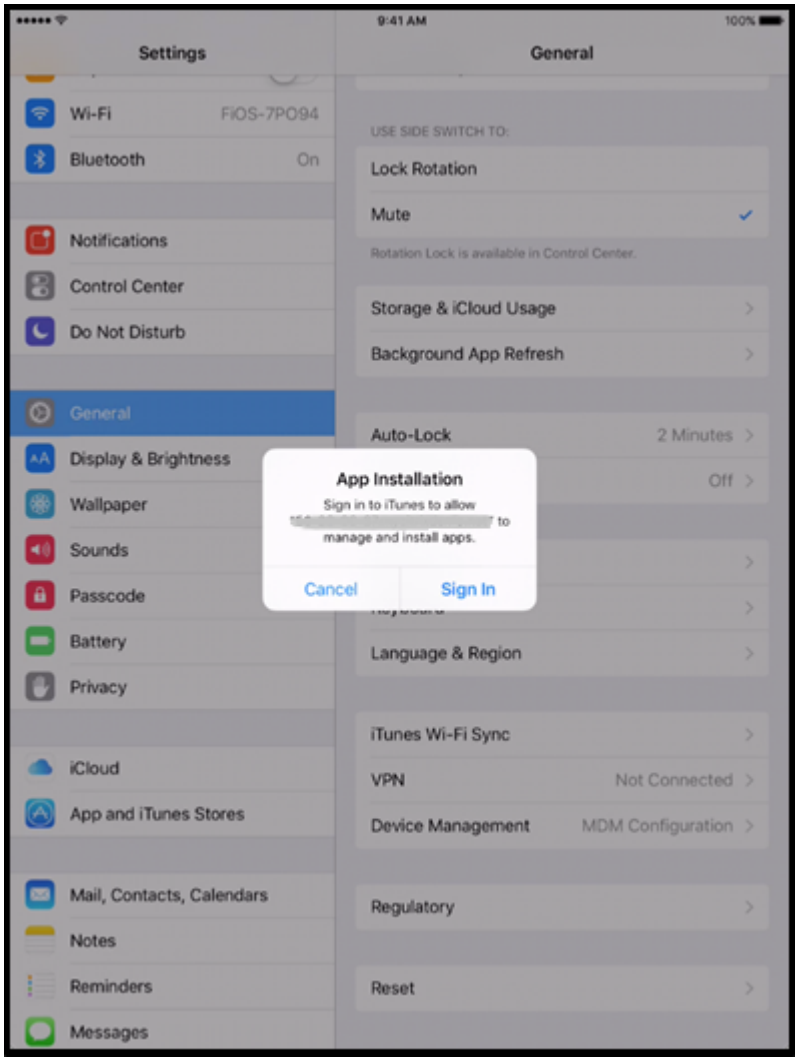


User experience when enrolling an Apple Deployment Program enabled device

When users enroll an Apple Deployment Program enabled device, their experience is as follows.

1. Users start their Apple Deployment Program enabled device.
2. XenMobile delivers the Apple Deployment Program configuration that you configured in the XenMobile console to the Apple Deployment Program enabled device.
3. Users configure the initial settings on their device.
4. The device automatically starts the XenMobile device enrollment process.
5. Users continue to configure the other initial settings on their device.
6. In the home screen, users might be prompted to sign in to Apple App Store so that they can download Citrix Secure Hub.

   > **Note:**
   >
   > This step is optional if you configure XenMobile 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.



7. Users open Secure Hub and type their credentials. If required by the policy, users might be prompted to create and verify a Citrix PIN.

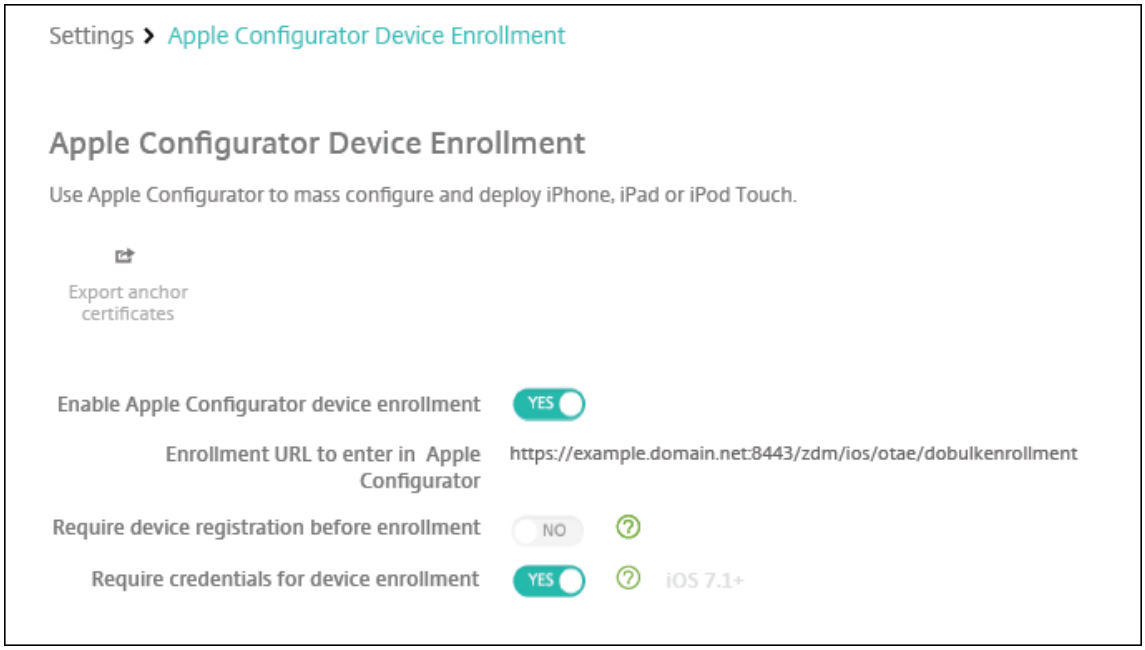
   XenMobile deploys any remaining required apps to the device.

To configure Apple Configurator 2 settings

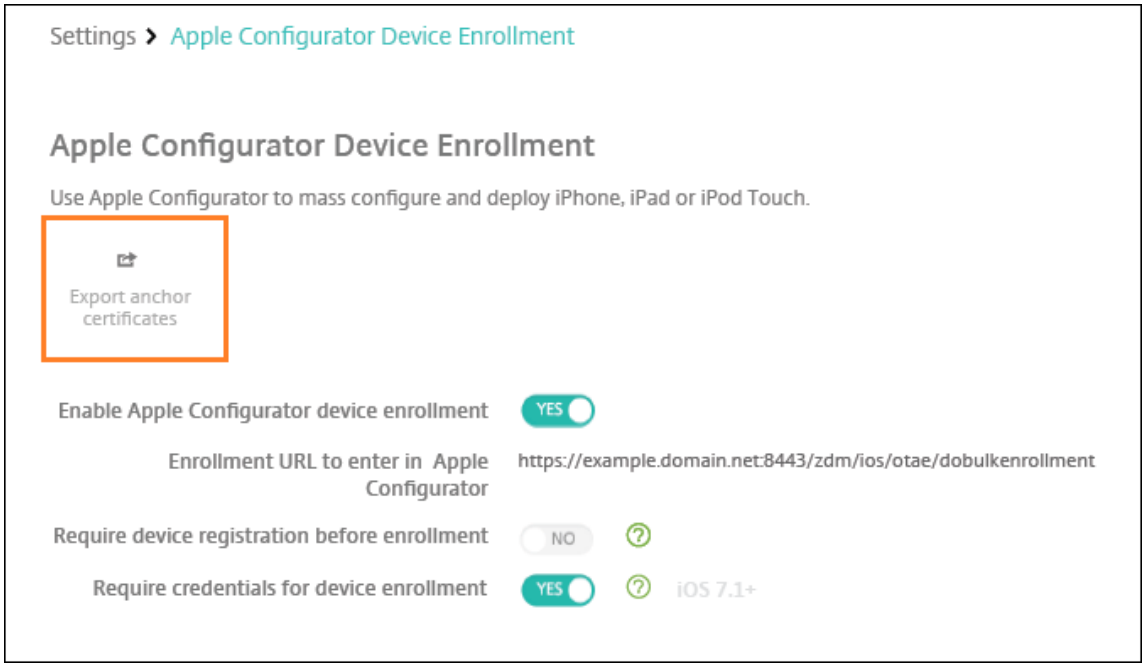
You can configure and deploy iPhone and iPad devices in bulk using Apple Configurator 2 instead of Apple Business Manager.

Step 1: Configure settings in XenMobile

1. In the XenMobile console, go to **Settings > Apple Configurator Device Enrollment**.



2. Set **Enable Apple Configurator device enrollment** to **Yes**.
3. The **Enrollment URL to enter in Apple Configurator** is a read-only field. This setting provides the URL for the XenMobile server that communicates with Apple. Copy and paste this URL when you configure settings in Apple Configurator 2. The enrollment URL is the XenMobile 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 XenMobile 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 not to require credentials for enrollment.
6. Note: If the XenMobile 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 System).



Step 2: Configure settings in Apple Configurator 2

1. Install Apple Configurator 2 from the App Store.
2. Use a Dock Connector-to-USB cable to connect devices to the Mac running Apple Configurator 2. 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 new server, click **Next**
6. In **Define an MDM server**, provide a name for the server and paste the MDM server URL from the XenMobile 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.

To assign devices from Apple Configurator 2 to Apple Business Manager

You can associate iPhone and iPad devices from Apple Configurator 2 with your Apple Business Manager account. When 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 Assign devices added from Apple Configurator 2 to Apple Business Manager.

Renew or update certificates when using the Apple Deployment Program

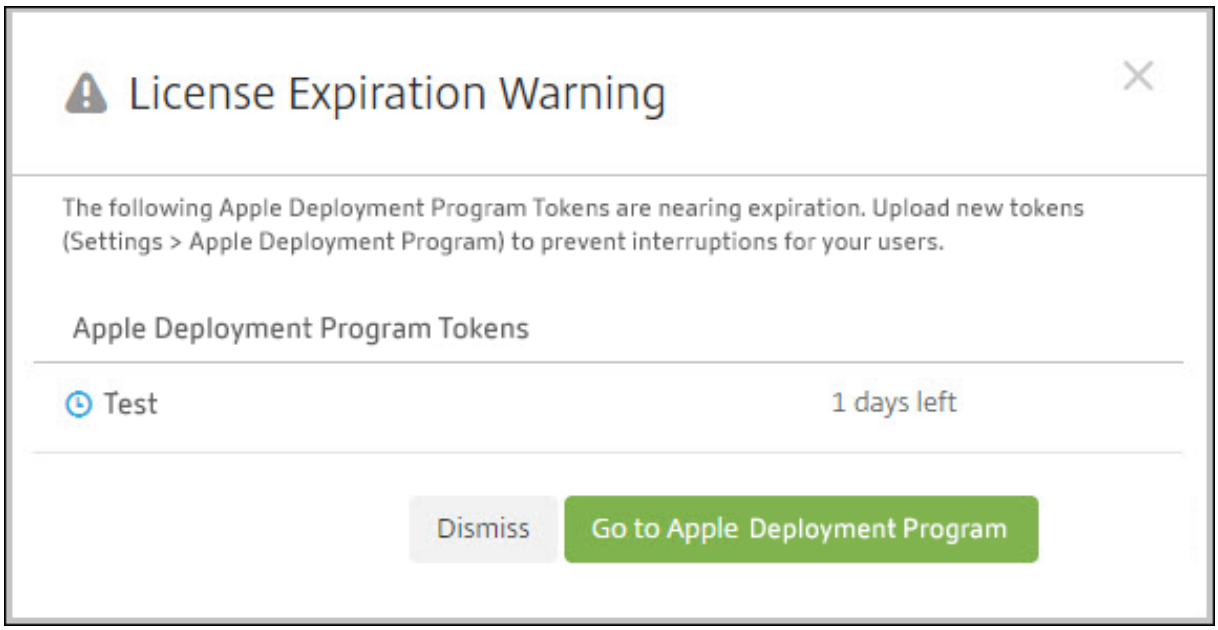
When the XenMobile Secure Sockets Layer (SSL) certificate is renewed, you upload a new certificate in the XenMobile console in **Settings > Certificates**. In the **Import** dialog box, in **Use as**, click **SSL Listener** so that the certificate is used for SSL. After you restart the server, XenMobile uses the new SSL certificate. For more information about certificates in XenMobile, see Uploading Certificates in XenMobile.

It is not necessary to reestablish the trust relationship between Apple Deployment Program and XenMobile when you renew or update the SSL certificate. You can, however, reconfigure your **Apple Deployment Program** settings at any time by following the preceding steps in this article.

For more information about the Apple Deployment Program, see the Apple documentation.

Renew your connection between the Apple Deployment Program and XenMobile

XenMobile displays a License Expiration Warning when your Automated Device Enrollment server token expires.



Replace the token from Apple School Manager/Apple Business Manager.

Step 1: Download a public key from your XenMobile server

1. In the XenMobile 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 Apple Business Manager 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 XenMobile and save the changes.
4. Click **Download Token** to download the new token.

Step 3: Upload a server token file in XenMobile

1. In Citrix XenMobile, 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.

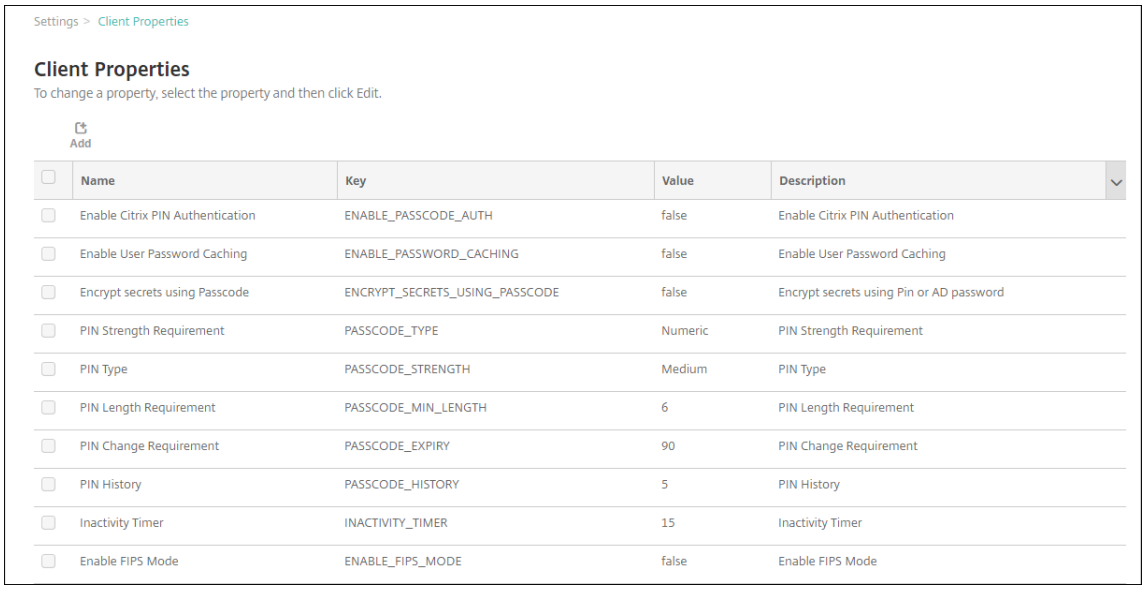
Client properties

April 5, 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.

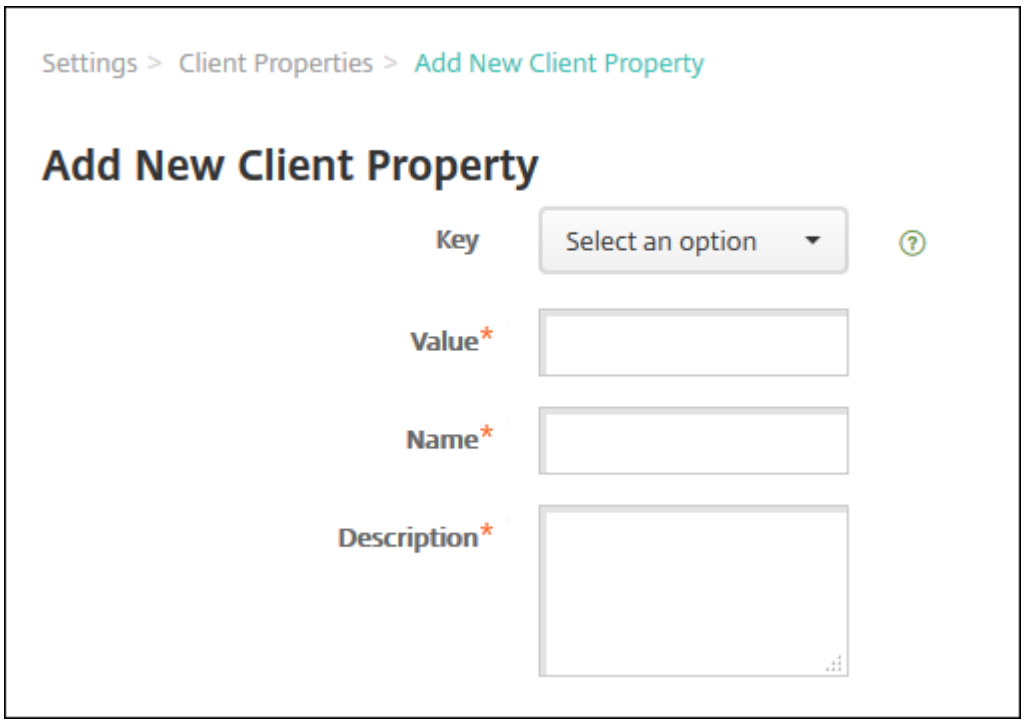
Client properties are subject to change with every release of Secure Hub and occassionally for client apps. For details about more commonly configured client properties, see Client property reference, later in this article.

1. In the XenMobile 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.



To add a client property

1. Click **Add**. The **Add New Client Property** page appears.

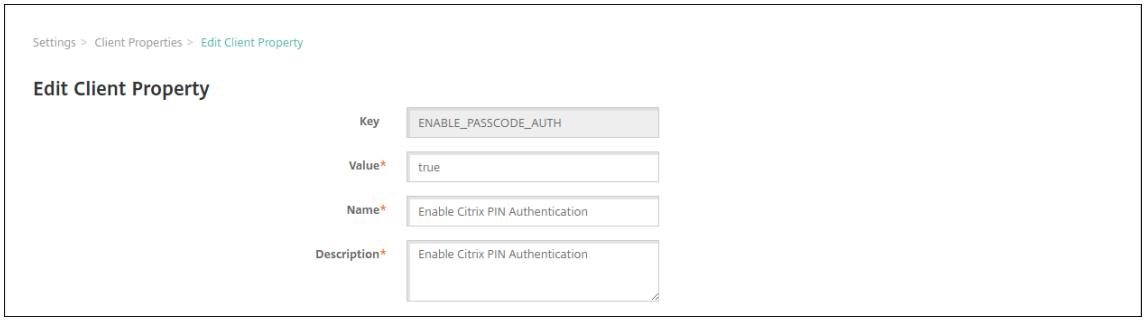


2. Configure these settings:
   - **Key:** In the list, click the property key that you want to add. Important: Contact Citrix Support before updating the settings. You can request a special key.
   - **Value:** The value of the selected property.
   - **Name:** A name for the property.
   - **Description:** 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.

   When you select the check box next to a client property, the options menu appears above the client property list. When you click anywhere else in the list, the options menu appears 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 XenMobile predefined client properties and their default settings are as follows.

- **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 does not receive an authentication request to validate the user over a specific length of time. For example, if this property is 30 days and 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 XenMobile 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 mobile productivity apps. You can use the credential store whether or not you enable Citrix PIN. If you don't enable Citrix PIN, users enter their Active Directory password. XenMobile supports 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, XenMobile 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_FIPS_MODE**
  - Display name: Enable FIPS Mode
  - This property enables or disables FIPS mode on mobile devices. After you change the value, Secure Hub passes the new value to the device when Secure Hub does the next online authentication.
  - Possible values: **true** or **false**
  - Default value: **false**

- **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 XenMobile 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 XenMobile.

    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, XenMobile 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, XenMobile 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 Worx Home 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 XenMobile.
  - Value: **true** or **false**
  - Default value: **false**
- **ENABLE_WORXHOME_GA**
  - Display name: Enable Google Analytics in Worx Home
  - 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 (previously named Worx Home).
  - 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 very 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 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
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	132132, 131313, 902030

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	AAAaaa, aaaaaa, abcdef
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
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, XenMobile pings the Auto Discovery 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 XenMobile 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, XenMobile 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 XenMobile 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`

Deploy devices through the Apple Deployment Program

April 21, 2021

Apple has device enrollment programs for business and education accounts. For business accounts, you enroll in the Apple Deployment Program to use the Apple Business Manager (ABM) or Apple School Manager (ASM) for device enrollment and management in XenMobile. That program is for iOS, iPadOS, and macOS devices.

The Apple Deployment Program is available for organizations and not individuals. You must provide a considerable amount of corporate details and information to create an Apple Deployment Program account. Thus, it might take time to request and receive approval for accounts.

For education accounts, you create an Apple School Manager account. ASM unifies the Apple Deployment Program and Apple volume purchase. To create an Apple School Manager account, go to the Apple School site.

Enroll in the Apple Deployment Program

To enroll in Apple Business Manager, go to 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. The enrollment process might take a few days. After you receive your logon credentials, follow the steps provided in Apple Business Manager to create an account.

> **Note:**
>
> For education accounts, see Integrate with Apple Education features.

Connect your Apple Business Manager account with XenMobile

To connect your Apple Business Manager account with your XenMobile deployment, enter information in the XenMobile console and Apple Business Manager. Follow these steps:

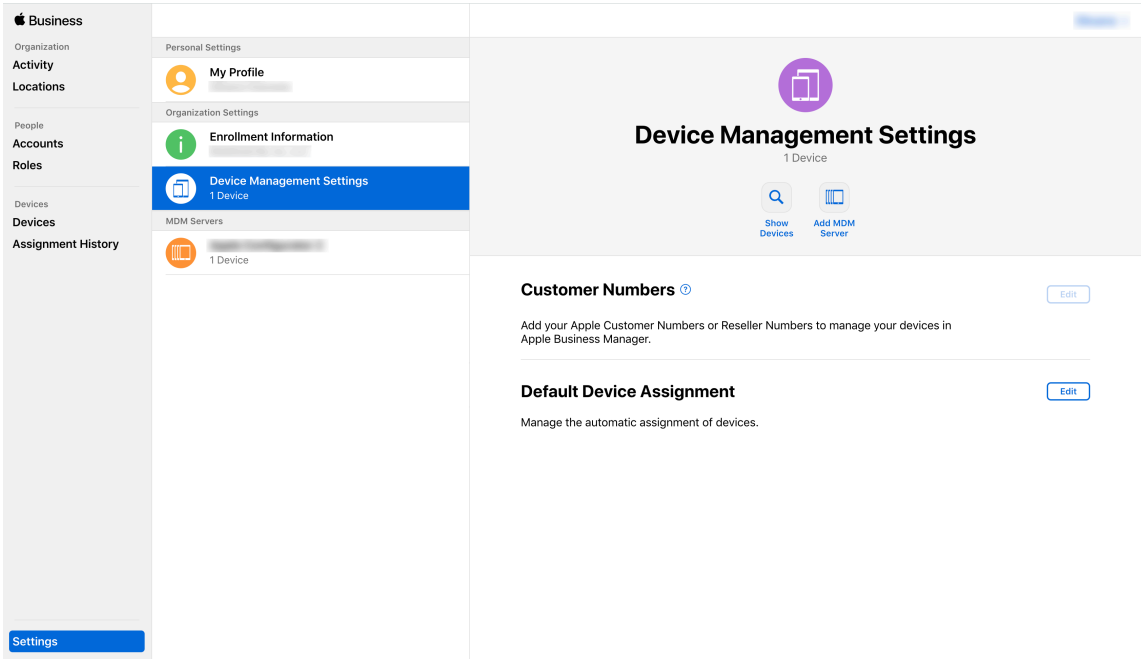
Step 1: Download a public key from your XenMobile server

1. In the XenMobile console, go to **Settings > Apple Deployment Program**.

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 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 XenMobile 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 XenMobile and then save the changes.
5. Click **Download Token** to download the server token file to your computer.

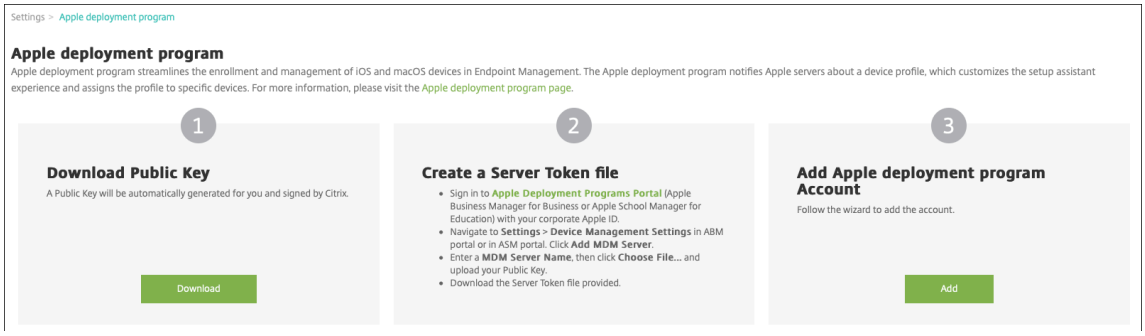
   You must upload the server token file when adding the ABM account to XenMobile. Your ABM token information appears in the XenMobile console after you import the token file.
6. Under **Default Device Assignment**, click **Change**. Choose how you want to assign devices and then provide the information requested. For information, see the ABM User Guide.

Step 3: Add an ABM account to XenMobile

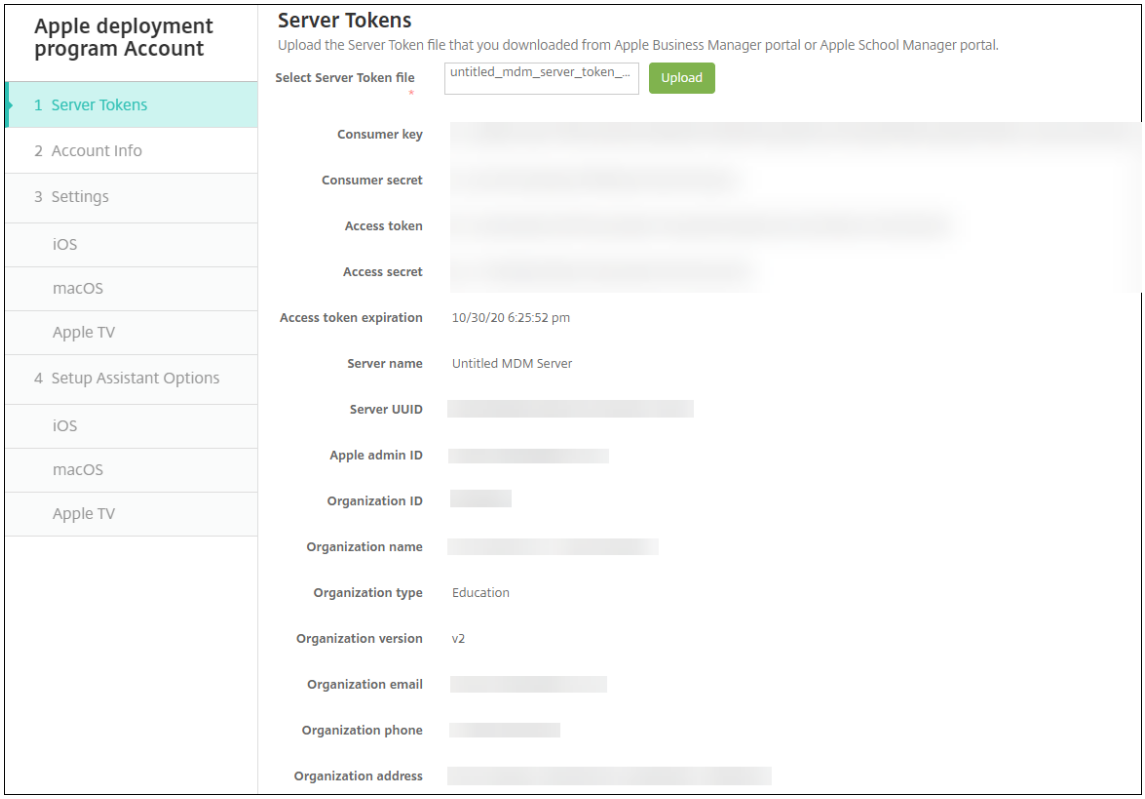
You can add multiple ABM accounts to XenMobile. This feature enables you to use different enrollment settings and setup assistant options by country, department, and so on. You then associate ABM accounts with different device policies.

For example, you might centralize all of your ABM accounts from different countries on the same XenMobile server, to import and supervise all ABM devices. By customizing enrollment settings and setup assistant options per department, organizational hierarchy, or other structure, policies provide appropriate functionality across your organization, and users receive the appropriate assistance.

1. In the XenMobile console, go to **Settings > Apple Deployment Program** and, under **Add Apple Deployment Program Account**, click **Add**.

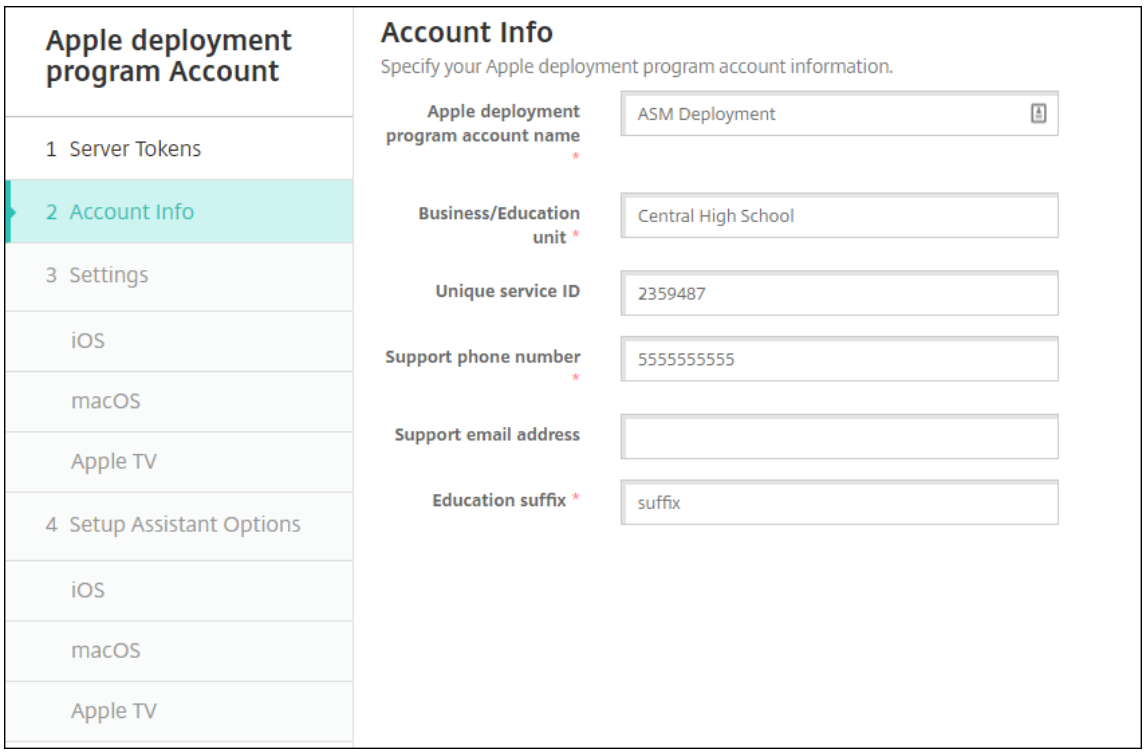


2. In the **Server Tokens** page, specify your server token file and then click **Upload**.



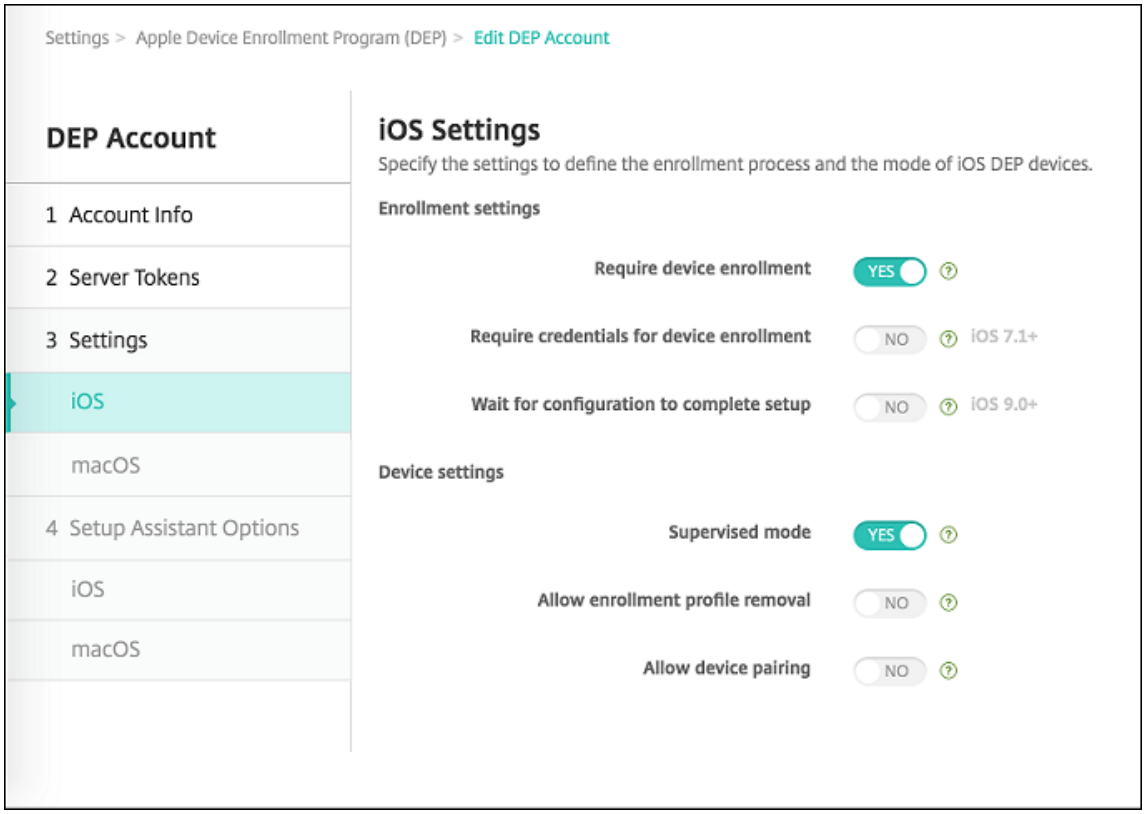
Your server token information appears.

3. In the **Account Info** page, specify these settings:



- **Apple Deployment Program account name:** A unique name for this Apple Deployment Program account. Use names that reflect how you organize Apple Deployment Program 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.

4. In **iOS Settings**, specify these settings:



Enrollment settings:

- **Require device enrollment:** Whether to require users to enroll their devices. The default is **Yes**.
- **Require credentials for device enrollment:** Whether to require users to enter their credentials during ABM setup. Citrix recommends that you require all users to enter their credentials during device enrollment, thus allowing only authorized users to enroll devices. The default is **Yes**.

  When you enable ABM before first time setup and you don't select this option, XenMobile creates the ABM components. This creation includes components such as ABM user, Secure Hub, software inventory, and ABM deployment group. If you do select this option, XenMobile 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 because these ABM components don't exist. To add ABM components, in that case, disable and enable the ABM 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 **No**.
- 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:** Must be set to **Yes** if you are using the Apple Configurator to manage ABM enrolled devices or when **Wait for configuration to complete setup** is enabled. The default is **Yes**. For details on placing an iOS device in supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator.
- **Allow enrollment profile removal:** Whether to allow devices to use a profile that you can remove remotely. The default is **No**.
- **Allow device pairing:** For devices enrolled through ABM, whether you can manage them through Apple Music and the Apple Configurator. The default is **No**.

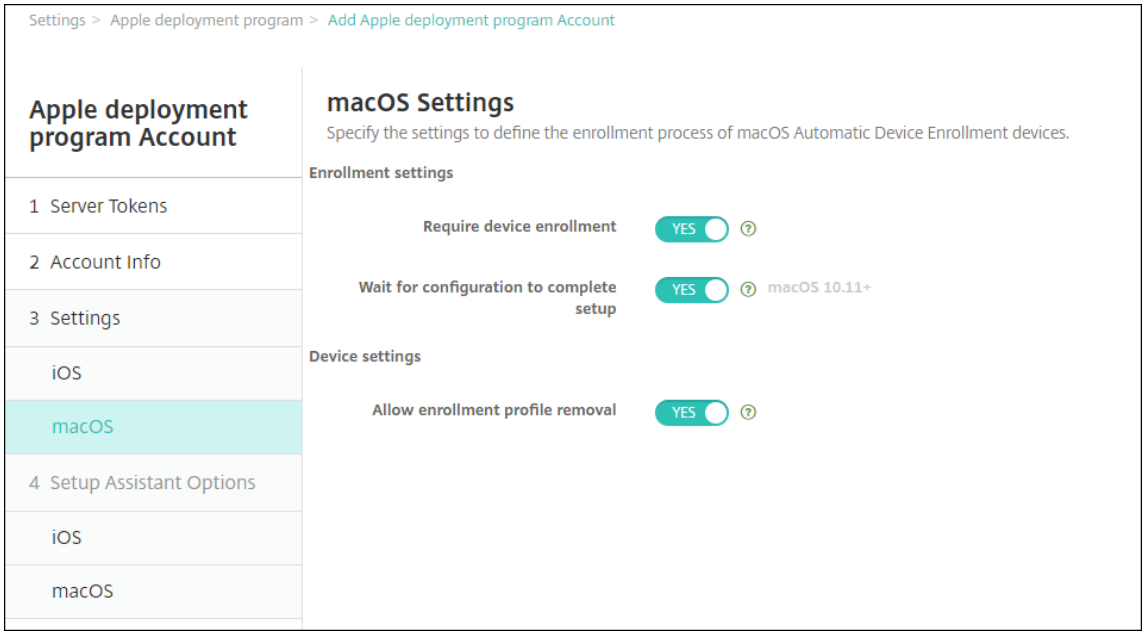
Supervision Identities

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 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 **Yes**.
- **Wait for configuration to complete setup:** If **Yes**, 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 **No**.

Device settings:

- **Allow enrollment profile removal:** Whether to allow devices to use a profile that you can remove remotely. The default is **No**.

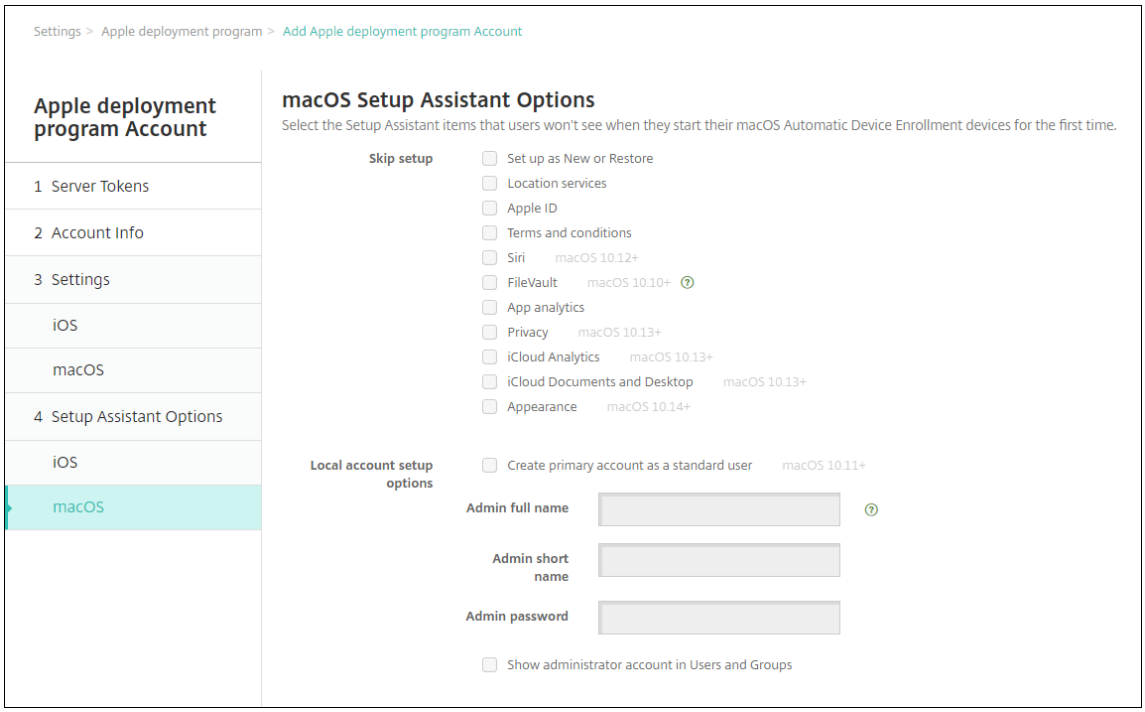
6. In **iOS Setup Assistant Options**, select the iOS Setup Assistant steps that your users skip when they start their devices the first time. The default for all items is cleared.

- **Location services:** Set up the location service on the device.
- **Touch ID:** Set up Touch ID on iOS devices.
- **Passcode lock:** Create a passcode for the device.
- **Set up as New or Restore:** Set up the device as new or from an iCloud or Apple App Store backup.
- **Move from Android:** Enable 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:** Set up a Managed Apple ID account for the device.
- **Terms and conditions:** Require users to accept terms and conditions for use of the device.
- **Apple Pay:** Set up Apple Pay on iOS devices.
- **Siri:** Use or not use Siri on the device.
- **App analytics:** Set up whether to share crash data and usage statistics with Apple.
- **Display zoom:** Set up the display resolution (either standard or zoomed) on iOS devices.
- **True Tone:** Set up the True Tone Display on iOS devices.
- **Home Button:** Set up the **Home** Button screen sensitivity on iOS devices.
- **New feature highlights:** Set up the onboarding informational screens, Access the Dock from Anywhere and Switch Between Recent Apps on iOS 11.0 devices (minimum version).
- **Privacy:** Prevent users from seeing the data and privacy pane during setup of ABM devices. For iOS 11.3 and later.
- **SoftwareUpdate:** Prevents the user from seeing the mandatory software update screen while setting up ABM devices. For iOS 12.0 and later.
- **ScreenTime:** Prevents the user from seeing the Screen Time screen during setup of the ABM devices. For iOS 12.0 and later.
- **SIM Setup:** Prevents the user from seeing the Add Cellular Plan screen during setup of the ABM devices. For iOS 12.0 and later.

- **iMessage & FaceTime:** Prevents the user from seeing the iMessage and FaceTime screen during setup of the ABM devices. For iOS 12.0 and later.
- **Appearance:** Prevents the user from seeing the **Choose Your Look** screen. For iOS 13.0 and later.
- **Welcome:** Prevents the user from seeing the **Getting Started** screen. For iOS 13.0 and later.

The ABM account appears on **Settings > Apple Deployment Program**.

7. In **macOS Setup Assistant Options**, select the macOS Setup Assistant steps that your users skip when they start their devices the first time. The default for all items is cleared.



- **Set up as New or Restore:** Set up the device as new or from an iCloud or Apple App Store backup.
- **Location services:** Set up the location service on the device.
- **Apple ID:** Set up a Managed Apple ID account for the device.
- **Terms and conditions:** Require users to accept terms and conditions for use of the device.
- **Siri:** Use or not use Siri on the device.
- **FileVault:** Use FileVault to encrypt the startup disk. XenMobile 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:** Set up whether to share crash data and usage statistics with Apple.
- **Privacy:** Prevent users from seeing the Data and privacy pane during setup of ABM devices. For macOS 10.13 and later.
- **iCloud Analytics:** Prevent users from seeing the iCloud analytics screen during setup of ABM devices. For macOS 10.13 and later.
- **iCloud Documents and Desktop:** Prevent users from seeing the iCloud documents and desktop screen during setup of ABM devices. For macOS 10.13 and later.
- **Appearance:** Prevents the user from seeing the Choose Your Look screen during setup of the ABM devices. For macOS 10.14 and later.
- **Local account setup options:** Specify the settings to create an administrator account on the device. Users log in to their macOS device with this information. XenMobile creates the account, using the specified information.
  - **Create primary account as a standard user:** Instead of granting this user administrator privileges on the device, XenMobile creates the user with standard permissions. Because macOS requires an administrator account, XenMobile creates an administrator account first, then makes a new standard account and sets it as primary.
  - **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 XenMobile creates first.

Order Deployment Program enabled devices

You can order Deployment Program enabled devices directly from Apple or Deployment Program enabled authorized resellers or carriers. To order from Apple, provide your Apple Customer ID in the Apple Deployment Program Portal. Your Customer ID enables Apple to associate your purchased devices with your Apple Deployment Program account.

To order from your reseller or carrier, contact your Apple reseller or carrier to check if they participate in the Apple Deployment Program. Ask for the Apple Deployment Program ID of the reseller when purchasing devices. Apple requires that information when you add your Apple Deployment Program

reseller to your Apple Deployment Program account. After you add the Apple Deployment Program ID for the reseller, you receive a Deployment Program customer ID. Provide the Deployment Program customer ID to the reseller, who uses the ID to submit information about your device purchases to Apple. For more information, see this Apple Use Device Enrollment site.

Manage Deployment Program enabled devices

After your order ships, you can associate iOS, iPadOS, and macOS devices with your XenMobile server.

1. Sign in to Apple Business Manager using an administrator or device enrollment manager account.
2. In the sidebar, click **Devices**. Devices you purchased directly from Apple appear automatically. To assign devices from Apple Configurator 2 to Apple Business Manager, see Apple Business Manager User Guide.
3. In the list, select a device or the total number of devices and click **Edit Device Management**. You have two options:
   - To assign a device to an MDM server, under **Assign to Server**, choose the name of your XenMobile server. Click **Continue**.
     To assign new devices to Apple Business Manager in bulk, set a default XenMobile server for deployment. For more information, see Set a default server for bulk enrollment.
   - To unassign a device from the XenMobile server, choose **Unassign**.

Your Apple Deployment Program devices are now associated with the selected XenMobile server.

If you send in an iOS, iPadOS, or macOS device for servicing, you need to remove the device from Apple Business Manager. When you receive the serviced device back, you must reassign the device to the XenMobile server. When you replace the device, you can assign a new device to the XenMobile server using an order number.

To review the history of assigned devices:

1. Sign in to Apple Business Manager using an administrator or device enrollment manager account.
2. In the sidebar, click **Assignment History**. Then choose an assignment to view more information.
3. Click **Download** to download a CSV file with the serial numbers of all assigned and unassigned devices.

You can remove iOS, iPadOS, and macOS devices from Apple Business Manager if the device has been sold, stolen, or can't be repaired.

1. Sign in to Apple Business Manager using an administrator or device enrollment manager account.
2. In the sidebar, click **Devices** and search for a device.

3. Select a device and click **Release Device**. In the dialog box, confirm your changes to remove the device from the program. To add iOS and iPadOS devices back, use Apple Configurator 2. You can't add macOS devices back with Apple Configurator 2.

Enroll devices

March 25, 2021

To manage user devices remotely and securely, you enroll user devices in XenMobile. The XenMobile client software is installed on the user device and the user identity is authenticated. Then, XenMobile and the user profile are installed. Next, in the XenMobile console, you can perform device management tasks. You can apply policies, deploy apps, push data to the device, and lock, wipe, and locate lost or stolen devices.

Azure Active Directory enrollment is supported for iOS, Android, and Windows 10 devices. For more information about configuring Azure as your identity provider (IDP), see XenMobile Integration with Azure Active Directory as IDP.

> **Note:**
>
> Before you can enroll iOS device users, you must request an APNs certificate. For details, see Certificates and authentication.

To update configuration options for users and devices, go to the **Manage > Enrollment Invitations** page. For details, see Send an enrollment invitation in this article.

Android devices

> **Note:**
>
> For information about enrolling Android Enterprise devices, see Android Enterprise.

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. Enter your corporate credentials, such as your XenMobile Server name, User Principal Name (UPN), or email address. Then, click **Next**.
5. In the **Activate device administrator** screen, tap **Activate**.
6. Enter your corporate password and then tap **Sign On**.
7. Depending on the way XenMobile is configured, you may be asked to create a Citrix PIN. You can use the PIN to sign on to Secure Hub and other XenMobile-enabled apps, such as Secure Mail and Citrix Files. You enter your Citrix PIN twice. On the **Create Citrix PIN** screen, enter a PIN.

8. Reenter the PIN. Secure Hub opens. You can then access the XenMobile Store to view the apps you can install on your Android device.
9. If you configured XenMobile to push apps to devices automatically after enrollment, users are prompted to install the apps. In addition, policies that you configure in XenMobile 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 XenMobile console. You cannot perform actions on the device, however. You cannot track the device, and you cannot monitor the 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:

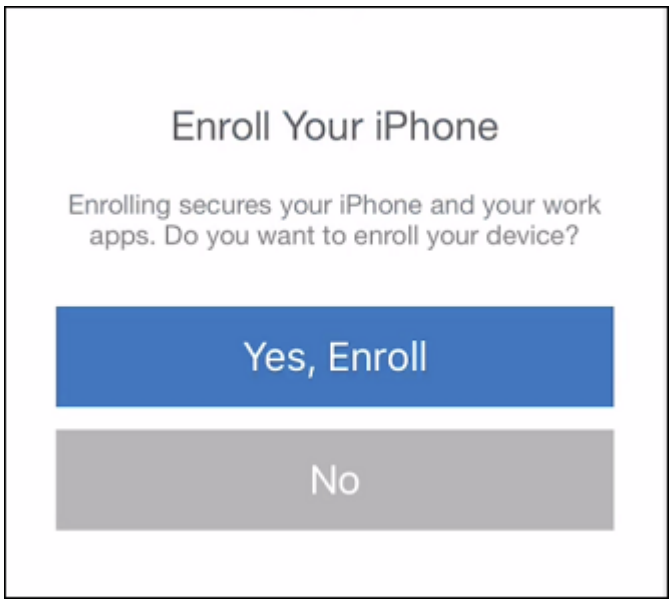
   - Tap the arrow next to your email address on the upper-right corner.
   - Tap **Preferences**, tap **Accounts**, and then tap **Delete Account**.
3. Tap **Re-Enroll**. A message appears to confirm you want to reenroll your device.
4. Tap **OK**.

   Your device is unenrolled.
5. Follow the on-screen instructions to reenroll your device.

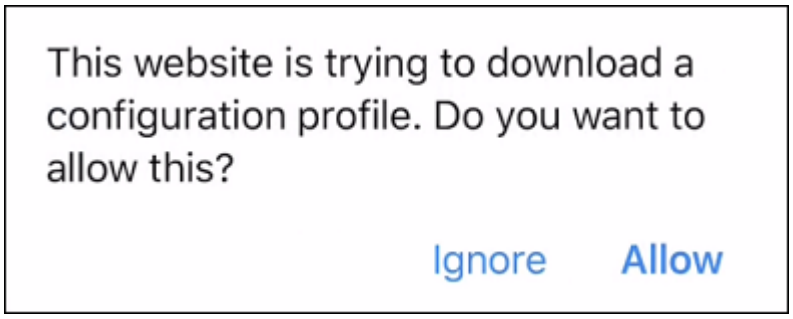
Enroll iOS devices

This section shows how users enroll iOS devices (12.2 or later) into XenMobile Server. For more information about the iOS enrollment, open the following video:

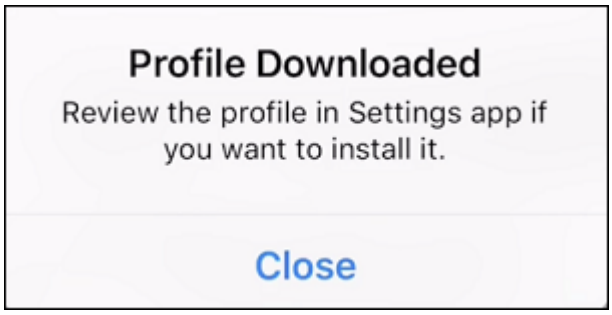
1. Go to the Apple store on your iOS device, download the Citrix Secure Hub app, and then tap the app.
2. When prompted to install the app, tap **Next** and then tap **Install**.
3. After Secure Hub installs, tap **Open**.
4. Enter your corporate credentials, such as your XenMobile Server name, User Principal Name (UPN), or email address. Then, click **Next**.
5. Tap **Yes, Enroll** to enroll your iOS device.



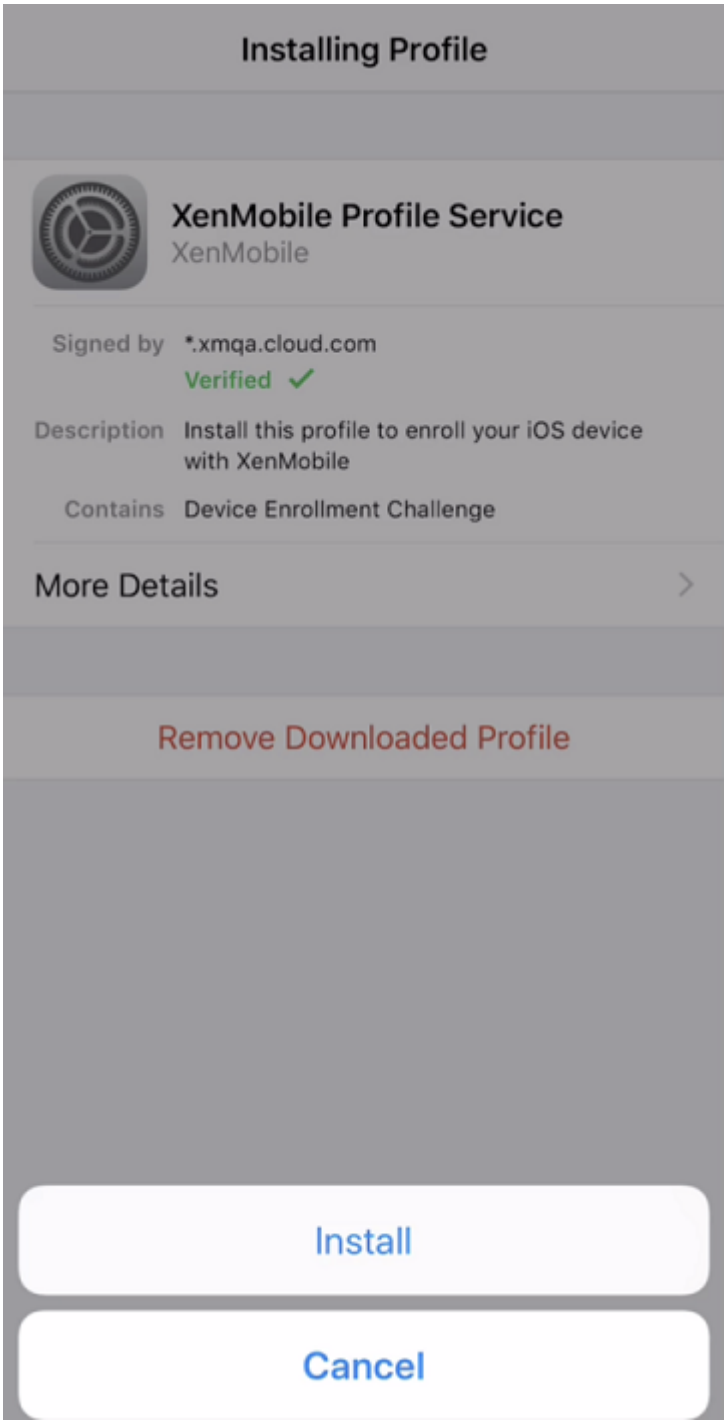
6. After you type your credentials, tap **Allow** when prompted, to download the configuration profile.



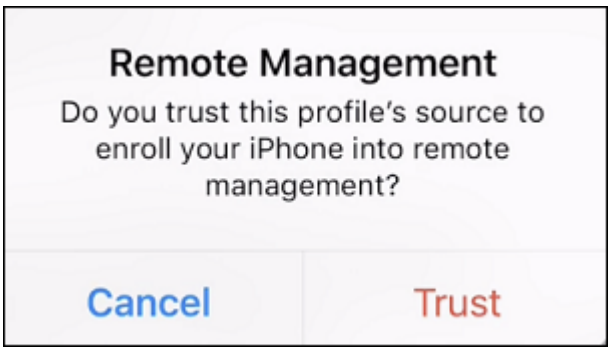
7. After you download the configuration profile, tap **Close**.



8. In your device settings, install the iOS certificate and add the device to the trusted list.
   - 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.



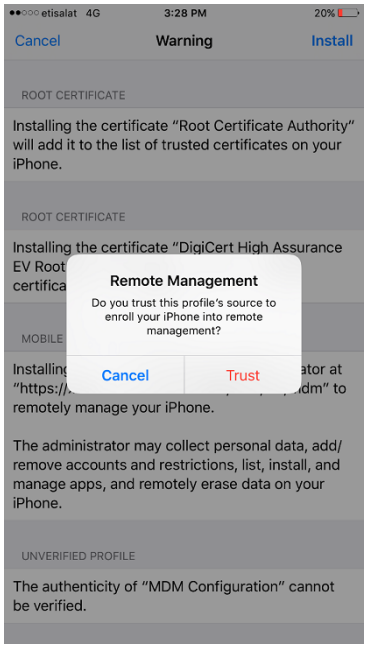
9. Sign in to Secure Hub. If you are enrolling into MDM+MAM: After your credentials validate, create and confirm your Citrix PIN when prompted.
10. After the workflow completes, the device is enrolled. You can then access the app store to view the apps you can install on your iOS device.

iOS devices

1. Download the Secure Hub app from the Apple iTunes App Store on the device and then install the app on the device.
2. On the iOS device Home screen, tap the Secure Hub app.
3. When the Secure Hub app opens, enter the server address that your help desk provided.

   The screens presented might differ from these examples, depending on how XenMobile is configured.
4. When prompted, enter your user name and password or PIN. Click **Next**.
5. When prompted to enroll, click **Yes, Enroll** and then enter your credentials when prompted.
6. Tap **Install** to install the Citrix Profile Services.

7. Tap **Trust**.



8. Tap **Open** and then enter your credentials.

macOS devices

XenMobile provides two methods to enroll devices that are running macOS. Both methods enable macOS users to enroll over the air, directly from their devices.

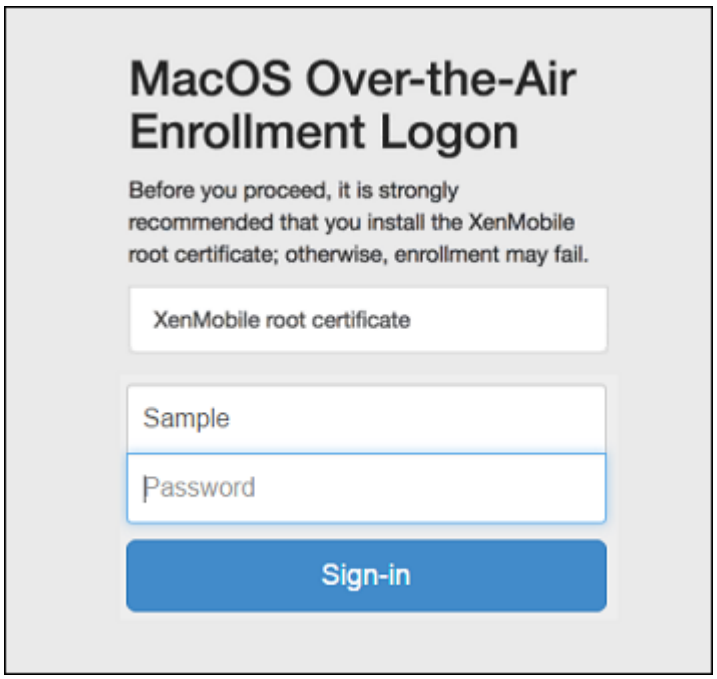
- **Send users an enrollment invitation:** This enrollment method enables you to set any of the following enrollment security modes for macOS devices:
  - User name + password
  - User name + PIN
  - Two Factor

  When the user follows the instructions in the enrollment invitation, a sign-on screen with the user name filled in appears.
- **Send users an installation 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 users an enrollment invitation

1. Optionally set up macOS device policies in the XenMobile console. For more information about device policies, see Device Policies.
2. Add an invitation for macOS user enrollment. For more information, see Send an enrollment invitation in this article.
3. After users receive the invitation and click the link, the following screen appears in the Safari browser. XenMobile fills in the user name. If you chose **Two Factor** for the enrollment security mode, another field appears.



4. 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 more information about certificates, see Certificates and authentication.
5. Users provide the requested credentials.

   The Mac device policies install. You can now start managing Macs with XenMobile just as you manage mobile devices.

Send users an installation link

1. Optionally set up macOS device policies in the XenMobile console. For more information about device policies, see Device Policies.
2. 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 XenMobile.
   - 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.
3. 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 more information about certificates, see Certificates and authentication.

4. Users sign on to their Macs.

   The Mac device policies install. You can now start managing Macs with XenMobile just as you manage mobile devices.

Windows devices

> **Note:**
>
> This section includes references to Windows Phone 8.1 devices, which Microsoft moved to End of Support on July 11, 2017. XenMobile supports Windows Phone 8.1 devices for MDM enrollment only.

Devices running Windows 10 enroll with Azure as a federated means of Active Directory authentication. 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 out-of-the-box the first time the device is powered on.
- Enroll in MDM as part of Azure AD Join from the Windows Settings page after the device is configured.

You can enroll devices in XenMobile that are running the following Windows operating systems:

- Windows 10 phone and tablet
- Windows Phone 8.1

Users can enroll directly through their devices.

> **Note:**
>
> For Windows 10 RS2 Phone and Tablet, during re-enrollment, a user isn't prompted for the Server URL. To work around this issue, restart the device. Or, on the email address screen, tap the X across from **Connecting to a service** to go to the Server URL page. This is a third-party issue.

You must configure autodiscovery and the Windows discovery service for user enrollment to enable the management of supported Windows devices.

Before Windows device users can enroll by using Azure, you must configure the Microsoft Azure server settings in XenMobile. For details, see Microsoft Azure Active Directory server settings.

To enroll Windows devices with self-discovery

To enable management of Windows devices, Citrix recommends you configure the AutoDiscovery Service and the Windows discovery service. For details, see XenMobile AutoDiscovery Service.

1. On the device, check for and install all available Windows Updates.
2. For Windows 10: In the charms menu, tap **Settings** and then tap **Accounts > Access work or school > Connect to work or school**. For Windows 8.1 phones: Tap **PC Settings > Network > Workplace**.

3. Enter your corporate email address and then tap **Continue** on Windows 10 or tap **Turn on device management** on Windows 8.1. To enroll as a local user, enter a nonexistent email address with the correct domain name (for example, `foo@mydomain.com`). This permits you to bypass a known Microsoft limitation where enrollment is performed by the built-in Device Management on Windows; in the **Connecting to a service** dialog box, enter the user name and password associated with the local user. The device automatically discovers a XenMobile Server and starts the enrollment process.
4. Enter your password. Use the password associated with an account that is part of a user group in XenMobile.
5. For Windows 10: In the **Terms of use** dialog box, indicate that you agree to have your device managed and then tap **Accept**. For Windows 8.1: In the **Allow apps and services from IT admin** dialog box, indicate that you agree to have your device managed and then tap **Turn on**.

To enroll Windows devices without self-discovery

It is possible to enroll Windows devices without autodiscovery. Citrix, however, recommends that you configure autodiscovery. Enrollment without autodiscovery results in a call to port 80 before connecting to the desired URL, so it is not considered best practice for production deployment. Citrix recommends that you use this process only in test environments and proof of concept deployment.

1. On the device, check for and install all available Windows Updates.
2. For Windows 10: In the charms menu, tap **Settings** and then tap **Accounts > Access work or school > Connect to work or school**. For Windows 8.1: Tap **PC Settings > Network > Workplace**.
3. Enter your corporate email address.
4. For Windows 10: If autodiscovery is not configured, an option appears where you can enter the server details, as described in step 5. For Windows 8.1: If **Automatically detect server address** is set to **on**, tap to turn the option **off**.
5. For Windows 10, in the **Enter server address** field, type the address: `https://serverfqdn:8443/serverInstance/wpe`.

   If a port other than 8443 is used for unauthenticated SSL connections, use that port number in place of 8443 in this address.

   For Windows 8.1: Type the server address in the following format: `https://serverfqdn:8443/serverInstance/Discovery.svc`.

   If a port other than 8443 is used for unauthenticated SSL connections, use that port number in place of 8443 in this address.
6. Type your password.

7. For Windows 10: In the **Terms of use** dialog box, indicate that you agree to have your device managed and then tap **Accept**. For Windows 8.1: In the **Allow apps and services from IT admin** dialog box, indicate that you agree to have your device managed and then tap **Turn on**.

To enroll Windows Phone devices

To enroll Windows Phone devices in XenMobile, 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 XenMobile 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, ensure that you have configured an Enterprise Hub policy (with a signed Secure Hub, Windows Phone app for each platform you support).

1. On the main screen of the Windows phone, tap the **Settings** icon.
   - For Windows 10: 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**.
   - For Windows 8.1: Tap **PC Settings > Network > Workplace** and then tap **Add Account**.
2. 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 Step 8.

   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`). This permits you to bypass a known Microsoft limitation; in the **Connecting to a service** dialog box, enter the user name and password associated with the local user.
3. On the next screen, type the web address of the XenMobile Server, such as: `https://<xenmobile_server>:<portnumber>/<instancename>/wpe`. For example, `https://mycompany.mdm.com:8443/zdm/wpe`.

   > **Note:**
   >
   > The port number has to be adapted to your implementation. It must be the same port that you used for an iOS enrollment.
4. Enter the user name and domain if authentication is validated through a user name and domain and then tap **sign in**.

5. On Windows Phone 8.1, when the account is added, you have the option of selecting **Install company app**. If your administrator has configured a Company App store, select this option and then tap **done**. If you clear this option, you will need to re-enroll your device to receive the Company app store.
6. On Windows Phone 8.1, on the **Account Added** screen, tap **done**.
7. To force a connection to the server, tap the refresh icon. If the device does not manually connect to the server, XenMobile attempts to reconnect. XenMobile connects to the device every 3 minutes 5 successive times, then every 2 hours afterward. You can alter this connection rate in the **Windows WNS Heartbeat 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.

Send an enrollment invitation

In the XenMobile console, you can send an enrollment invitation to users with iOS, macOS, and Android devices. You can also send an installation link to users with iOS or Android 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.

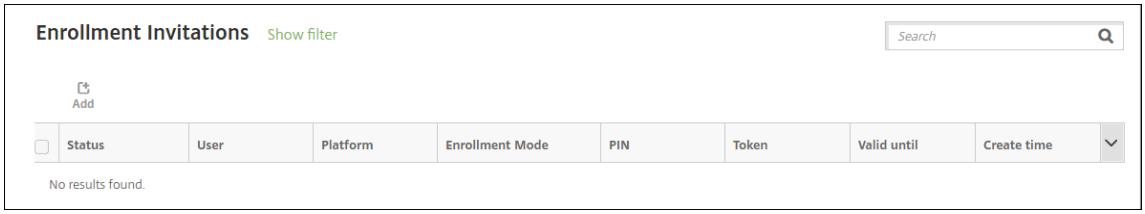
After users enroll, their devices appear as managed on **Manage > Devices**. The status of the invitation URL is shown as **Redeemed**.

Prerequisites

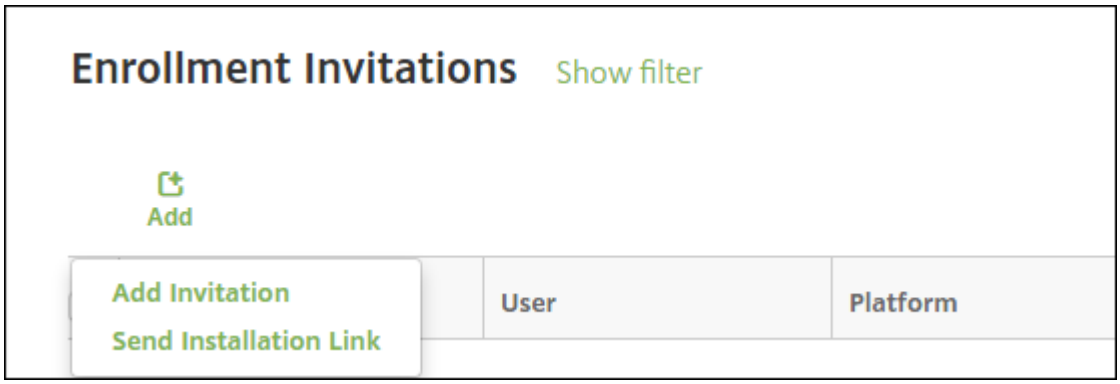
- XenMobile Server configured in Enterprise (XME) or MDM mode
- LDAP configured
- If using local groups and local users:
  - One or more local groups.
  - Local users assigned to local groups.
  - Delivery groups are associated with local groups.
- If using Active Directory:
  - Delivery groups are associated with Active Directory groups.

Create an enrollment invitation

1. In the XenMobile console, click **Manage > Enrollment Invitations**. The **Enrollment Invitations** page appears.



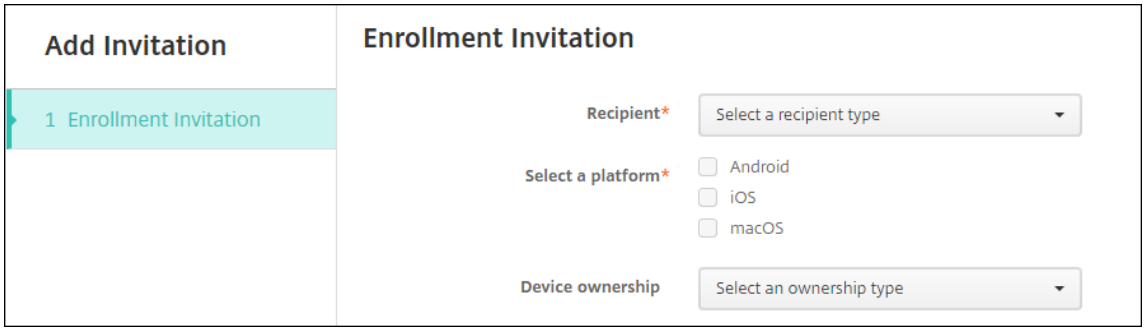
2. Click **Add**. A menu of enrollment options appears.



   - 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.

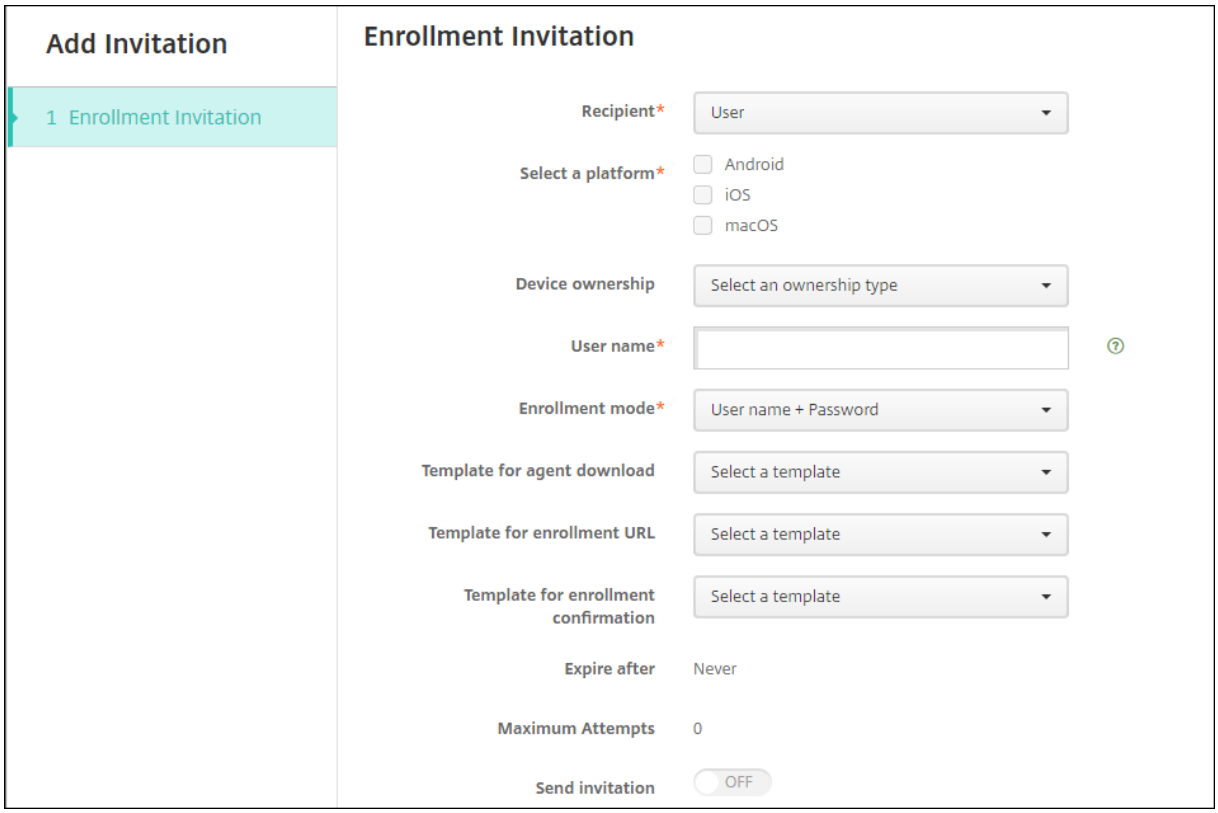


4. Configure these settings:

   - **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.
   - **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



1. Configure these **User** settings:

   - **User name:** Type a user name. The user must exist in the XenMobile Server as a local user or as a user in Active Directory. If the user is local, ensure that the email property of the user is set so you can send that user notifications. If the user is in Active Directory, ensure that LDAP is configured.
   - **Device info:** This setting doesn't appear if you select multiple platforms or if you select only macOS. Choose **Serial number**, **UDID**, or **IMEI**. After you choose an option, a field appears where you can type the corresponding value for the device.
   - **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

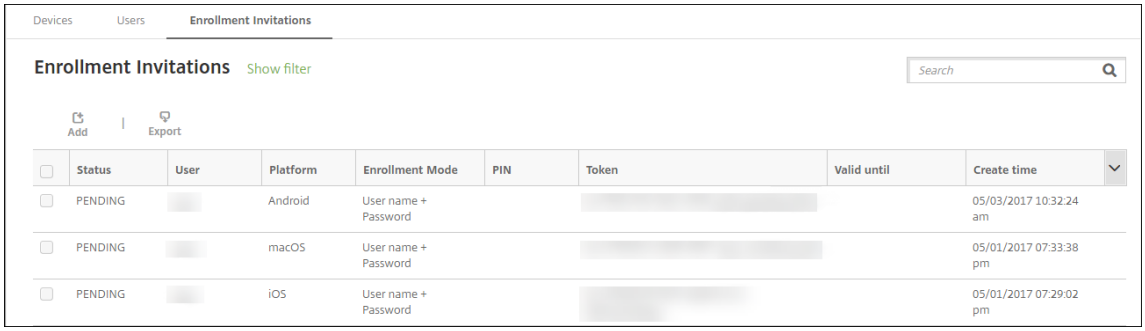
- Invitation URL
- Invitation URL + PIN
- Invitation URL + Password
- Two Factor
- User name + PIN

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, where you click **Enrollment PIN**.

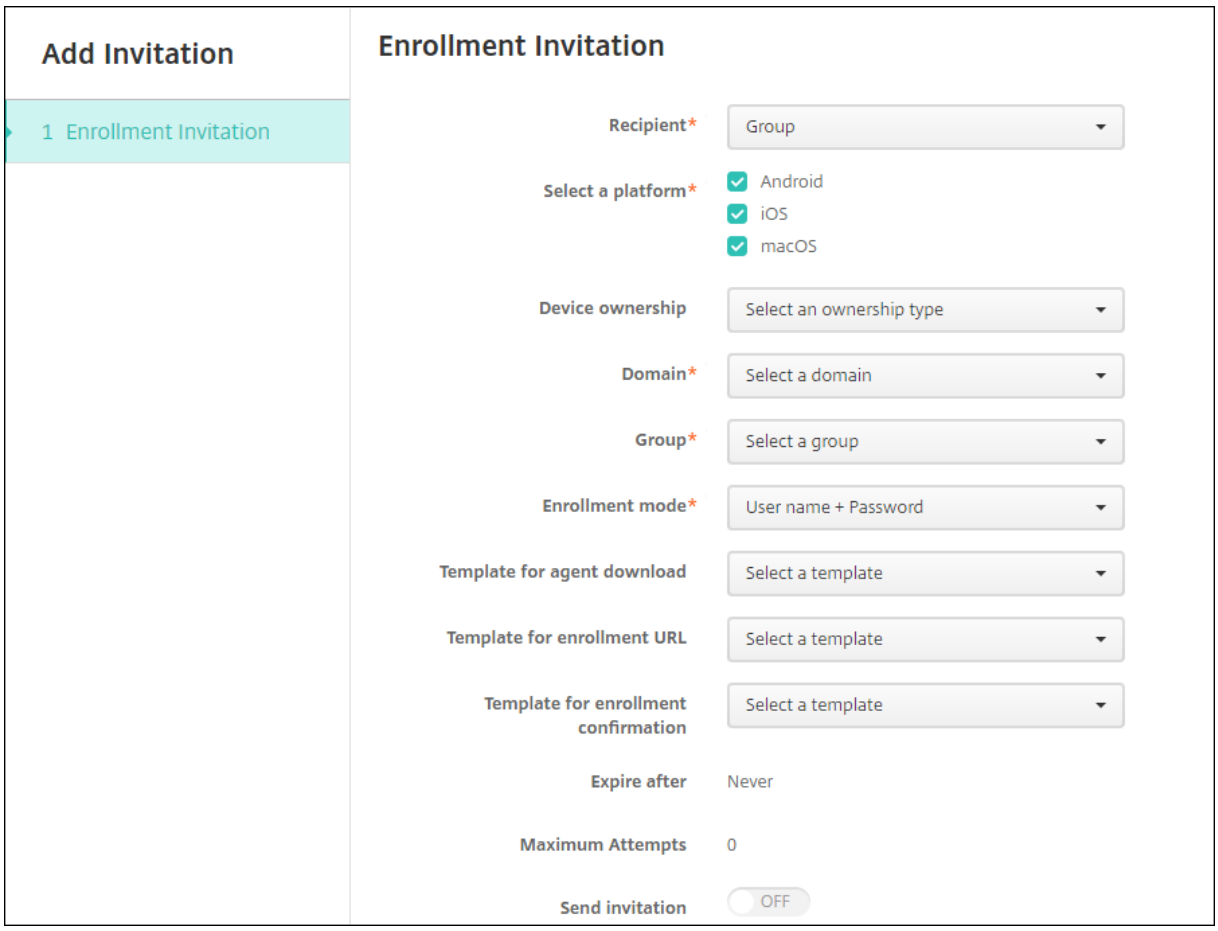
- **Template for agent download:** Choose the download link template named **Download link**. That template is for all supported platforms.
- **Template for enrollment URL:** Choose **Enrollment Invitation**.
- **Template for enrollment confirmation:** Choose **Enrollment Confirmation**.
- **Expire after:** This field is set when you configure the Enrollment Mode and indicates when the enrollment expires. For more information about configuring enrollment security modes, see To configure enrollment security modes.
- **Maximum Attempts:** This field is set when you configure the **Enrollment Mode** and indicates the maximum number of times the enrollment process occurs. For more information about configuring enrollment security modes, see To configure enrollment security modes.
- **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.



To send an enrollment invitation to a group

The following figure shows the settings for configuring an enrollment invitation to a group.



1. Configure these settings:

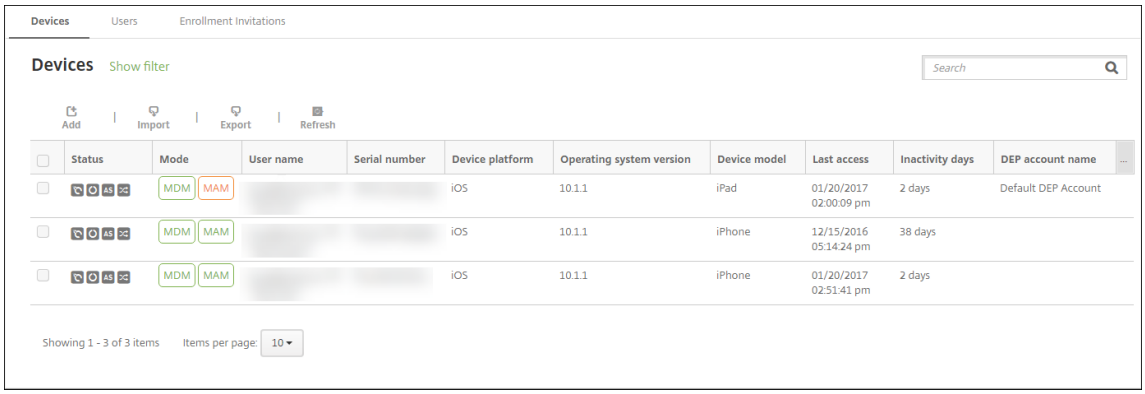
   - **Domain:** Choose the domain of the group to receive the invitation.
   - **Group:** Choose the group to receive the invitation.
   - **Enrollment mode:** Choose how you want users in the group to enroll. The default is **User name + Password**. Some of the following options aren't available for all platforms:
     - User name + Password
     - High Security
     - Invitation URL
     - Invitation URL + PIN
     - Invitation URL + Password
     - Two Factor
     - User name + PIN

   Only the enrollment security modes that are valid for each of the selected platforms appear.

   > **Note:**
   >
   > When you select any enrollment security mode that includes a PIN, the **Template for enrollment PIN** field appears, where you click **Enrollment PIN**.

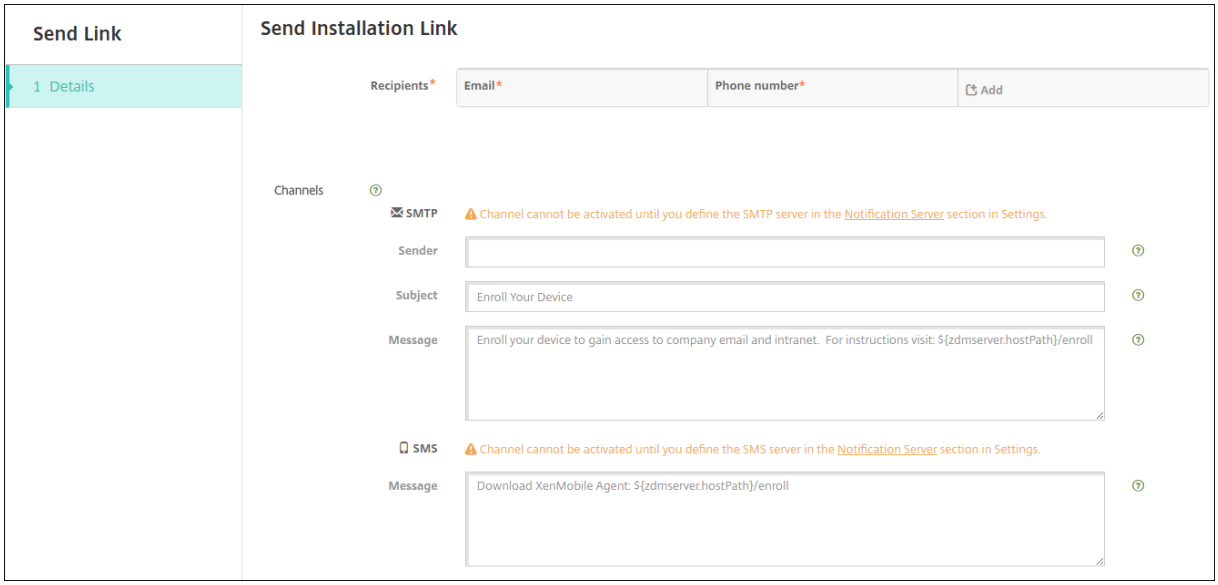
- **Template for agent download:** Choose the download link template named **Download link:**. That template is for all supported platforms.
- **Template for enrollment URL:** Choose **Enrollment Invitation**.
- **Template for enrollment confirmation:** Choose **Enrollment Confirmation**.
- **Expire after:** This field is set when you configure the Enrollment Mode and indicates when the enrollment expires. For more information about configuring enrollment security modes, see To configure enrollment security modes.
- **Maximum Attempts:** This field is set when you configure the Enrollment Mode and indicates the maximum number of times the enrollment process occurs. For more information about configuring enrollment security modes, see To configure enrollment security modes.
- **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.



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](/en-us/xenmobile/server/users/notifications.html



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 an existing 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 an existing recipient, hover over the line containing the listing and then click the pen icon on the right-hand 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.

> **Note:** 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.

Firebase Cloud Messaging

July 13, 2021

> **Note:**
>
> Firebase Cloud Messaging (FCM) was previously known as Google Cloud Messaging (GCM). Some XenMobile 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 XenMobile. XenMobile, 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 XenMobile server.

After you complete the configuration steps in this article and a device checks in, the device registers with the FCM service in XenMobile Server. That connection enables near real-time communication from your XenMobile service to your device by using FCM. FCM registration works for new device enrollments and previously enrolled devices.

When XenMobile 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

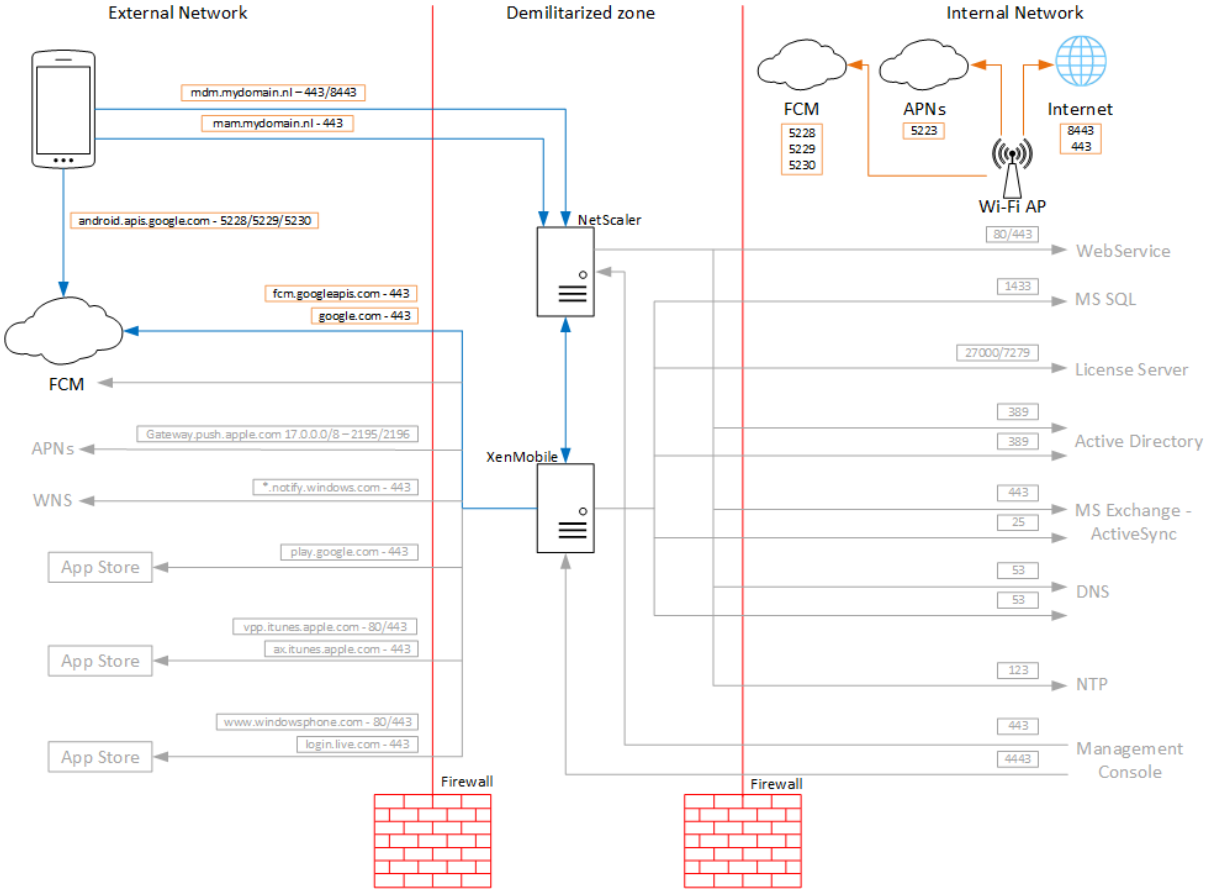
Firewall ports

- Open port 443 on XenMobile to `fcm.googleapis.com` and `Google.com`.
- Open outgoing, Internet communication for device Wi-Fi on ports 5228, 5229, and 5230.
- To allow outgoing connections, FCM recommends allowing ports 5228 through 5230 with no IP restrictions. However, if you require IP restrictions, FCM recommends allowing all the IP addresses in the IPv4 and IPv6 blocks. 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.

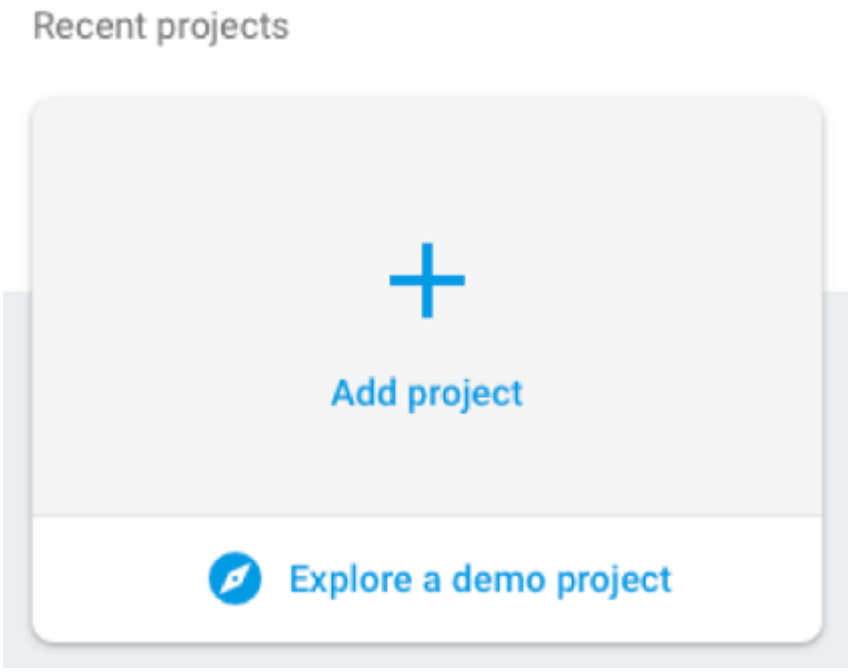


To configure your Google account for FCM

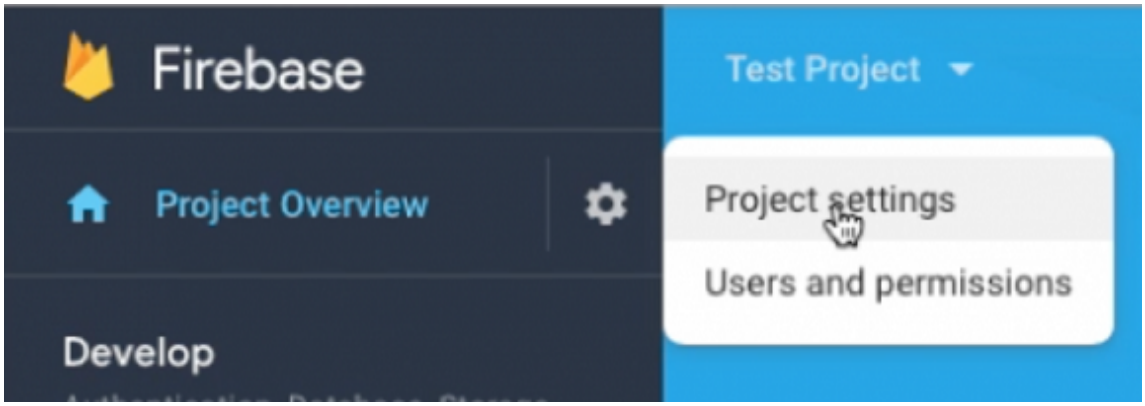
1. Sign in to the following URL using your Google developer account credentials:

   https://console.firebase.google.com/

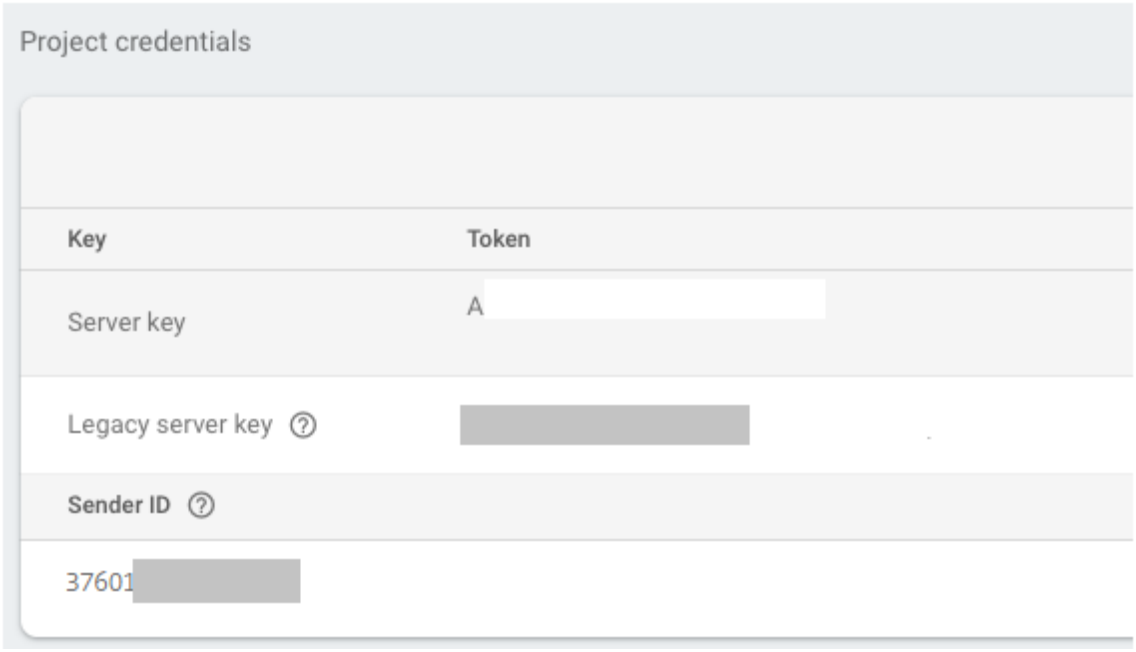
2. Click **Add project**.



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 XenMobile console. As of October 2016, you must create Server Keys in the Firebase console.

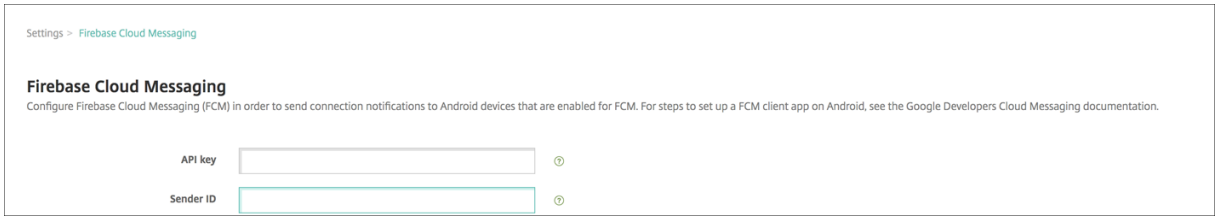


For steps to set up an FCM client app on Android, see this Google Developers Cloud Messaging article: https://firebase.google.com/docs/cloud-messaging/android/client.

To configure XenMobile for FCM

In the XenMobile 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.

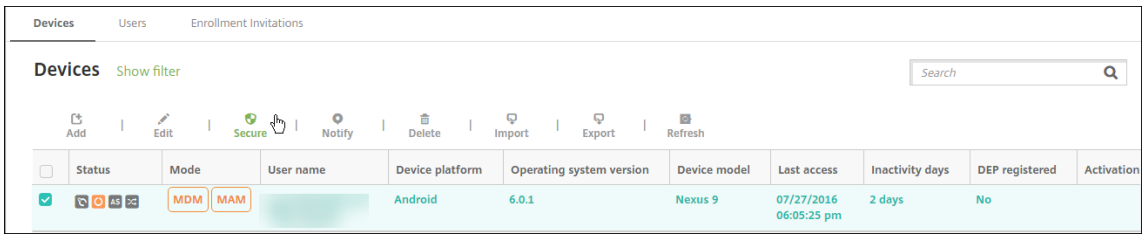


After you complete the setup, you can remove your Scheduling device policy or change that policy to connect less often.

To test your configuration

1. Enroll an Android device.
2. Leave the device idle for some time, so that it disconnects from XenMobile.

3. Sign in to the XenMobile console, click **Manage**, select the Android device, and then click **Secure**.



4. Under **Device Actions**, click **Selective Wipe**.

In a successful configuration, selective wipe occurs on the device.

Integrate with Apple Education features

April 20, 2021

You can use XenMobile as your mobile device management (MDM) solution in an environment that uses Apple Education. XenMobile support includes Apple School Manager (ASM) and Classroom app for iPad. The XenMobile 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 XenMobile, a Managed Apple ID account configured with a new password, and required volume purchase apps and iBooks.

Here are highlights of XenMobile support for Apple Education features.

Apple School Manager

ASM is a service that lets you set up, deploy, and manage iOS (iPadOS) devices and macOS laptops used in educational institutions. ASM includes a web-based portal that lets IT administrators:

- Assign Apple Deployment Program devices to different MDM servers.
- Purchase volume purchase licenses for apps and iBooks
- Create **Managed Apple IDs** in bulk. These customized Apple IDs provide access to Apple services such as storing documents in iCloud Drive and enrolling in Apple App Store courses.

You can add multiple ASM accounts to XenMobile. For example, this feature enables you to use different enrollment settings and Setup Assistant options by Education unit or department. You then associate ASM accounts with different device policies.

After you add an ASM account to the XenMobile console, XenMobile retrieves class and roster information. During device setup, XenMobile:

- Enrolls the devices.
- Installs the resources you configured for deployment, such as device policies (Education Configuration, Home screen layout, and so on).
- Also installs both apps and iBooks purchased through volume purchase.

You then provide the preconfigured devices to instructors and students. If a device is lost or stolen, you can use MDM Lost Mode feature to lock and locate 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, and share and open web links.

Classroom is free in the App Store. You upload the app to the XenMobile console. You then use the Education Configuration device policy to configure the Classroom app, which you deploy to instructor devices.

For more information about Apple Education features, see the Apple Education site and the Apple Education Deployment Guide from the same site.

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:**
>
> XenMobile doesn't validate ASM user accounts against LDAP or Active Directory. However, you can connect XenMobile 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 Active Directory users). Therefore, XenMobile deploys only required volume purchase apps and iBooks to instructor and student devices.

Prerequisites for Shared iPads

- Any iPad Pro, iPad 5th generation, iPad Air 2 or later, and iPad mini 4 or later
- At least 32 GB of storage
- Supervised

Configure Apple School Manager and XenMobile

After you purchase iPads from Apple or from Apple Authorized Resellers or carriers: Follow the workflow in this section to set up your ASM account and devices. This workflow includes steps that you perform in the ASM portal and in the XenMobile console.

Follow these instructions to configure your integration for any iPads that you use in a one-to-one model (one iPad per student) or for instructor iPads (unshared). To configure Shared iPads, see Configure Shared iPads.

Step 1: Create your Apple School Manager account and complete the Setup Assistant

If you plan to upgrade from Apple Deployment Program, see the Apple Support article, Upgrade your institution to ASM. To create your ASM account, go to https://school.apple.com/ 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, use a domain name that differs from the domain name for Active Directory. For example, prefix the domain name for ASM with something like `appleid`.
- 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 ASM User Guide, referenced earlier.

- You can customize the Managed Apple ID format for your institution, as described in the ASM User Guide, referenced earlier.

  > **Important:**
  >
  > Don’t change Managed Apple IDs after you import ASM information into XenMobile.

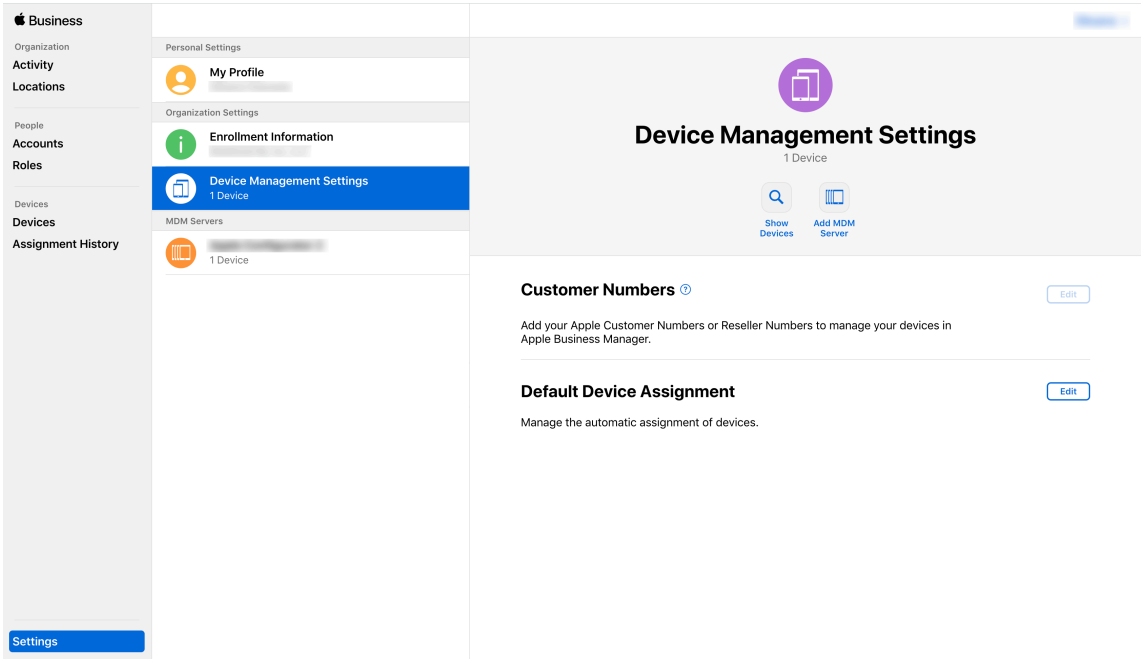
- If you purchased devices through resellers or carriers, link those devices to ASM. For information, see the ASM User Guide, referenced earlier.

Step 2: Configure XenMobile as the MDM Server for Apple School Manager and configure device assignments

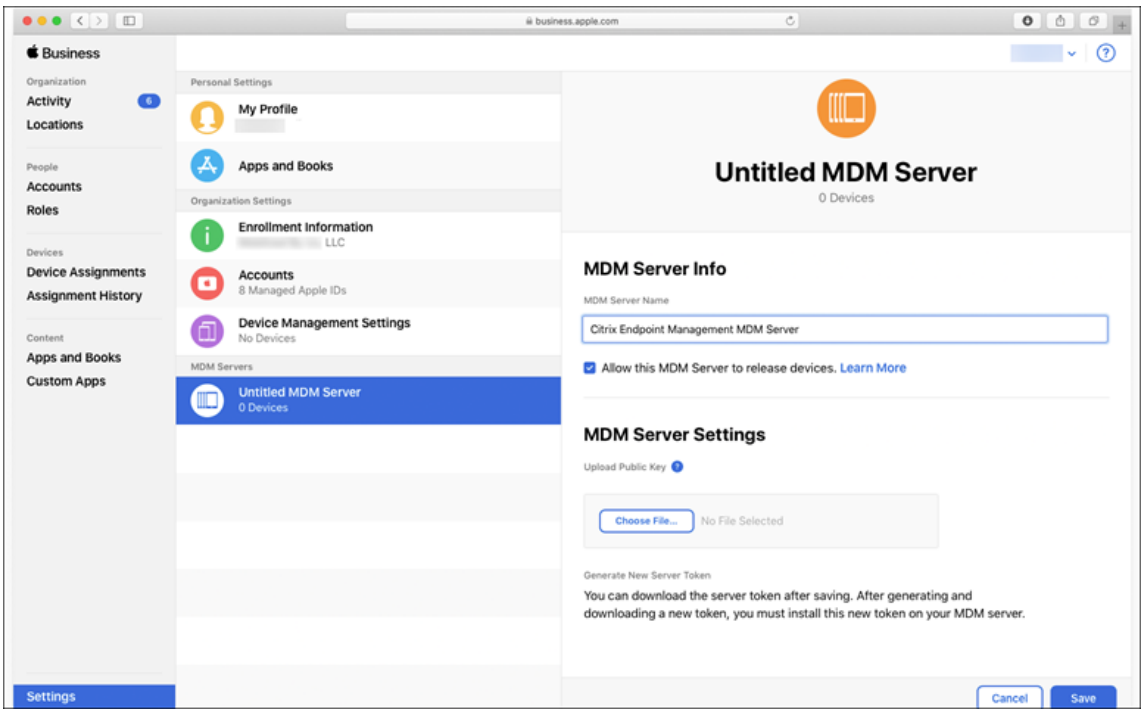
The ASM portal includes an **MDM Servers** tab. You need the public key file from XenMobile to complete that setup.

1. Download the public key for your XenMobile to your local computer: In the XenMobile console, go to **Settings > Apple Deployment Program**.

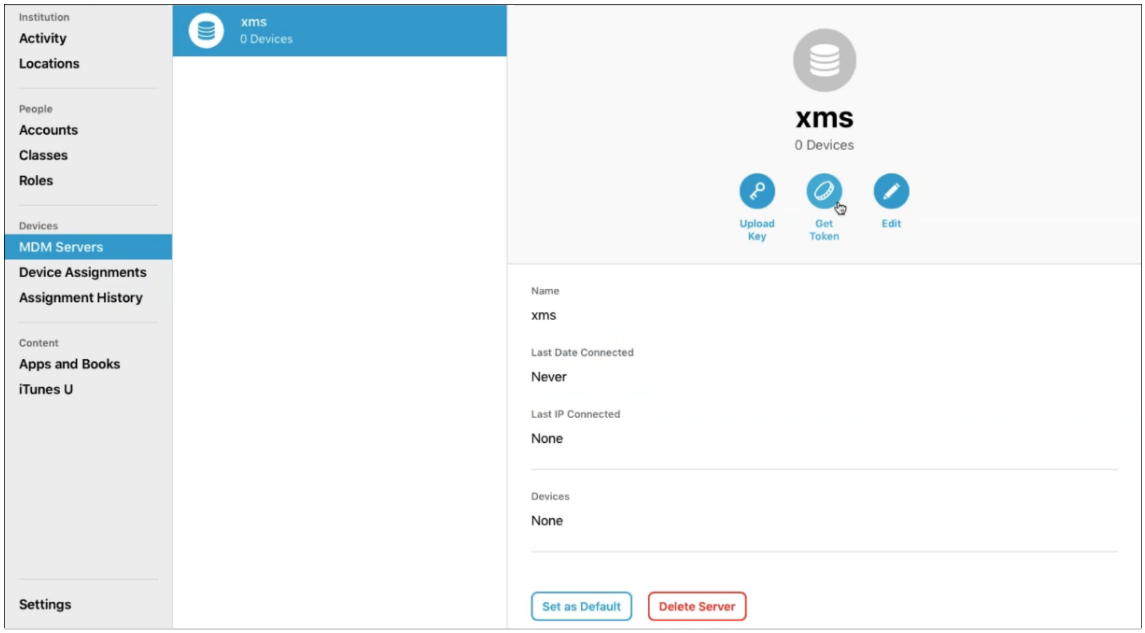
2. Under **Download Public Key**, click **Download** and then save the PEM file.
3. In the **Apple School Manager** portal, click **Settings**, then **Device Management Settings**. Click **Add MDM Server**.



4. Type a name for XenMobile. The server name that you type is for your reference and is not the server URL or name. Under **Upload Public Key**, click **Choose File**.



5. Upload the public key that you downloaded from XenMobile and then click **Save**.
6. Generate a server token: Click **Download Token** to download the server token file to your computer.

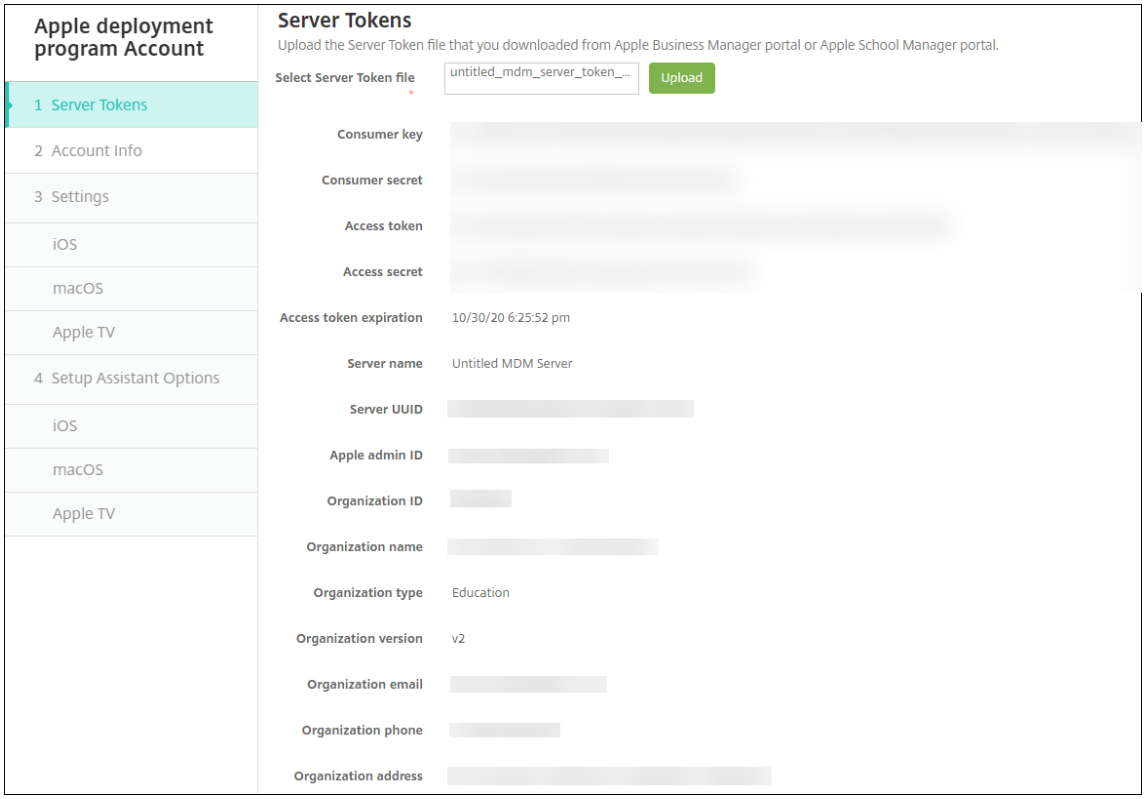


7. Under **Default Device Assignment**, click **Change**. Choose how you want to assign devices and then provide the information requested. For information, see the ASM User Guide.

Step 3: Add the Apple School Manager account to XenMobile

1. In XenMobile console, go to **Settings > Apple Deployment Program** and under **Add Apple Deployment Program Account**, click **Add**.

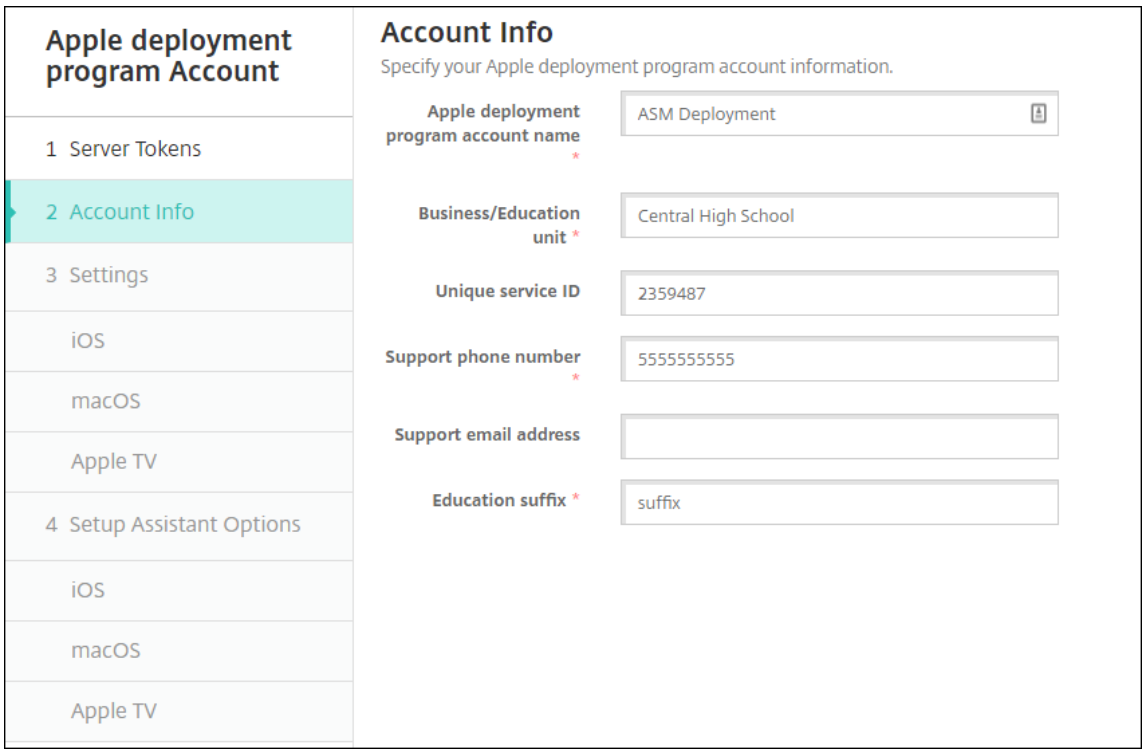
2. In the **Server Tokens** page, click **Upload** and choose the server token (a P7M file) file that you downloaded from the ASM portal. The token information appears.



Notes:

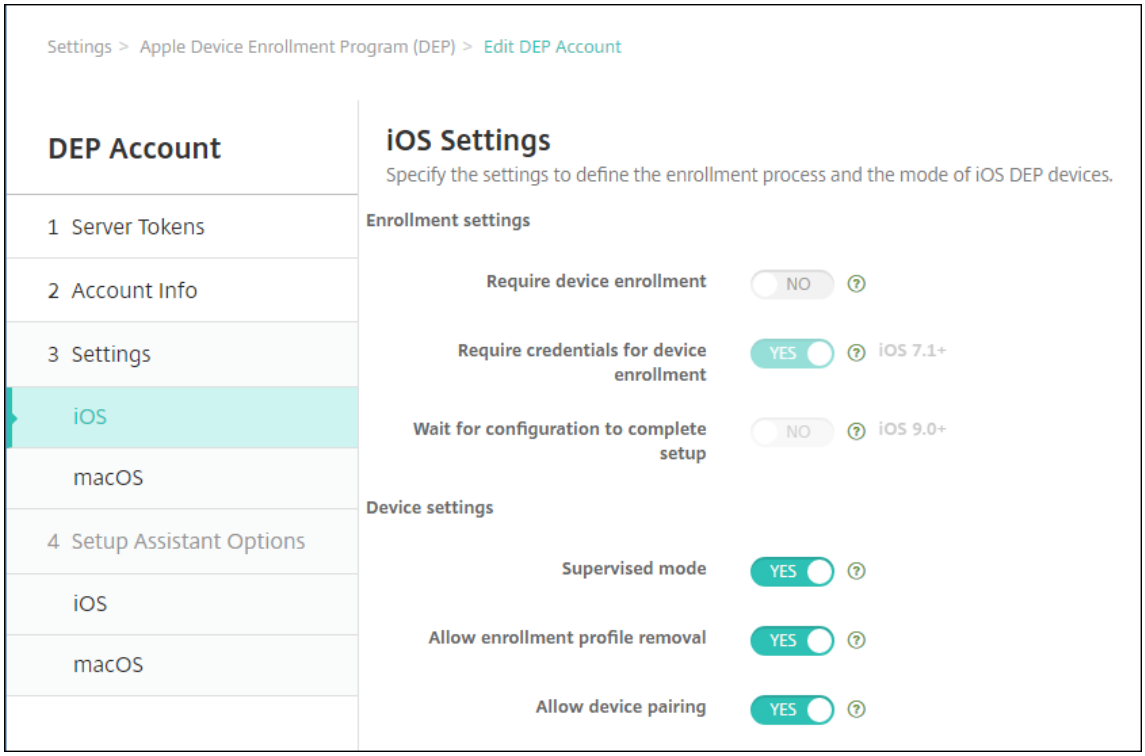
- **Organization ID** is your customer ID for Apple Deployment Program.
- ASM accounts have an **Organization type** of **Education** and an **Organization version** of **v2**.

3. In the **Account Info** page, specify the following settings.



- **Apple Deployment Program account name:** A unique name for this Apple Deployment Program account. Use names that reflect how you organize Apple Deployment Program accounts, such as by country or organizational hierarchy.
- **Business/Education unit:** The Education unit or department for device assignment. 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 can call for help during setup. This field is required.
- **Support email address:** An optional support email address available to end users.
- **Education suffix:** Flags the classes for a given ASM Deployment Program account. (The volume purchase suffix flags apps and iBooks for a given volume purchase account.) The recommendation is to use the same suffix for both accounts, ASM Deployment Program and ASM volume purchase.

4. Click **Next**. In **iOS Settings**, specify the following settings.

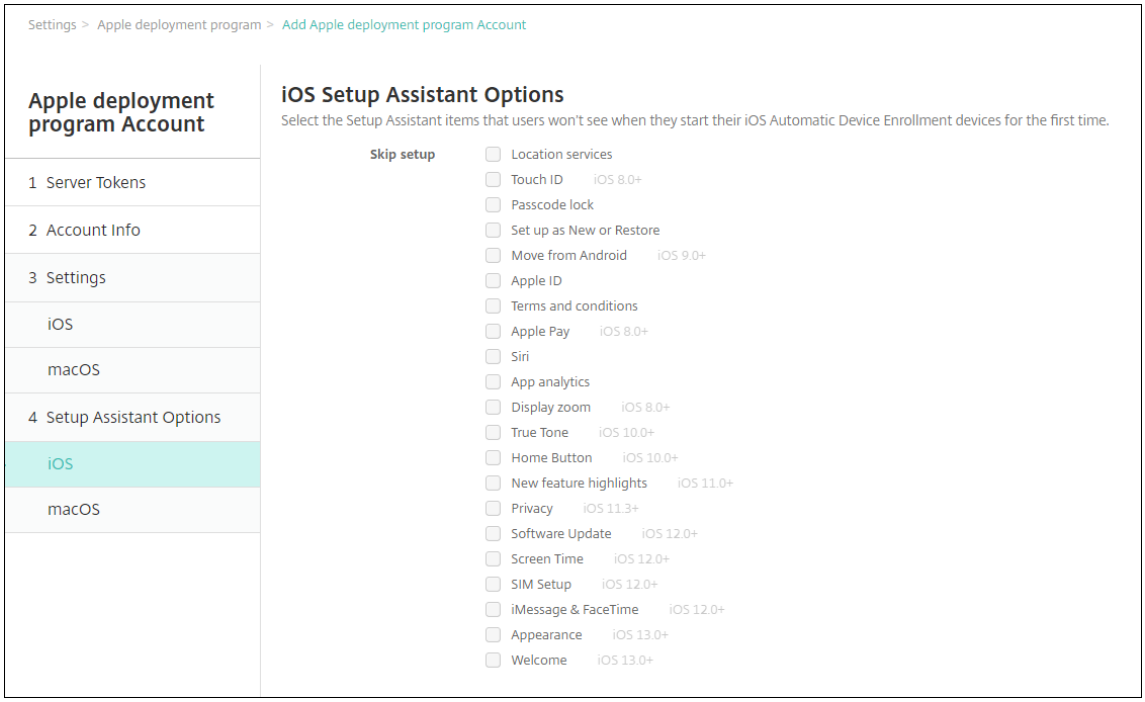


- **Enrollment settings**
  - **Require device enrollment:** Require users to enroll their devices. Change this setting to **No**.
  - **Require credentials for device enrollment:** Require users to enter their credentials during Apple Deployment Program setup. For ASM integration with XenMobile, this setting is **Yes** by default and can't be changed. Apple Deployment Program requires credentials for device enrollment.
  - **Wait for configuration to complete setup:** Whether to require user devices to remain in Setup Assistant mode until all MDM resources deploy to the device. For ASM integration with XenMobile, this setting is **No** by default. According to Apple documentation, the following commands might not work while a device is in Setup Assistant mode:
    * InviteToProgram
    * InstallApplication
    * InstallMedia
    * ApplyRedemptionCode
- **Device settings**
  - **Supervised mode:** Place iOS devices in supervised mode. Don't change the default, **Yes**. For details on placing an iOS device in supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator.

- **Shared mode:** Enable shared mode on iPads. Devices that don't meet the minimum requirements can't share.
- **Allow enrollment profile removal:** For ASM integration, allow user to remove the enrollment profile from the device. Change this setting to **Yes**.
- **Allow device pairing:** For ASM integration, allow device pairing so you can manage them through Apple App Store and the Apple Configurator. Change this setting to **Yes**.

5. In **iOS Setup Assistant Options**, select the iOS Setup Assistant steps to skip when users start their devices the first time. By default, the Setup Assistant includes all steps. Consider that removing steps from the Setup Assistant simplifies the user experience.

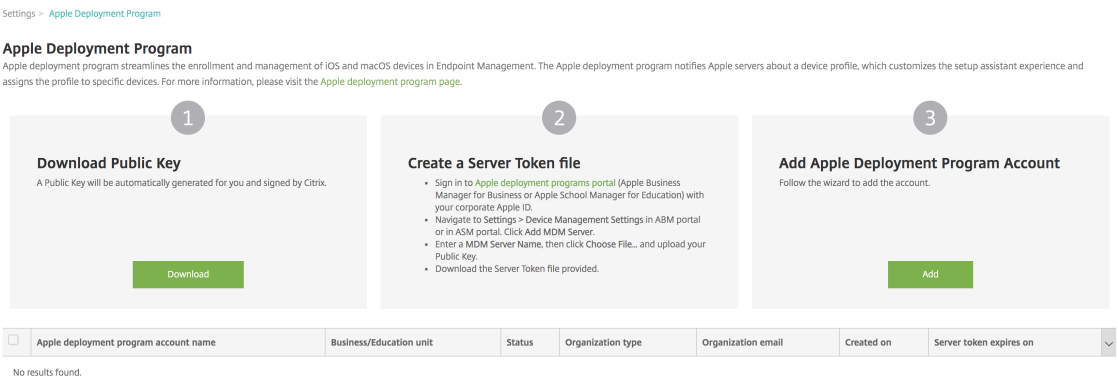
> **Important:**
>
> Citrix strongly recommends that you include the **Apple ID** and **Terms & Conditions** steps. Those steps enable instructors and students to provide their new Managed Apple ID passwords and accept the required terms and conditions.



- **Location services:** Set up the location service on the device.
- **Touch ID:** Set up Touch ID on iOS devices.
- **Passcode lock:** Create a passcode for the device.
- **Set up as New or Restore:** Set up the device as new or from an iCloud or Apple App Store backup.
- **Move from Android:** Enable 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).

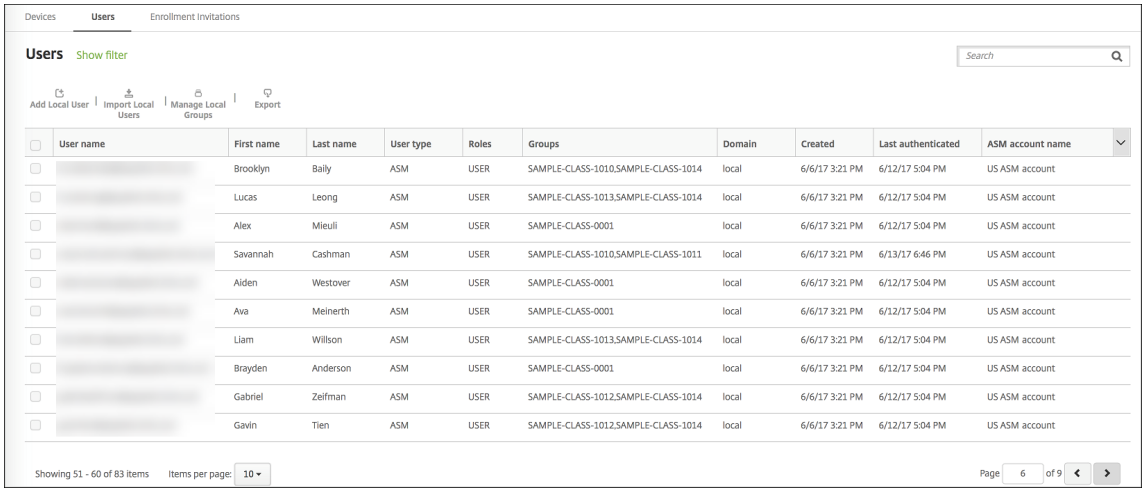
- **Apple ID:** Set up an Apple ID account for the device. Citrix recommends that you select the check box to include this step.
- **Terms and conditions:** Require users to accept terms and conditions for use of the device. Citrix recommends that you select the check box to include this step.
- **Apple Pay:** Set up Apple Pay on iOS devices.
- **Siri:** Use or not use Siri on the device.
- **App analytics:** Set up whether to share crash data and usage statistics with Apple.
- **Display zoom:** Set up the display resolution (either standard or zoomed) on iOS devices.
- **True Tone:** Set up the True Tone Display on iOS devices.
- **Home Button:** Set up the Home Button screen sensitivity.
- **New feature highlights:** Set up the onboarding informational screens, Access the Dock from Anywhere and Switch Between Recent Apps on iOS 11.0 devices (minimum version).
- **Privacy:** Prevent users from seeing the data and privacy pane during setup of Apple Deployment Program devices. For iOS 11.3 and later.
- **SoftwareUpdate:** Prevents the user from seeing the mandatory software update screen during setup of the Apple Deployment Program devices. For iOS 12.0 and later.
- **ScreenTime:** Prevents the user from seeing the Screen Time screen during setup of the Apple Deployment Program devices. For iOS 12.0 and later.
- **SIM Setup:** Prevents the user from seeing the Add Cellular Plan screen during setup of the Apple Deployment Program devices. For iOS 12.0 and later.
- **iMessage & FaceTime:** Prevents the user from seeing the iMessage and FaceTime screen during setup of the Apple Deployment Program devices. For iOS 12.0 and later.

6. The account appears on **Settings > Apple Deployment Program**. To test connectivity between XenMobile and your ASM account, select the account and click **Test Connectivity**.



A status message appears.

After a few minutes, the user accounts from ASM appear on **Manage > Users** page. XenMobile creates local user accounts based on the imported Managed Apple ID for each user. In the following example, the domain name prefix of customized Apple IDs for user accounts is `appleid`.

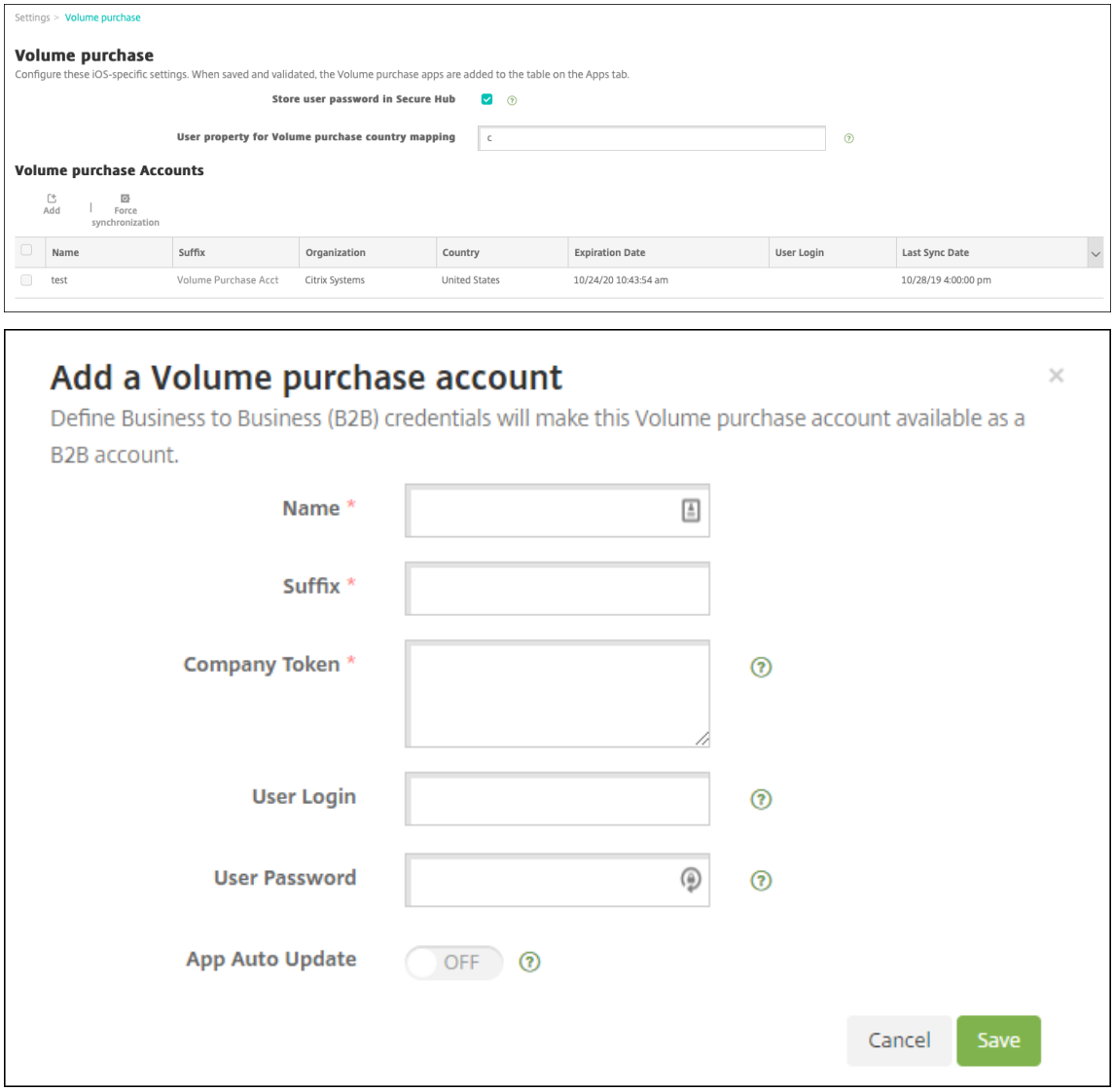


To find all users for a given ASM account, type the account name in the user search filter.

Step 4: Configure an Education volume purchase account for Apple School Manager

In this section, you point XenMobile to the volume purchase account that you use to purchase volume purchase licenses for apps and iBooks.

1. To configure an Education volume purchase account for ASM, follow the instructions in Apple Volume Purchase. The Add a volume purchase account screen requires that you supply a Company Token. Download your token directly from your Education volume purchase account and paste it into the **Add a Volume purchase account** screen.



2. Wait a few minutes for the volume purchase licenses to import into XenMobile.

Step 5: Add passwords for Apple School Manager users

After you add an ASM account, XenMobile imports classes and users from ASM. XenMobile treats classes as local groups and uses the term “group” in the console. If a class has a group name in ASM, XenMobile assigns the group name to the class. Otherwise, XenMobile uses the source system ID for the group name. XenMobile doesn’t use the course name for the class name because course names in ASM aren’t unique.

XenMobile 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, XenMobile doesn’t use a directory server to authenticate these new users.

ASM doesn’t send temporary user passwords to XenMobile. 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 XenMobile. 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`

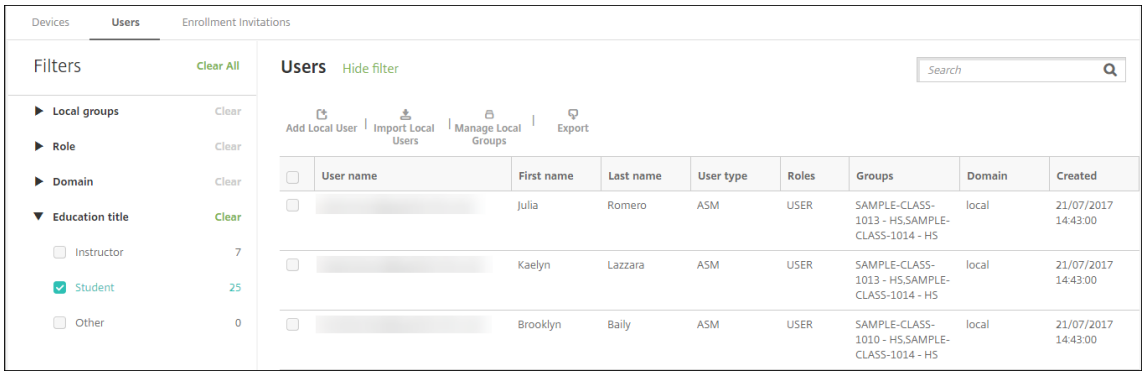
   Middle name: `Middle`

   Last name: `Lastname`

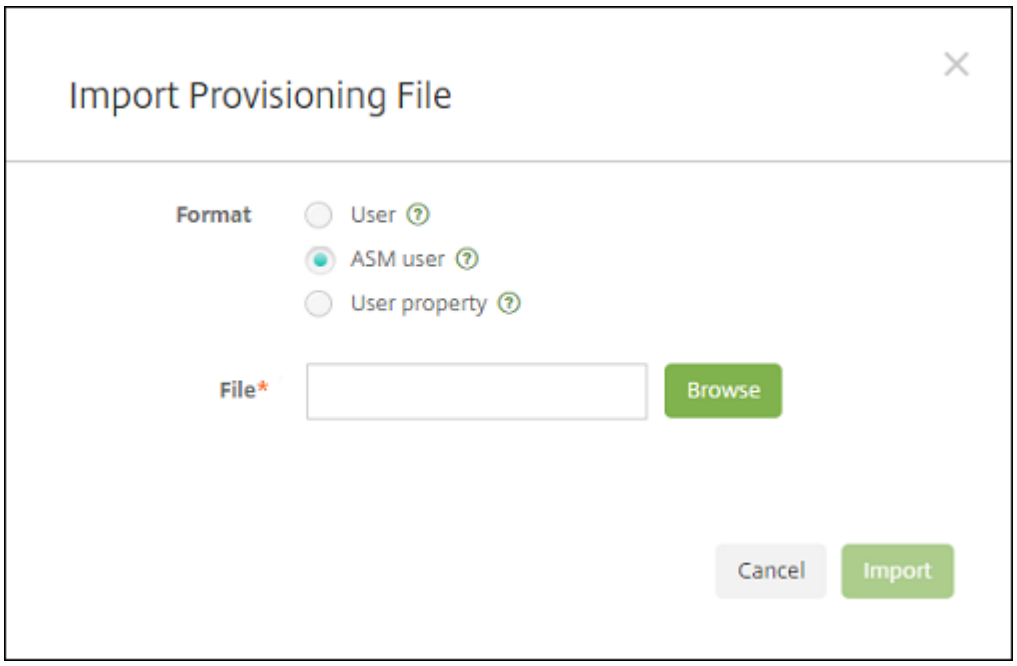
   Password: `Password123!`
3. In the XenMobile console, click **Manage > Users**. The **Users** page appears.

   The following **Manage > Users** screen sample shows a list of users imported from ASM. In the **Users** list:

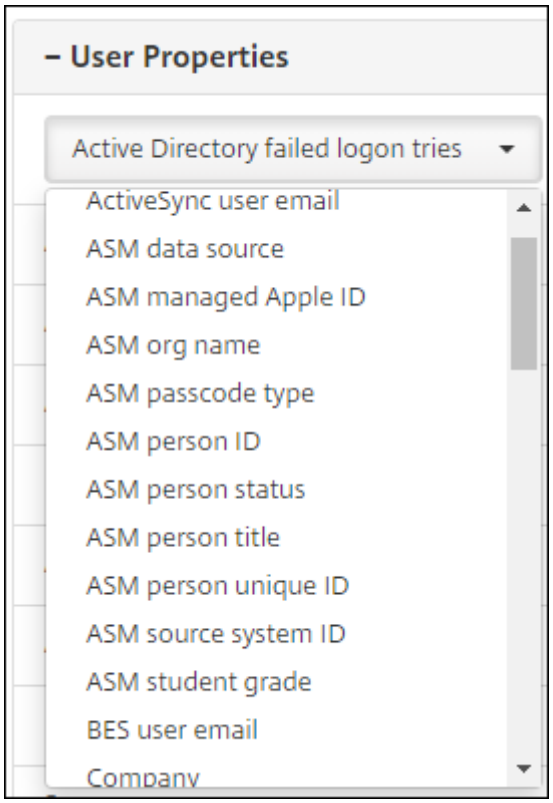
   - **User name** shows the managed Apple ID.
   - User type is **ASM**, to indicate the account originated from ASM.
   - **Groups** show the classes.



4. Click **Import Local Users**. The **Import Provisioning File** dialog box appears.
5. 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. XenMobile requires a Managed Apple ID for authentication.

- **ASM org name:** The name you gave the account in XenMobile.
- **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).

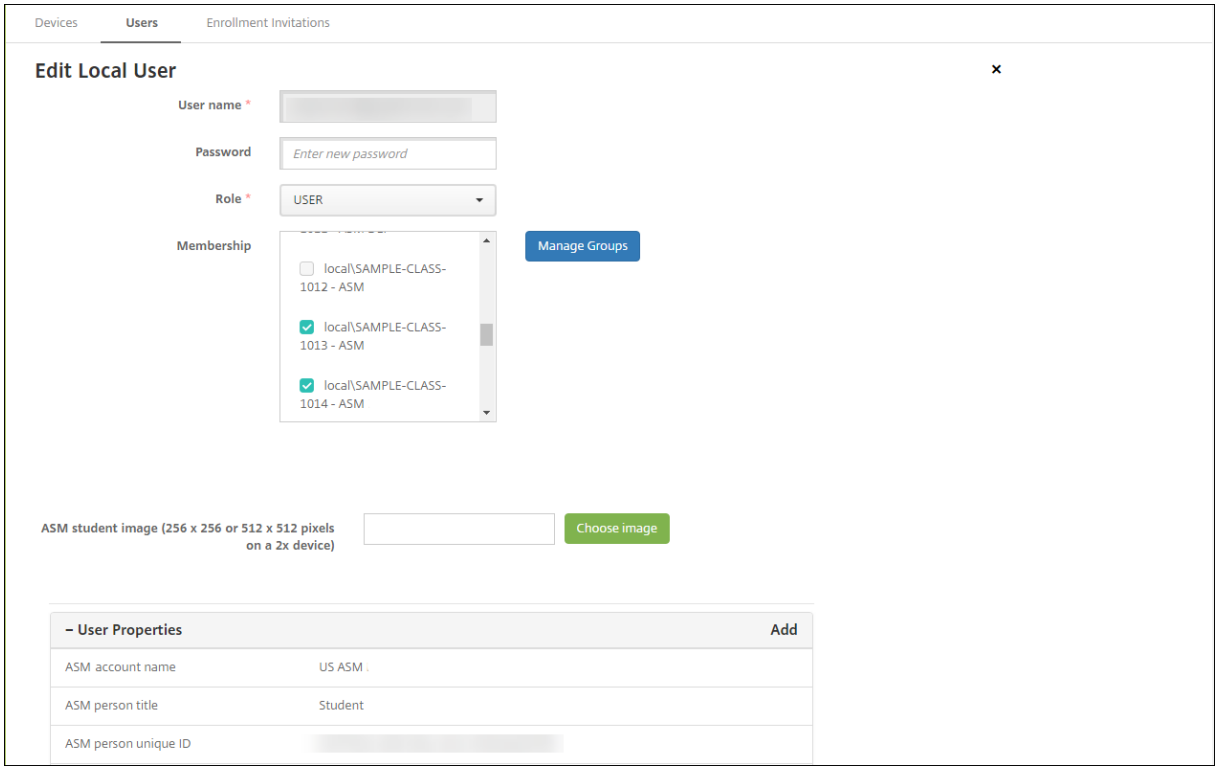
Step 6: Optionally add photos of students

You can add a photo of each student. If the instructors use the Apple Classroom app, the photos appear in this app.

Recommended for photos:

- Resolution: 256 x 256 pixels (512 x 512 pixels on a 2x device)
- Format: JPEG, PNG, or TIFF

To add a photo, go to **Manage > Users**, select a user, click **Edit**, and then click **Choose image**.



Step 7: Plan and add resources and delivery groups to XenMobile

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:

  XenMobile requires that you deploy volume purchase apps as required apps for education users. XenMobile doesn't support deploying such volume purchase apps as optional.

  If you use the Apple Classroom app, deploy it only to instructor devices.

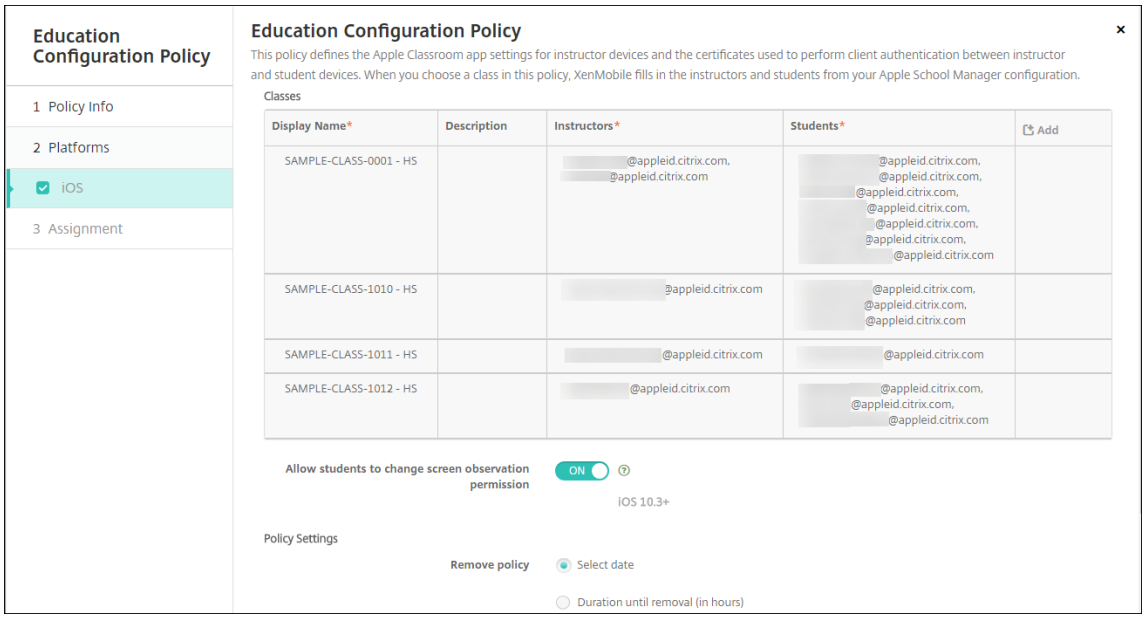
  Deploy any other apps that you want to provide to instructors or students. This solution doesn't use Citrix Secure Hub app, so there's no need to deploy it to instructors or students.

- Volume purchase iBooks:

  After XenMobile connects to your ASM account, your purchased iBooks appear in the XenMobile console, in **Configure > Media**. The iBooks listed on that page are available to add to delivery groups. XenMobile 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 XenMobile 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.

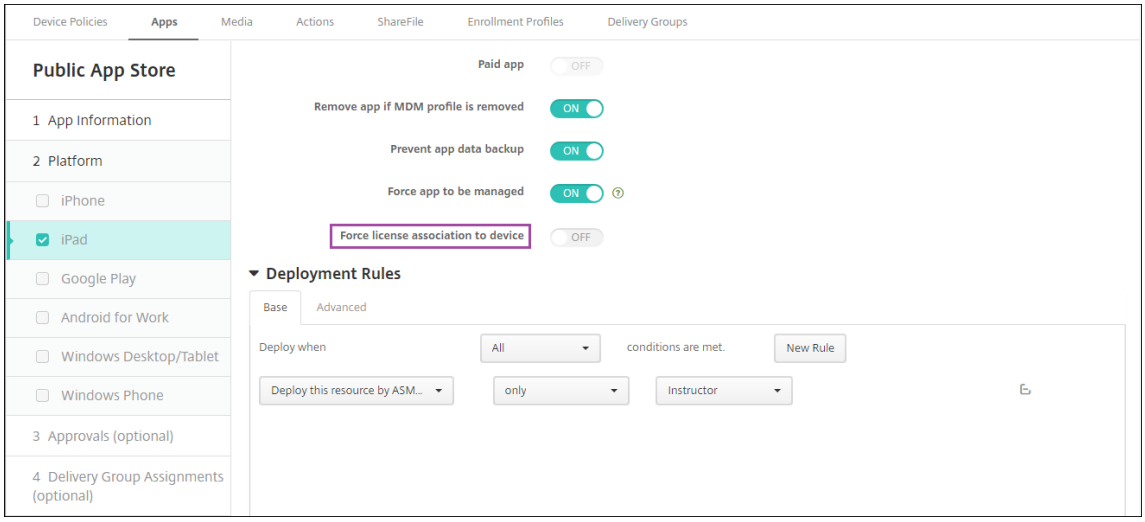


   For information about device policies, see Device policies and the individual policy articles.

2. Configure apps (**Configure > Apps**) and iBooks (**Configure > Media**):

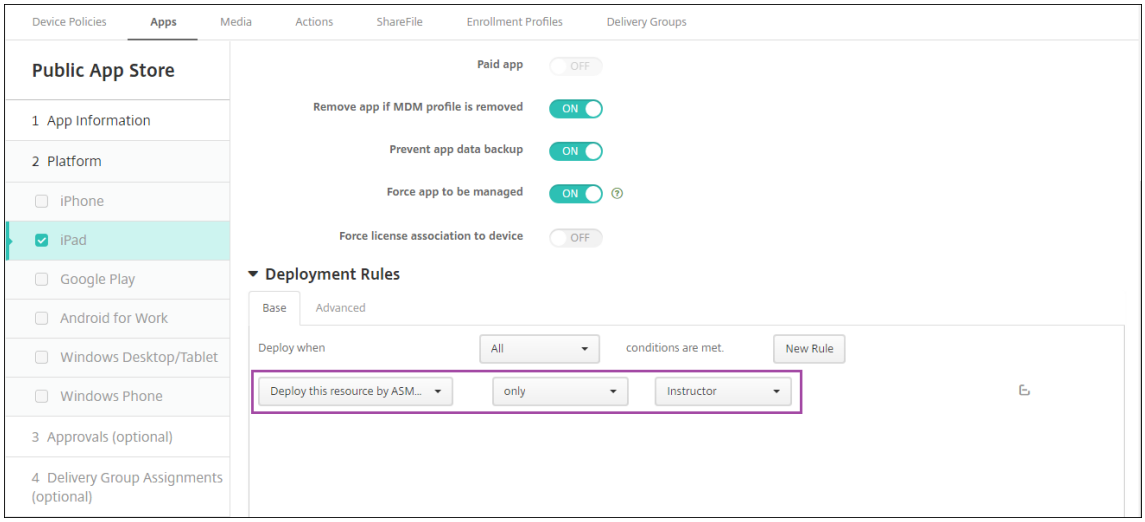
   - By default, XenMobile assigns apps and iBooks at the user level. During first-time deployment, instructors and students receive a prompt to register to ASM. After accepting the invitation, users receive their ASM apps and iBooks at the next deployment (within six hours). Citrix recommends that you 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 Apple volume purchase.



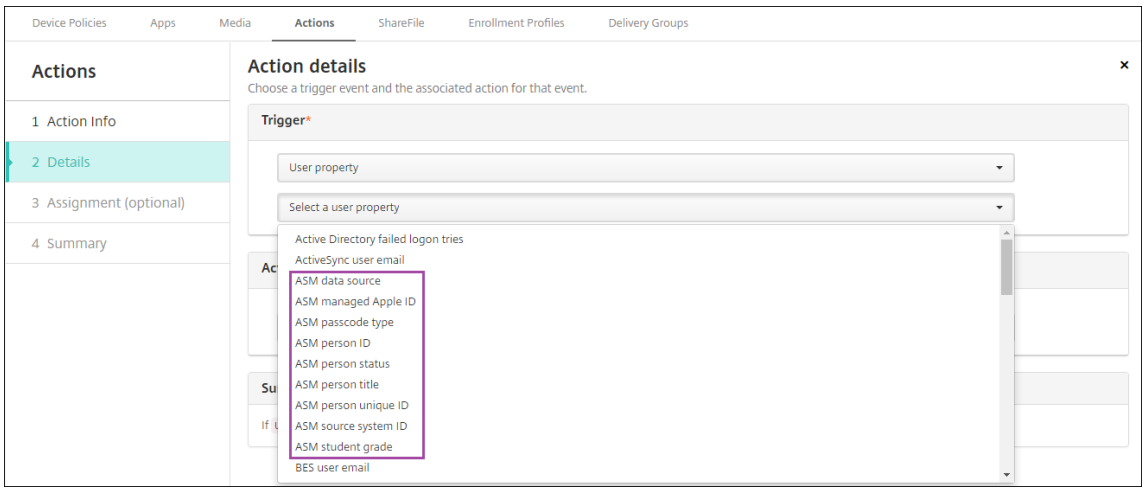
- To deploy an app only to instructors, select a delivery group that includes only instructors or use the following deployment rule:

```
Deploy this resource by ASM device type
only
Instructor
<!--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.

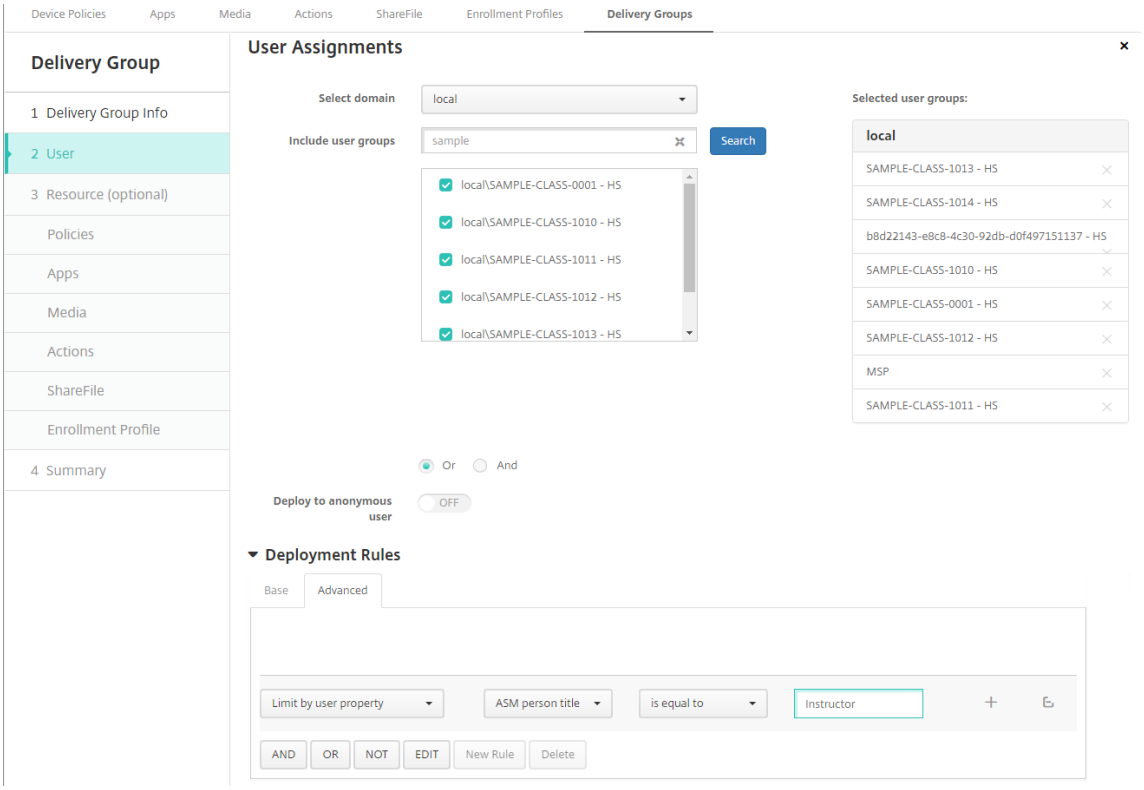


To create an action, go to **Configure > Actions**. For information about configuring actions, see Automated actions.

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.

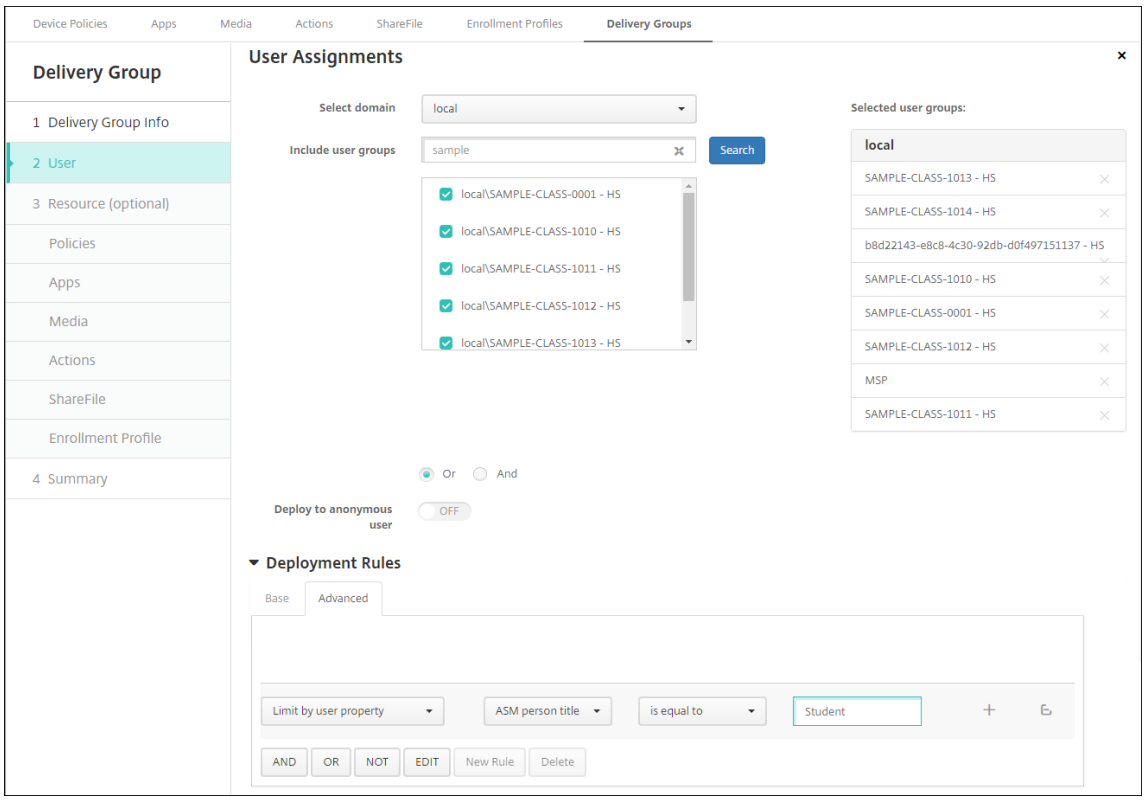
   For example, the following user assignments are for instructors. The deployment rule is:

```
Limit by user property
ASM person title
is equal to
Instructor
<!--NeedCopy-->
```

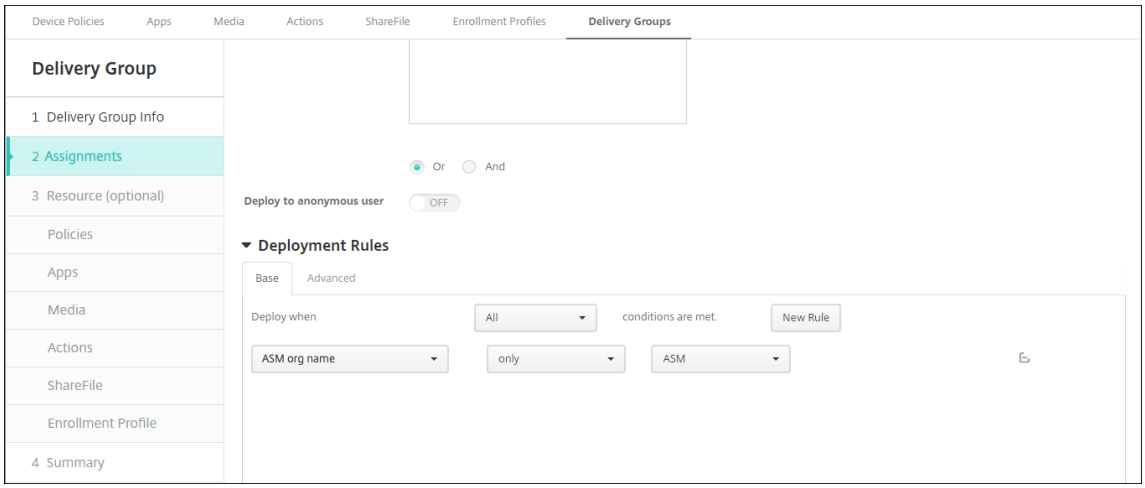



The following user assignments are for students. The deployment rule is:

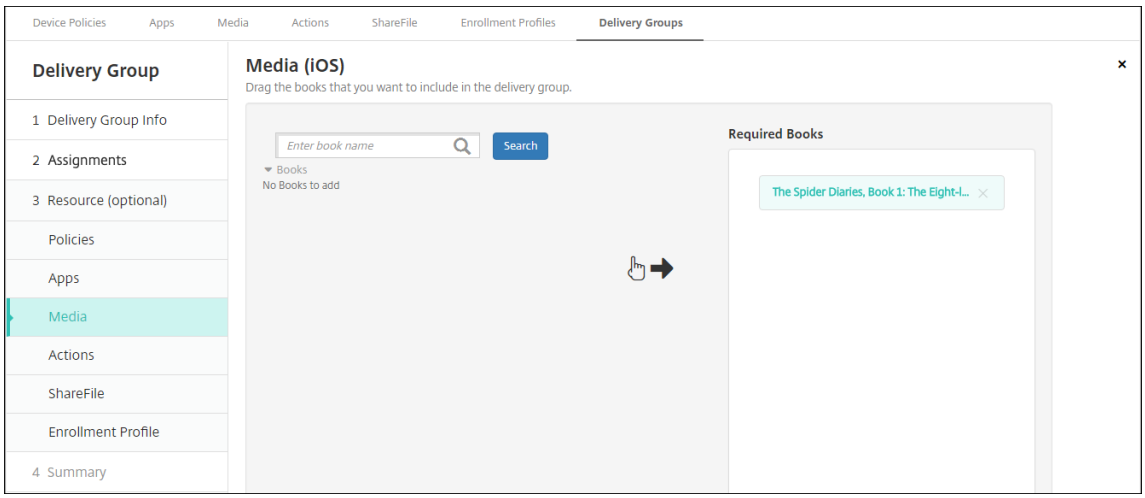
```
Limit by user property
ASM person title
is equal to
Student
<!--NeedCopy-->
```

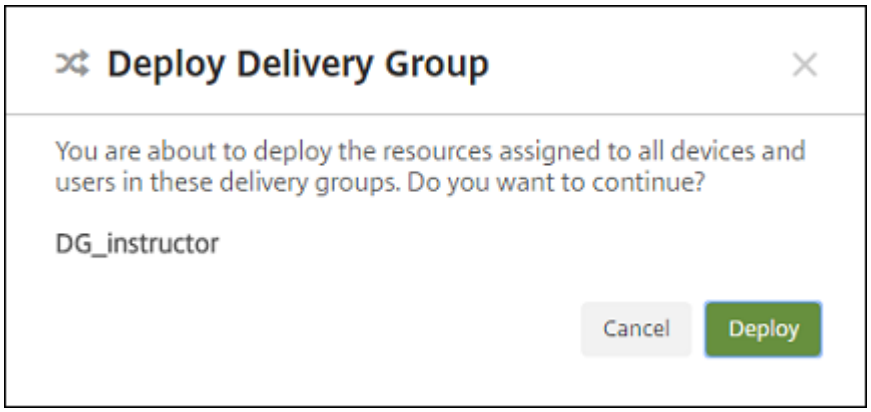
You can also filter a delivery group by using a deployment rule based on the ASM org name.



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.

Step 8: Test instructor and student device enrollments

You can enroll devices through either of the following methods:

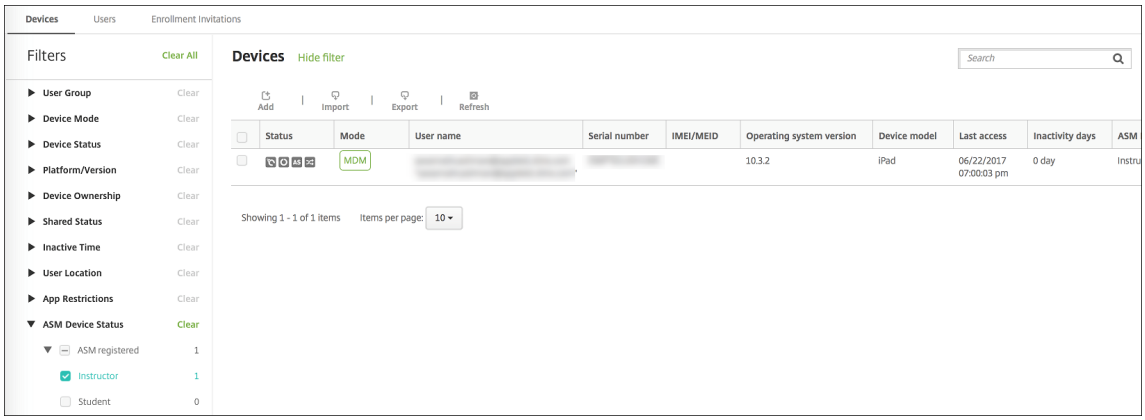
- A school administrator can enroll instructor and student devices by using the user password you can set in the XenMobile console. As a result, you can provide users with devices that are already set up with apps and media.
- When users receive the devices, they enroll using the user password that you provide to them. After enrollment completes, XenMobile sends device policies, apps, and media to the devices.

To test enrollment, use Apple Deployment Program devices that are linked to ASM.

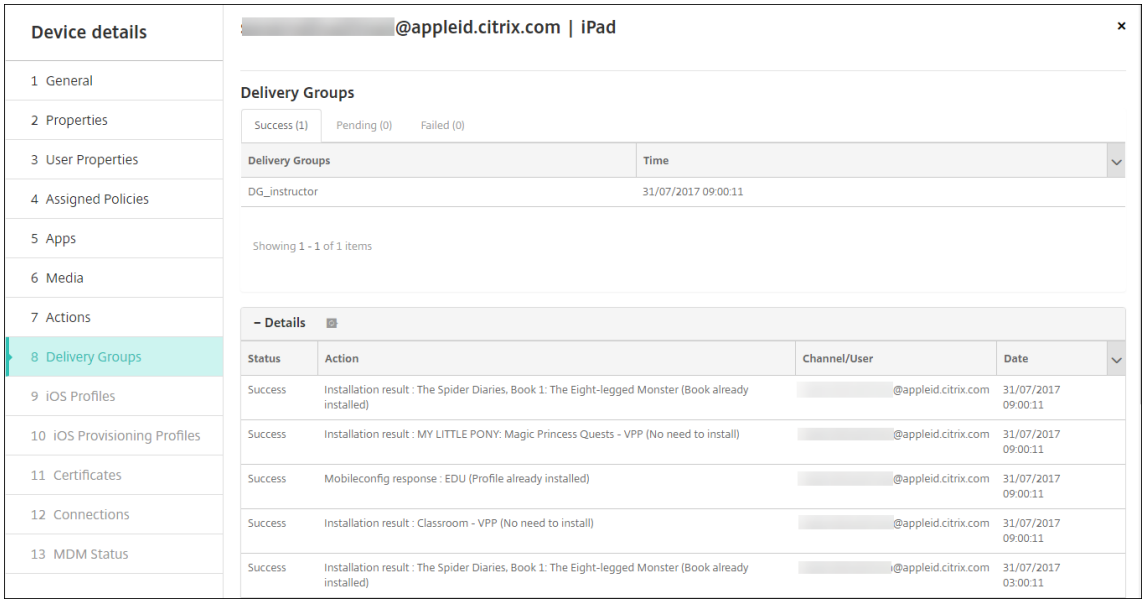
1. If the devices aren’t linked to ASM, erase the device contents and settings by performing a hard reset.

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.



Step 9: 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:

- XenMobile 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, XenMobile prompts them in the enrollment screen to enroll their device.
2. The user provides their Managed Apple ID and XenMobile password used to authenticate to XenMobile.
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, XenMobile 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).

Configure Shared iPads

Multiple students in a classroom can share an iPad for different subjects taught by one or several instructors.

Either you or instructors enroll Shared iPads and then deploy device policies, apps, and media to the devices. After that, students 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.

XenMobile uses two communications channels for Shared iPads: The system channel for the device owner (instructor) and the user channel for the current resident user (student). XenMobile 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

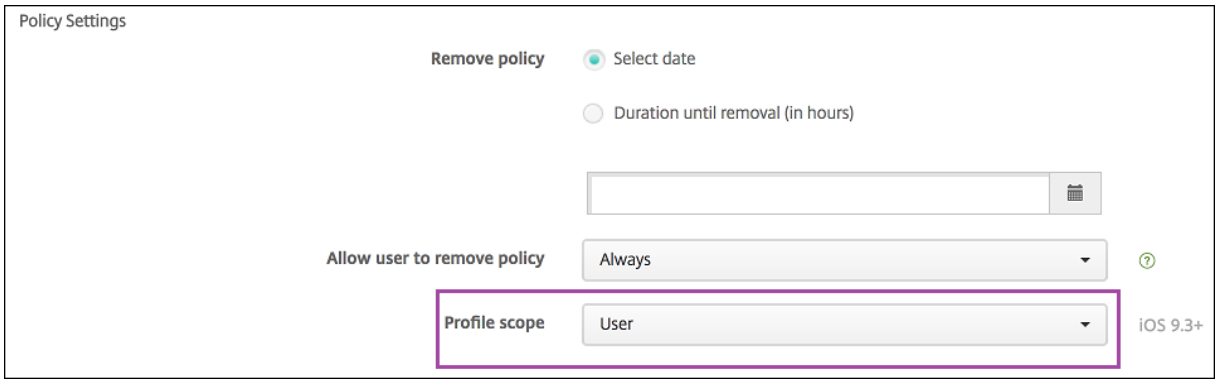
  Apple supports assignment of user-based volume purchase iBooks on Shared iPads.

Resources that deploy over the user channel are:

- Device policies: Apps Notifications, Home Screen Layout, and Restrictions

  XenMobile supports only those 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 instructors. The instructors then distribute the devices to students. If you don't distribute pre-enrolled Shared iPads to instructors: Be sure to provide the instructors with their XenMobile server passwords so they can enroll their devices.

The general workflow for configuring and enrolling Shared iPads is as follows.

1. Use the XenMobile server console to add ASM accounts (**Settings > Apple Deployment Program**) with **Shared mode** enabled. For more information, see "Manage ASM accounts for Shared iPads" next.
2. As described in this section, add the required device policies, apps, and media to XenMobile. Assign those resources to delivery groups.
3. Have the instructors perform a hard reset on the Shared iPads. The Remote Management screen for enrollment appears.
4. The instructors enroll the Shared iPads.
   XenMobile deploys configured resources to each enrolled Shared iPad. After an automatic restart, instructors can share the devices with students. A sign in page appears on the iPad.
5. A student chooses the class and then enters their Managed Apple ID and temporary ASM (ASM) password.
   The Shared iPad authenticates to ASM and prompts the student to create an ASM password. For the next sign into the Shared iPad, the student provides the new ASM password.
6. Another student who is sharing the iPad can then sign in by repeating the previous step.

Manage ASM accounts for Shared iPads

If you already use XenMobile with Apple Education: You have an existing ASM account configured in XenMobile for devices that aren't shared, such as the devices used by instructors. You can use the same ASM and the same XenMobile server for both shared and non-shared devices.

XenMobile supports these deployment scenarios:

- A group of Shared iPads per class

  In this scenario, you assign the Shared iPads to a class of students. The iPads stay in the classroom. Instructors who teach different subjects in that class use the same set of iPads.

- A group of Shared iPads per instructor

  In this scenario, you assign the Shared iPads to an instructor, who uses those iPads for the various classes that they teach.

Organize Shared iPads into device groups

ASM 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, per class or per instructor:

- 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

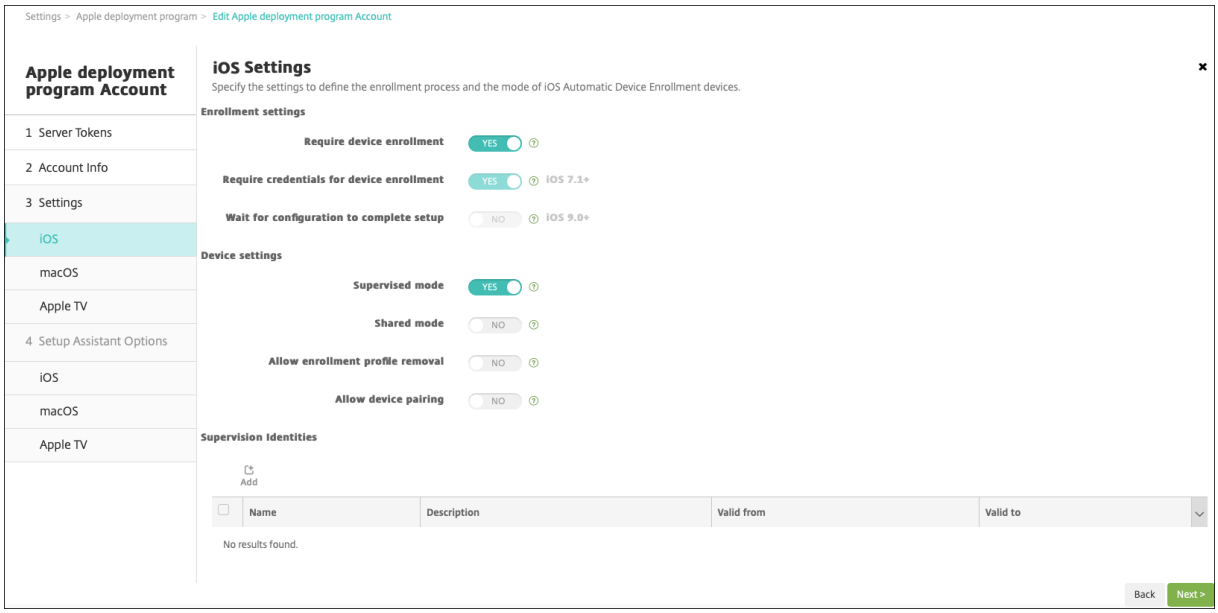
When you create multiple ASM accounts from the XenMobile server console, you automatically import groups of Shared iPads (one for each class or instructor):

- 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 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.

To add an account, go to **Settings > Apple Deployment Program**.

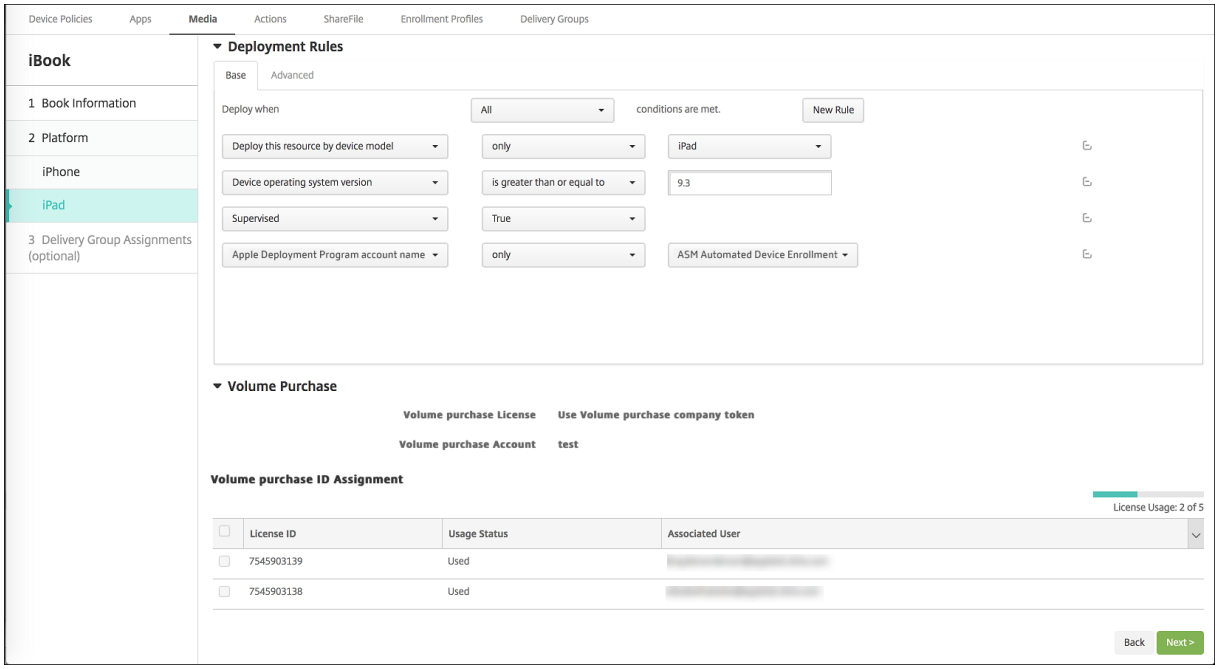


Apps for Shared iPads

Shared iPads support assignment of device-based volume purchase apps. Before deploying an app on a Shared iPad, XenMobile sends a request to the Apple volume purchase server to assign volume purchase licenses to 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, XenMobile sends a request to the Apple volume purchase server to assign volume purchase licenses to students. To check the volume purchase assignments, go to **Configure > Media > iPad** and expand **Volume Purchase**.



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:

```
Apple Deployment Program account name
Only
Device Group 1 account

<!--NeedCopy-->
```

- For the Device Group 2 account, set this deployment rule:

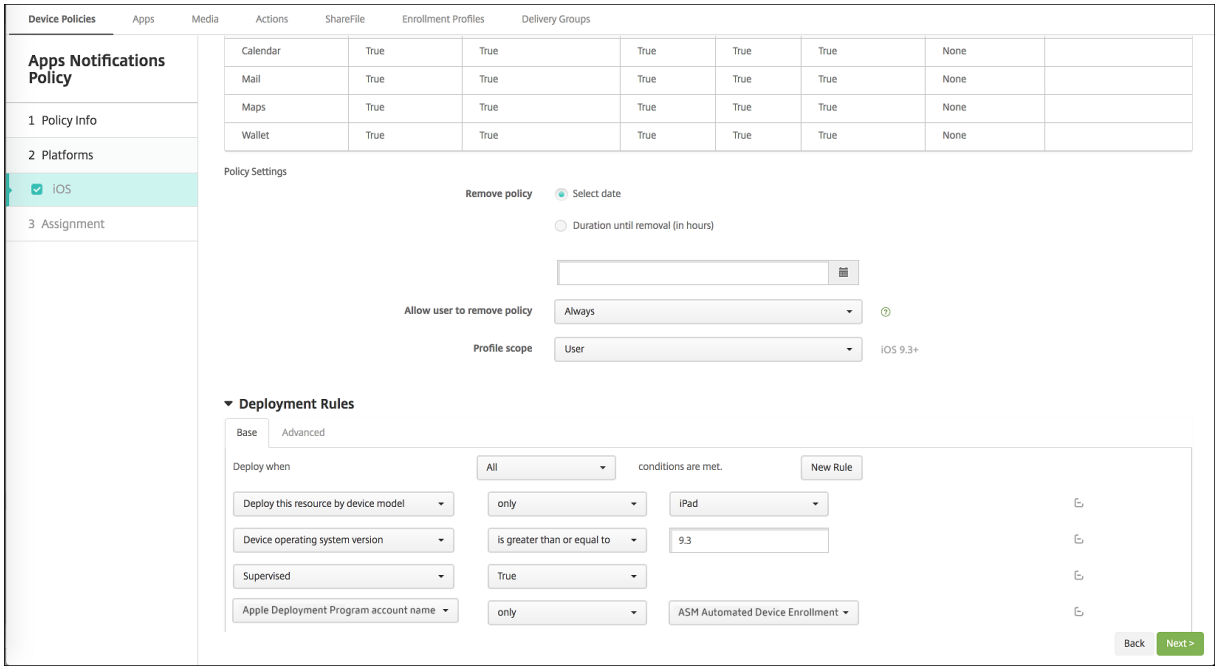
```
Apple Deployment Program account name
Only
Device Group 2 account

<!--NeedCopy-->
```

- For the Device Group N account, set this deployment rule:

```
Apple Deployment Program account name
Only
Device Group N account
```



```
4
5     <!--NeedCopy-->
```

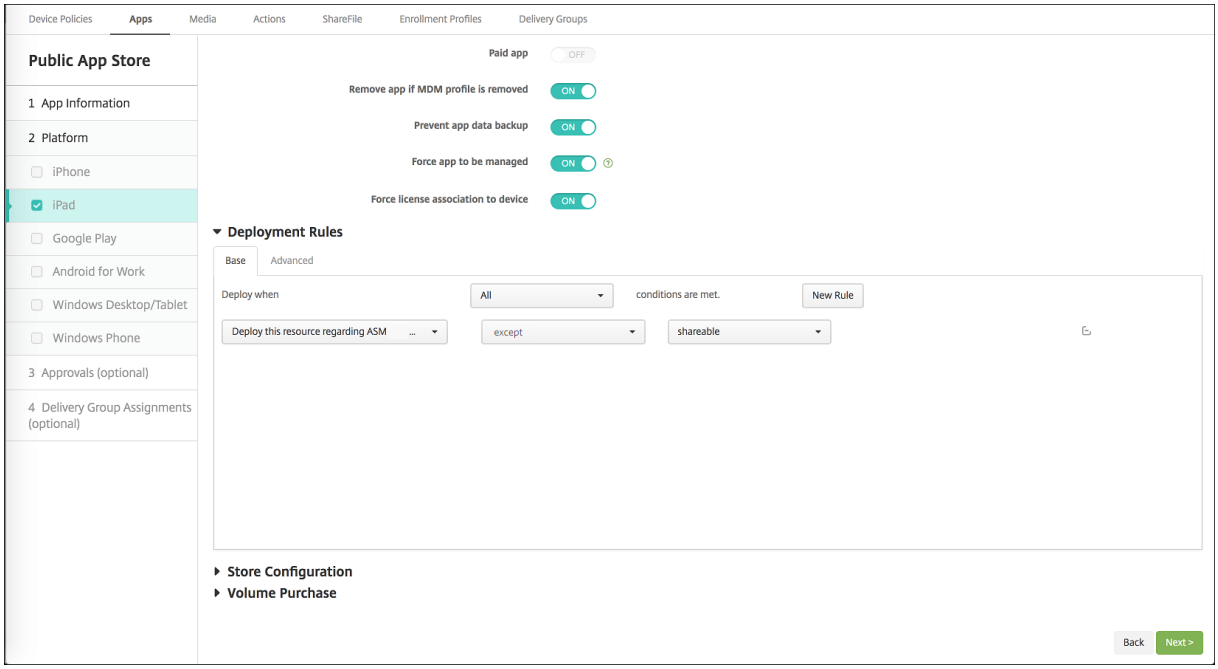


To deploy the Apple Classroom app only to instructors (using unshared iPads), filter the resources by ASM shared status with these deployment rules:

```
1 Deploy this resource regarding ASM shared mode
2 only
3 unshared
4
5 <!--NeedCopy-->
```

Or:

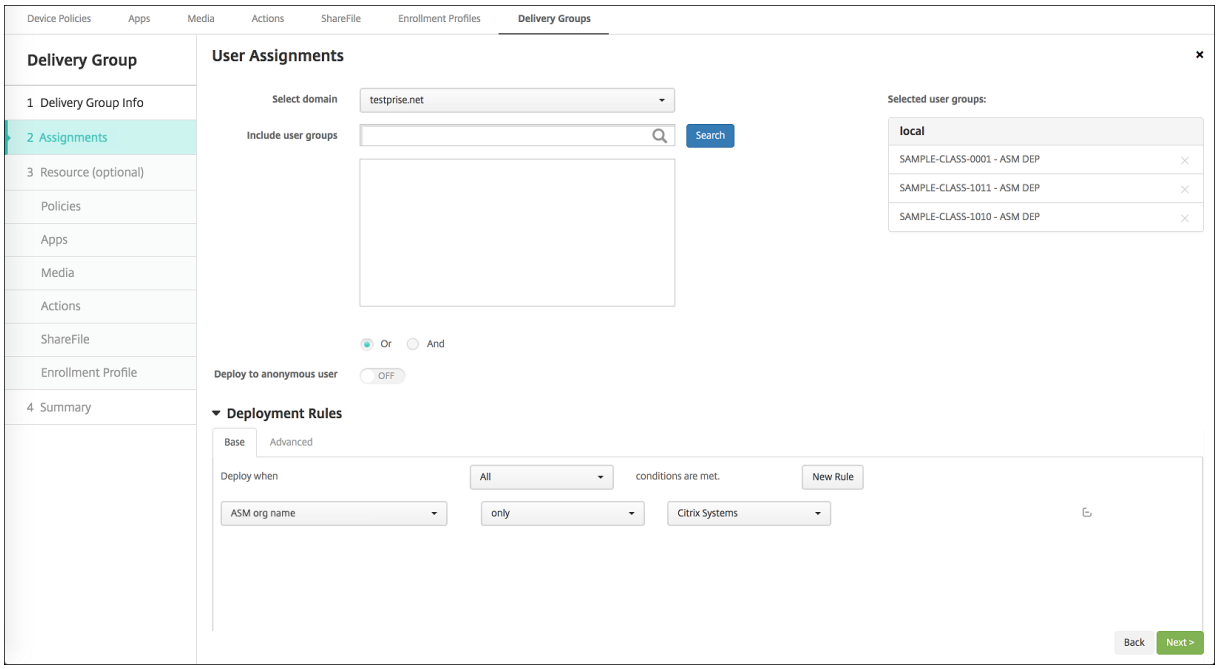
```
1 Deploy this resource regarding ASM shared mode
2 except
3 shareable
4
5 <!--NeedCopy-->
```

Delivery groups for Shared iPads

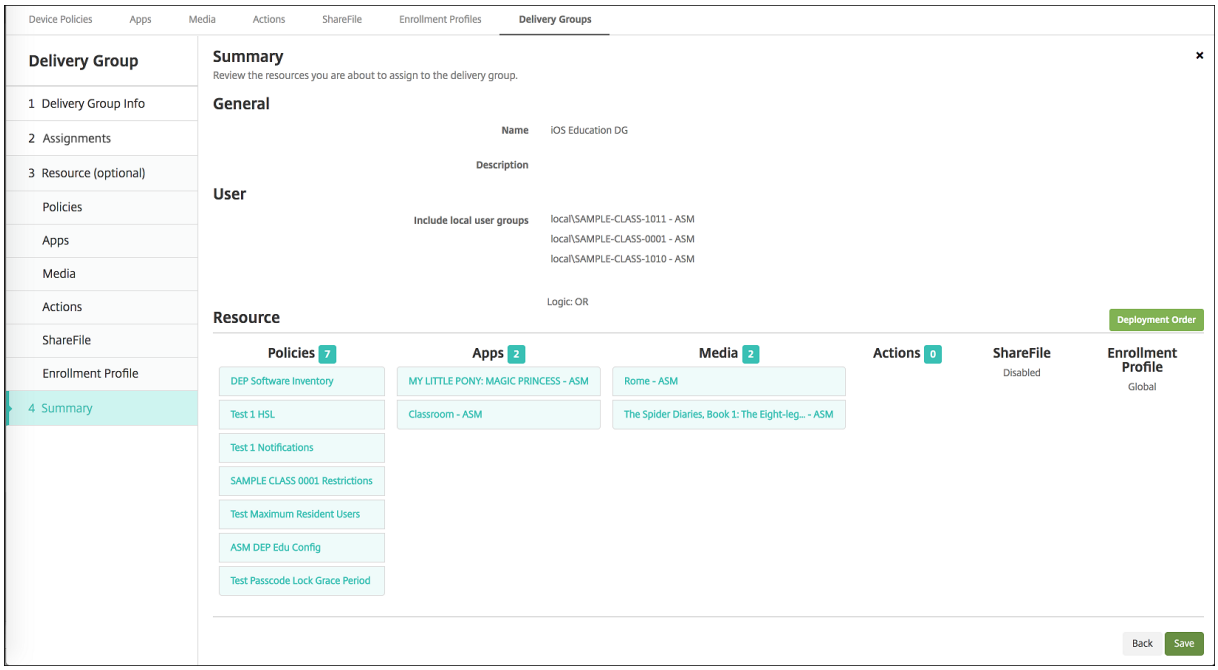
For the device group for each instructor:

- Configure one delivery group. For the instructor, assign all the classes that the Education Configuration policy defines.



- That delivery group must include these MDM resources:
  - Device policies:

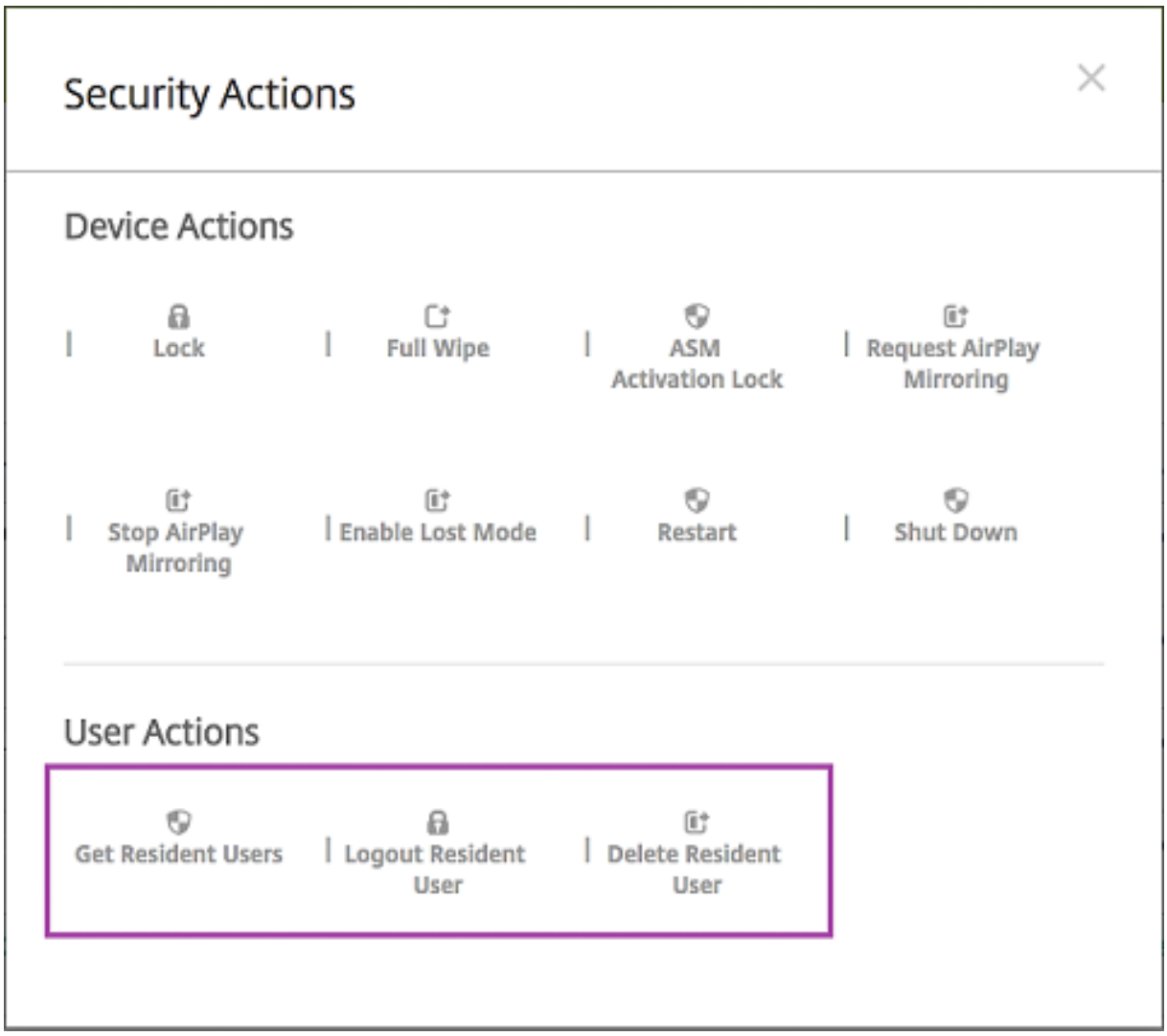
    * Education Configuration
    * Lock Screen Message
    * Apps Notifications
    * Home Screen Layout
    * Restrictions
    * Maximum Resident Users
    * Passcode Lock Grace Period
  - Required volume purchase apps
  - Required volume purchase iBooks



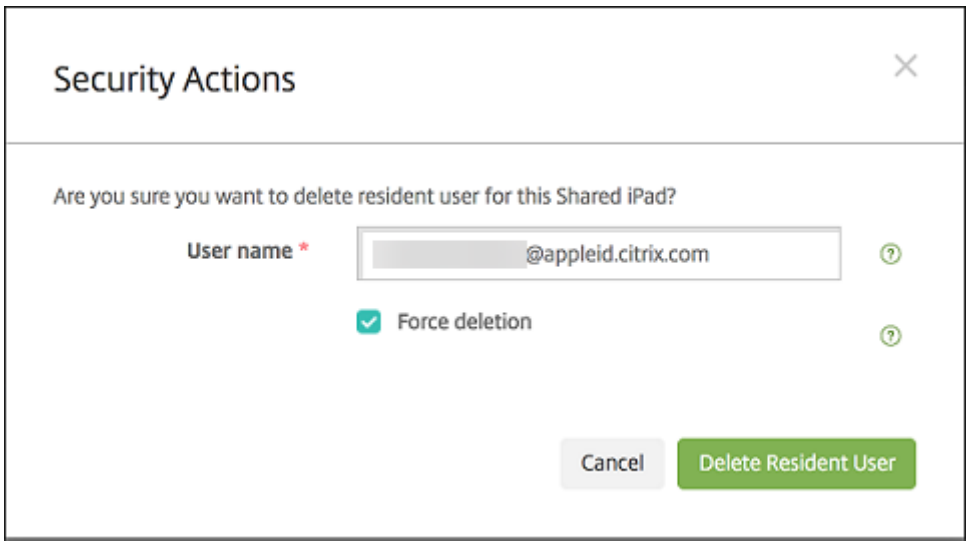
Security actions for Shared iPads

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 XenMobile 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.



After you click **Delete Resident User**, you can specify the user name.

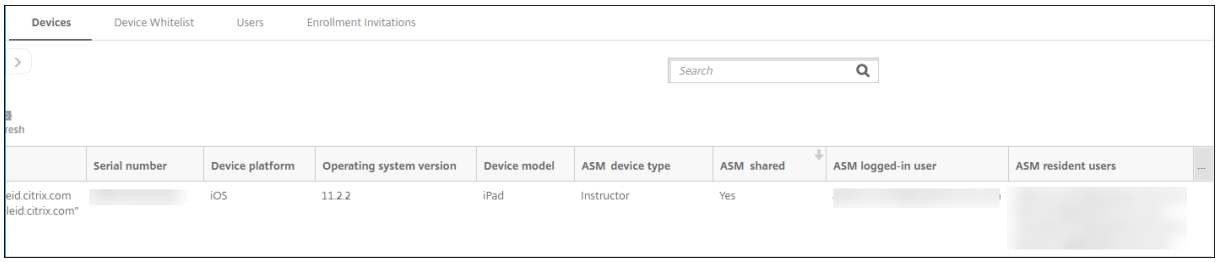


Results of security actions appear on the **Manage > Devices > General** and **Manage > Devices > Delivery Groups** pages.

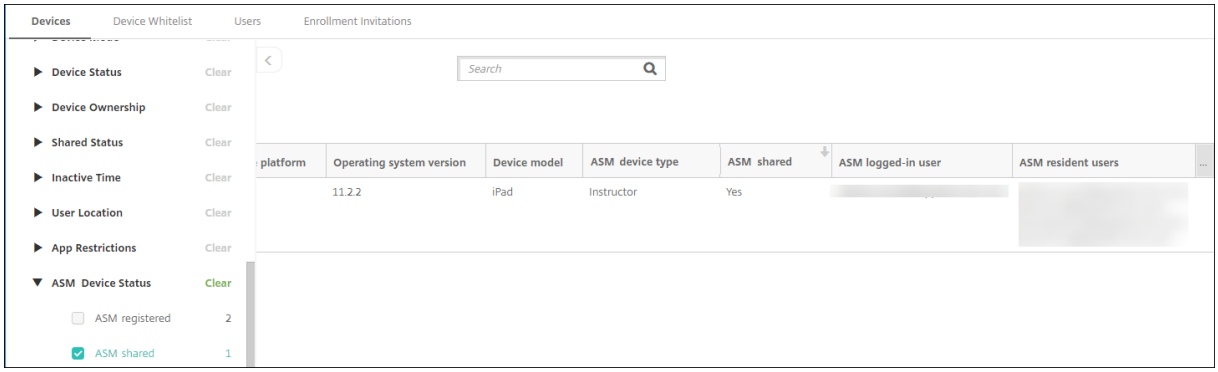
Get information about Shared iPads

Find information specific to Shared iPads on the **Manage > Devices** page:

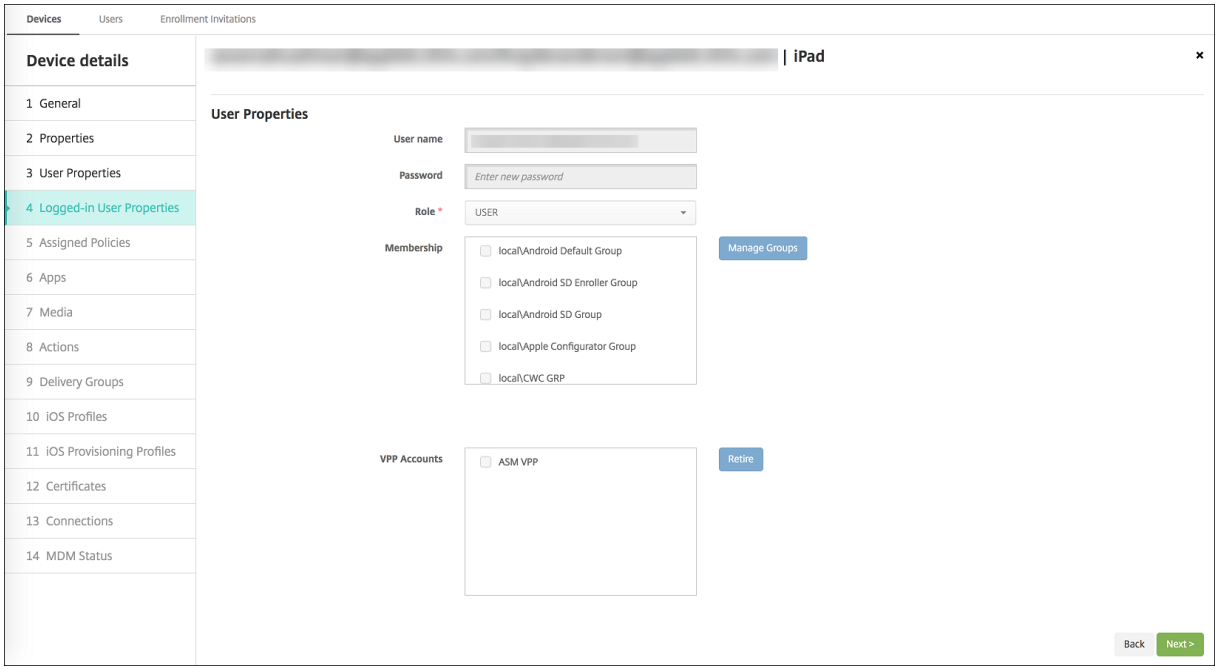
- Look up:
  - Whether a device is shared (**ASM shared**)
  - Who is logged in to the shared device (**ASM logged-in user**)
  - All users assigned to the shared device (**ASM resident users**)

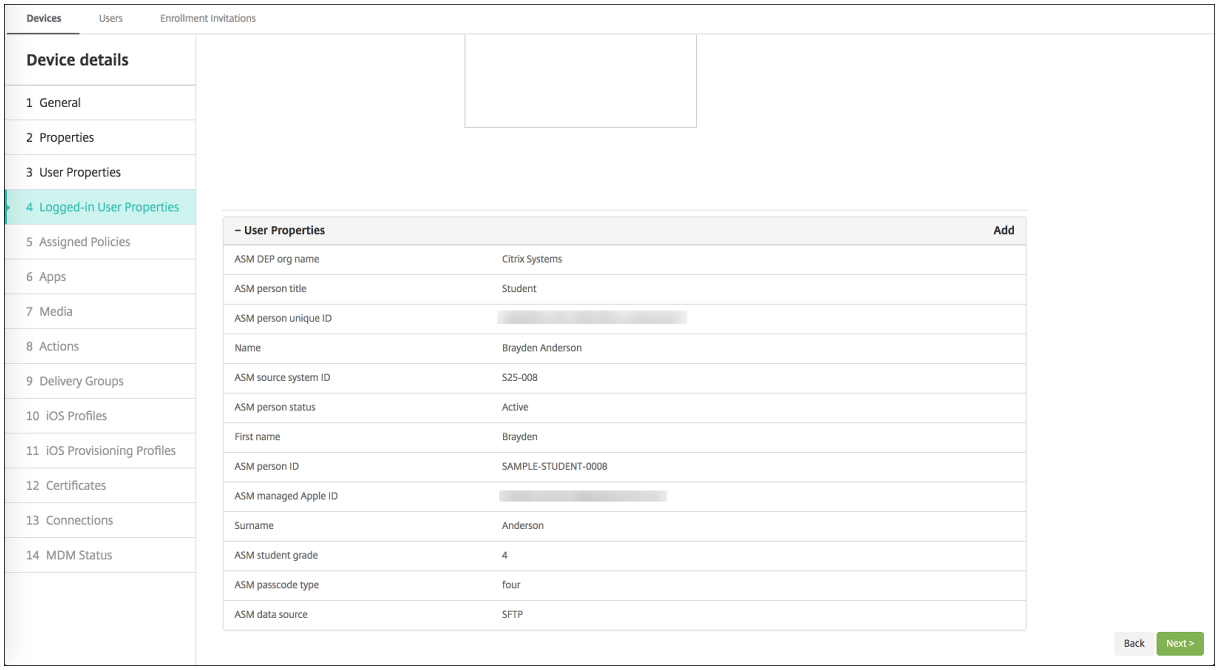


- Filter the device list by its **ASM Device Status:**

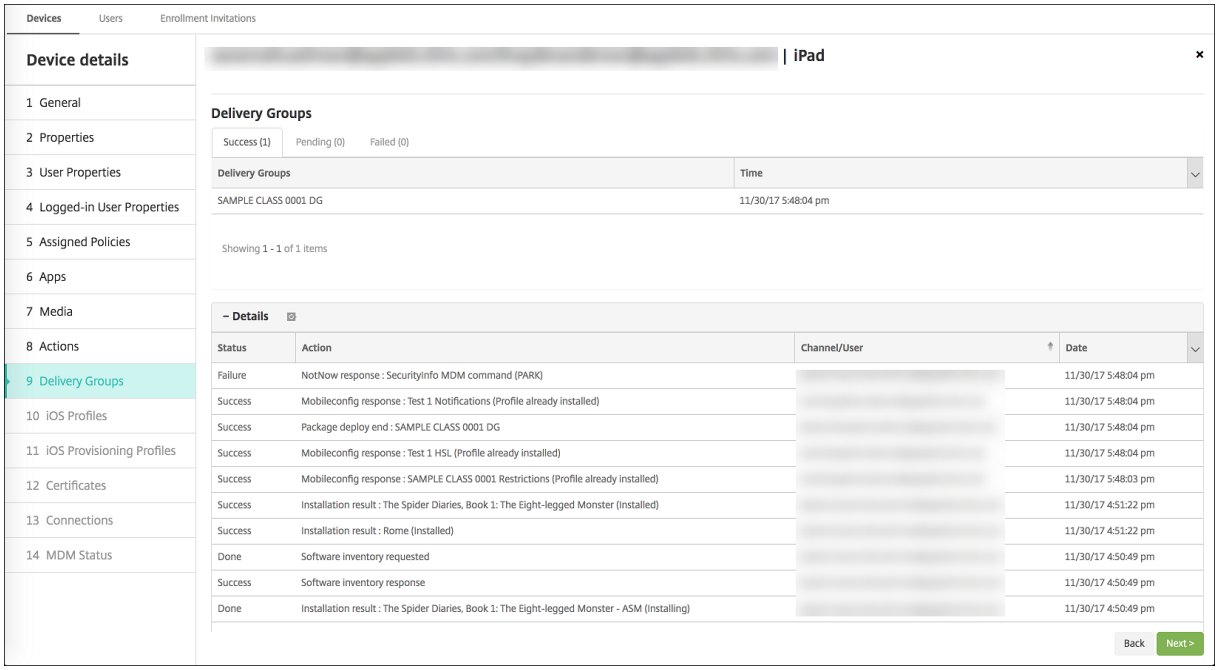


- View details about the user logged in to a Shared iPad, on the **Manage > Devices > Logged-in User Properties** page.

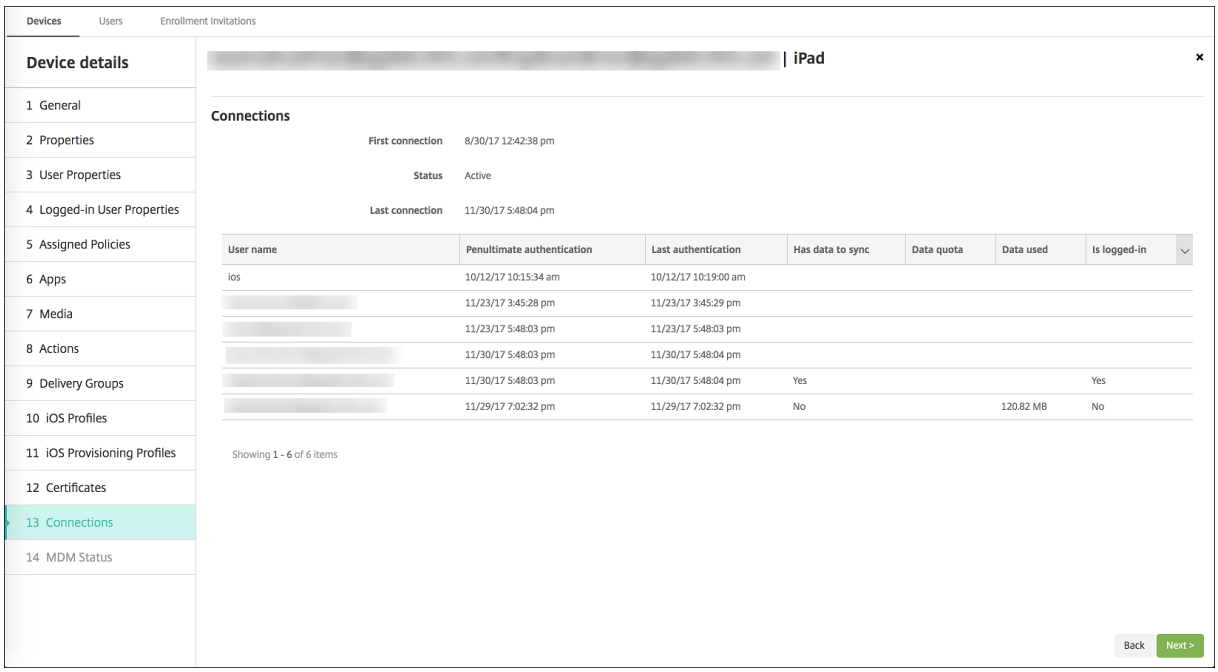




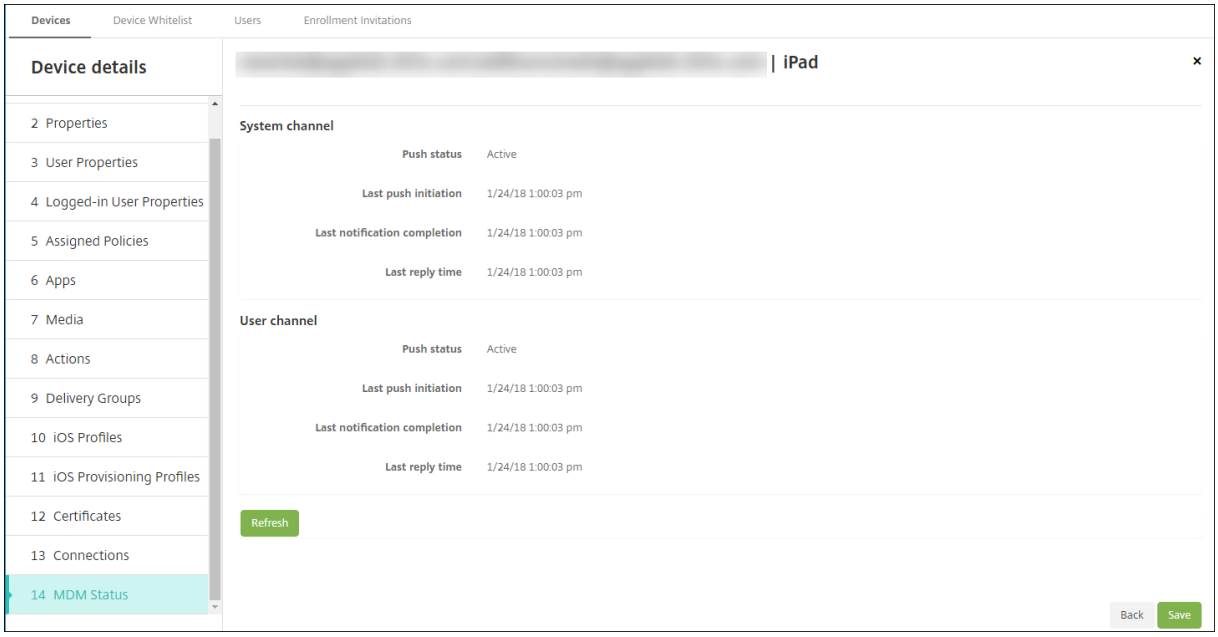
- See the channel used to deploy resources to instructors and users in a delivery group on the **Manage > Devices > Delivery Groups** page. The **Channel/User** column shows the type (**System** or **User**) and the recipient (instructor or student).



- 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.



- View the push status for both channels.



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 XenMobile. XenMobile 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 XenMobile console and then redeploy the policy.
- If you update user properties in the ASM portal, XenMobile also updates those properties in the console. However, XenMobile 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 XenMobile.

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 XenMobile 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, XenMobile also deletes that user from the XenMobile 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 that's enrolled in Apple School Manager Apple Deployment Program

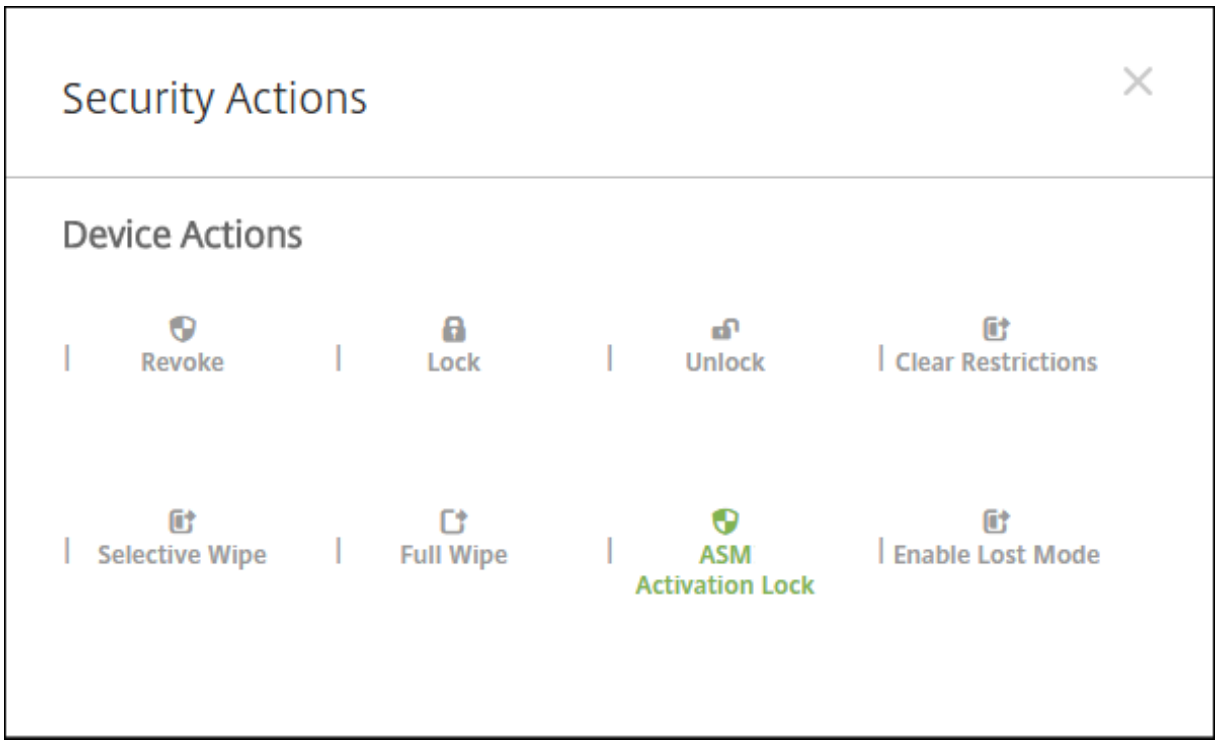
The Apple Find My iPhone/iPad service includes an Activation Lock feature. Activation Lock prevents non-authorized users from using or reselling a lost or stolen device that's enrolled in Apple Deployment Program.

XenMobile includes an **ASM Activation Lock** security action that enables you to send a lock code to an ASM Apple Deployment Program enrolled device.

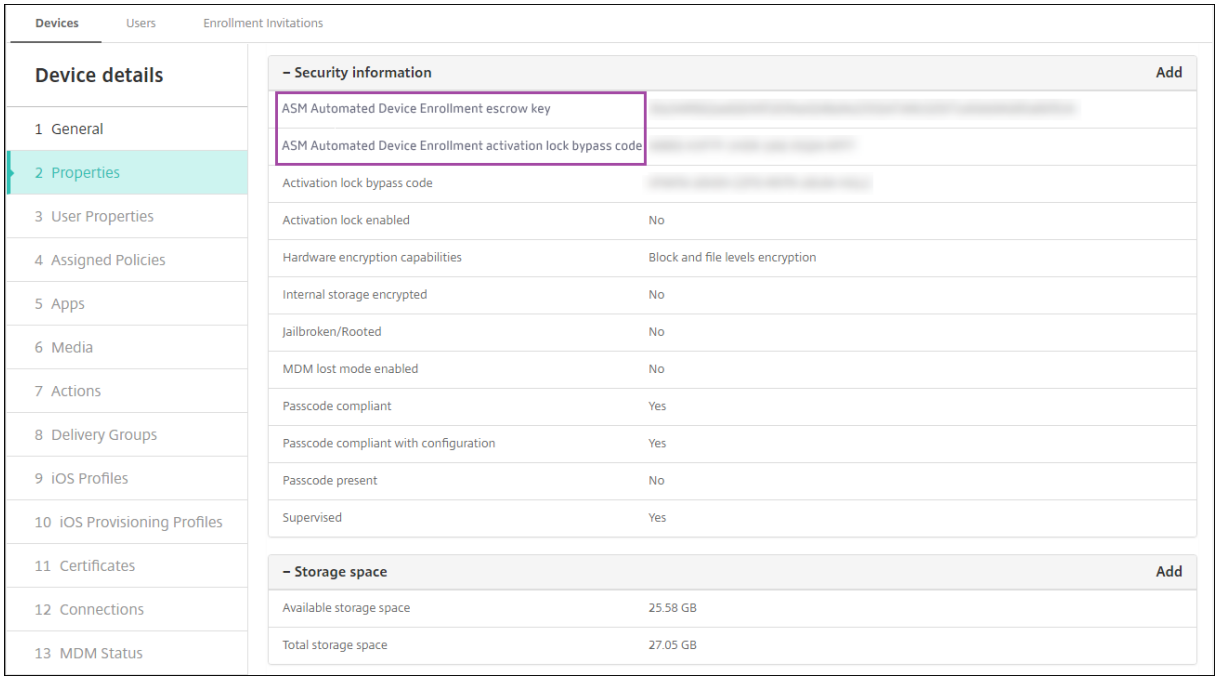
When you use the **ASM Activation Lock** security action, XenMobile can locate devices without requiring users to enable the Find My iPhone/iPad service. When an ASM device is hard-reset or fully wiped, the user provides their Managed Apple ID and password to unlock the device.

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.

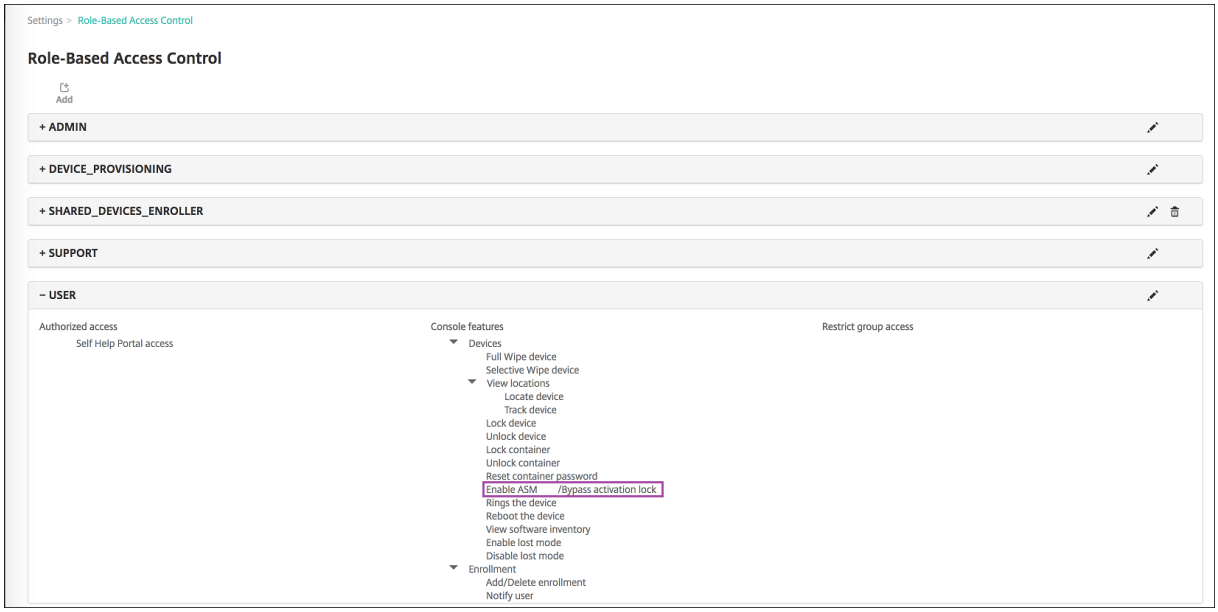
To set the activation lock, go to **Manage > Devices**, select the device, click **Security**, and then click **ASM Activation Lock**.



The properties **ASM escrow key** and **ASM activation lock bypass code** appear in **Device details**.



The RBAC permission for an ASM Activation Lock is **Devices > Enable ASM Bypass activation lock**.



Distribute Apple apps

September 17, 2020

XenMobile 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 Service or 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	**In XenMobile: Configure > Apps**, add **Public App Store** apps for iPhone or iPad. Configure the apps and assign them to delivery groups.	**In XenMobile:** 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. **In XenMobile:** Go to **Settings > Volume purchase** to add your volume purchase account.	**In ABM or ASM:** Purchase and add apps from Apps and Books. **In XenMobile:** Go to **Configure > Apps**, configure the apps, and assign them to delivery groups.	**In XenMobile:** Configure and deploy apps using delivery groups.
Enterprise apps	Not applicable	**In XenMobile:** Go to **Configure > Apps**. Click **Add** then click **Enterprise**. Upload the IPA file. Configure the apps and assign them to delivery groups.	**In XenMobile:** 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	**In XenMobile:** Go to **Configure > Apps**. Click **Add** then click **MDX**. Ensure that you select **iPad**/**iPhone** for the platform. Upload the MDX file. Configure the apps and assign them to delivery groups.	**In XenMobile:** Configure and deploy apps using delivery groups.
MDX apps distributed using Apple volume purchase	Enroll in an Apple deployment program. **In XenMobile:** Go to **Settings > Volume purchase** to add your volume purchase account.	**In ABM:** Purchase and add MDX apps from Apps and Books. Link the app to your ABM account. **In XenMobile:** Go to **Configure > Apps**, configure the apps, and assign them to delivery groups.	**In XenMobile:** Configure and deploy apps using delivery groups.
Custom apps	Enroll in an Apple deployment program. **In XenMobile:** Go to **Settings > Volume purchase** to add your volume purchase account.	**In ABM:** Add your app to the App Store as a private app. Link the app to your ABM account. **In XenMobile:** Go to **Configure > Apps**, configure the apps, and assign them to delivery groups.	**In XenMobile:** 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-enabled custom apps	Enroll in an Apple deployment program. **In XenMobile:** Go to **Settings > Volume purchase** to add your volume purchase account.	**In ABM:** Add your app to the app store as a private app. Link the app to your ABM account. **In XenMobile:** Go to **Configure > Apps** and upload the MDX file. Configure the apps and assign them to delivery groups.	**In XenMobile:** Configure and deploy apps using delivery groups.

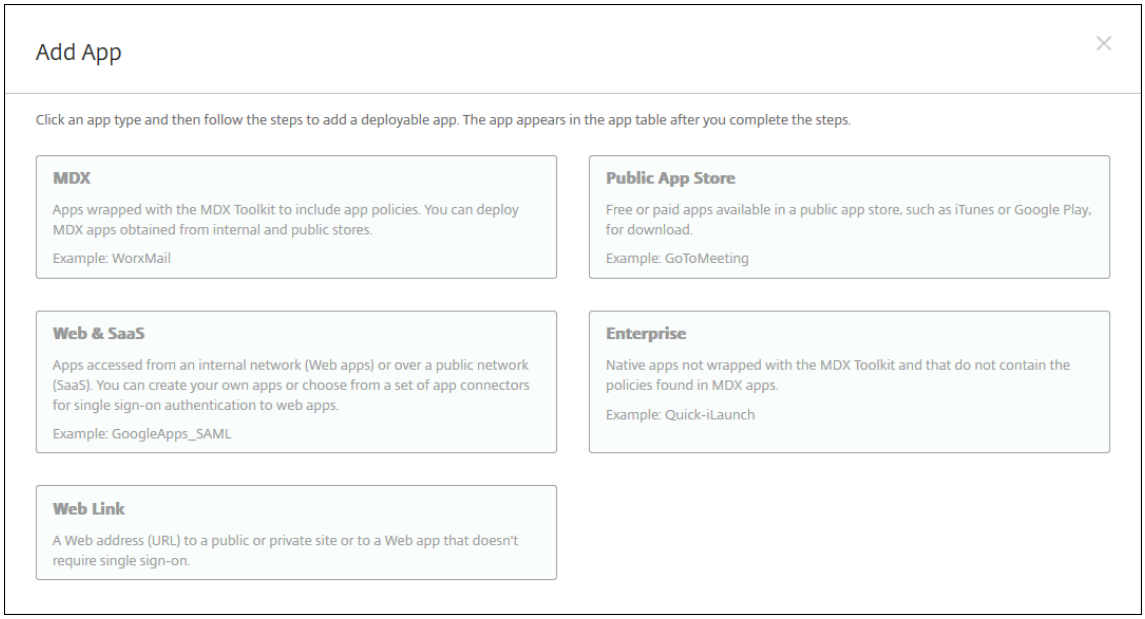
Public app store apps

You can add free and paid apps available on the App Store to XenMobile.

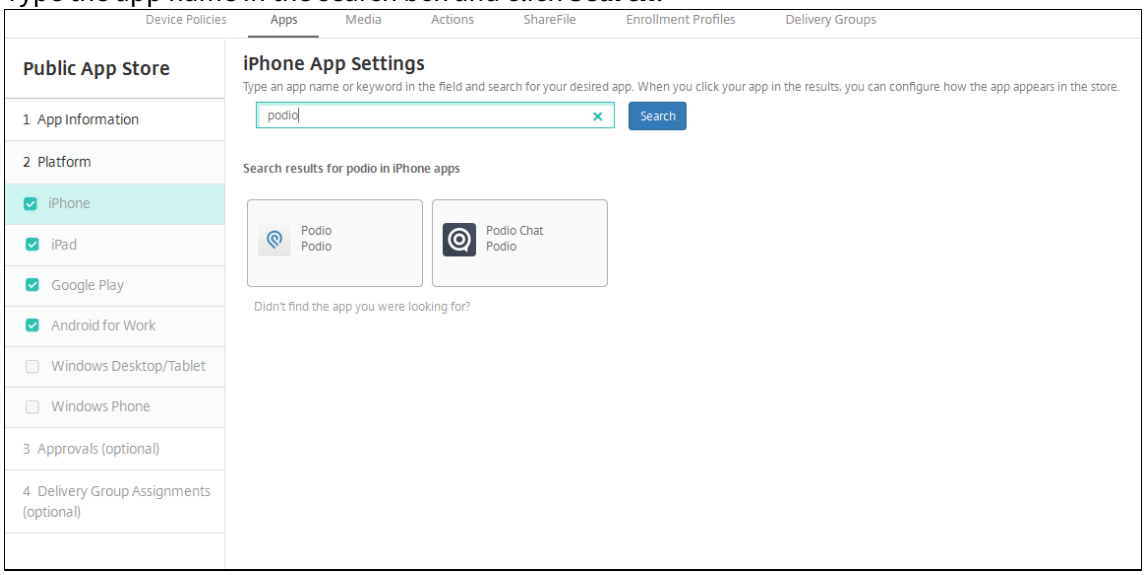
Feature availability	
Requires device supervision	No
Available for user enrollment mode	No
Available on	iOS/iPadOS

Step 1: Add and configure apps

1. In the XenMobile 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**.

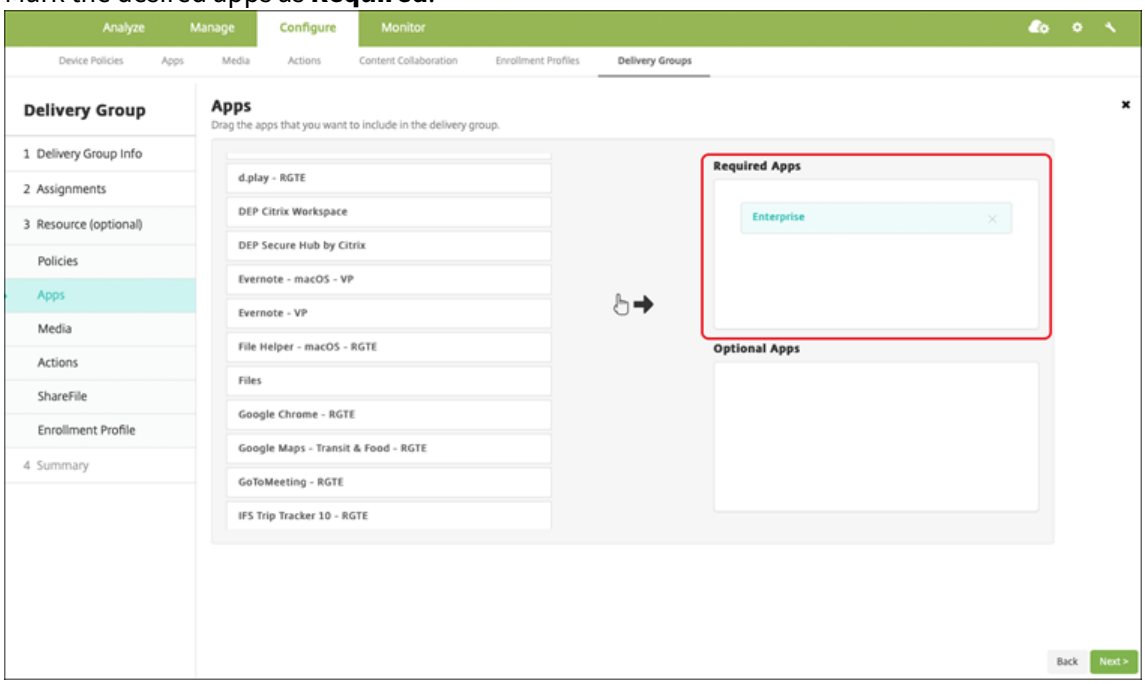


5. Apps matching the search criteria appear. Click the desired app.
6. Assign a delivery group to the app and click **Save**.

Step 2: Configure app deployment

1. In the XenMobile 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 > Apps**.

6. Mark the desired apps as **Required**.



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 XenMobile.

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 XenMobile. 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.

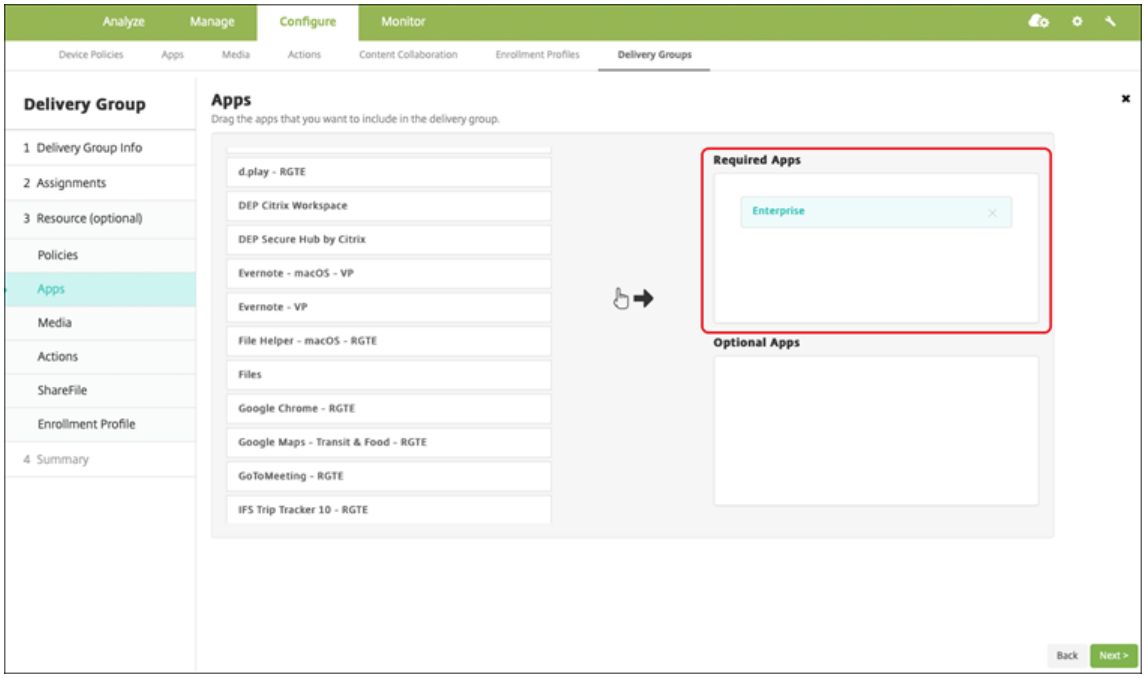
Step 2: Get apps and licenses from Apple

Add apps on your ABM/ASM account. You can add purchases from the Apple App Store or Apple Books (for iOS/iPadOS only). Keep in mind that you must purchase all apps, even if they are free.

For information about how to make apps available to your business, see Apple documentation.

Step 3: Configure app deployment

1. In the XenMobile 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 > Apps**.
7. Mark the desired apps as **Required**.



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.

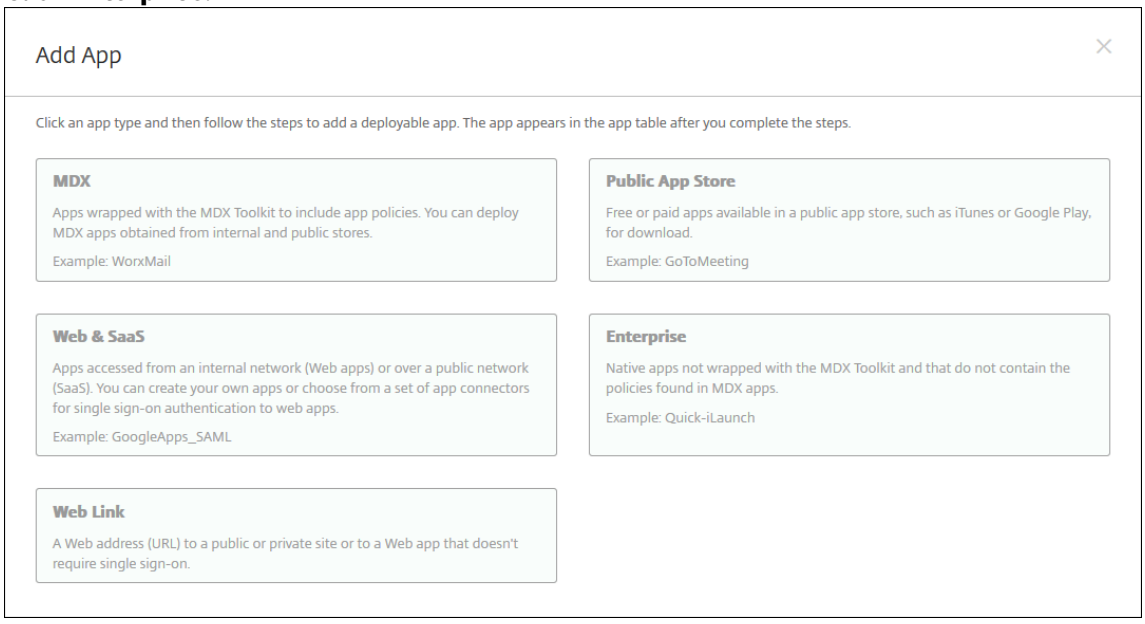
Enterprise apps

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

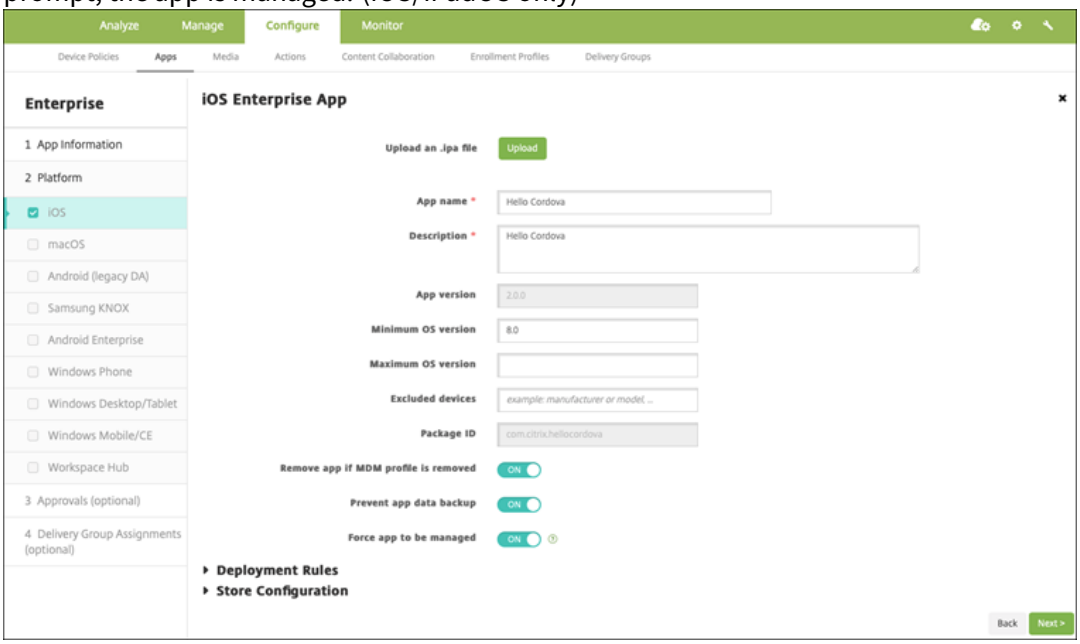
Step 1: Add and configure apps

1. In the XenMobile console, navigate to **Configure > Apps**. Click **Add**.
2. Click **Enterprise**.



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:

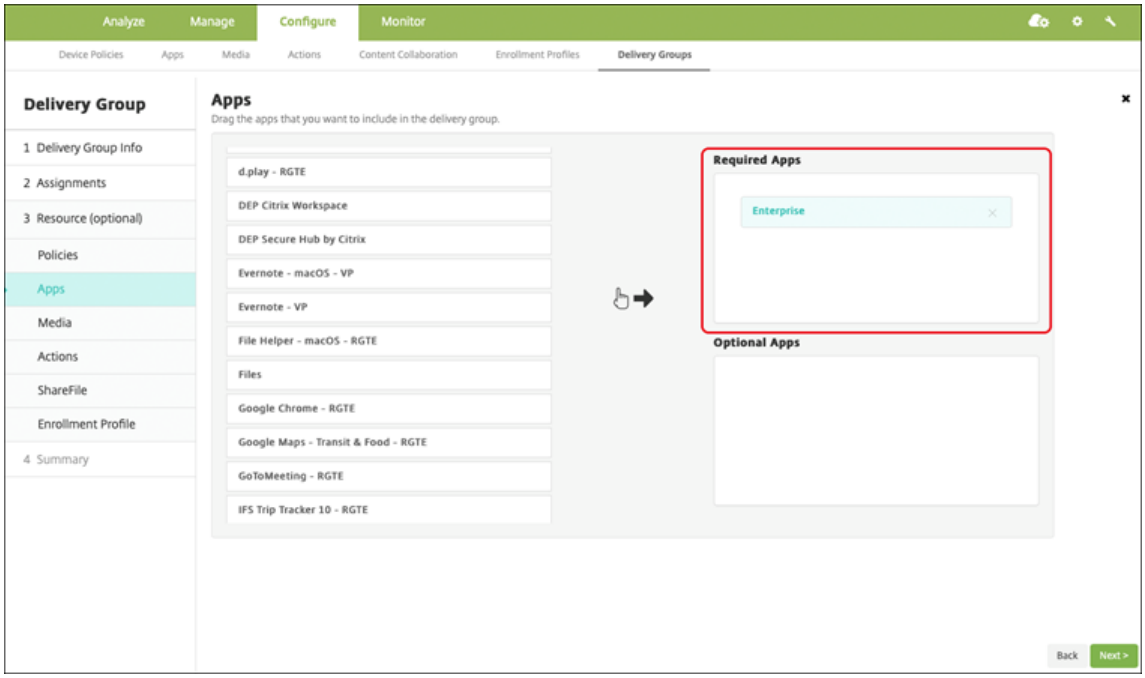
- **File name:** Optionally, type a new name for the app.
- **App description:** Optionally, type a new description for the app.
- **App version:** You can't change this field.
- **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
- **Maximum 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. (iOS/iPadOS only)



9. Assign a delivery group to the app and click **Save**.

Step 2: Configure app deployment

1. In the XenMobile console, navigate to **Configure > Delivery Groups**. Select the delivery group to configure and click the **Apps** page.
2. Mark the desired apps as **Required**.



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.

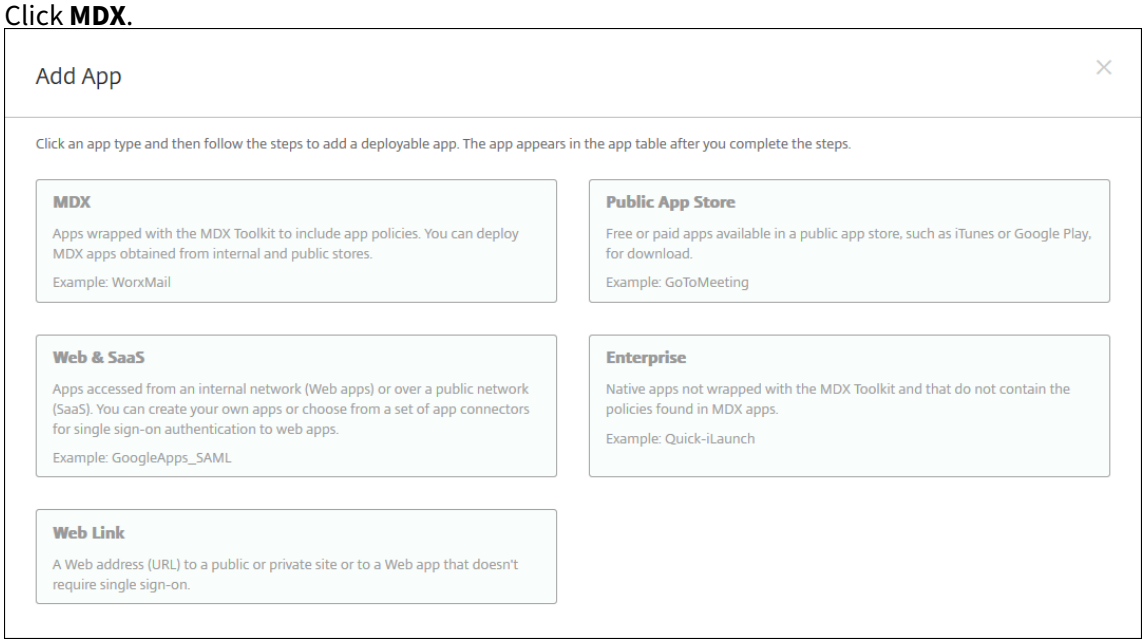
MDX apps

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.

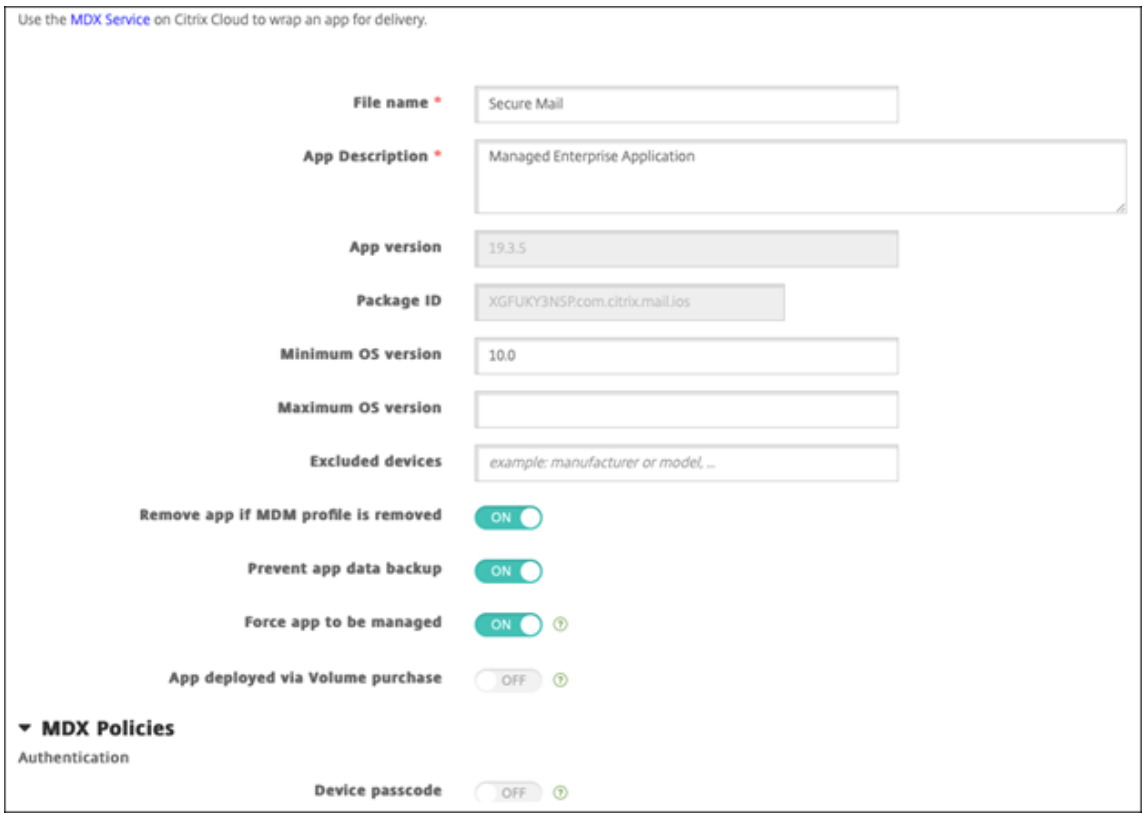
Feature availability	
Requires device supervision	No
Available for user enrollment mode	Yes
Available On	iOS/iPadOS

Step 1: Add and configure apps

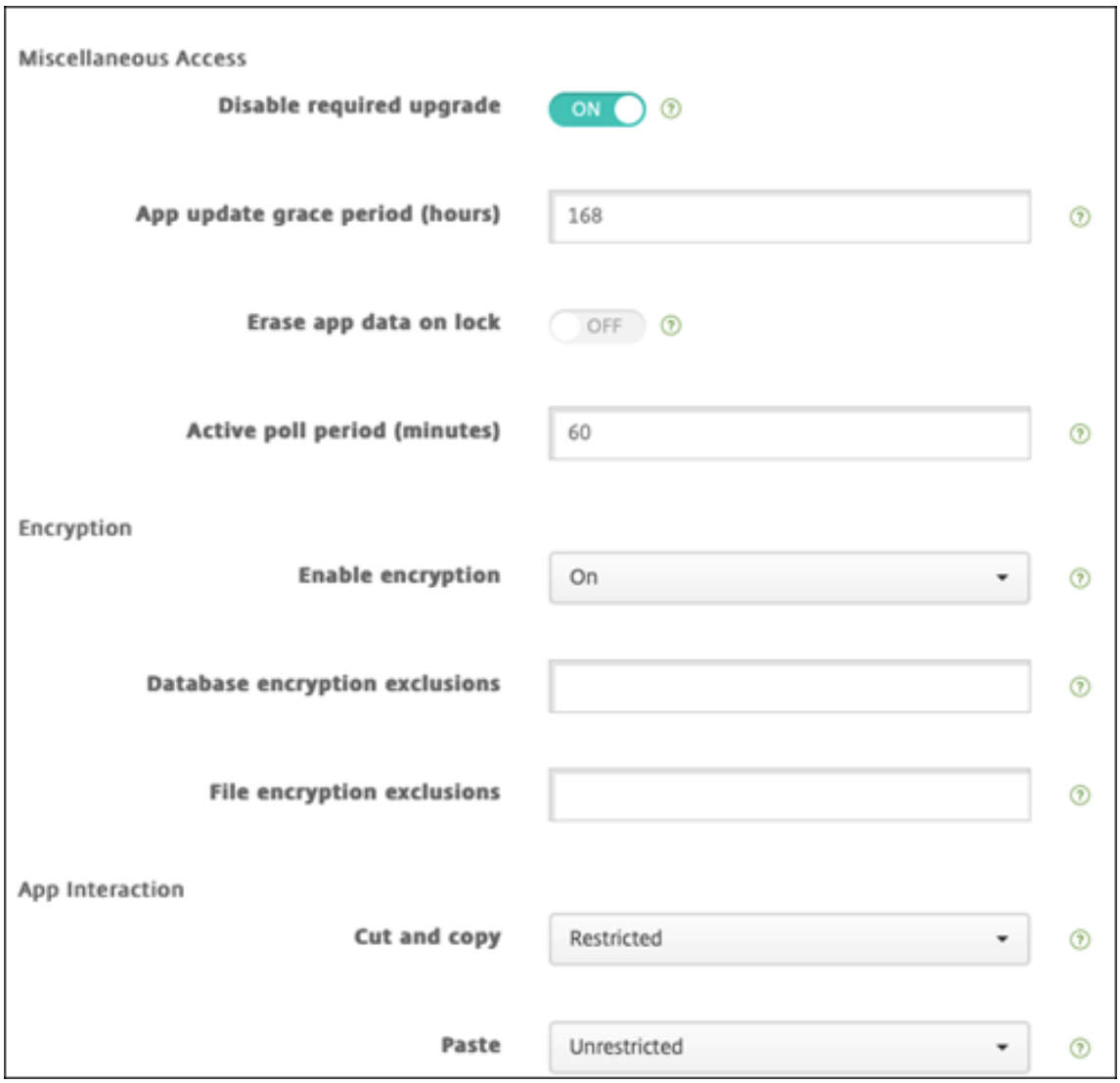
1. In the XenMobile console, navigate to **Configure > Apps**. Click **Add**.
2. Click **MDX**.



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.



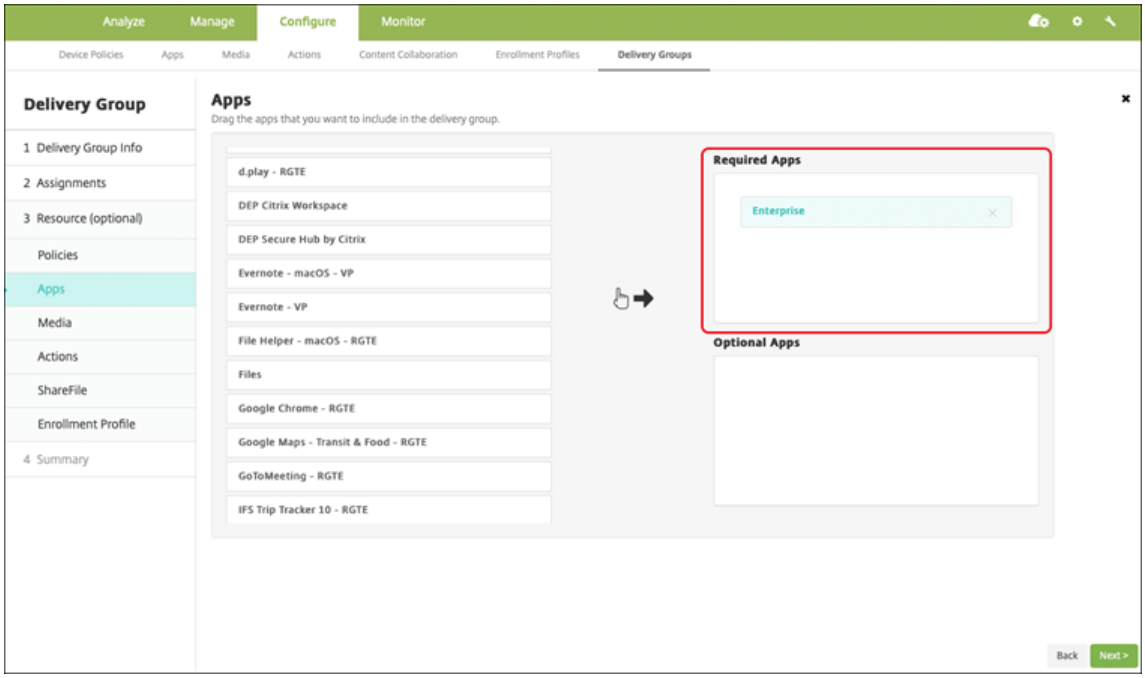
6. Configure the MDX policies. Set **Disable required upgrade** to **On**.



7. Assign a delivery group to the app and click **Save**.

Step 2: Configure app deployment

1. In the XenMobile console, navigate to **Configure > Delivery Groups > Apps**.
2. Mark the desired apps as **Required**.



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.

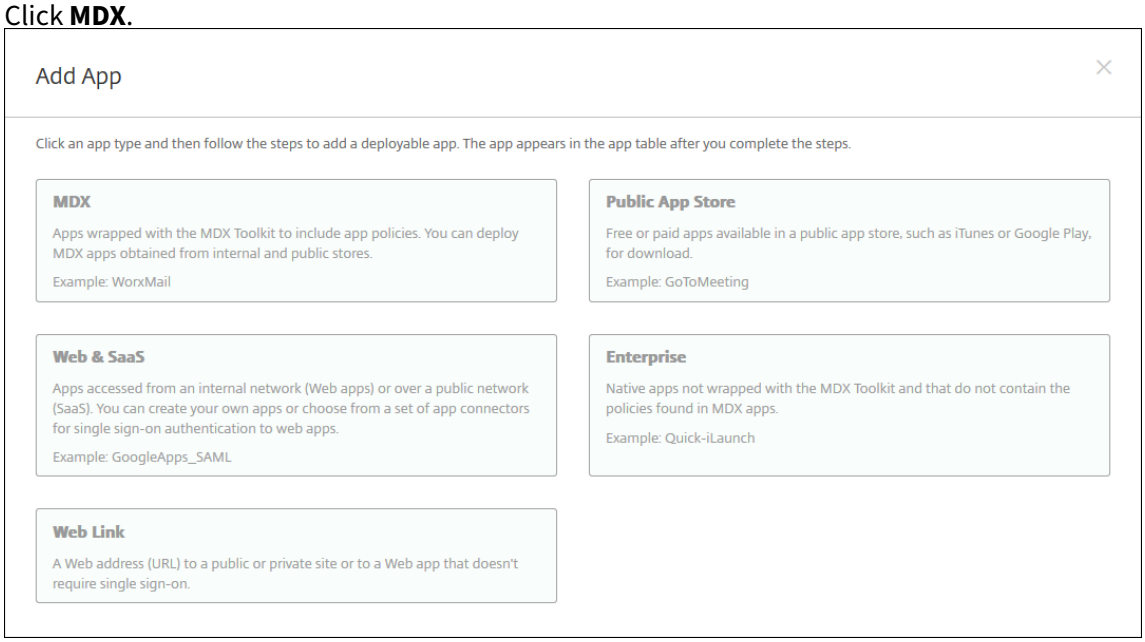
Feature availability	
Requires device supervision	No
Available for user enrollment mode	Yes
Available on	iOS/iPadOS

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 XenMobile. 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.

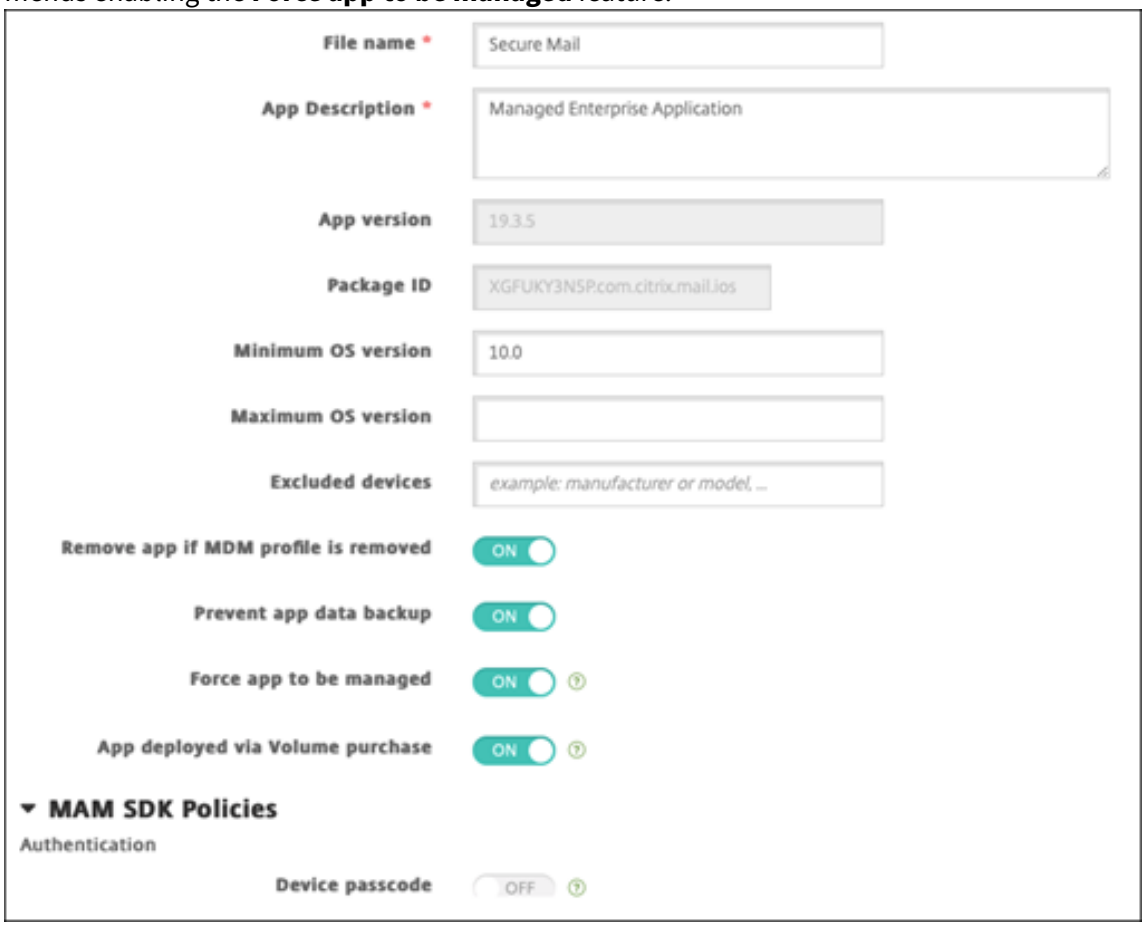
Step 2: Add and configure apps

1. In the XenMobile console, navigate to **Configure > Apps**. Click **Add**.
2. Click **MDX**.

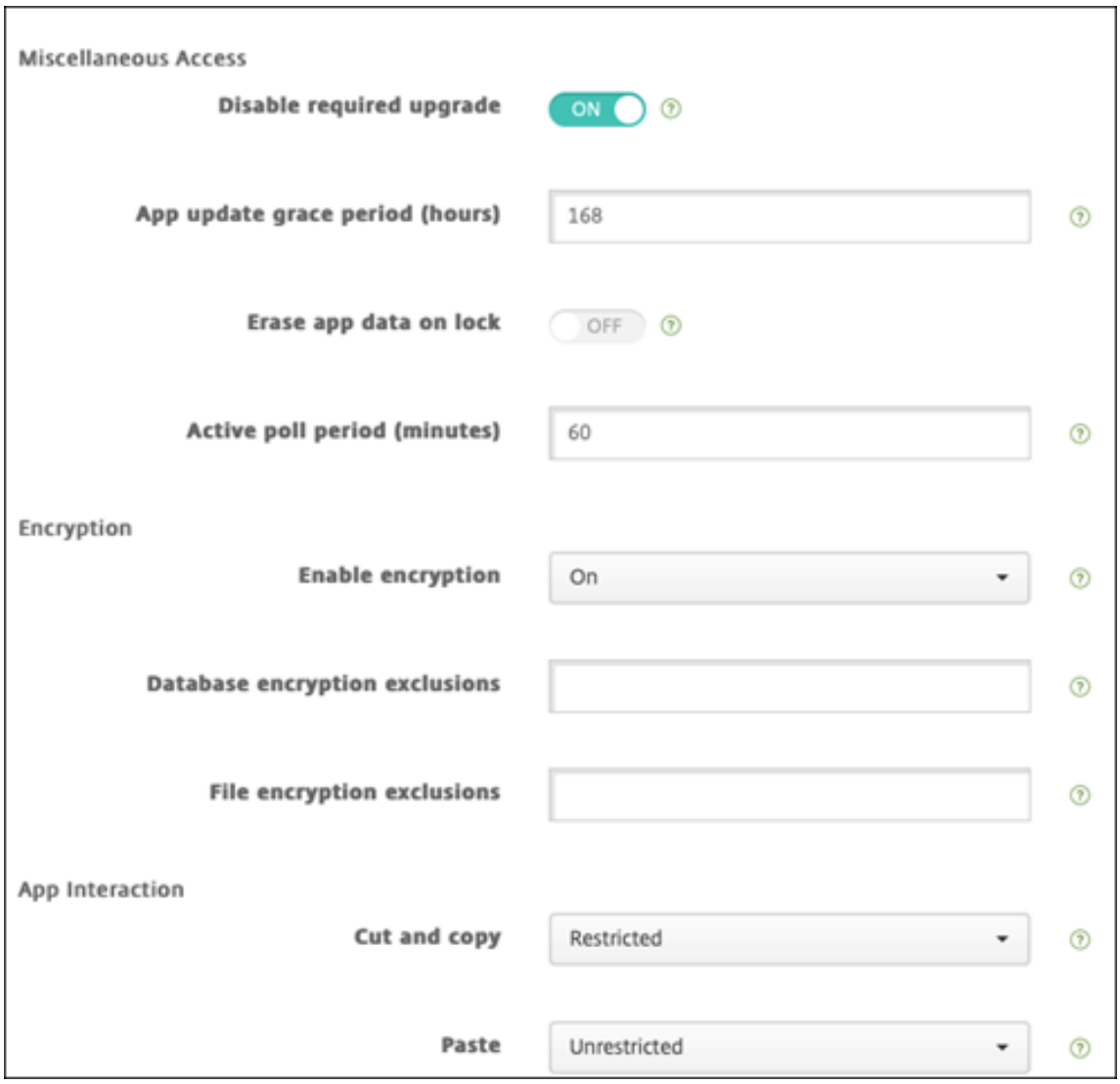


3. Select **iPhone** or **iPad** for platforms.

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.



6. Configure the MDX policies. Set **Disable required upgrade** to **On**.

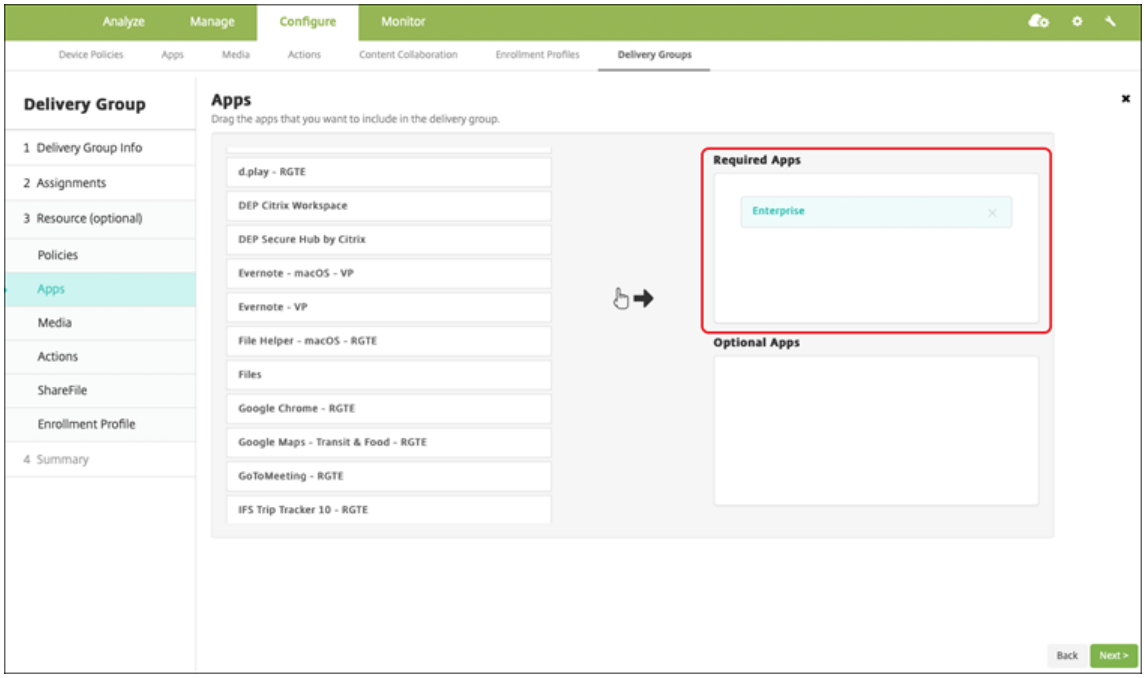


7. Assign a delivery group to the app for each platform and click **Save**.

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 3: Configure app deployment

1. In the XenMobile console, navigate to **Configure > Delivery Groups > Apps**.
2. Mark the desired volume purchase apps as **Required**.



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 XenMobile 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 XenMobile, 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 XenMobile.

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 XenMobile. 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.

Step 2: Configure apps on ABM

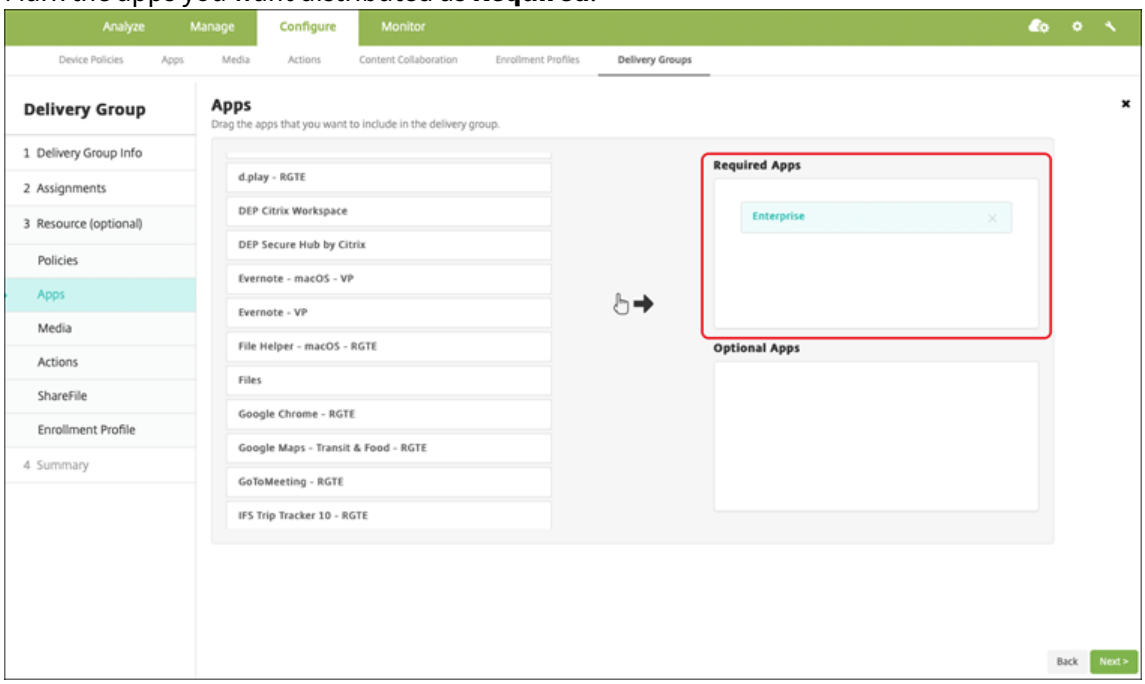
Add apps on your ABM account. You can upload and distribute your own custom apps or buy licenses for custom apps from other organizations. For more information on adding and enabling custom apps on ABM, see Apple documentation.

Step 3: Add and configure apps in XenMobile

1. In the XenMobile 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 XenMobile console, navigate to **Configure > Delivery Groups > Apps**.
2. Mark the apps you want distributed as **Required**.



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 XenMobile.

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 XenMobile. For more information on linking volume purchase accounts, see Apple Volume Purchase.

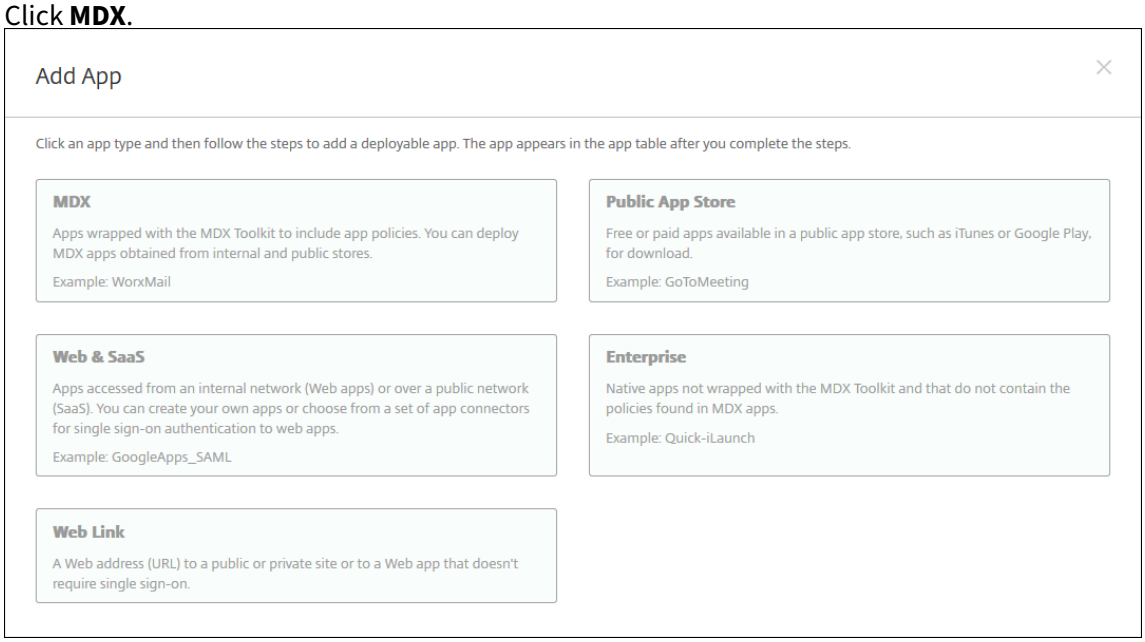
3. When you add your volume purchase account, enable **App Auto Update**. This setting ensures that apps on user devices automatically update when an update appears in the Apple store.

Step 2: Configure apps on ABM

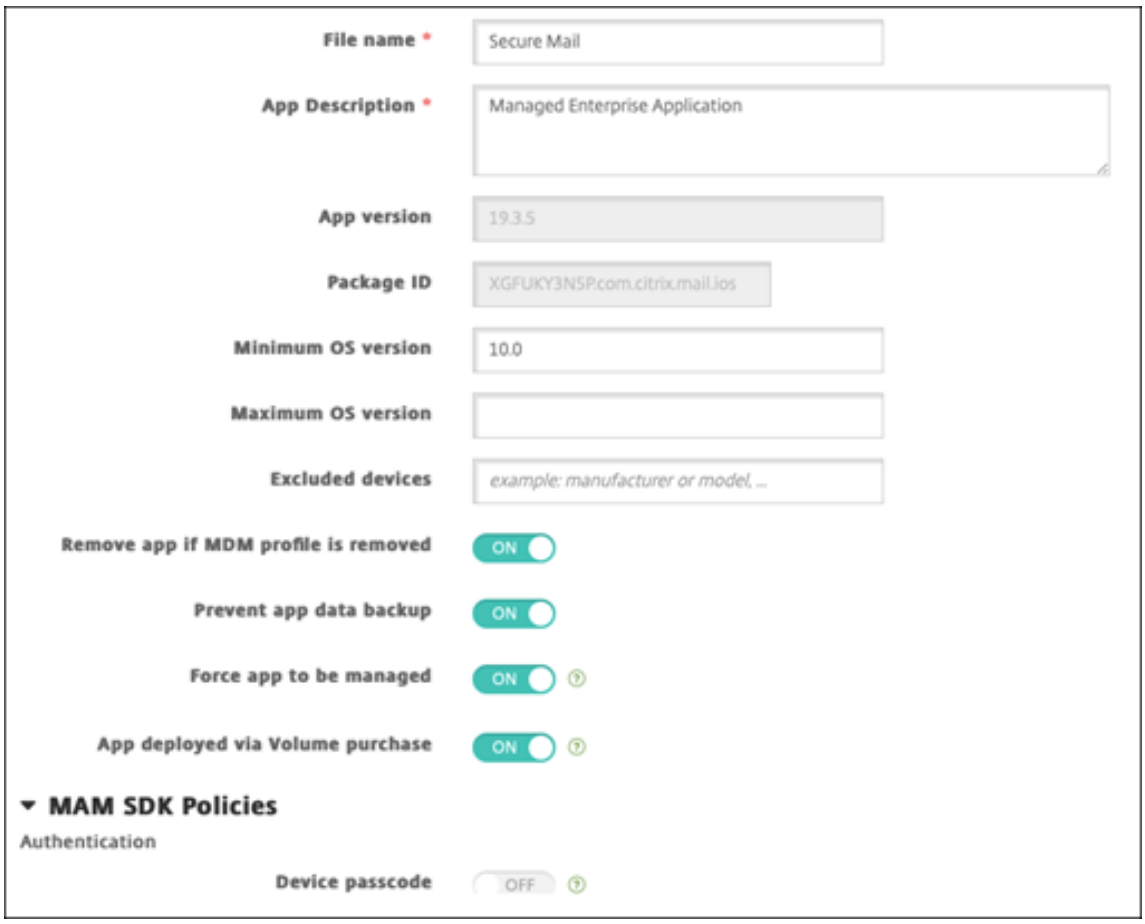
Add apps on your ABM account. You can upload and distribute your own custom apps or buy licenses for custom apps from other organizations. For more information on adding and enabling custom apps on ABM, see Apple documentation.

Step 3: Add and configure apps in XenMobile

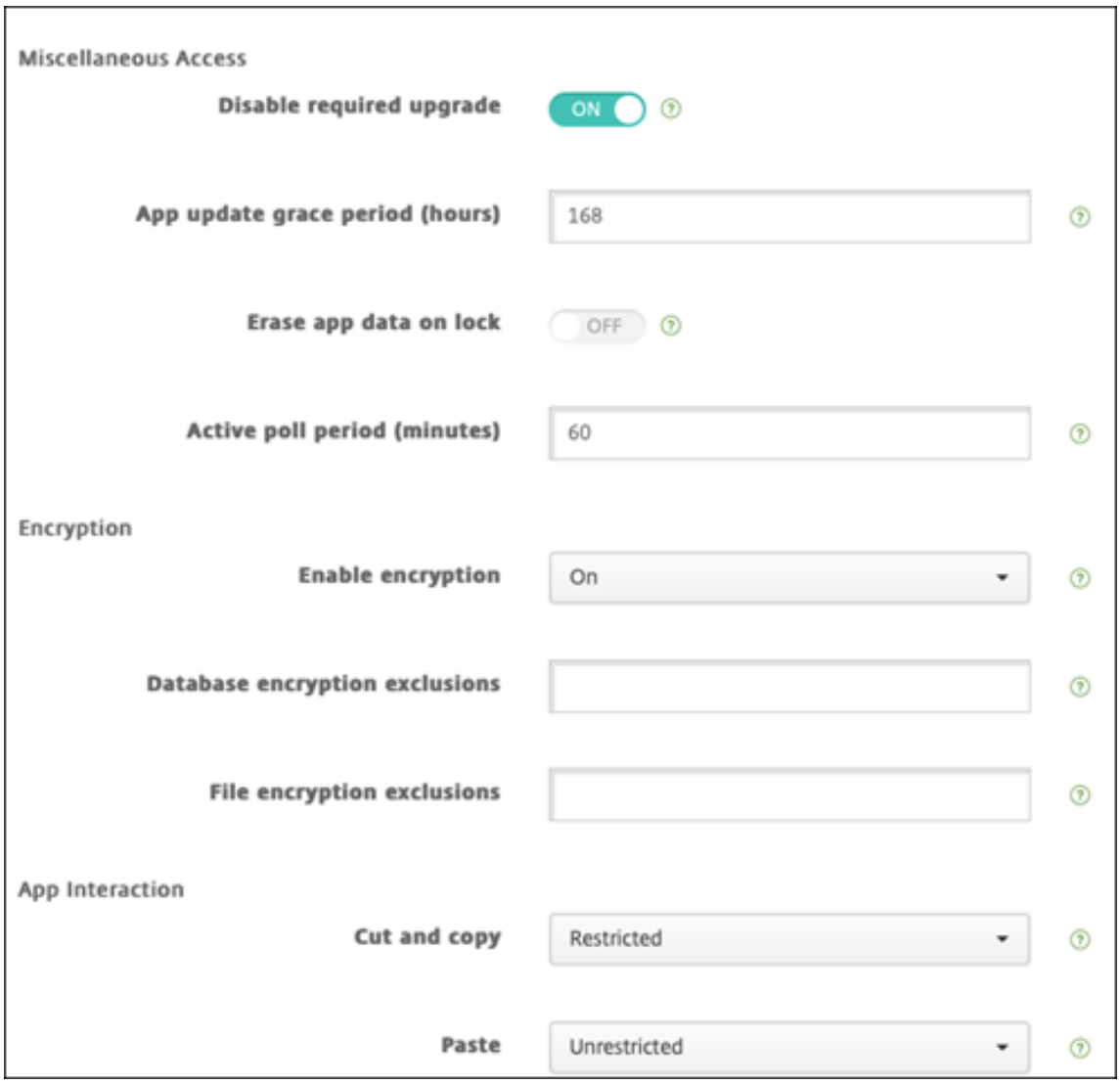
1. In the XenMobile console, navigate to **Configure > Apps**. Click **Add**.
2. Click **MDX**.



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.



6. Configure the MDX policies. Set **Disable required upgrade** to **On**.

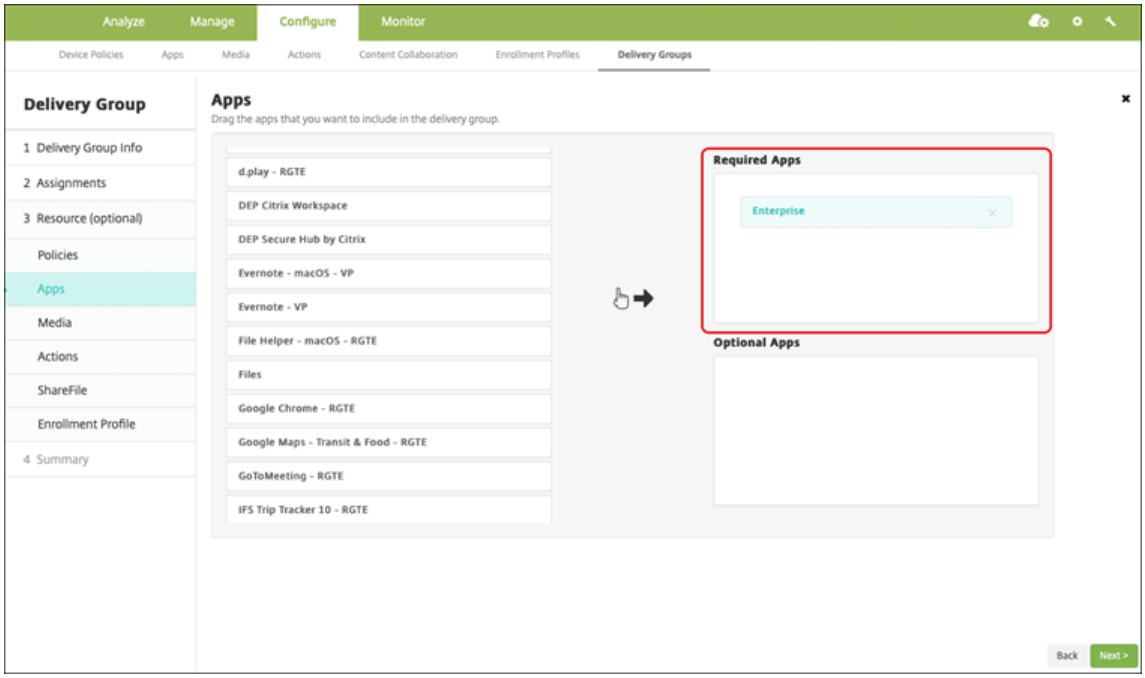


7. Assign a delivery group to the app and click **Save**.

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 XenMobile 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 back to **Configure > Delivery Groups > Apps**.
5. Mark the apps you want distributed as **Required**.



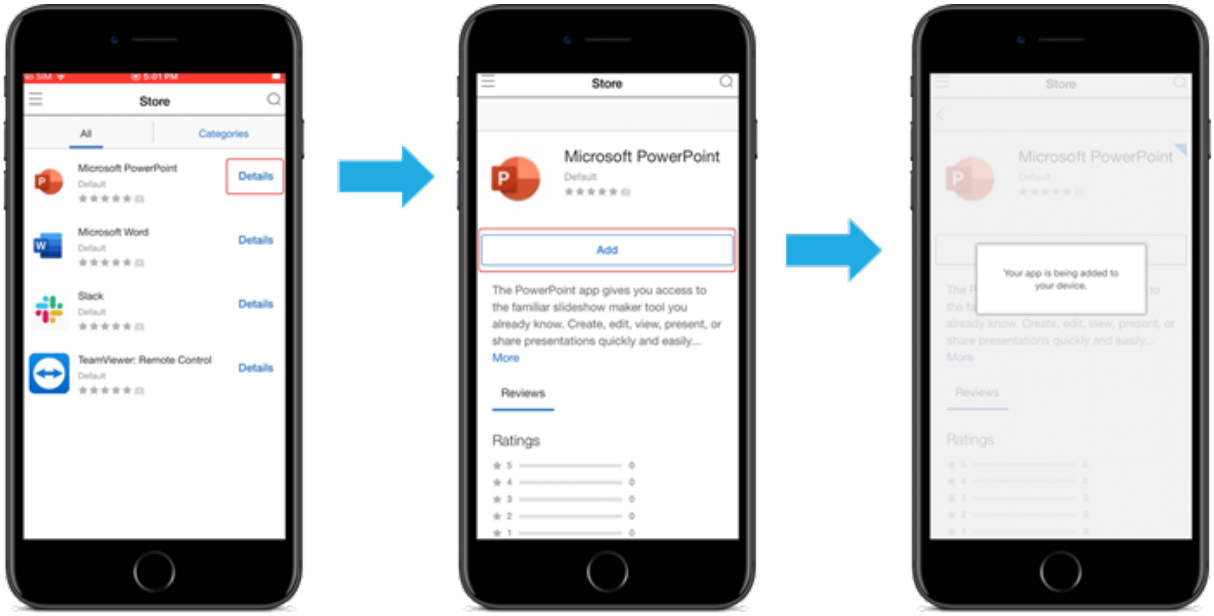
6. Navigate back to **Configure > Delivery Groups**.
7. Select the delivery group you want deployed and click **Deploy**.
8. Users receive a request to deploy apps. Apps install in the background after they accept.

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 XenMobile security assessment to facilitate and handle authentication decisions. After you configure your NAC appliance, the device policies and NAC filters that you configure in XenMobile get enforced.

Using XenMobile 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 XenMobile, see Access control.

Citrix supports these solutions for integration with XenMobile:

- Citrix Gateway
- Cisco Identity Services Engine (ISE)

- ForeScout

Citrix doesn't guarantee integration for other NAC solutions.

With a NAC appliance in your network:

- XenMobile supports NAC as an endpoint security feature for iOS, Android Enterprise, and Android devices.
- You can enable filters in XenMobile to set devices as compliant or non-compliant for NAC, based on rules or properties. For example:
  - If a managed device in XenMobile doesn't meet the specified criteria, XenMobile marks the device as non-compliant. A NAC appliance blocks non-compliant devices on your network.
  - If a managed device in XenMobile 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

XenMobile Server supports the following NAC compliance filters:

Anonymous Devices: Checks if a device is in anonymous mode. This check is available if XenMobile 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 device policy. For 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, XenMobile 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 XenMobile 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 XenMobile APIs change that device 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 a device is still in a managed state, under XenMobile control. 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 XenMobile 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.

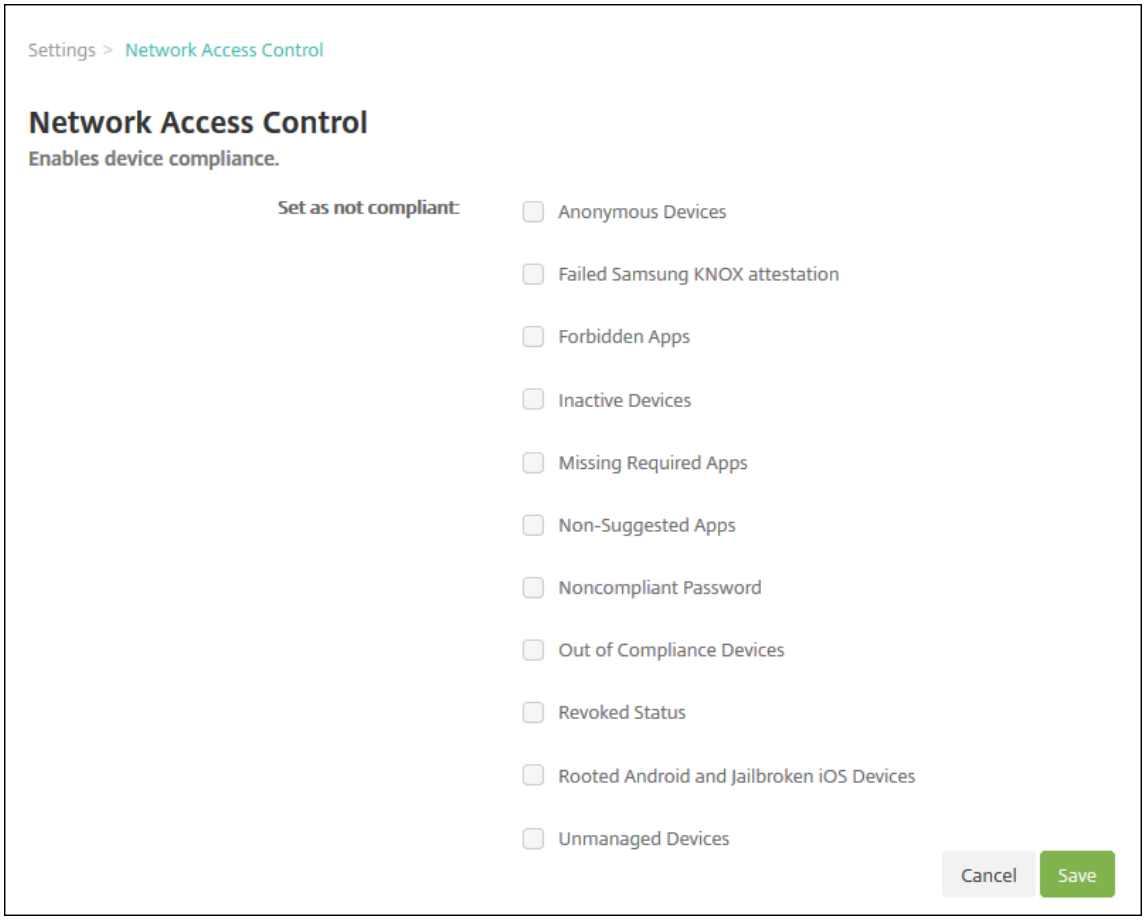
   For Android devices: See Configure the Citrix SSO protocol for Android.

2. Enable NAC filters in XenMobile.
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 XenMobile

1. In the XenMobile 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 a XenMobile Server environment.
- Or, is set up for VPN, not part of the XenMobile Server environment, and can reach XenMobile.

On your virtual VPN server from a console window, do the following. The 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_XenMobileGateway -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>
   ```

   For example: `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_XenMobileGateway -authnProfile xm_nac_prof
   ```

8. Check the connection from Citrix Gateway to a device by typing the following.

   ```
   curl -v -k https://<XenMobile 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 XenMobile. 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 XenMobile by typing the following. In this example, the XenMobile Server IP is 10.207.87.82 and the FQDN is example.em.server.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.server.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 XenMobile 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 to 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
    ```

Samsung Knox

April 1, 2021

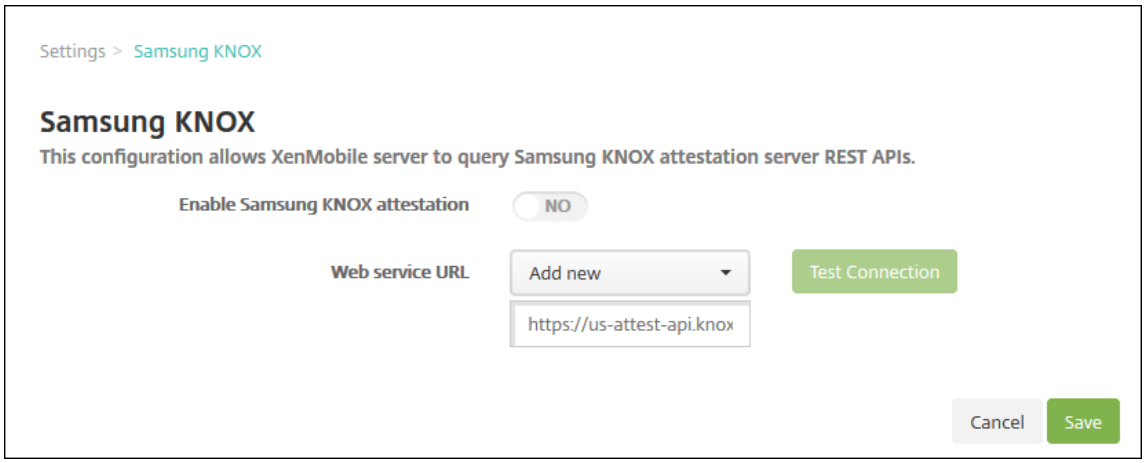
Samsung offers several solutions that are compatible with XenMobile Server.

- XenMobile 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.

You can configure XenMobile to query the Samsung Knox attestation server REST APIs.

Samsung Knox uses 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 trusted boot.

1. In the XenMobile web console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Platforms**, click **Samsung KNOX**. The **Samsung KNOX** page appears.



3. In **Enable Samsung KNOX attestation,** select whether to enable Samsung Knox attestation. The default is **NO**.
4. When you set **Enable Samsung KNOX attestation**, to **YES**, the **Web service URL** option is enabled. Then, in the 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**.

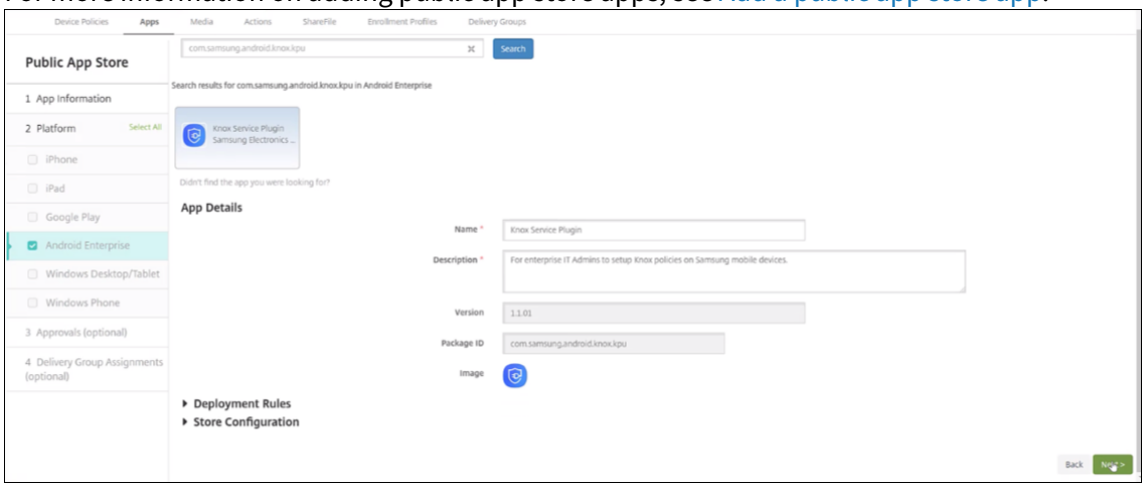
> **Note:**
>
> You can use Samsung Knox Mobile Enrollment to enroll multiple Samsung Knox devices into XenMobile (or any mobile device manager) without manually configuring each device. For information, see Samsung Knox bulk enrollment.

Add the Knox service plug-in app

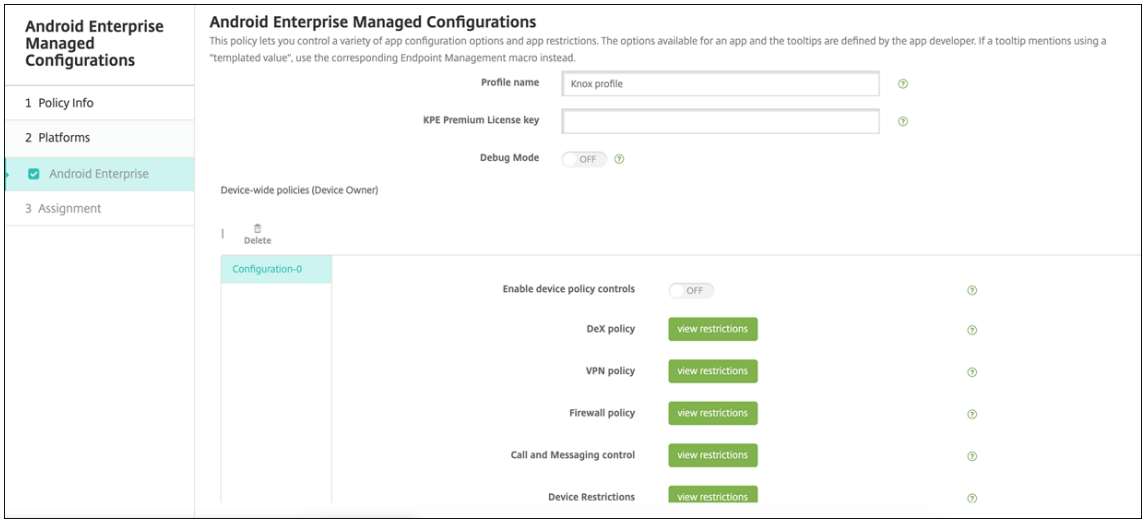
If you plan on using Android Enterprise with Knox, add the Knox service plug-in (KSP) to XenMobile. The KSP app uses AndroidOEMConfig to support features such as security policies, flexible VPN configuration, and biometric authentication controls. AndroidOEMConfig enables OEMs and endpoint mobility managers (EMM) to support custom OEM APIs. Those APIs cover use cases not supported through Android Enterprise.

For more information on KSP, see the Knox Service Plug-in Admin Guide.

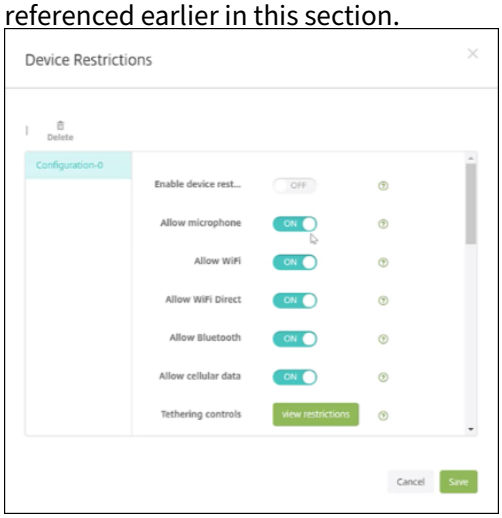
1. Sign in to your Google account and navigate to `https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu`. Approve the Knox Service Plug-in app.
2. Sign in to your XenMobile console and add the Knox service plug-in as a public app store app. For more information on adding public app store apps, see Add a public app store app.



3. In your XenMobile 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 Android Enterprise 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 Plug-in Guide referenced earlier in this section.



7. Click **Next** and configure deployment rules for the policy.
8. Click **Save**.

Samsung Knox bulk enrollment

March 22, 2021

To enroll multiple Samsung Knox devices into XenMobile (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 XenMobile Knox container. For more information on Knox Mobile Enrollment, see the Knox Mobile Enrollment Admin Guide.

Prerequisites for Knox Mobile Enrollment

- XenMobile 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 XenMobile 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	`https://gslb.secb2b.com`	443	Global load balancer for Knox Mobile Enrollment initiation
All	`https://gslb.secb2b.com`	80	Global load balancer for Knox Mobile Enrollment initiation on some limited legacy devices
All	`umc-cdn.secb2b.com`	443	Samsung agent update servers
All	`bulkenrollment.s3.amazonaws.com`	80	Knox Mobile Enrollment customer EULAs
All	`eula.secb2b.com`	443	Knox Mobile Enrollment customer EULAs

Device Region	URL	Port	Destination
All	us-be-api-mssl.samsungknox.com	443	Samsung servers for IMEI verification
United States	https://us-segd-api.secb2b.com	443	Samsung Enterprise Gateway for US region
Europe	https://eu-segd-api.secb2b.com	443	Samsung Enterprise Gateway for European region
China	https://china-segd-api.secb2b.com	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. XenMobile does not use the Samsung MDM protocol.
- **Custom JSON Data:** Secure Hub needs the XenMobile 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", "xm_username":"Username", "xm_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", "xm_username":"userN", "
  xm_password":"password1234"}
  { "serverURL":"https://pmdm.mycorp-inc.net/zdm", "xm_username":"userN2"
  , "xm_password":"password7890"}
  ```

  In this example, typical for kiosk-based devices, Secure Hub prompts users for their credentials:

  ```
  { "serverURL":"https://example.com/zdm"}
  ```

  You can also enter custom JSON for zero-touch enrollment for Android Enterprise.

  ```
  1       {
  ```



```
2
3           "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4           {
5
6               "serverURL":"URL","xm_username":"username","
                   xm_password":"password"
7            }
8
9       }
10
11  <!--NeedCopy-->
```

When a device starts enrollment, the device downloads Secure Hub from the given URL, installs Secure Hub, and opens Secure Hub.

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**.

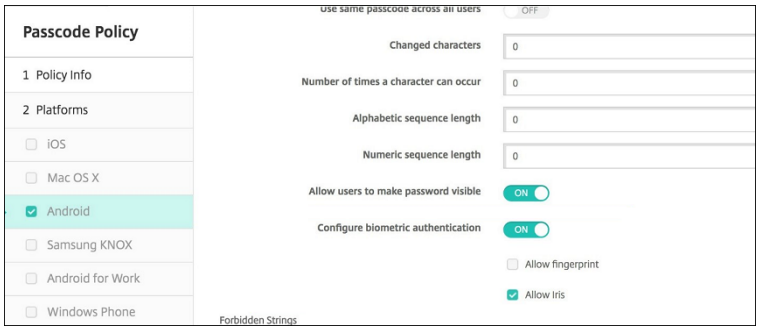
4. If prompted, enter the **User ID** and **Password** provided by the IT administrator.

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

XenMobile 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 XenMobile, users and third-party apps cannot enable the feature.

1. In the XenMobile 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.



Security actions

April 27, 2021

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 device 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 XenMobile. 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 DEP.
- **Clear restrictions:** On supervised iOS devices, this command allows XenMobile 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 XenMobile 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.
  - 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 and macOS devices, the wipe occurs immediately, even if the device is locked. For iOS 11 devices (minimum version): When you confirm the full wipe, you can choose to preserve the cellular data plan on the device.
  - For Windows Phone devices, a full wipe removes all XenMobile information and all user data. This data includes personal content such as apps, emails, contacts, and media.
  - For Windows Mobile devices that are running Windows Mobile 6 or earlier: After the wipe, you might need to send the device back to the manufacturer to reload the original operating system, software, or both.
  - 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, XenMobile 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, this command succeeds only if the devices are in MDM Lost Mode.
- **Lock:** Remotely locks a device. This action is useful when you lose a device and don't know if the device is stolen. XenMobile 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 XenMobile console.
- **Lock and Reset Password:** Remotely locks a device and resets the passcode.
  - Not supported for devices enrolled in Android Enterprise in work profile mode that are running Android versions before Android 8.0.
  - On devices enrolled in Android Enterprise in work profile mode that are running Android 8.0 or greater:
    * The passcode sent locks the work profile. The device is not locked.
    * If no passcode is sent, or the passcode sent doesn't meet passcode requirements, and no passcode is already set on the work profile: The device is locked.
    * If no passcode is sent, or the passcode sent doesn't meet passcode requirements, but a passcode is already set on the work profile: The work profile is locked but the device is not locked.
- **Notify (Ring):** Plays a sound on Android devices.
- **Reboot:** Restarts Windows 10 devices. For Windows Tablet and PCs, the message "System will reboot soon" appears and then 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 iOS devices.
- **Revoke:** Prohibits a device from connecting to XenMobile Server.

- **Revoke/Authorize (iOS, macOS):** 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.
- **Selective wipe:** Erases all corporate data and apps from a device, leaving personal data and apps in place. After a selective wipe, a user can reenroll the device.
  - 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 XenMobile to install apps on the device. The wipe also removes all XenMobile 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.

Security actions for Android devices

Security action	Android (except for Android Enterprise devices)	Android Enterprise (BYOD)	Android Enterprise (corporate-owned)
App Lock	Yes	No	No
App Wipe	Yes	No	No
Full Wipe	Yes	No	Yes
Locate	Yes: For devices running Android 6.0+, Locate 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, XenMobile again requests location permission when sending the Locate command.	Yes: For devices running Android 6.0+, Locate 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, XenMobile again requests location permission when sending the Locate command.	Yes: For devices running Android 6.0+, Locate 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, XenMobile again requests location permission when sending the Locate command.
Lock	Yes	Yes	Yes
Lock and Reset Password	Yes	No	Yes
Notify (Ring)	Yes	Yes	Yes
Revoke	Yes	Yes	Yes
Selective Wipe	Yes	Yes	No

Security actions for iOS and macOS devices

Security action	**iOS**	**macOS**
Activation Lock Bypass	Yes	No
App Lock	Yes	No
App Wipe	Yes	No

Security action	iOS	macOS
ASM Deployment Program Activation Lock	Yes	No
Clear Restrictions	Yes	No
Enable/Disable Lost Mode	Yes	No
Enable/Disable Tracking	Yes	No
Full Wipe	Yes	Yes
Locate	Yes	No
Lock	Yes	Yes
Ring	Yes	Yes
Request/Stop AirPlay Mirroring	Yes	No
Restart/Shut Down	Yes	No
Revoke/Authorize	Yes	Yes
Selective Wipe	Yes	Yes
Unlock	Yes	No

Security actions for Windows devices

Security action	Windows Phone 10	Windows Tablet 10	Windows Phone 8.1
Locate	Yes	Yes	No
Lock	Yes	Yes	Yes
Lock and Reset Password	Yes	No	Yes
Reboot	Yes	Yes	No
Revoke	Yes	Yes	Yes
Ring	Yes	No	Yes
Selective Wipe	Yes	Yes	Yes
Wipe	Yes	Yes	Yes

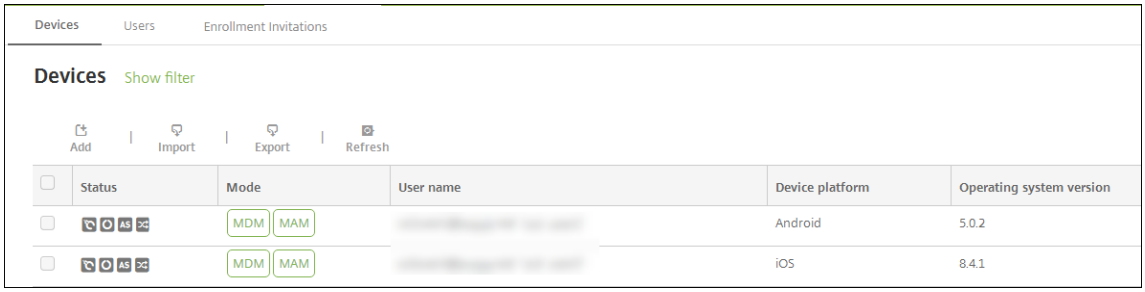
The remainder of this article provides the steps for performing various security actions. You can also automate some actions. For more information, see Automated actions.

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. This feature is supported on devices running iOS 7 and above.

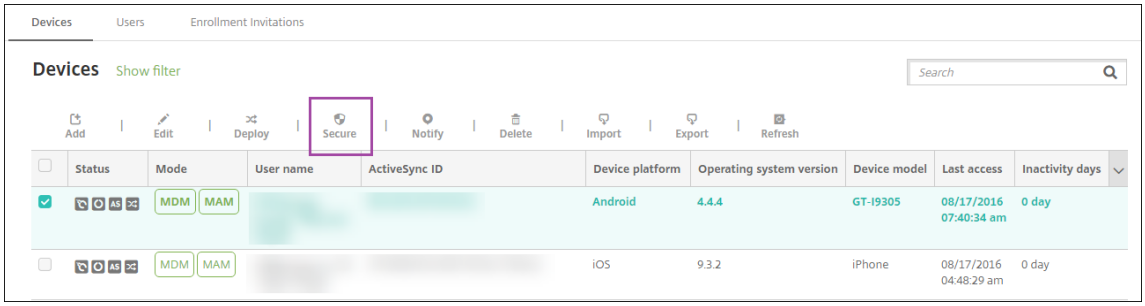
To display a message and phone number on a locked device, set the Passcode policy to **true** in the XenMobile console. Alternatively, users can enable the passcode on the device manually.

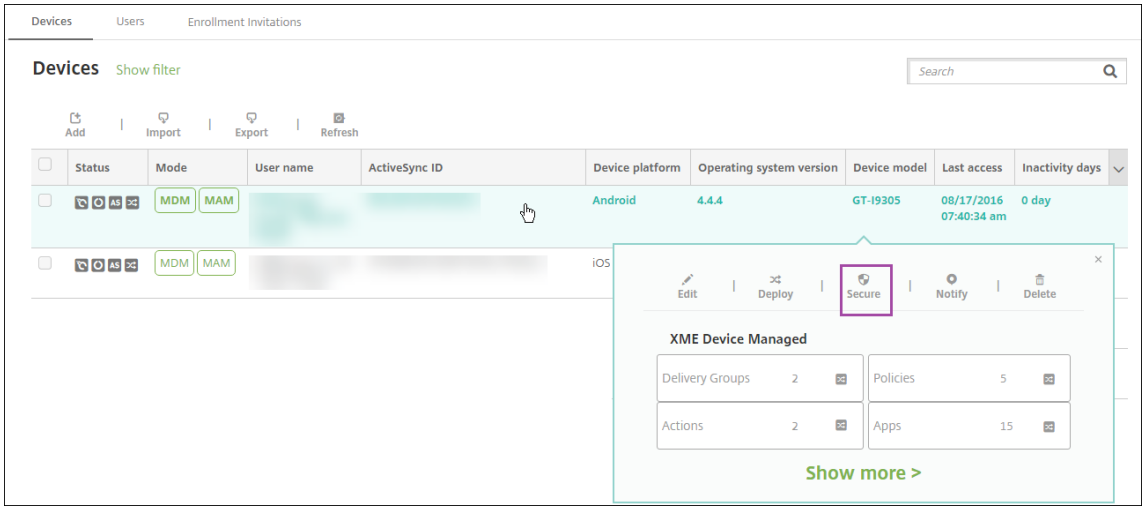
1. Click **Manage > Devices**. The **Devices** page appears.



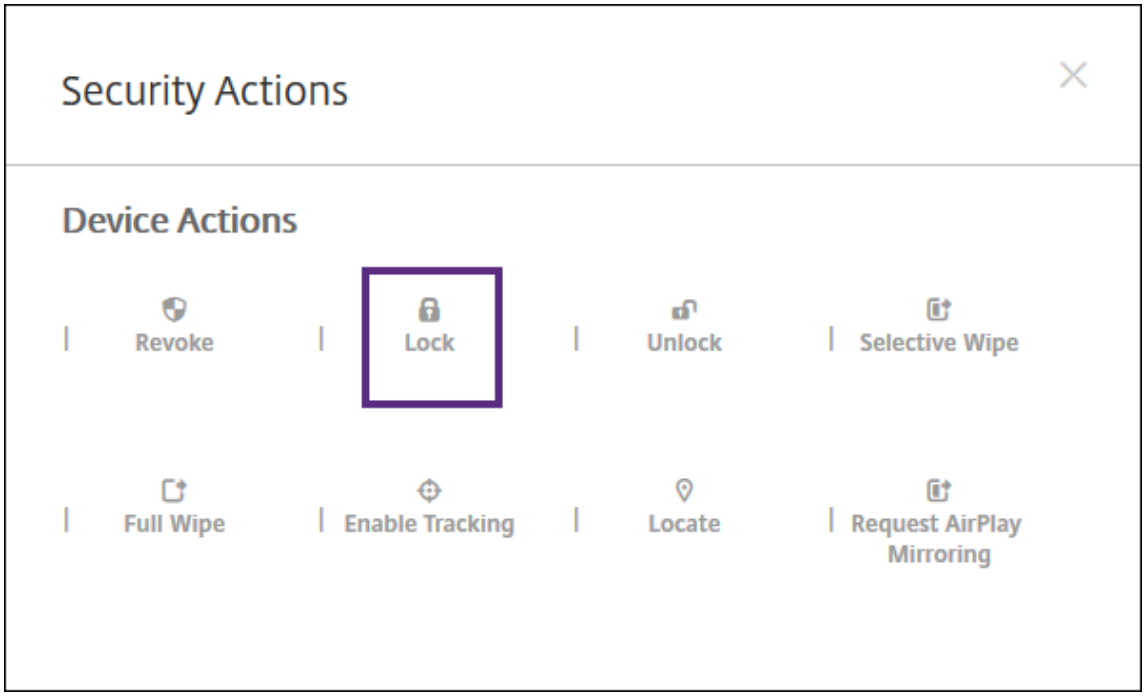
2. Select the iOS device you want to lock.

   When you select the check box next to a device, the options menu displays above the device list. When you click anywhere else in the list, the options menu appears on the right side of the listing.

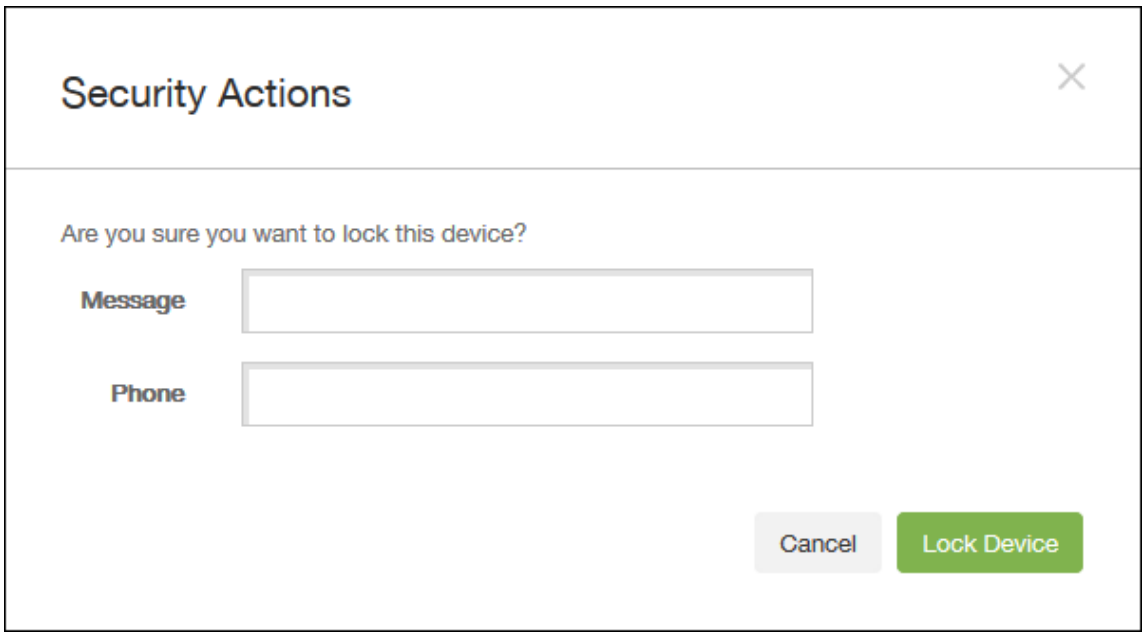




3. In the options menu, click **Secure**. The **Security Actions** dialog box appears.



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.

   For iPads running iOS 7 and later: iOS appends the words “Lost iPad” to what you type in the **Message** field.

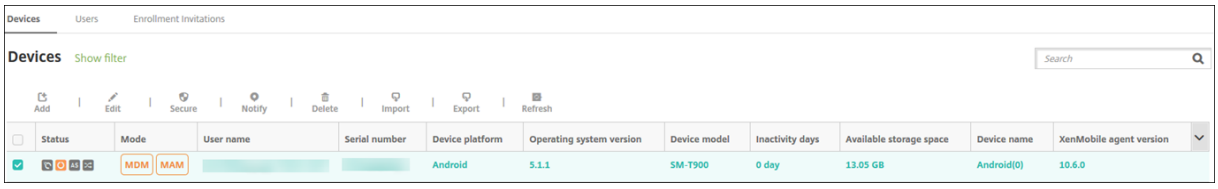
   For iPhones running iOS 7 and later: If you leave the **Message** field empty and provide a phone number, Apple displays the message “Call owner” on the device lock screen.

6. Click **Lock Device**.

Remove a device from the XenMobile console

> **Important:**
>
> When you remove a device from the XenMobile 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 XenMobile console, go to **Manage > Devices**, select a managed device, and then click **Delete**.



Selectively wipe a device

1. Go to **Manage > Devices**, select a managed device, and then click **Secure**.

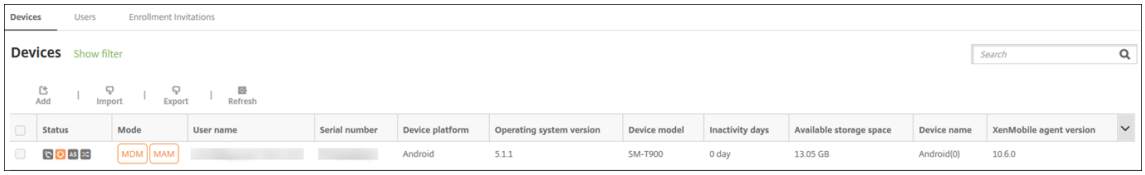
2. In **Security Actions**, click **Selective wipe**.
3. For Android devices only, disconnect the device from the corporate network: After the device is wiped, in **Security Actions**, click **Revoke**.

   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 XenMobile 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.



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.

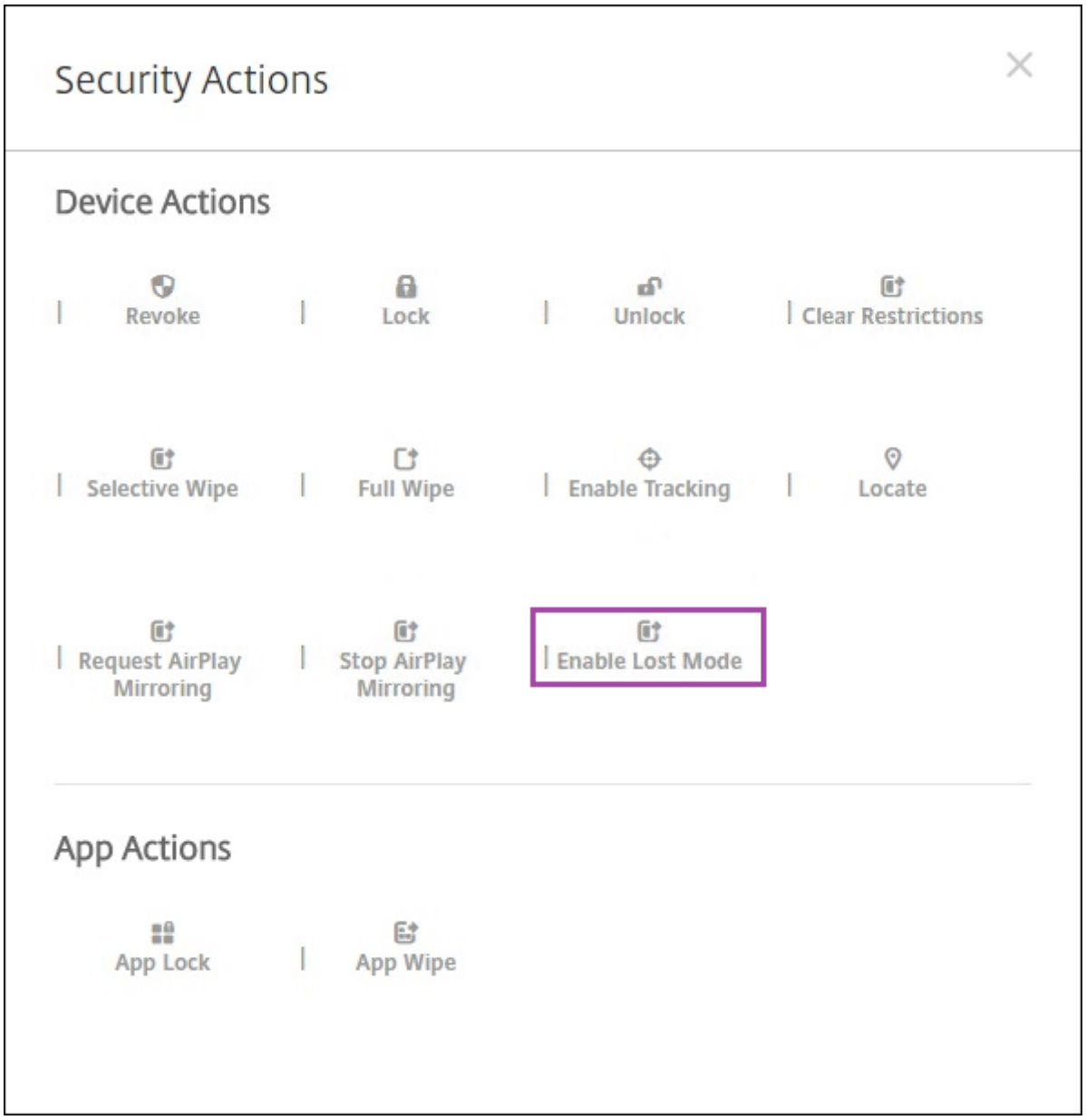
   You can also use the **Security Actions** box to check the device status for a user whose account is disabled or deleted from Active Directory. The presence of the App Unlock or App Unwipe actions indicate apps that are locked or wiped.

Put iOS devices in Lost Mode

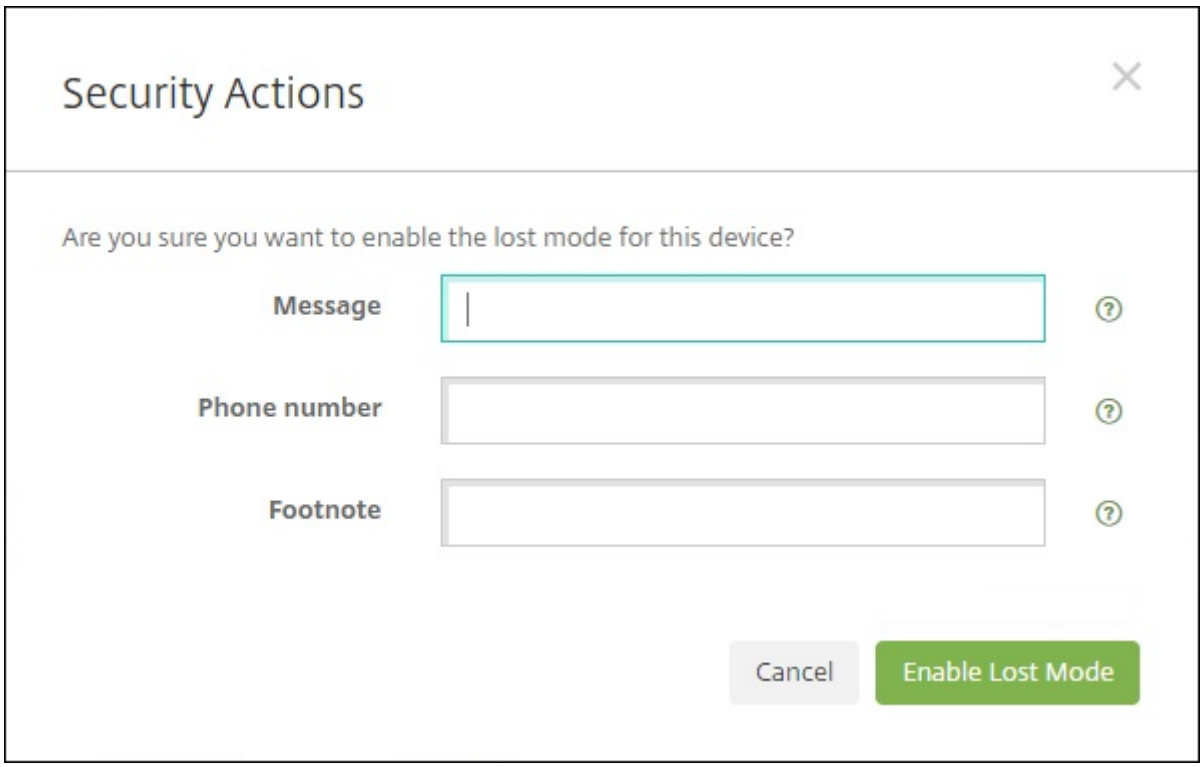
The XenMobile Lost Mode device property puts an iOS device in Lost Mode. Unlike Apple Managed Lost Mode, XenMobile Lost Mode doesn't require a user to perform either of the following actions to enable locating their device: Configure the **Find My iPhone/iPad** setting or enable the Location Services for Citrix Secure Hub.

In XenMobile Lost Mode, only the XenMobile Server can unlock the device. (In contrast, if you use the XenMobile 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**.

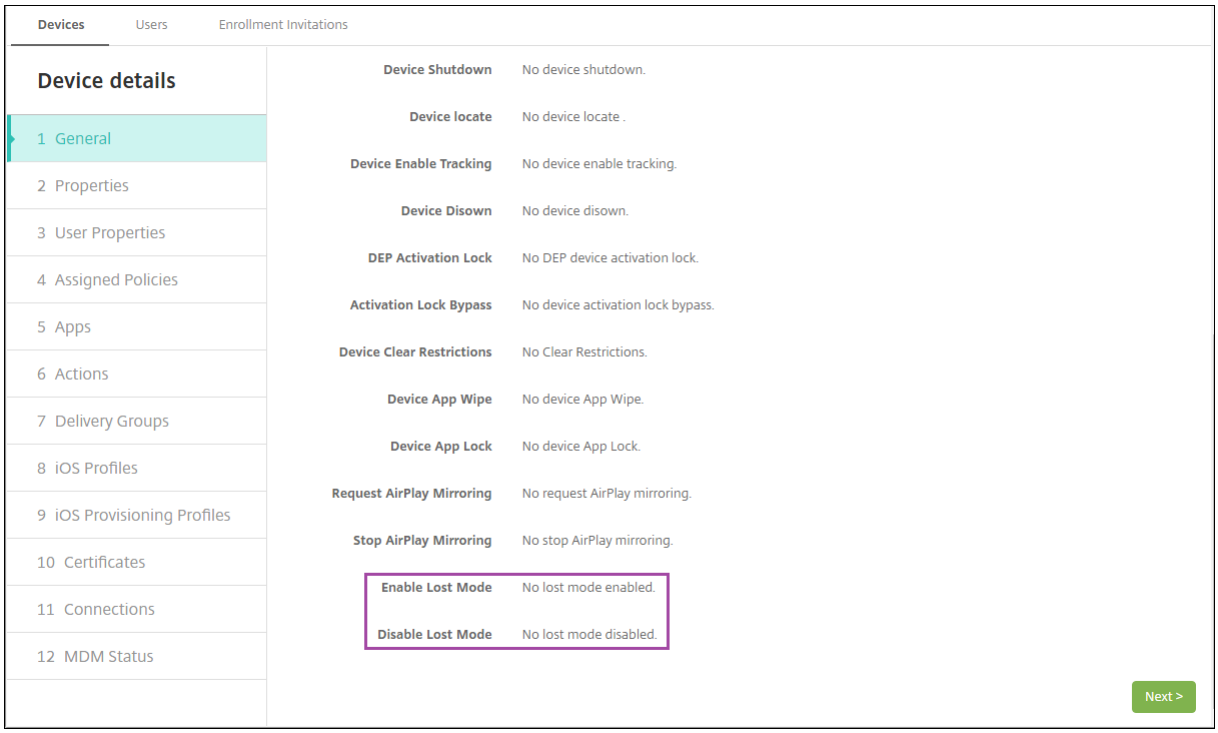


If you click **Enable Lost Mode**, type information to appear on the device when it's in lost mode.

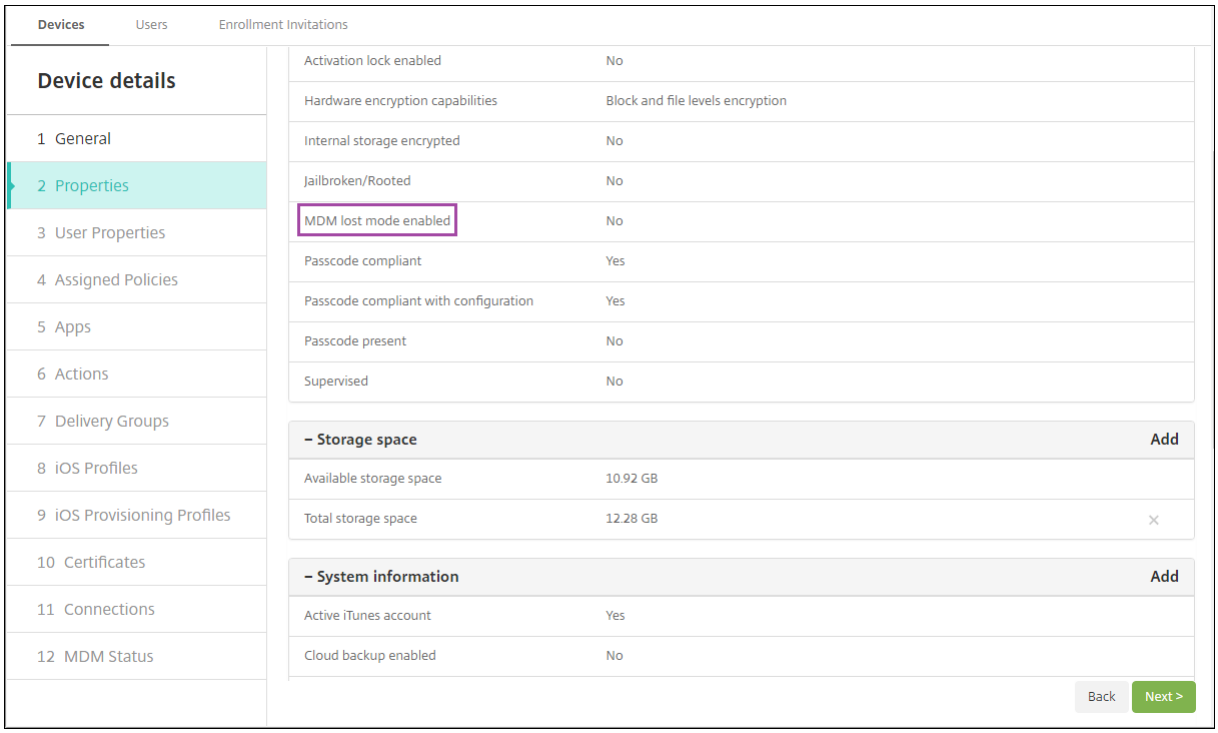


Use any of the following methods to check Lost Mode status:

- 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.



- From **Manage > Devices**, on the **Properties** tab, verify that the value of the **MDM lost mode enabled** setting is correct.



If you enable XenMobile Lost Mode on an iOS device, the XenMobile 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.

For iPads running iOS 7 and later: iOS appends the words "Lost iPad" to what you type in the **Message** in the **Security Actions** screen.

For iPhones running iOS 7 and later: 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 disable 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 XenMobile MDM Options device policy. You can then manage a device from the XenMobile 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 XenMobile 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 iTunes account credential, you can bypass that step by issuing the Activation Lock Bypass security action from the XenMobile console.

Device requirements for activation lock bypass

- iOS 7.1 (minimum version)
- Supervised through Apple Configurator or Apple DEP
- Configured with an iCloud account
- Find My iPhone/iPad enabled
- Enrolled in XenMobile
- 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 disable 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 with a generated Activation lock bypass code and with the Activation lock enabled: If you can't bypass the Activate iPhone/iPad page after a Full Wipe, there is no need to delete the device from XenMobile. Either you or the user can contact Apple support to unblock the device directly.
- During a hardware inventory, XenMobile queries a device for an Activation lock bypass code. If a bypass code is available, the device sends it to XenMobile. Then, to remove the bypass code from the device, send the Activation Lock Bypass security action from the XenMobile console. At that point, XenMobile Server 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 as follows. On the device, manually enter the credentials of the iCloud account. Or, 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**.

Shared devices

September 8, 2020

XenMobile 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 to 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. Doesn't support the basic Apple Deployment Program enrollment for a XenMobile Enterprise shared device. Use an authorized Apple Deployment Program to enroll a shared device in this mode.
- Doesn't support client certificate authentication, Citrix PIN, Touch ID, User Entropy, and two-factor authentication.

MDM+MAM enrollment

- Available only on iOS and Android devices.
- Supports only Active Directory user name and password authentication.
- Doesn't support client certificate authentication, Secure Hub passcode, Touch ID, User Entropy, and two-factor authentication.
- Doesn't support MAM-only enrollment. The devices must enroll in MDM.
- Supports only Secure Mail, Secure Web, and the ShareFile mobile apps. Doesn't support HDX apps.
- Supports only Active Directory users. Doesn't support local users and groups.
- To update to MDM+MAM, requires re-enrollment of existing MDM-only shared devices.
- Users cannot share native apps on the devices.

- Once downloaded during first-time enrollment, mobile productivity apps are not downloaded again during user sign-in.
- On Android, to isolate each user's data for security purposes, set the **Disallow rooted devices** policy in the XenMobile console to **On**.

Prerequisites for enrolling shared devices

Before you can enroll shared devices, you must do the following:

- Create a shared device enrollment user role. See Configuring Roles with RBAC.
- Create a shared device user. See To add, edit, unlock, or delete local user accounts.
- Create a delivery group that contains the base policies, apps, and actions that you want to apply to the shared device user. See Deploy resources.

Prerequisites for MDM+MAM enrollment

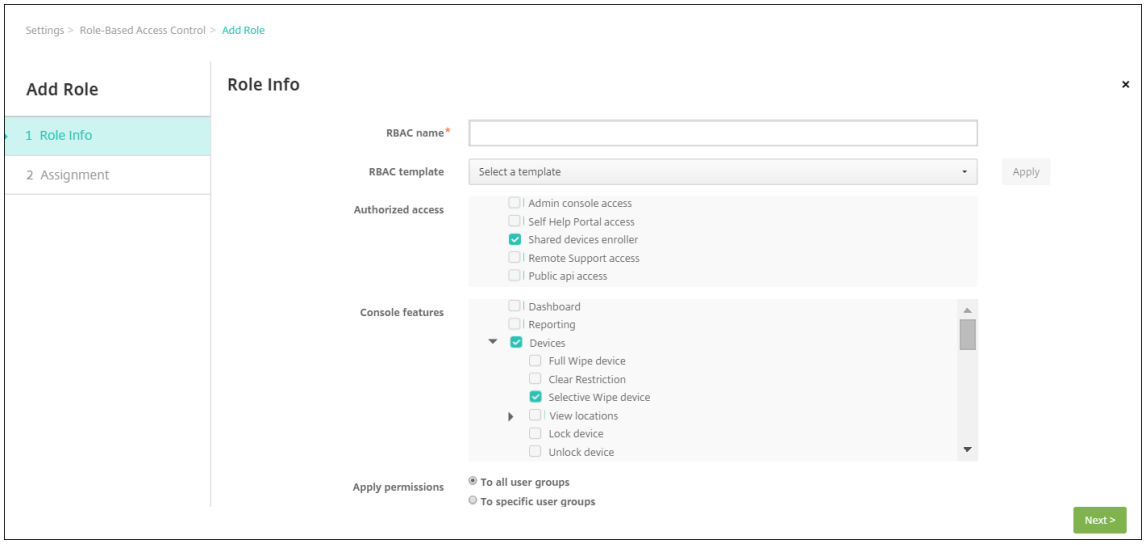
1. Create an Active Directory group. Give it a descriptive name, such as **Shared Device Enrollers**.
2. Add to the group the Active Directory users who enroll shared devices. If you want a new account for this purpose, create a new Active Directory user (for example, **sdenroll**) and add that user to the Active Directory group.

Configuring a shared device

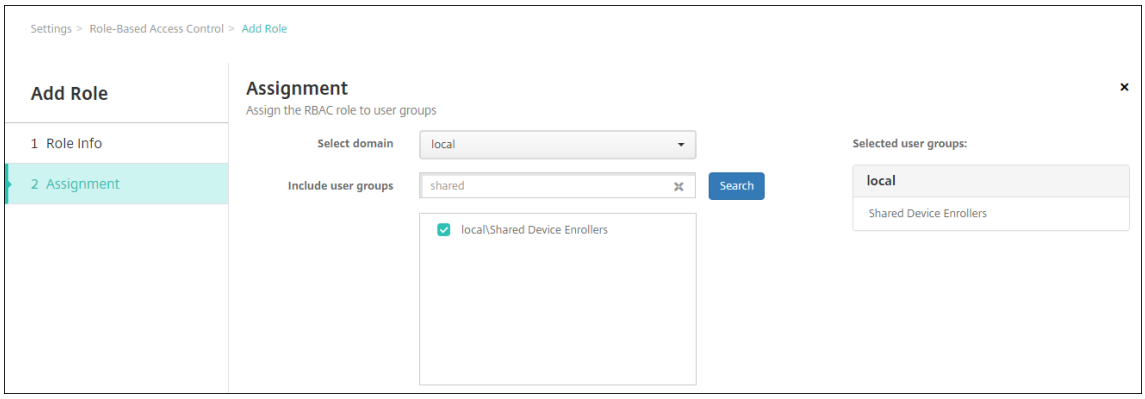
Follow these steps to configure a shared device.

1. From the XenMobile 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.

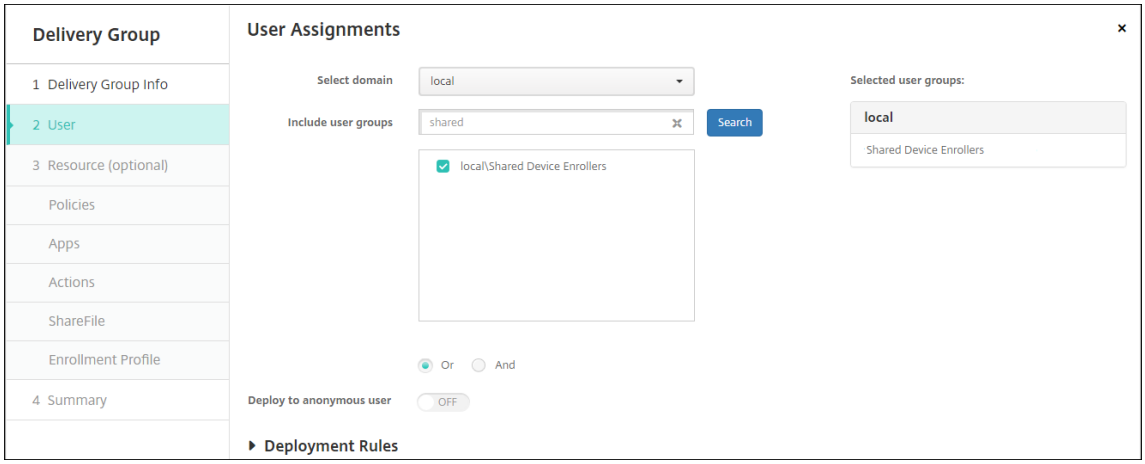
   For **Apply Permissions**, keep the default setting, **To all user groups**, or assign permissions to specific Active Directory user groups with the **To specific user groups**.



Click **Next** to move to the **Assignment** screen. Assign the shared-device enrollment role to the Active Directory group for shared device enrollment users, created in Step 1 under Pre-requisites. 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 that you want to apply to the device when a user is not signed on. Then associate that delivery group with the Active Directory group of the shared device enrollment user.



5. Install Secure Hub on the shared device and enroll it in XenMobile using the shared device enrollment user account. You can now view and manage the device through the XenMobile console. For more information, see Enroll devices.
6. To apply different policies or to provide more apps for authenticated users, you must create a delivery group associated with those users and deployed 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. Remove 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, that person's policies and apps get deployed to the device. When that user signs off, any policies and apps that aren't part of 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. Secure Hub blocks new sign-ons until it removes the policies, apps, and data associated with the previous user.

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

XenMobile AutoDiscovery Service

August 9, 2021

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 XenMobile deployments.

With the AutoDiscovery service, users:

- Can use their corporate network credentials to enroll their devices.

- Don't need to enter details about the XenMobile 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 XenMobile. To configure certificate pinning for your XenMobile 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

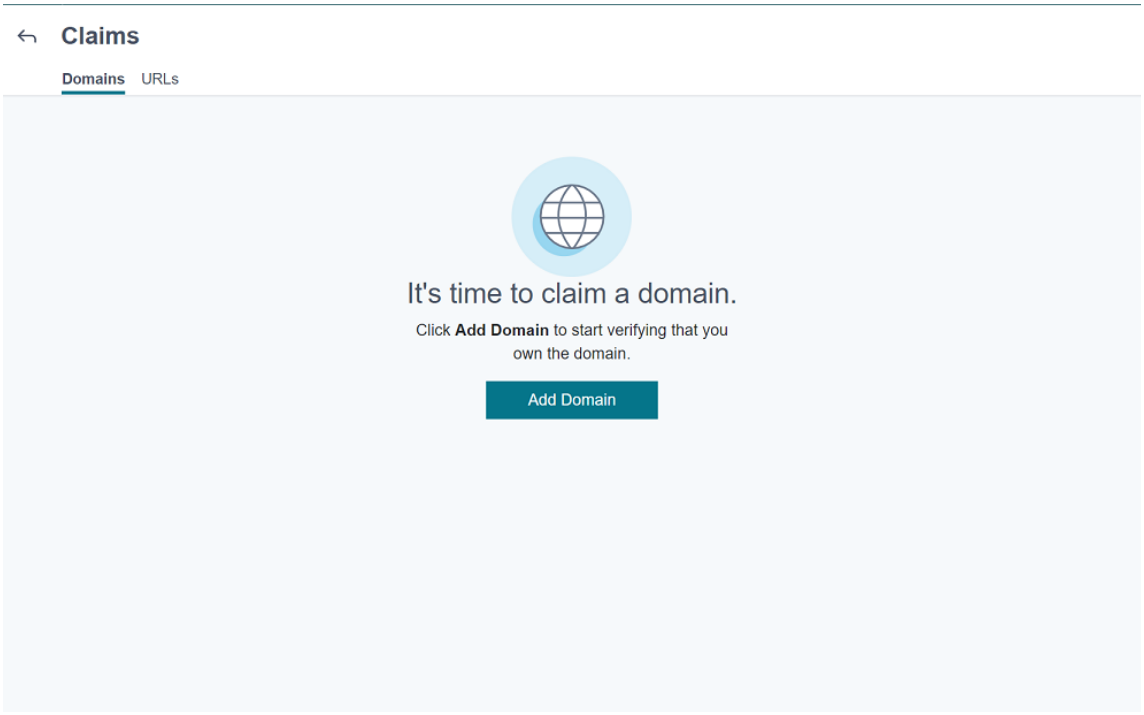
- The new AutoDiscovery service in Citrix Cloud requires the latest version of Secure Hub:
  - For iOS, Secure Hub version 21.1.0 or later
  - For Android, Secure Hub version 21.2.1 or later

    Devices 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.

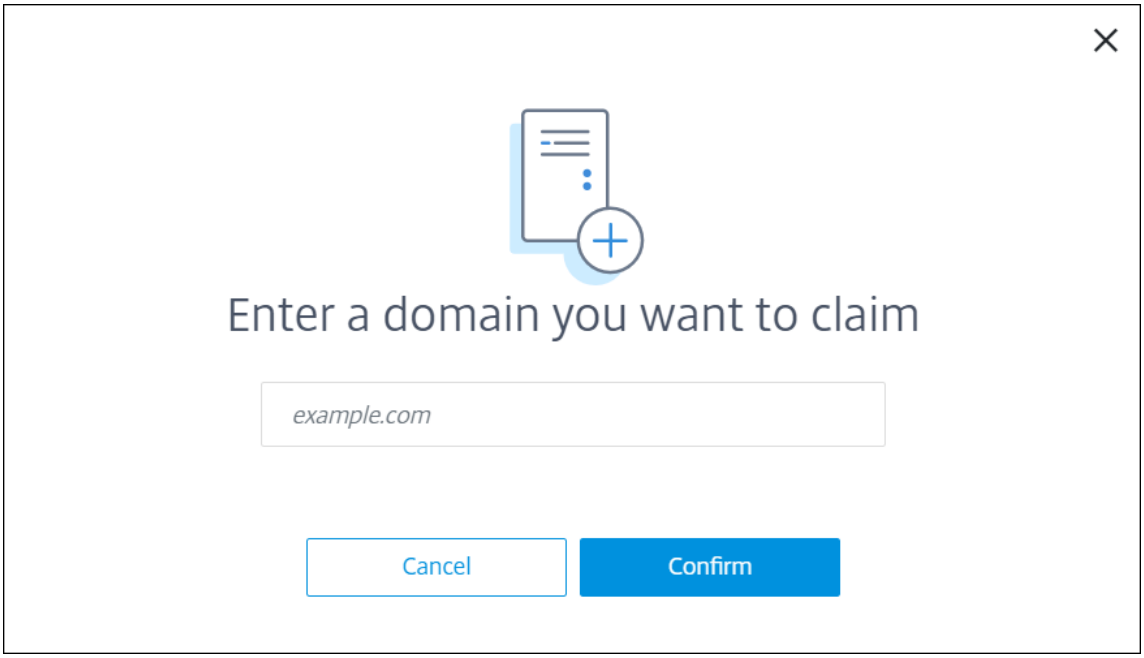
  Citrix migrated all existing AutoDiscovery records to Citrix Cloud without a disruption in service. The migrated records don't automatically appear in the new console. You must reclaim domains in the new AutoDiscovery service to prove ownership. For more information, see CTX312339.
- Before starting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

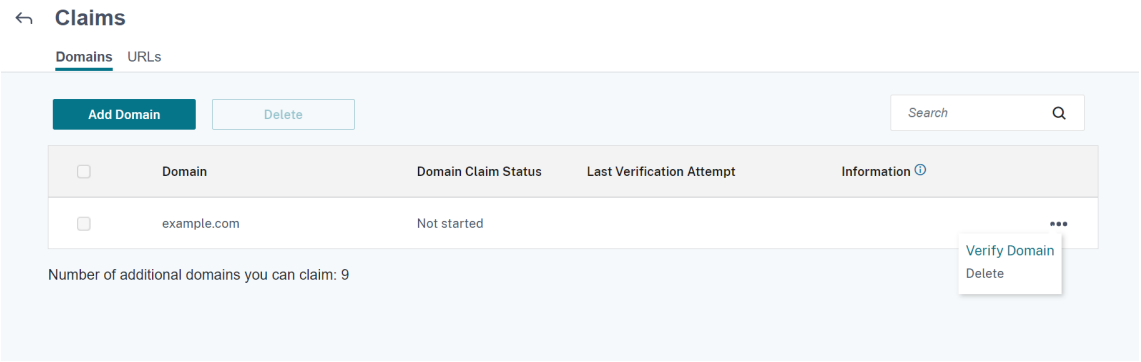
1. On the **Claims > Domains** tab, click **Add Domain**.



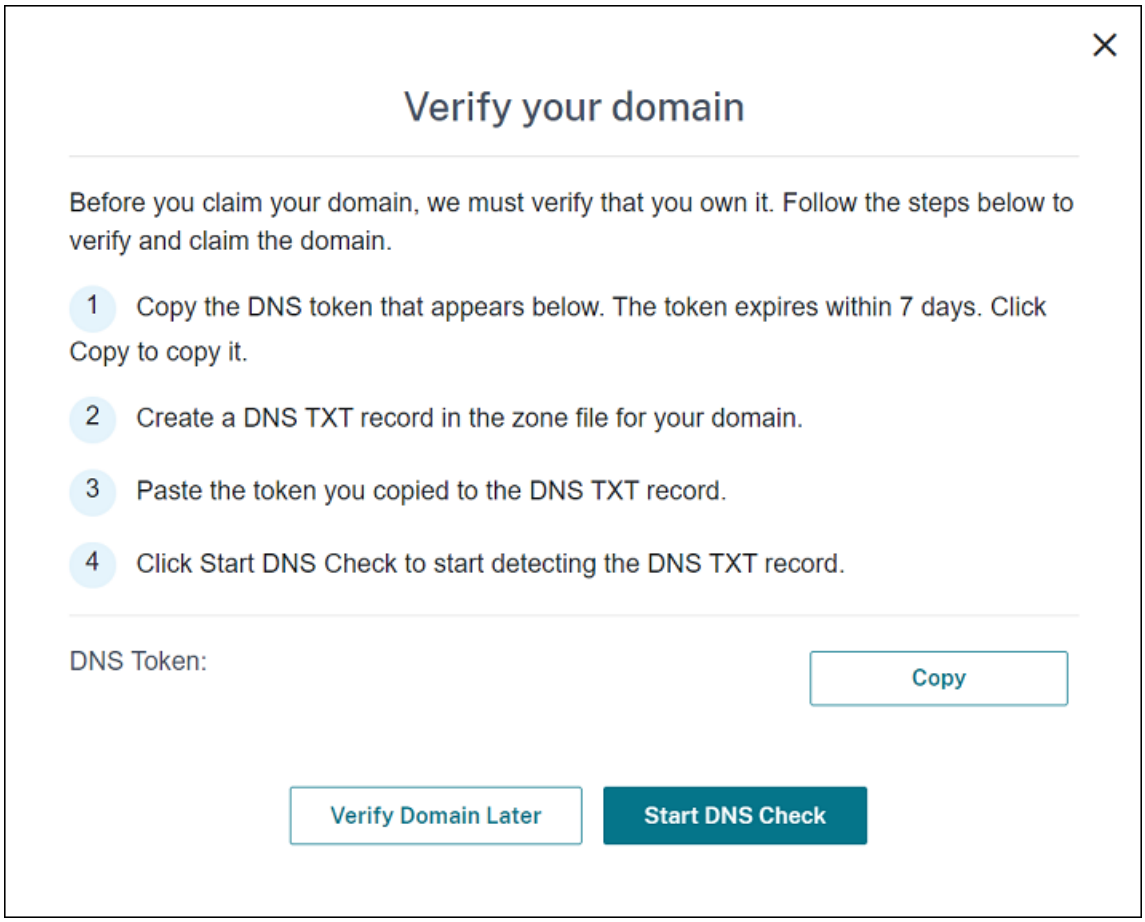
2. In the dialog box that appears, enter the domain name of your XenMobile environment and then click **Confirm**. Your domain appears in **Claims > Domains**.



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.



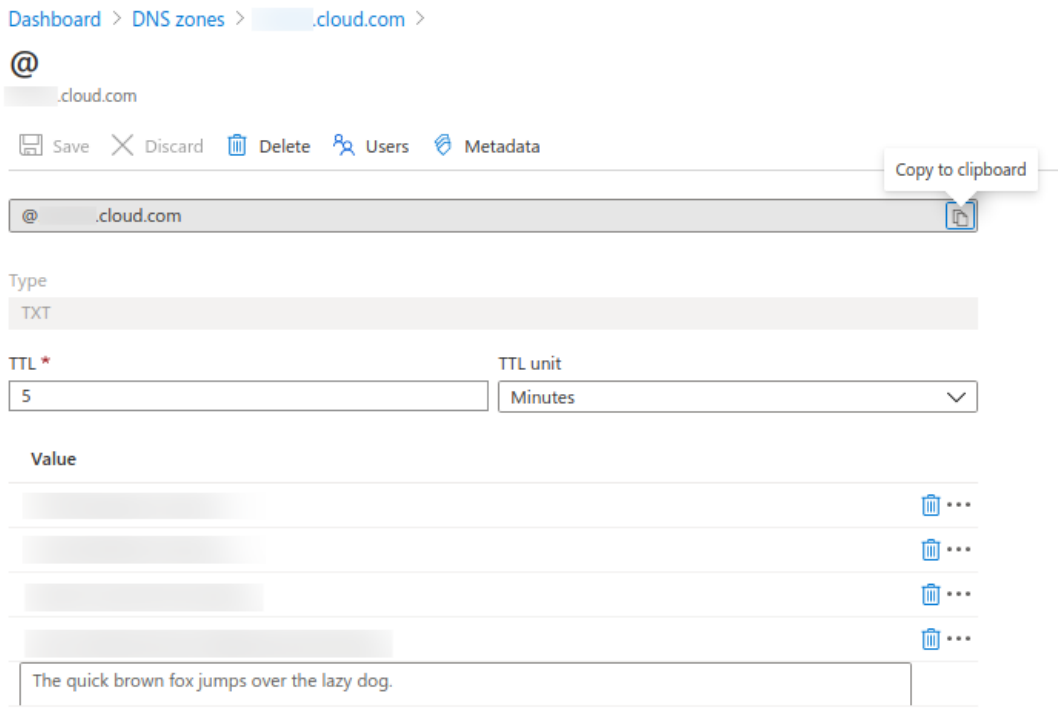
4. On the **Verify your domain** page, follow the instructions to verify that you own the domain.



   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 XenMobile 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 XenMobile 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 XenMobile Server.
   - Instructs the device to request a valid certificate from XenMobile.

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

Device policies

April 20, 2021

You can configure how XenMobile 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.

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 XenMobile device policies for Windows 10, keep the following rule in mind. If a policy on one or more enrolled Windows 10 devices conflicts, the policy aligned with the GPO takes precedence.

To see which policies the Android Enterprise container supports, see Android Enterprise.

Prerequisites

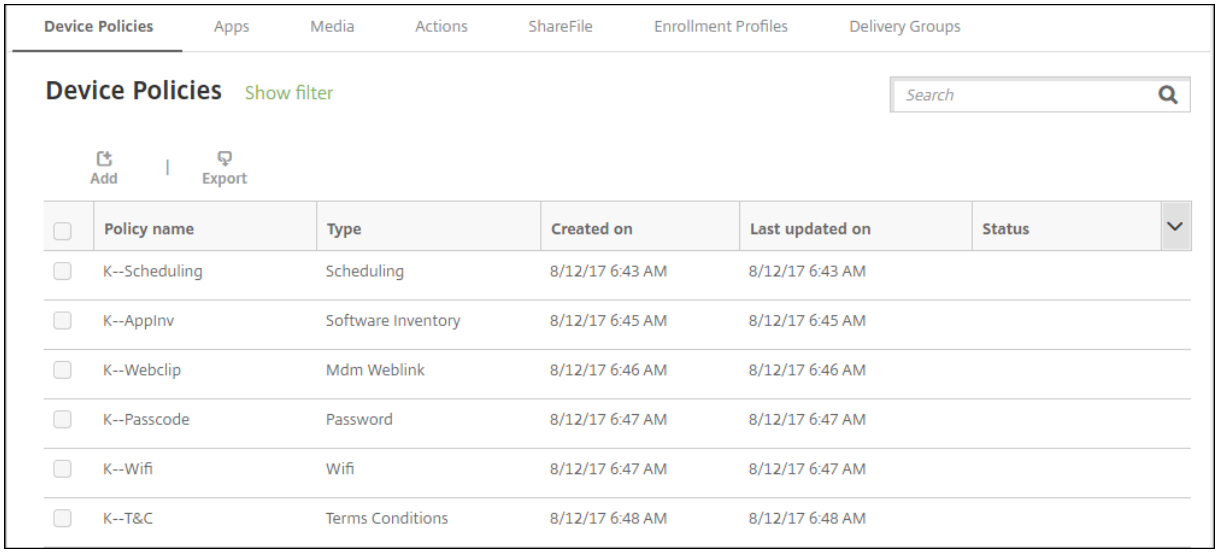
- Create any delivery groups you plan to use.
- Install any necessary CA certificates.

Add a device policy

The basic steps to create a device policy are as follows:

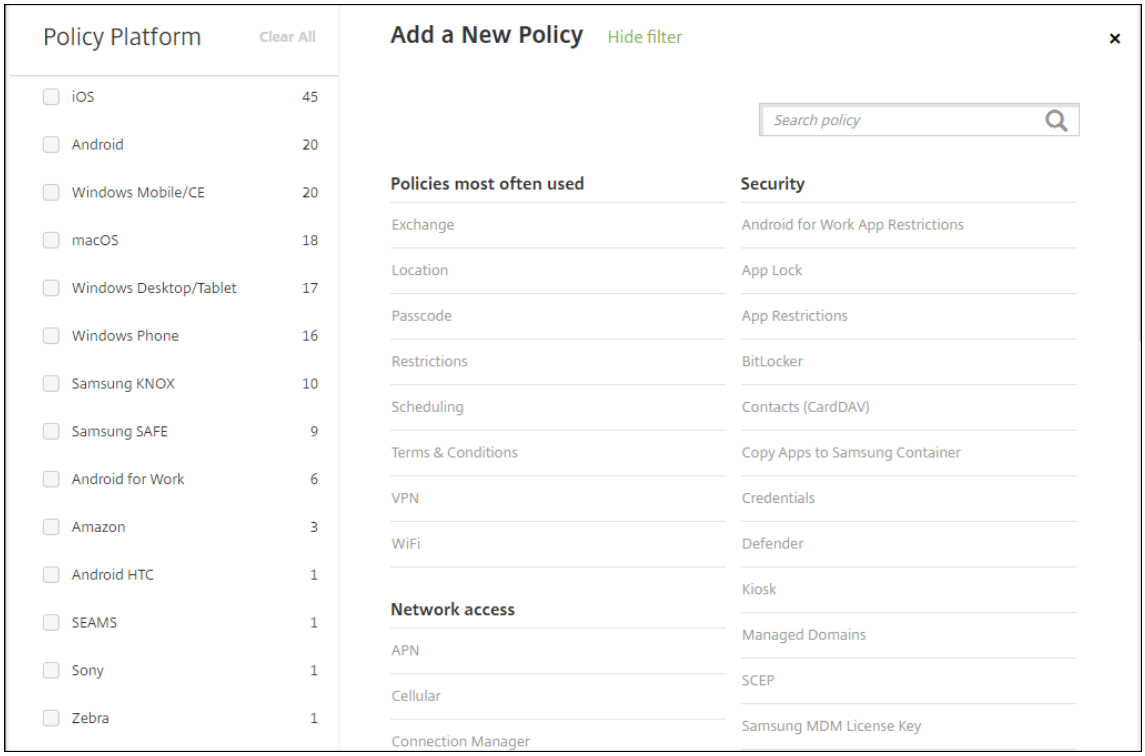
1. Name and describe the policy.
2. Configure the policy for one or more platforms.
3. Create deployment rules (optional).
4. Assign the policy to delivery groups.
5. Configure the deployment schedule (optional).

To create and manage device policies, go to **Configure > Device Policies**.

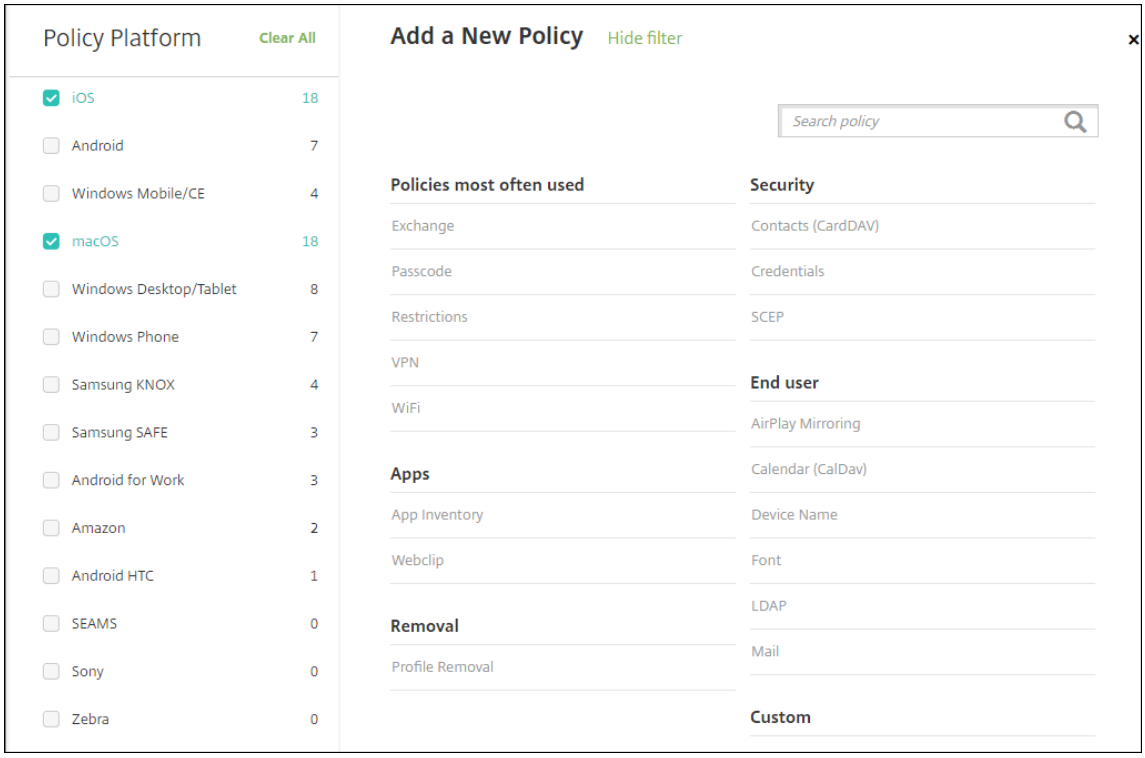


To add a policy:

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.

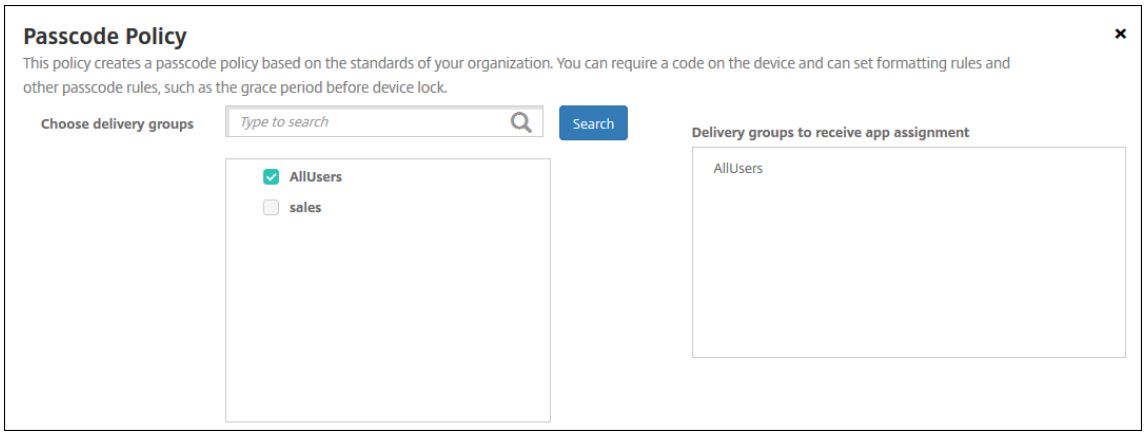
To configure deployment rules, assignments, and schedule

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 determine when the policy should be deployed. 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** to change the condition or **Delete** to remove the condition.
   - 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.

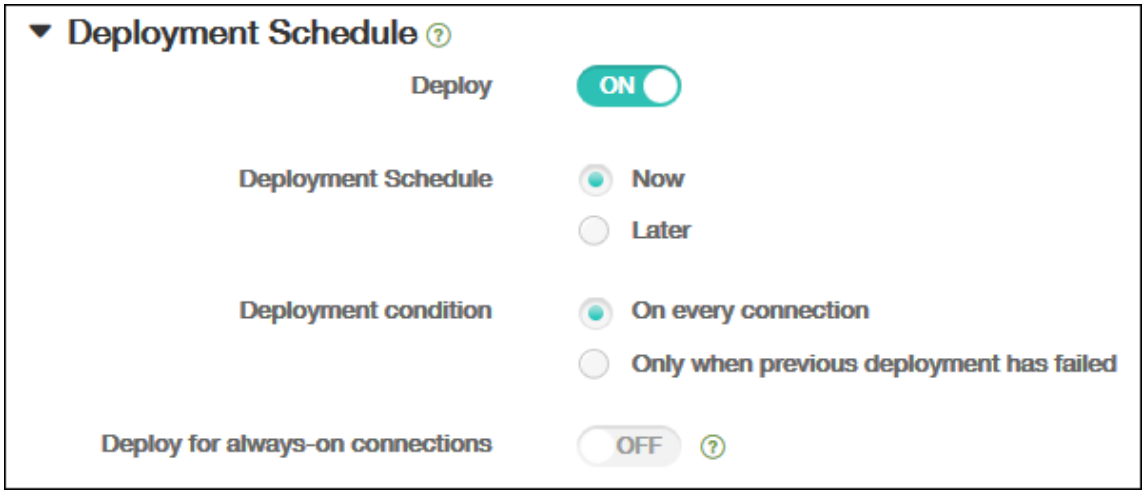
   Delivery groups to receive app assignment doesn't appear until you select a delivery group.



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.
>
> 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**, which does not apply to iOS.



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 XenMobile uninstall device policy. For information, see XenMobile 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

  You can't directly remove a device policy from a Windows 10 Desktop or Tablet device. However, you can use either of the following methods:

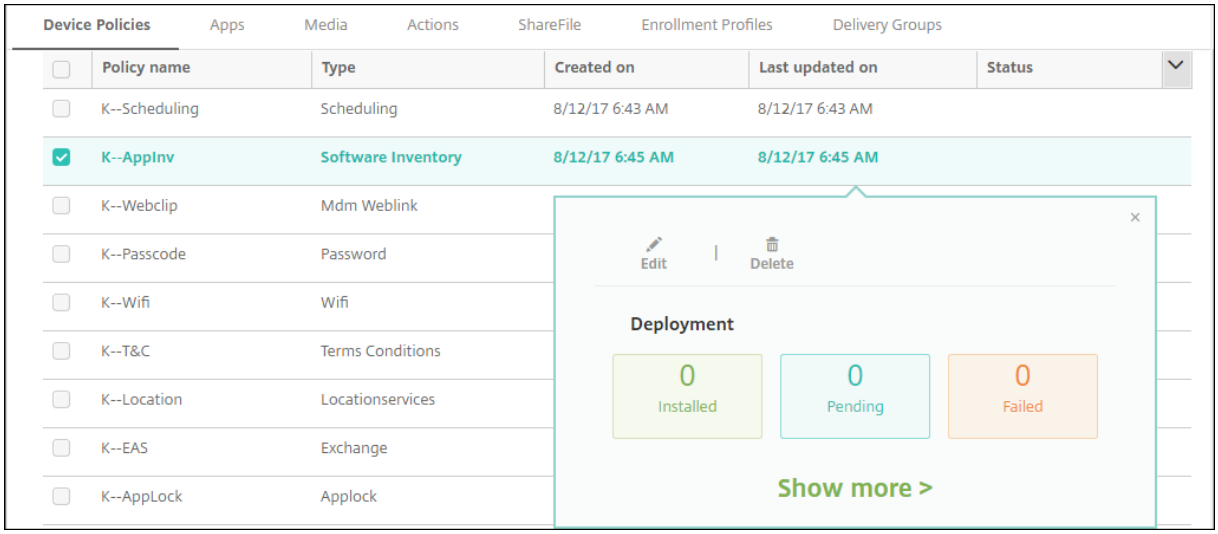
  - Unenroll the device and then push a new set of policies to the device. Users then re-enroll to continue.
  - Push a security action to selectively wipe the specific device. That action removes all corporate apps and data from the device. You then remove the device policy from a delivery group that 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 to show the options menu above the policy list. Or, click a policy in the list to show the options menu to the right of the listing.



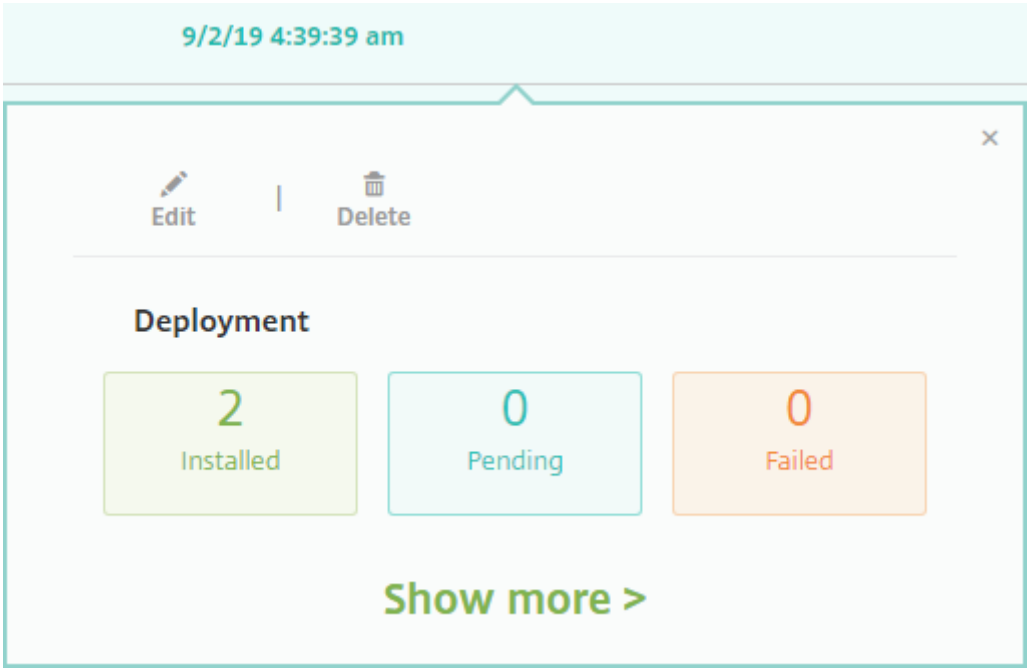
To view policy details, click **Show more**.

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

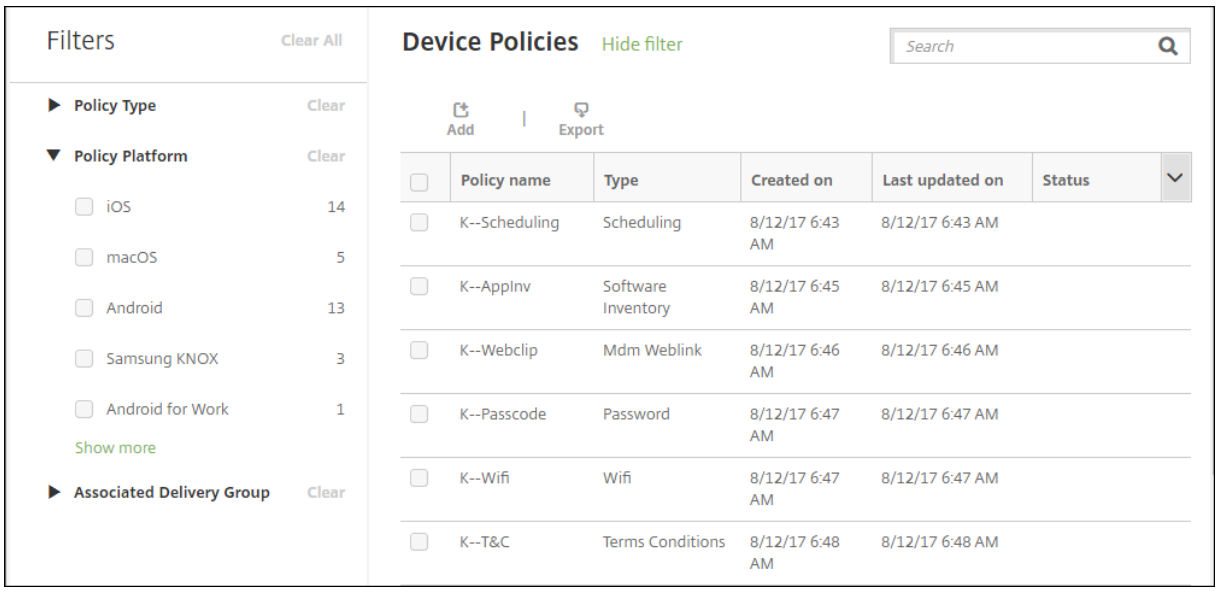
Click a policy row on the **Configure > Device Policies** page to check its deployment status.



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 another Mac computer) to iOS devices. You also have the option of adding 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.
Android Enterprise App Permissions	Configures how requests to Android Enterprise apps within work profiles handle what Google calls “dangerous” permissions.
Android Enterprise App Restrictions	Updates the restrictions associated with Android apps.

Device Policy Name	Device Policy Description
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 plist) to iOS devices. Or, you deploy key/value pairs to Windows 10 phone, desktop, or tablet devices.
App Inventory	Collects an inventory of the apps on managed devices. XenMobile then compares the inventory to any app access policies deployed to those devices. In this way, you can detect apps that are on an app access allow or block list 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.
App 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 XenMobile.

Device Policy Name	Device Policy Description
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 users can install.
App Uninstall	Remove apps from user devices.
App Uninstall Restrictions	Specifies the apps that users can or can't uninstall.
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 devices.
Browser	Defines whether user devices can use the browser or which browser functions the devices can use.
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 Manager	Specifies the connection settings for apps that connect automatically to the internet and to private networks. This policy is only available on Windows Pocket PCs.
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.
Control OS Updates	Deploys the latest OS updates to supported, supervised devices.

Device Policy Name	Device Policy Description
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 XenMobile. For example, with a PKI entity, a keystore, a credential provider, or a server certificate.
Custom XML	Customizes features such as device provisioning, device feature enablement, device configuration, and fault management.
Defender	Configures Windows Defender settings for Windows 10 for desktop and tablet.
Delete Files and Folders	Deletes specific files or folders from Windows Mobile/CE devices.
Delete Registry Keys and Values	Deletes specific registry keys and values from Windows Mobile/CE devices.
Device Health Attestation	Requires that Windows 10 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 XenMobile. When XenMobile 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.

Device Policy Name	Device Policy Description
Enterprise Hub	Distributes apps to Windows Phones through the Enterprise Hub Company store. XenMobile 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 XenMobile Enterprise Edition. You can deploy the initial Enterprise Hub policy only during device enrollment.
Exchange	Enables ActiveSync email for the native email client on the device.
Files	Adds script files to XenMobile 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. XenMobile doesn't support font collections (.TTC or .OTC).
Home screen layout	Specifies the layout of apps and folders for the iOS Home screen on iOS 9.3 and later supervised devices.

Device Policy Name	Device Policy Description
Import iOS & macOS Profile	Imports device configuration XML files for iOS and macOS devices into XenMobile. The file contains device security policies and restrictions that you prepare by using the Apple Configurator.
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.
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 the XenMobile Server. The device then responds with its location coordinates. XenMobile also supports geofencing and tracking policies.

Device Policy Name	Device Policy Description
Mail	Configures an email account on iOS or macOS 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 8 and later supervised devices, you can specify URLs or subdomains to control how users can open documents, attachments, and downloads from the browser.
MDM Options	Manages Find My Phone and iPad Activation Lock on supervised iOS 7.0 and later phone devices.
Organization Info	Specifies organization information for alert messages that XenMobile deploys to iOS devices.
Passcode	Enforces a PIN code or password on a managed device. You can set the complexity and timeouts for the passcode on the device.
Personal Hotspot	Allows users to connect to the internet when they are not in range of a WiFi network. Users connect through the cellular data connection on their iOS device, using personal hotspot functionality.
Profile Removal	Removes the app profile from iOS or macOS devices.
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.

Device Policy Name	Device Policy Description
Proxy	Specifies global HTTP proxy settings for devices running Windows Mobile/CE and iOS. You can deploy only one global HTTP proxy policy per device.
Registry	Defines the registry keys and values that let you administer Windows Mobile/CE devices. The Windows Mobile/CE registry stores data about apps, drivers, user preferences, and configuration settings.
Remote Support	Provides you with remote access to Samsung KNOX devices. Remote Support is no longer available for new customers as of January 1, 2019. Existing customers can continue to use the product, however Citrix won't provide enhancements or fixes.
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 and Windows Mobile/CE 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. XenMobile also supports the Samsung Enterprise Firmware-Over-The-Air (E-FOTA) service. XenMobile supports and extends both Samsung for Enterprise (SAFE) and Samsung KNOX policies.

Device Policy Name	Device Policy Description
Scheduling	Required for Android and Windows Mobile devices to connect back in to the XenMobile Server 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.
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 XenMobile. To do that, create a PKI entity and a PKI provider in distributed mode.
SSO Account	Creates single sign-on (SSO) accounts so users sign on one-time only to access XenMobile and your internal company resources. Users do not need to store any credentials on the device. XenMobile 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.
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 XenMobile, they must accept the terms and conditions to enroll their devices. Declining the terms and conditions cancels the enrollment process.

Device Policy Name	Device Policy Description
Tunnel	Used only for Remote Support. Remote support enables your help desk representatives to take remote control of managed Windows CE and Android mobile devices. Remote support isn't available for clustered on-premises XenMobile Server deployments. Remote Support is no longer available for new customers as of January 1, 2019. Existing customers can continue to use the product, however Citrix won't provide enhancements or fixes.
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. XenMobile 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 wallpaper on an iOS device lock screen, home screen, or both. To use different wallpaper on iPads and iPhones, create different wallpaper policies and deploy them to the appropriate users.
Web Content Filter	Filters web content on iOS devices. XenMobile uses the Apple auto-filter function and the sites that you add to allow and blocklists. Available only for iOS supervised devices.
Webclip	Places shortcuts, or webclips, to websites so that they appear alongside apps on user devices. You can specify your own icons to represent the webclips for iOS, macOS, and Android devices. Windows tablet only requires a label and a URL.

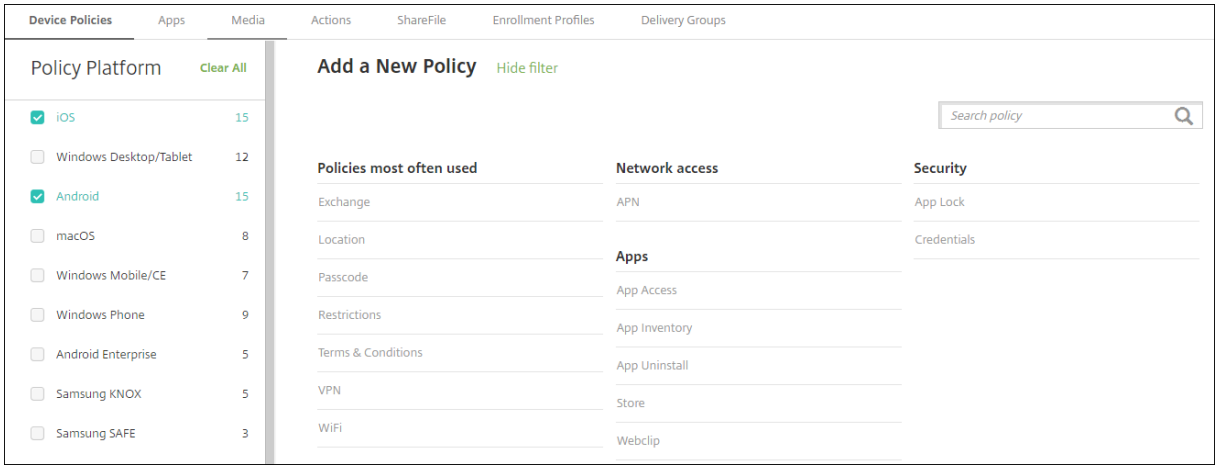
Device Policy Name	Device Policy Description
WiFi	Allows administrators to deploy WiFi router details to managed devices. The router details include SSID, authentication data, and configuration data.
Windows CE Certificate	Creates and delivers Windows Mobile/CE certificates from an external PKI to user devices.
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 version 1607 and later supervised devices.
XenMobile Store	Specifies whether a XenMobile Store webclip appears on the home screen of user devices.
XenMobile Options	Configures the Secure Hub behavior when connecting to XenMobile from Android and Windows Mobile/CE devices.
XenMobile Uninstall	Uninstalls XenMobile from Android and Window Mobile/CE devices. When deployed, this policy removes XenMobile from all devices in the deployment group.

Device policies by platform

January 6, 2021

To view the policies that are available per platform:

1. In the XenMobile 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.



The latest release of XenMobile supports device policies for the following platforms:

- Amazon
- Android
- Android Enterprise
- Android Zebra
- Chrome OS
- iOS
- macOS
- Samsung SAFE
- Samsung KNOX
- Windows 10 Desktop/Tablet
- Windows 10 Phone
- Windows Mobile/CE

For details on supported devices in the latest release of XenMobile, see Supported device platforms.

> **Note:**
>
> If your environment is configured with Group Policy Objects (GPOs):
>
> When you configure XenMobile device policies for Windows 10, keep the following rule in mind. If a policy on one or more enrolled Windows 10 devices conflicts, the policy aligned with the GPO takes precedence.

AirPlay mirroring device policy

April 20, 2021

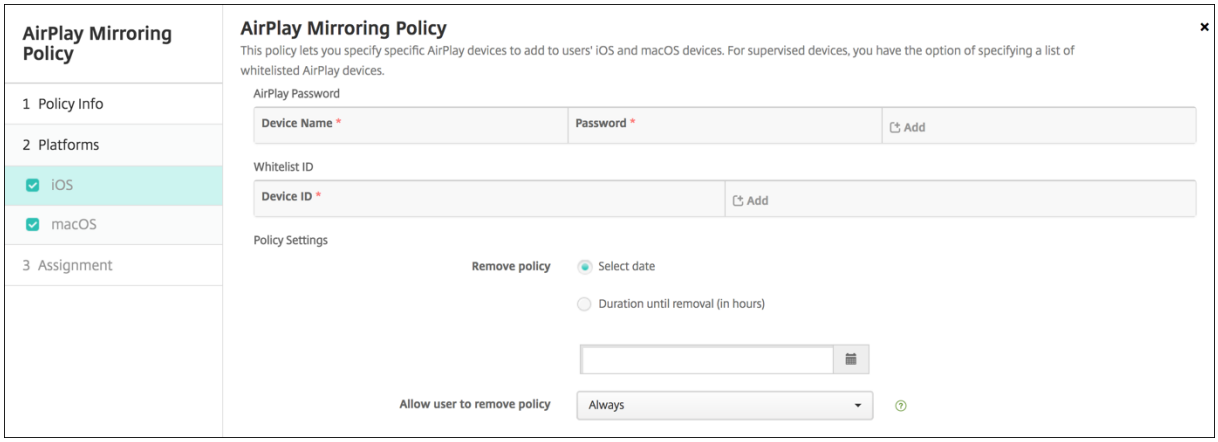
The Apple AirPlay feature allows users to mirror exactly what's on a device display to another Mac computer.

You can add a device policy in XenMobile to add specific AirPlay devices (such as 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 the AirPlay devices on the allow list. For information about placing a device into Supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator.

> **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



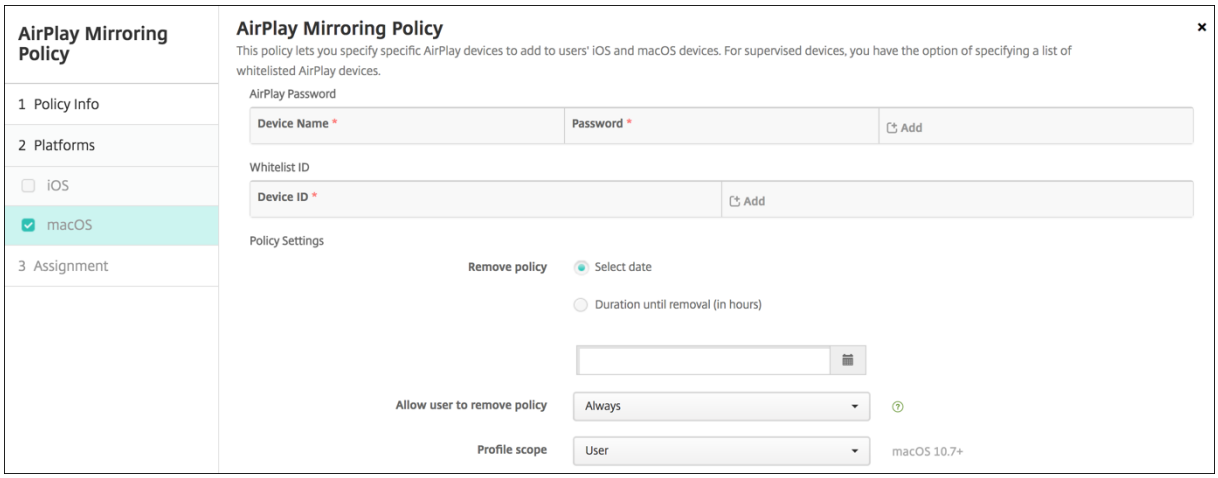
- **AirPlay Password:** For each device you want to add, click **Add** and then do the following:
  - **Device ID:** Enter the hardware address (Mac address) in xx:xx:xx:xx:xx:xx format. This field is not case-sensitive.
  - **Password:** Enter an optional password for the device.
  - Click **Add** to add the device or click **Cancel** to cancel adding the device.
- **Whitelist 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:

  > **Note:**
  >
  > The XenMobile Server console includes the terms "blacklist" and "whitelist". We are changing those terms in an upcoming release to "block list" and "allow list".

  - **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 ID:** 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.
- **Whitelist ID:** This list is ignored for unsupervised devices. The device IDs in this list are the only AirPlay devices available to user 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 26, 2020

You can add a device policy in XenMobile to add 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.

This policy applies to iOS 7.0 and later.

> **Note:**
>
> Be sure to have 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.
  - Click **Save** to add the printer or click **Cancel** to cancel adding the printer.
- **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.

Android Enterprise managed configurations policy

May 12, 2021

The Android Enterprise managed configurations device policy controls various app configuration options and app restrictions. The app developer defines the options and tooltips available for an app. If a tooltip mentions using a "templated value," use the corresponding XenMobile 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:

- App email 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 XenMobile. For more information, see Adding Apps to XenMobile.

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 Android Enterprise managed configurations 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

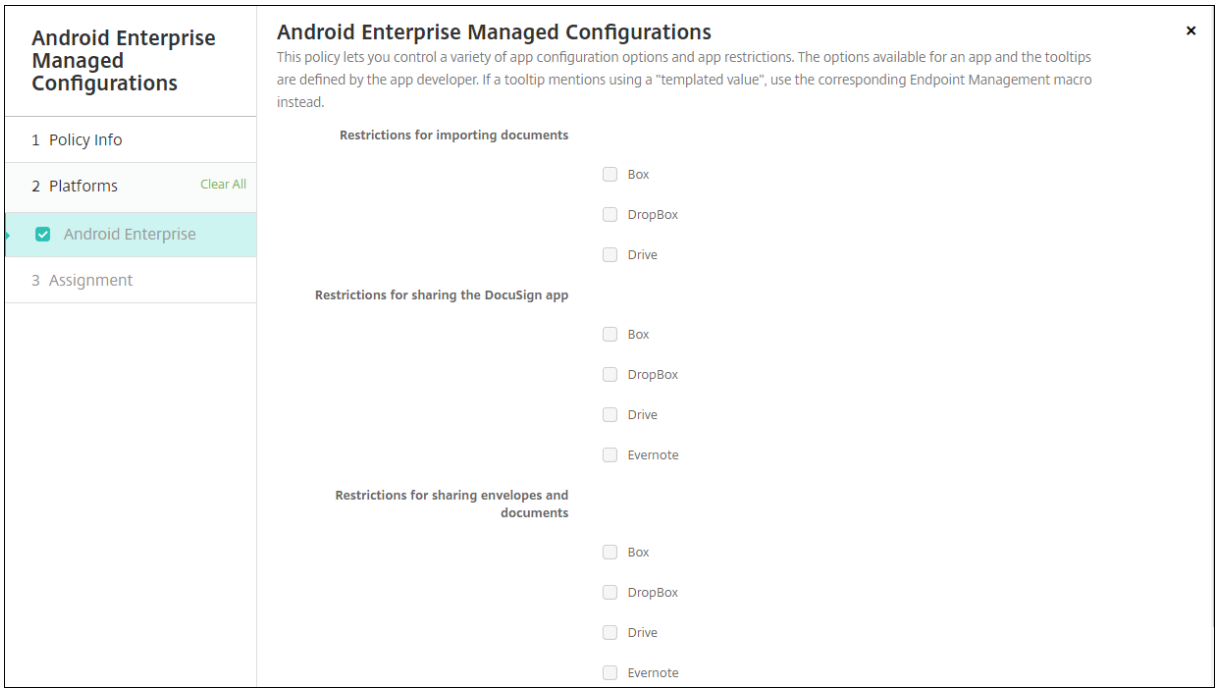
A general workflow to configure a per-app VPN for AE devices is as follows:

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 an Android Enterprise managed configurations device policy, a prompt to select an app appears. If there are no Android Enterprise apps added to XenMobile, you cannot proceed.

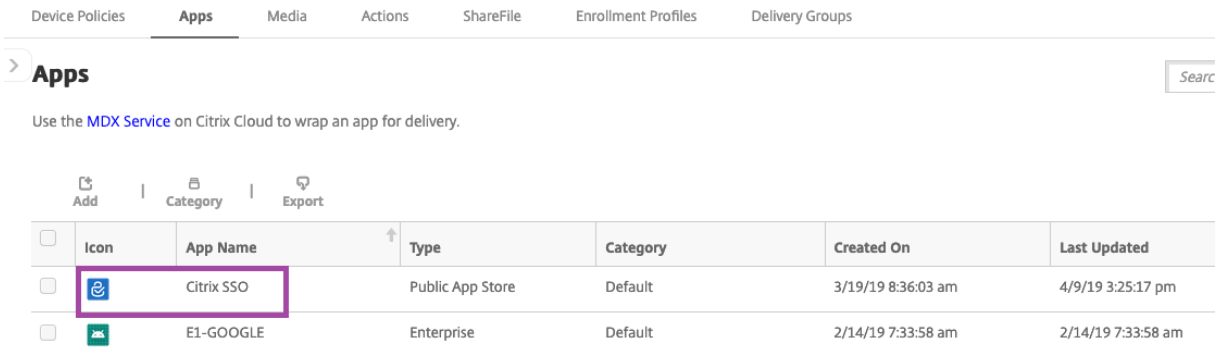
After you select an app, then configure the policy settings. The settings are specific to each app.



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 XenMobile console as a Google Play store app. See Add a public app store app.

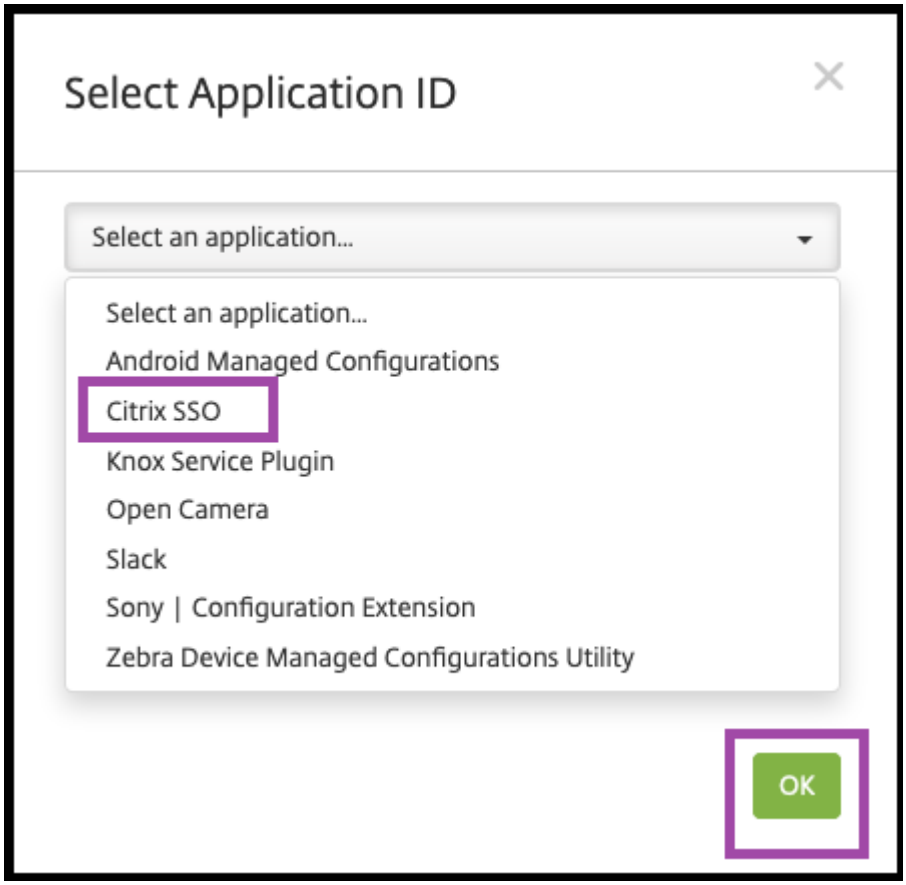


Create an Android Enterprise managed configuration for Citrix SSO

Configure the Android Enterprise managed configurations device policy for Citrix SSO to create VPN profiles. Devices that have the Citrix SSO app installed and the policy deployed have access to the VPN profiles you create.

You need your Citrix Gateway FQDN and port.

1. In the XenMobile console, click **Configure > Device Policies**. Click **Add**.
2. Select **Android Enterprise**. Click **Android Enterprise 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**.

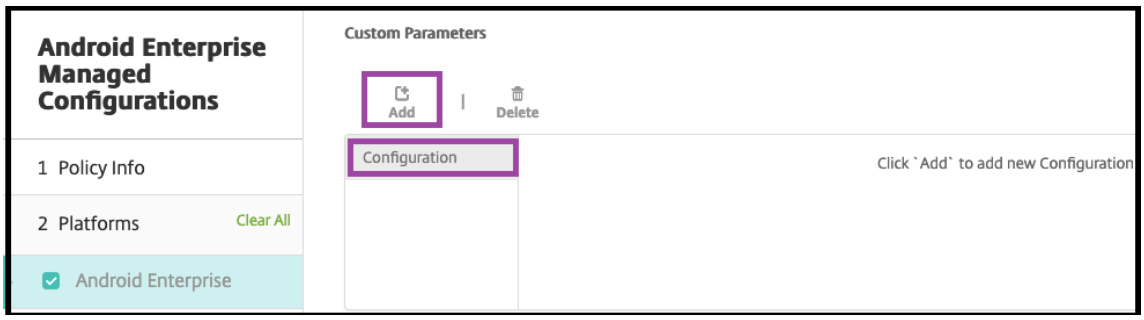
5. Configure VPN profile parameters.

   - **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 XenMobile 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 the 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 the 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**.

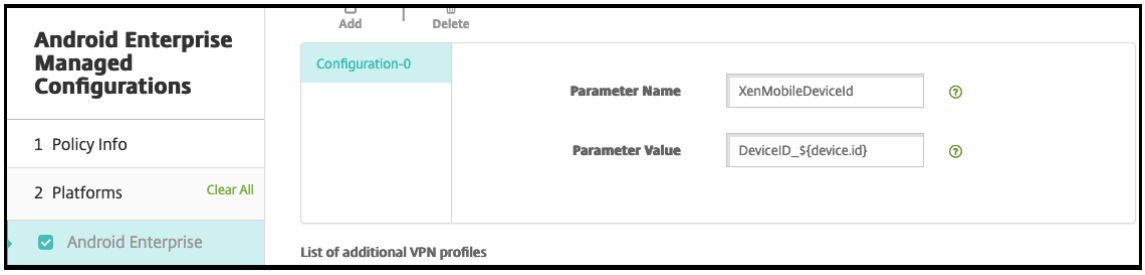
- **PerAppVPN app list.** A list of apps whose traffic is allowed or blocked on the VPN, depending on the value of **Per-App VPN Type**. List the app package names separated by commas or semicolons. App package names are case sensitive and must appear on this list exactly as they appear in the Google 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 user interface of the Citrix SSO app instead of tapping 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 when using a self-signed certificate for Citrix Gateway or 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:

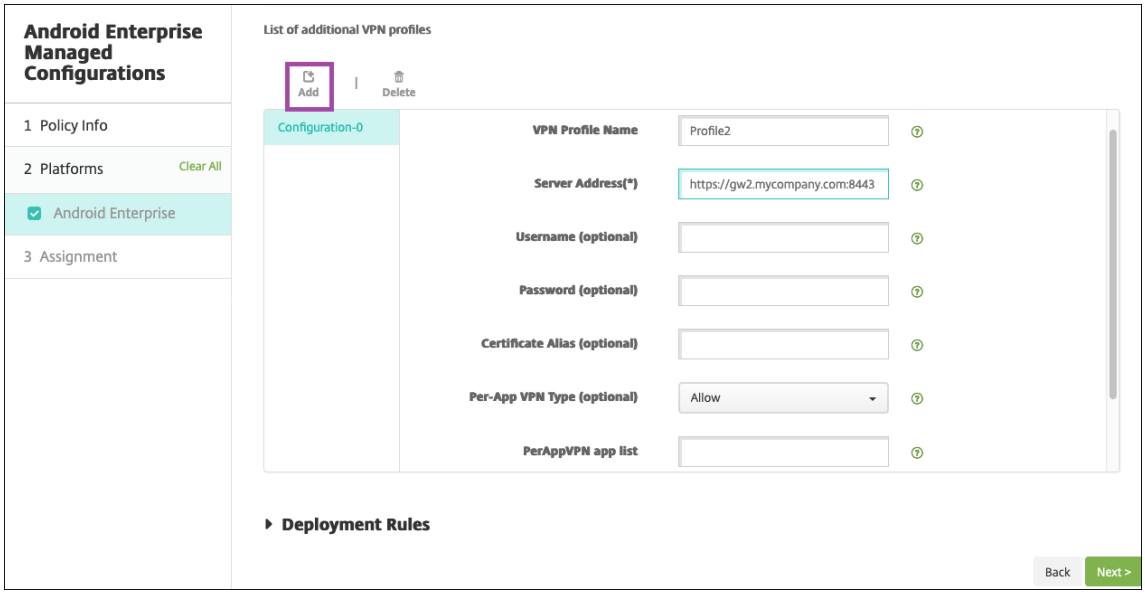
- **Parameter name.** Type **XenMobileDeviceId**. This field is the device ID to use for Network Access Check based on device enrollment in XenMobile. If XenMobile enrolls and manages the device, the VPN connection is allowed. Otherwise, authentication is denied at the time of VPN establishment.
- **Parameter value** For XenMobile 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.



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.

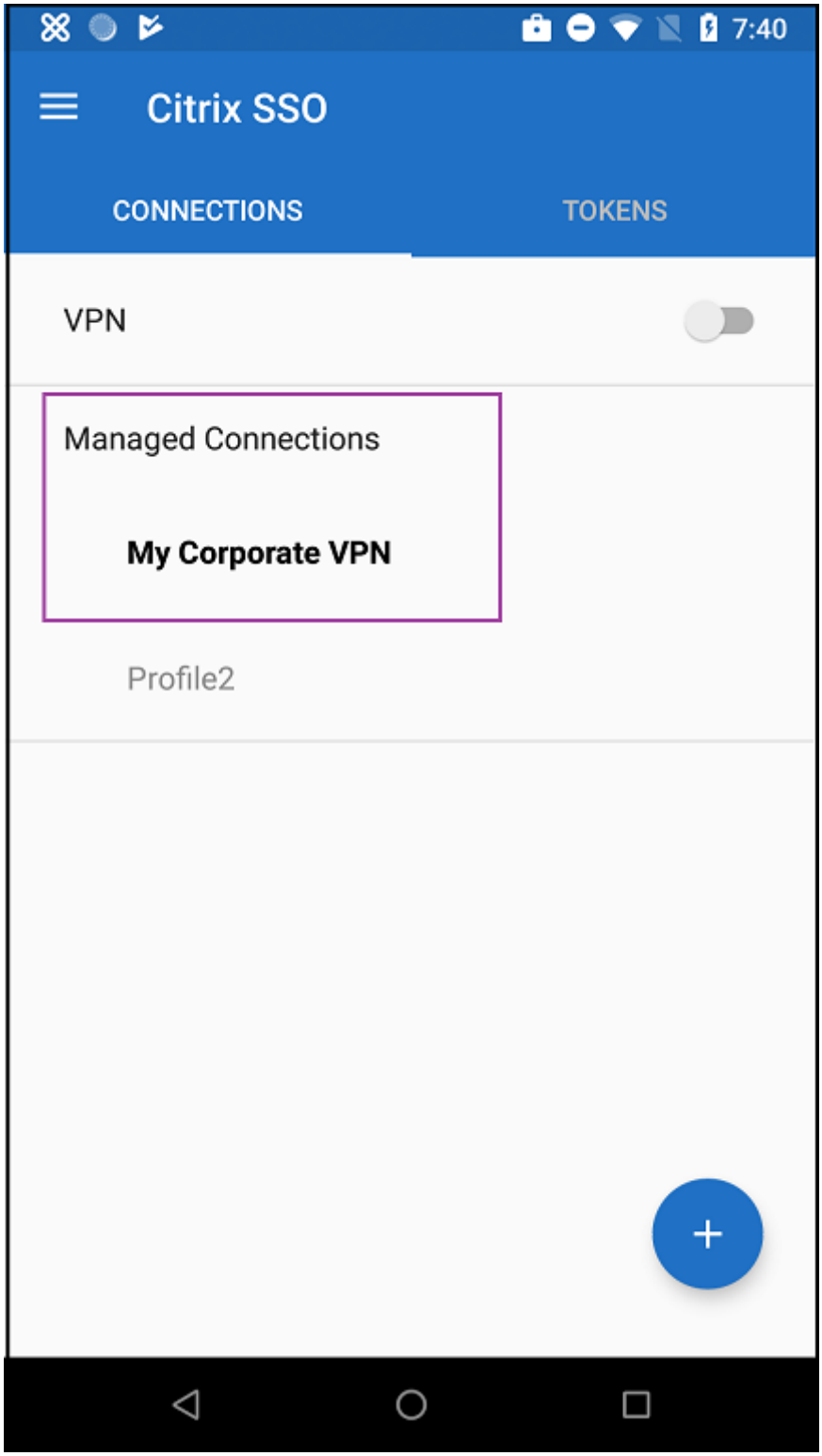
To enable always-on for the VPN profiles you configured, set the XenMobile options device policy.

> **Note:**
> Citrix Secure Hub 19.5.5 or higher is required for always-on VPN for Android Enterprise.

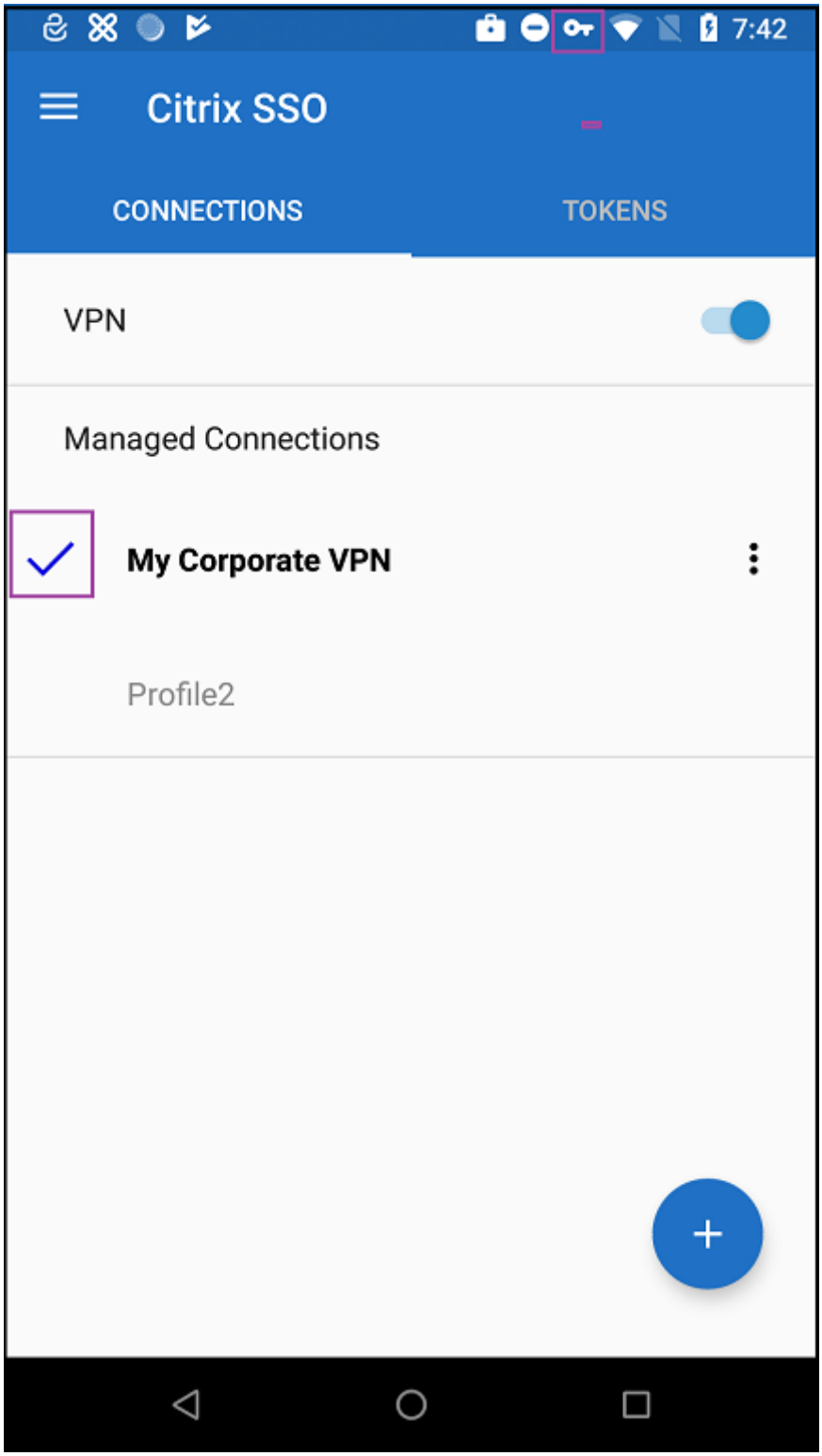
Accessing VPN profiles from the device

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.

XenMobile 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.

Start by adding the Zebra OEMConfig app to the XenMobile console 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 Android Enterprise 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 XenMobile console, click **Configure > Device Policies**. Click **Add**.
2. Select **Android Enterprise**. Click **Android Enterprise 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** for 12-hour format or **24** for 24-hours format.

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**.

Android Enterprise app permissions

September 21, 2020

You can configure how requests to Android Enterprise apps, that are within work profiles, 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.

Google defines dangerous permissions as permissions that give the app access to data or resources that involve the user’s private information or could potentially affect the user’s stored data or the operation of other apps. For example, the ability to read the user’s contacts is a dangerous permission.

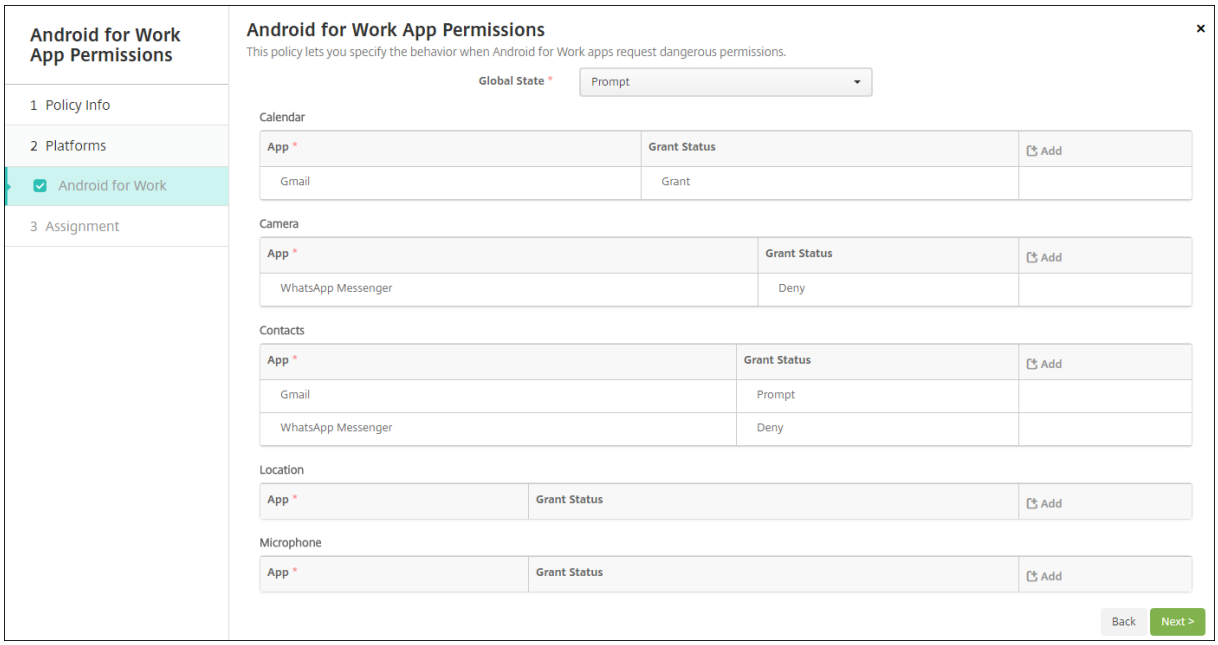
You can configure a global state that controls the behavior of all dangerous permission requests to Android Enterprise apps within work profiles. You can also control the behavior of dangerous permission request for individual permission groups, as defined by Google, for each app. These individual settings override the global state.

For information on how Google defines permission groups, see “Permission groups” in this Android developers guide.

By default, users are prompted to grant of deny dangerous permission requests.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Android Enterprise settings



- **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 configure Android Enterprise system apps, click **Add new** and enter the application package name you enabled in the Restrictions device policy. Under Grant State, choose **Prompt**, **Grant,**, or **Deny**. This grant state overrides the global state.
  - **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 state.
- To add more apps for the permission group, click **Add** again and repeat these steps.
- When you have finished setting grant states for all permission groups you want to, click **Next**.

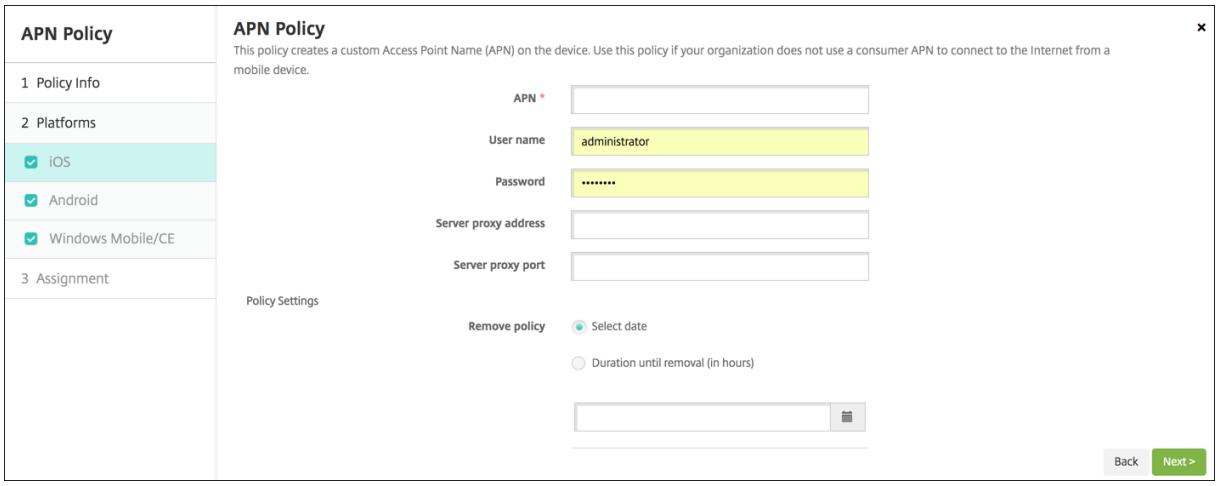
APN device policy

March 26, 2020

You can add a custom Access Point Name (APN) device policy for iOS, Android, and Windows Mobile/CE 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.

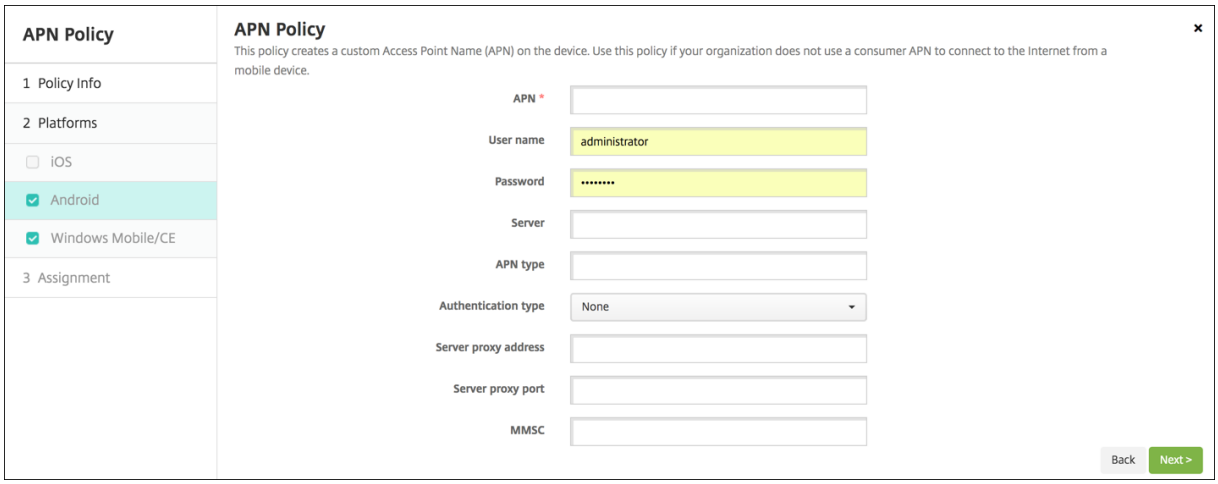
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **APN:** Type the name of the access point. This must match an accepted iOS APN or the policy will fail.
- **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. This 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)**.
  - If you click **Select date**, click the calendar to select the specific date for removal.
  - In the **Allow user to remove policy list**, click **Always**, **Password required**, or **Never**.
  - If you click **Password required**, next to **Removal password**, type the necessary 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 and later.

Android settings

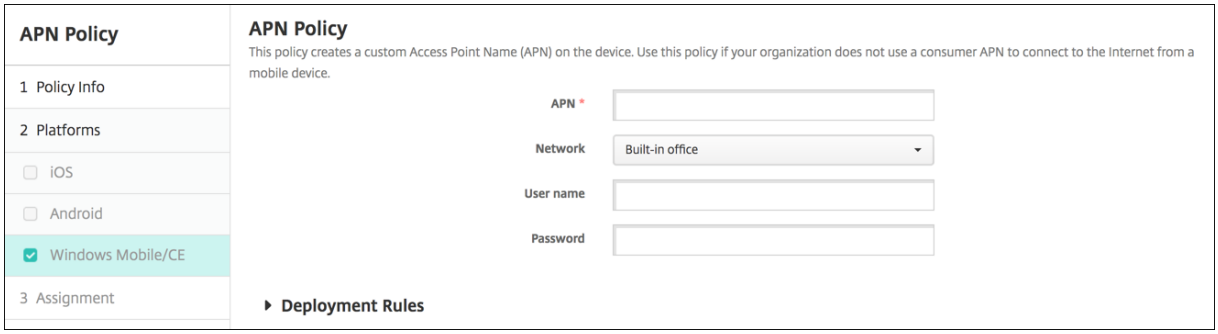


- **APN:** Type the name of the access point. This must match an accepted Android APN or the policy will fail.
- **User name:** This string specifies the user name for this APN. If the user name is missing, the device prompts for the string during profile installation.
- **Password:** The password for 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 could not 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 should rarely be 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. This 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:** This is the multimedia messaging ser-

vice 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.

Windows Mobile/CE settings



- **APN:** Type the name of the access point. This must match an accepted Android APN or the policy will fail.
- **Network:** In the list, click the type of network to use. The default is **Built-in office**.
- **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.

App access device policy

July 3, 2018

The app access device policy in XenMobile allows you to define a list of apps that are either required to be installed on the device, can be installed on the device, or must not be installed on the device. You can then create an automated action to react to the device compliance with that list of apps. You can create app access policies for iOS, Android, and Windows Mobile/CE devices.

You can only configure one type of access policy at a time. You can add a policy for either 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, we recommend that you name each policy carefully, so you know which policy in XenMobile applies to which list of apps.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Platform settings

- **Access policy:** Click **Required**, **Suggested**, or **Forbidden**. The default is **Required**.
- To add one or more apps to the list, click **Add** and then do the following:
  - **App name:** Enter an app name.
  - **App Identifier:** Enter an optional app identifier.
  - Click **Save** or **Cancel**.
  - Repeat these steps for each app you want to add.

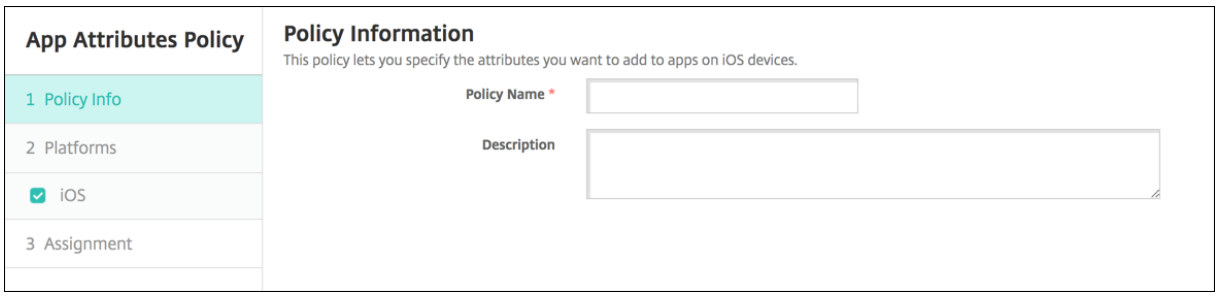
App attributes device policy

July 3, 2018

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

July 3, 2018

You can remotely configure apps that support managed configuration by deploying:

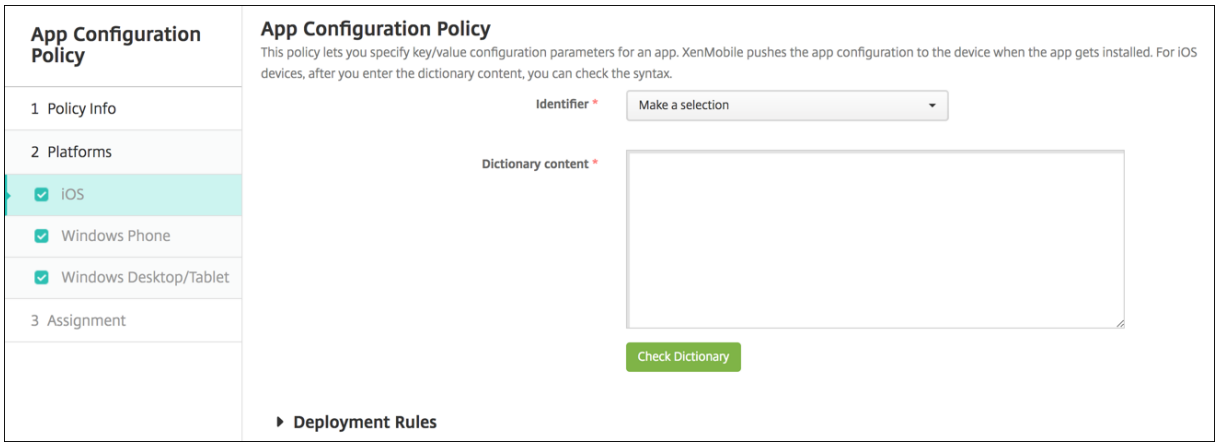
- An XML configuration file (called a property list, or plist) to iOS devices

- Or, key/value pairs for Windows 10 phone, tablet, or desktop devices.

The configuration specifies various settings and behaviors in the app. XenMobile 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.

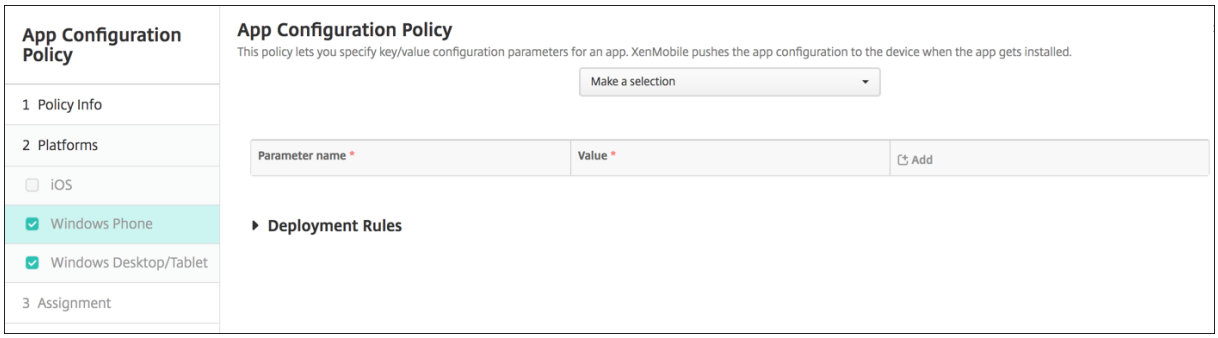
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

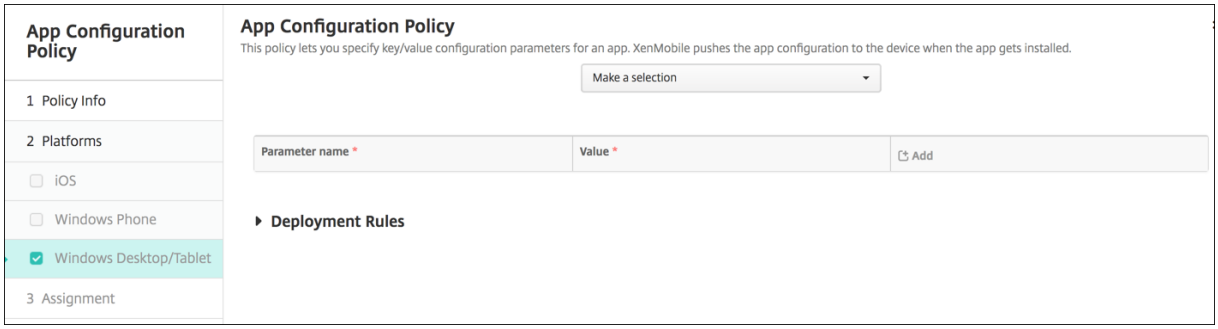
iOS settings



- **Identifier:** In the list, click the app you want to configure or click **Add new** to add a new 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**. XenMobile 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 or Desktop/Tablet settings





- In the **Make a selection** list, click the app you want to configure or click **Add new** to add a new 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.

App inventory device policy

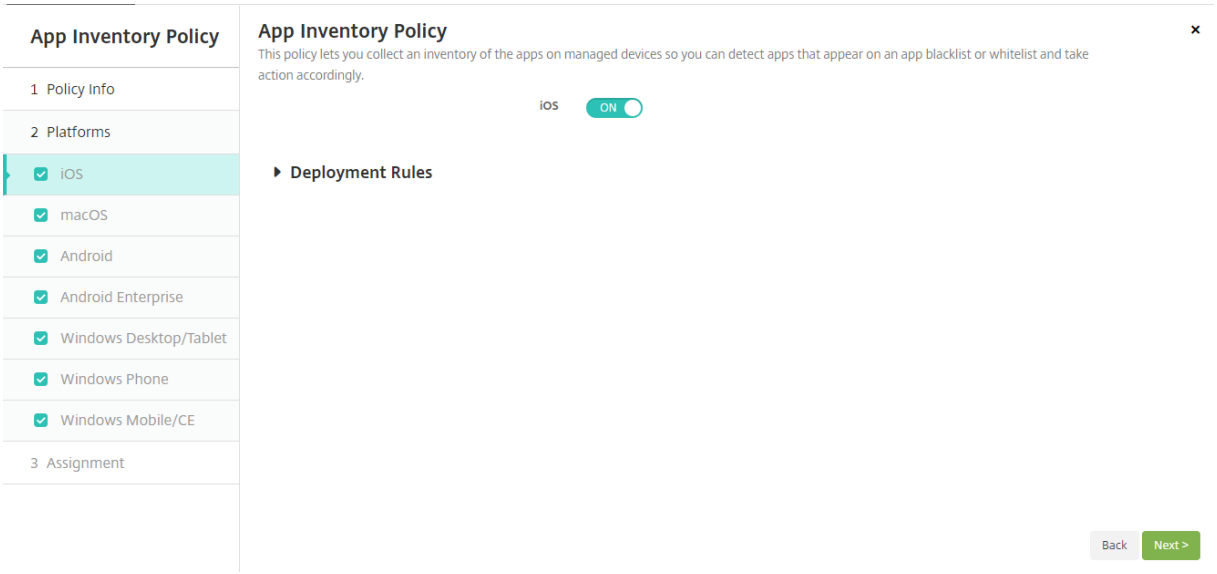
June 19, 2020

The App inventory policy lets you collect an inventory of the apps on managed devices. XenMobile 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.

You can create app access policies for iOS, macOS, Android, Android Enterprise, Windows Desktop/Tablet, Windows phone, or Windows Mobile/CE devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Platform settings



- For each platform you select, leave the default setting or change the setting to **Off**. The default is **On**.

App lock device policy

June 19, 2020

The App lock device policy defines a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device. You can configure this policy for both iOS and Android devices, but the exact way the policy works differs for each platform. For example, you cannot block multiple apps on an iOS device.

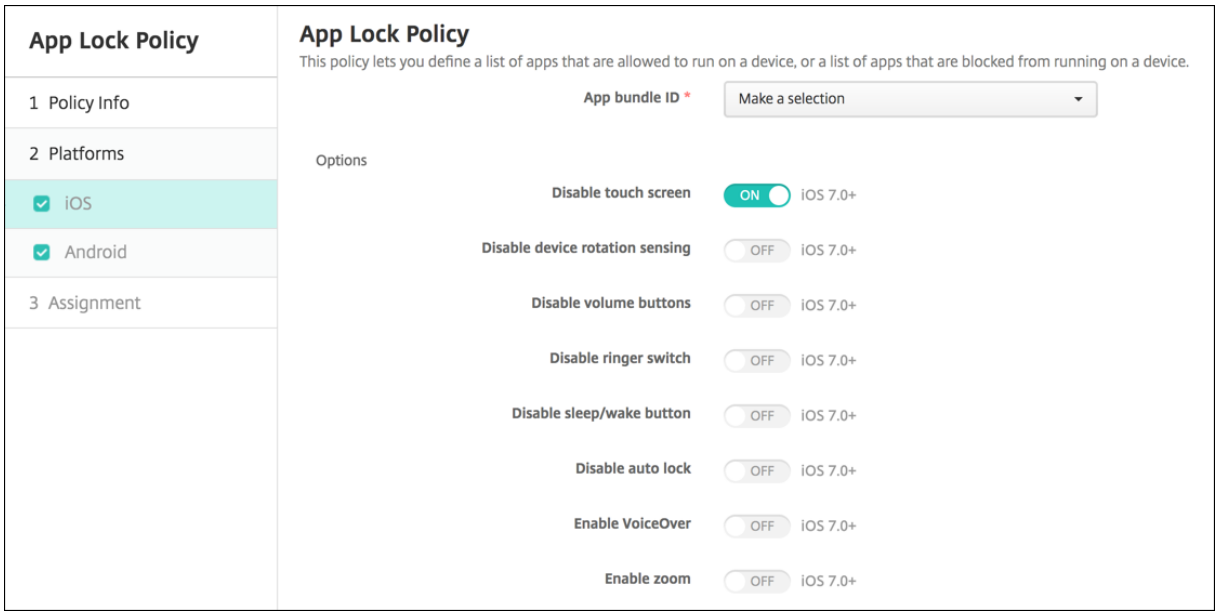
Likewise, for iOS devices, you can select only one iOS app per policy. This means that users are only able to use their device to run a single app. They cannot do any other activities on the device except for the options you specifically allow when the app lock policy is enforced.

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 does not function on Android N or later devices because Google deprecated the required API.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



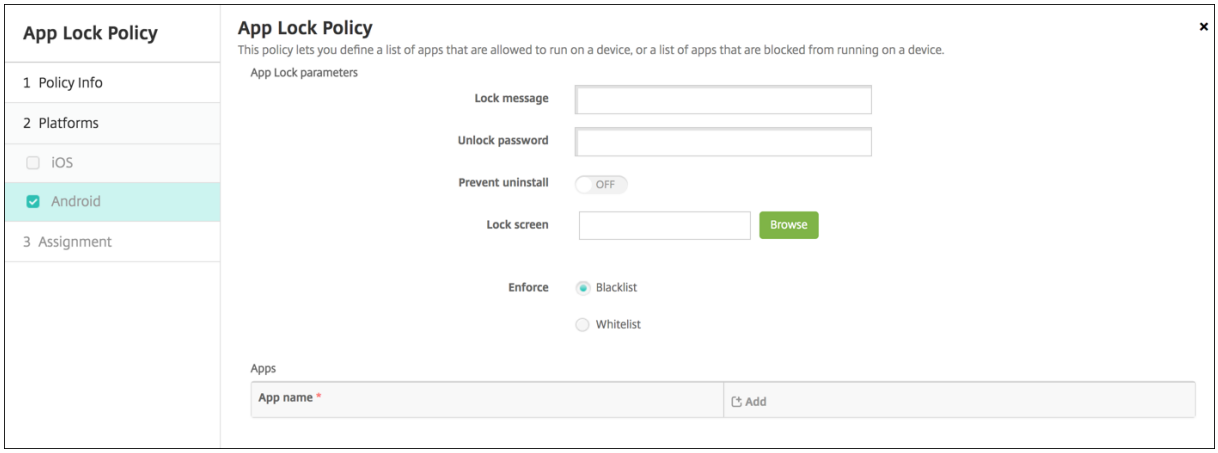
- **App bundle ID:** In the list, click the app to which this policy applies or click **Add new** to add a new app to the list. If you select **Add new**, type the app name in the field that appears.
- **Options:** Each of the following options applies only to iOS 7.0 or later. For each option, the default 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
- **User Enabled Options:** Each of the following options applies only to iOS 7.0 or later. For each option, the default is **Off**.
  - Allow VoiceOver adjustment
  - Allow zoom adjustment
  - Allow invert colors adjustment

  - Allow AssitiveTouch 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 and later.

Android settings

> **Note:**
>
> You can't block the Android Settings app by using the App Lock device policy.



- **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 either **Blacklist** to create a list of apps that are not allowed to run on devices or click **Whitelist** to create a list of apps that are allowed to run on devices.

    > **Note:**
    >
    > The XenMobile Server console includes the terms "blacklist" and "whitelist". We are changing those terms in an upcoming release to "block list" and "allow list".
- **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 lists, or click **Add new** to add a new 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 lists.

App network usage device policy

July 3, 2018

You can set 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 those that you deploy to users' devices through XenMobile. They do not include apps that users have downloaded directly to their devices without being deployed through XenMobile or those already installed on the devices when the devices were enrolled in XenMobile.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **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 do the following:
  - **App Identifier:** Enter an app identifier.
  - Click **Save** to save the app to the list or **Cancel** to not save the app to the list.

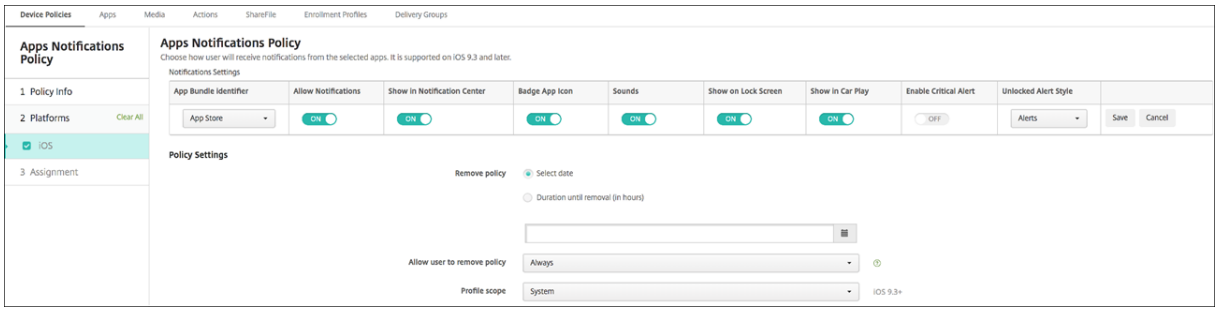
Apps notifications device policy

March 26, 2020

The Apps notifications policy lets you control how iOS users receive notifications from specified apps. This policy is supported on devices running iOS 9.3 or later.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **App Bundle identifier:** Specify the apps you want to apply this policy to.
- **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 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.

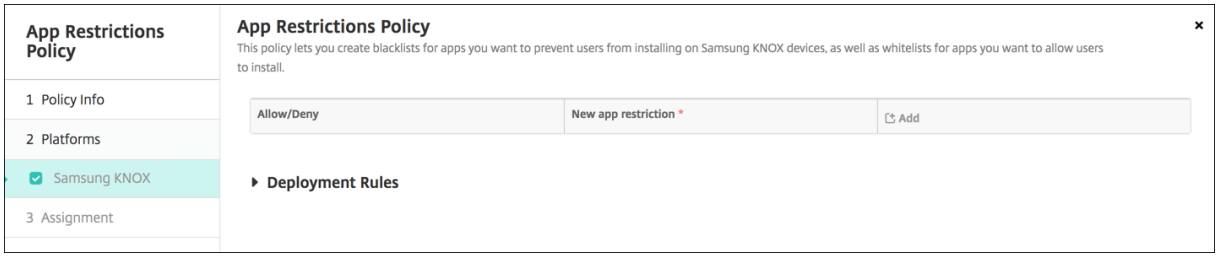
App restrictions device policy

June 19, 2020

You can create block lists for the apps you want to prevent users from installing on Samsung KNOX devices. You can also create allow lists for the apps you want to allow users to install.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Samsung KNOX settings



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.
- **New app restriction:** 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.

App tunneling device policy

June 25, 2019

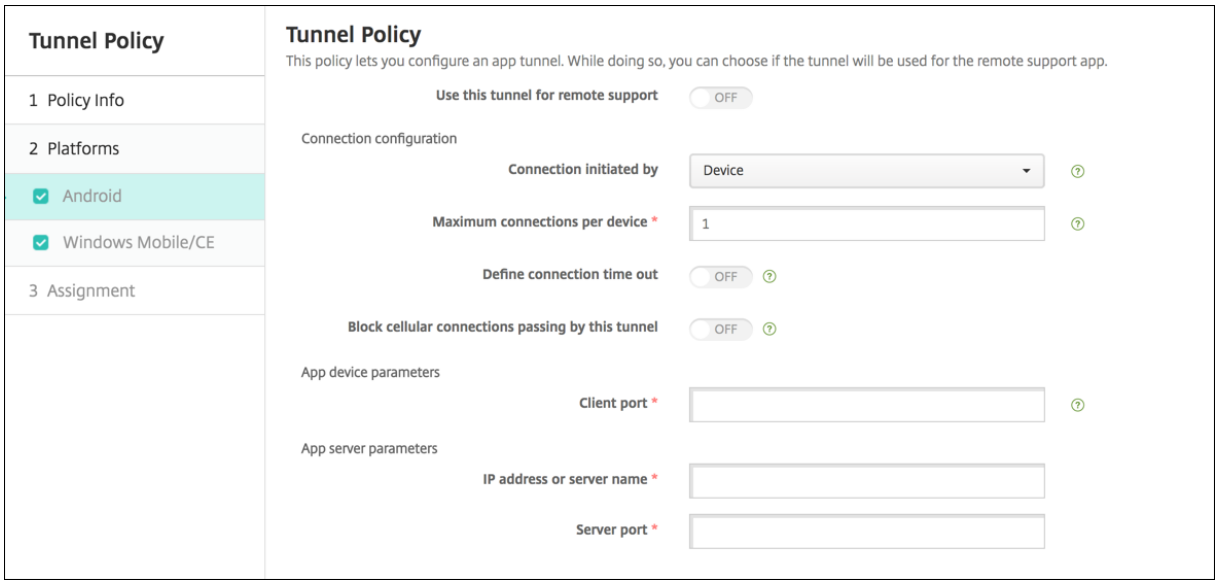
> **Important:**
>
> The App tunneling policy is used only for Remote Support. For information about Remote Support, see Support options and Remote Support. Remote Support is no longer available for new customers as of January 1, 2019. Existing customers can continue to use the product, however Citrix won't provide enhancements or fixes.

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 also use app tunnels to create remote support tunnels to a device for management support. You can configure the app tunneling policy for Android and Windows Mobile/CE devices.

Any app traffic sent through a tunnel that you define in this policy goes through XenMobile 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



- **Use this tunnel for remote support:** Select whether the tunnel will be used for remote support.

  The configuration steps are different depending on whether you select remote support.

- If you do not select remote support, do the following:
  - **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.

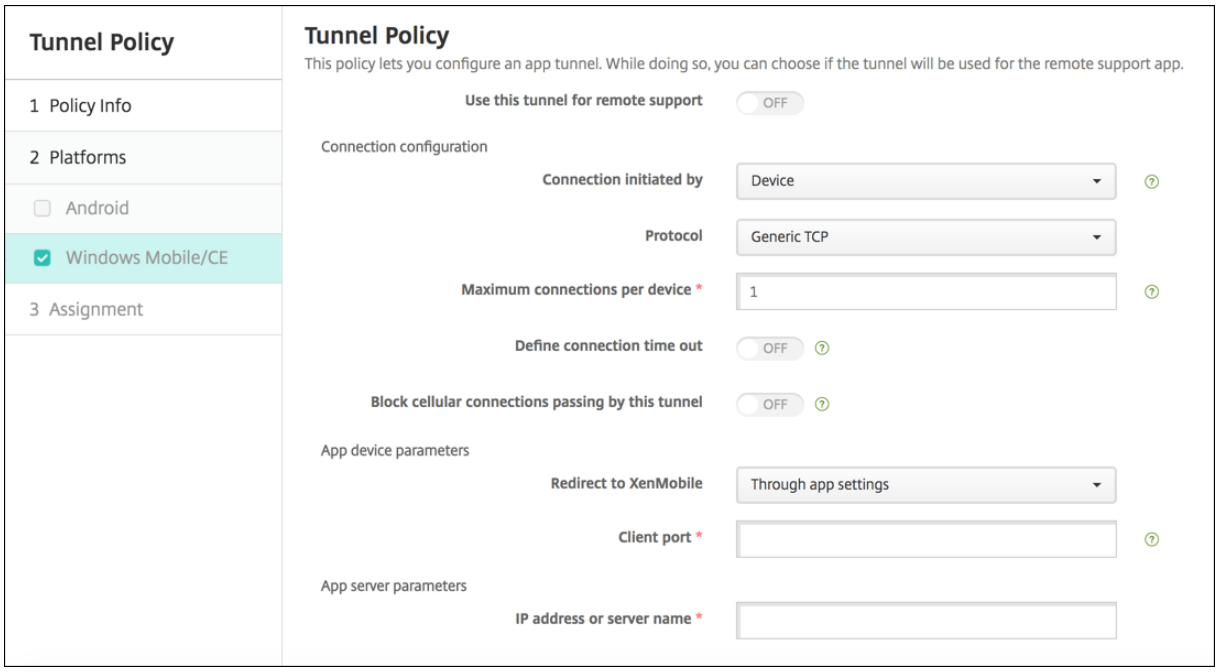
    > **Note:**
    >
    > WiFi and USB connections will not be blocked.

  - **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.

- If you do select remote support, do the following:
  - **Use this tunnel for remote support:** Set to **On**.
  - **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.
  - **Use SSL connection:** Select whether to use a secure SSL connection for this tunnel.
  - **Block cellular connections passing by this tunnel:** Select whether this tunnel is blocked while roaming. This setting doesn't block WiFi and USB connections.

Windows Mobile/CE settings



- **Use this tunnel for remote support:** Select whether the tunnel will be used for remote support.

The configuration steps are different depending on whether you select remote support.

- If you do not select remote support, do the following:
  - **Connection initiated by:** Click **Device** or **Server** to specify the source initiating the connection.
  - **Protocol:** In the list, click the protocol to use. The default is **Generic TCP**.

  - **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.

    > **Note:**
    > WiFi and USB connections will not be blocked.

  - **Redirect to XenMobile:** In the list, click how the device connects to XenMobile. The default is **Through app settings**.
    * If you select **Using a local alias**, type the alias in **Local alias**. The default is **localhost**.
    * If you select **An IP address range**, type the from IP address in **IP address range from** and type the to IP address in **IP address** range to.
  - **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.
- If you do select remote support, do the following:
  - **Use this tunnel for remote support:** Set to **On**.
  - **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.
  - **Use SSL connection:** Select whether to use a secure SSL connection for this tunnel.
  - **Block cellular connections passing by this tunnel:** Select whether this tunnel is blocked while roaming. WiFi and USB connections aren't blocked.

App uninstall device policy

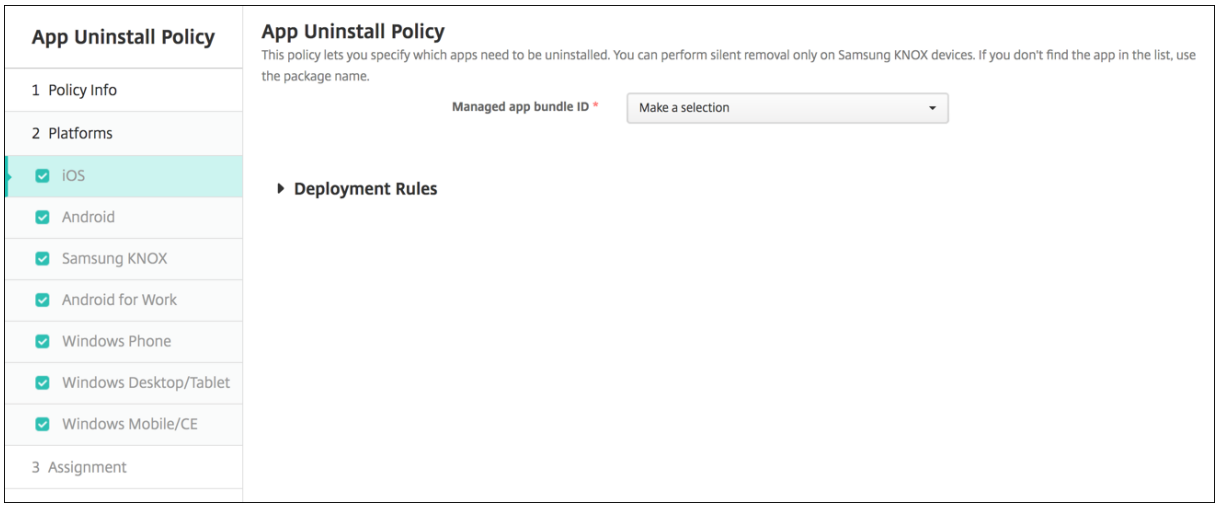
April 8, 2019

You can create an app uninstall policy for iOS, Android, Samsung KNOX, Android Enterprise, Windows Desktop/Tablet, and Windows Mobile/CE platforms. An app uninstall policy lets you remove apps from user devices for any number of reasons. It may be that you no longer want to support certain apps, your company may want to replace existing apps with similar apps from different vendors, and so on.

The apps are removed when this policy is deployed to user devices. With the exception of Samsung KNOX devices, users receive a prompt to uninstall the app. Samsung KNOX device users do not receive a prompt to uninstall the app.

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 existing app or click **Add new**. If there are no apps configured for this platform, the list will be empty and you must add a new app.
  - When you click **Add**, a field appears where you can type an app name.

All other platform 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 will be empty and you must add new apps.
  - Click **Add** to add the app or click **Cancel** to cancel adding the app.

Automatically uninstall an Enterprise app after the corresponding public app store app installs

You can configure XenMobile 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 XenMobile to remove older apps from user devices upon installation of the new version. This feature is available only for managed iOS devices connected to a XenMobile 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, XenMobile removes the Enterprise version (com.citrix.mail).

App uninstall restrictions device policy

July 3, 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

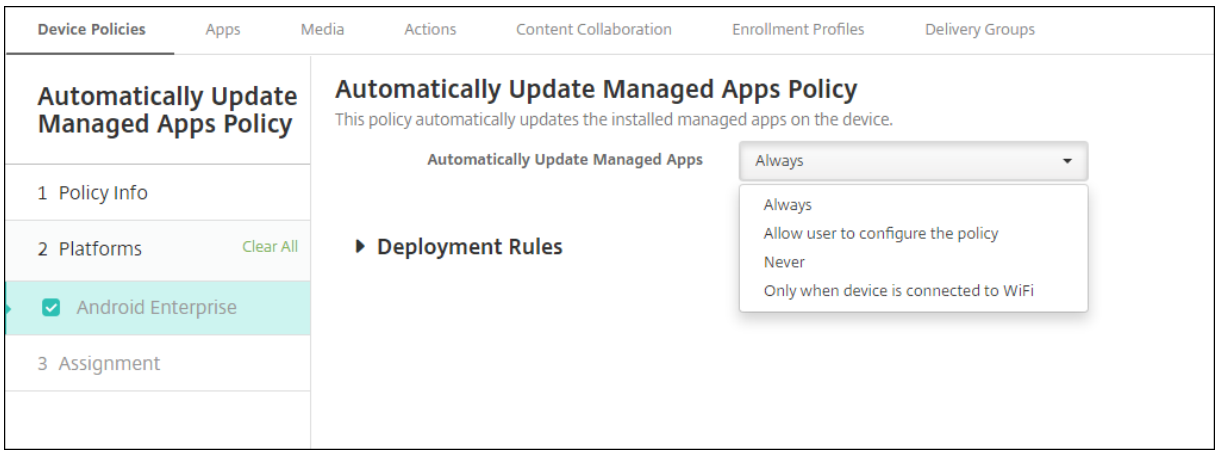
- **App Uninstall Restrictions Settings:** For each app rule you want to adds, click **Add** and then do the following:
  - **App Name:** In the list, click an app or **Add new** to add a new app.
  - **Rule:** Select whether users can uninstall the app. The default is to allow uninstallation.
  - Click **Save** or **Cancel**.

Automatically update managed apps device policy

December 16, 2020

This policy controls how installed managed apps are updated on Android Enterprise 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

October 4, 2019

Windows 10 includes 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 XenMobile to configure the settings available in the BitLocker wizard on Windows 10 devices. For example, on a device with BitLocker enabled, BitLocker can prompt users for how they want to unlock their drive at startup, how to back up their recovery key, and 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.

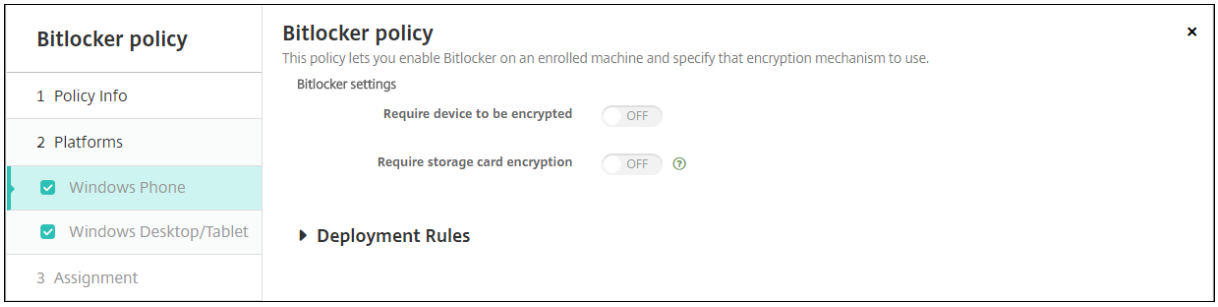
> **Note:**
>
> After BitLocker encryption starts on a device, you can't subsequently change the BitLocker settings on the device by deploying an updated BitLocker device policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Requirements

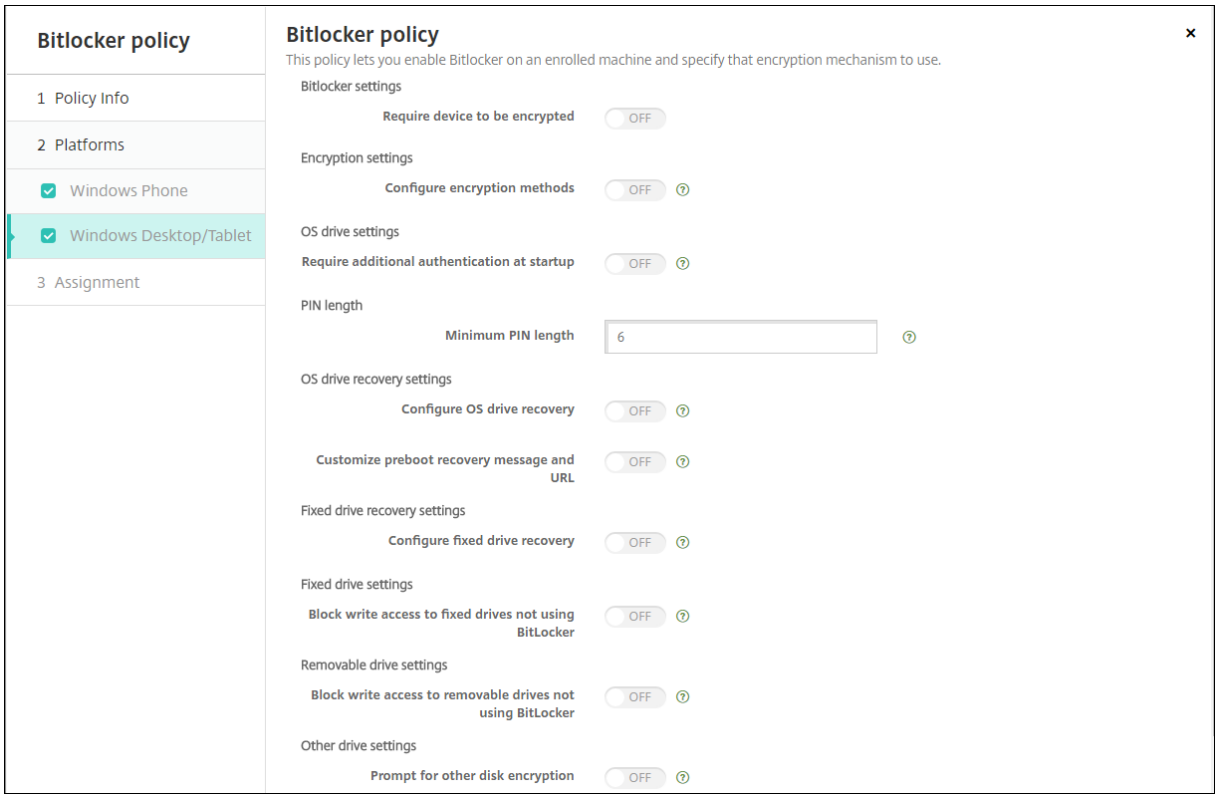
- The BitLocker device policy requires Windows 10 Enterprise edition.
- Before deploying the BitLocker device policy, prepare your environment for BitLocker use. For detailed information from Microsoft, including BitLocker system requirements and setup, see BitLocker and the articles under that node.

Windows Phone settings



- **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



- **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**.
- **Configure encryption methods:** Determines the encryption methods to use for specific drive types. If **Off**, the BitLocker wizard prompts the 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**.
- **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 TPM chip:** On a device with no TPM chip, BitLocker requires users to create a 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 additional 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. If the unlock fails, the device enters recovery mode.

- **Minimum PIN length:** The minimum length of the TPM startup PIN. Defaults to **6**.
- **Configure 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**.
  - **Create 48-bit recovery password for OS drive recovery:** 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-digit password**.
  - **Create 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 AD DS:** Specifies whether to save the recovery options to Active Directory Domain Services. Default is **Off**.

  - **Configure recovery info stored in AD DS:** 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 AD DS:** 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**.

- **Customize 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**, and **Use custom recovery URL**. If **Off**, the default recovery message and URL display. Default is **Off**.
- **Configure fixed drive recovery:** Configures the recovery options to 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**.
- **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**.
- **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**.
- **Prompt for other disk encryption:** Allows you to disable the warning prompt for other disk encryption on devices. Defaults to **Off**.

Browser device policy

July 3, 2018

You can create browser device polices 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 26, 2020

You can add a device policy in XenMobile 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 and 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 26, 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

- **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. Only available for iOS 6.0 and later.

Connection manager device policy

April 25, 2019

In XenMobile, you can specify the connection settings for apps that connect automatically to the Internet and to private networks. This policy is only available on Windows Pocket PCs.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows Mobile/CE settings

> **Note:**
>
> **Built-in office** means all connections are to your company's intranet. **Built-in Internet** means that all connections are to the Internet.

- **Apps that connect to a private network automatically use:** In the list, click either **Built-in office** or **Built-in Internet**. The default is **Built-in office**.
- **Apps that connect to the Internet automatically use:** In the list, click either **Built-in office** or **Built-in Internet**. The default is **Built-in office**.

Connection scheduling device policy

April 25, 2019

> **Important:**
>
> Citrix recommends that you use Firebase Cloud Messaging (FCM) to control connections from Android, Android Enterprise, and Chrome OS devices to XenMobile Server. 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 XenMobile Server.

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.

Platform settings

- **Require devices to connect:** Click the option you want to set for this schedule.
  - **Always:** Keep the connection alive permanently. XenMobile on the user's device attempts to reconnect to the XenMobile server after a network connection loss and will monitor the connection by transmitting control packets at regular intervals. Citrix recommends this option for optimized security. When you choose **Always**, also use for the device **Tunnel Policy**, the **Define connection time-out** setting to ensure the connection is not draining battery. By keeping the connection alive, you can push security commands like wipe or lock to the device on-demand. You must also select the **Deployment Schedule** option **Deploy for always-on connections** in each policy deployed to the device.
  - **Never:** Connect manually. Users must initiate the connection from XenMobile on their devices. Citrix doesn't recommend this option for production deployments because it prevents you from deploying security policies to devices, thus users will never receive any new apps or policies.
  - **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, XenMobile 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 is **20**.
  - **Define schedule:** When enabled, XenMobile on the user's device attempts to reconnect to the XenMobile server after a network connection loss and monitors the connection by transmitting control packets at regular intervals within the time frame you define. See

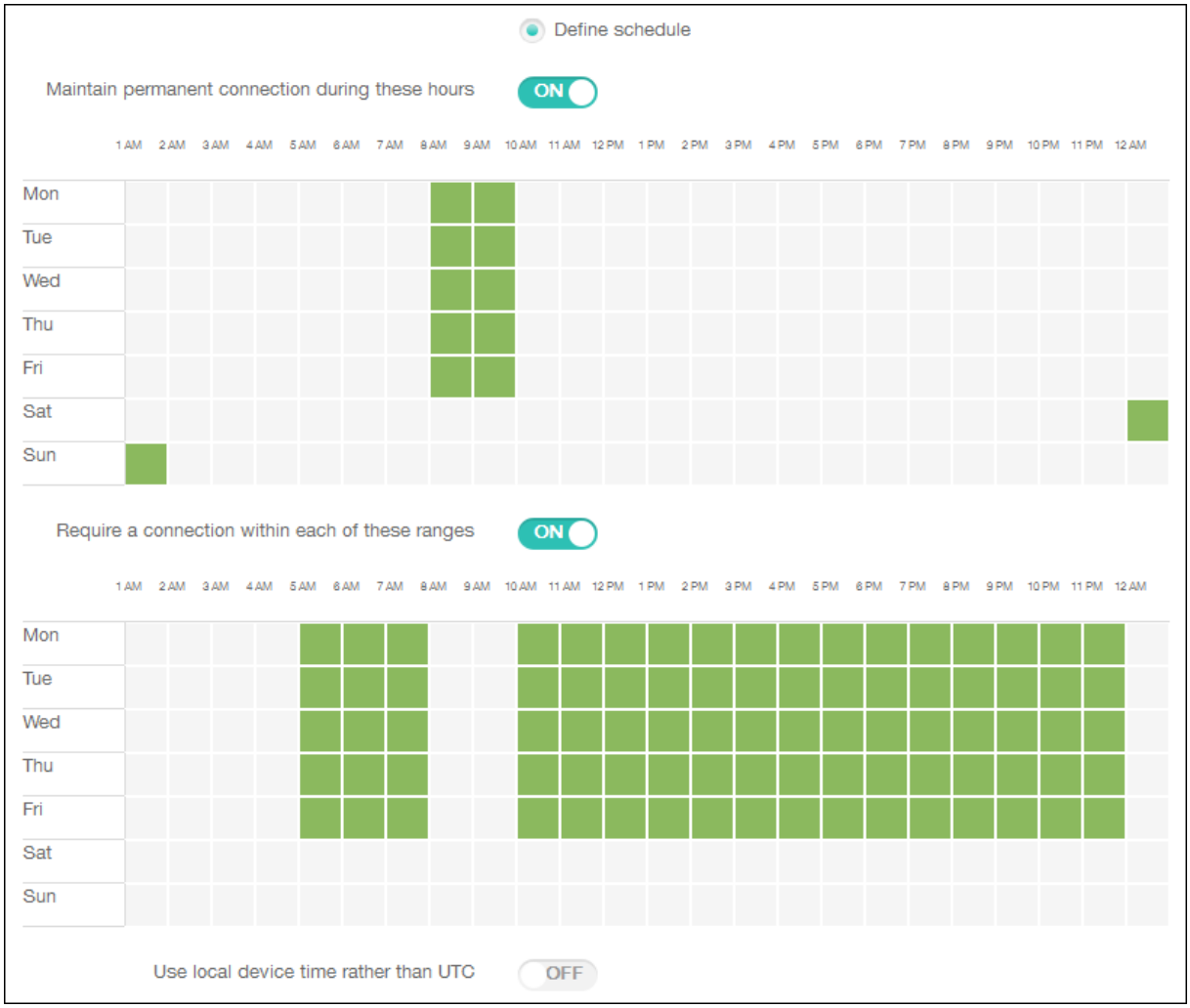
Defining a connection time frame, next, for how to define a connection time frame.

* **Maintain permanent connection during these hours:** Users' devices must be connected for the defined 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 30 minutes, so if you want a connection between 8:00 AM and 9:00 AM every weekday, you click the two squares 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 9:00 AM every weekday, a permanent connection between 12:00 AM Saturday and 1:00 AM Sunday, and at least one connection every weekday between 5:00 AM and 8:00 AM or between 10:00 AM and 11:00 PM.



Contacts (CardDAV) device policy

March 26, 2020

You can add a device policy in XenMobile 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. Only available for iOS 6.0 and later.

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.

Control OS Updates device policy

July 30, 2020

The Control OS Updates device policy lets you deploy:

- The latest OS updates to supervised iOS devices.

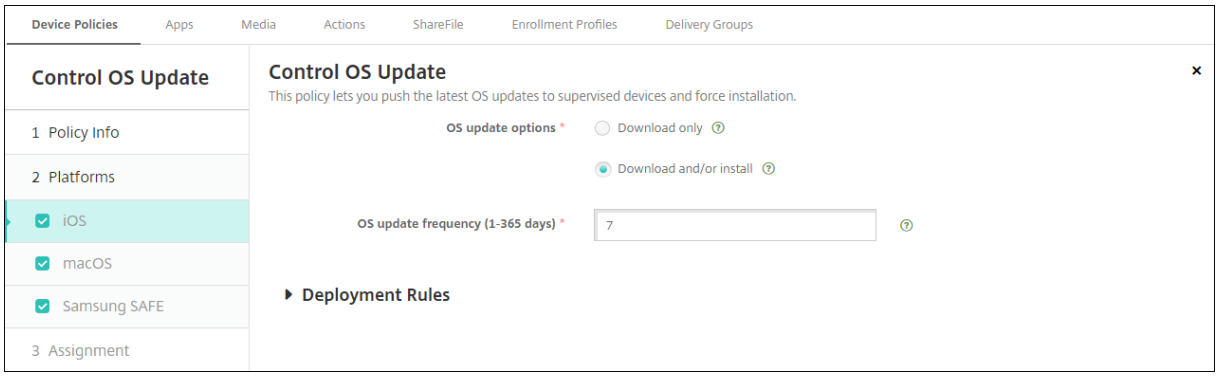
  The OS Update device policy only works for supervised devices enrolled in Apple Deployment Program.

- The latest OS and app updates to DEP-enrolled macOS devices running macOS 10.11.5 and later.
- The latest OS updates to supervised Samsung SAFE devices.

  For Samsung SAFE devices, XenMobile sends the Control OS Updates policy to Secure Hub, which then applies the policy to the device. The **Manage > Devices** page shows when XenMobile Server sends the policy and when the device receives the policy.

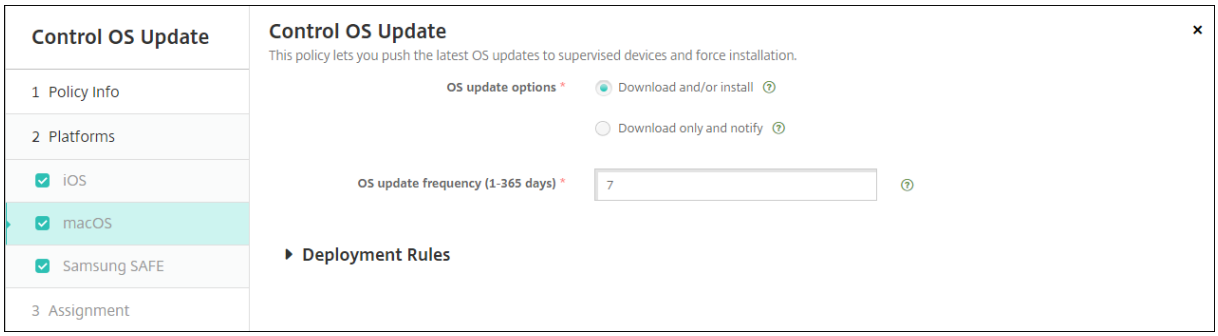
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **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 XenMobile checks and updates the device OS. The default is **7** days.

macOS settings



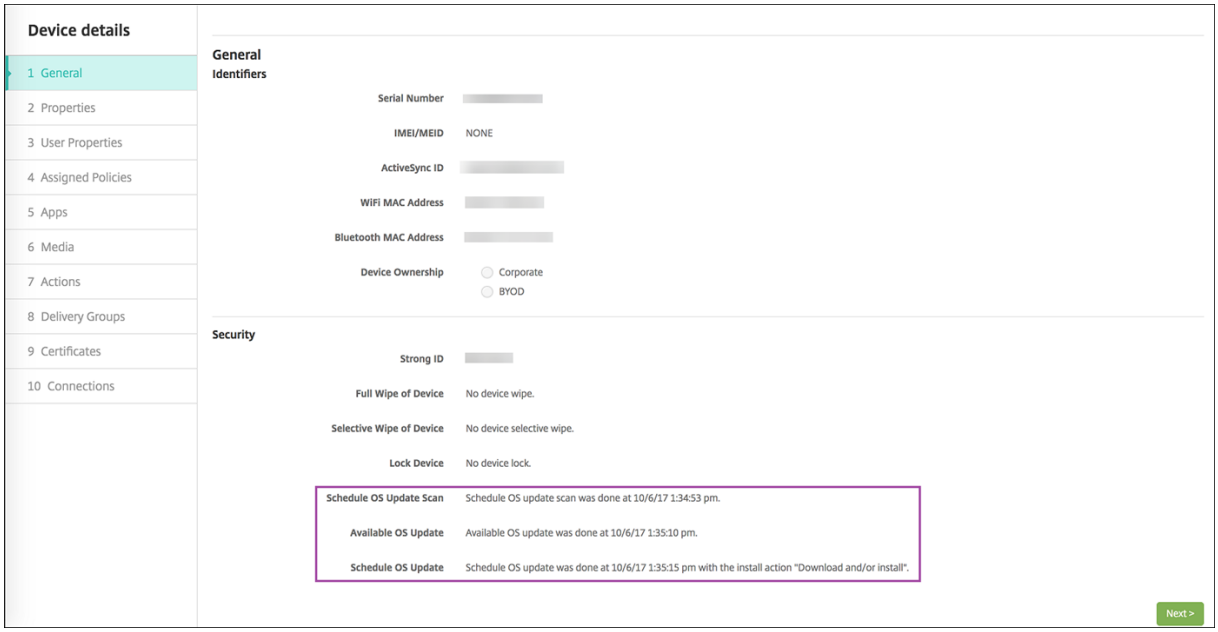
- **OS update options:** Both of the options download the latest macOS updates according to the **OS update frequency**. You can choose to install the updates or notify the user through the App Store that updates are available.
- **OS update frequency:** Determines how frequently XenMobile checks and updates the device OS. The default is **7** days.

Get status for iOS and macOS update actions

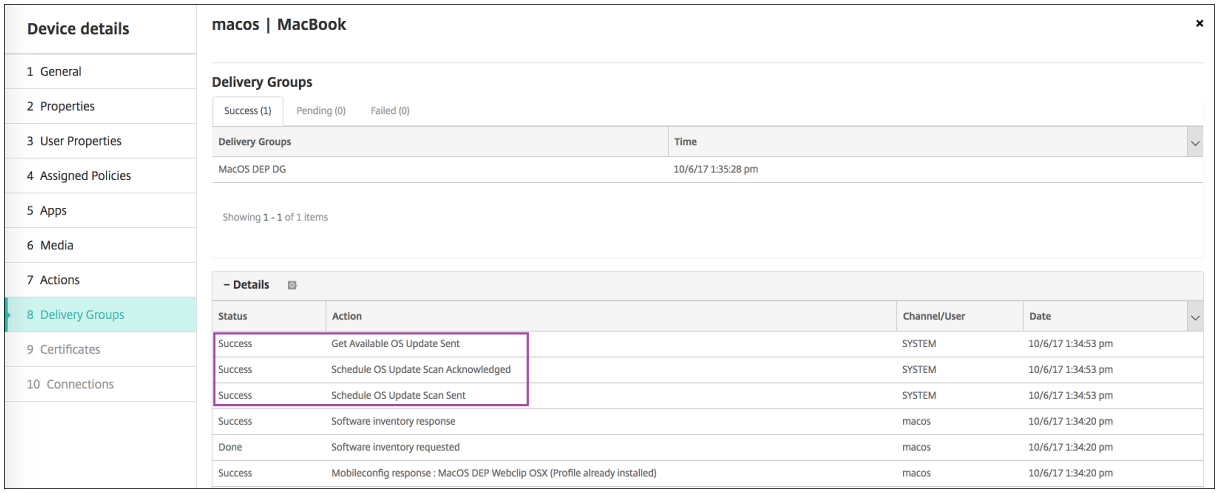
For iOS and macOS, XenMobile doesn't deploy the Control OS Updates policy to devices. Instead, XenMobile uses the policy to send these MDM commands to devices:

- 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 should download or install the OS and app updates.

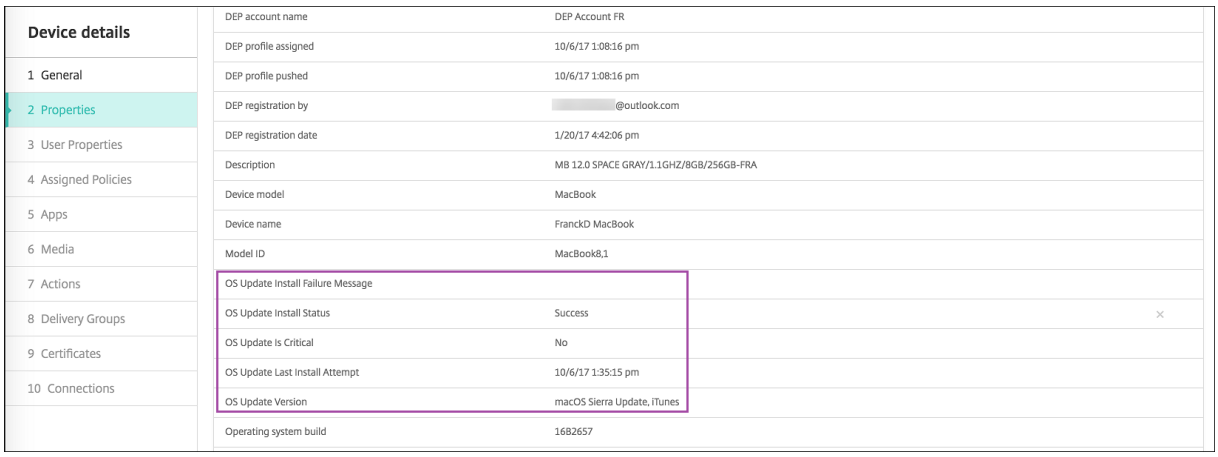
The **Manage > Devices > Device details (General)** page shows the status of scheduled and available OS update scans, and scheduled macOS and app updates.

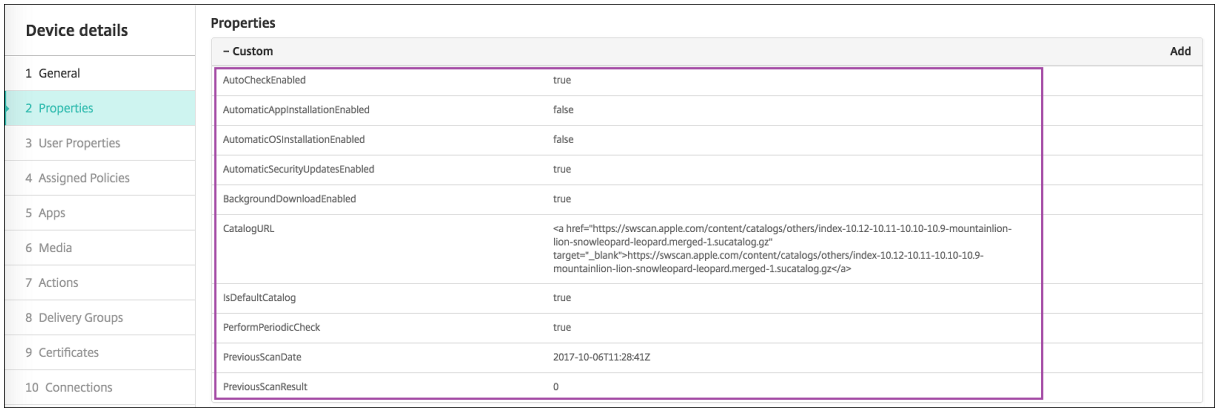


For more details about the status of update actions, go to the **Manage > Devices > Device details (Delivery Groups)** page.



For details such as available OS updates and the last installation attempt, go to the **Manage > Devices > Device details (Properties)** page.

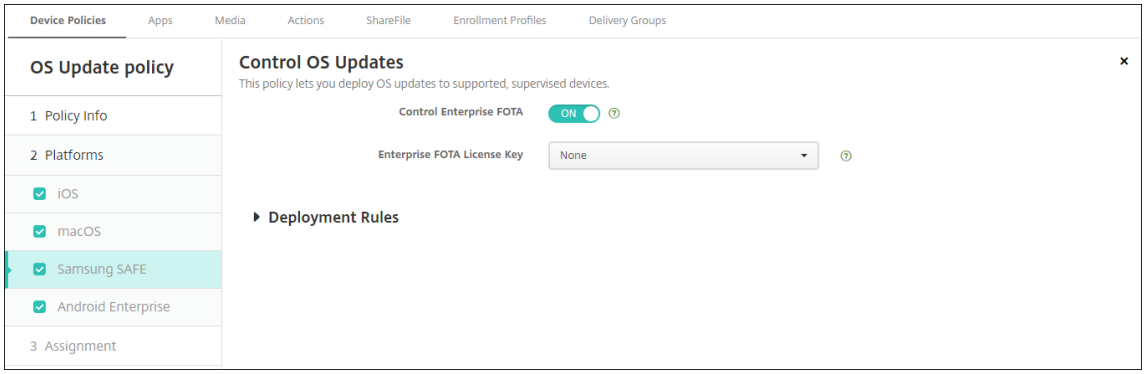




Samsung SAFE settings

Samsung Enterprise FOTA, also referred to as E-FOTA, lets you determine when devices get updated and the firmware version to use. To use E-FOTA:

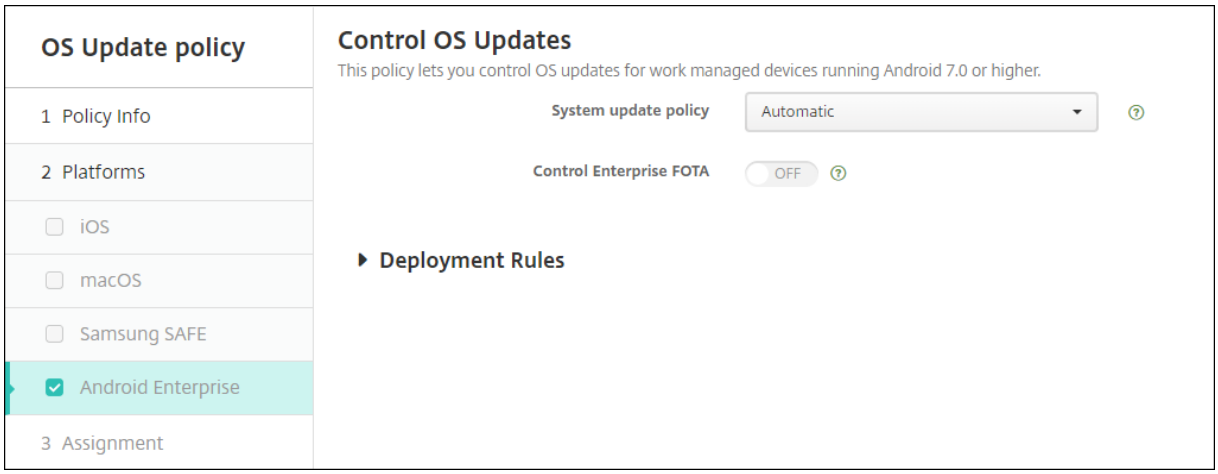
1. Create a Samsung MDM License Key device policy with the keys and license information you received from Samsung. For more information, see Samsung MDM license key device policy.
2. Create a Control OS Updates device policy to enable Enterprise FOTA.



   - **Enable Enterprise FOTA:** Set to **On**.

- **Enterprise FOTA License Key:** Select the Samsung MDM License Key device policy name.

Android Enterprise settings



- **System update policy.** Determines when system updates occur. **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**. **Postpone** allows a user to postpone an update for up to 30 days.
  - **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**.
- **Control Enterprise FOTA.** Enables you to control updates to Samsung devices that use the Samsung Enterprise Firmware-Over-the-Air (FOTA) service. For Android Enterprise devices running Samsung Knox 3.0 or later. Default is **Off**.
- **Enterprise FOTA license key.** When **Control Enterprise FOTA** is **On**, **Enterprise FOTA license key** lets you specify the license key to use for Samsung FOTA updates. For Android Enterprise devices running Samsung Knox 3.0 or later. Defaultis **None**. The key can be set using the **Samsung MDM license key** device policy. See Samsung MDM license key device policy.

Copy Apps to Samsung Container device policy

October 6, 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 Devices built on Knox.

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 XenMobile.
- 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.

Platform 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

November 6, 2020

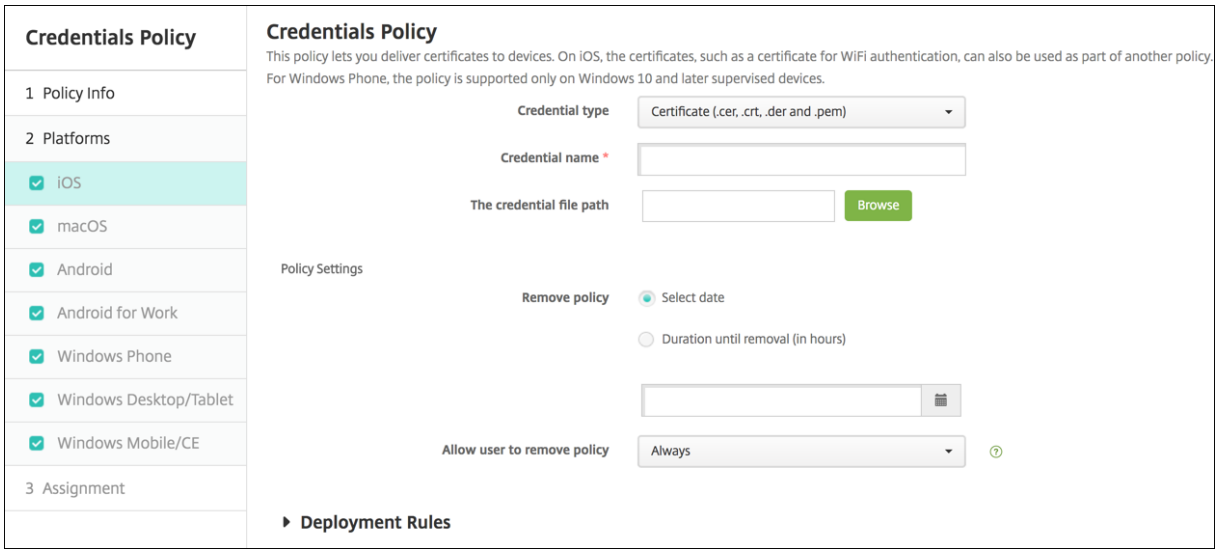
Credentials device policies point to a PKI configured in XenMobile. For example, your PKI configuration might include a PKI entity, a keystore, a credential provider, or a server certificate. For more information about credentials, see Certificates and authentication.

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.

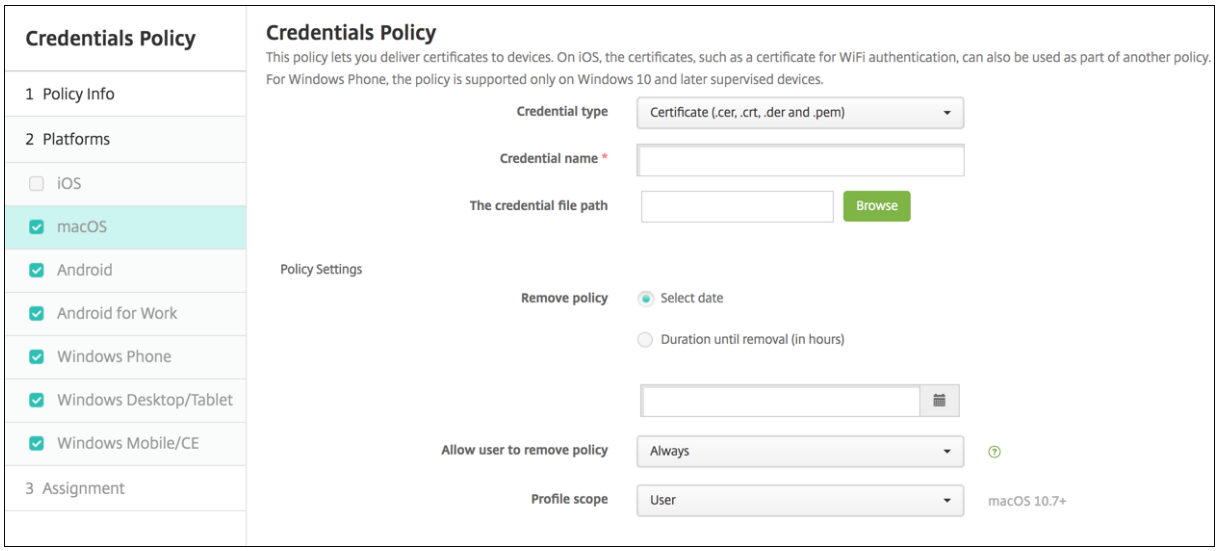
iOS settings



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. Only available for iOS 6.0 and later.

macOS settings

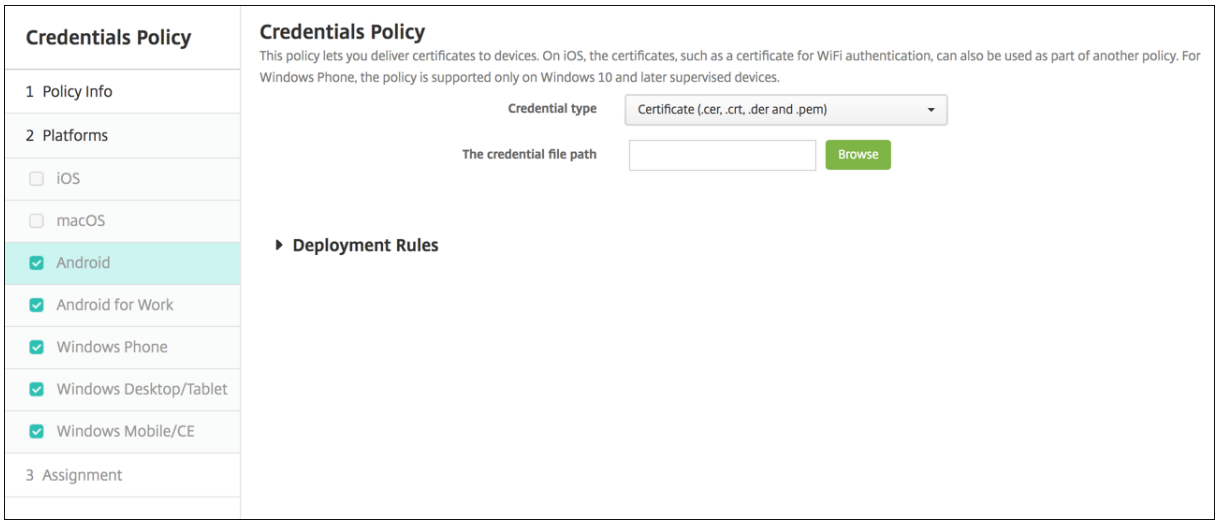


Configure the following settings:

- **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.

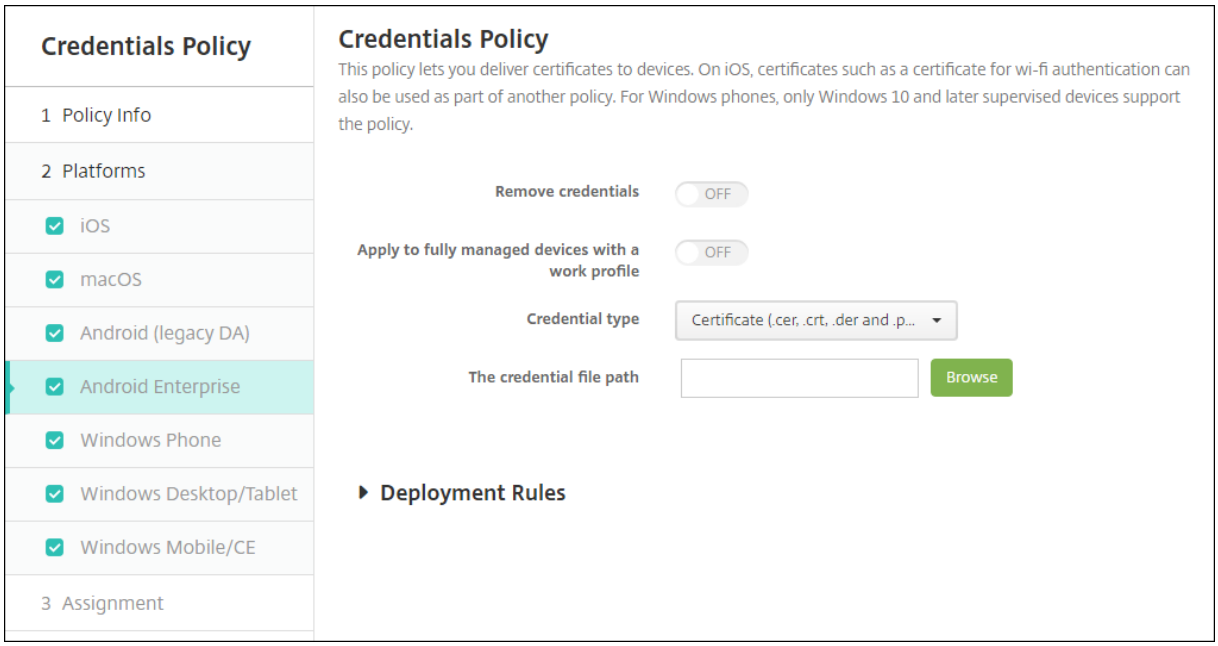
Android settings



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



Configure these settings to determine how XenMobile applies credentials settings:

- **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:** Allows you to configure credentials policy settings for fully managed devices with work profiles. When this setting is **On**, select one of these settings:
  - **Work profile:** The credentials settings you configure apply only to the work profile on the device.
  - **Manage device:** The credentials settings you configure apply only to the device.
  - **Both:** The credentials settings you configure apply to the work profile and the device.

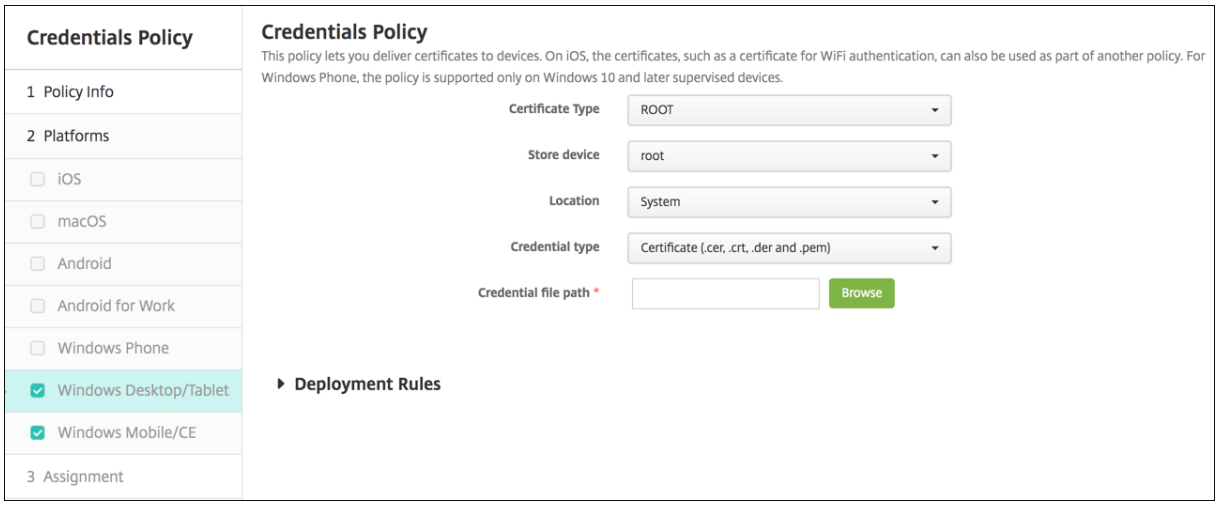
  When this setting is **Off**, the credentials settings you configure apply only to the device. Default is **Off**.

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**
    - **The credential file path:** Select the credential file by clicking **Browse** and then navigating to the file location.

- **Keystore**
  - **The credential file path:** Select the credential file by clicking **Browse** and then navigating to the file location.
  - **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.
  - **Password:** Type the keystore password for the credential.
- **Server certificate**
  - **Server certificate:** In the list, click the certificate to use.
- **Credential provider**
  - **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.
  - **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**.

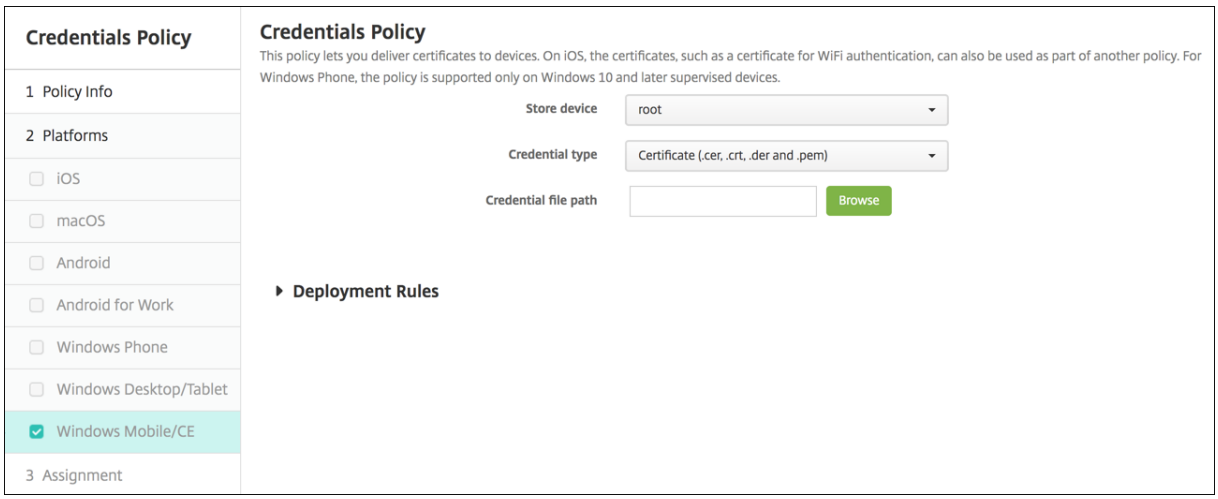
Windows Desktop/Tablet settings



- **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 tablets, **System** is the only location.

  - **Credential type:** For Windows 10 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 tablets, **System** is the only location.
- **Credential type:** For Windows 10 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 Mobile/CE settings



- **Store device:** In the list, click the location of the certificate store for the credential. The default is **root**. Options are:
  - **Privileged execution trust authorities:** Applications signed with a certificate belonging to this store will run with privileged trust level.
  - **Unprivileged execution trust authorities:** Applications signed with a certificate belonging to this store will run with normal trust level.
  - **SPC (Software Publisher Certificate):** The Software Publishing Certificate (SPC) is used for signing .cab files.
  - **root:** A certificate store that contains root certificates.
  - **CA:** A certificate store that contains cryptographic information, including intermediary certification authorities.
  - **MY:** A certificate store that contains end-user personal certificates.
- **Credential type:** Certificate is the only credential type for Windows Mobile/CE devices.
- **The credential file path:** Select the credential file by clicking **Browse** and then navigating to the file's location.

Custom XML device policy

March 9, 2021

You can create custom XML policies in XenMobile to customize the following features on supported Windows and 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 Device Management on the Microsoft Developer Network site.

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 About MX on the Zebra 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.

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**, XenMobile 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.

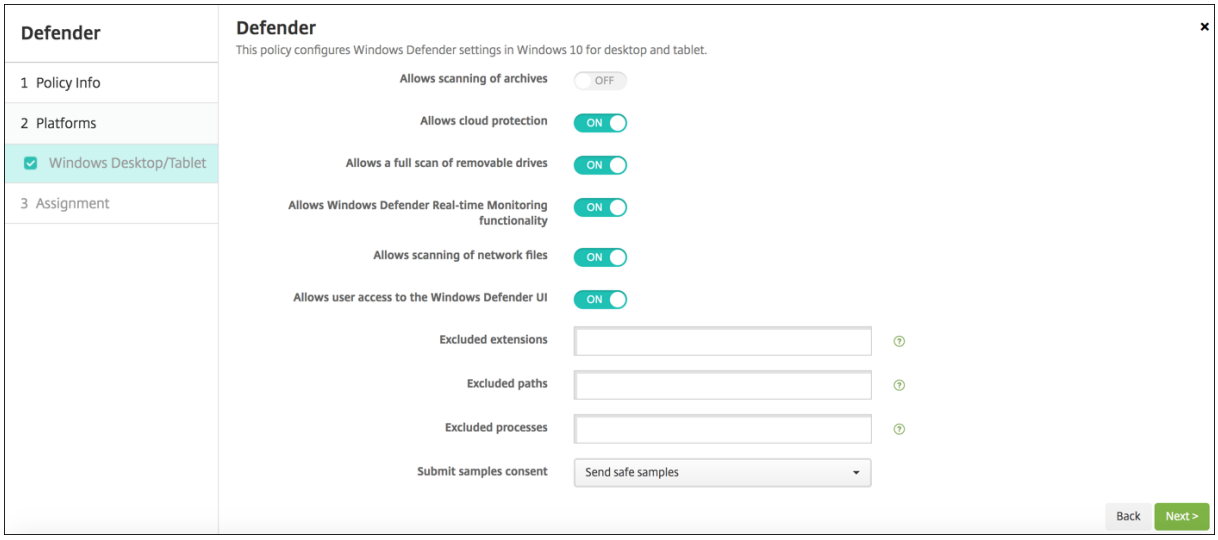
Defender device policy

July 3, 2018

Windows Defender is malware protection included with Windows 10. You can use the XenMobile device policy, Defender, to configure the Microsoft Defender policy for Windows 10 for desktop and tablet.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows Desktop and Tablet settings



- **Allows scanning of archives:** Allows or disallows Defender to scan archived files. Defaults to **Off**.
- **Allows cloud protection:** Allows or disallows Defender to send information to Microsoft about malware activity. Defaults to **On**.
- **Allows a full scan of removable drives:** Allows or disallows Defender to scan removable drives such as USB sticks. Defaults to **On**.
- **Allows Windows Defender Real-time Monitoring functionality:** Defaults to **On**.
- **Allows scanning of network files:** Allows or disallows Defender to scan network files. Defaults to **On**.
- **Allows user 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 consent:** 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**.

Delete files and folders device policy

July 3, 2018

You can create a policy in XenMobile to delete specific files or folders from Windows Mobile/CE devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows Mobile/CE settings

- **Files and folders to delete:** for each file or folder you want to delete, click Add and then do the following:
  - **Path:** Type the path to the file or folder.
  - **Type:** In the list, click File or Folder. The default is File.
  - Click **Save** to save the file or folder, or click **Cancel** to not save the file or folder.

Delete registry keys and values device policy

July 3, 2018

You can create a policy in XenMobile to delete specific registry keys and values from Windows Mobile/CE devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows Mobile/CE settings

- **Registry keys and values to delete:** for each registry key and value you want to delete, click **Add** and then do the following:

- **Key:** Type the registry key path. This is a required field.The registry key path should either start with HKEY_CLASSES_ROOT\ or HKEY_CURRENT_USER\ or HKEY_LOCAL_MACHINE\ or HKEY_USERS\.
- **Value:** Type the value name to be deleted or leave this field blank to delete the entire registry key.
- Click **Save** to save the key and value, or click **Cancel** to not save the key and value.

Device Health Attestation device policy

August 20, 2020

In XenMobile, you can require Windows 10 devices to report the state of their health by having those 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 XenMobile. When XenMobile receives the Health Attestation Certificate, based on the contents of the Health Attestation Certificate, it can deploy automatic actions that you have set up previously.

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.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

To configure DHA using Microsoft Cloud

Add a Device Health Attestation policy and configure this setting for each platform that you choose:

- **Enable Device Health Attestation:** Select whether to require Device Health Attestation. The default is **Off**.

To configure DHA using an on-premises Windows DHA server

To enable DHA on-premises, you first configure a DHA server. Then you create a XenMobile Server policy to enable the on-premises DHA service.

1. 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 Heath Attestation server.
2. Add a Device Health Attestation policy and configure these settings:
    - **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.

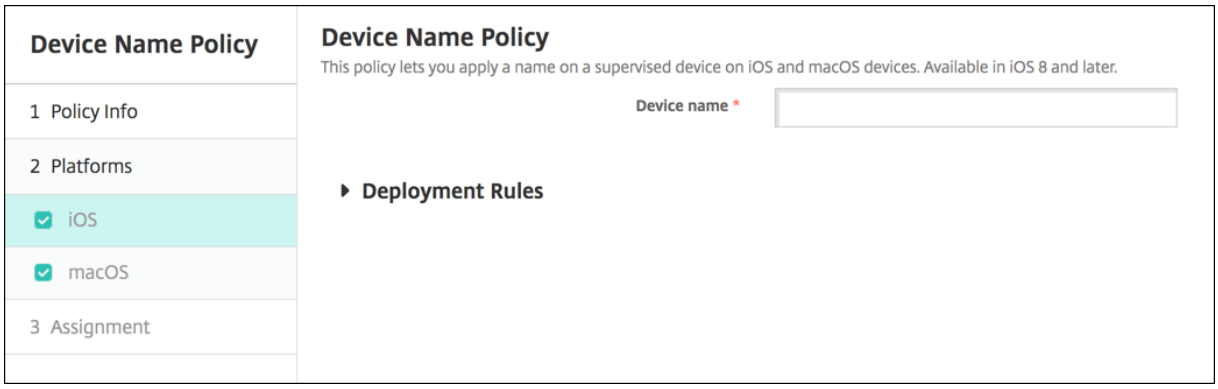
Device name device policy

July 3, 2018

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 XenMobile.

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

September 10, 2020

The Education Configuration device policy defines:

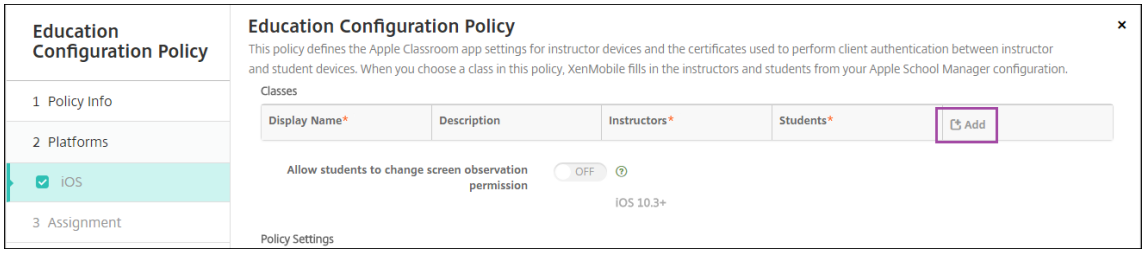
- The Apple Classroom app settings for instructor devices.
- The certificates used to perform client authentication between instructor and student devices.

When you choose a class in this policy, the XenMobile 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.

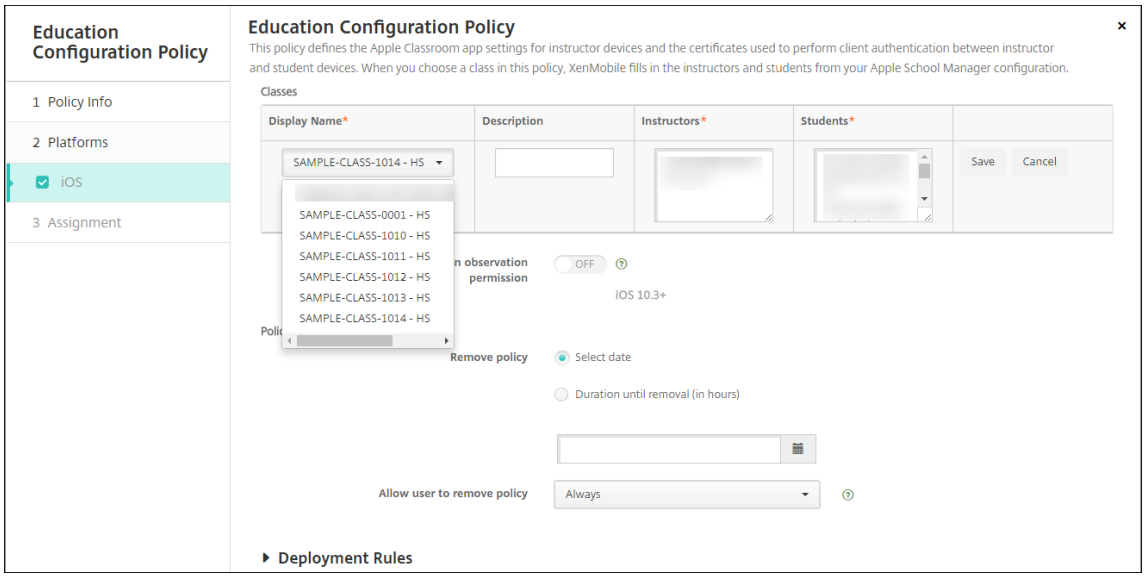
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

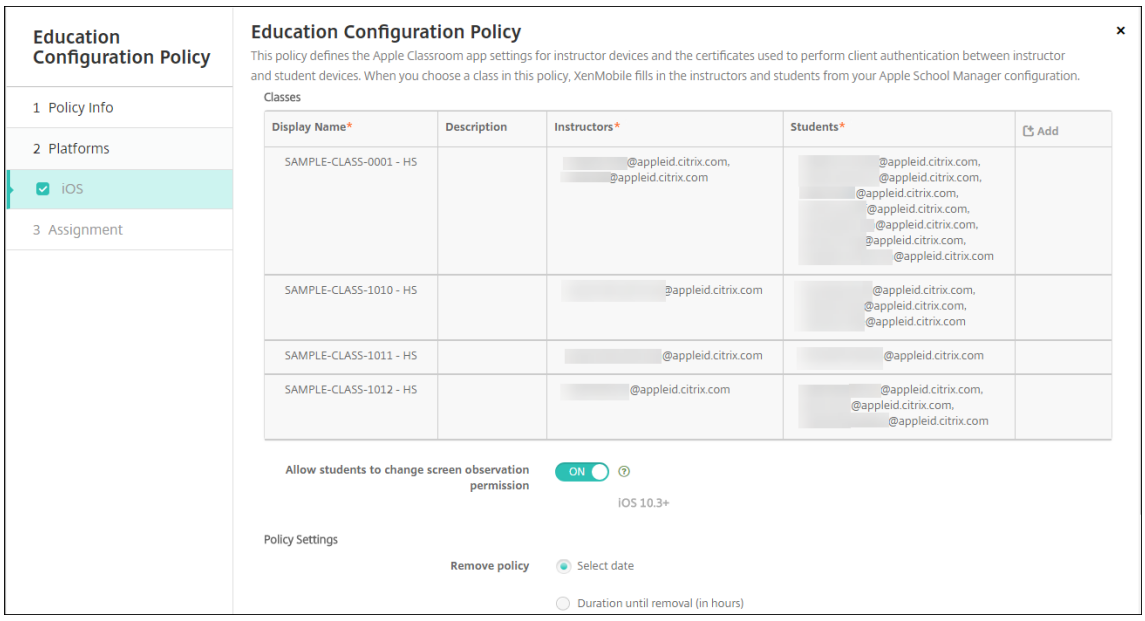
- **Classes:** To add a class, click **Add**.



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**, XenMobile fills in the instructors and students. Continue adding classes.



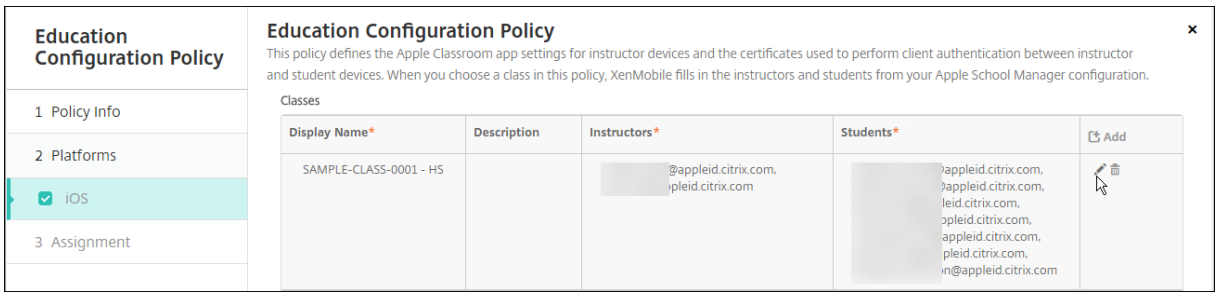
- **Allow students to change screen observation permission:** If **On**, students enrolled in managed classes can choose whether to allow their teacher to observe their device screens. Default is **Off**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available 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. XenMobile 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.



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.

Enterprise Hub device policy

October 14, 2019

An Enterprise Hub device policy for Windows Phone lets you distribute apps through the Enterprise Hub Company store.

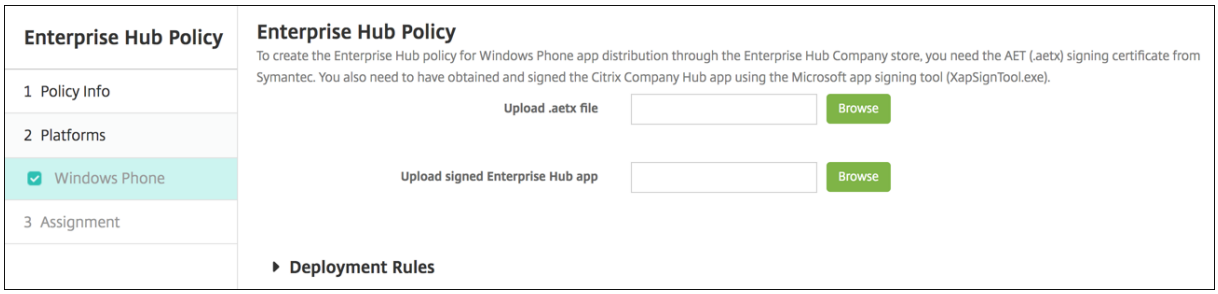
Before you can create the policy, you need the following:

- An AET (.aetx) signing certificate from DigiCert
- The Citrix Company Hub app signed by using the Microsoft app signing tool (XapSignTool.exe)

> **Note:**
>
> XenMobile supports only one Enterprise Hub policy for one mode of Windows Phone Secure Hub. For example, to upload Windows Phone Secure Hub for XenMobile Enterprise Edition, you should not create multiple Enterprise Hub policies with different versions of Work Home for XenMobile Enterprise Edition. 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



- **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

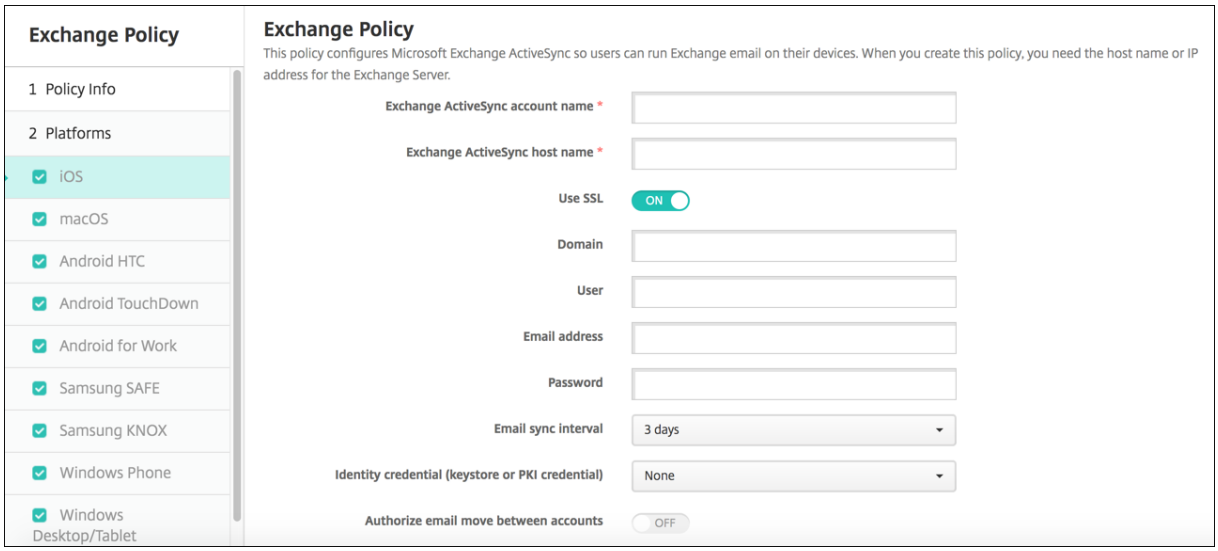
January 6, 2021

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. You can create policies for iOS, macOS, Android Enterprise, Samsung SAFE, Samsung KNOX, Windows Phone, and Windows Tablet. 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.

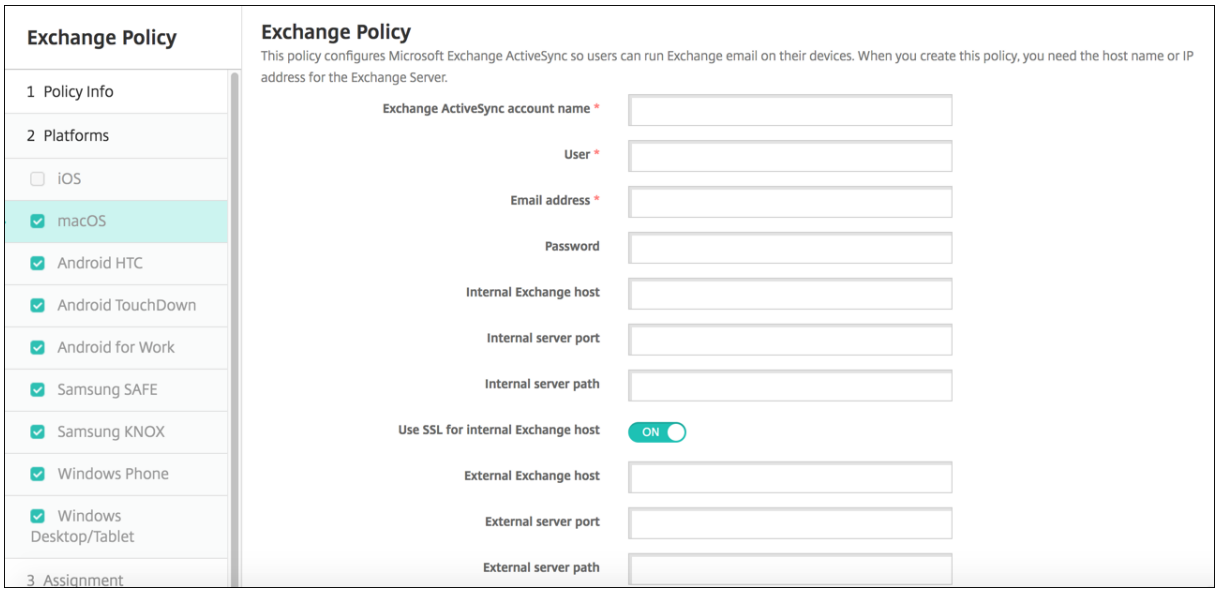
iOS settings



- **Exchange 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 XenMobile. This field is only required when Exchange requires a client certificate authentication. The default is **None**.
- **Authorize email move between accounts:** Select whether to allow users to move email out of this account into another account and to forward and reply from a different account. The default is **Off**.
- **Send email only from email app:** Select whether to restrict users to the iOS mail app for sending email. The default is **Off**.

- **Disable email recent syncing:** Select whether to prevent users from syncing recent addresses. The default is **Off**. This option applies only to iOS 6.0 and later.
- **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 Overrideable:** 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 Overrideable:** 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 Overrideable:** 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 Overrideable:** 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. Only available for iOS 6.0 and later.

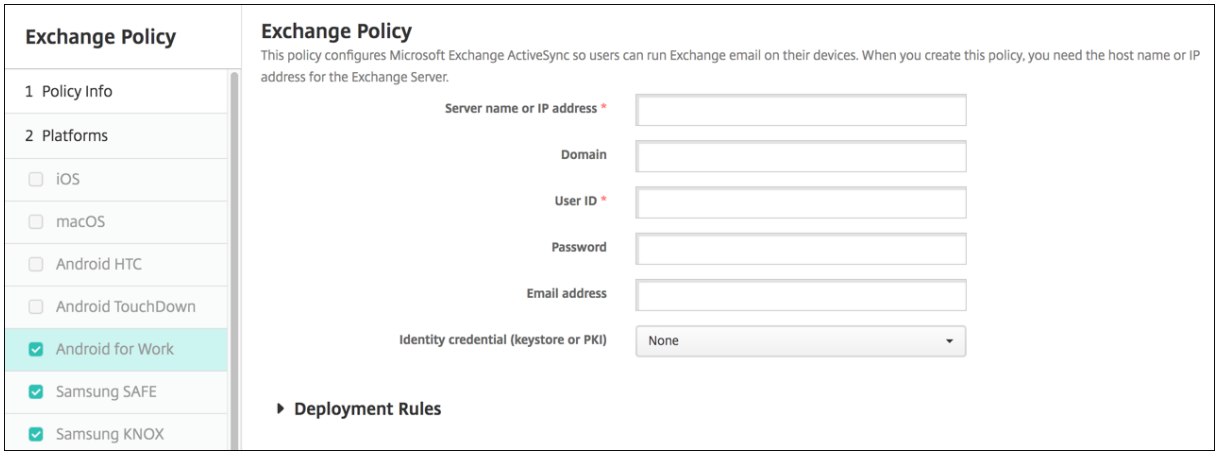
macOS settings



- **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 SignIn URL:** Specifies the URL to load into a webview to authenticate using OAuth when AutoDiscovery Service is not used. 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.

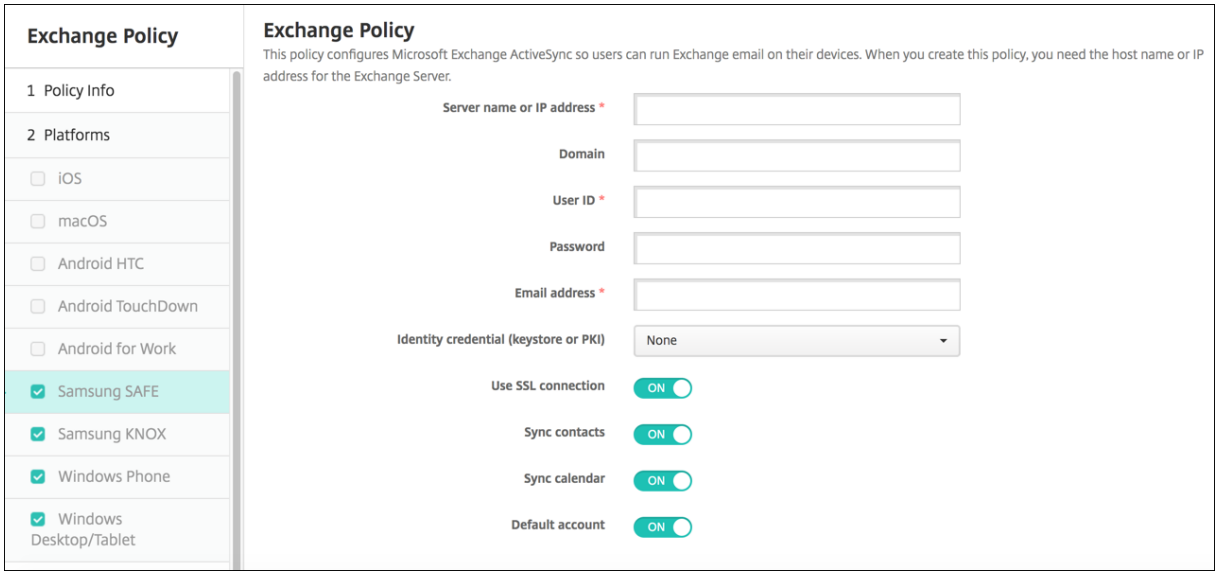
Android Enterprise



- **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 XenMobile. This field is only required when Exchange requires a client certificate authentication. The default is **None**.

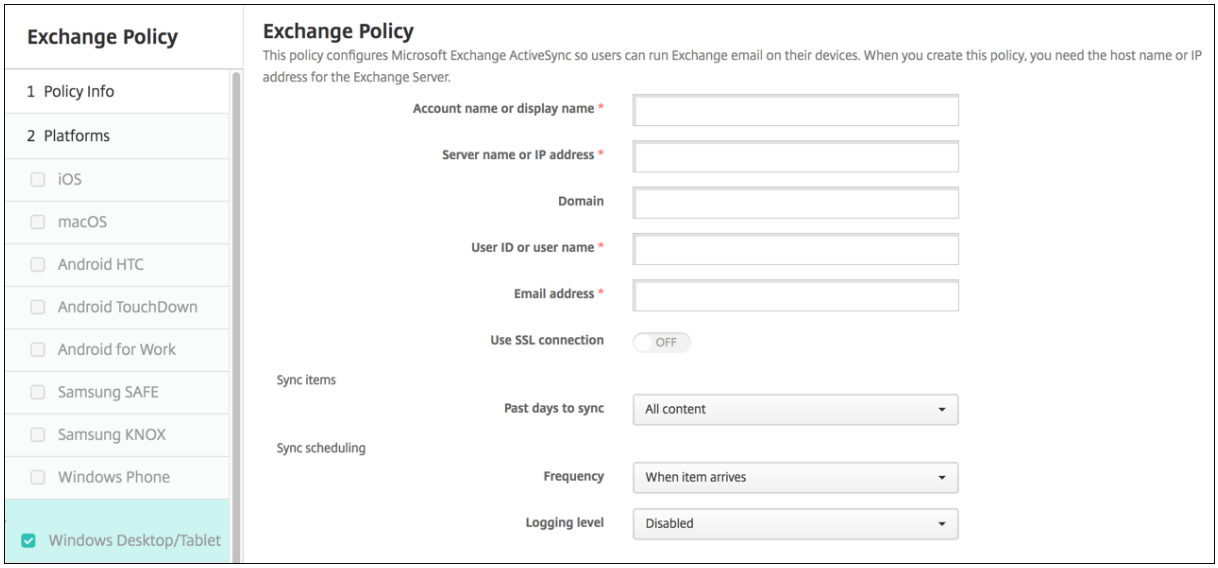
Samsung SAFE and Samsung KNOX settings



- **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 XenMobile. 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



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 it 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 22, 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.

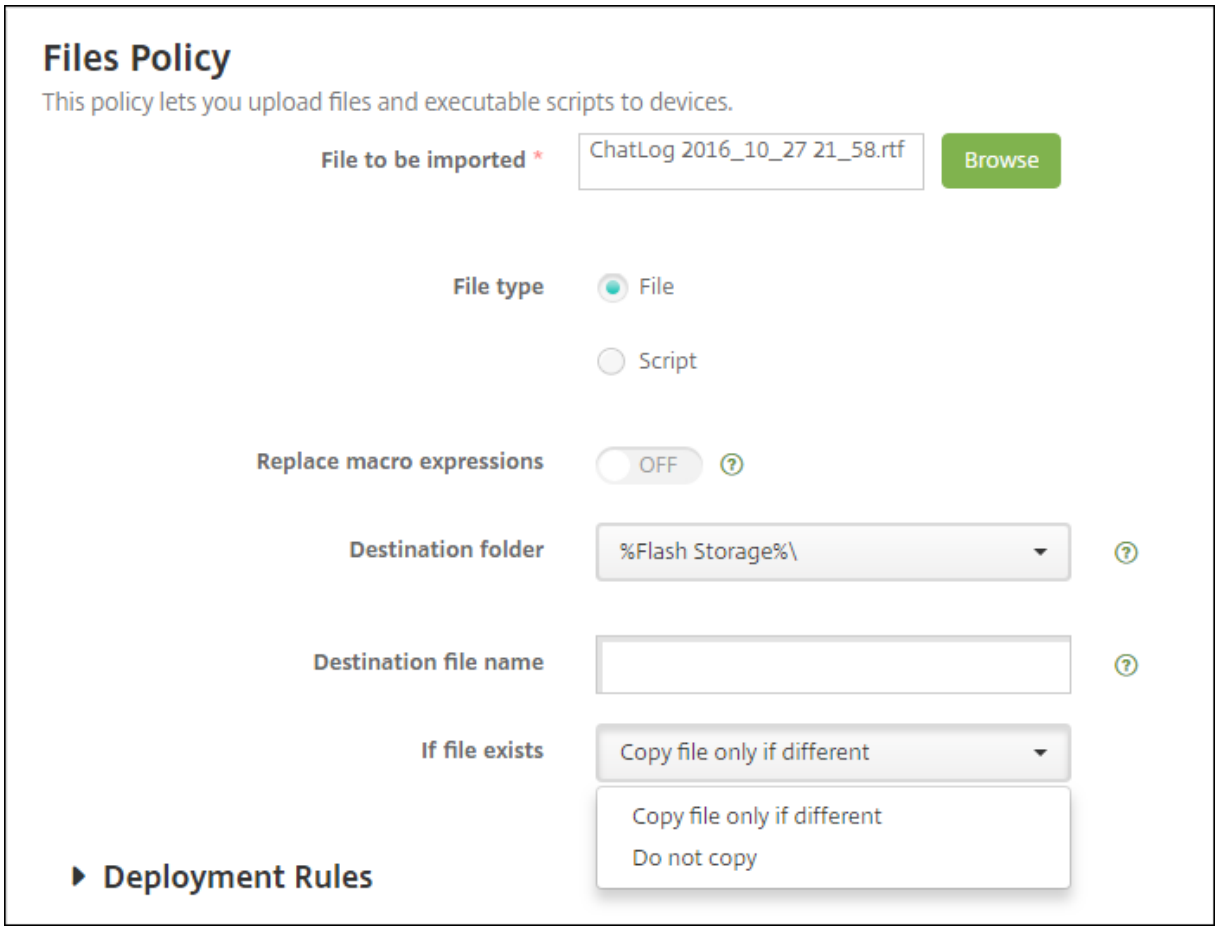
Android devices don't support running scripts natively. Users need third-party software to run scripts.

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
- For Windows Mobile and Windows CE only: Script files created with MortScript

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Android Enterprise 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 in which to store the uploaded file or click **Add new** to choose an unlisted file location. You can use the macros %XenMobile Folder%\ or %Flash Storage%\ as the start of any path identifier.
- **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:** Select the file to import by clicking **Browse** and navigating to the file's 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. The default is **Off**.
- **Destination folder:** In the list, select the location in which to store the uploaded file or click **Add new** to choose an unlisted file location. In addition, you can use the macros %XenMobile Folder%\ or %Flash Storage%\ as the start of a path identifier.
- **Destination file name:** Optionally, type a different name for the file if it must be changed before being deployed on a device.
- **Copy file only if different:** In the list, select whether to copy the file if it is different from the existing file. The default is to copy the file only if it is different.

Windows Mobile/CE settings

- **File to be imported:** Select the file to import by clicking Browse and navigating to the file's location.
- **File type:** Select either **File** or **Script**.
- **Execute immediately:** When you select **Script**, **Execute immediately** appears. Select whether the script is executed as soon as the file is uploaded. The default is **Off**.
- **Replace macro expressions:** Select whether to replace macro token names in a script with a device or user property. The default is **Off**.
- **Destination folder:** In the list, select the location in which to store the uploaded file or click **Add new** to choose an unlisted file location. In addition, you can use any of the following macros as the start of a path identifier:
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Destination file name:** Optionally, type a different name for the file if it must be changed before being deployed on a device.
- **Copy file only if different:** In the list, select whether to copy the file if it is different from the existing file. The default is to copy the file only if it is different.
- **Read only file:** Select whether the file is to be read-only. The default is **Off**.
- **Hidden file:** Select whether the file is not to be shown in the file list. The default is **Off**.

FileVault device policy

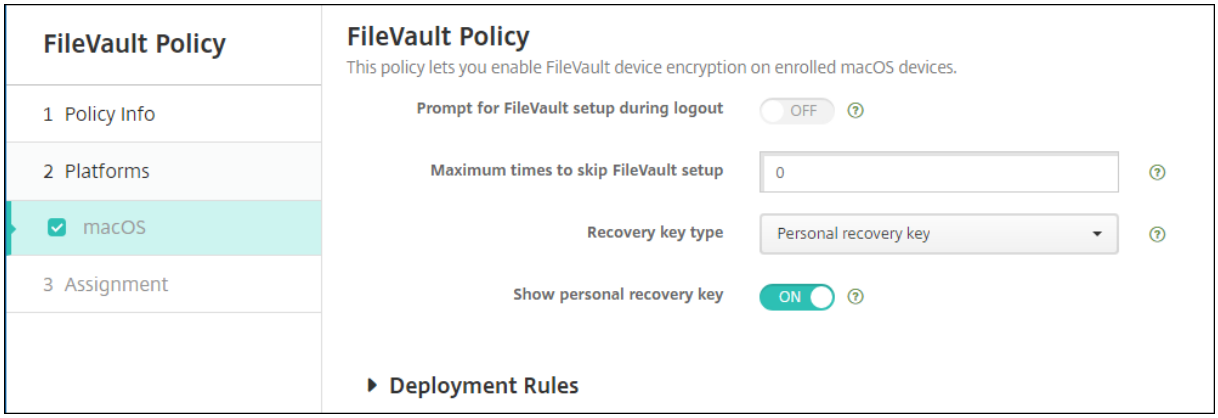
July 3, 2018

The macOS FileVault Disk Encryption feature protects the system volume by encrypting its contents. With FileVault enabled on a macOS device, a user logs in 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.

The XenMobile device policy, FileVault, enables FileVault user setup screens and configures settings such as recovery keys. For more information about FileVault, see the Apple support site, https://support.apple.com.

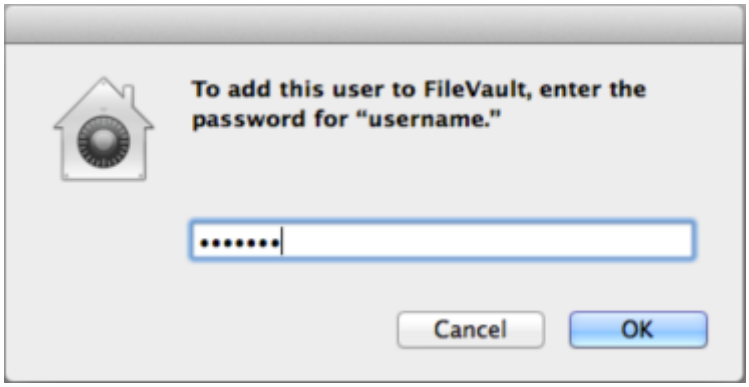
To add the FileVault policy, go to **Configure > Device Policies**.

macOS settings

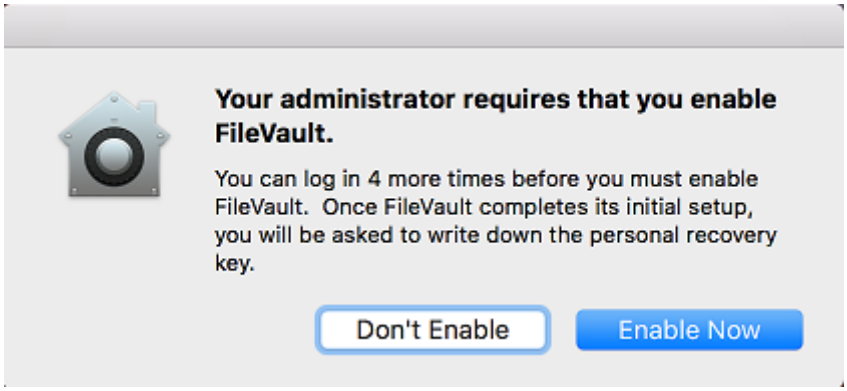


- **Prompt for FileVault setup during logout:** If **On**, prompts the user to enable FileVault during the next N logouts, as specified by the option, **Maximum times to skip FileVault setup**. If **Off**, the FileVault password prompt doesn't appear.

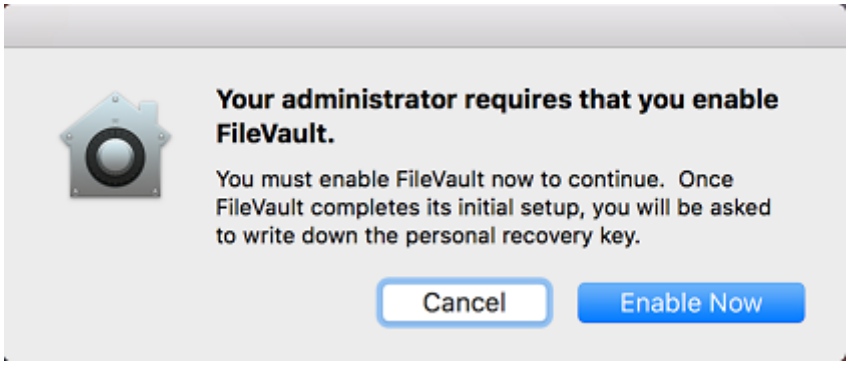
After you deploy the FileVault policy with this setting on, the following screen appears when a user signs off the device. The screen gives the user the option to enable FileVault before signing off.

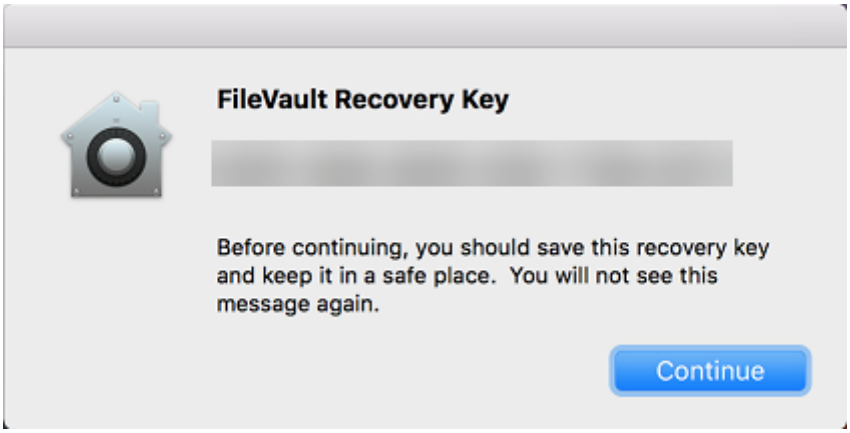


If the **Maximum times to skip FileVault setup** value isn't 0: After you deploy the FileVault policy with this setting off and then the user signs on, the following screen appears.



If the **Maximum times to skip FileVault setup** value is 0 or the user has skipped setup the maximum number of times, the following screen appears.





Font device policy

March 26, 2020

You can add a device policy in XenMobile to add additional fonts to iOS and macOS devices. Fonts must be TrueType (.ttf) or OpenType (.oft) fonts. Font collections (.ttc or .otc) are not supported.

For iOS, this policy applies only to iOS 7.0 and later.

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:** Select the font file to be added to users' devices by clicking **Browse** and then navigating to the file's 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. Only available for iOS 6.0 and later.

macOS settings

- **User-visible name:** Type the name that users see in their font lists.

- **Font file:** Select the font file to be added to users' devices by clicking **Browse** and then navigating to the file's 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

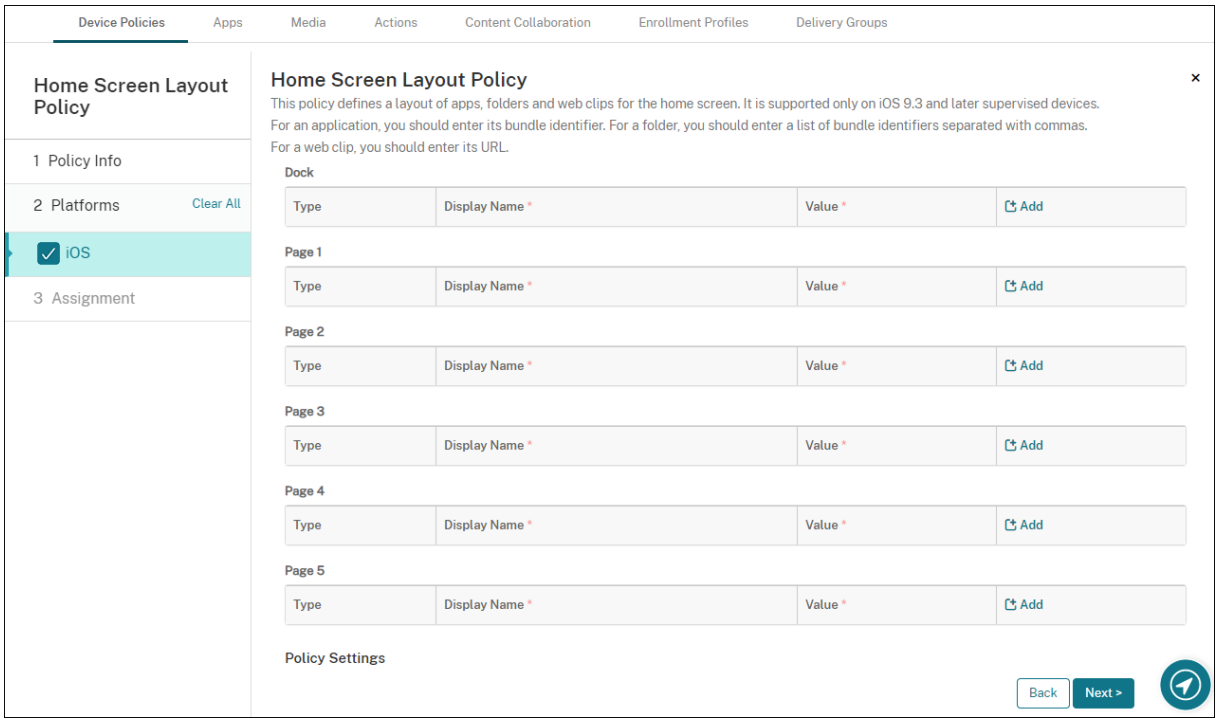
March 10, 2021

You can specify the layout of apps and folders for the iOS Home screen. The Home screen layout device policy is for iOS 9.3 and later supervised 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 XenMobile policy or through the Apple Configurator.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

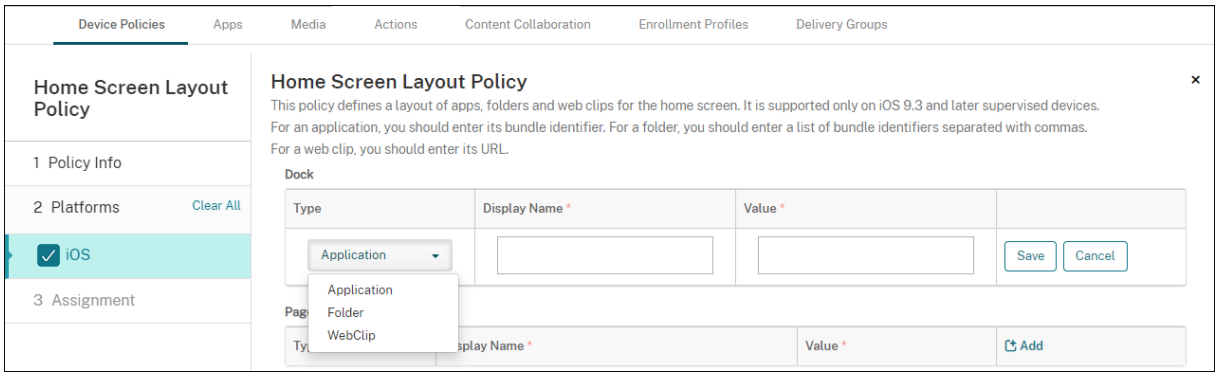
iOS settings



- For each of the screen areas you want to configure (such as **Dock** or **Page 1**), click **Add**.
- **Type:** Choose either **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, sepa-

rated 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. 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.

Import iOS & macOS Profile device policy

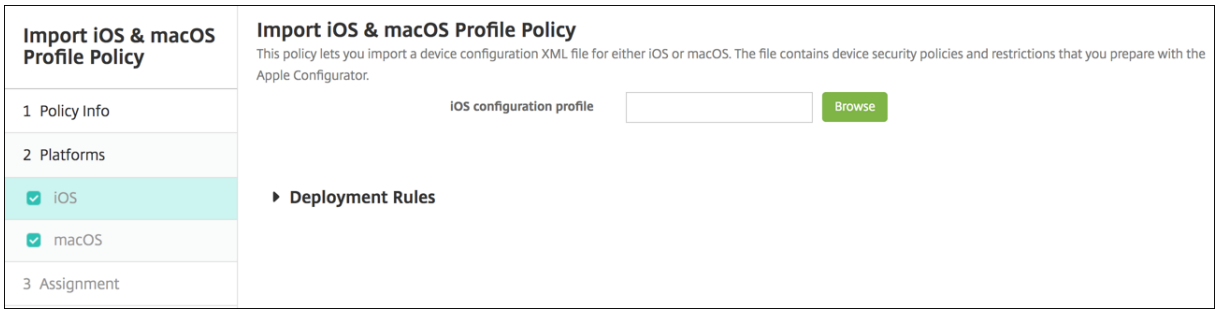
April 25, 2019

You can import device configuration XML files for iOS and macOS devices into XenMobile. The file contains device security policies and restrictions that you prepare with the Apple Configurator.

You can place an iOS device in Supervised mode with the Apple Configurator, as described later in this article. For more information about using the Apple Configurator to create a configuration file, see Apple Configurator Support.

To add or configure this policy, 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 impor, click **Browse** and navigate to the file location.

Place an iOS device in Supervised mode with the Apple Configurator

To use the Apple Configurator, you need an Apple computer running macOS 10.7.2 or later.

> **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.

1. Install the Apple Configurator from iTunes.
2. Connect the iOS device to your Apple computer.
3. Start the Apple Configurator. The Configurator shows that you have a device to prepare for supervision.
4. To prepare the device for supervision:
    a) Switch the **Supervision** control to **On**. Citrix recommends that you choose this setting if you intend to maintain control of the device on an ongoing basis by reapplying a configuration regularly.
    b) Optionally, provide a name for the device.
    c) In iOS, click **Latest** for the latest version of iOS you want to install.
5. When you are ready to prepare the device for supervision, click **Prepare**.

Keyguard Management device policy

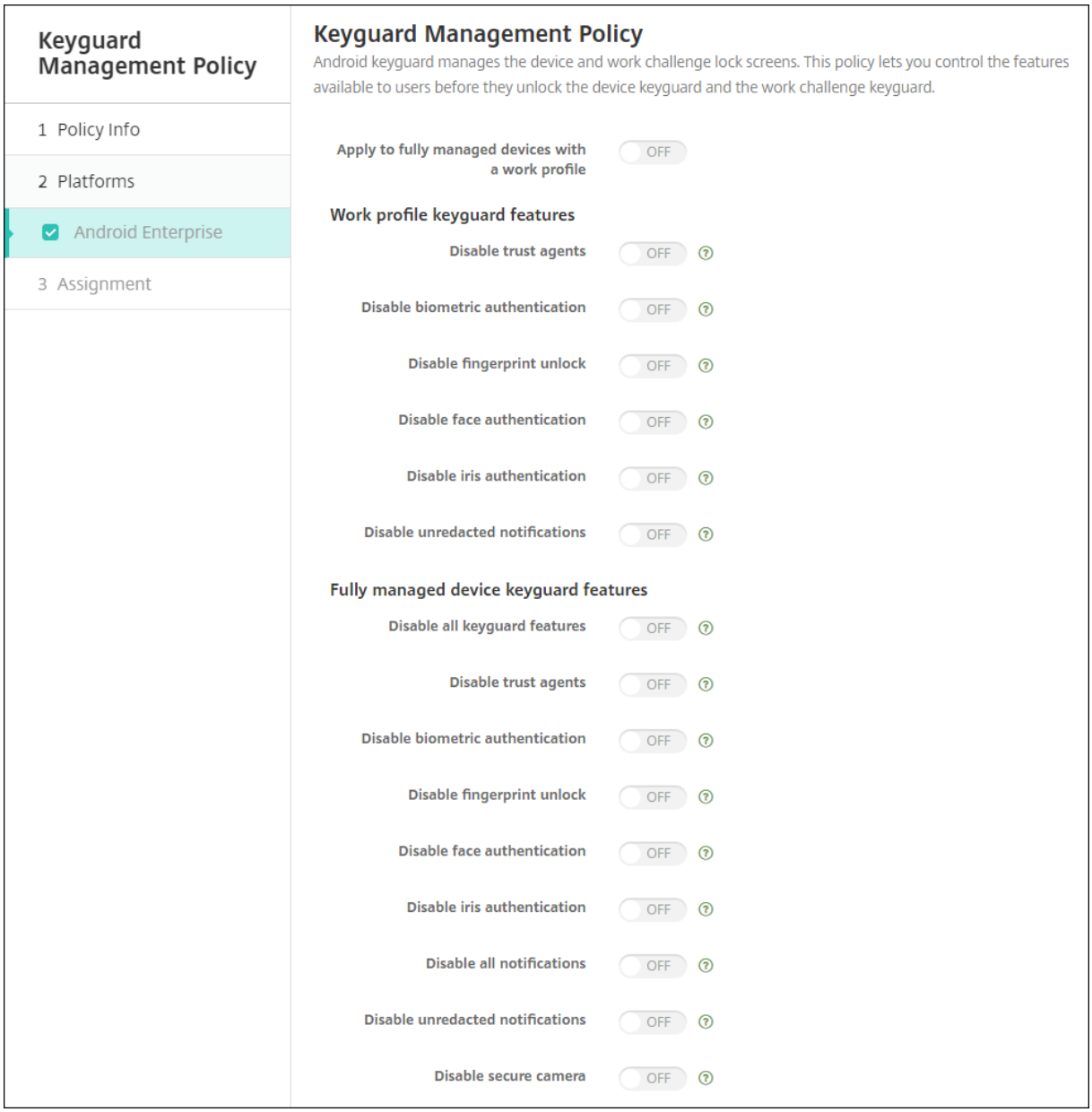
November 6, 2020

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. 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.

Android Enterprise settings



- **Apply to fully managed devices with a work profile:** 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 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 **On**, fingerprint unlock is not available on secure keyguard screens when a challenge is set on the work profile. Set to **Off** to enable 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. This 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 device. Set to **On** to disable fingerprint unlock on the device. Default is **Off**.
  - **Disable face authentication:** If **Off**, face authentiction is available on secure keyguard screens when a challenge is set on the device. Set to **On** to disable face authentiction on the device. Default is **Off**. For Android 9.0 and later.

- **Disable iris authentiction:** If **Off**, iris authentiction is available on secure keyguard screens when a challenge is set on the device. Set to **On** to disable iris authentiction 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**.

Kiosk device policy

September 17, 2020

The Kiosk policy lets you restrict devices to Kiosk mode by limiting the apps that can run. XenMobile 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 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 to connect back to XenMobile.
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

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.

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.

- **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.

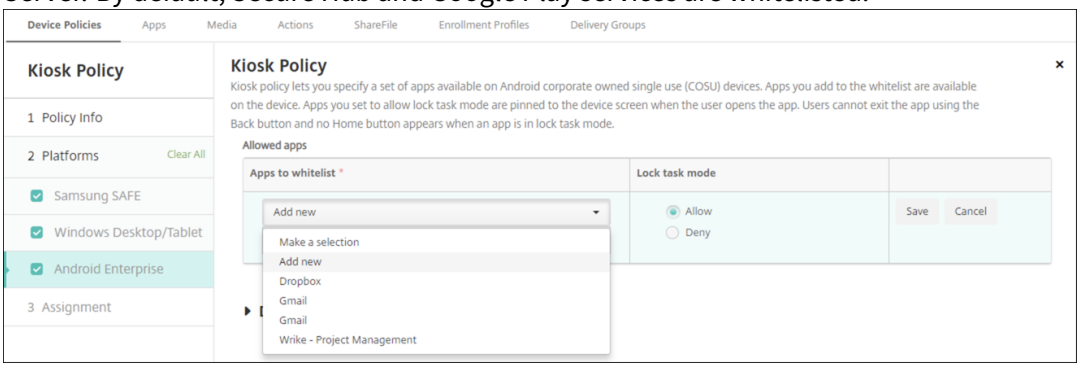
Android Enterprise settings

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. By default, Secure Hub and Google Play services are on the allow list.

To allow an app, click **Add**. You can allow multiple apps. For more information, see Android Enterprise.

> **Note:**
>
> The XenMobile Server console includes the terms “blacklist” and “whitelist”. We are changing those terms in an upcoming release to “block list” and “allow list”.

- **Apps to whitelist:** Enter the package name of the app you want to whitelist or select the app from the list.
  - Click **Add new** to enter the package name of the app approved to show in the list.
  - Select the existing app from the list. The list shows apps that are uploaded in XenMobile Server. By default, Secure Hub and Google Play services are whitelisted.



- **Lock task mode:** 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. By default, Secure Hub and Google Play services are allowed. The 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.

Launcher configuration device policy for Android

October 12, 2018

Citrix Launcher lets you customize the user experience for Android devices deployed by XenMobile. Citrix Launcher and the Launcher Configuration device policy are not compatible with Android Enterprise.

You can add a Launcher Configuration policy to control these Citrix Launcher features:

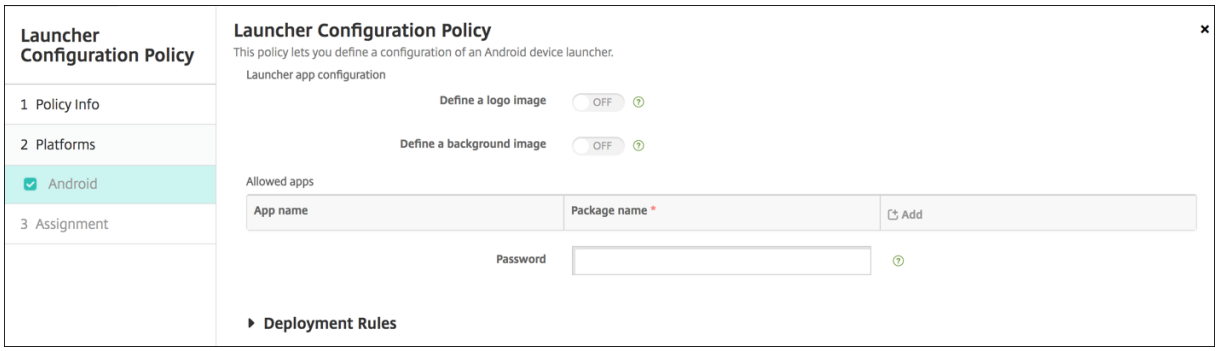
- Manage Android devices so that users can access only the apps that you specify.
- Optionally specify a custom logo image for the Citrix Launcher icon and a custom background image for Citrix Launcher.
- Specify a password that users must enter to exit the launcher.

While Citrix Launcher enables you to apply those device-level restrictions, the launcher grants users the operational flexibility they need through built-in access to device settings such as WiFi settings, Bluetooth settings, and device passcode settings. Citrix Launcher isn't intended as an extra layer of security over what the device platform already provides.

After you deploy Citrix Launcher, XenMobile installs it, replacing the default Android launcher.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Android settings



- **Define a logo image:** Select whether to use a custom logo image for 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 26, 2020

You create an LDAP policy for iOS devices in XenMobile 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 0=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. Only available for iOS 6.0 and later.

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 leve**l, 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 0=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 **Pass-**

code 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.

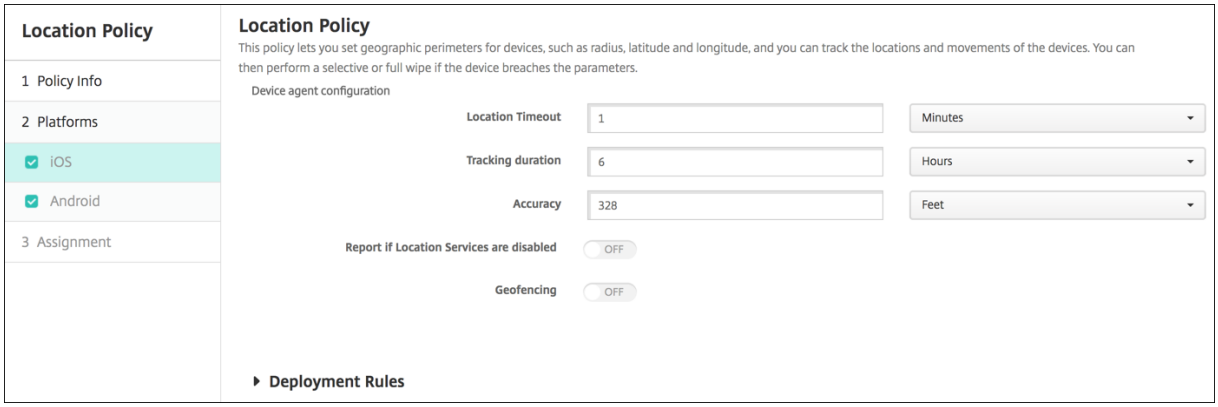
Location device policy

April 27, 2021

You create location device policies in XenMobile to enforce geographic boundaries. When users breach the defined boundary, also called a *geofence*, XenMobile 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.

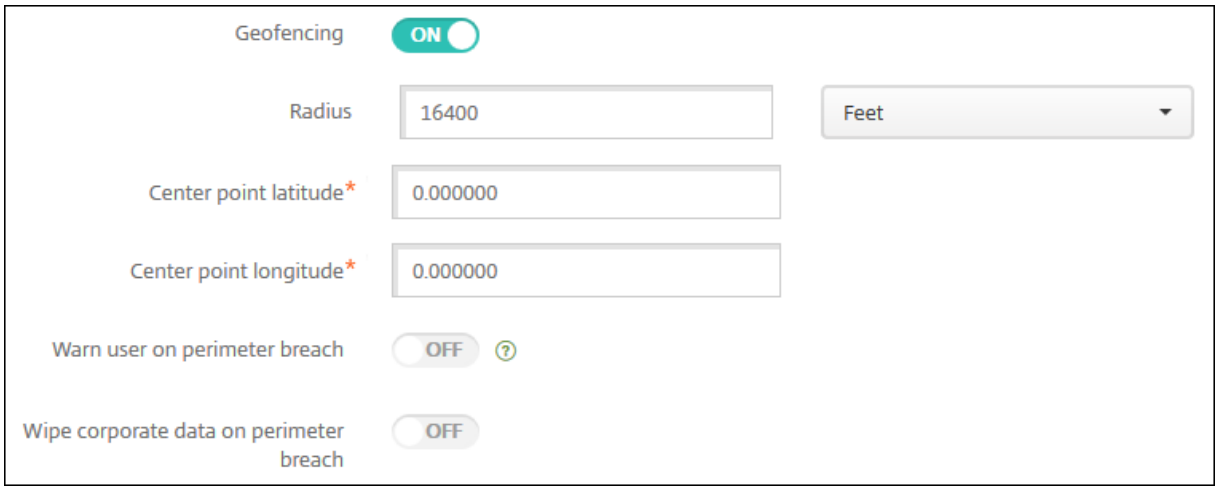
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **Location timeout:** Type a numeral and then, in the list, click **Seconds** or **Minutes** to set how often XenMobile 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, in the list, click **Hours** or **Minutes** to set how long XenMobile tracks the device. Valid values are 1-6 hours or 10-360 minutes. The default is 6 hours.
- **Accuracy:** Type a numeral and then, in the list, click **Meters**, **Feet**, or **Yards** to set how close to a device XenMobile tracks the device. Valid values are 10-5000 yards or meters, or 30-15000 feet. The default is 328 feet.

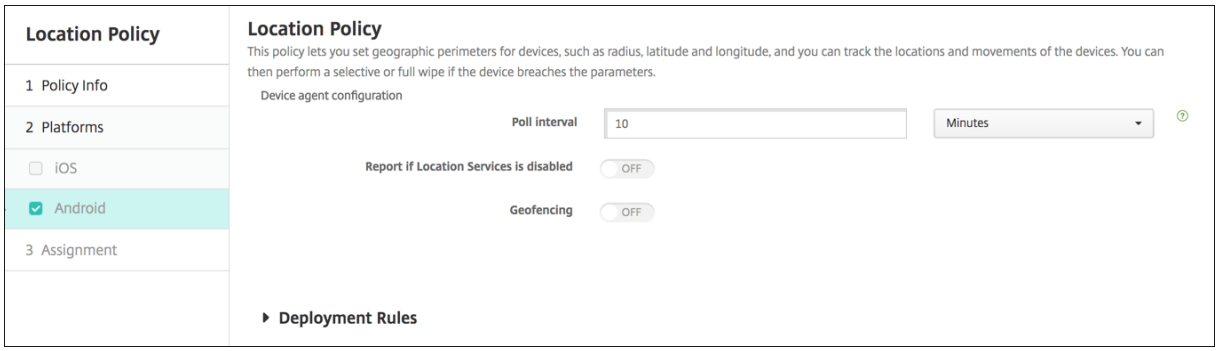
- **Report if Location Services are disabled:** Select whether the device sends a report to XenMobile when GPS is disabled. The default is **Off**.
- **Geofencing**



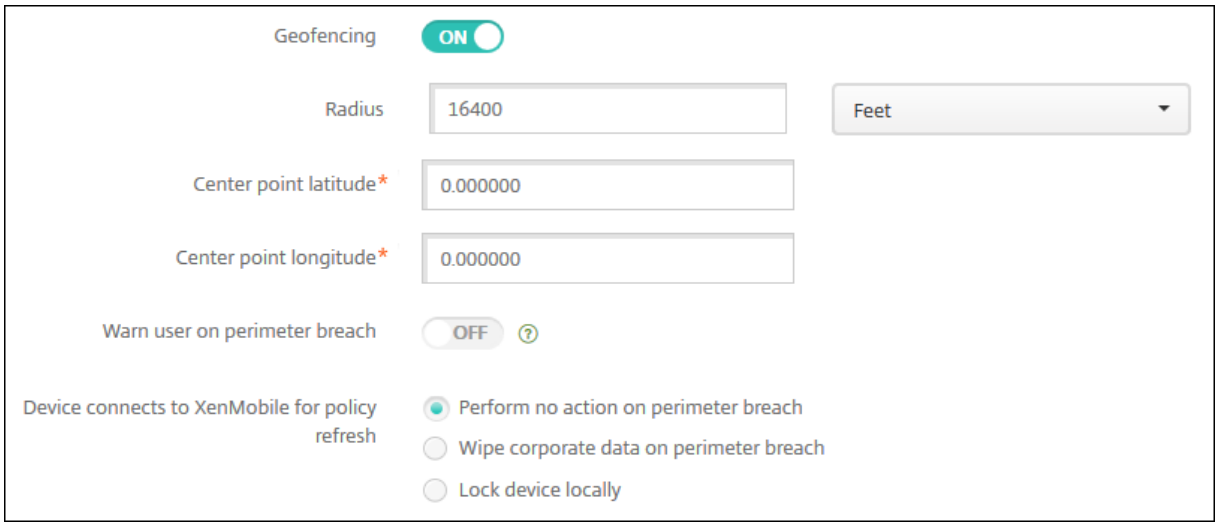
When you enable Geofencing, configure these settings:

- **Radius:** Type a numeral and then, in the list, click the units to be used to measure the radius. The default is 16,400 feet. Valid values for radius are:
  - 164-164000 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 XenMobile 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, in the list, click **Seconds** or **Minutes** to set the length of time to delay before wiping corporate data from users' devices. This gives users an opportunity to return to the allowed location before XenMobile selectively wipes their devices. The default is 0 seconds.

Android settings



- **Poll interval:** Type a numeral and then, in the list, click **Minutes** or **Hours**, or **Days** to set how often XenMobile 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 may adversely affect the device's battery life.
- **Report if Location Services are disabled:** Select whether the device sends a report to XenMobile when GPS is disabled. The default is **Off**.
- **Geofencing**



When you enable Geofencing, configure these settings:

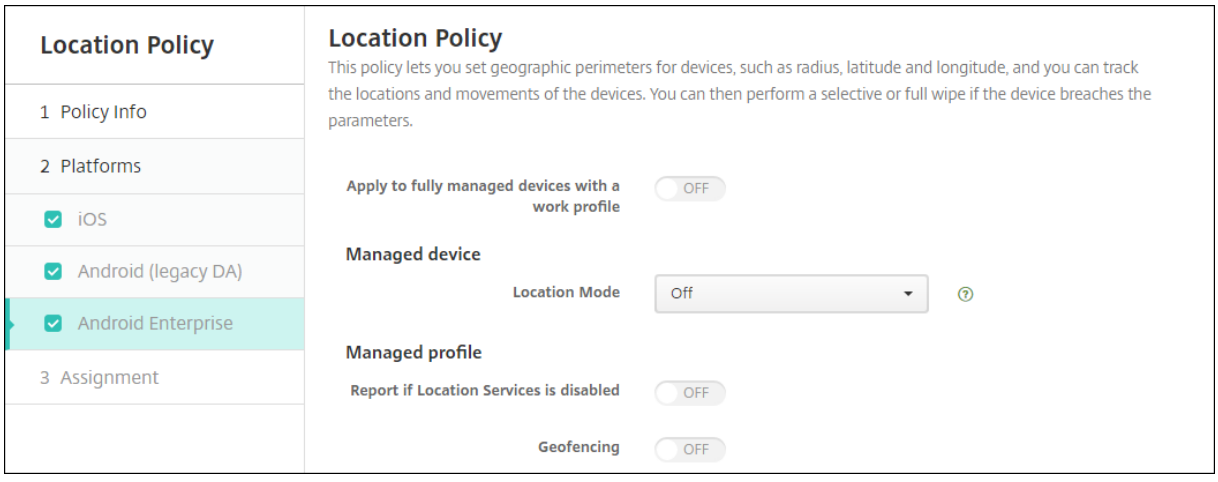
- **Radius:** Type a numeral and then, in the list, click the units to be used to measure the radius. The default is 16,400 feet. Valid values for radius are:
  - 164-164000 feet
  - 1-50 kilometers
  - 50-50000 meters
  - 54-54680 yards
  - 1-31 miles
- **Center point latitude:** Type a latitude, such 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 XenMobile is required to display the warning message.
- **Device connects to XenMobile 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, in the list, click Seconds or Minutes to set the length of time to delay before wiping corporate data from users' devices. This gives users an opportunity to return to the allowed location before XenMobile selectively wipes their devices. The default is 0 seconds.
  - **Delay on lock:** 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, in the list, click Seconds or Minutes to set the length of time to delay before locking users' devices. This gives users an opportunity to return to the allowed location before XenMobile locks their devices. The default is 0 seconds.

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)



Apply to fully managed devices with a work profile

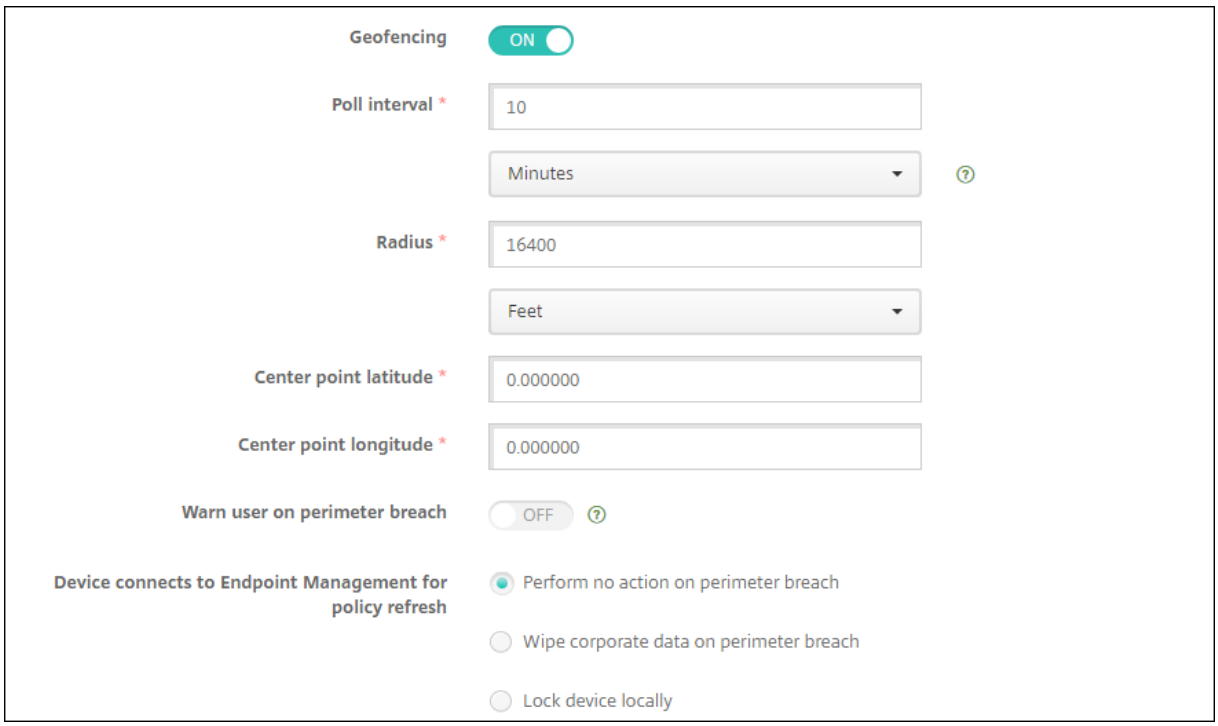
For fully managed devices with work profiles, only the location mode setting is available.

- **Apply to fully managed devices with a work profile:** Allows you to configure the location mode for fully managed devices with work profiles. When this setting is on, configure the location mode setting:
  - **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.

When **Apply to fully managed devices with a work profile** 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:**



When you enable Geofencing, configure these settings:

- **Poll interval:** Type a numeral and then click **Minutes** or **Hours**, or **Days** to set how often XenMobile Server 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, XenMobile Server 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 XenMobile Server is required

to display the warning message.

- **Device connects to XenMobile Server 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 XenMobile Server 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 XenMobile Server locks their devices. The default is **0 seconds**.

Managed profile

- **Report if Location Services are disabled:** Select whether the device sends a report to XenMobile Server when the user turns off GPS. The default is **Off**.
- **Geofencing:** See the settings in this article under Managed device.

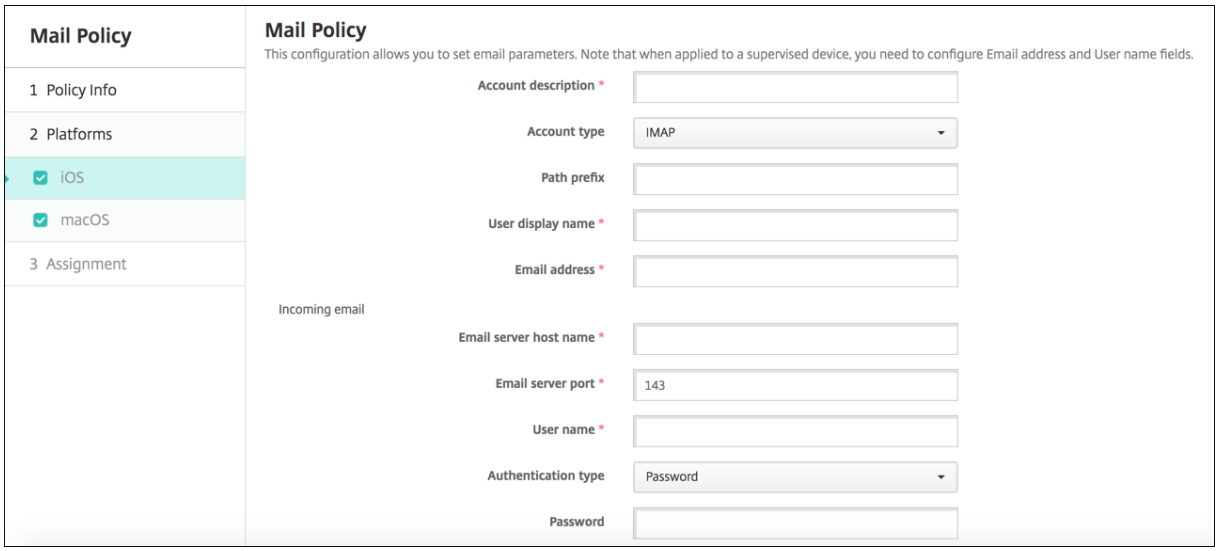
Mail device policy

September 3, 2019

You can add a mail device policy in XenMobile 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



- **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 and to forward and 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 Overrideable:** 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 Overrideable:** 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 Overrideable:** 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 Overrideable:** 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 at a later time, you can 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**.
  - **Profile scope:** For macOS only, choose whether the policy applies on a per **User** level or across the whole **System**.

Managed domains device policy

April 20, 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 8 and later supervised devices, you specify URLs or subdomains to control how users can open documents, attachments, and downloads from the browser. For iOS 9.3 and later supervised devices, you can specify the URLs from which users can save passwords in Safari.

For the steps on setting an iOS device to supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator.

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
example.com	Treat any path under example.com as managed, but not site.example.com/.
foo.example.com	Treat any path under foo.example.com as managed, but not example.com/ or bar.example.com/.
*.example.com	Treat any path under foo.example.com or bar.example.com as managed, but not example.com/.
example.com/sub	Treat example.com/sub and any path under it as managed, but not example.com/.
foo.example.com/sub	Treat any path under foo.example.com/sub as managed, but not example.com, example.com/sub, foo.example.com/, or bar.example.com/sub.
*.example.com/sub	Treat any path under foo.example.com/sub or bar.example.com/sub as managed, but not example.com or foo.example.com/.

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.

MDM options device policy

April 20, 2021

You can create a device policy in XenMobile to manage Find My Phone/iPad Activation Lock on supervised iOS 7.0 and later phone devices. For the steps on setting an iOS device to supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator.

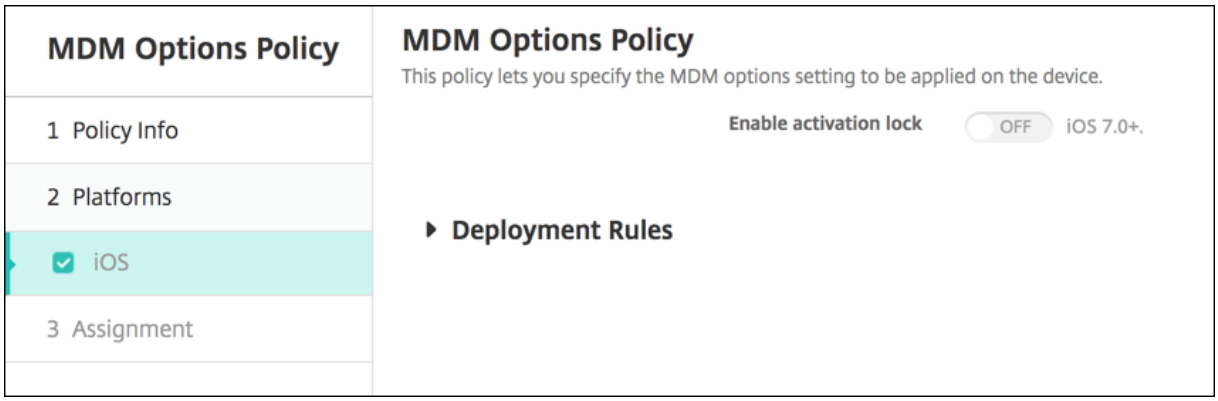
Activation Lock is a feature of Find My iPhone/iPad that prevents reactivation of a lost or stolen supervised device. Activation Lock requires the user Apple ID and password before anyone can turn off Find My iPhone/iPad, erase the device, or reactivate the device. For the devices that your organization owns, bypassing an Activation Lock is necessary to, for example, reset or reallocate devices.

To enable Activation Lock, you configure and deploy the XenMobile MDM Options device policy. You can then manage a device from the XenMobile 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 XenMobile 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 iTunes account credential, you can bypass that step by issuing the Activation Lock Bypass security action from the XenMobile 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 in the Security actions article.

Organization information device policy

July 3, 2018

You can add a device policy in XenMobile to specify your organization's information for alert messages that are pushed from XenMobile to iOS devices. The policy is available for iOS 7 and later 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 XenMobile.
- **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.

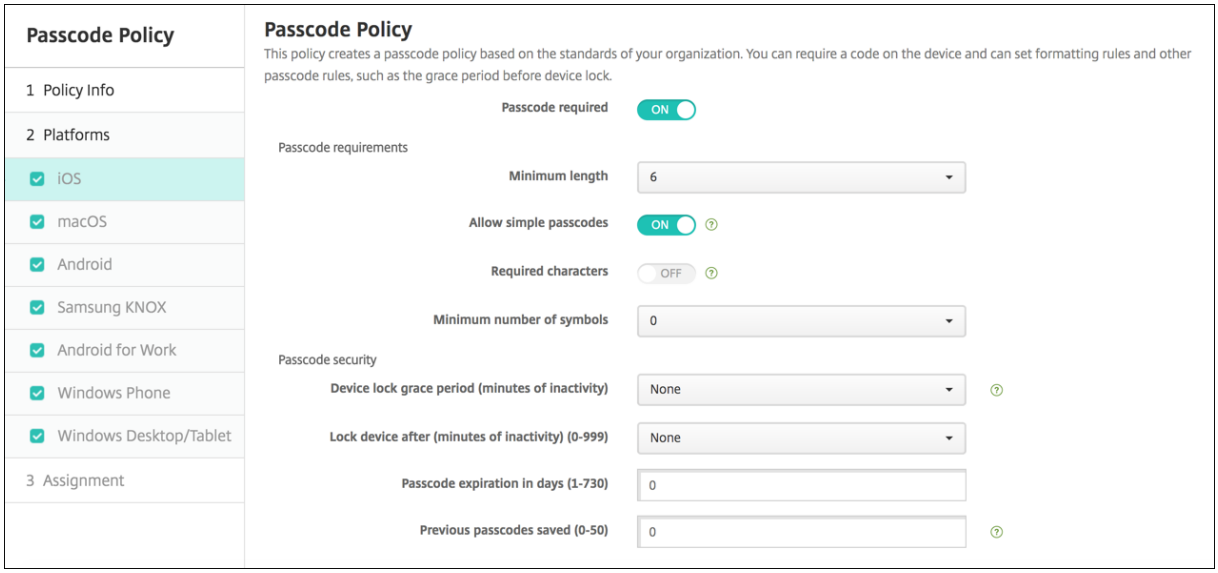
Passcode device policy

August 24, 2020

You create a passcode policy in XenMobile based on your organization's standards. You can require passcodes on users' devices and can set various formatting and passcode rules. You can create policies for iOS, macOS, Android, Samsung KNOX, Android Enterprise, 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.

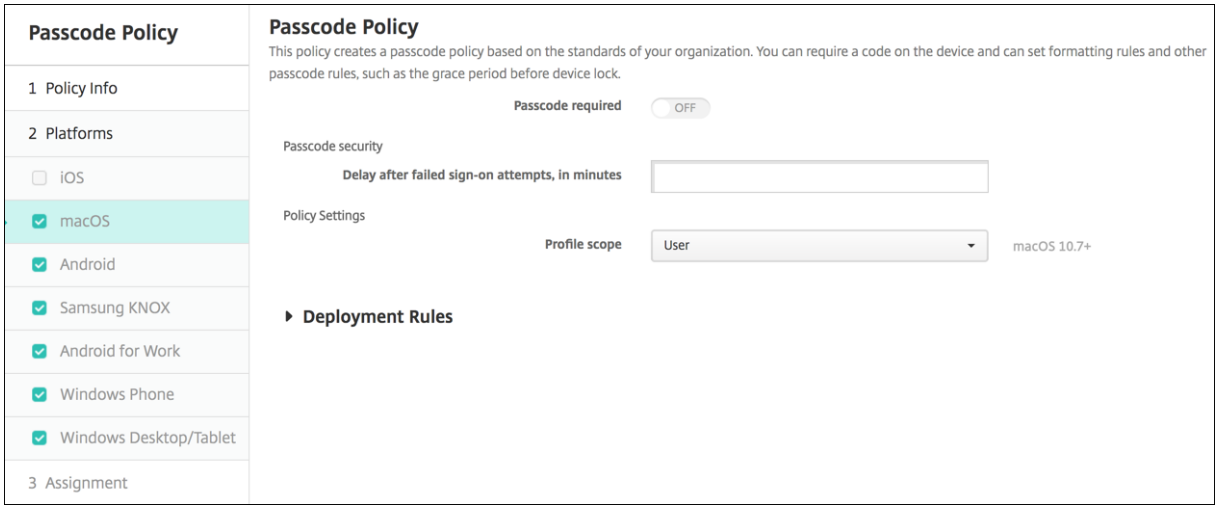
iOS settings



- **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 (minutes of 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 fully wiped. The default is **Not defined**.

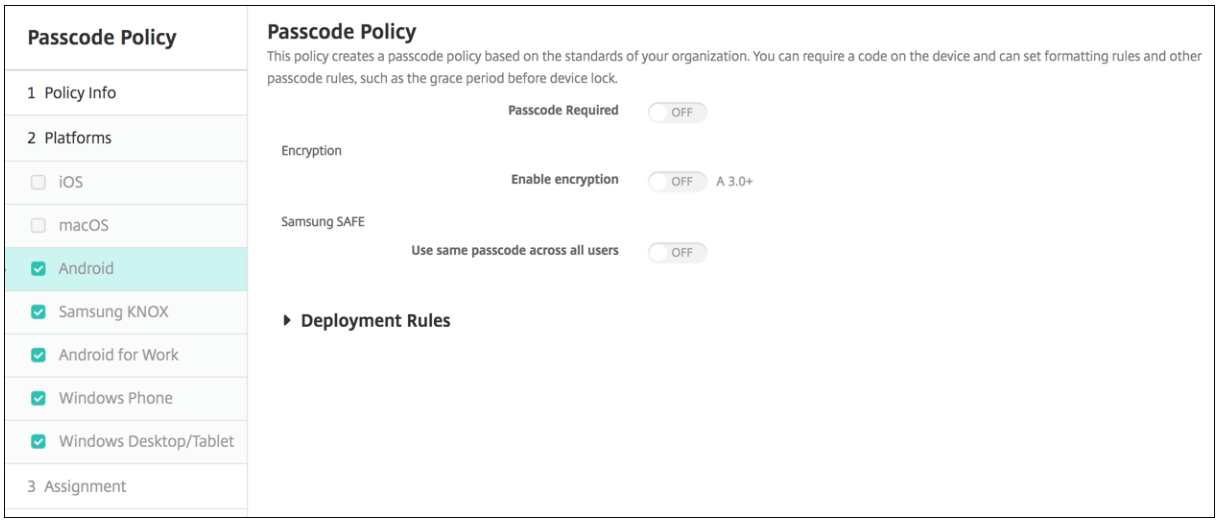
macOS settings



- **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 you do not enable **Passcode required**, 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 (minutes of 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 locked. The default is **Not defined**.
  - **Delay after failed sign-on attempts, in minutes:** Type the number of minutes to delay before allowing a user to reenter a passcode.
  - **Force passcode reset:** The next time a user authenticates, they must reset their passcode.
- **Policy settings**
  - **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



> **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.

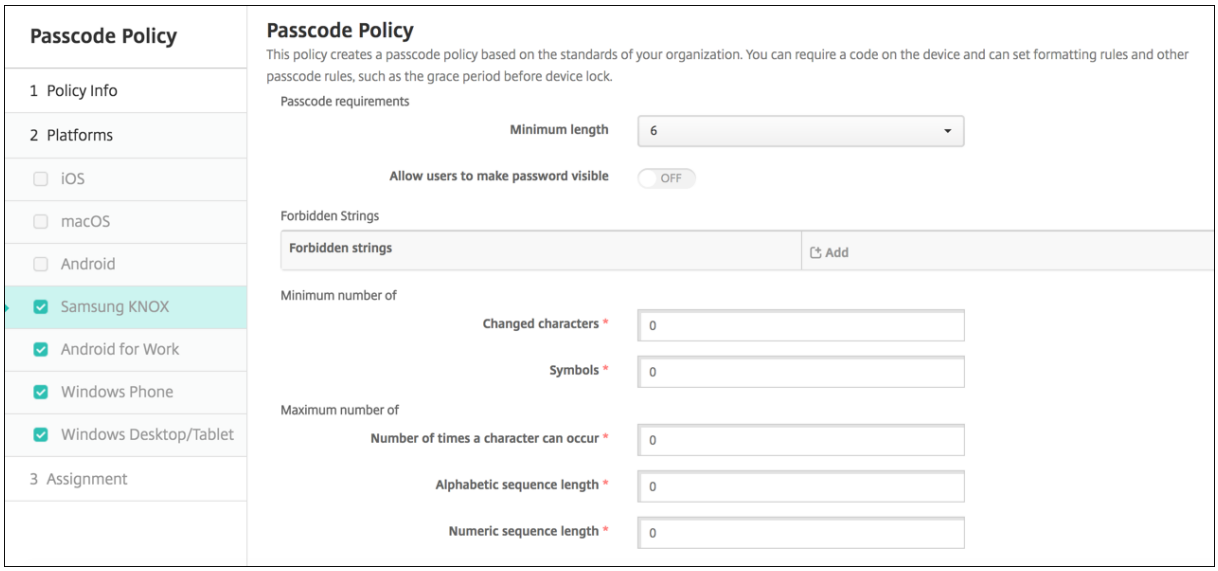
- **Passcode requirements**
  - **Minimum length:** In the list, click the minimum passcode length. The default is 6.
  - **Biometric recognition:** Select whether to enable biometric recognition. If you enable this option, the Required characters field is hidden. The default is **Off**.
  - **Required 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. This option is available for Android 3.0 and later. 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 (minutes of 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. This option is available for Android 3.0 and later. 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 for the hour or more that encryption takes. If they interrupt the encryption process, they may lose some or all of the data on their devices. After a device is encrypted, the process cannot 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**.
  - **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**.
  - **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 authenicate using a fingerprint.
    - **Allow iris**. Select to allow users to authenicate 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 may not use.
    - Click **Save** to add the string or click **Cancel** to cancel adding the string.

Samsung KNOX settings

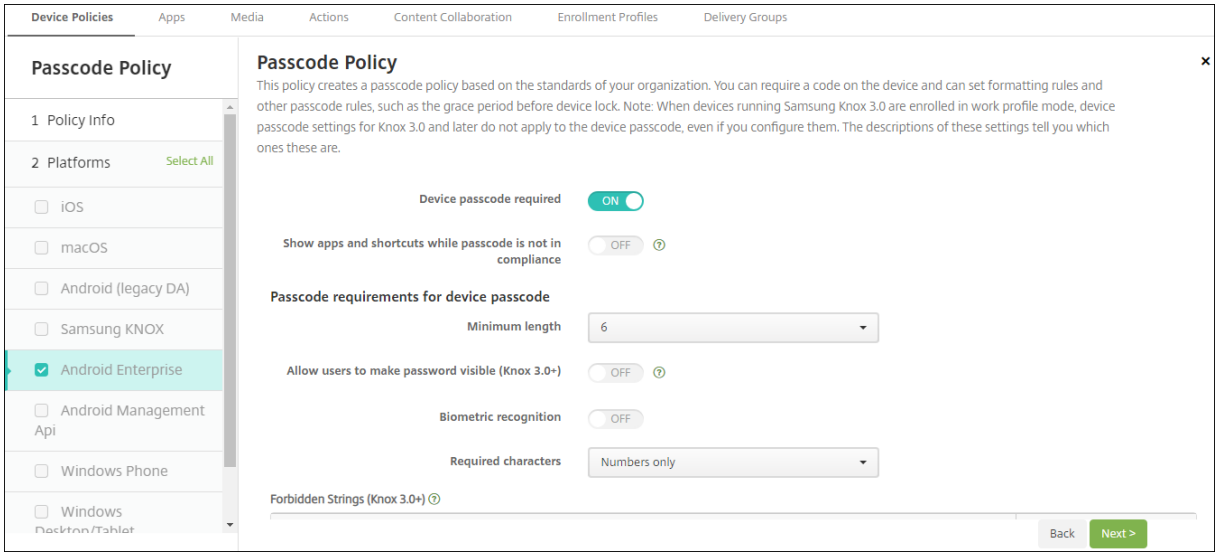


- **Passcode requirements**
  - **Minimum length:** In the list, click the minimum passcode length. The default is **6**.
  - **Allow users to make password visible:** Select whether to let users make the password visible.
  - **Forbidden strings:** You create forbidden strings to prevent users from 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 may not 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 previous passcode. The default is **0**.
  - **Symbols:** Type the minimum number of required symbols in a passcode. The default is **0**.
- **Maximum number of**
  - **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 (minutes of 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.
- **If the number of failed sign on attempts is exceeded, the device is locked:** 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**.
- **If the number of failed sign on attempts is exceeded, the device is wiped:** In the list, click the number of times a user can fail to sign on successfully, after which the KNOX container (along with the KNOX data) is wiped from the device. Users need to reinitialize the KNOX container after the wiping occurs.The default is **Not defined**.

Android Enterprise settings



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 are enrolled as work profile devices, device passcode settings for Knox 3.0 and later do not apply to the device passcode, even if you configure them.

- **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 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 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 charac-

ters 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.
  - **Number of 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 (minutes of inactivity) (0-999):** Specifies the number of minutes a device can be inactive before it is locked. The default is **None**.
  - **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**.

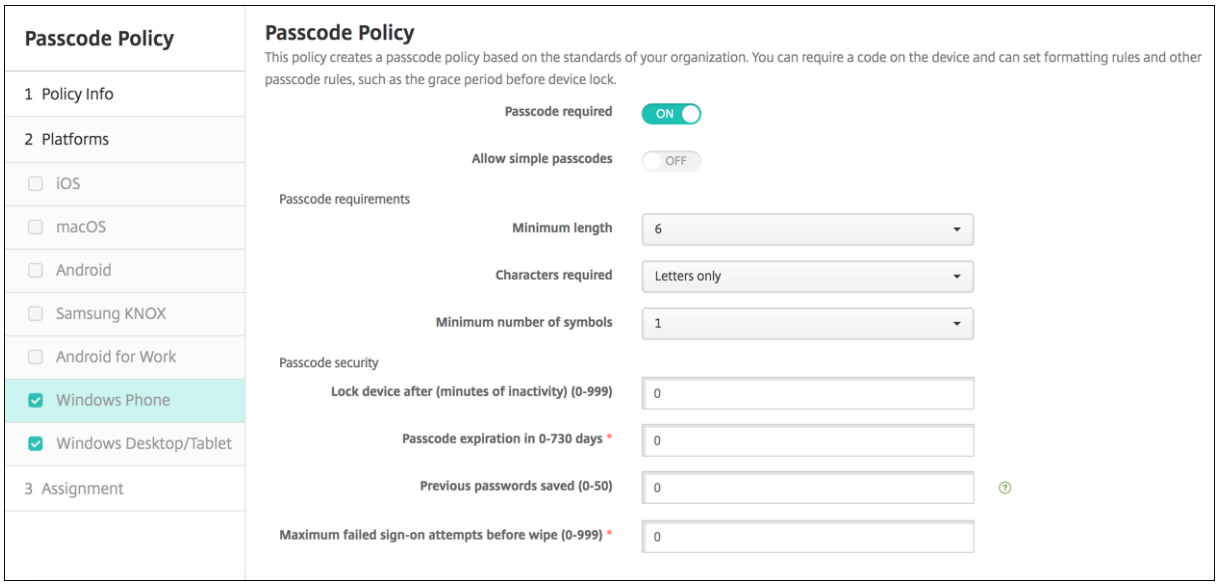
- **Forbidden strings:** For device running Knox 3.0 and later that have a valid Knox license key configured. Specifies strings users can't use as passcodes. You create forbidden strings to prevent users from using insecure strings that are easy to guess like "password", "pwd", "welcome", "123456", "111111", 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.
  - **Number of 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.
- **Enable unified passcode:** If **On**, users use one passcode for their device and work profile. If **Off**:
  - Users must use different passcodes for their device and work profile.
  - The **Use one lock** setting on the device, which users set if they want to use one passcode for their device and work profile, is disabled. User can't enable it.
  - If the passcode requirement for the work profile security challenge is more complex

than the device passcode: Users with the **Use one lock** setting enabled are prompted to change their work profile passcodes.

The default is **Off**. Available starting with Android 9.0.

- **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 is wiped from the device. Users need to reinitialize the work profile after the wiping occurs. Default is **Not defined**.
  - **Lock container after (minutes of inactivity):** Specifies the number of minutes a device can be inactive before the work profile is locked. The default is **None**.
  - **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**.

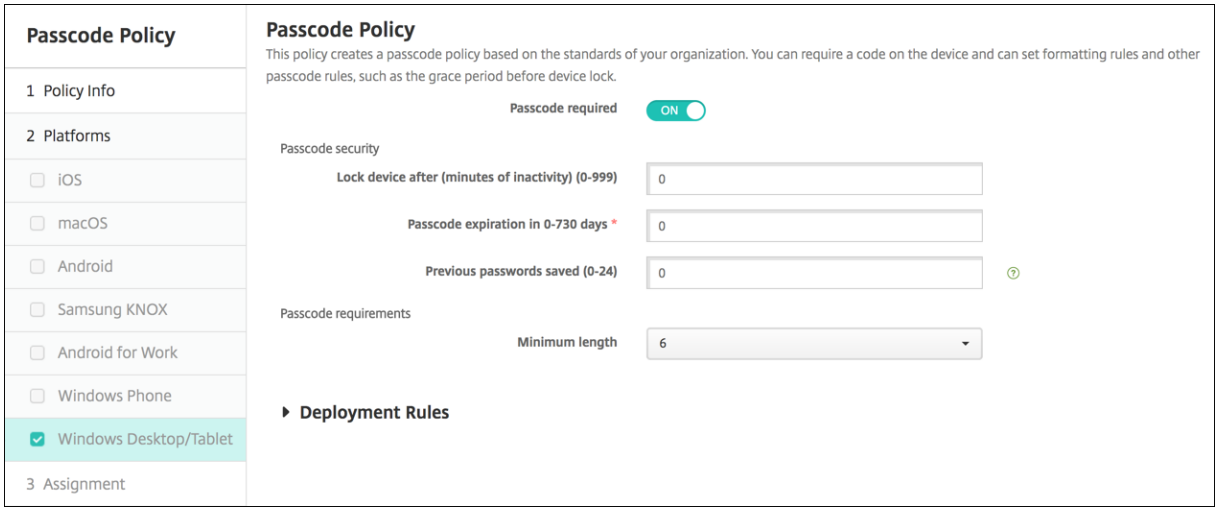
Windows Phone settings



- **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 options 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 (minutes of inactivity):** Type the number of minutes a device can be inactive before it is locked. The default is **0**.
  - **Passcode expiration in 0-730 days:** 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.
  - **Maximum failed sign-on attempts before wipe (0-999):** 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



- **Disallow convenience logon:** Select whether to allow users to access their devices with picture passwords or biometric logons. The default is **Off**.
- **Minimum passcode length:** In the list, click the minimum passcode length. The default is **6**.
- **Maximum passcode attempts before wipe:** In the list, click the number of times a user can fail to sign in successfully after which corporate data is wiped from the device. The default is **4**.
- **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.

- **Passcode history: (1-24):** Type the number of used passcodes to save. Users are unable to use any passcode found in this list. Valid values are 1-24. You must enter a number between 1 and 24 in this field. The default is **0**.
- **Maximum inactivity before device lock in minutes (1-999):** Type the length of time in minutes that a device can be inactive before it is locked. Valid values are 1-999. You must enter a number between 1 and 999 in this field. The default is **0**.

Personal hotspot device policy

July 3, 2018

You can allow users to connect to the Internet when they are not in range of a WiFi network by using the cellular data connection through their iOS devices' personal hotspot functionality. Available on iOS 7.0 and later.

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.

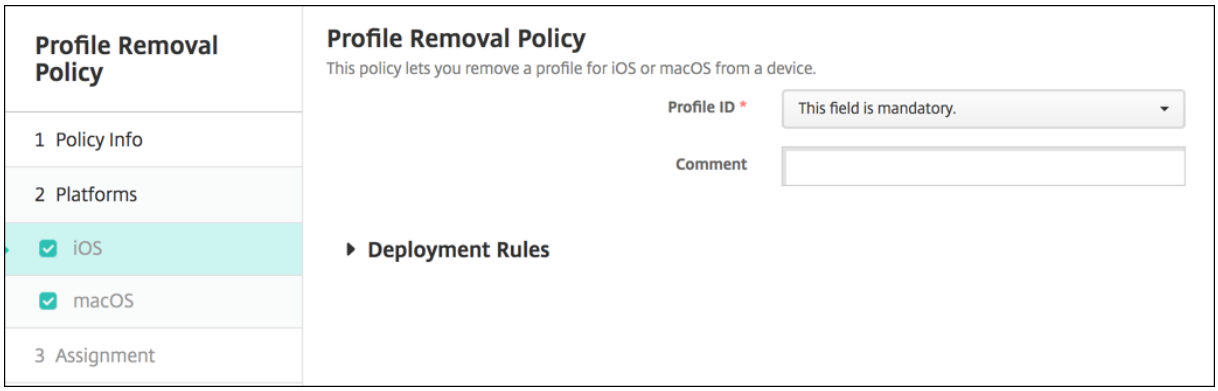
Profile Removal device policy

July 3, 2018

You can create an app profile removal device policy in XenMobile. The policy, when deployed, removes the app profile from users' iOS or macOS devices.

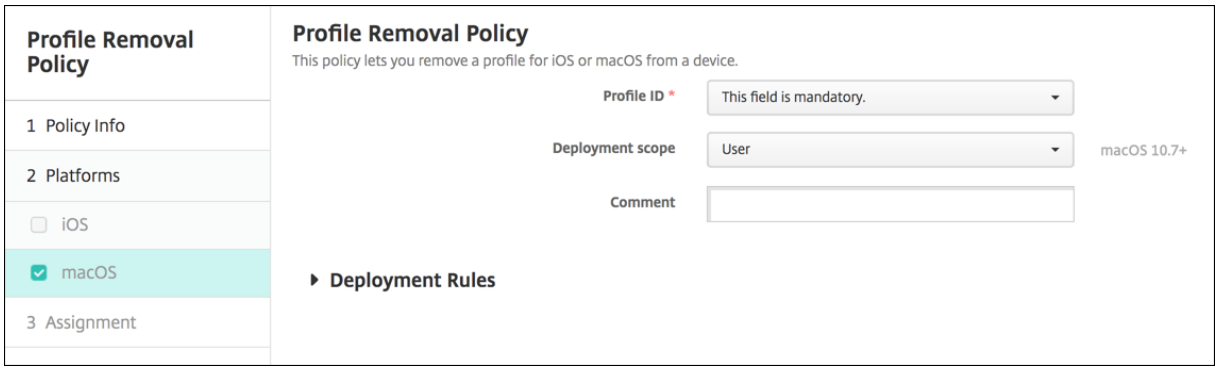
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **Profile ID:** In the list, click the app profile ID. This field is required.
- **Comment:** Type an optional comment.

macOS settings



- **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 8, 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.

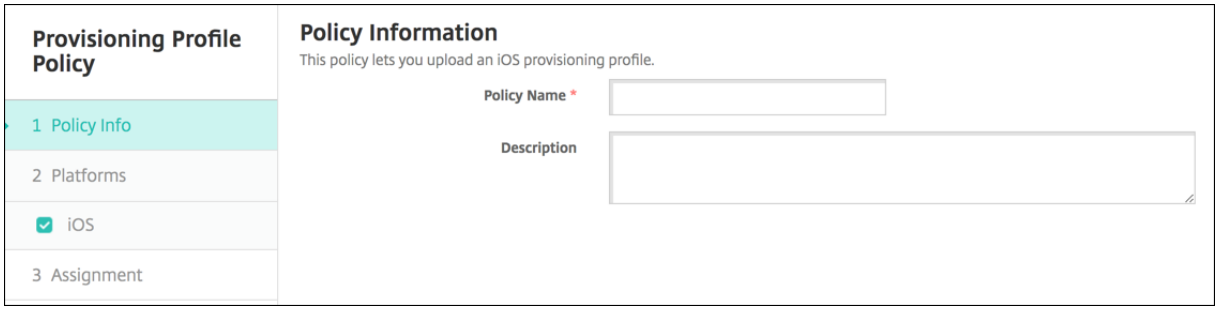
The primary problem with provisioning profiles is that they expire one year after they are generated on the Apple Developer Portal and you must keep track of the expiration dates for all your provision-

ing 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 XenMobile 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

September 11, 2020

You can remove iOS provisioning profiles with device policies. For more information on provisioning profiles, see Provisioning profile device policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **iOS provisioning profile:** In the list, click the provisioning profile you want to remove.

- **Comment:** Optionally, add a comment.

Proxy device policy

May 27, 2021

You can add a device policy in XenMobile to specify global HTTP proxy settings for devices running Windows Mobile/CE andiOS 6.0 or later. 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 To place an iOS device in Supervised mode by using the Apple Configurator 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**. This option is available only on iOS 7.0 and later.
- **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.

Windows Mobile/CE settings

- **Network:** In the list, click the network type to use. The default is **Built-in office**. Possible options are:
  - User-defined office
  - User-defined Internet
  - Built-in office
  - Built-in Internet
- **Network:** In the list, click the network connection protocol to use. The default is **HTTP**. Possible options are:
  - HTTP
  - WAP
  - Socks 4
  - Socks 5
- **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. The default is **80**.
- **User name:** Type an optional user name to authenticate to the proxy server.
- **Password:** Type an optional password to authenticate to the proxy server.
- **Domain name:** Type an optional domain name.
- **Enable:** Select whether to enable the proxy. The default is **On**.

Registry device policy

July 3, 2018

The Windows Mobile/CE registry stores data about apps, drivers, user preferences, and configuration settings. In XenMobile, you can define the registry keys and values that let you administer Windows Mobile/CE devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows Mobile/CE settings

For each registry key or registry key/value pair you want to add, click **Add** and do the following:

- **Registry key path:** Type the full path for the registry key. For example, type **HKEY_LOCAL_MACHINE\Softwa** to specify the route to the Windows key from the HKEY_LOCAL_MACHINE root key.
- **Registry value name:** Type the name for the registry key value. For example, type **ProgramFilesDir** to add that value name to the registry key path HKEY_LOCAL_MACHINE\Software\Microsoft\Window If you leave this field blank, it means that you are adding a registry key and not a registry key/value pair.
- **Type:** In the list, click the data type for the value. The default is **DWORD**. Possible options are:
  - **DWORD:** A 32-bit unsigned integer.
  - **String:** Any string.
  - **Extended string:** A string value that can contain environment variables like %TEMP% or %USERPROFILE%.
  - **Binary:** Any arbitrary binary data.
- **Value:** Type the value associated with Registry value name. For example, to specify the value of ProgramFilesDir, type **C:\Program Files**.
- Click **Save** to save the registry key information or click **Cancel** to not save the registry key information.

Remote support device policy

September 11, 2020

> **Note:**
>
> For on-premises XenMobile Server deployments: Remote support enables your help desk representatives to take remote control of managed Windows CE and Android mobile devices. Screen cast is supported on Samsung KNOX devices only.
>
> Remote support isn't supported for clustered on-premises XenMobile Server deployments.
>
> For more information, see Support options and Remote Support.

You create a remote support policy in XenMobile to give you remote access to supported Windows and Android devices. You can configure two types of support:

- **Basic**, which lets you view diagnostic information about the device, such as system information, processes that are running, task manager (memory and CPU usage), installed software folder contents, and so on.
- **Premium**, which lets you remotely control the device screen, including:
  - control colors (in either the main window, or in a separate, floating window)

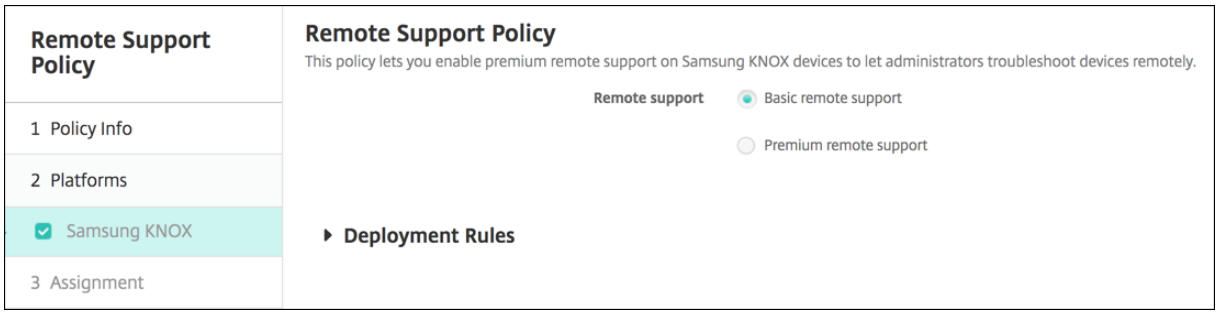
- establish a Voice-over-IP session (VoIP) between the help desk and the user
- configure settings
- establish a chat session between the help desk and the user.

To implement this policy, you must do the following:

- Install the XenMobile Remote Support app in your environment.
- Configure a remote support app tunnel. For details, see App tunneling device policies.
- Configure a Samsung KNOX remote support device policy as described in this topic.
- Deploy both the app tunnel remote support policy and the Samsung KNOX remote support policy to user devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Android and Windows CE settings



- **Remote support:** Select **Basic remote support** or **Premium remote support**. The default is **Basic remote support**.

Restrictions device policy

July 28, 2021

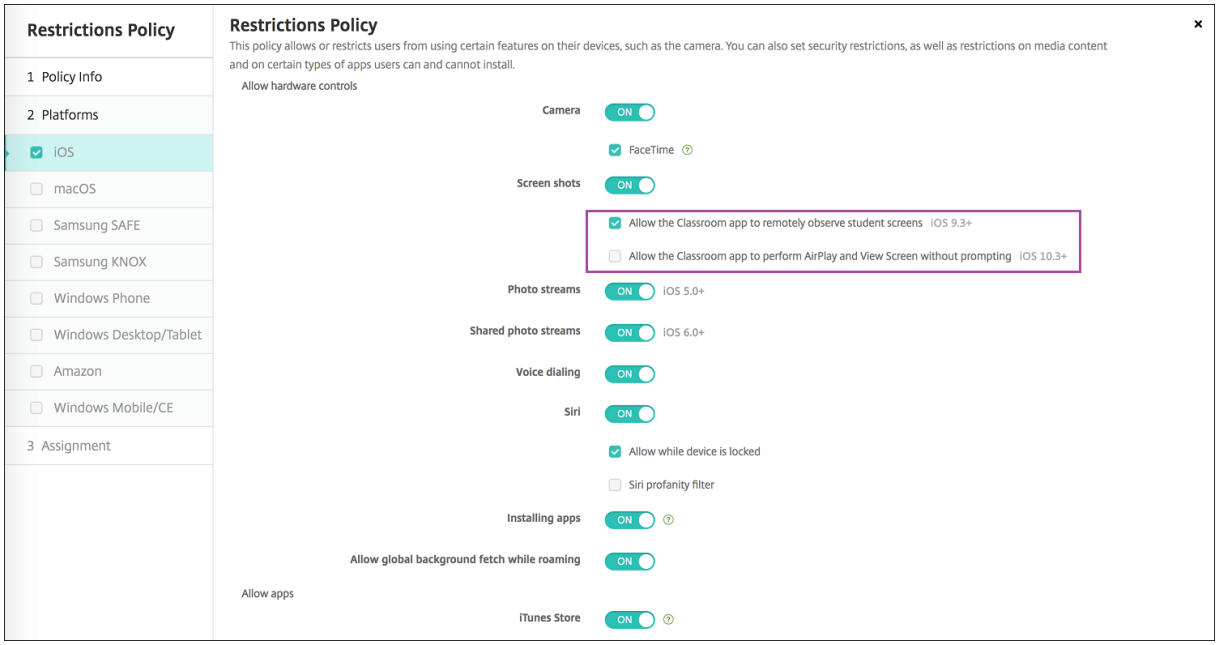
The Restrictions device policy allows or restricts certain features or functionality on user devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and restrictions on the types of apps users can and cannot install. Most of the restriction settings 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*.

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.

> **Tip:**
>
> 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.
>
> **Screen shots**. If **On**, the user can take screen shots on their device. If **Off**, the user cannot take screen shots on their device.

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 XenMobile console Restrictions policy page.

iOS restrictions policy settings may 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.

As noted 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:

- If a supervised iOS 13+ device enrolls in XenMobile, the settings apply to the device.
- If an unsupervised iOS 13+ device enrolls in XenMobile, the settings don't apply to the device.

- If an iOS 12 (or lower) device already enrolled in XenMobile 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 To place an iOS device in Supervised mode by using the Apple Configurator.

Setting	User Enrollment	Unsupervised	Supervised
Allow hardware controls			
Camera	No	Yes	Yes
FaceTime	No	No (new in iOS 13)	Yes
Screenshots	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
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 (new in iOS 13)	Yes
Allow global background fetch while roaming	No	Yes	Yes
Allow apps			
iTunes Store	No	No (new in iOS 13)	Yes
In-app purchases	No	Yes	Yes

Setting	User Enrollment	Unsupervised	Supervised
Require iTunes password for purchases	No	Yes	Yes
Safari	No	No (new in iOS 13)	Yes
Autofill	No	No (new in iOS 13)	Yes
Force fraud warning	Yes	Yes	Yes
Enable JavaScript	No	Yes	Yes
Block pop-ups	No	Yes	Yes
Accept cookies	No	Yes	Yes
Network - Allow iCloud actions			
iCloud documents and data	No	No (new in iOS 13)	Yes
iCloud backup	No	Yes	Yes
iCloud photo keychain	No	Yes	Yes
iCloud photo library	No	Yes	Yes
Security - Force			
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
Security - Allow			
Accepting untrusted SSL certificates	No	Yes	Yes

Setting	User Enrollment	Unsupervised	Supervised
Automatic update to certificate trust settings	No	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
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
Supervised only settings - Allow			

Setting	User Enrollment	Unsupervised	Supervised
Erase all content and settings	No	No	Yes
Configuring restrictions	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
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 (new in iOS 13)	Yes
Add friends	No	No	Yes
Multiplayer gaming	No	No (new in iOS 13)	Yes
Modifying account settings	No	No	Yes

Setting	User Enrollment	Unsupervised	Supervised
Modifying app cellular data settings	No	No	Yes
Modifying app cellular data settings	No	No	Yes
Modifying Find My Friends settings	No	No	Yes
Pairing with non-Configurator hosts	No	No	Yes
Predictive keyboards	No	No	Yes
Keyboard auto-corrections	No	No	Yes
Keyboard spell-check	No	No	Yes
Definition lookup	No	No	Yes
Single App bundle ID			
News	No	No	Yes
Apple Music service	No	No	Yes
iTunes Radio	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
Join only WiFi networks installed by a WiFi policy	No	No	Yes

Setting	User Enrollment	Unsupervised	Supervised
Allow the Classroom app to perform AirPlay and View Screen without prompting	No	No	Yes
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

Setting	User Enrollment	Unsupervised	Supervised
Enforced software update delay	No	No	Yes
Force classroom request permission to leave classes	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
Security - Show in lock screen			
Control Center	Yes	Yes	Yes
Notification	Yes	Yes	Yes
Today view	Yes	Yes	Yes
Media content - Allow			
Explicit music, podcasts, and iTunes U material	No	No (new in iOS 13)	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.
  - **Screenshots:** 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.
  - **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**

  - **iTunes Store:** Allow users to access the iTunes Store. For supervised iOS devices.
  - **In-app purchases:** Allow users to make in-app purchases.
    * **Require iTunes 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.
  - **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 as well as 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 To place an iOS device in Supervised mode by using the Apple Configurator.

  - **Erase all content and settings:** Allow users to erase all content and settings from their devices.
  - **Configuring restrictions:** Allow users to configure parental controls on their devices.
  - **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.
- **Modifying Find My Friends settings:** Allow users to change their Find My Friends settings.
- **Pairing with non-Configurator hosts:** Allow admin 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 that are 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.
- **iTunes Radio:** Allow users to use iTunes Radio.
- **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**.
- **Join only WiFi networks installed by a WiFi 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 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.

- **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 automatic date and time:** Allows you to automatically set the date and time on supervised devices. If **On**, device users can't turn off **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 AirDrop Passwords feature. Default is **On**. Available as of iOS 12.

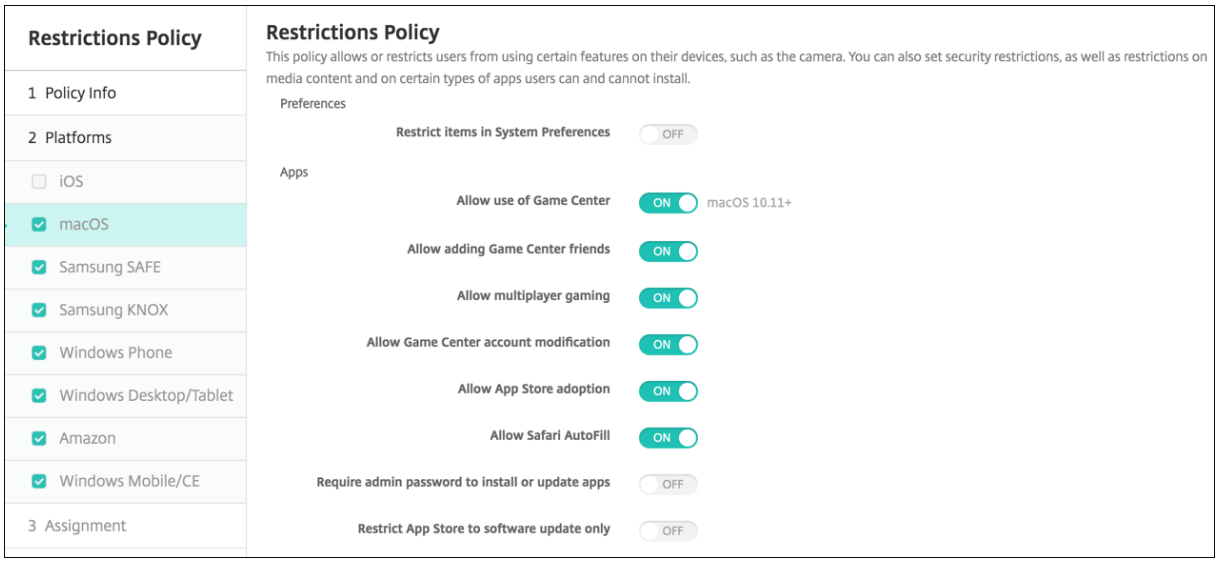
- **Security - Show in lock screen**
  - **Control Center:** Allow access to Control Center on the lock screen. Control Center lets users easily modify Airplane Mode, Wi-Fi, Bluetooth, Do Not Disturb Mode, and Lock Rotation settings.
  - **Notification:** Allow notifications on the lock screen.
  - **Today 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



- **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
        - Diction & 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**. Repeat this step for each app allowed to launch.
  * **Disallowed Folders:** Click **Add**, type the file path to a folder to which 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:** Allow or restrict which Dashboard widgets, such as World Clock or Calculator, users are allowed to run. 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, web sites, 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 microblogging 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.

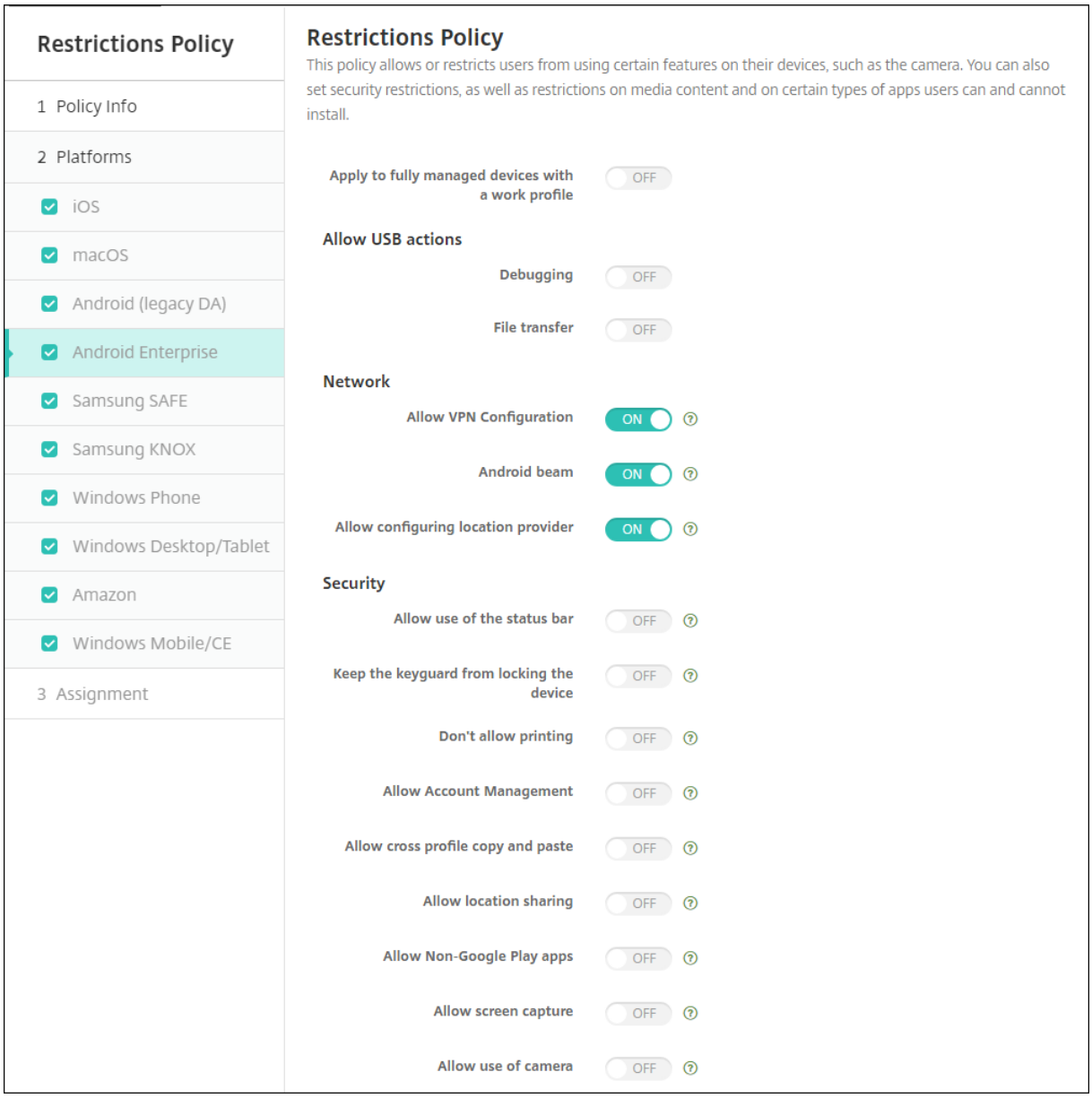
- **Functionality**
  - **Lock desktop picture:** Select whether users can change the desktop picture. The default is **Off**, which means users can change the desktop picture.
  - **Allow use of camera:** Select whether users can use the camera on their Macs. The default is **Off**, which means users 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, iTunes, 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 **Off**, 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.
- **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**. Available as of macOS 10.14.
- **Password proximity requests:** Optional. If disabled, users' devices don't request passwords from nearby devices. Default is **On**. Available as of macOS 10.14.
- **Password Sharing:** Optional. If disabled, users can't share their passwords using the Airdrop Passwords feature. Default is **On**. Available as of macOS 10.14.

Android settings

- **Camera:** Allow users to use the camera on their devices. If **Off**, the camera is disabled. Defaults to **On**.

Android Enterprise settings



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 or later 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.

Citrix recommends that you use Samsung Knox 3.4 or higher for the latest Samsung Knox management features.

- **Apply to fully managed devices with a work profile:** Allows restrictions policy settings to be configured for fully managed devices with work profiles. 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.
- **Manage 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** is off, configure these settings:

- **Allow USB actions**
  - **Debugging:** Allows debugging over USB. Default is **Off**.
  - **File transfer:** Allows file transfers over USB. Default is **Off**.
- **Network**
  - **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**.
  - **Android beam:** Allow users to send web pages, photos, videos, or other content from their devices to another device using Near Field Communication (NFC). For MDM 4.0 and later. Default if **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:** Allows location sharing. For managed profiles, the device owner can override this setting. Default is **Off**.

    > **Tip:**
    >
    > You can create Location device policies in XenMobile to enforce geographic boundaries. See Location device policy.
- **Security**
  - **Allow use of the status bar:** If set to **On**, this setting enables the status bar on managed devices and dedicated devices (also known as COSU devices). This 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**.
  - **Keep the keyguard from locking the device:** If set to **On**, this setting disables the keyguard on the lock screen on managed devices and dedicated devices (also known as COSU devices). Default is **Off**.
  - **Don't allow printing:** If **On**, the setting prevents users from printing to any printer accessible from the user device. The default is **Off**. Available for: Android 9 and later.
  - **Allow Account Management:** Allows account to be added to in work profile and managed devices. Default is **Off**.

- **Allow cross profile copy and paste:** Allows or prevents use of the clipboard to copy and paste between apps in the Android Enterprise profile and apps in the personal area. Default is **Off**.
- **Allow location sharing:** Allows location sharing. For managed profiles, the device owner can override this setting. Default is **Off**.
- **Allow Non-Google Play apps:** Allows the installation of apps from stores other than Google Play. 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 user control of application settings:** Allows users to uninstall apps, disable apps, clear cache and data, force stop any app, and clear defaults. Default is **Off**.
- **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 whose widgets will be allowed:** 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**.
- **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 managed configurations policy 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, XenMobile 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 user to configure user credentials:** Specify whether users can configure credentials in the managed keystore. Default is **On**.

- **Fully Managed Device**
  - **Allow multiple users:** Allows multiple users to use a device (MDM 4.0 and later). Default is **On**.
  - **Allow roaming:** Allows users to use cellular data while roaming. The default is OFF, which disables roaming on users' devices. Default is **Off**. When this setting is on, these settings are available for Samsung SAFE devices:
    - **Data:** Allow users to use cellular data for data.
    - **Push:** Allow users to use cellular data for pushing.
    - **Sync:** Allow users to use cellular data for syncing.
    - **Voice calls:** Allow users to use cellular data for voice calls.
  - **Allow SMS:** Allows users to send and receive SMS messages. Default is **Off**.
  - **Backup:** Allows users to back up application and system data on their devices. Default is **On**.
  - **Bluetooth:** Allows users to use Bluetooth. Default is **On**.
  - **Date Time Change:** Allows users to change the date and time on their devices. Default is **On**.
  - **Factory reset:** Allows users to do a factory reset on their devices. Default is **On**.
  - **Mass storage:** Allows transfer of large data files between users' devices and a computer over a USB connection. Default is **On**.
  - **Microphone:** Allows users to use the microphone on their devices. Default is **On**.
  - **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:
    - **USB:** Allows users to share a mobile data connection with another device using their USB connection.
    - **Bluetooth:** Allows users to share a mobile data connection with another device using their Bluetooth connection.
    - **WiFi:** Allows users to share a mobile data connection with another device using their WiFi connection.
  - **WiFi:** Allows users to connect to WiFi networks. Default is **On**. When this setting is on, these settings are available:
    - **Direct:** Allows users to connect directly to another device through their WiFi connec-

tion. For Samsung devices only. For MDM 4.0 and later.
    * **State Change:** Allows apps to change WiFi connectivity state.

- **Samsung SAFE: 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. Default is **On**.
  - **Allow Emergency Call 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 is in contrast to full disk encryption, which encrypts all data, including settings, application data, downloaded files and applications, media, and other files. Default is **On**.
  - **Common Criteria Mode:** Places device into Common Criteria Mode. The Common Criteria configuration enforces stringent security processes. Default is **On**.
  - **DOD boot banner:** Displays a DoD approved system use notification message or banner when users' devices are restarted. Default is **Off**.
  - **Settings changes:** Allows users to change settings on their fully managed devices. Default is **On**.
  - **Over The Air Upgrade:** Allows users' devices to receive software updates wirelessly (MDM 3.0 and later). Default is **On**.
  - **Background data:** Allows apps to sync data in the background. for fully managed devices. Default is **On**.
  - **Clipboard:** Allow users to copy data to the clipboard on their devices.
    * **Clipboard share:** Allow users to share clipboard content between their devices and a computer (MDM 4.0 and later).
  - **Home key:** Allows users to use the **Home** key on their fully managed devices. Default is **On**.
  - **Mock location:** Allows users to fake their GPS location. For fully managed devices. Default is **On**.
  - **NFC:** Allows users to use NFC on their fully managed devices (MDM 3.0 and later). Default is **On**.
  - **Power Off:** Allows users to turn off their fully managed devices (MDM 3.0 and later). Default is **On**.
  - **SD card:** Allows users to use an SD card, if available, with their devices. Default is **On**.
  - **Voice dialer:** Allows users to use the voice dialer on their devices (MDM 4.0 and later). Default is **On**.
  - **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**.
  - **SBeam:** Allows users to share content with others using NFC and Wi-Fi Direct (MDM 4.0

and later). Default is **On**.

- **SVoice:** Allows users to use the intelligent personal assistant and knowledge navigator on their devices (MDM 4.0 and later). Default is **On**.

- **Samsung SAFE: Allow apps**
  - **Face Recognition:** Allows users to use the face recognition app. Default is **On**.
  - **Browser:** Allows users to use the web browser. Default is **On**.
  - **Youtube:** Allows users to access YouTube. Default is **On**.
  - **Google Play/Marketplace:** Allows users to access Google Play and the Google Apps Marketplace. Default is **On**.
  - **Force stop system app:** Allows users to disable pre-installed system apps (MDM 4.0 and later). Default is **On**.

- **Samsung SAFE: Network**
  - **Incoming MMS:** Allows users to receive MMS messages. Default is **On**.
  - **Outgoing MMS:** Allows users to send MMS messages. Default is **On**.
  - **Incoming SMS:** Allows users to receive SMS messages. Default is **On**.
  - **Outgoing SMS:** Allows users to send SMS messages. Default is **On**.
  - **Configure mobile network:** Allows users to configure mobile networks. Default is **On**.
  - **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).
  - **Only secure connections:** Allows users to only use secure connections (MDM 4.0 and later). Default is **On**.
  - **Audio record:** Allows users to record audio with their devices (MDM 4.0 and later). Default is **On**.
  - **Video record:** Allows users to record video with their devices (MDM 4.0 and later). Default is **On**.

- **Samsung Knox**
  - **Enable Revocation Check:** Enables checking for revoked certificates. Default is **On**.
  - **Move Apps To Container:** Allows users to move apps between the Knox container and the personal area on their devices. Default is **On**.
  - **Enforce Multifactor Authentication:** Users must use a fingerprint and one other authentication method, such as password or PIN, to open their devices. Default is **On**.
  - **Enable TIMA Key store:** 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 **On**.

- **Enforce Authentication For Container:** Use separate, and different, authentication to open the Knox container from that used to unlock the device. Default is **On**.
- **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 **On**.
- **Use Secure Keypad:** Forces users to use a secure keyboard inside the Knox container. Default is **On**.
- **Authentication Smart Card Browser:** Enables browser authentication on devices equipped with a smart card reader.

When **Apply to fully managed devices with a work profile** is on and set to **Work profile**, configure these settings:

- **Network**
  - **Allow configuring location provider:** Allows users to turn on GPS on their devices. For Android API 28 and later. Default is **On**.
- **Security**
  - **Don't allow printing:** If **On**, the setting prevents users from printing to any printer accessible from the user device. The default is **Off**. Available for: Android 9 and later.
  - **Allow account management:** Allows account to be added to in work profile and managed devices. Default is **Off**.
  - **Allow cross profile copy and paste:** Allows or prevents use of the clipboard to copy and paste between apps in the Android Enterprise profile and apps in the personal area. Default is **Off**.
  - **Allow location sharing:** Allows location sharing. For managed profiles, the device owner can override this setting. Default is **Off**.

    > **Tip:**
    >
    > You can create Location device policies in XenMobile to enforce geographic boundaries. See Location device policy.

  - **Allow Non-Google Play apps:** Allows the installation of apps from stores other than Google Play. 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 user control of application settings:** Allows users to uninstall apps, disable apps, clear cache and data, force stop any app, and clear defaults. Default is **Off**.

- **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 whose widgets will be allowed:** 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**.
- **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, XenMobile 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**.
- **Don't allow printing:** If **On**, the setting prevents users from printing to any printer accessible from the user device. The default is **Off**. Available for: Android 9 and later.
- **Allow users to configure credentials:** Allows users to set their user names and passwords. Default is **On**.

- **Samsung SAFE: Allow hardware controls**
  - **Clipboard:** Allow users to copy data to the clipboard on their devices.
    - **Clipboard share:** Allow users to share clipboard content between their devices and a computer (MDM 4.0 and later).
- **Samsung SAFE: Allow apps**
  - **Browser:** Allows users to use the web browser. Default is **On**.
  - **Youtube:** Allows users to access YouTube. Default is **On**.
  - **Google Play/Marketplace:** Allows users to access Google Play and the Google Apps Marketplace. Default is **On**.
- **Samsung Knox**
  - **Enable Revocation Check:** Enables checking for revoked certificates. Default is **On**.
  - **Move Apps To Container:** Allows users to move apps between the Knox container and the personal area on their devices. Default is **On**.
  - **Enforce Multifactor Authentication:** Users must use a fingerprint and one other authentication method, such as password or PIN, to open their devices. Default is **On**.
  - **Enable TIMA Key store:** 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 **On**.
  - **Enforce Authentication For Container:** Use separate, and different, authentication to open the Knox container from that used to unlock the device. Default is **On**.
  - **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 **On**.
  - **Use Secure Keypad:** Forces users to use a secure keyboard inside the Knox container. Default is **On**.
  - **Authentication Smart Card Browser:** Enables browser authentication on devices equipped with a smart card reader.

When **Apply to fully managed devices with a work profile** is on and set to **Manage device**, configure these settings:

- **Allow USB actions**
  - **Debugging:** Allows debugging over USB. Default is **Off**.
  - **File transfer:** Allows file transfers over USB. Default is **Off**.
- **Network**
  - **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**.
  - **Android beam:** 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 if **Off**.

- **Allow configuring location provider:** Allows users to turn on GPS on their devices. For Android API 28 and later. Default is **On**.

- **Security**
  - **Allow use of the status bar:** If set to **On**, this setting enables the status bar on managed devices and dedicated devices (also known as COSU devices). This 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**.
  - **Keep the keyguard from locking the device:** If set to **On**, this setting disables the keyguard on the lock screen on managed devices and dedicated devices (also known as COSU devices). Default is **Off**.
  - **Don't allow printing:** If **On**, the setting prevents users from printing to any printer accessible from the user device. The default is **Off**. Available for: Android 9 and later.
  - **Allow account management:** Allows account to be added to in work profile and managed devices. Default is **Off**.
  - **Allow cross profile copy and paste:** Allows or prevents use of the clipboard to copy and paste between apps in the Android Enterprise profile and apps in the personal area. Default is **Off**.
  - **Allow location sharing:** Allows location sharing. For managed profiles, the device owner can override this setting. Default is **Off**.

    > **Tip:**
    > You can create Location device policies in XenMobile to enforce geographic boundaries. See Location device policy.

  - **Allow Non-Google Play apps:** Allows the installation of apps from stores other than Google Play. 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 user control of application settings:** Allows users to uninstall apps, disable apps, clear cache and data, force stop any app, and clear defaults. Default is **Off**.
  - **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 whose widgets will be allowed:** 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 An-

droid Enterprise profile in the parent profile, for incoming calls (Android 7.0 and later). Default is **Off**.

- **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 managed configurations policy 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, XenMobile 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**.

- **Fully Managed Device**
  - **Allow multiple users:** Allows multiple users to use a device (MDM 4.0 and later). Default is **On**.
  - **Allow roaming:** Allows users to use cellular data while roaming. The default is OFF, which disables roaming on users' devices. Default is **Off**. When this setting is on, these settings are available for Samsung SAFE devices:
    - **Data:** Allow users to use cellular data for data.
    - **Push:** Allow users to use cellular data for pushing.
    - **Sync:** Allow users to use cellular data for syncing.
    - **Voice calls:** Allow users to use cellular data for voice calls.
  - **Allow SMS:** Allows users to send and receive SMS messages. Default is **Off**.
  - **Backup:** Allows users to back up application and system data on their devices. Default is **On**.
  - **Bluetooth:** Allows users to use Bluetooth. Default is **On**.
  - **Date Time Change:** Allows users to change the date and time on their devices. Default is

On.

- **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**.
- **Mass storage:** Allows transfer of large data files between users' devices and a computer over a USB connection. Default is **On**.
- **Microphone:** Allows users to use the microphone on their devices. Default is **On**.
- **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:
  - **USB:** Allows users to share a mobile data connection with another device using their USB connection.
  - **Bluetooth:** Allows users to share a mobile data connection with another device using their Bluetooth connection.
  - **WiFi:** Allows users to share a mobile data connection with another device using their Wi-Fi connection.
- **WiFi:** Allows users to connect to Wi-Fi networks. Default is **On**. When this setting is on, these settings are available:
  - **Direct:** Allows users to connect directly to another device through their Wi-Fi connection. For Samsung devices only. For MDM 4.0 and later.
  - **State Change:** Allows apps to change Wi-Fi connectivity state.

- **Samsung SAFE: 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. Default is **On**.
  - **Allow Emergency Call 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 is in contrast to full disk encryption, which encrypts all data, including settings, application data, downloaded files and applications, media, and other files. Default is **On**.
  - **Common Criteria Mode:** Places device into Common Criteria Mode. The Common Criteria configuration enforces stringent security processes. Default is **On**.
  - **DOD boot banner:** Displays a DoD approved system use notification message or banner when users' devices are restarted. Default is **Off**.
  - **Settings changes:** Allows users to change settings on their fully managed devices. Default is **On**.
  - **Over The Air Upgrade:** Allows users' devices to receive software updates wirelessly (MDM 3.0 and later). Default is **On**.
  - **Background data:** Allows apps to sync data in the background. for fully managed devices.

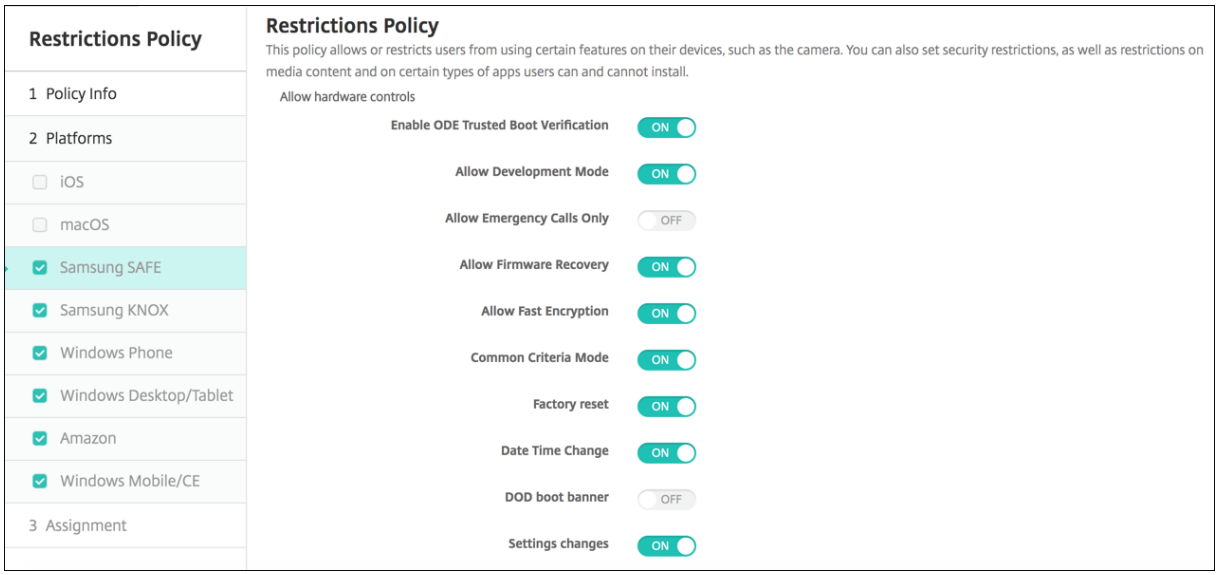
Default is **On**.

- **Clipboard:** Allow users to copy data to the clipboard on their devices.
  - **Clipboard share:** Allow users to share clipboard content between their devices and a computer (MDM 4.0 and later).
- **Home key:** Allows users to use the **Home** key on their fully managed devices. Default is **On**.
- **Mock location:** Allows users to fake their GPS location. For fully managed devices. Default is **On**.
- **NFC:** Allows users to use NFC on their fully managed devices (MDM 3.0 and later). Default is **On**.
- **Power off:** Allows users to turn off their fully managed devices (MDM 3.0 and later). Default is **On**.
- **SD card:** Allows users to use an SD card, if available, with their devices. Default is **On**.
- **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**.
- **Voice dialer:** Allows users to use the voice dialer on their devices (MDM 4.0 and later). Default is **On**.
- **SBeam:** Allows users to share content with others using NFC and Wi-Fi Direct (MDM 4.0 and later). Default is **On**.
- **SVoice:** Allows users to use the intelligent personal assistant and knowledge navigator on their devices (MDM 4.0 and later). Default is **On**.

- **Samsung SAFE: Allow apps**
  - **Face Recognition:** Allows users to use the face recognition app. Default is **On**.
  - **Browser:** Allows users to use the web browser. Default is **On**.
  - **Youtube:** Allows users to access YouTube. Default is **On**.
  - **Google Play/Marketplace:** Allows users to access Google Play and the Google Apps Marketplace. Default is **On**.
- **Samsung SAFE: Network**
  - **Incoming Mms:** Allows users to receive MMS messages. Default is **On**.
  - **Outgoing Mms:** Allows users to send MMS messages. Default is **On**.
  - **Incoming SMS:** Allows users to receive SMS messages. Default is **On**.
  - **Outgoing SMS:** Allows users to send SMS messages. Default is **On**.
  - **Configure mobile network:** Allows users to configure mobile networks. Default is **On**.
  - **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).

  - **Only secure connections:** Allows users to only use secure connections (MDM 4.0 and later). Default is **On**.
  - **Audio record:** Allows users to record audio with their devices (MDM 4.0 and later). Default is **On**.
  - **Video record:** Allows users to record video with their devices (MDM 4.0 and later). Default is **On**.
- **Samsung Knox**
  - **Enable Revocation Check:** Enables checking for revoked certificates. Default is **On**.
  - **Move Apps To Container:** Allows users to move apps between the Knox container and the personal area on their devices. Default is **On**.
  - **Enforce Multifactor Authentication:** Users must use a fingerprint and one other authentication method, such as password or PIN, to open their devices. Default is **On**.
  - **Enable TIMA Key store:** 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 **On**.
  - **Enforce Authentication For Container:** Use separate, and different, authentication to open the Knox container from that used to unlock the device. Default is **On**.
  - **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 **On**.
  - **Use Secure Keypad:** Forces users to use a secure keyboard inside the Knox container. Default is **On**.
  - **Authentication Smart Card Browser:** Enables browser authentication on devices equipped with a smart card reader.

Samsung SAFE settings



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 is in contrast to full disk encryption, which encrypts all data, including settings, application data, downloaded files and applications, media, and other files.
  - **Common Criteria Mode:** Place device into Common Criteria Mode. The Common Criteria configuration enforces stringent security processes.
  - **Factory Reset:** Allow users to do a factory reset on their devices.
  - **Date Time Change:** Allow users to change the date and time on their devices.
  - **DOD reboot banner:** Display a DoD approved system use notification message or banner when users' devices are restarted.
  - **Settings changes:** Allow users to change settings on their devices.
  - **Backup:** 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).
  - **Background data:** Allow apps to sync data in the background.
  - **Camera:** Allow users to use the camera on their devices.

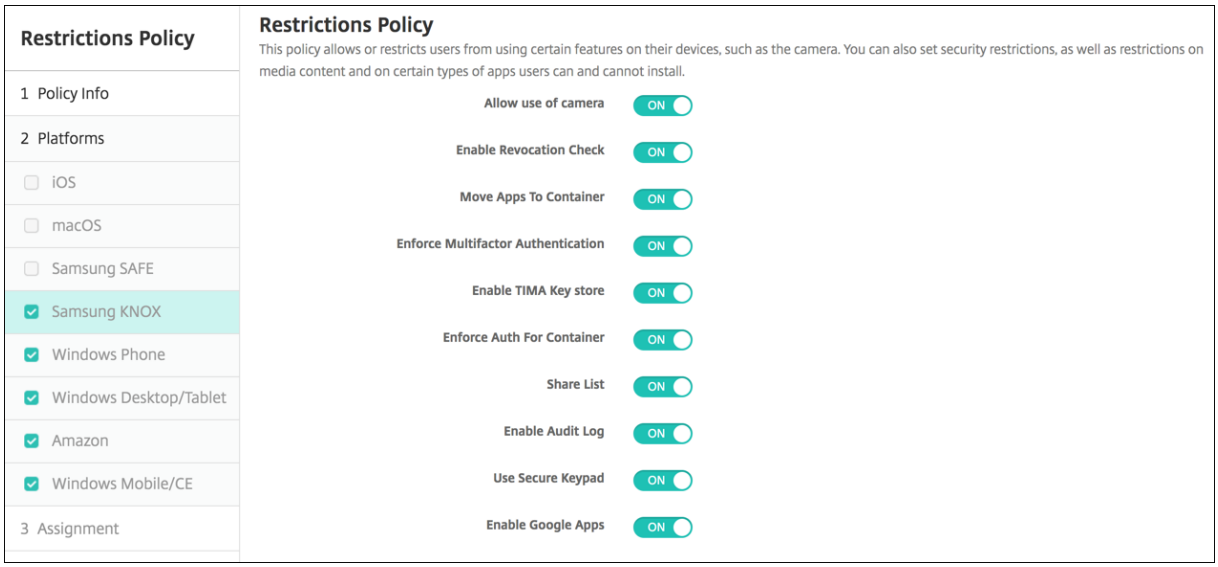
  - **Clipboard:** Allow users to copy data to the clipboard on their devices.
    - **Clipboard share:** Allow users to share clipboard content between their devices and a computer (MDM 4.0 and later).
  - **Home key:** Allow users to use the Home key on their devices.
  - **Microphone:** Allow users to use the microphone on their devices.
  - **Mock location:** Allow users to fake their GPS location.
  - **NFC:** Allow users to use NFC (Near Field Communication) on their devices (MDM 3.0 and later).
  - **Power off:** Allow users to turn off their devices (MDM 3.0 and later).
  - **Screenshot:** Allow users to take screen shots on their devices.
  - **SD card:** Allow users to use an SD card, if available, with their devices.
  - **Voice Dialer:** Allow users to use the voice dialer on their devices (MDM 4.0 and later).
  - **SBeam:** Allow users to share content with others using NFC and Wi-Fi Direct (MDM 4.0 and later).
  - **SVoice:** Allow users to use the intelligent personal assistant and knowledge navigator on their devices (MDM 4.0 and later).
  - **Allow multiple users:** Allow multiple users to use a device (MDM 4.0 and later). Defaults to **Off**.
- **Allow apps**
  - **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.
  - **Stop 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.
- **Network**
  - **Incoming Mms:** Allow users to receive MMS messages.
  - **Incoming Sms:** Allow users to receive SMS messages.
  - **Outgoing Mms:** Allow users to send MMS messages.
  - **Outgoing Sms:** Allow users send SMS messages.
  - **User Add profiles Vpn:**
  - **Bluetooth:** Allow users to use Bluetooth.
    - **Tethering:** Allow users to share a mobile data connection with another device using their Bluetooth connection.
  - **WiFi:** Allow users to connect to WiFi networks.

        * **Tethering:** Allow users to share a mobile data connection with another device using their WiFi connection.
        * **Direct:** Allow users to connect directly to another device through their WiFi connection (MDM 4.0 and later).
        * **State Change:** Allow apps to change WiFi connectivity state.
        * **User Policy Changes:** Allow users to change WiFi policies. If not selected, users can change only the WiFi user name and password. If selected, users can change all WiFi policies.
    - **Tethering:** Allow users to share a mobile data connection with another device.
    - **Cellular data:** Allow users to use their cellular connection for data.
    - **Allow roaming:** Allow users to use cellular data while roaming. The default is OFF, which disables roaming on users' devices.
    - **Only secure connections:** Allow users to only use secure connections (MDM 4.0 and later).
    - **Android beam:** Allow users to send web pages, photos, videos, or other content from their devices to another device using NFC (MDM 4.0 and later).
    - **Audio record:** Allow users to record audio with their devices (MDM 4.0 and later).
    - **Video record:** 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.
    - **Debugging:** Allow debugging over 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.
    - **Mass storage:** Allow transfer of large data files between users' devices and a computer over a USB connection.
    - **Kies media player:** Allow users to use the Samsung Kies tool to sync files between their devices and a computer.
    - **Tethering:** Allow users to share a mobile data connection with another device through a USB connection.
- **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

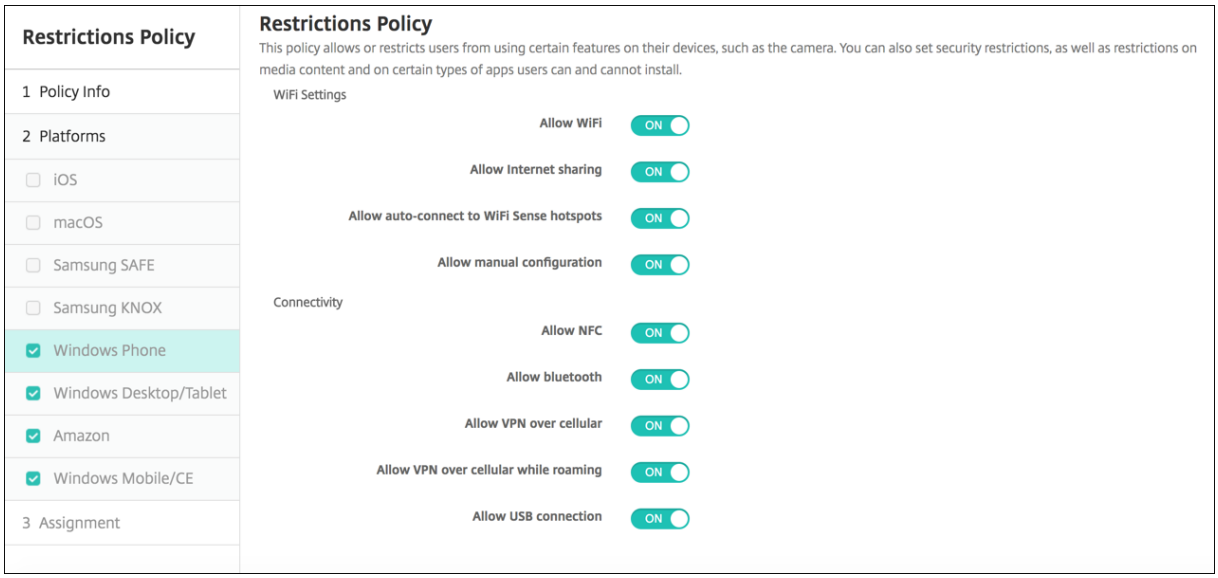


These options are available only under Samsung KNOX Premium (KNOX 2.0).

- **Allow Use of Camera:** Allow users to use the camera on their devices.
- **Allow 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 Multifactor Authentication:** Users must use a fingerprint and one other authentication method, such as password or PIN, to open their devices.
- **Enable TIMA Key store:** 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 Auth For Container:** Use separate, and different, authentication to open the KNOX container from that used to unlock the device.
- **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.
- **Use 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.

Windows Phone and Windows Desktop/Tablet settings

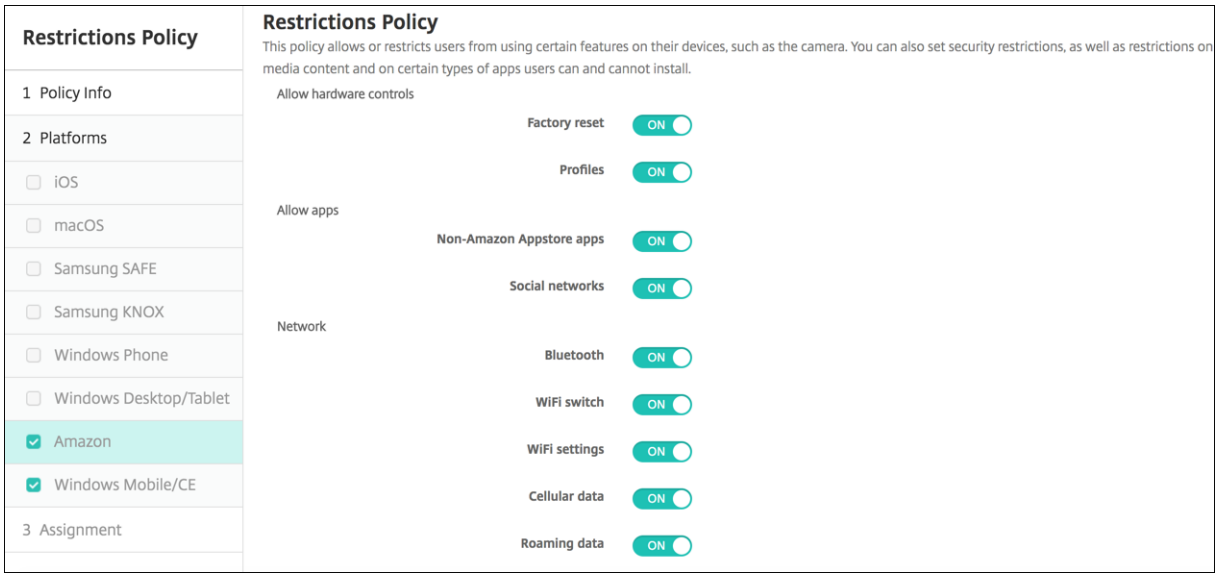


- **WiFi Settings**
  - **Allow WiFi:** Allow a device to connect to a Wi-Fi network. Windows Phone only.
  - **Allow Internet sharing:** Allow a device to share its internet connection with other devices by turning it into a WiFi hotspot.
  - **Allow auto-connect to WiFi Sense hotspots:** Allow a device to connect automatically to WiFi Sense hotspots. Location services must be enabled for this option to work. For more information about WiFi Sense, see the Windows Phone WiFi Sense FAQ.
  - **Allow manual configuration:** Allow users to manually configure WiFi connections. Windows Phone only.
- **Connectivity**
  - **Allow NFC:** Allow device to communicate with an NFC (Near Field Communication) tag or another NFC-enabled transmitting device. Windows Phone only.
  - **Allow bluetooth:** Allow device to connect through Bluetooth. Windows Phone only.
  - **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. Note that 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.

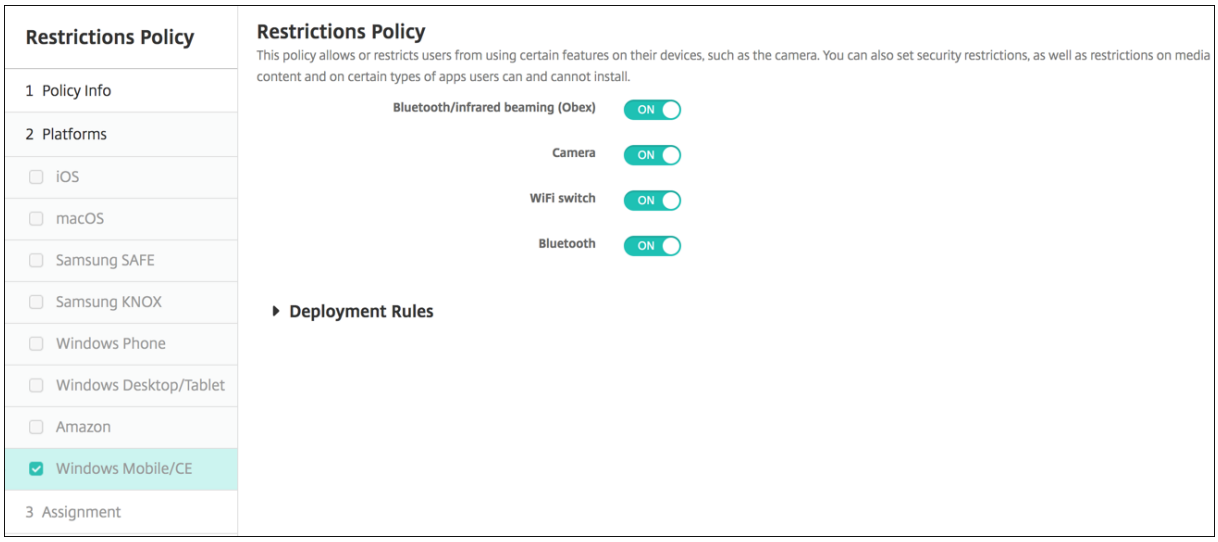
  - **Allow manual MDM unenrollment:** Allow users to manually unenroll their device from XenMobile MDM.
  - **Allow sync of device settings:** Allow users to sync settings between Windows 10 devices when roaming.
- **Above Lock:** Windows Desktop/Tablet only
  - **Allow toasts:** Allow toast notifications 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 appstore auto update:** 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, to improve 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 signin settings.
  - **Allow workplace:** Allows users to change workplace settings.
  - **Allow your account:** Allows users to change account settings.

Amazon settings



- **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 Appstore apps on their devices.
  - **Social networks:** Allow users to access social networks from their devices.
- **Network**
  - **Bluetooth:** Allow users to use Bluetooth.
  - **WiFi switch:** Allow apps to change WiFi connectivity state.
  - **WiFi settings:** Allow users to change WiFi settings.
  - **Cellular data:** Allow users to use their cellular connection for data.
  - **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.

Windows Mobile/CE settings



- **Bluetooth/infrared beaming (Obex):** Enable OBEX (OBject EXchange protocol) over Bluetooth or infrared to exchange data between devices.
- **Camera:** Enable the camera on user devices.
- **WiFi switch:** Allow users to switch WiFi networks.
- **Bluetooth:** Enable Bluetooth on users' devices.
- **Camera:** Enable the camera on user devices.
- **WiFi switch:** Allow users to switch WiFi networks.
- **Bluetooth:** Enable Bluetooth on users' devices.

Roaming device policy

July 3, 2018

You can add a device policy in XenMobile to configure whether to allow voice and data roaming on users iOS and Windows Mobile/CE devices. When voice roaming is disabled, data roaming is automatically disabled. For iOS, this policy is available only on iOS 5.0 and later devices.

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.

Windows Mobile/CE settings

- **While roaming**
  - **Use on-demand connection only:** The device only connects to XenMobile if users manually trigger the connection on their devices, or if a mobile application requests a forced connection (such as a push mail request if the Exchange Server has been set accordingly). Note that this option temporarily disables the default device connection schedule policy.
  - **Block all cellular connections except the ones managed by XenMobile:** Except for the data traffic officially declared in a XenMobile application tunnel or other XenMobile device management task, no other data is sent or received by the device. For example, this option disables all connections to the Internet through the device's web browser.
  - **Block all cellular connections managed by XenMobile:** All application data transiting through a XenMobile tunnel is blocked (including XenMobile Remote Support). The data traffic related to pure device management, however, is not blocked.
  - **Block all cellular connections to XenMobile:** In this case, until the device is either reconnected through USB, WiFi, or its default mobile operator cellular network, there is no traffic transiting between the device and XenMobile.
- **While domestic roaming**
  - **Ignore domestic roaming:** No data is blocked while users roam domestically.

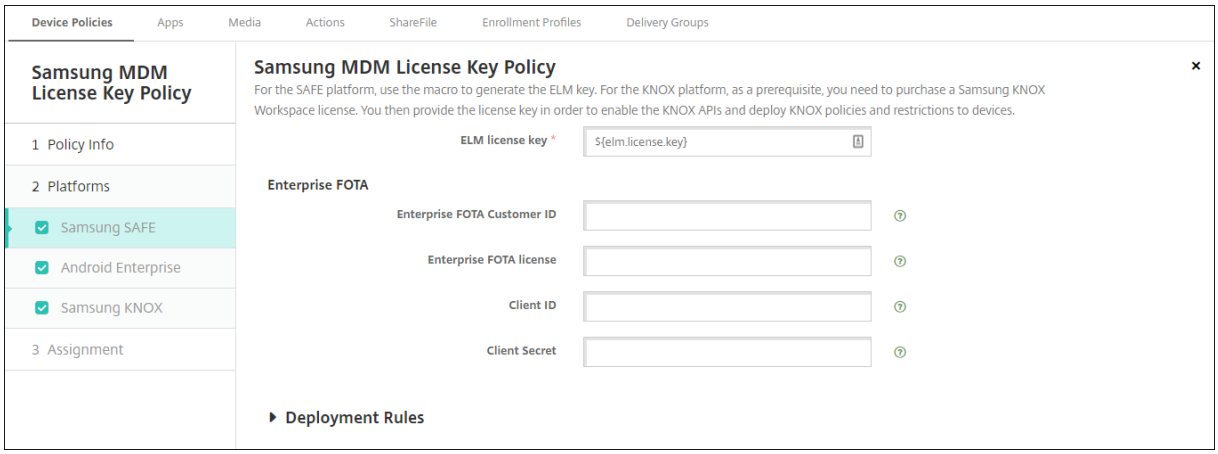
Samsung MDM license key device policy

September 10, 2020

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. XenMobile also supports the Samsung Enterprise Firmware-Over-The-Air (E-FOTA) service. XenMobile 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



- **ELM License key:** XenMobile 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.

XenMobile supports adding devices from the XenMobile console to Knox E-FOTA One. For more information about exporting a device list from XenMobile, see Export the Devices table. For more information about adding a device to Knox E-FOTA One, see the Samsung documentation.

XenMobile 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. XenMobile Server then validates and registers the information. If XenMobile 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 Developer Guides.

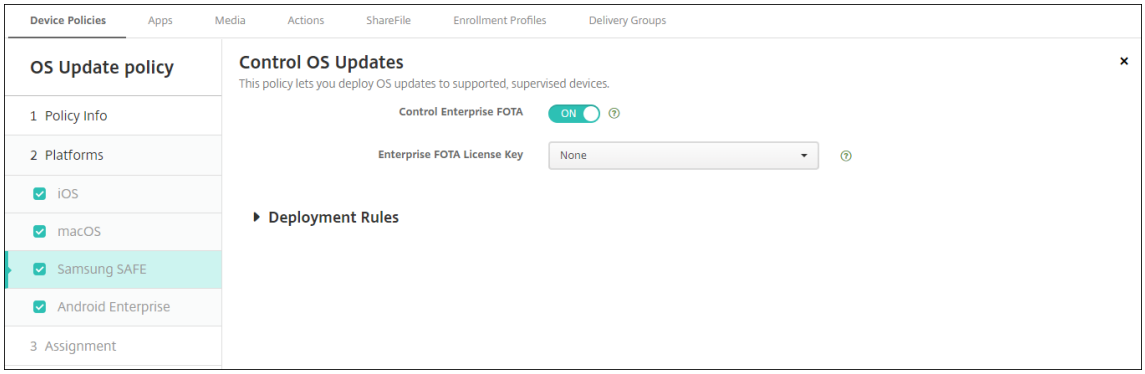
   Type the **ELM License key:** XenMobile pre-fills this field with the macro that generates the ELM license key. If the field is blank, type this macro: ${elm.license.key}

   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**

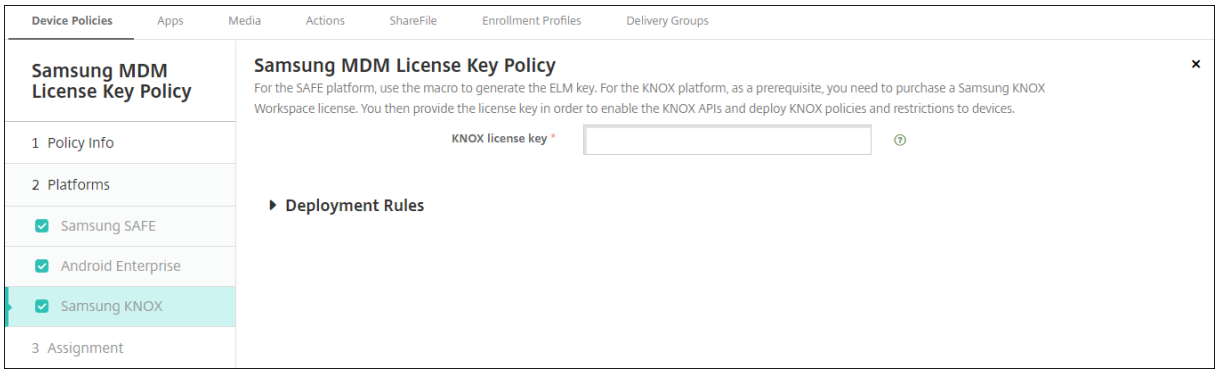
2. Optionally, create a Control OS Update device policy.



- **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.

Samsung SAFE firewall device policy

June 19, 2020

This policy lets you configure the firewall settings for Samsung devices. You enter IP addresses, ports, and host names that you want to allow or block. You can also configure proxy and proxy reroute settings.

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 **Whitelist** to allow access or click **Blacklist** to deny access to the site.

    > **Note:**
    > The XenMobile Server console includes the terms “blacklist” and “whitelist”. We are changing those terms in an upcoming release to “block list” and “allow list”.
- **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.

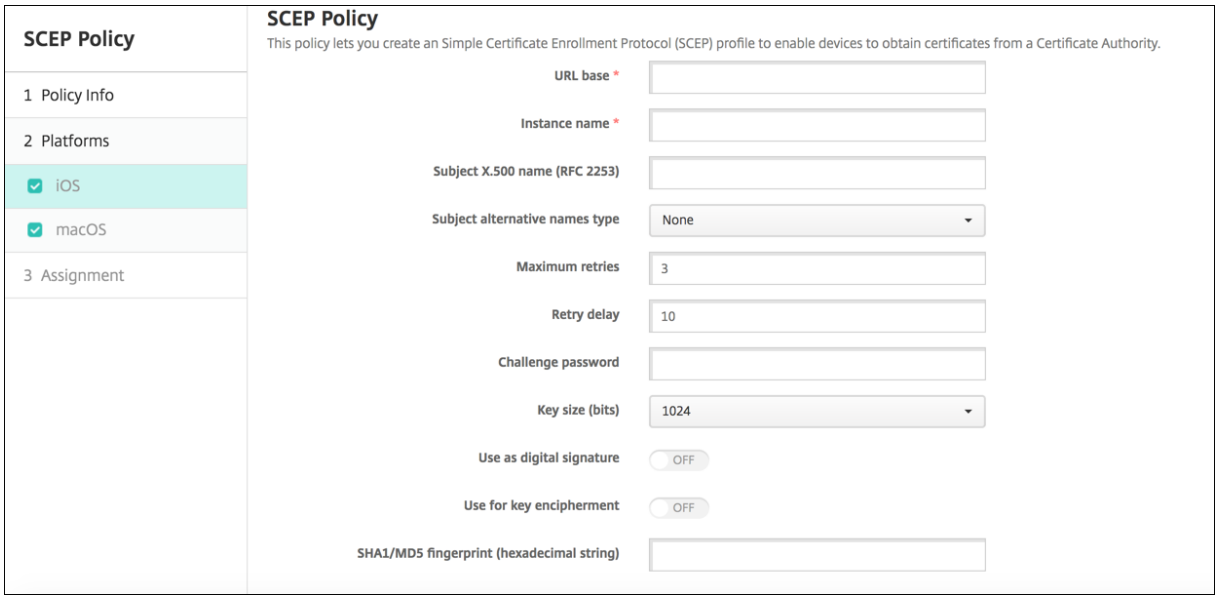
SCEP device policy

March 5, 2021

This policy allows you to configure iOS and macOS devices to retrieve a certificate using Simple Certificate Enrollment Protocol (SCEP) from an external SCEP server. If you want to deliver a certificate to the device using SCEP from a PKI that is connected to XenMobile, you should 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.

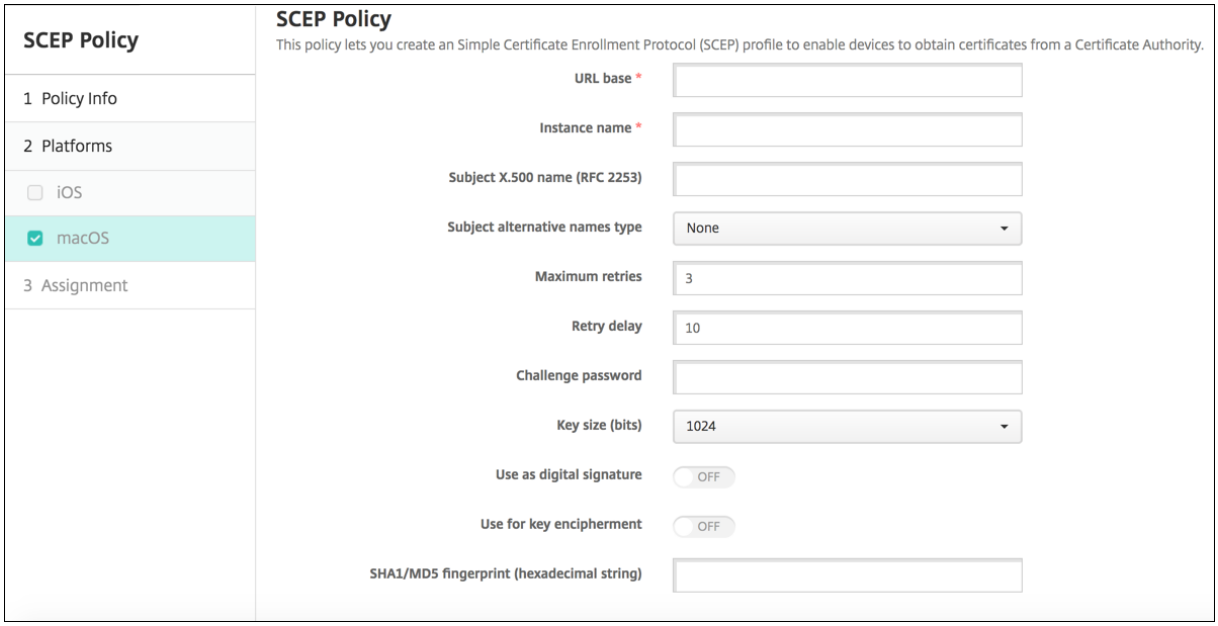
iOS settings



- **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 may be safe to send the request unencrypted. If, however, the one-time password is allowed to be reused, you should 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 a X.500 name represented as an array of Object Identifier (OID) and value. For example, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, which would translate 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:** In the list, click an alternative name type. The SCEP policy can specify an optional alternative name type that provides 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:** Specify whether you want the certificate to be used as a digital signature. If someone is using the certificate to verify a digital signature, such as verifying whether a certificate was issued by a CA, the SCEP server would verify that the certificate can be used in this manner prior to using the public key to decrypt the hash.
- **Use for key encipherment:** Specify whether you want the certificate to be used for key encipherment. If a server is using the public key in a certificate provided by a client to verify that a piece of data was encrypted using the private key, the server would first check to see whether the certificate can be used for key encipherment. If not, the operation fails.
- **SHA1/MD5 fingerprint (hexadecimal string):** If your CA uses HTTP, use this field to provide the fingerprint of the CA certificate, which the device uses to confirm authenticity of the CA response during enrollment. You can enter a SHA1 or MD5 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



- **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 may

be safe to send the request unencrypted. If, however, the one-time password is allowed to be reused, you should 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 a X.500 name represented as an array of Object Identifier (OID) and value. For example, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, which would translate 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:** In the list, click an alternative name type. The SCEP policy can specify an optional alternative name type that provides 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:** Specify whether you want the certificate to be used as a digital signature. If someone is using the certificate to verify a digital signature, such as verifying whether a certificate was issued by a CA, the SCEP server would verify that the certificate can be used in this manner prior to using the public key to decrypt the hash.
- **Use for key encipherment:** Specify whether you want the certificate to be used for key encipherment. If a server is using the public key in a certificate provided by a client to verify that a piece of data was encrypted using the private key, the server would first check to see whether the certificate can be used for key encipherment. If not, the operation fails.
- **SHA1/MD5 fingerprint (hexadecimal string):** If your CA uses HTTP, use this field to provide the fingerprint of the CA certificate, which the device uses to confirm authenticity of the CA response during enrollment. You can enter a SHA1 or MD5 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.

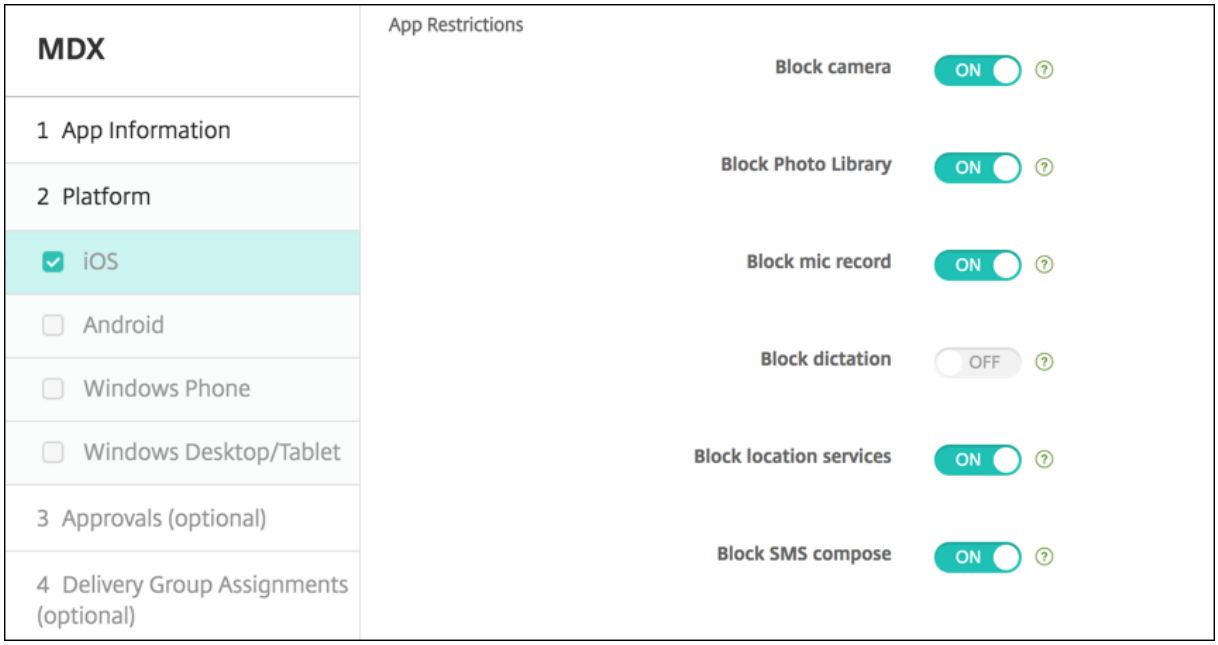
Siri and dictation policies

October 4, 2018

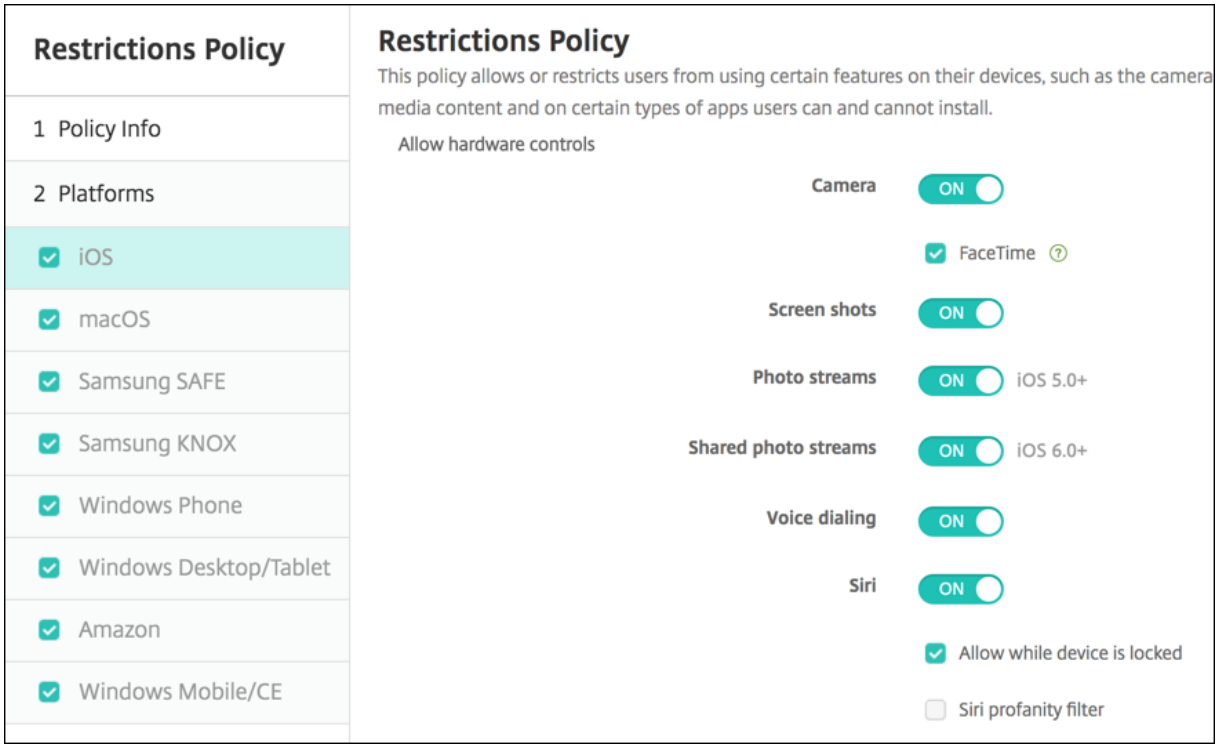
When users ask Siri something or dictate text on managed iOS devices, Apple collects the voice data for purposes of improving Siri. The voice data passes through Apple's cloud-based services, and therefore exists outside the secure XenMobile container. The text that results from dictation, however, remains within the container.

XenMobile 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 XenMobile 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. For more information, see this Wired article, Apple reveals how long Siri keeps your data.
- 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 26, 2020

You create single sign-on (SSO) accounts in XenMobile to let users sign on one-time only to access XenMobile 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.

This policy applies only to iOS 7.0 and later.

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` 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.
  - Click **Add** to add the app identifier or click **Cancel** to cancel adding the app identifier.
- **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 XenMobile 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 devices. 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.

Configure 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

July 3, 2018

You can create a policy in XenMobile to specify whether iOS, Android, or Windows Tablet devices display a XenMobile Store webclip on the devices' home screen.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Platform settings

For each platform that you configure, select whether a XenMobile Store webclip appears on user devices. The default is **On**.

Subscribed calendars device policy

March 26, 2020

You can add a device policy in XenMobile to add a subscribed calendar to the calendars list on iOS devices. The list of public calendars to which you can subscribe is available at www.apple.com/downloads/macosx/calendars.

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

July 3, 2018

You create terms and conditions device policies in XenMobile when you want users to accept your company's specific policies governing connections to the corporate network. When users enroll their devices with XenMobile, 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**.

VPN device policy

April 1, 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

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.

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.	
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 **Generic**
Samsung Knox	IPSEC, SSL	VPN type set to **Generic**

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:

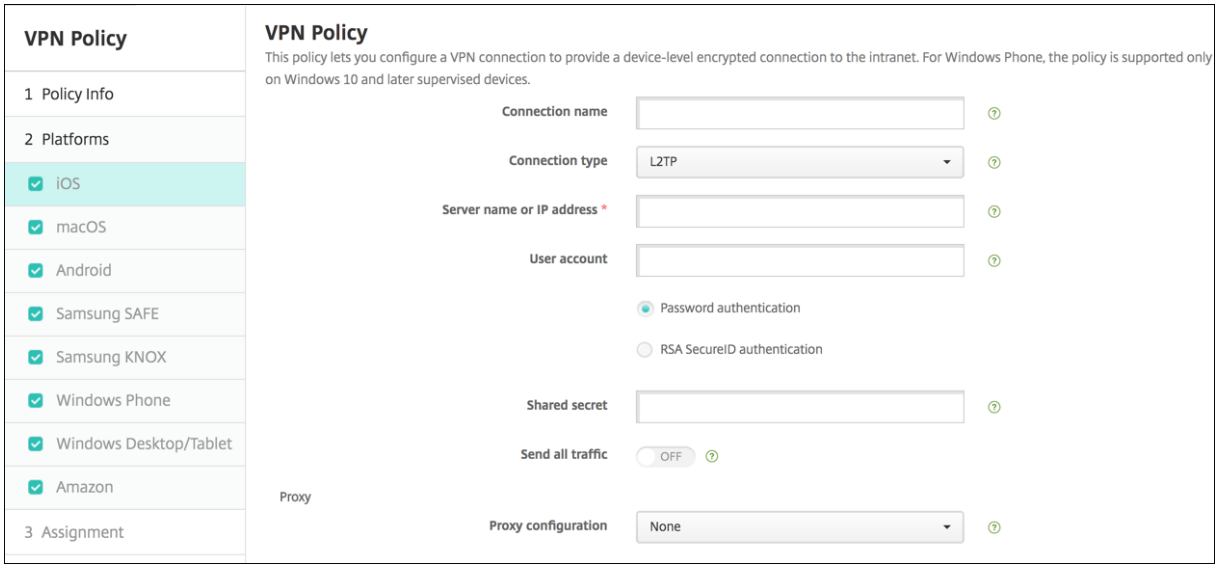
  - Citrix SSO
  - Citrix Secure Hub

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

> **To prepare for device upgrades to iOS 12:**
>
> 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. Important 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**.



- **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. For more information, see the support article https://support.citrix.com/article/CTX227708.
    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 **Auth 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 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 **Auth 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 **Auth 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 **Auth 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 **Auth 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, AlwaysOn IKEv2, and AlwaysOn IKEv2 Dual Configuration protocols. For the AlwaysOn IKEv2 Dual Configuration protocol, configure all these settings for both Cellular and Wi-Fi networks.

- **Allow user to disable automatic connection:** For the AlwaysOn protocols. Select whether to allow users to turn off 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 to iOS devices in bulk with the REST API. Only available when you select **Always On IKEv2**.
- **Extended Authentication Enabled:** Select whether to enable Extended Authentication Protocol (EAP). If you choose **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 NAT keepalive while the device is asleep:** For the AlwaysOn 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. This is how 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 **SHA1-96**.

  - **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 AlwaysOn protocols. Service exceptions are system services that are exempt from AlwaysOn 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 at https://apps.apple.com/us/app/citrix-sso/id1333396910.

- **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 **Auth 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.
  - **useragent:** 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 XenMobile, 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 **Auth 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:** 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 **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 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 IP address to be used for resolving the specified domains, click **Add** and do the following:
    * **DNS Server:** Valid only when **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Type the DNS server to add. This server doesn't need to be part of the device's current network configuration. If the DNS server is not reachable, a VPN connection is established in response. This DNS server should 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 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. You see Valid XML in green text below the **XML content** text box if the XML is valid. If it isn't valid, you see an error message in orange text describing the error.

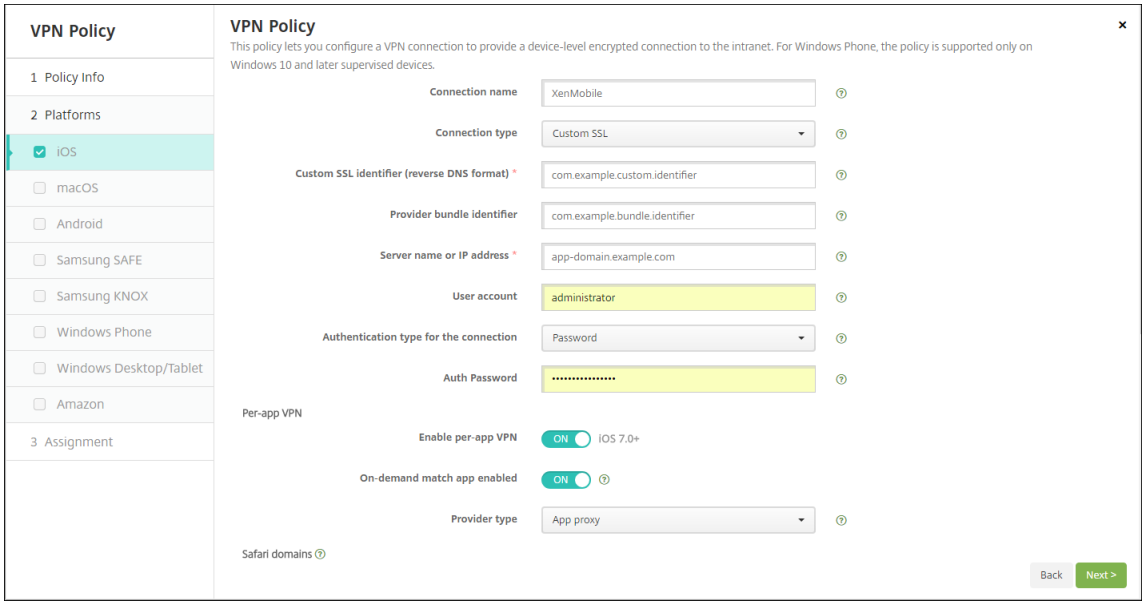
- **Proxy**
  - **Proxy configuration:** In the list, select how the VPN connection routes through a proxy server. The default is **None**.
    - If you enable **Manual**, configure these settings:
      - **Host name or IP address for the proxy server:** Type the host name or IP address for the proxy 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**
  - Under **Policy Settings**, next to **Remove policy**, select either **Select date** or **Duration until removal (in hours)**.
  - If you select **Select date**, click the calendar to select the specific date for removal.
  - In the **Allow user to remove policy** list, select **Always**, **Password required**, or **Never**.
  - If you select **Password required**, next to **Removal password**, type the necessary password.

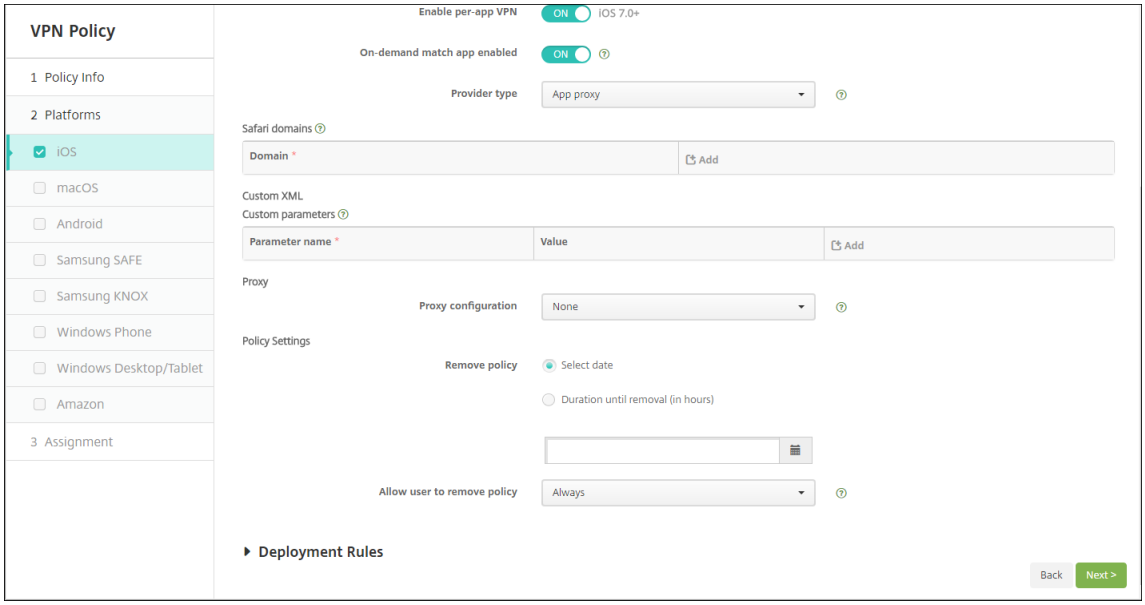
Configure a per-app VPN

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.

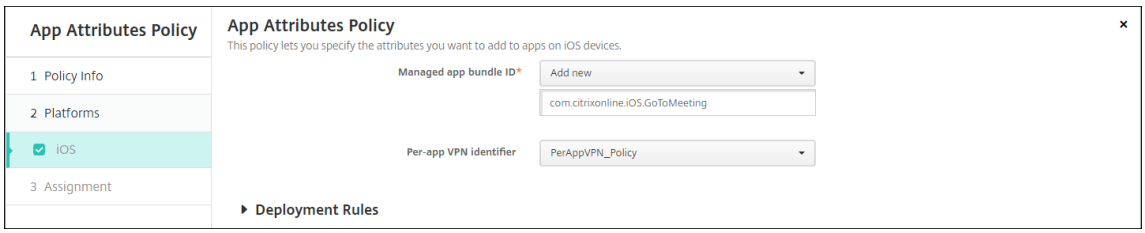
To configure a per-app VPN:

1. In **Configure > Device Policies**, create a VPN policy. For example:





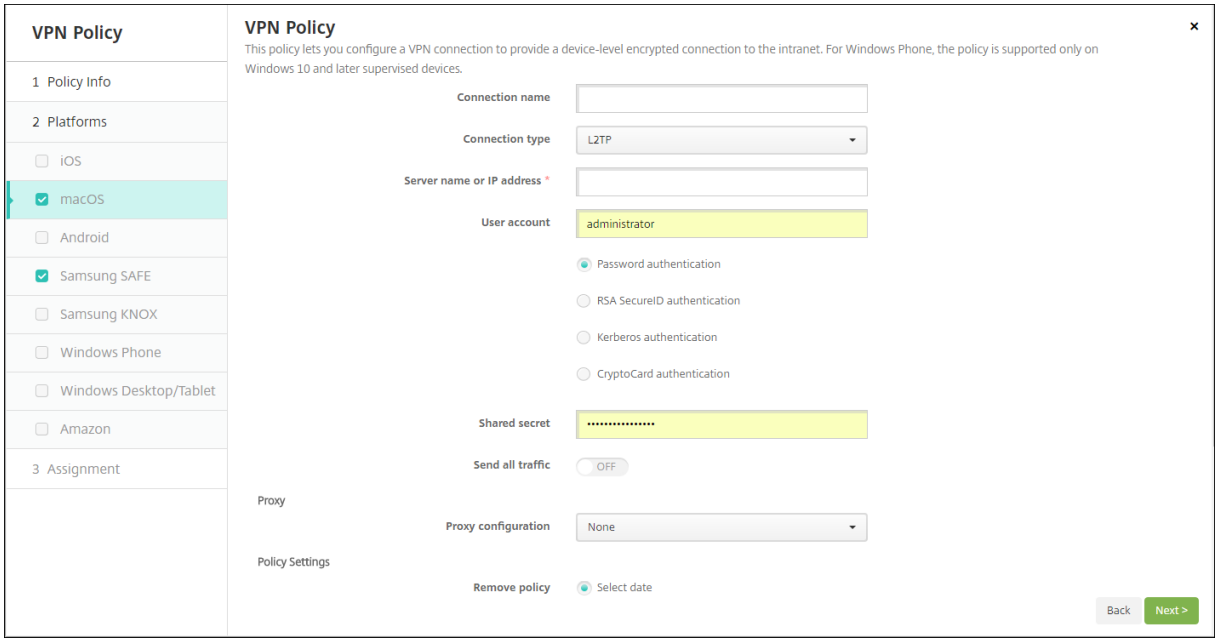
2. In **Configure > Device Policies**, create an App Attributes policy to associate an app to the per-app VPN policy. For **Per-app VPN identifier**, choose the name of the VPN policy created in Step 1. For **Managed app bundle ID**, choose from the app list or type the app bundle ID. (If you deploy an iOS App Inventory policy, the app list contains apps.)



- **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



- **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 **Auth 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 **Auth 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 **Auth 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 **Auth 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 **Auth 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 **Auth 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.

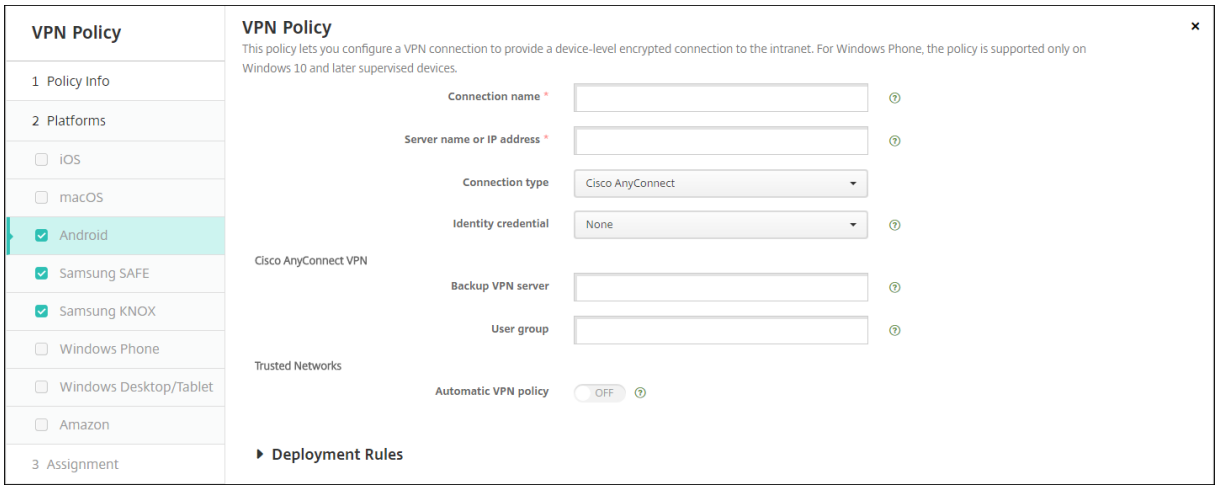
Configure enable VPN on demand options

- **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 each domain against which a user device's search domain list can match that you want to add, 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 IP address to be used for resolving the specified domains, click **Add** and do the following:
        * **DNS Server:** Valid only when **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Type the DNS server to add. This server doesn't need to be part 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. You see Valid XML in green text below the **XML content** text box if the XML is valid. If it isn't valid, you see an error message in orange text describing 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.

Android settings



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**.
  - **Whitelist** or **Blacklist:** If **Whitelist**, all allowed apps tunnel through this VPN. If **Blacklist**, all apps except those apps on the block list tunnel through this VPN.

    > **Note:**
    >
    > The XenMobile Server console includes the terms "blacklist" and "whitelist". We are changing those terms in an upcoming release to "block list" and "allow list".

  - **Application List:** Specify the allowed or blocked apps. Click **Add** and then type a comma-separated list of app package names.
- **Custom XML:** Click **Add** and then type custom parameters. XenMobile supports these parameters for Citrix VPN:
  - **DisableUserProfiles:** Optional. To enable this parameter, type **Yes** for the **Value**. If enabled, XenMobile 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.

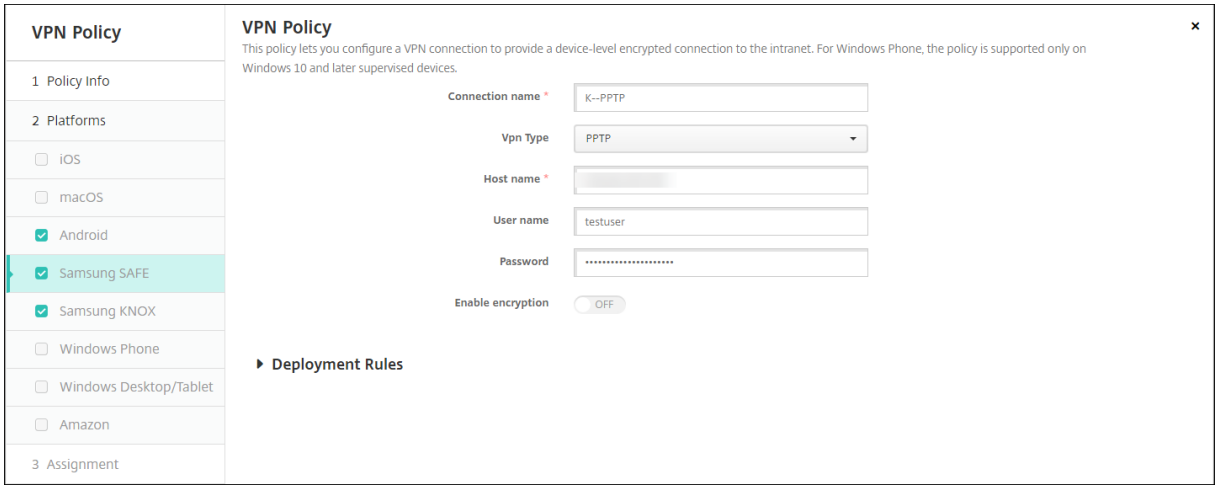
Configure VPNs to support NAC

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 XenMobile. If XenMobile 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.

Samsung SAFE settings



- **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 credentia**l: 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:** 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. 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 Microsoft's Challenge-Handshake authentication 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:** Select whether to 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 credentia**l 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 Microsoft's Challenge-Handshake authentication 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:** Select whether to enable mobile option.
- **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 negoti-

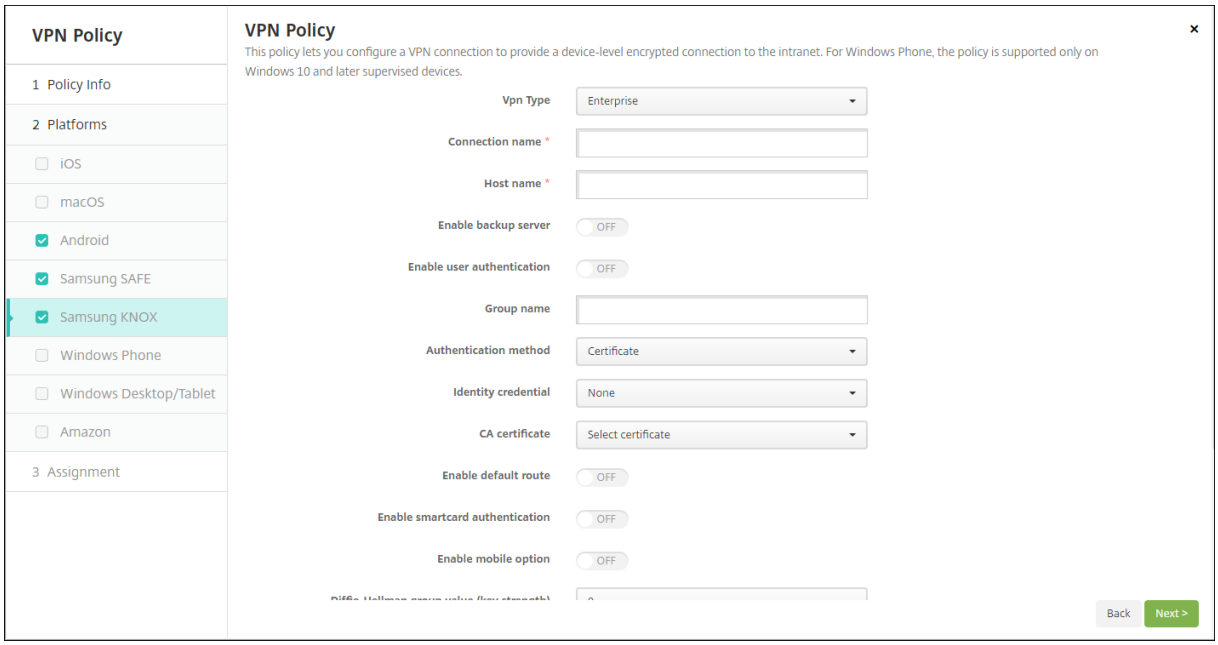
ation mode. The default is **Main**.
  - **Main:** No information is exposed to potential attackers during negotiation, but is slower than **Aggressive** mode.
  - **Aggressive:** Some information (for example, the identity of the negotiating peers) is exposed to potential attackers during negotiation, 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:** Select whether to enable mobile option.
- **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.
- **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



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 Microsoft's Challenge-Handshake authentication 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:** Select whether to enable mobile option.
- **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.

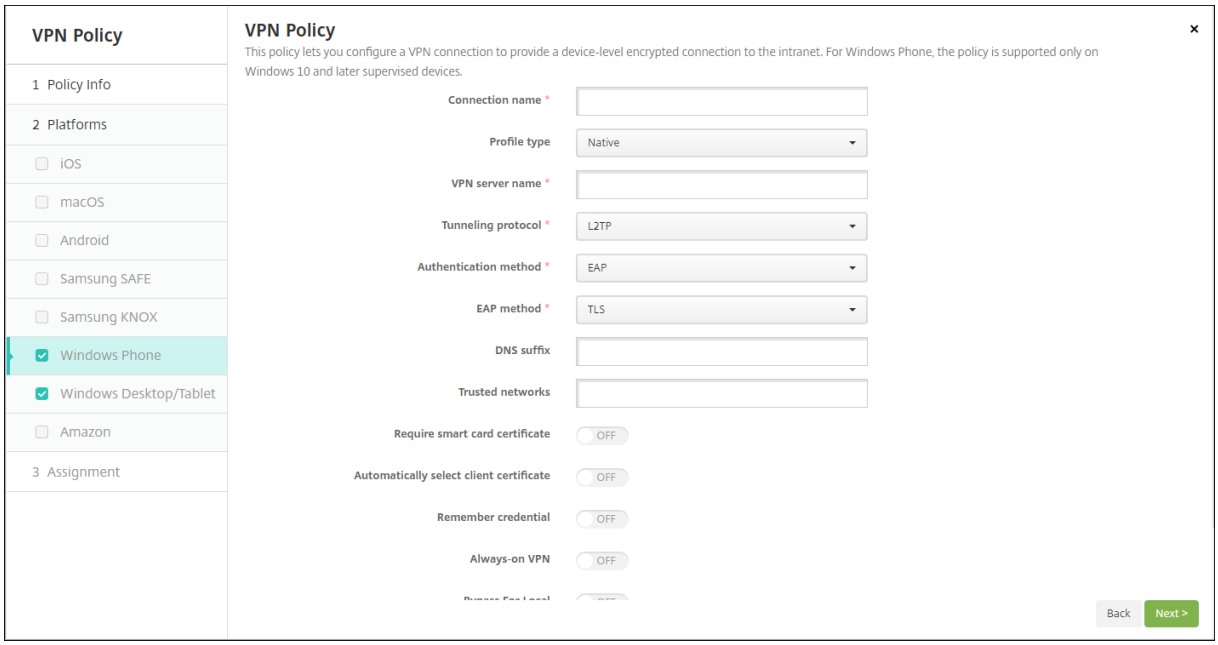
Configure generic protocol for Samsung Knox

- **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 connection 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 Microsoft's Challenge-Handshake authentication for mutual au-

thentication.
    * **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:** Select whether to enable mobile option.
- **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 for-

warding 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:** Select whether to enable mobile option.
  - **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

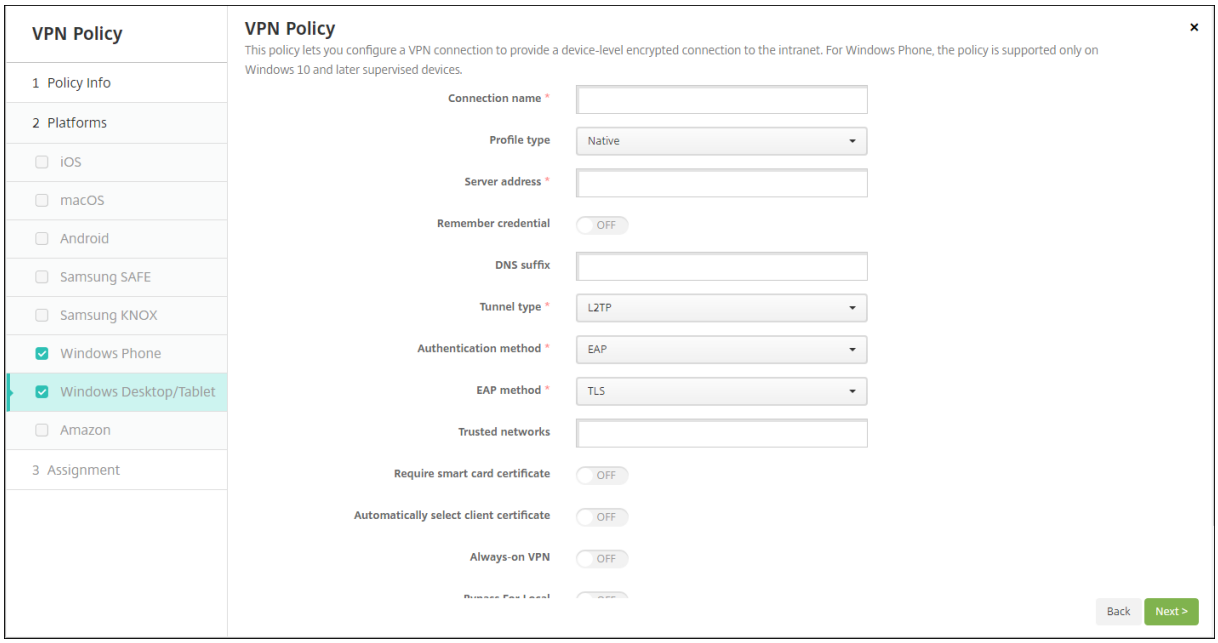


These settings are supported only on Window 10 and later supervised phones.

- **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 Microsoft Challenge-Handshake authentication 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



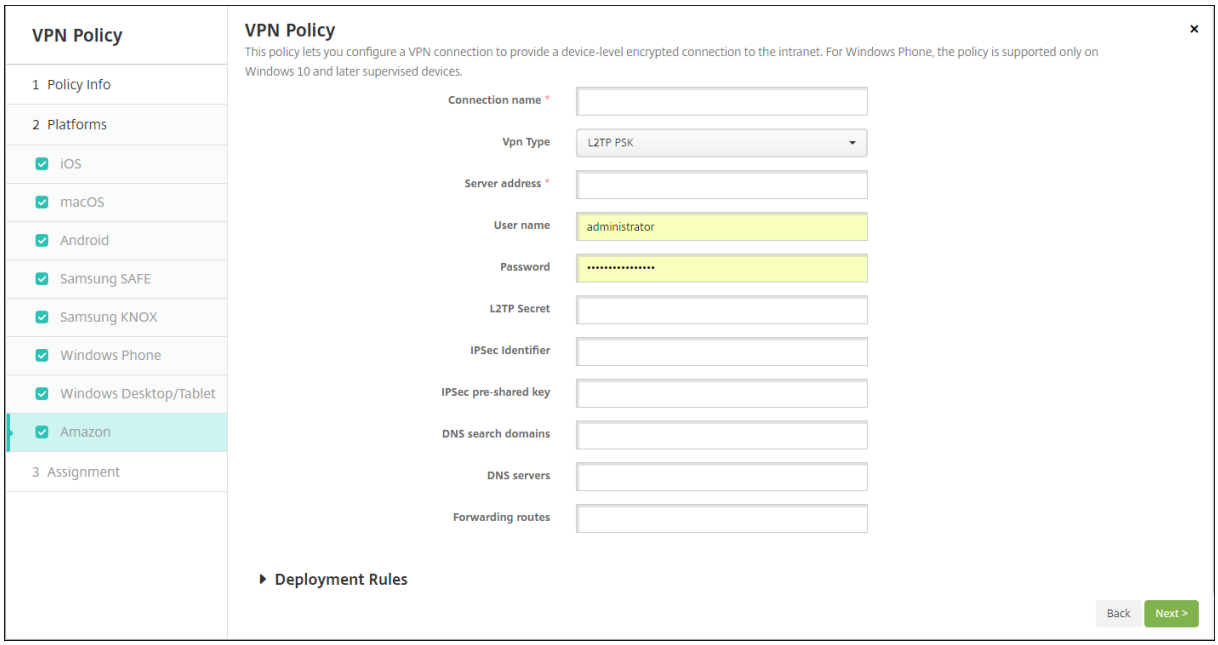
- **Connection name:** Enter a name for the connection. This field is required.
- **Profile type:** In the list, select either **Native** or **Plugin**. The default is **Native**.
- **Configure Native profile type:** These settings apply to the VPN built into users' Windows devices.
  - **Server address:** 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 Microsoft's Challenge-Handshake authentication 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



- **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.

Wallpaper device policy

July 13, 2021

You can add a .png or .jpg file to set wallpaper on an iOS device lock screen, home screen, or both. Available in iOS 7.1.2 and later 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 Apple's 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

Device	Image dimensions in pixels
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:** Select the wallpaper file by clicking **Browse** and navigating to the file location.

Web content filter device policy

April 20, 2021

You can add a device policy in XenMobile to filter web content on iOS devices by using Apple’s auto-filter function in conjunction with specific sites that you add to allow and block lists. This policy is available only on iOS 7.0 and later devices in Supervised mode. For information about placing an iOS device into Supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator.

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 `http://` or `https://` before the web address.
    * Click **Save** to save the website to the allow list or click **Cancel** not to save it.
  - **Blacklisted 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 `http://` or `https://` before the web address.
    * Click **Save** to save the website to the block list or click **Cancel** not to save it.

      > **Note:**
      > The XenMobile Server console includes the terms “blacklist” and “whitelist”. We are changing those terms in an upcoming release to “block list” and “allow list”.
- **Bookmark whitelist**
  - **Bookmark Whitelist:** 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 XenMobile Server URL to the **URL** list. You must add `http://` or `https://` 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

September 1, 2020

You can place shortcuts, or web clips, to websites to appear alongside apps on users' devices. You can specify your own icons to represent the web clips for iOS, iPadOS, macOS, and Android devices. Windows tablet only requires 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. 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.

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.
- **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.

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.

Wi-Fi device policy

December 2, 2020

You create new or edit existing Wi-Fi device policies in XenMobile by using the **Configure > Device Policies** page. Wi-Fi policies let 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 WiFi-related details

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

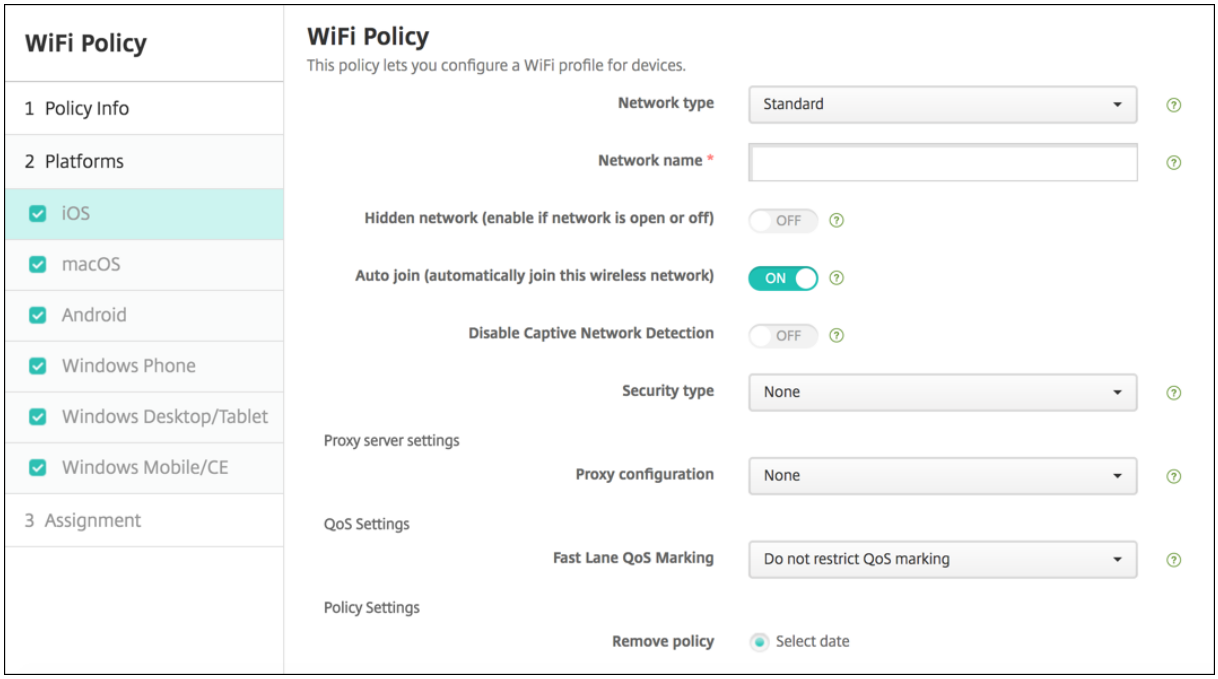
Prerequisites

Before you create a policy, be sure that you complete these steps:

- 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 settings



- **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**.
- **Hidden network (enable if network is open or off):** Choose whether the network is hidden.
- **Auto Join (automatically join this wireless network):** Choose whether the network is joined automatically. If an iOS device is already connected to another network, it won't join this network. The user must disconnect from the previous network before the device automatically connects. The default is **On**.
- **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 Personal
  - Any (Personal)

  - WEP Enterprise
  - WPA/WPA2 Enterprise: For the latest release of Windows 10, use of WPA-2 Enterprise requires that you configure the Simple Certificate Enrollment Protocol (SCEP). XenMobile 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.

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.

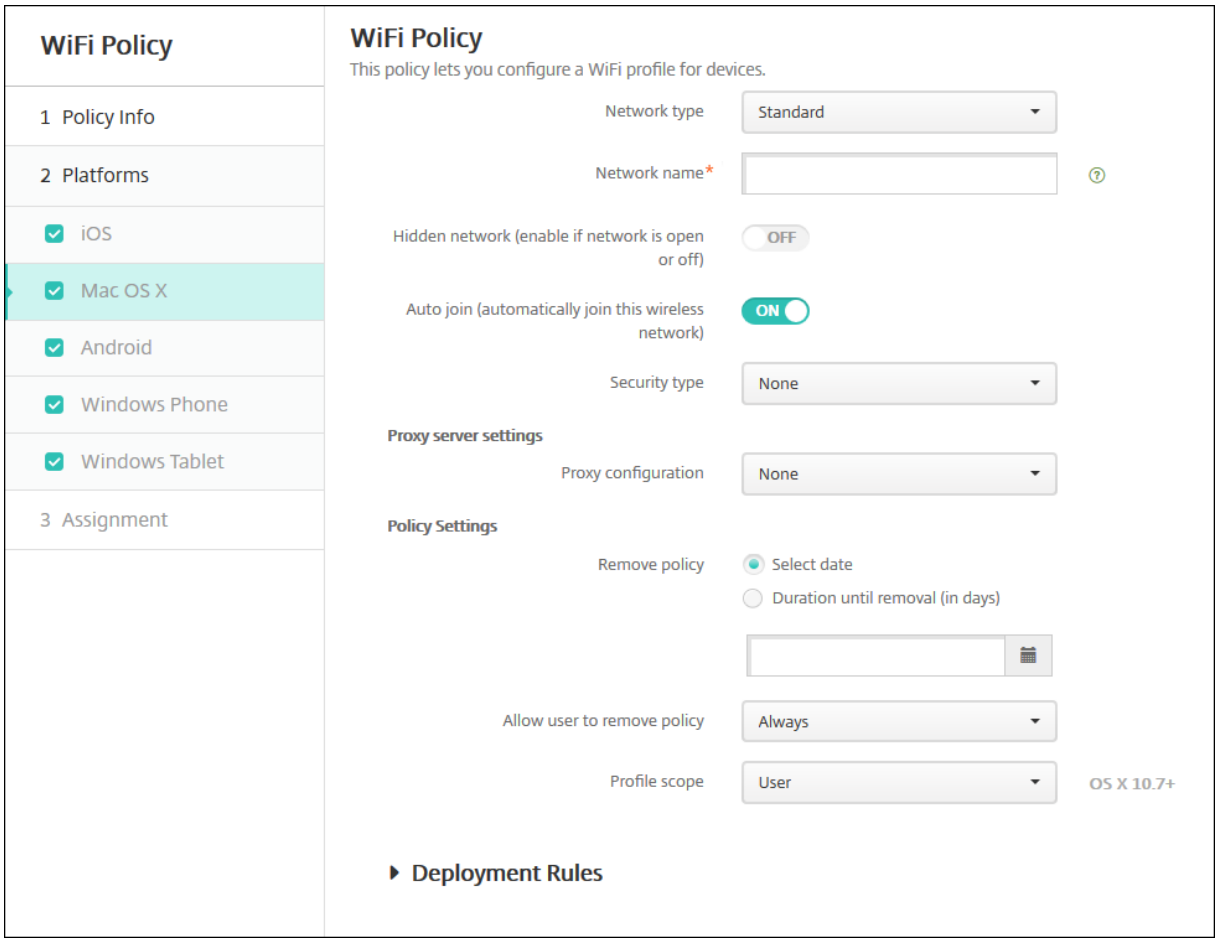
WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise) settings for iOS

When you choose any of these settings, their settings are listed after **Proxy server settings**.

- **Protocols, accepted EAP types:** 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**.
- **Protocols, EAP-FAST:** 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 XenMobile.
      - **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**.
- **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:
    * **Hostname/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**. This option is available only on iOS 7.0 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. Only available for iOS 6.0 and later.

macOS settings



- **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**.
- **Hidden network (enable if network is open or off):** Choose whether the network is hidden.
- **Auto Join (automatically join this wireless network):** Choose whether the network is joined automatically. If a device is already connected to another network, it won'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.

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.

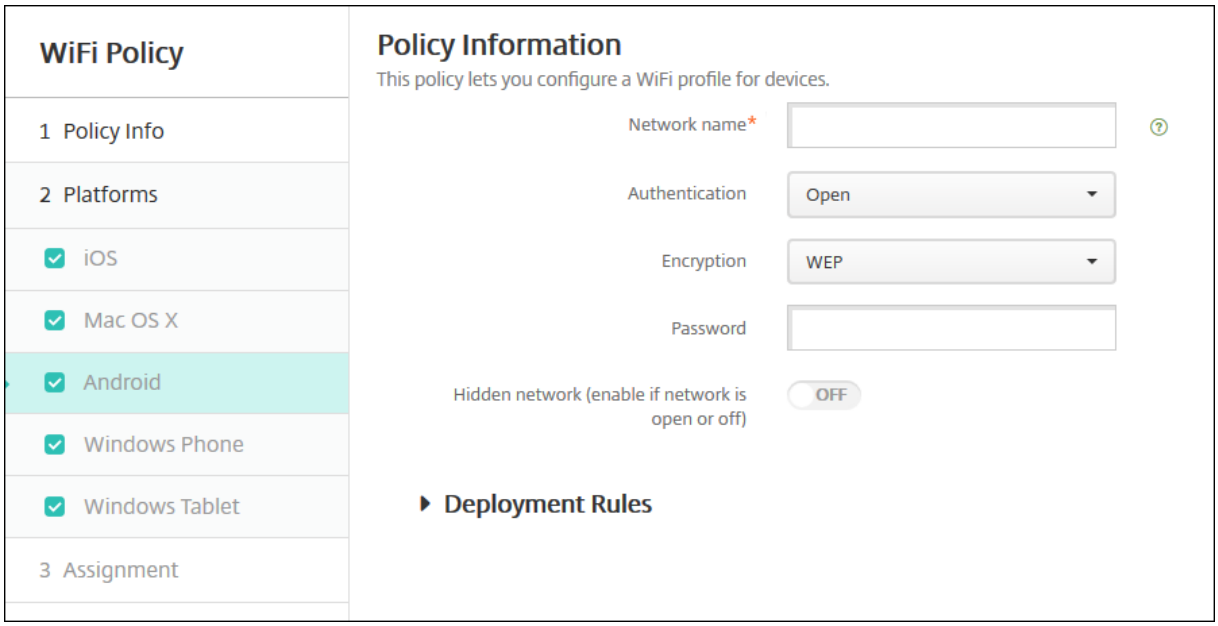
WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise) settings for macOS

When you choose any of these settings, their settings are listed after **Proxy server settings**.

- **Protocols, accepted EAP types:** 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**.
- **Protocols, EAP-FAST:** 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 XenMobile.
      - **Provisioning PAC anonymously**
- **Authentication:**
  - **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**.
- **Use as a Login Window configuration:** Choose whether to use the same credentials entered at the login window to authenticate the user.
- **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:
    * **Hostname/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**. This option is available only on iOS 7.0 and later.

Android settings



- **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.

Open, Shared settings for Android

- **Encryption:** In the list, choose either **Disabled** or **WEP**. The default is **WEP**.
- **Password:** Type an optional password.

WPA, WPA-PSK, WPA2, WPA2-PSK settings for Android

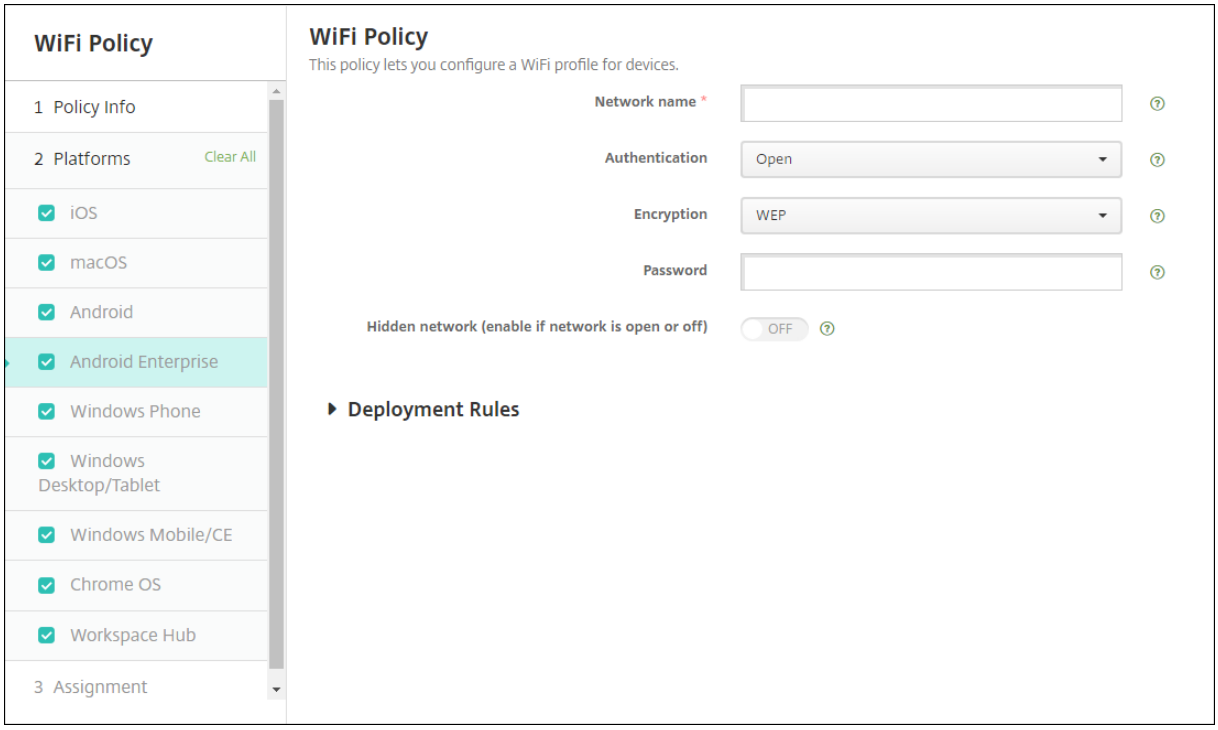
- **Encryption:** In the list, choose either **TKIP** or **AES**. The default is **TKIP**.
- **Password:** Type an optional password.

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**.
- **Hidden network (Enable if network is open or off):** Choose whether the network is hidden.

Android Enterprise settings



- **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.

Open, Shared settings for Android

- **Encryption:** In the list, choose either **Disabled** or **WEP**. The default is **WEP**.
- **Password:** Type an optional password.

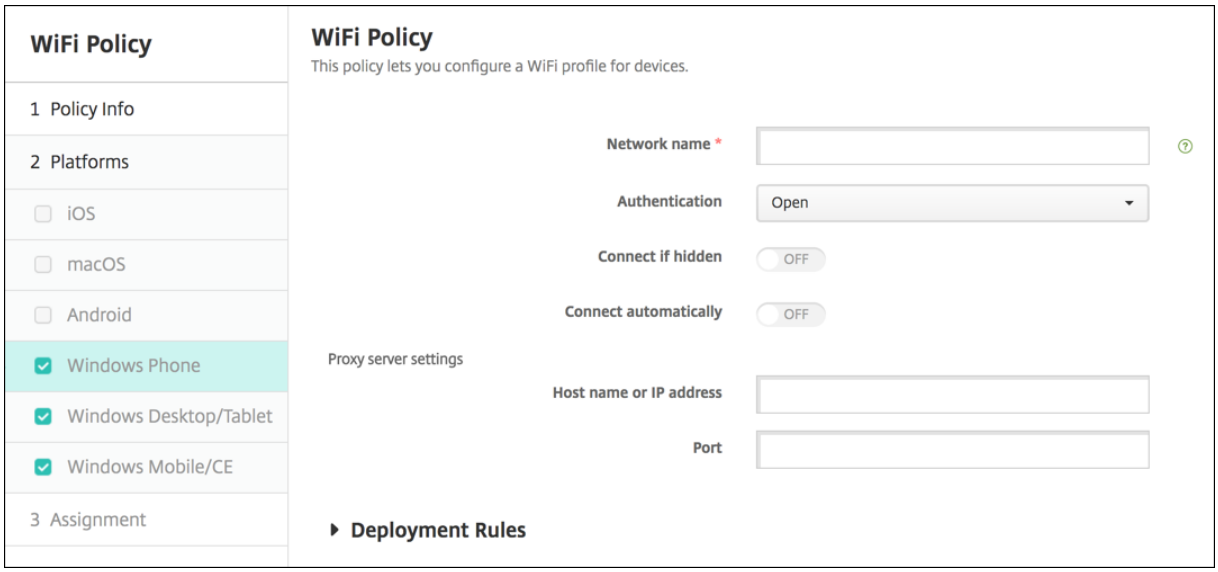
WPA, WPA-PSK, WPA2, WPA2-PSK settings for Android

- **Encryption:** In the list, choose either TKIP or AES. The default is TKIP.
- **Password:** Type an optional password.

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**.
- **Hidden network (Enable if network is open or off):** Choose whether the network is hidden.

Windows Phone settings



- **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, use of WPA-2 Enterprise requires that you configure SCEP. SCEP configuration enables XenMobile 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

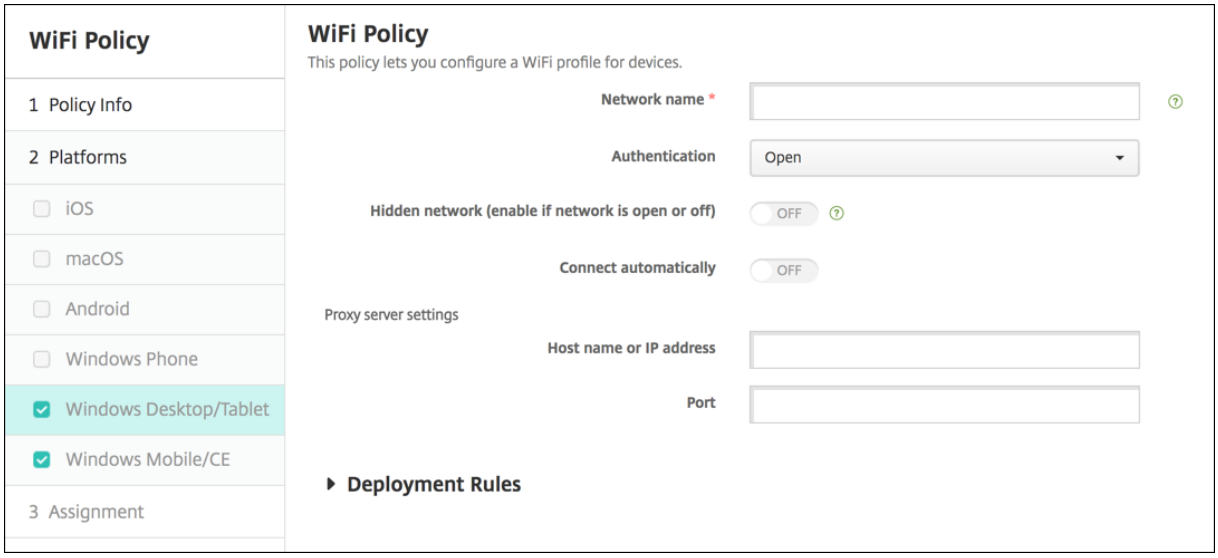
- **Encryption:** In the list, choose either **AES** or **TKIP** to set the type of encryption. The default is **AES**.
- **Connect if hidden:** Choose whether to connect when the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.

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 via Simple Certificate Enrollment Protocol (SCEP).
- **Credential provider for SCEP:** In the list, choose the SCEP credential provider. The default is **None**.
- **Proxy server settings**
  - **Host name or IP address:** Type the name or IP address of the proxy server.
  - **Port:** Type the port number for the proxy server.
- **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.

Windows 10 settings



- **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, use of WPA-2 Enterprise requires that you configure SCEP. SCEP configuration enables XenMobile 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

- **Hidden network (Enable if network is open or off):** Choose whether the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.

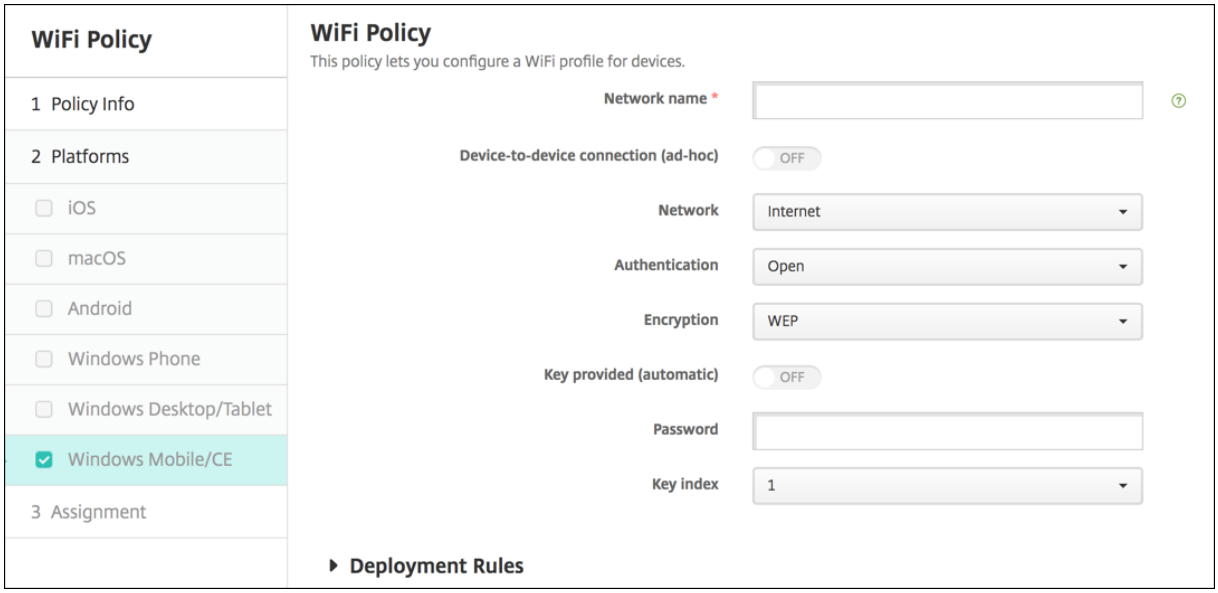
WPA Personal, WPA-2 Personal settings for Windows 10

- **Encryption:** In the list, choose either **AES** or **TKIP** to set the type of encryption. The default is **AES**.
- **Hidden network (Enable if network is open or off):** Choose whether the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.

WPA-2 Enterprise settings for Windows 10

- **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 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 by using Simple Certificate Enrollment Protocol (SCEP).
- **Credential provider for SCEP:** In the list, choose the SCEP credential provider. The default is **None**.

Windows Mobile/CE settings



- **Network name:** Type the SSID that is in the list of available networks on the user device.
- **Device-to-device connection (ad-hoc):** Allows two devices to connect directly. Default is **Off**.
- **Network:** Choose whether the device is connected to an external internet source or an Office intranet.

- **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

The following sections list the options you configure for each of the preceding connection types.

Open settings for Windows Mobile/CE

- **Hidden network (Enable if network is open or off):** Choose whether the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.

WPA Personal, WPA-2 Personal settings for Windows Mobile/CE

- **Encryption:** In the list, choose either **AES** or **TKIP** to set the type of encryption. The default is **AES**.
- **Hidden network (Enable if network is open or off):** Choose whether the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.

WPA-2 Enterprise settings for Windows Mobile/CE

- **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 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 by using the Simple Certificate Enrollment Protocol (SCEP).
- **Credential provider for SCEP:** In the list, choose the SCEP credential provider. The default is **None**.
- **Key provided (automatic):** Choose whether the key is automatically provided. Default is **Off**.
- **Password:** Type the password in this field.
- **Key index:** Choose the key index. Available options are **1**, **2**, **3**, and **4**.

Windows CE certificate device policy

July 3, 2018

You can create a device policy in XenMobile to create and deliver Windows Mobile/CE certificates from an external PKI to user devices. For more information about Certificates and PKI entities, see Certificates.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows CE settings

- **Credential provider:** In the list, click the credential provider. The default is **None**.
- **Password of generated PKCS#12:** Type the password used to encrypt the credential.
- **Destination folder:** In the list, click the destination folder for the credential or click **Add new** to add a folder not already in the list. The predefined options are:
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Destination file name:** Type the name of the credential file.

Windows Information Protection device policy

July 2, 2020

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 XenMobile to specify the apps that require Windows Information Protection at the enforcement level you set. The Windows Information Protection policy is for Windows 10 version 1607 and later supervised Phone, Tablet, and Desktop.

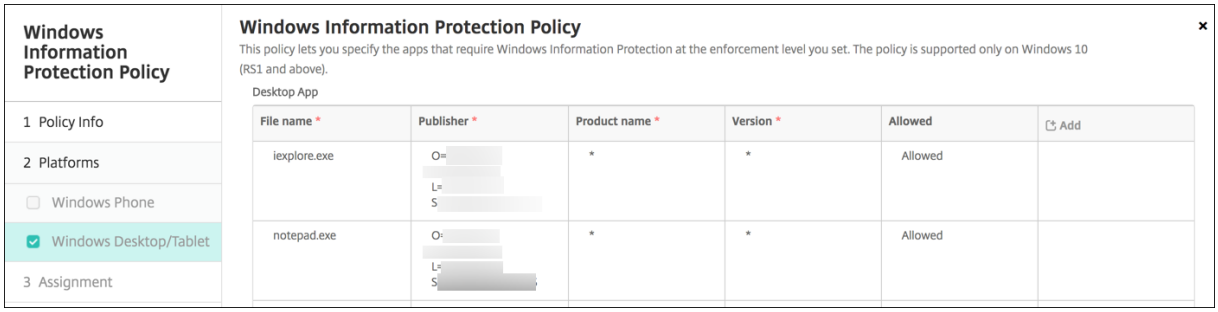
XenMobile includes some common apps and you can add others. You specify for the policy an enforcement level that affects the user experience. For example, you can:

- 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 XenMobile.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows 10 settings



- **Desktop App** (Windows 10 Tablet), **Store App** (Windows 10 Phone and Tablet): XenMobile 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.

  - **AppLocker XML:** 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. XenMobile combines the uploaded AppLocker XML and the configured desktop and store apps in the policy sent to the device. For more information, see Recommended deny 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 "	" 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 a comma 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`
- **IP ranges list is authoritative:** To prevent auto-detection of IP ranges by Windows, change this setting to **On**. 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 WiFi hotspots at hotels and restaurants. Use commas 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 commas 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 commas to separate list items. For example:

  ```
  domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.
  domain2.com
  ```

- **Set Require 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 **Require protection under lock** appears. Default is **Off**.
- **Require 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 XenMobile 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
   ```

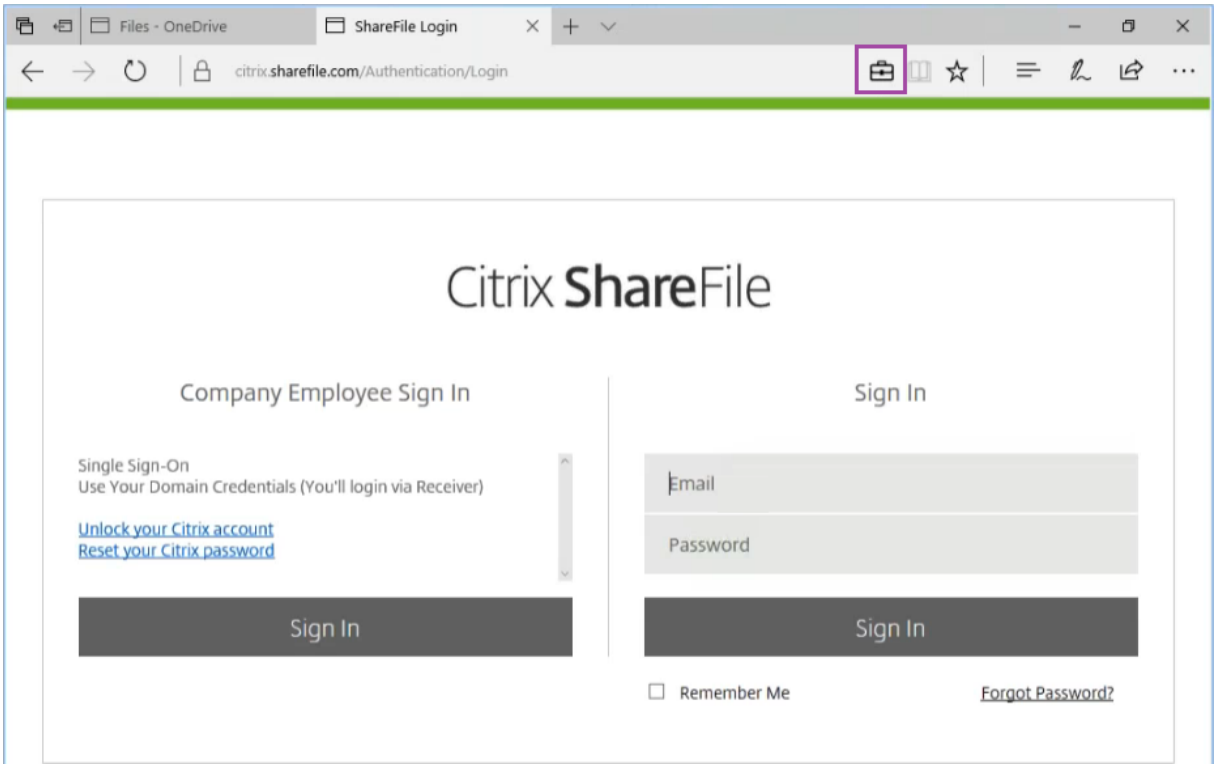
3. When prompted, enter a password to protect the private key file.

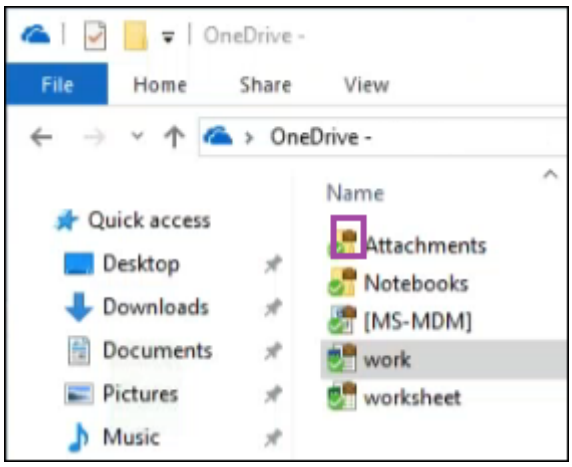
   The cipher command creates a .cer and a .pfx file.

4. In the XenMobile console, go to **Settings > Certificates** and import the .cer file, which applies to both Windows 10 tablets and phones.

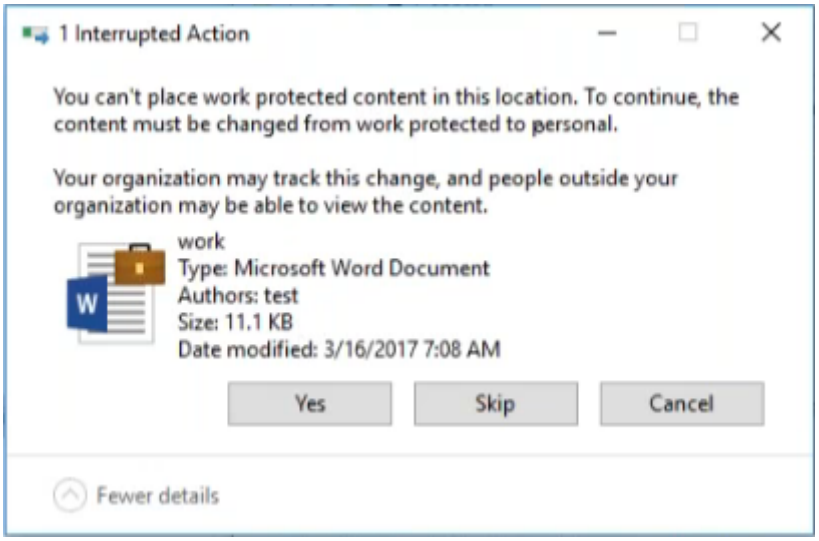
User experience

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.



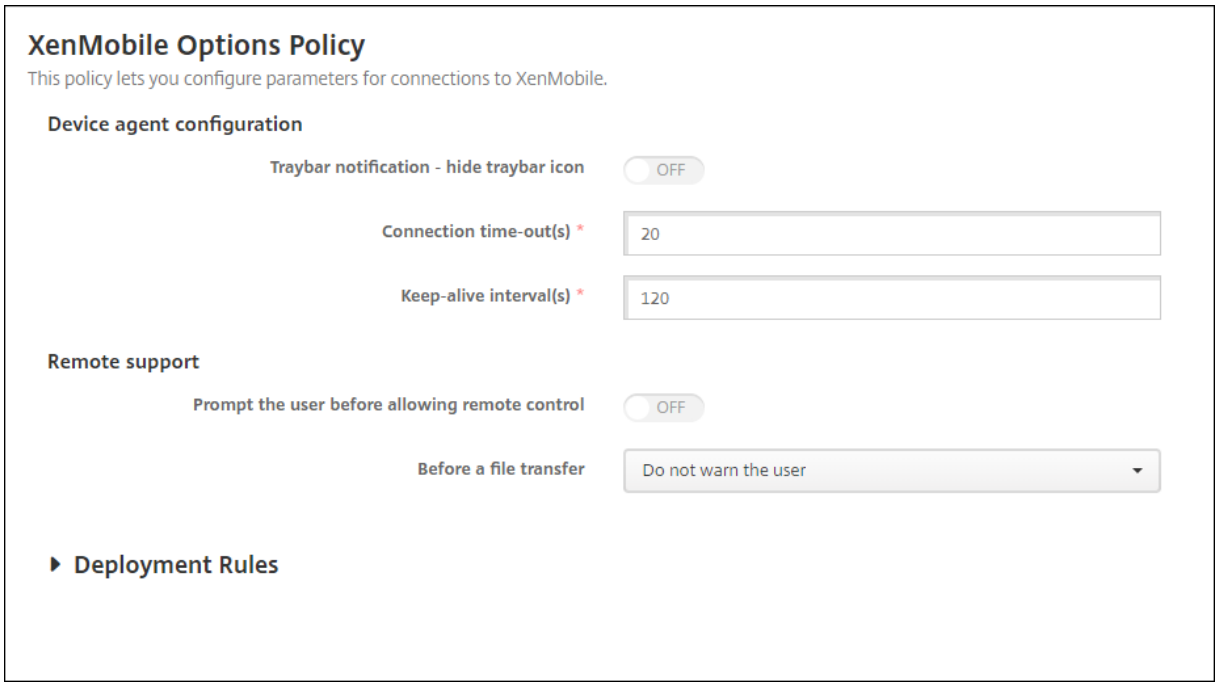
XenMobile options device policy

August 31, 2020

You add a XenMobile options policy to configure Secure Hub behavior when connecting to XenMobile from Android and Windows Mobile/CE devices.

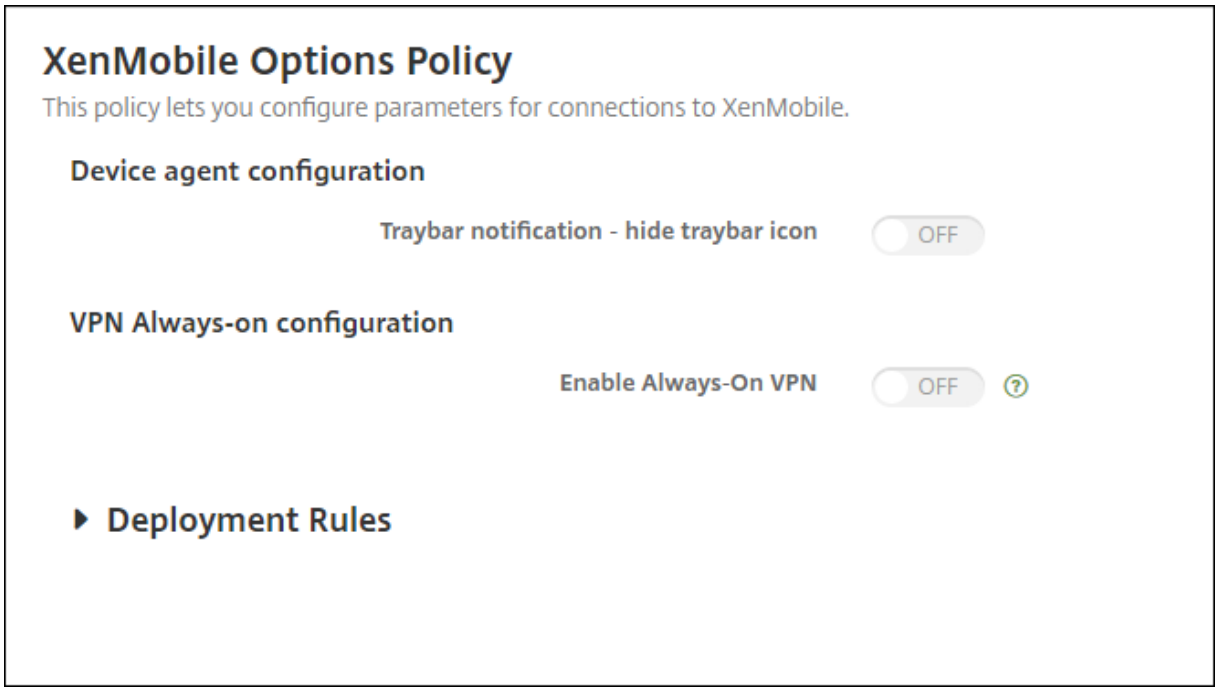
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Android settings



- **Traybar notification - hide traybar icon:** Select whether the traybar icon is hidden or visible. The default is **Off**.
- **Connection: time-out(s):** 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 interval(s):** 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**.

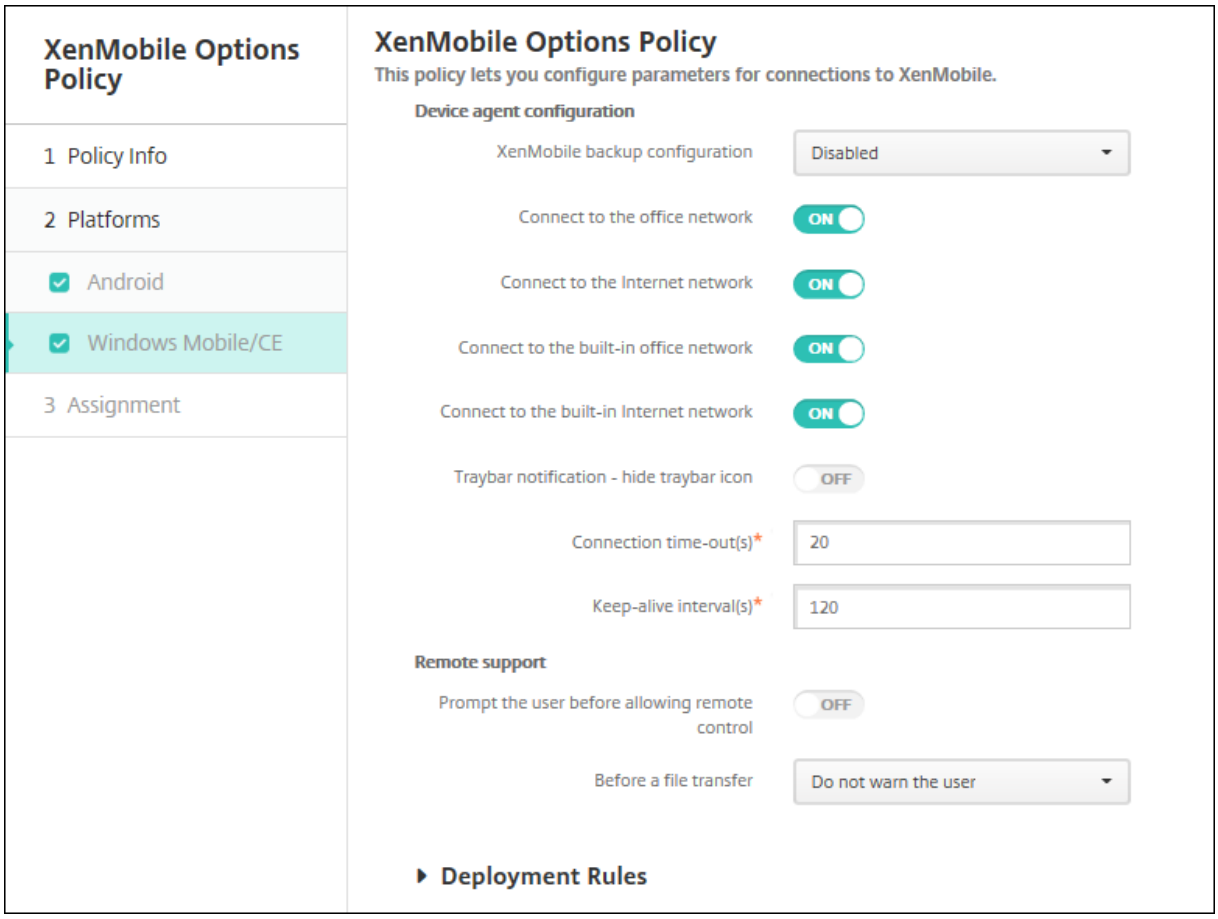
Android Enterprise settings



Supported starting with Android version 7.

- **Traybar notification - hide traybar icon:** Select whether the traybar 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 and 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.

Windows Mobile/CE settings



- **Device agent configuration**
  - **XenMobile backup configuration:** In the list, click an option for backing up the XenMobile configuration on the users' devices. The default is **Disabled**. Available options are:
    - Disabled
    - At first connection after XenMobile installation
    - At first connection after each device reboot
  - **Connect to the office network**
  - **Connect to the Internet network**
  - **Connect to the built-in office network:** When set to **On**, XenMobile automatically detects the network.
  - **Connect to the built-in Internet network:** When set to **On**, XenMobile automatically detects the network.
  - **Traybar notification - hide traybar icon:** Select whether the traybar icon is hidden or visible. The default is **Off**.
  - **Connection time-out(s):** 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 interval(s):** Type the length of time in seconds to keep a connection open. The default is 120 seconds.
- **Remote support**
  - **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**.

XenMobile uninstall device policy

July 3, 2018

You can add a device policy in XenMobile to uninstall XenMobile from Android and Window Mobile/CE devices. When deployed, this policy removes XenMobile from all devices in the deployment group.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Configure Android and Windows Mobile/CE settings

- **Uninstall XenMobile from devices:** Select whether to uninstall XenMobile from every device to which you deploy this policy. The default is **Off**.

Add apps

May 10, 2021

Adding apps to XenMobile provides mobile application management (MAM) capabilities. XenMobile assists with application delivery, software licensing, configuration, and application life cycle management.

MDX-enabling apps is an important part of preparing most types of apps for distribution to user devices. For an introduction to MDX, see About the MDX Toolkit 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 Service or 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 XenMobile 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 apps
- Distribute Apple apps

App types and features

The following table summarizes the types of apps you can deploy with XenMobile.

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 Service or Toolkit. For the mobile productivity apps, download the public-store MDX files from Citrix downloads. Then, add the apps to XenMobile.	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 XenMobile.	Add a public app store app

App type	Sources	Notes	See
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
Enterprise	Private apps, including Win32 apps, that aren't MDX-enabled. Private Android Enterprise apps that are MDX-enabled. Enterprise apps reside in Content Delivery Network locations or XenMobile servers.	Add the apps to XenMobile.	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 XenMobile.	Add a Web link

When planning app distribution, consider these features:

- About silent installations
- About required and optional apps
- About app categories
- Enable Microsoft 365 apps
- Apply workflows

- App store and Citrix Secure Hub branding

About silent installations

Citrix supports the silent installation and upgrade of iOS, Android Enterprise, 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, the apps install in the Android work profile on the device. For details, see Android Enterprise.
- 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

- XenMobile Server 10.6 (minimum version)
- Secure Hub 10.5.15 for iOS and 10.5.20 for Android (minimum versions)
- MAM SDK, MDX Service, or MDX Toolkit 10.6 (minimum version)

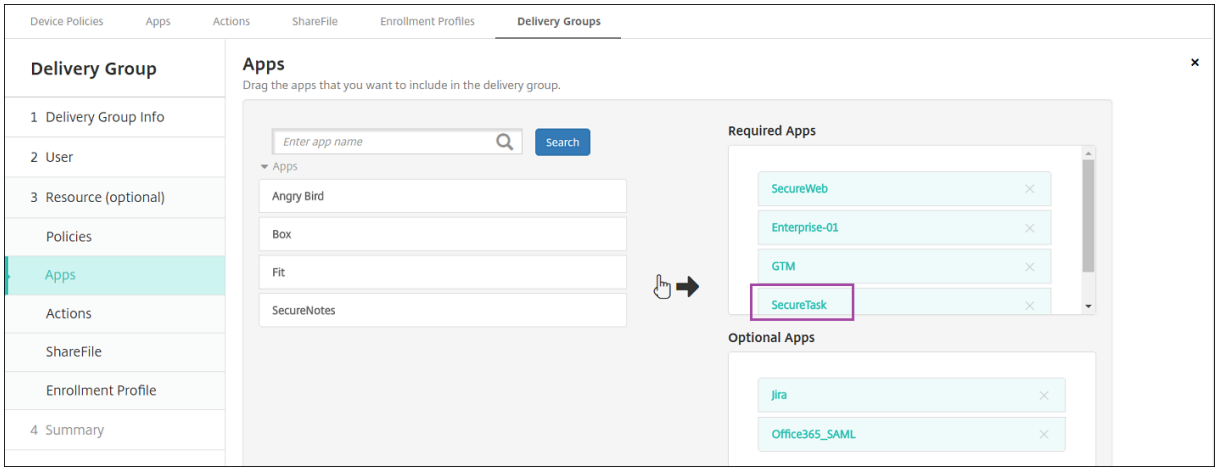
- Custom server property, force.server.push.required.apps

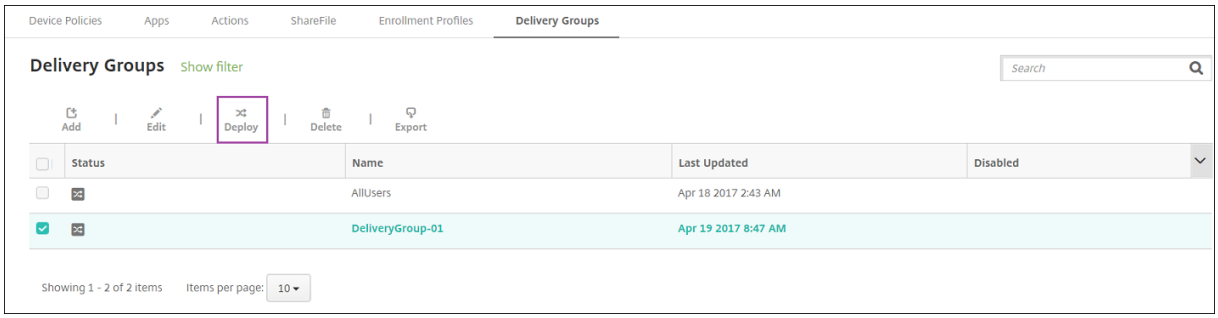
  The forced deployment of required apps is disabled by default. To enable the feature, create a Custom Key server property. Set the **Key** and **Display name** to **force.server.push.required.apps** and set the **Value** to **true**.

- After you upgrade XenMobile Server and Secure Hub: Users with enrolled devices must sign off and then sign on to Secure Hub, one time, to obtain the required app deployment updates.

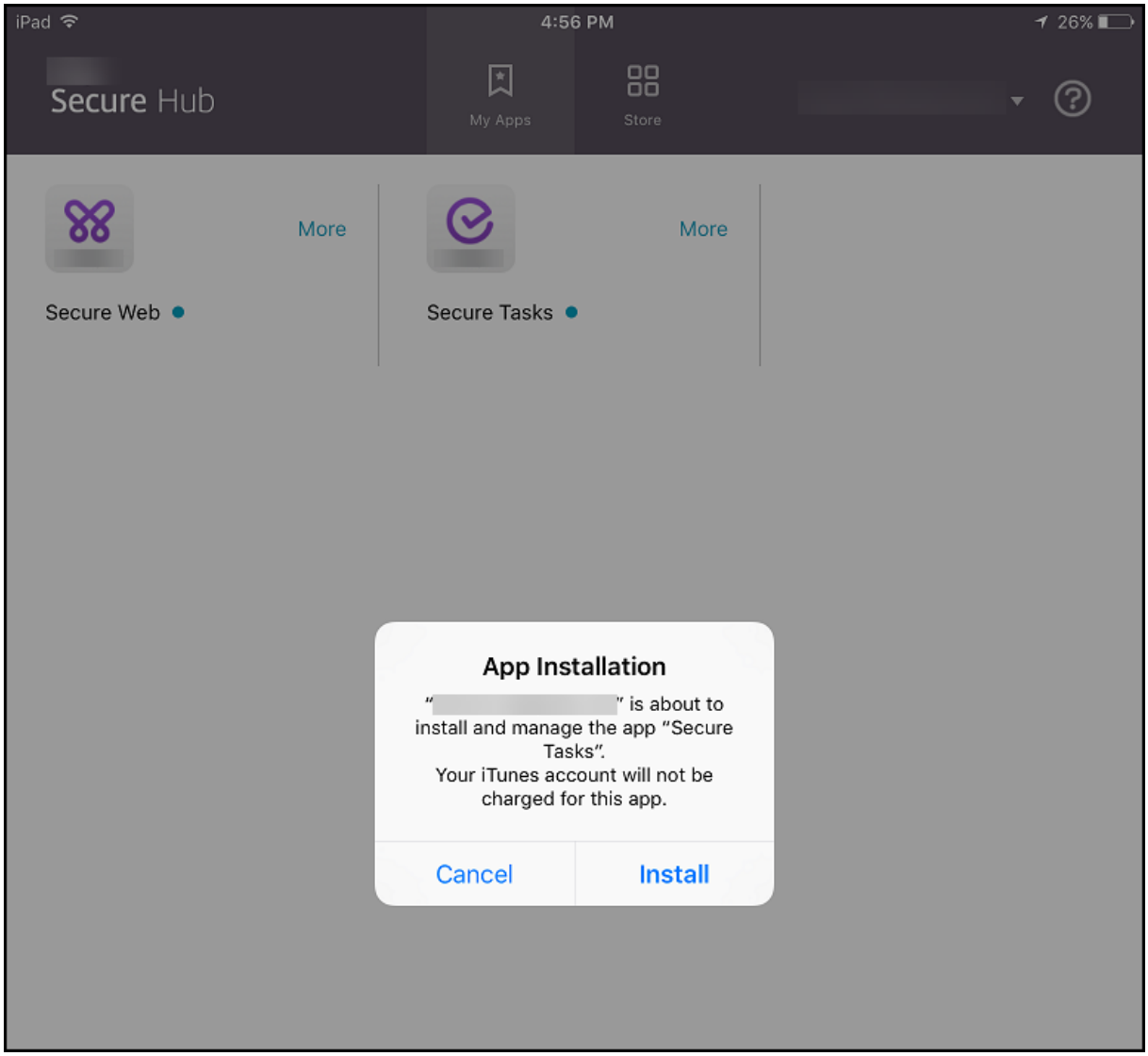
Examples

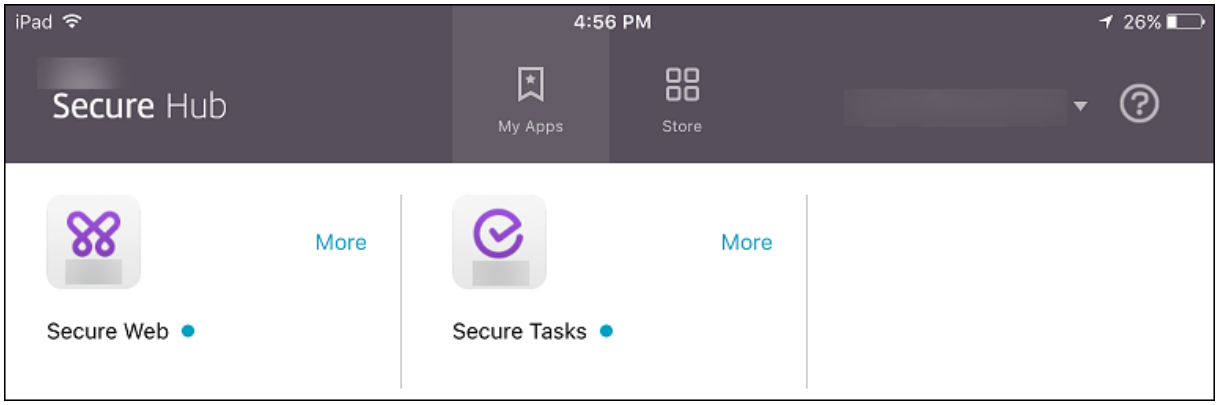
The following examples show the sequence of adding an app named Secure Tasks to a delivery group and then deploying the delivery group.





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. The 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 XenMobile App during initial enrollment. The required app is installed on the device.
2. Update the app on the XenMobile console.
3. Use the XenMobile 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 XenMobile App during initial enrollment. The required app is installed on the device.
2. Use the XenMobile 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 XenMobile App during initial enrollment. The required app is installed on the device.
2. Update the app on the XenMobile console.
3. Use the XenMobile 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**.

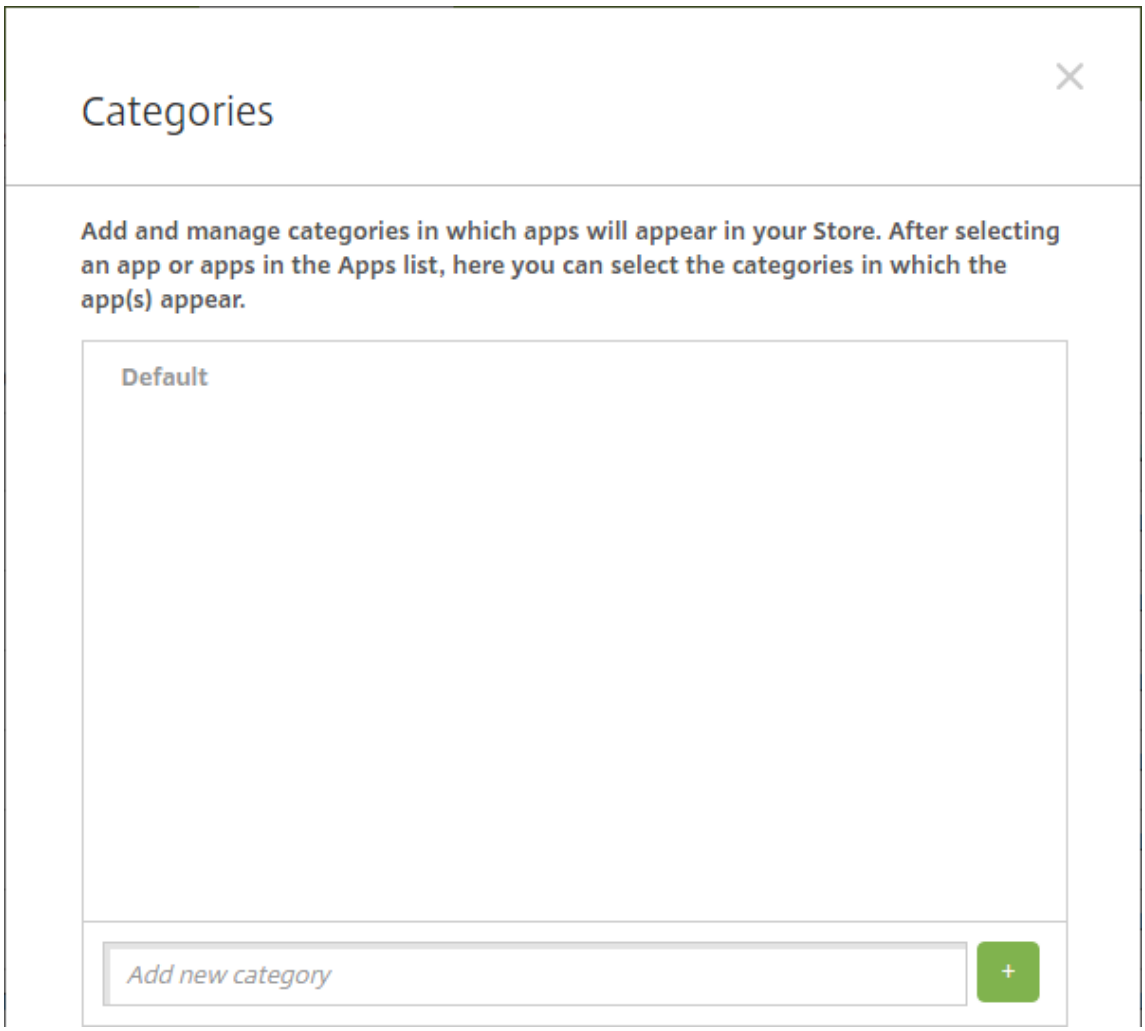
Recommended: Use a special delivery group to temporarily change an app to optional, so that specific users can uninstall the app. You can then change an existing required app to optional, deploy the app to that delivery group, and then uninstall the app from those devices. After that, if you want future 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 XenMobile. 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.

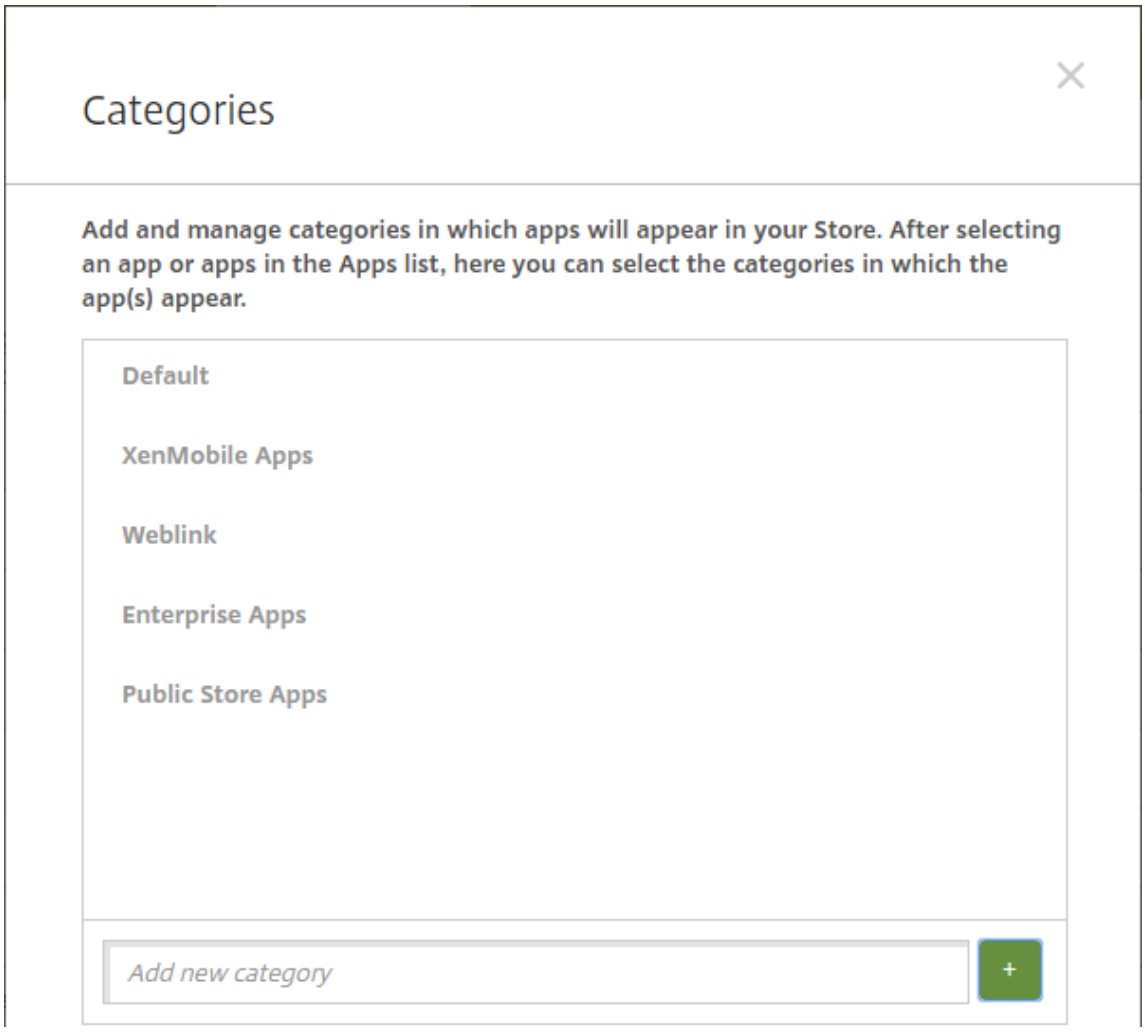
When you add or edit an app, web link, or store, you can add the app to one or more of the configured categories.

1. In the XenMobile 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.



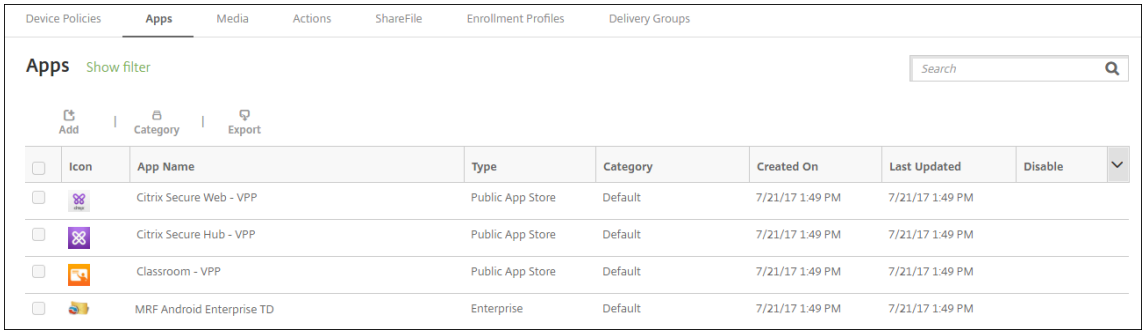
3. When you're done adding categories, close the **Categories** dialog box.
4. On the **Apps** page, you can place an existing app into a new category.
   - Select the app you want to categorize.
   - Click **Edit**. The **App Information** page appears.
   - In the **App category** list, apply the new 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

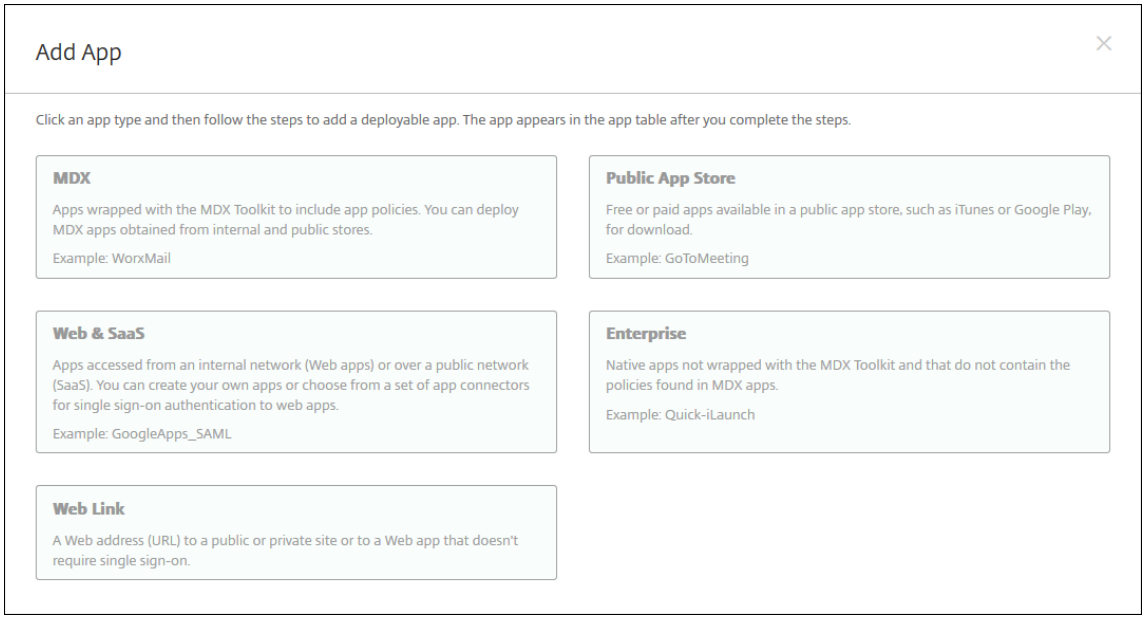
When you receive an MDX file for an iOS or Android app, you can upload the app to XenMobile. After you upload the app, you can configure app details and policy settings. For more information about the app policies that are available for each device platform type, see:

- MAM SDK Overview
- MDX Policies at a Glance

1. In the XenMobile console, click **Configure > Apps**. The **Apps** page appears.

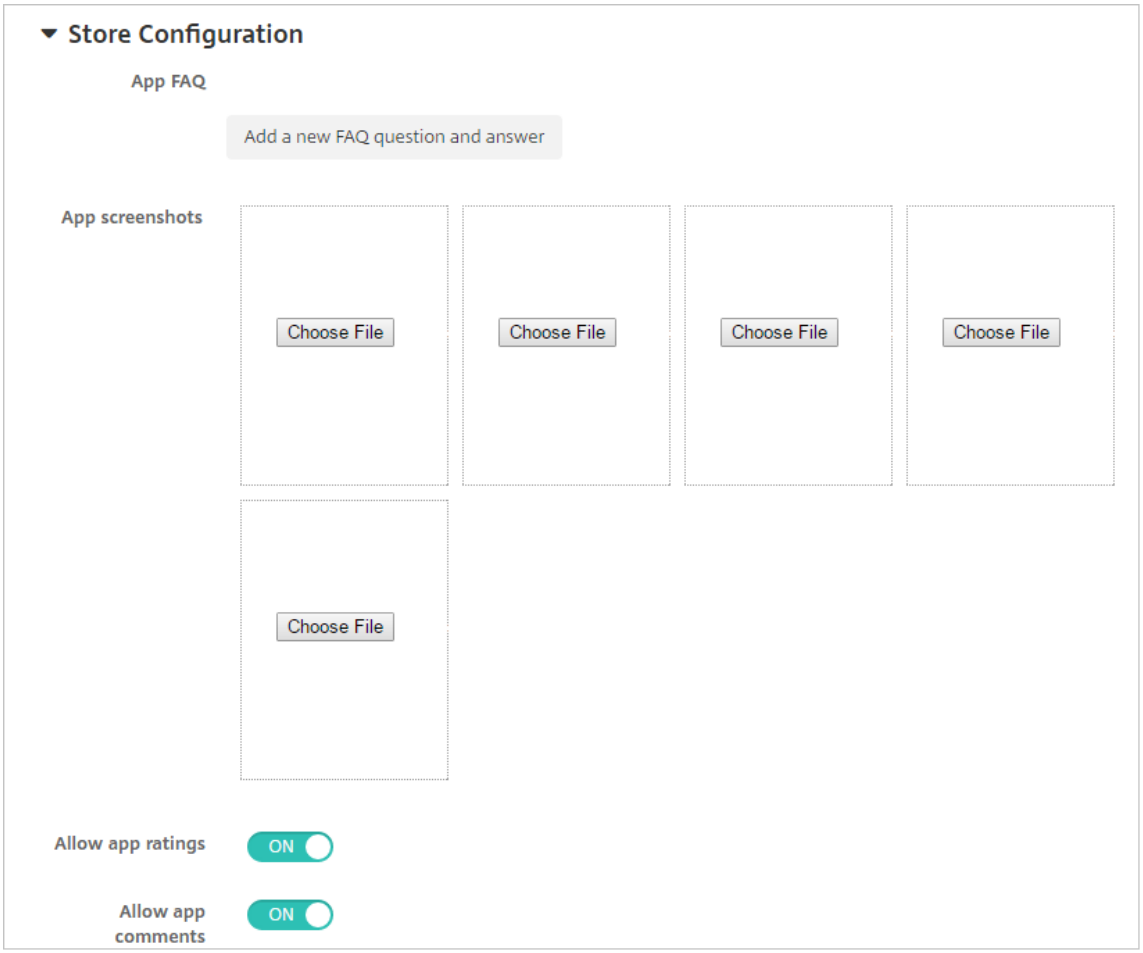


2. Click **Add**. The **Add App** dialog box appears.



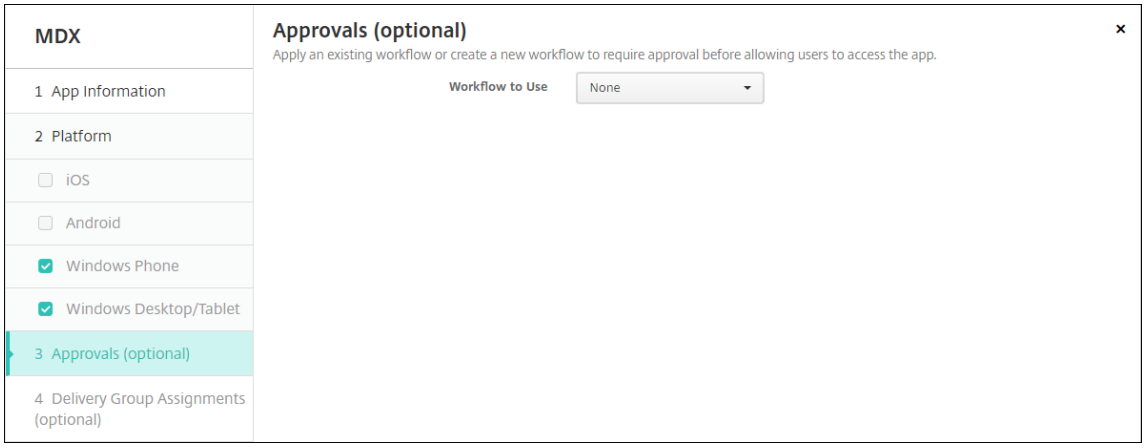
3. Click **MDX**. The **MDX App Information** page appears.
4. On the **App Information** pane, type the following information:
   - **Name:** Type a descriptive name for the app. The name appears under **App Name** on the **Apps** table.
   - **Description:** Type an optional description of the app.
   - **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.

5. Click **Next**. The **App Platforms** page appears.
6. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.
7. To select an MDX file to upload, click **Upload** and navigate to the file location.
8. 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**.
9. Configure the **MDX Policies**. MDX policies vary by platform and include options for such policy areas as authentication, device security, and app restrictions. In the console, each of the policies has a tooltip that describes the policy.
10. Configure the deployment rules. For information, see Deployment rules.
11. Expand **Store Configuration**.



- **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.

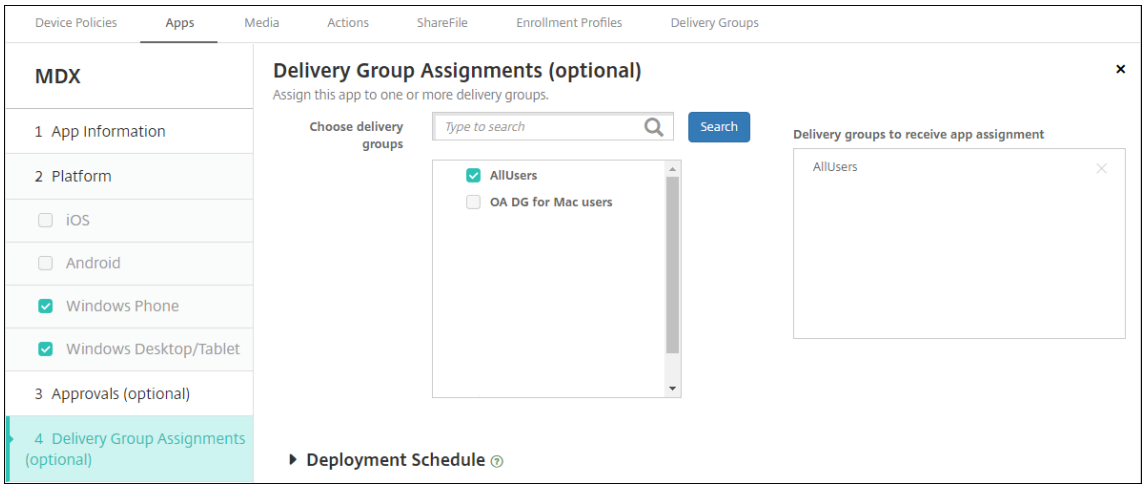
12. Click **Next**. The **Approvals** page appears.



To use workflows to require approval before allowing users to access the app, see Apply work-

flows. If you don't want to set up approval workflows, continue with the next step.

13. Click **Next**. The **Delivery Group Assignment** page appears.



14. 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.
15. 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 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**.

16. Click **Save**.

Add a public app store app

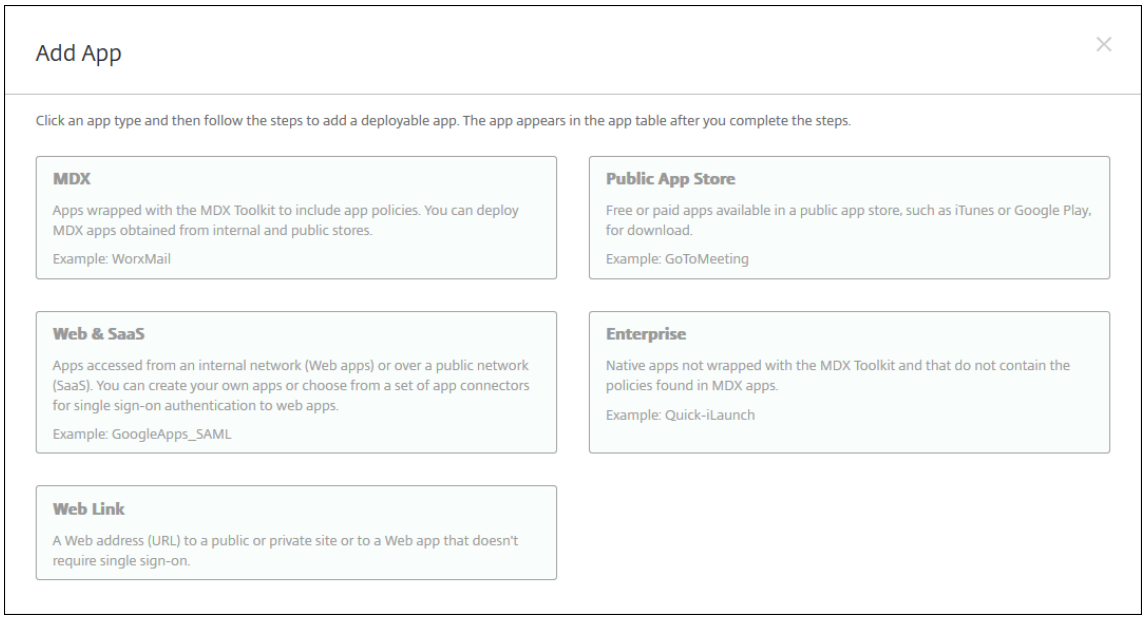
You can add free or paid apps to XenMobile that are available in a public app store, such as the Apple App Store or Google Play.

You can configure settings to retrieve app names and descriptions from the Apple App Store. When you retrieve the app information from the store, XenMobile 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 for an organization.

Configure app information and choose platforms to deliver the app to:

1. In the XenMobile console, click **Configure > Apps > Add**. The **Add App** dialog box appears.



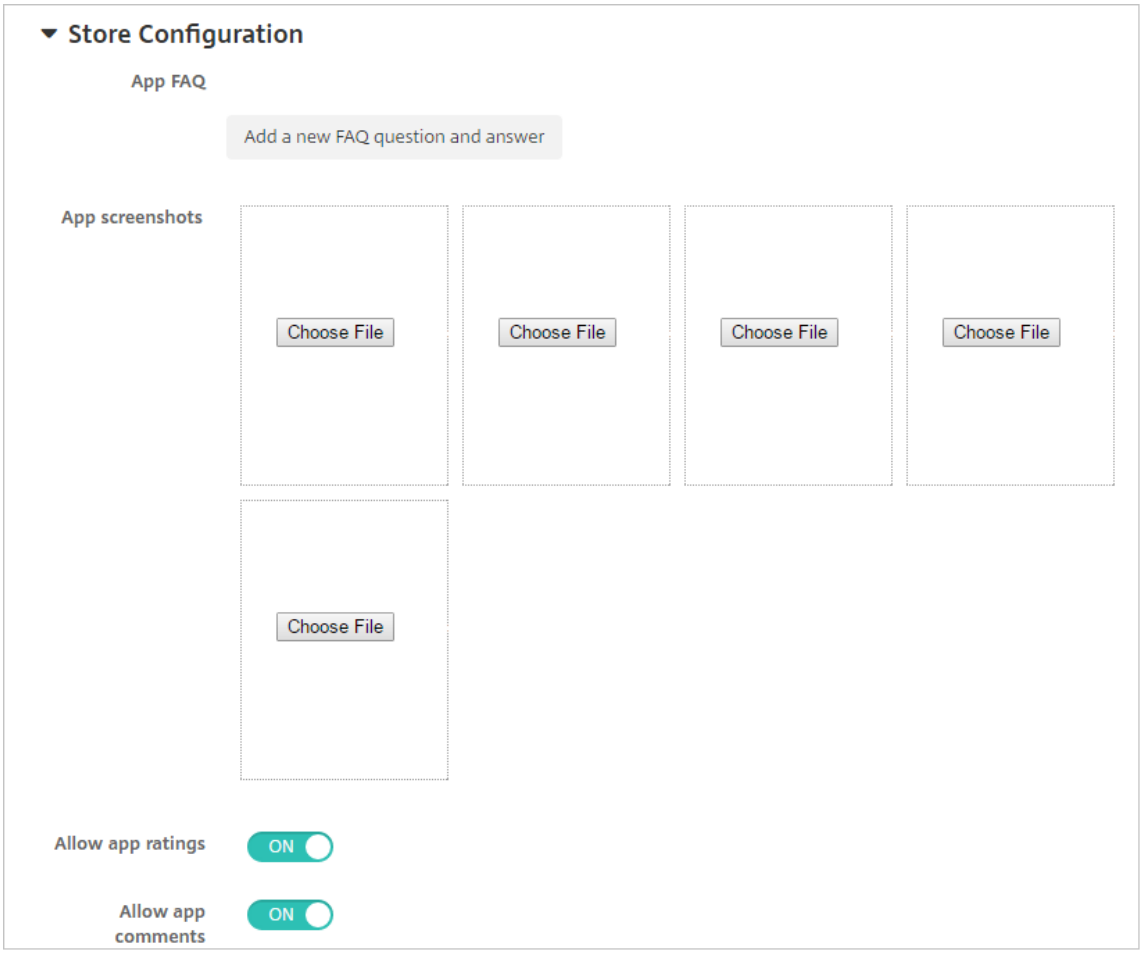
2. Click **Public App Store**. The **App Information** page appears.
3. On the **App Information** pane, type the following information:
   - **Name:** Type a descriptive name for the app. This name appears under **App Name** on the **Apps** table.
   - **Description:** Type an optional description of 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 Deployment rules.
2. Expand **Store Configuration**.



- **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.

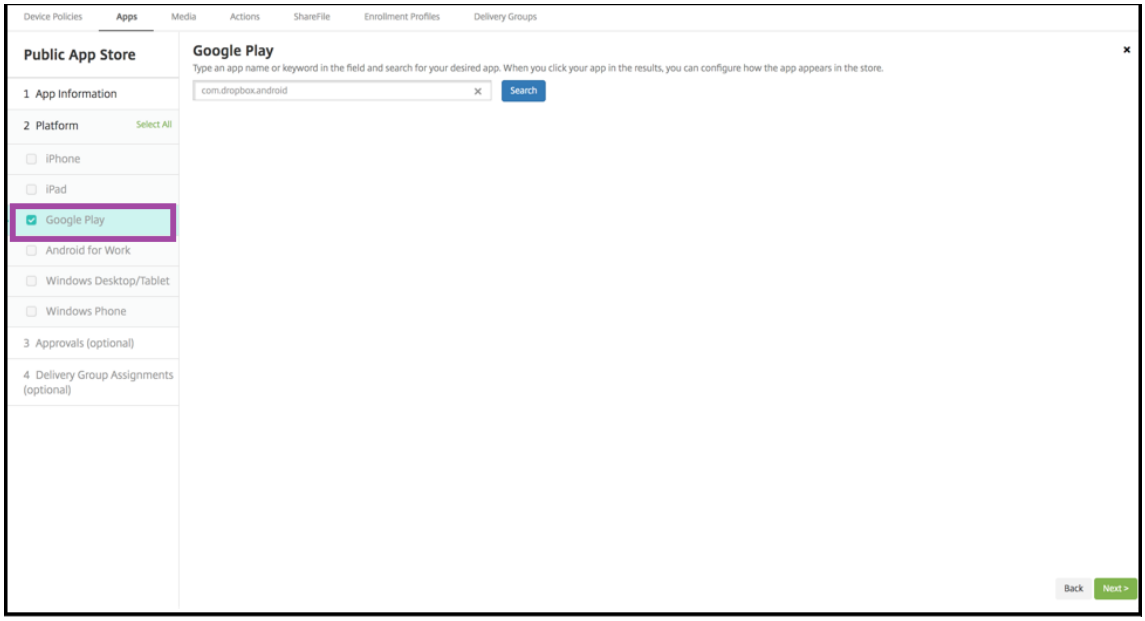
Configure app settings for Google Play apps

> **Note:**
>
> To make all apps in the Google Play store accessible from managed Google Play, use the XenMobile server property, **Access all apps in the managed Google Play store**. See Server properties. Setting this property to **true** allows the public Google Play store apps for all Android Enterprise users. You can then use can then use the Restrictions device policy to control access to these

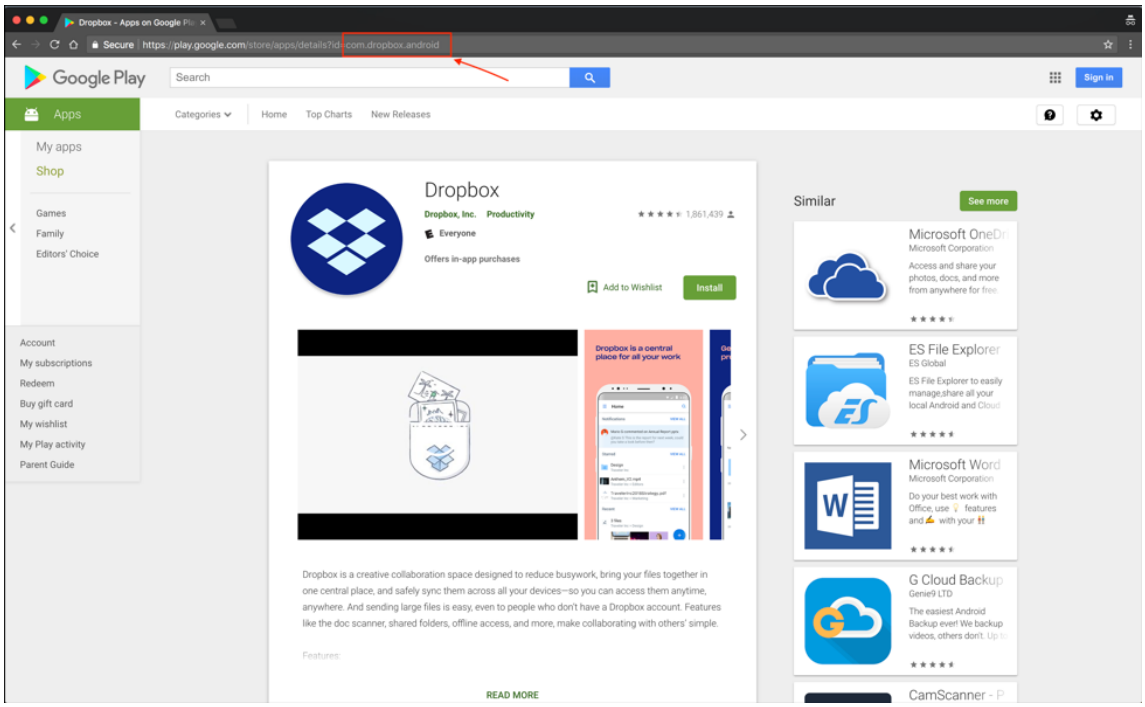
> apps.

Configuring settings Google Play store apps requires different steps than apps for other platforms. You must manually configure Google Play store app information.

1. Ensure that **Google Play** is selected under **Platforms**.

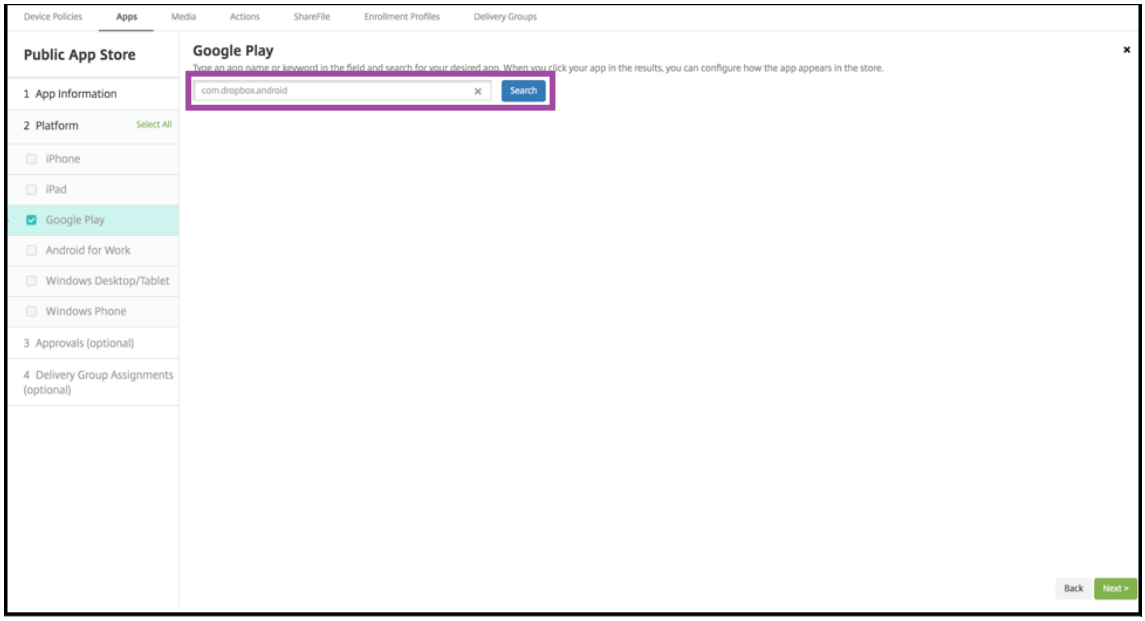


2. Go to the Google Play store. From the Google Play store, copy the package ID. The ID can be found in the URL of the app.

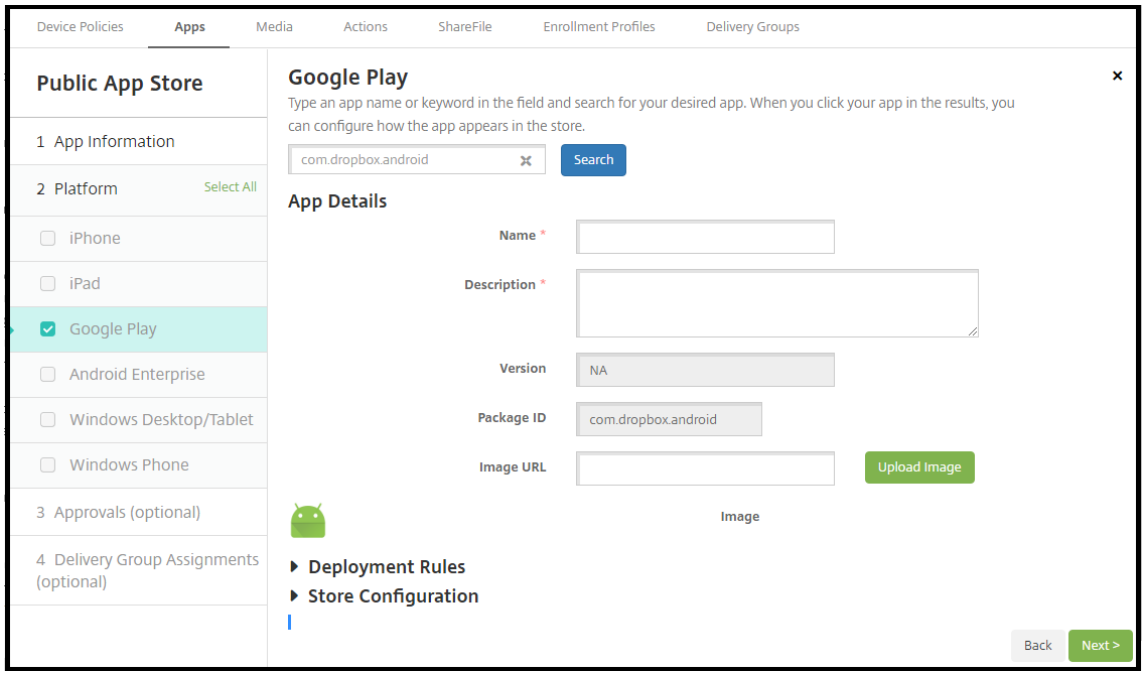


3. When adding a Public Store app in the XenMobile Server console, paste the package ID in the

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.

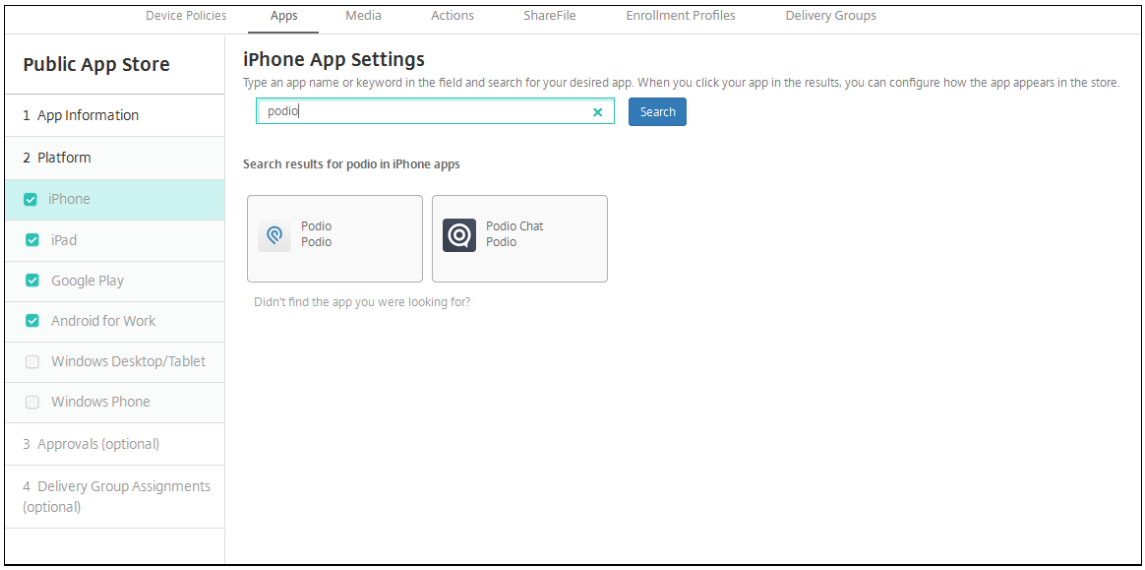
   c) Click **Upload image**. The image appears beside **Image**.

If you don't configure an image, the generic Android image appears with the app.

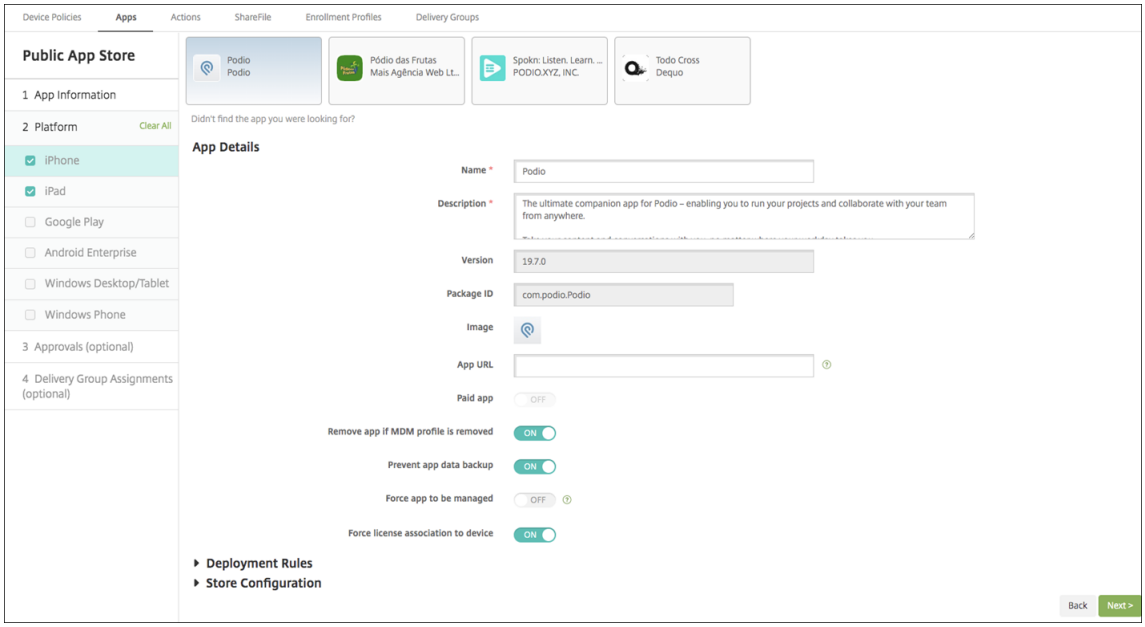
Configure app settings for iOS apps

1. Type the app name in the search box and click **Search**. Apps matching the search criteria appear. Apps matching the search criteria appear.

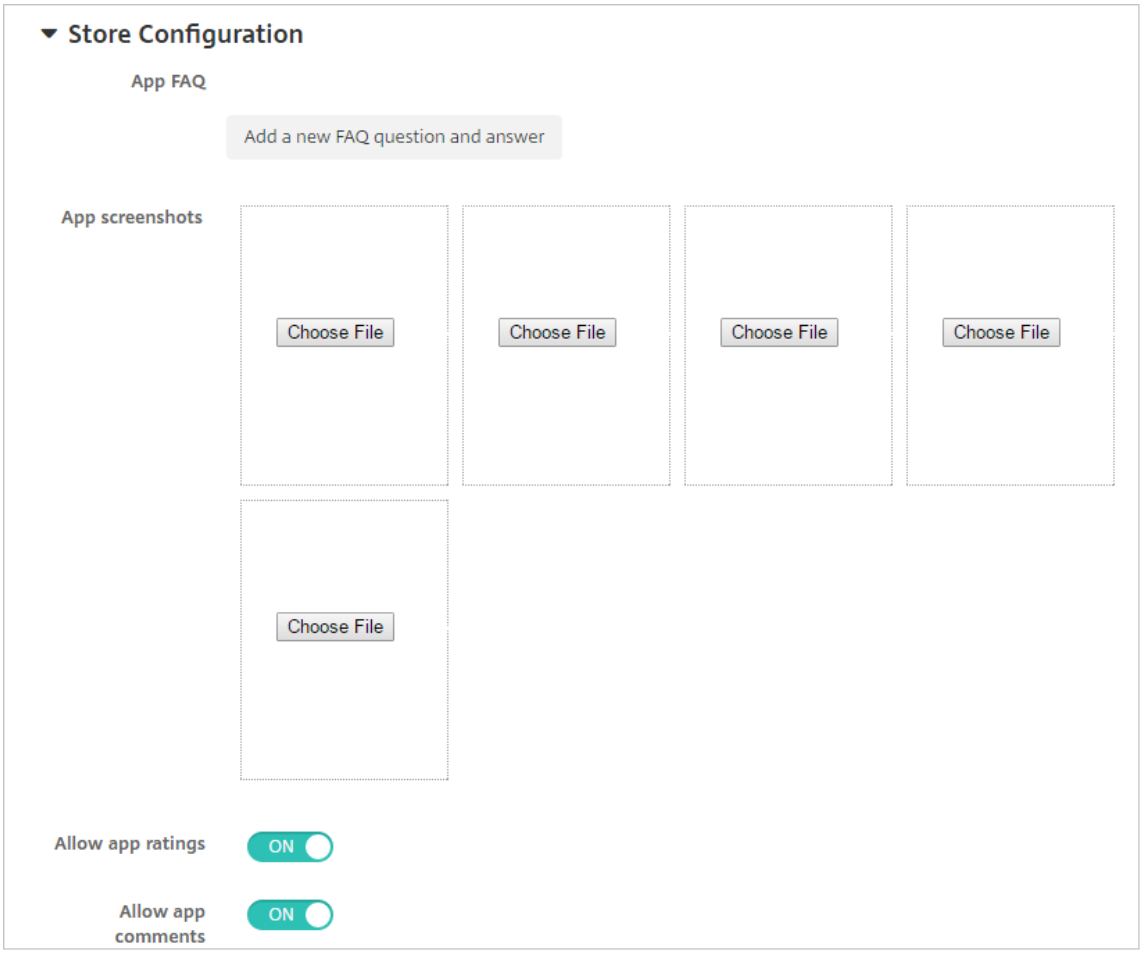
   The following figure shows the result of searching for **podio** in apps on an iPhone.



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.
    - **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:** Select whether, when the app is installed unmanaged, to prompt users to allow the app to be managed on unsupervised devices. The default is **OFF**. Available in iOS 9.0 and later.
    - **Force license to association to device:** Select whether to associate an app that has been developed with device association enabled to a device rather than to a user. Available in iOS 9 and later. If the app you chose does not support assignment to a device, this field can't be changed.
5. Configure the deployment rules. For information, see Deployment rules.
6. Expand **Store Configuration**.



- **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 XenMobile 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.

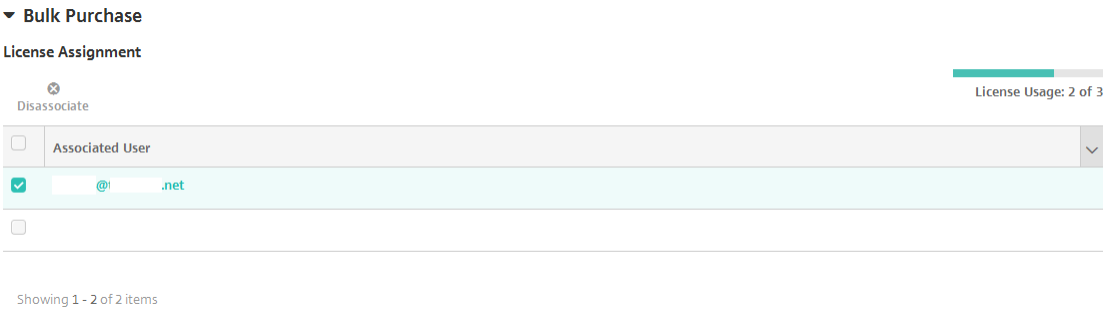
   The License Assignment table shows the number of licenses in use for the app, out of the total licenses available.

   You can disassociate Volume Purchase licenses for an individual user. Doing so ends the license assignments and frees licenses.

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** 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**.

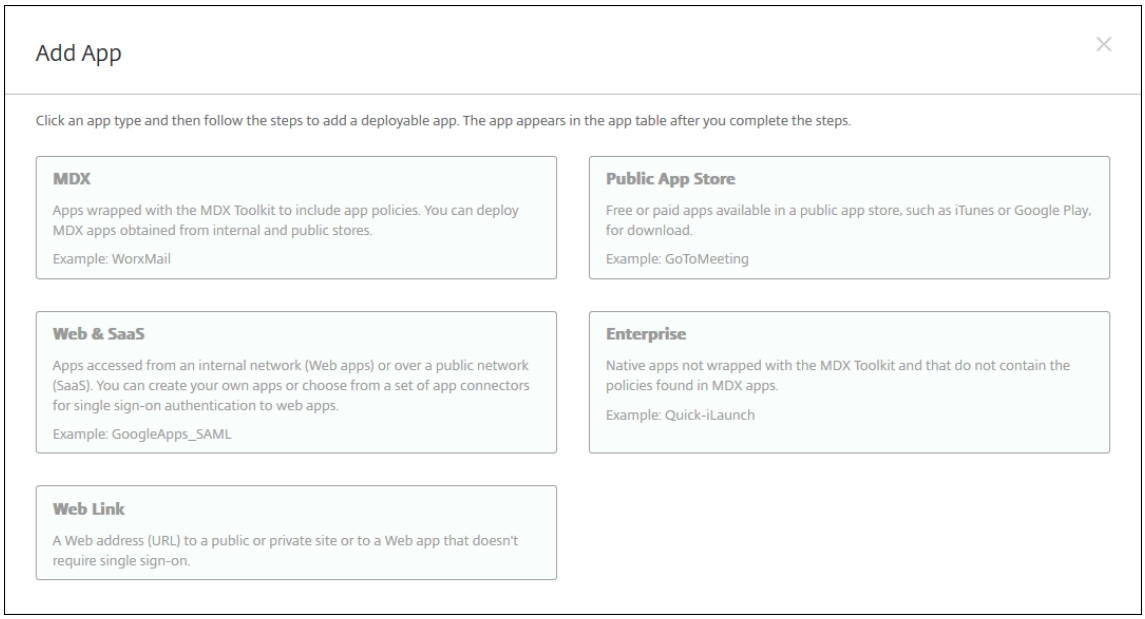
13. Click **Save**.

Add a Web or SaaS app

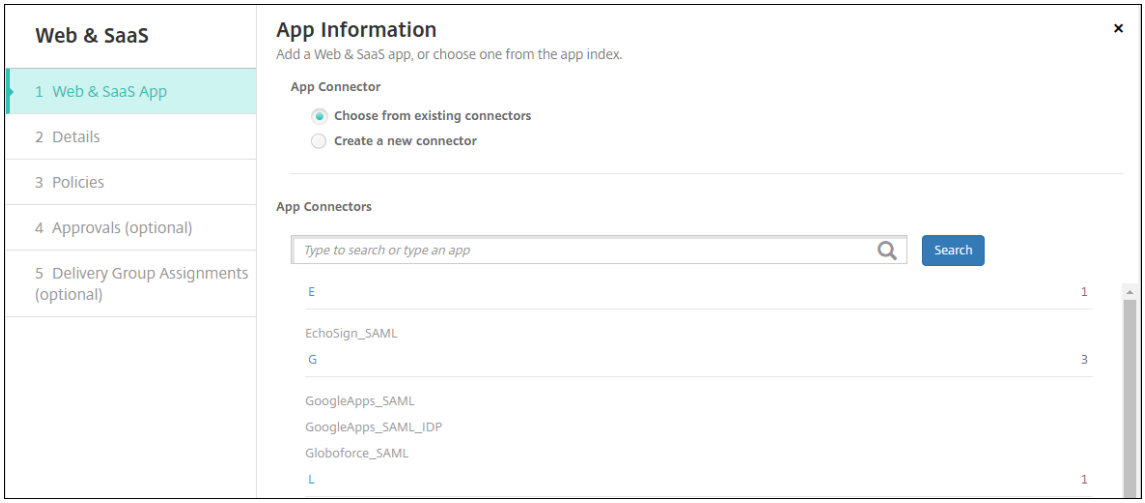
Using the XenMobile console, you can give users single sign-on (SSO) authorization to your mobile, enterprise, web, and SaaS apps. You can enable apps for SSO by using application connector templates. For a list of connector types available in XenMobile, see Application connector types. You can also you build your own connector in XenMobile 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 XenMobile console.

1. In the XenMobile 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.

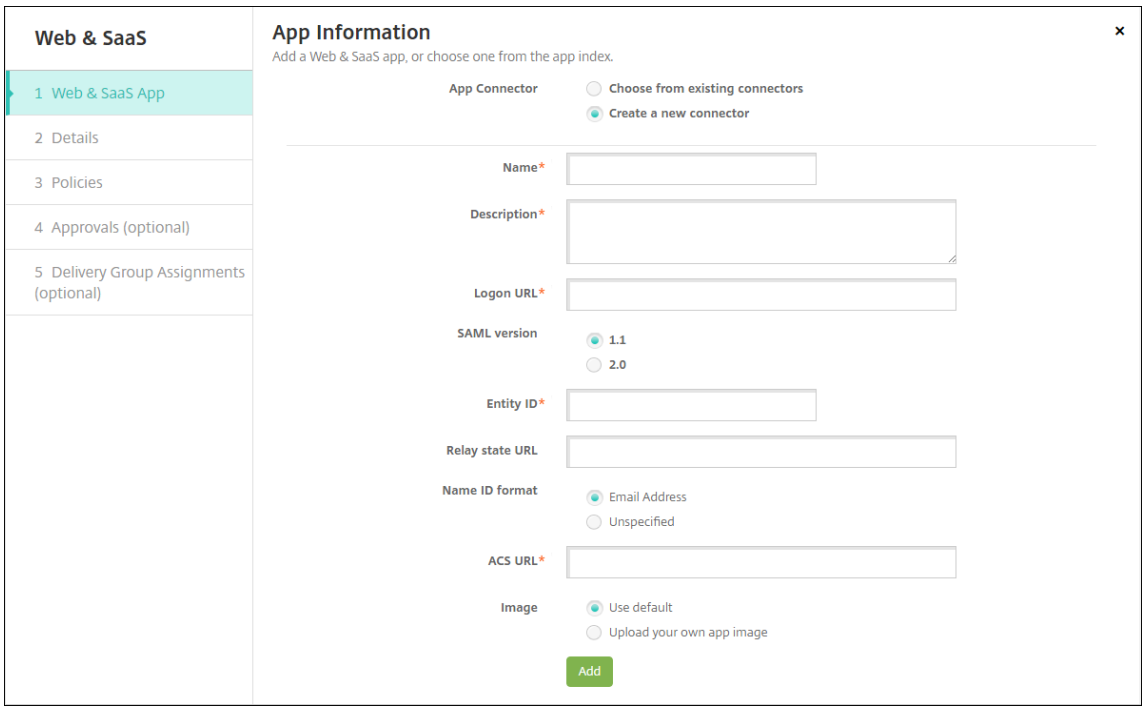
To configure an existing app connector

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 may 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 application. 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.

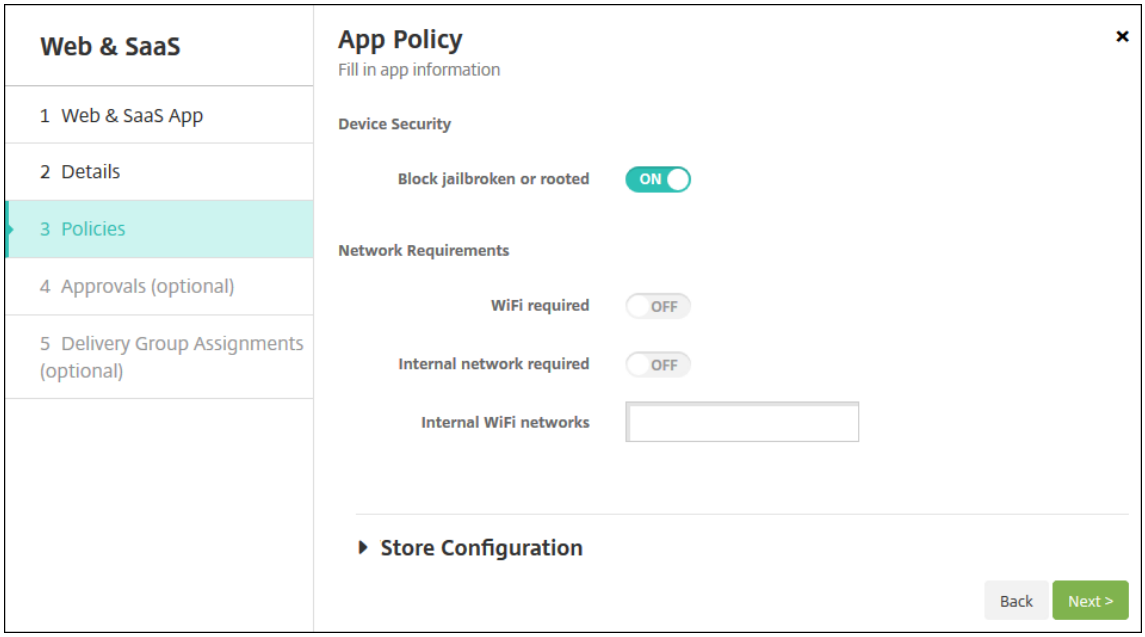


2. Configure these settings:

   - **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.

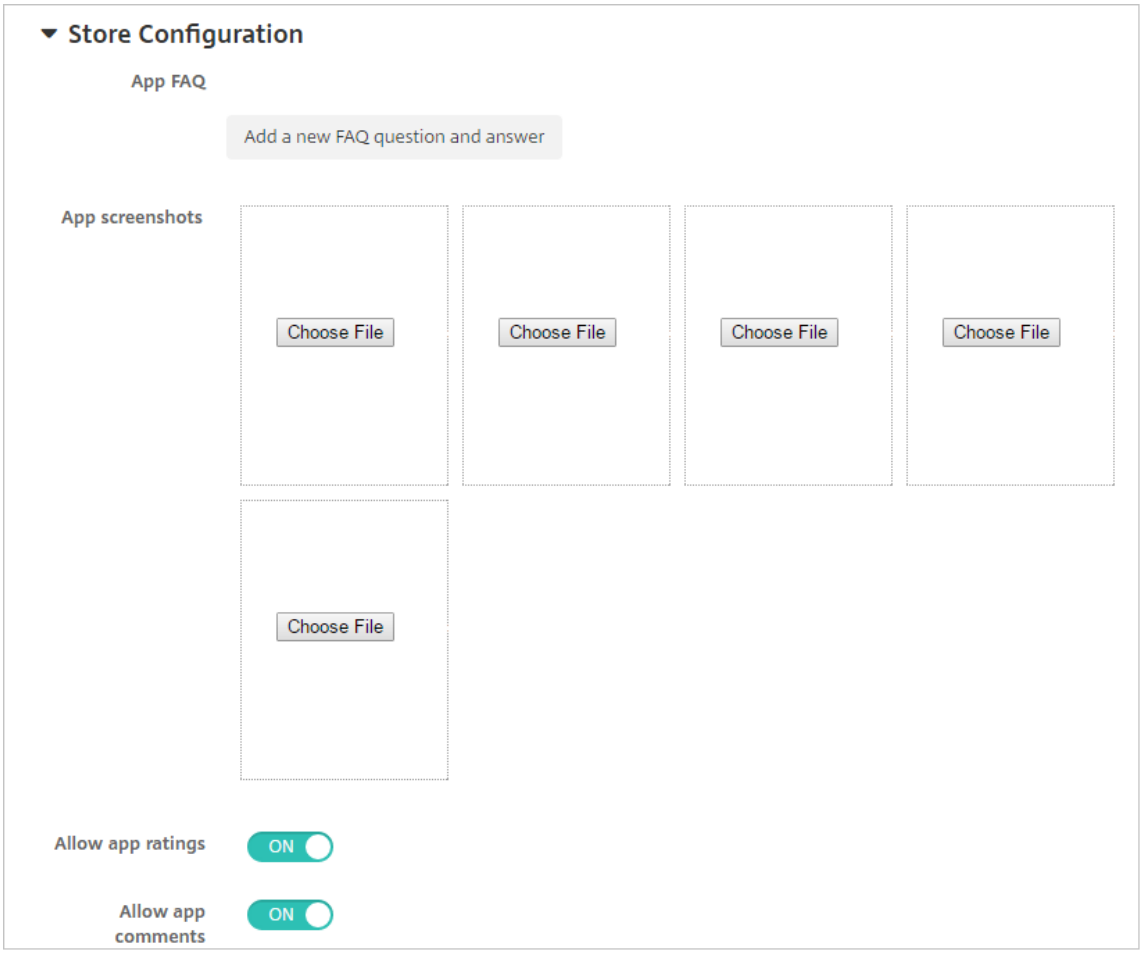


5. Configure these settings:

   - **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.

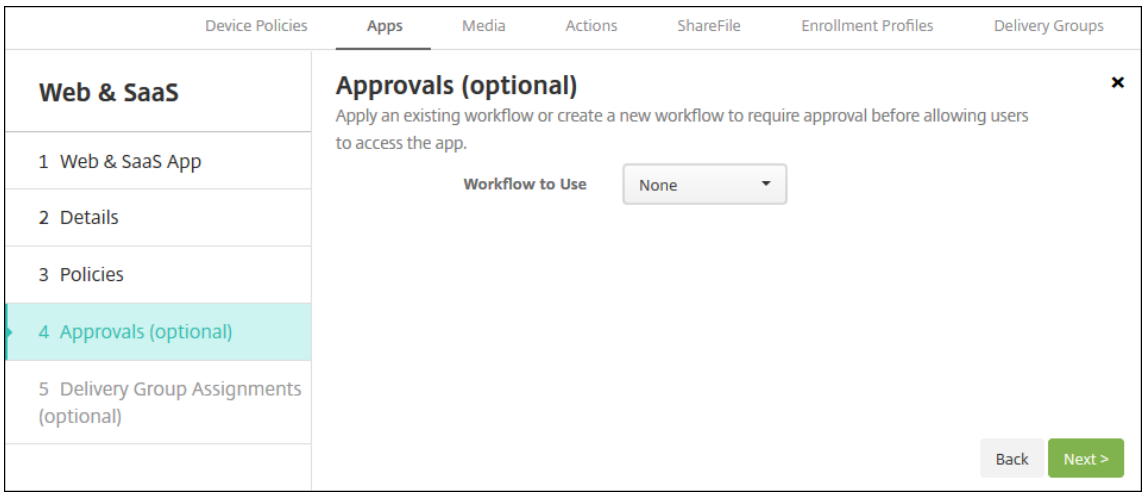
6. Configure the deployment rules. For information, see Deployment rules.

7. Expand **Store Configuration**.



- **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.

8. Click **Next**. The **Approvals** page appears.



To use workflows to require approval before allowing users to access the app, see Apply workflows.

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. 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** 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**.
12. Click **Save**.

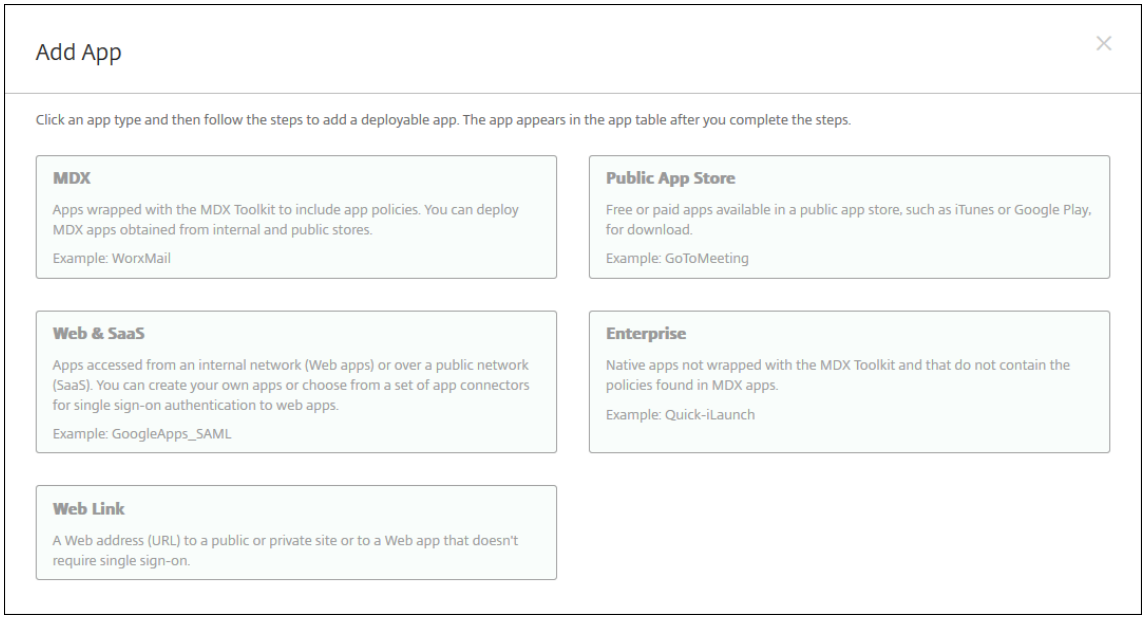
Add an enterprise app

Enterprise apps in XenMobile represent native apps that are not prepared with the MAM SDK or MDX Toolkit. Those apps don't contain the policies associated with MDX apps. You can upload an enterprise app on the **Apps** tab in the XenMobile console. Enterprise apps support the following platforms (and corresponding file types):

- iOS (.ipa file)
- Android (.apk file)
- Samsung Knox (.apk file)
- Android Enterprise (.apk file)
- 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.

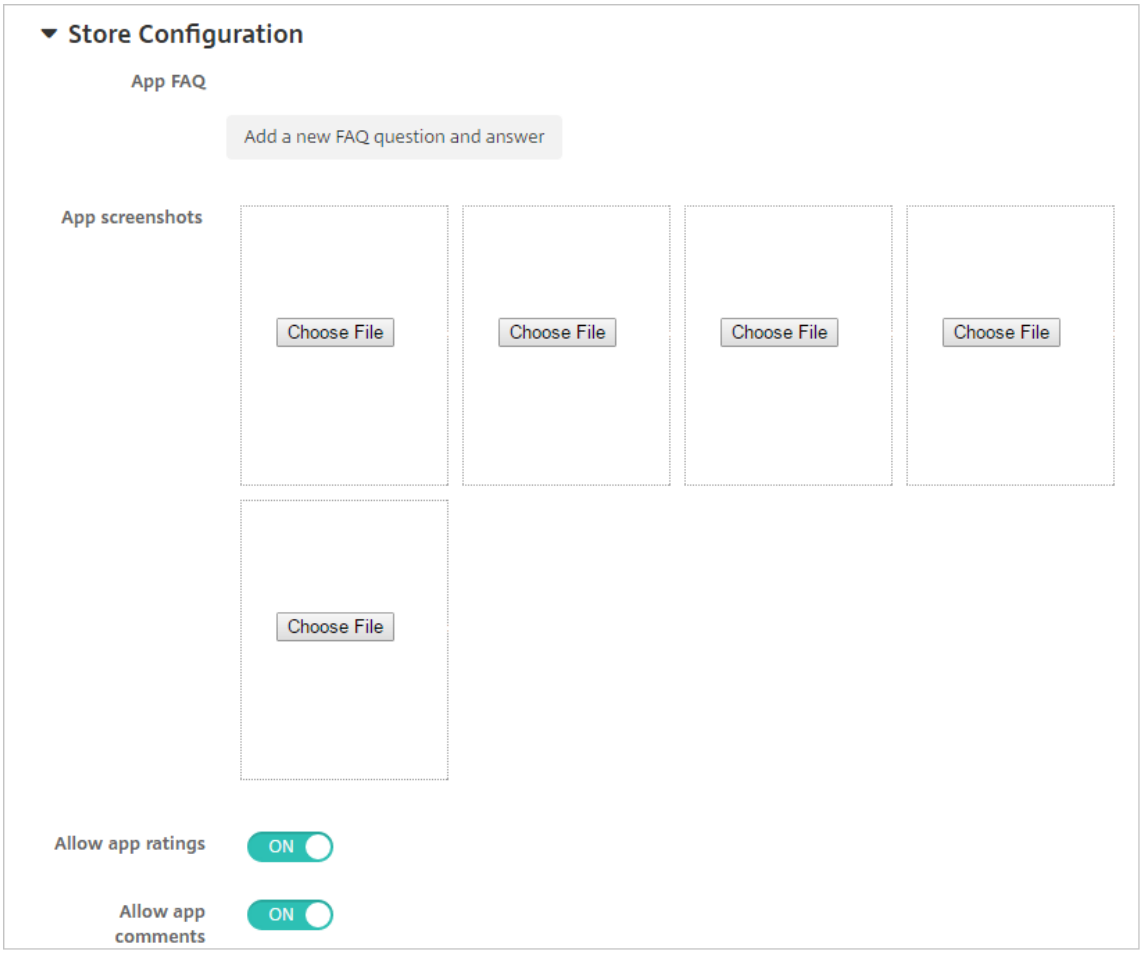
1. In the XenMobile console, click **Configure > Apps > Add**. The **Add App** dialog box appears.



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**.
- **Prevent app data backup:** Select whether to prevent the app from backing up data. The default is **On**.
- **Force app to be managed:** If you are installing an unmanaged app, select **On** if you want users on unsupervised devices to be prompted to allow management of the app. If they accept the prompt, the app is managed.

9. Configure the deployment rules. For information, see Deployment rules.
10. Expand **Store Configuration**.



- **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** 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**.

15. Click **Save**.

Add a Web link

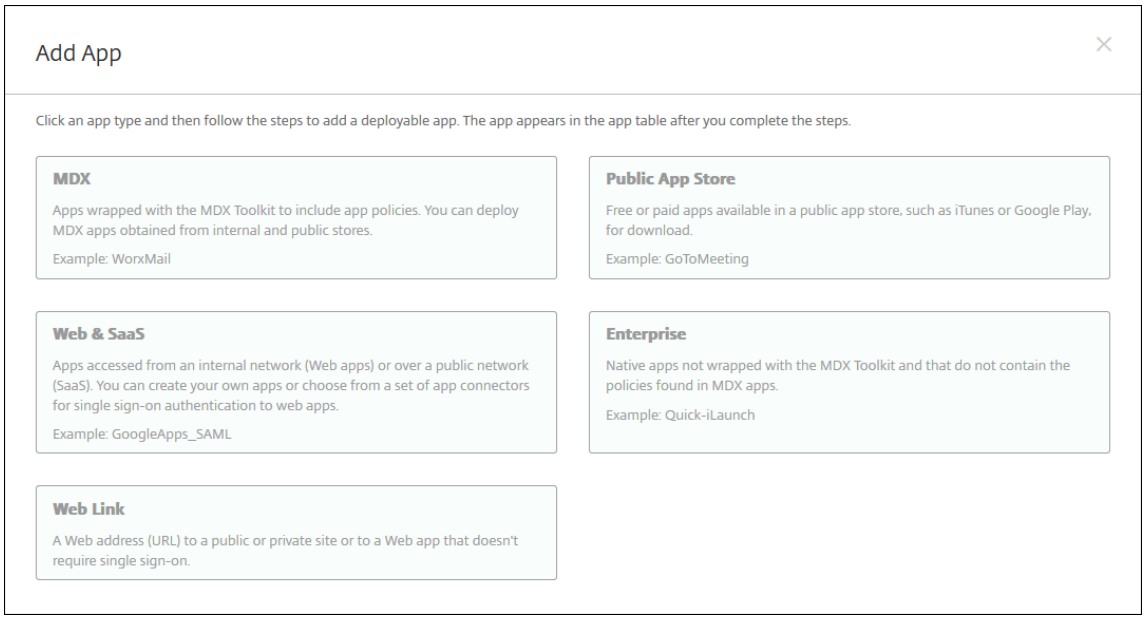
A web link is a web address to an internet or intranet site. A web link can also point to a web application that doesn't require SSO. After you finish configuring a web link, the link appears as an icon in the app store. When users log on with Secure Hub, the link appears with the list of available apps and desktops.

You can configure web links from the **Apps** tab in the XenMobile 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.

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 XenMobile console, click **Configure > Apps > Add**. The **Add App** dialog box appears.

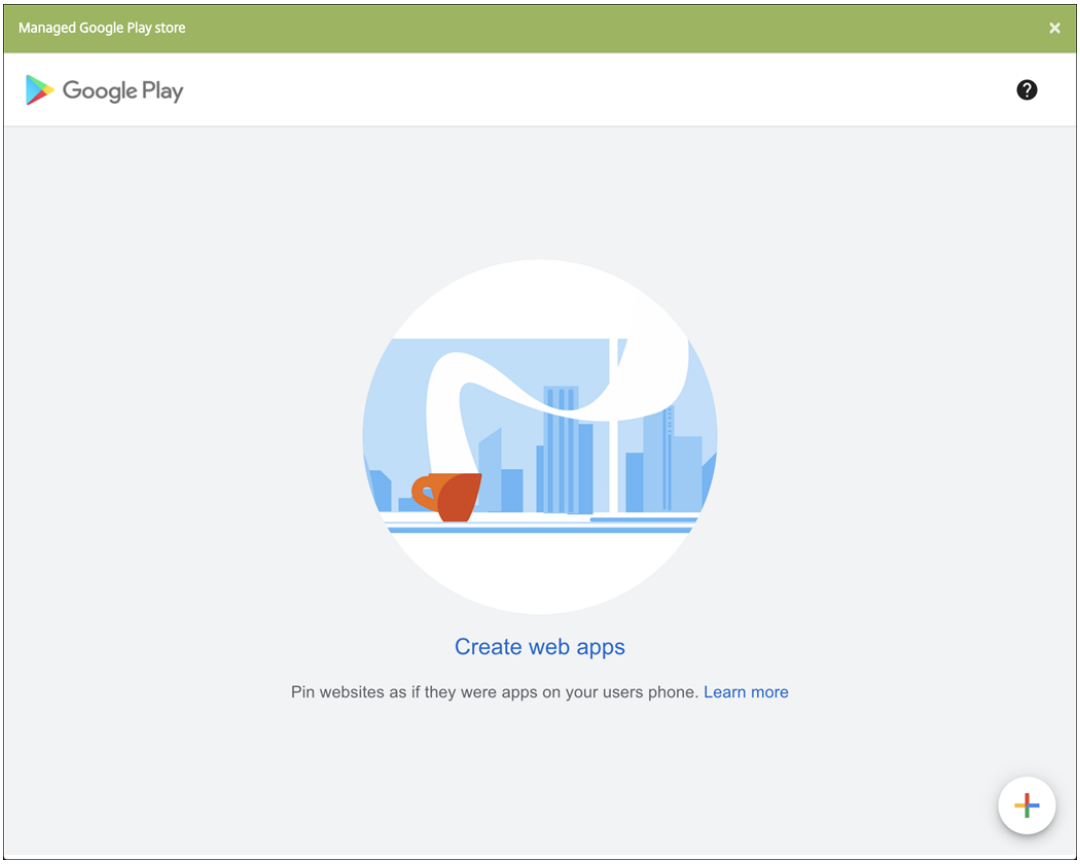


2. Click **Web Link**. The **App Information** page appears.
3. On the **App Information** pane, type the following information:

   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.

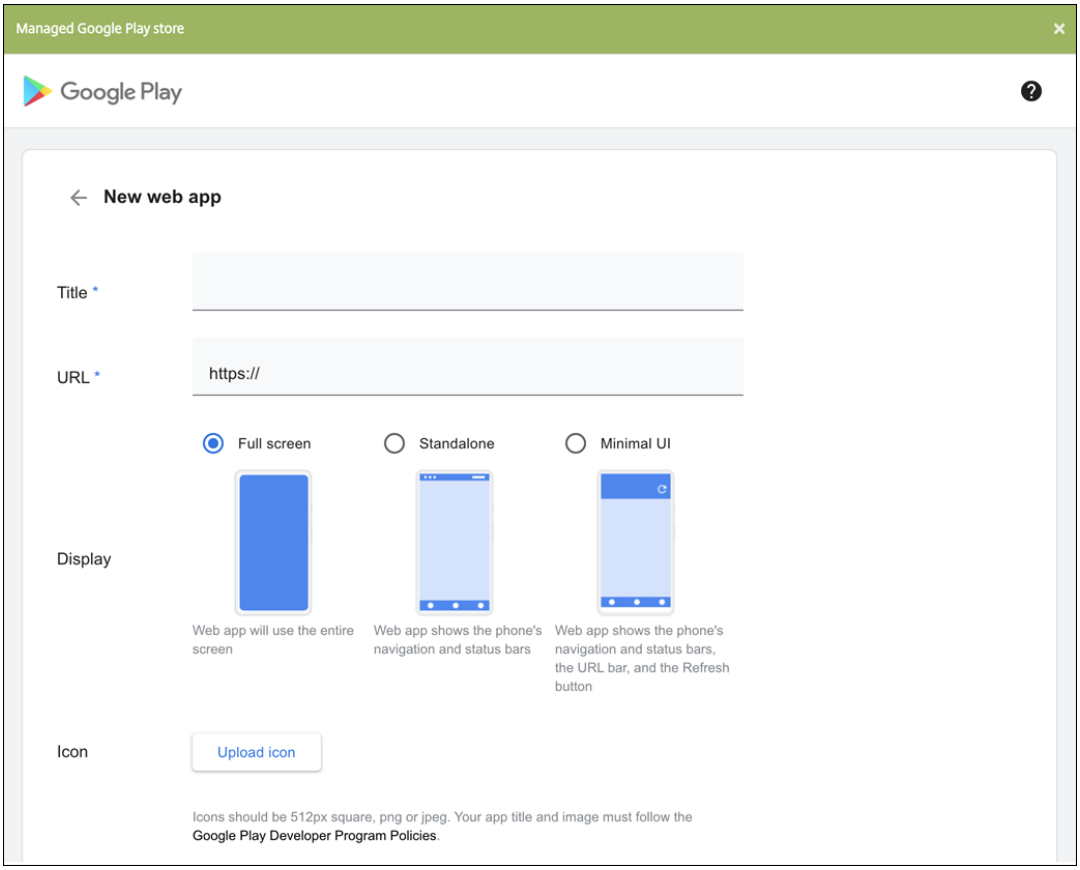
4. Click **Next**. The **App Platforms** page appears.
5. Under **Platforms**, select **Other platforms** to add a web app for iOS and Android (legacy DA), or select **Android Enterprise**. Clear the check box you don't want to add.

   - If you select **Other platforms**, continue to the next step to configure the settings.
   - If you select **Android Enterprise**, 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:

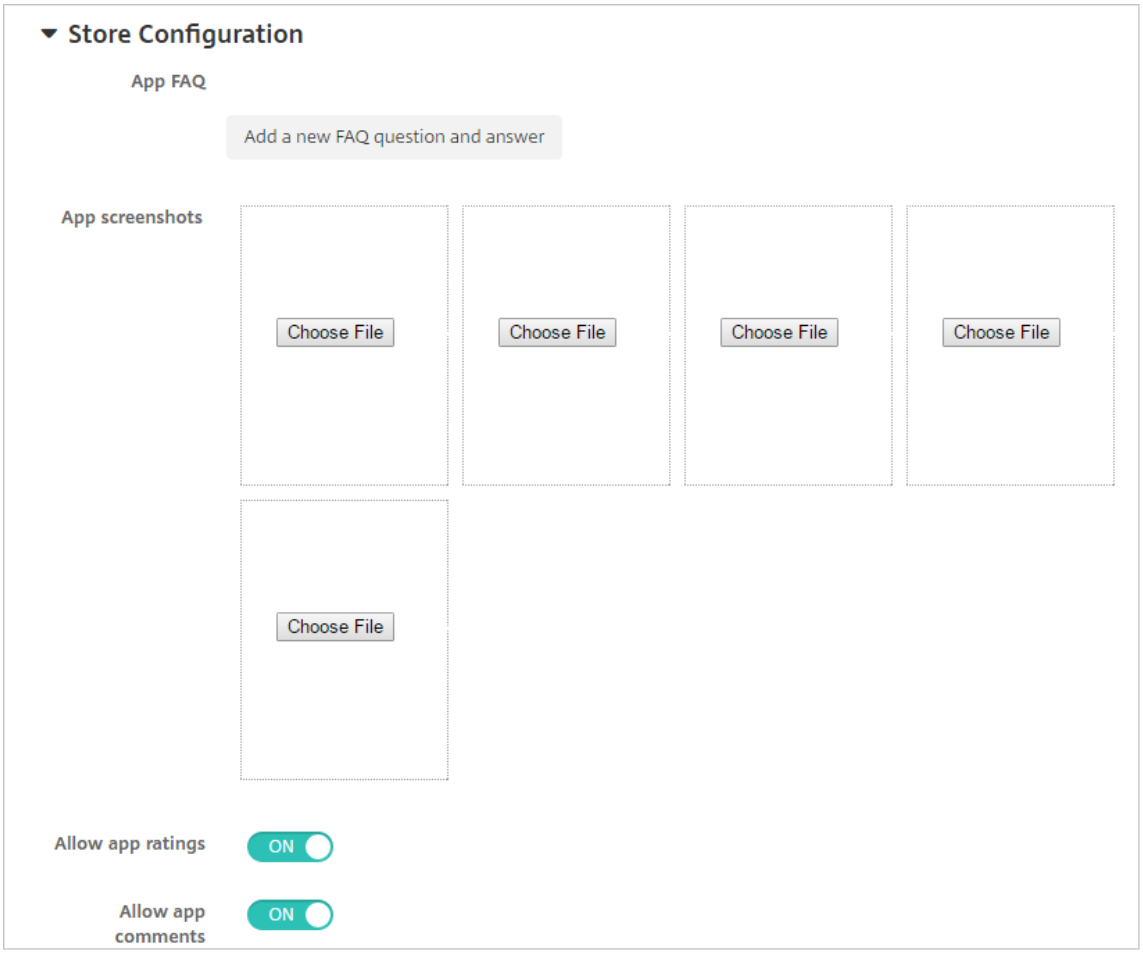
- **Title:** Type the name for the web app.
- **URL:** Type the web address for the app.
- **Display:** Choose how to display the web app on the user devices. The available options are **Full screen**, **Standalone**, and **Minimal UI**.
- **Icon:** Upload your own image to represent the web app.



When finished, click **Create**. It might take up to 10 minutes for your web app to publish.

6. For platforms other than Android Enterprise, 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 may 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 Deployment rules.

8. Expand **Store Configuration**.



   - **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** 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**.

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

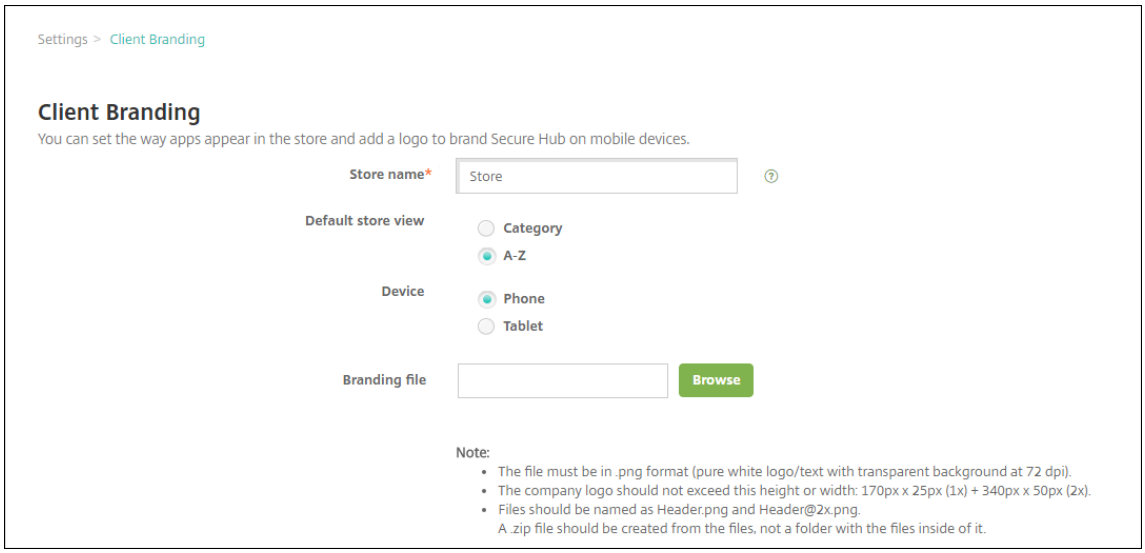
You can set how apps appear in the store and add a logo to brand Secure Hub and the app store. These branding features are available for iOS and Android devices.

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 should not 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 XenMobile Server 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.



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:** Select an image or .zip file of images to use for branding by, clicking **Browse** and navigating to the file's location.

3. Click **Save**.

App connector types

July 3, 2018

The following table lists the connectors and the types of connectors that are available in XenMobile when you add a Web or SaaS app. You can also add a new connector to XenMobile 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		**Note:** 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
Office365_SAML	Y	Y

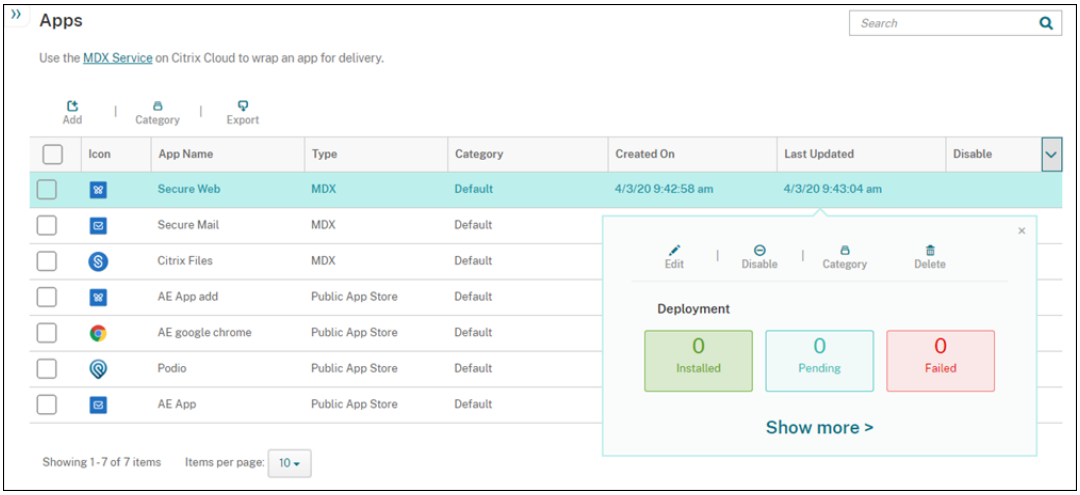
Connector name	SSO SAML	Supports user account management
Salesforce_SAML	Y	Y
Salesforce_SAML_SP	Y	Y
SandBox_SAML	Y	
SuccessFactors_SAML	Y	
ShareFile_SAML	Y	
ShareFile_SAML_SP	Y	
WebEx_SAML_SP	Y	Y

Upgrade MDX or enterprise apps

March 26, 2021

To upgrade an MDX or Enterprise app in XenMobile, disable the app in the XenMobile console, and then upload the new version of the app. You don't need to disable public app store apps such as Citrix Secure Mail.

1. In the XenMobile console, click **Configure > Apps**. The **Apps** page appears.
2. For managed devices (devices enrolled in XenMobile for mobile device management), skip to Step 3. For unmanaged devices (devices enrolled in XenMobile 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.



c) Click **Disable** in the confirmation dialog box. *Disabled* appears in the **Disable** column for the app.

> **Note:**
>
> While the app is disabled, users cannot reconnect to the app after they log off. Disabling an app is optional, but we recommend disabling the app to avoid issues with app functionality. For example, users requesting to download the app at the same time you upload the new version might result in an issue.

3. In the **Apps** table, click the check box next to the app or click the line containing the app you want to update.
4. Click **Edit** in the menu that appears. The **App Information** page appears with the platforms you originally chose for the app selected.
5. Configure these settings:
   - **Name:** Optionally, change the app name.
   - **Description:** Optionally, change the app description.
   - **App category:** Optionally, change the app category.
6. Click **Next**. The first selected platform page appears. Do the following for each selected platform:
   a) Choose the replacement file you want to upload by clicking **Upload** and navigating to the file location. The app uploads to XenMobile.

   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 apps.

b) Optionally, change the app details and policy settings for the platform.

c) Optionally, configure deployment rules and XenMobile Store configurations. For information, see Add an MDX app in Add apps.

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.

Citrix Launcher

June 19, 2020

Citrix Launcher replacement

Citrix is removing Citrix Launcher from the app store in August 2020. To replace Citrix Launcher, you can use features that are already available.

To provision devices as kiosks (dedicated devices):

1. Add an RBAC role that allows XenMobile administrators to enroll dedicated devices to your XenMobile deployment. See Provisioning dedicated Android Enterprise devices.
2. Create an enrollment profile with a **Enrollment type** of **Fully managed/Work profile**. See To create an enrollment profile.
3. Create a Kiosk device policy to configure an app to pin to the device screen by enabling the **Lock task mode** setting. See Android Enterprise settings.

About Citrix Launcher

Citrix Launcher lets you customize the user experience for Android devices deployed by XenMobile. The minimum Android version supported for Secure Hub management of Citrix Launcher is Android 4.0.3. Citrix Launcher and the Launcher Configuration device policy are not compatible with Android Enterprise.

You can add the **Launcher Configuration Policy** to control these Citrix Launcher features:

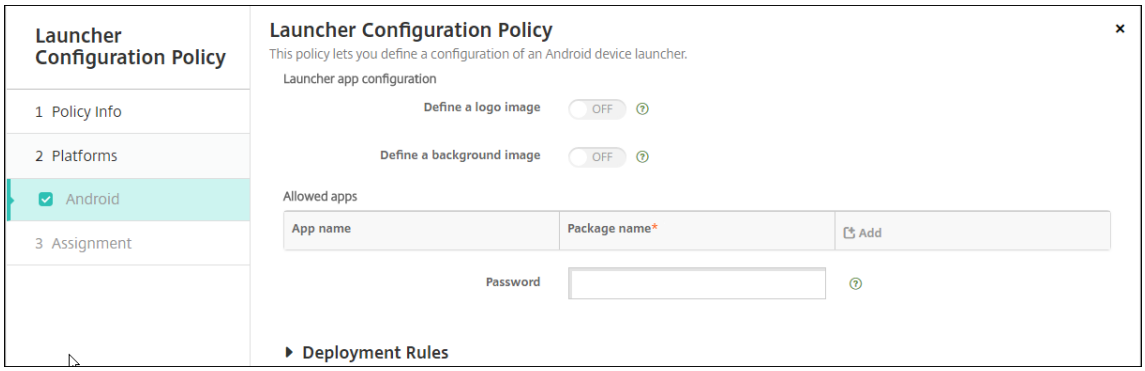
- Manage Android devices so that users can access only the apps that you specify.

- 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 enter to exit the launcher.

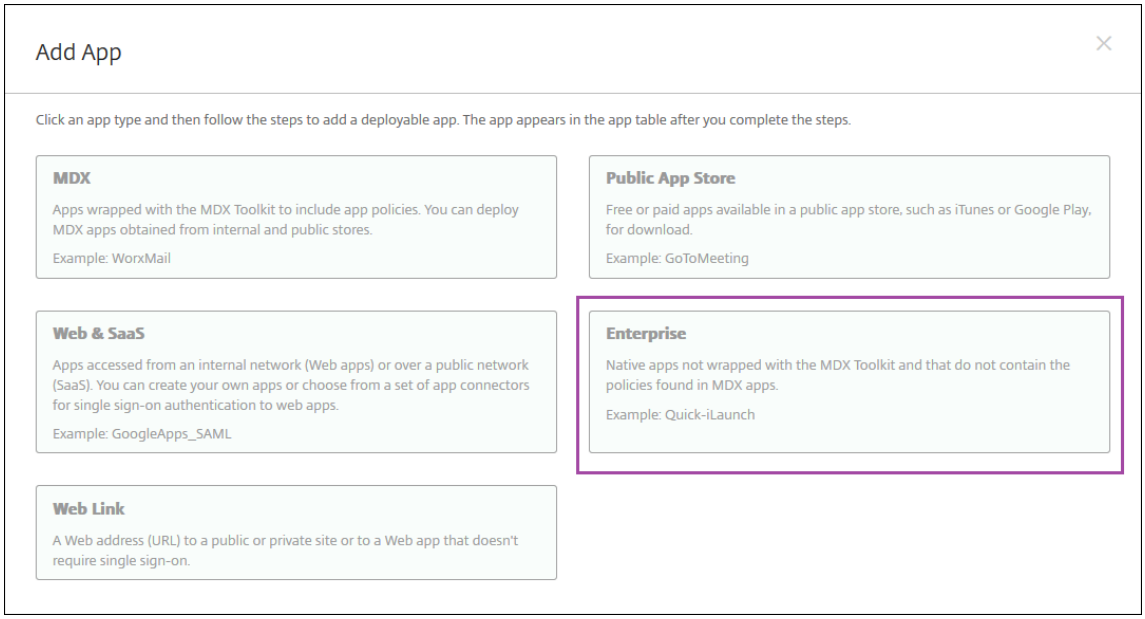
While Citrix Launcher enables you to apply those device-level restrictions, the launcher grants users built-in access to device settings such as Wi-Fi settings, Bluetooth settings, and device passcode settings. Citrix Launcher isn't intended as an extra layer of security over what the device platform already provides.

To provide Citrix Launcher to Android devices, follow these general steps.

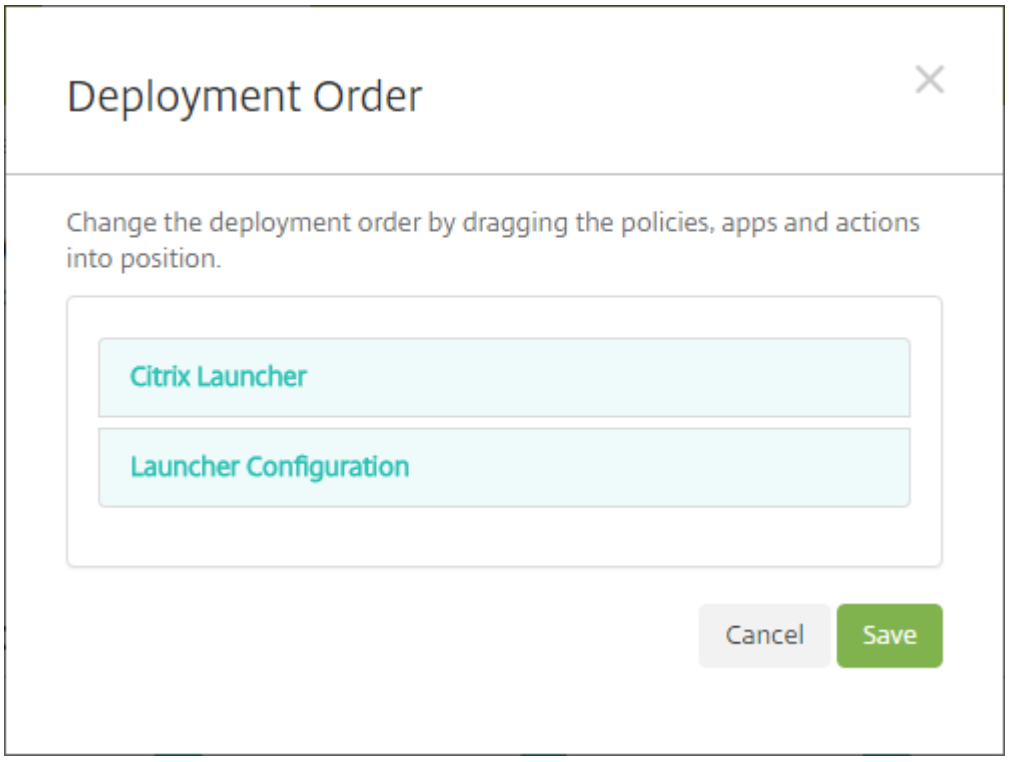
1. To download the Citrix Launcher app: Go to https://www.citrix.com/downloads. Search for **Citrix Launcher**. The file name is CitrixLauncher.apk. The file is ready for uploading into XenMobile and doesn't require wrapping.
2. Add the device policy **Launcher Configuration Policy**. Go to **Configure > Device Policies**, click **Add**, and in the **Add a New Policy** dialog box, start typing **Launcher**. For more information, see Launcher Configuration Policy.



3. Add the Citrix Launcher app to XenMobile 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 for Citrix Launcher with the following configuration in **Configure > Delivery groups**.
   - On the **Policies** page, add the **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.



For more information, see Deploy resources.

Apple Volume Purchase

October 19, 2020

You can manage iOS app licensing by using Apple iOS volume purchase. The volume purchase solution simplifies the process to find, buy, and distribute apps and other data in bulk for an organization.

With volume purchase, you can use XenMobile to distribute public app store apps.

- Volume purchase is not supported for MAM enrollment. You must enroll volume purchase devices in MDM or MDM+MAM.
- Volume purchase is not supported for Citrix mobile productivity apps.
- Although you can distribute the XenMobile public store apps with volume purchase, the deployment is not optimal. Enhancements to XenMobile and the Secure Hub store are required to address the limitations.
- For a list of known issues with distributing the XenMobile public store apps through volume purchase, see this article in the Citrix knowledge center.

With volume purchase, you can distribute the applicable apps directly to your devices. Or, you assign content to your users by using redeemable codes. You configure settings specific to the iOS volume purchase in XenMobile.

XenMobile periodically reimports volume purchase licenses from Apple to ensure that the licenses reflect all changes. Such changes include when you manually delete an imported app from the volume purchase. By default, XenMobile refreshes the volume purchase license baseline a minimum of every 1440 minutes (24 hours). You can change the volume purchase baseline interval through the server property, `VPP.baseline`. See Server properties.

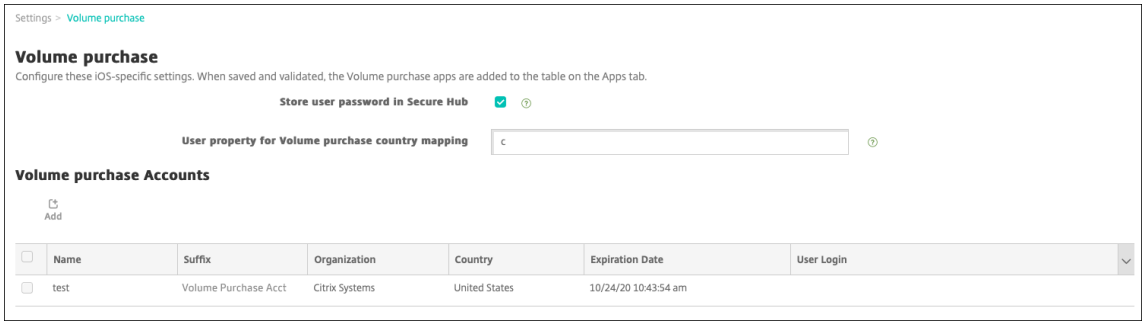
The **App auto update** setting also relies in the `VPP.baseline` server property, and apps update on the same schedule set in that property.

This article focuses on using volume purchase with managed licenses, which enables you to use XenMobile to distribute apps. If you currently use redemption codes and want to change to managed distribution, see this Apple Support document: Migrate from redemption codes to managed distribution with the Volume Purchase.

For information about the iOS volume purchase, see https://volume.itunes.apple.com/us/store. To enroll in volume purchase, go to https://deploy.apple.com/qforms/open/register/index/avs. To access your volume purchase store in iTunes, go to https://volume.itunes.apple.com/?l=en.

After you save these iOS volume purchase settings in XenMobile, the purchased apps appear on the **Configure > Apps** page in the XenMobile console.

1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **Volume purchase**. The **Volume purchase** configuration page appears.



3. Configure these settings:

   - **Store user password in Secure Hub:** Select whether to store a user name and password in Secure Hub for XenMobile authentication. The default is to store the information by using this secure method.
   - **User property for Volume purchase country mapping:** Type a code to allow users to download apps from country-specific app stores.

   XenMobile uses this mapping to choose the property pool of the volume purchase. For example, if the user property is United States, that user cannot download apps if the volume purchase code is for the United Kingdom. Contact your volume purchase plan administrator for more information about the country mapping code.

4. For each volume purchase account you want to add, click **Add**. The **Add a Volume purchase account** dialog box appears.
5. Configure these settings for each account you add:

   > **Note:**
   >
   > If you use Apple Configurator 1, upload a license file: Go to **Configure > Apps**, go to a platform page, and then expand **Volume purchase**.

   - **Name:** Type the volume purchase account name.
   - **Suffix:** Type the suffix to appear with the app names obtained through the volume purchase account. 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 volume purchase service token obtained from Apple. To obtain the token: In the **Account Summary** page of the Apple volume purchase portal, click the **Download** button to generate and download the volume purchase file. The file contains the service token and other information, like the country code and expiry. Save the file in a secure location.

- **User Login:** Type an optional authorized volume purchase account administrator name used to import custom B2B apps.
- **User Password:** Type the volume purchase account administrator password.
- **App Auto Update:** If **On**, volume purchase apps automatically update when an update exists on the Apple store. Default is **Off**.

6. Click **Save** to close the dialog box.
7. Click **Save** to save the Volume purchase configuration.

   A message appears stating that XenMobile adds the apps to the list on the **Configure > Apps** page. On that page, notice that the app names from your volume purchase account include the suffix you provided in the preceding configuration.

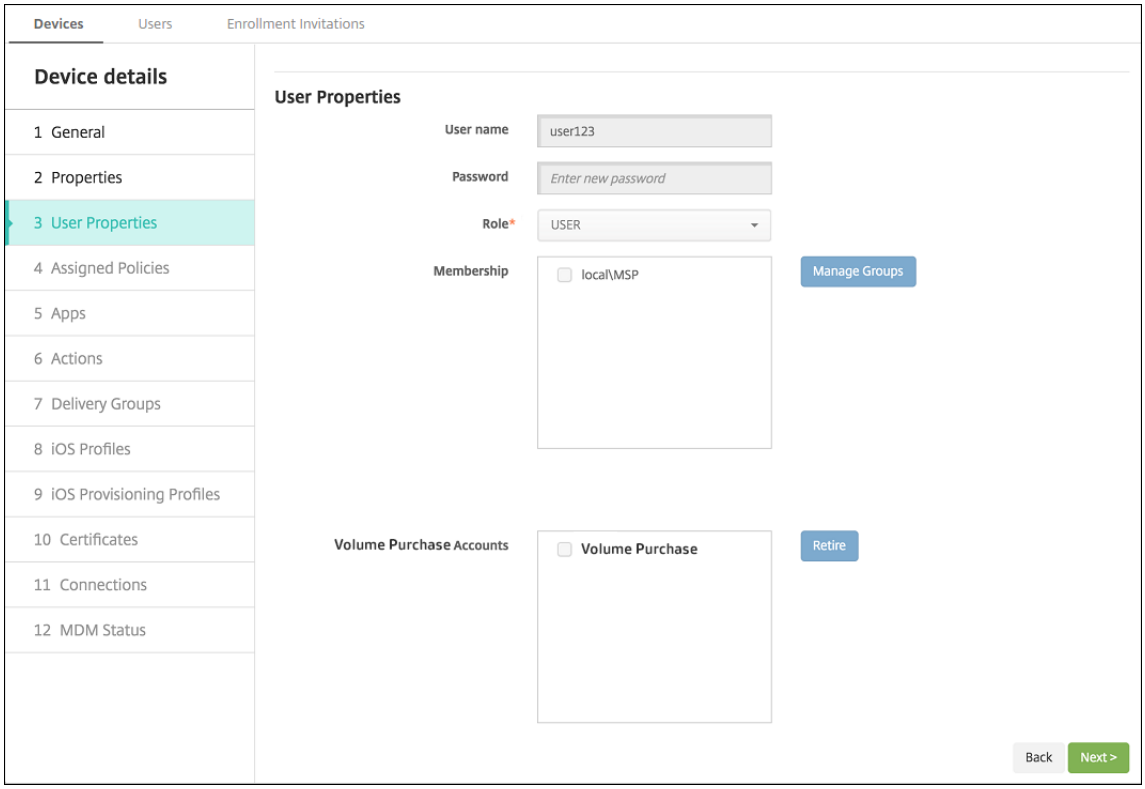
You can now configure the volume purchase app settings and then tune your delivery group and device policy settings for volume purchase apps. After you complete those configurations, users can enroll their devices. The following notes provide considerations for those processes.

- When configuring volume purchase app settings (**Configure > Apps**), enable **Force license association to device**. An advantage of using Apple volume purchase and Deployment Program with supervised devices: The ability to use XenMobile to assign the app at the device (rather than user) level. As a result, you don't have to use an Apple ID device. Also, users don't receive an invitation to join Apple volume purchase. Users can also download the apps without signing into their iTunes account.

  To view the volume purchase info for that app, expand **Volume purchase**. Notice in the **Volume purchase License Keys** table, the license is associated with a device. If the user removes the token and then imports it again, the word **Hidden** appears instead of the serial number, due to Apple privacy restrictions.

  To disassociate a license, click the row for the license and then click **Disassociate**.

  If you associate volume purchase licenses with users, XenMobile integrates users into your volume purchase account and associates their iTunes ID with the volume purchase account. The iTunes ID of users is never visible to your company or to the XenMobile server. Apple transparently creates the association to retain user privacy. You can retire a user from Apple volume purchase, to disassociate all licenses from the user account. To retire a user, go to **Manage > Devices**.



- When you assign an app to a delivery group, by default XenMobile identifies the app as an optional app. To ensure that XenMobile deploys an app to devices, go to **Configure > Delivery Groups.** On the **Apps** page, move the app to the **Required Apps** list.
- When an update for a public app store app is available: When volume purchase pushes the app, the app automatically updates on devices. To push an update for Secure Hub, when assigned to a device and not to a user, do the following. In **Configure > Apps**, on a platform page, click **Check for Updates** and apply the update.

  XenMobile displays a License Expiration Warning when Apple volume purchase has expired.

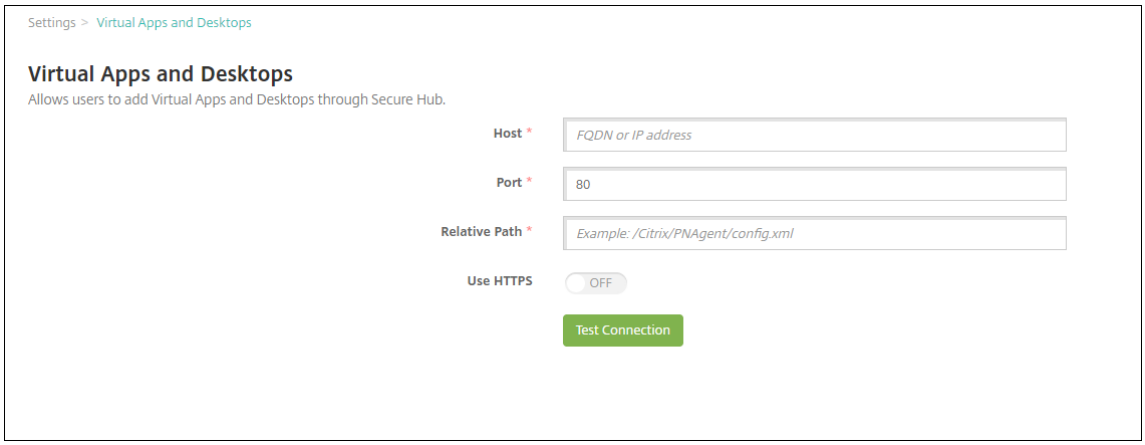
Virtual Apps and Desktops through Citrix Secure Hub

August 31, 2020

XenMobile can collect apps from Virtual Apps and Desktops and make them available to mobile device users in the XenMobile Store. Users subscribe to the apps directly inside XenMobile Store and launch them from Secure Hub. Citrix Receiver must be installed on user devices to launch the apps, but it does not need to be configured.

To configure this setting, you need the fully qualified domain name (FQDN) or IP address and port number for the Web Interface site or StoreFront.

1. In the XenMobile 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.



3. Configure these settings:
   - **Host:** Type the fully qualified domain name (FQDN) or IP address for the Web Interface site or StoreFront.
   - **Port:** Type the port number for the Web Interface site or 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 the Web Interface site or StoreFront and the client device. The default is **OFF**.
4. Click **Test Connection** to verify that XenMobile can connect to the specified Virtual Apps and Desktops server.
5. Click **Save**.

Use Citrix Content Collaboration with XenMobile

August 25, 2020

XenMobile has two options for integrating with Citrix Content Collaboration: Citrix Files and storage zone connectors. Integration with Citrix Files or storage zone connectors requires XenMobile Enterprise Edition.

Citrix Files

If you have XenMobile Enterprise Edition, you can configure XenMobile to provide access to your Citrix Files account. That configuration:

- Gives mobile users access to the full Enterprise feature set, such as file sharing, file sync, and storage zone connectors.
- Can provide Citrix Files with single sign-on authentication of XenMobile App users and comprehensive access control policies.
- Provides Citrix Files configuration, service level monitoring, and license usage monitoring through the XenMobile console.

For more information about configuring XenMobile for Citrix Files, see SAML for single sign-on with Citrix Files.

Storage zone connectors

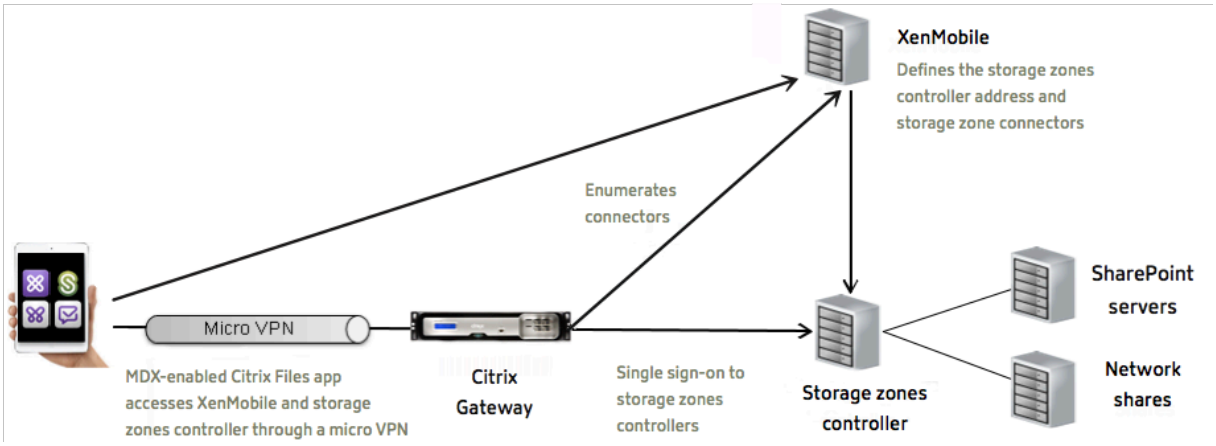
You can configure XenMobile to provide access only to storage zone connectors that you create through the XenMobile console. That configuration:

- 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 Files mobile productivity apps 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 XenMobile console. If you later decide to use the full Citrix Files functionality with XenMobile, you can change the configuration in the XenMobile console.
- Requires XenMobile Enterprise Edition.

For a XenMobile integration with storage zone connectors only:

- Citrix Content Collaboration uses your single sign-on configuration to Citrix Gateway to authenticate with storage zones controller.
- XenMobile doesn't authenticate through SAML because the Citrix Files control plane isn't used.

The following diagram shows the high-level architecture for XenMobile use with storage zone connectors.



Requirements

- Minimum component versions:
  - XenMobile Server 10.5 (on-premises)
  - ShareFile for iOS (MDX) 5.3
  - ShareFile for Android (MDX) 5.3
  - Storage zones controller 5.0

    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 a XenMobile integration with storage zone connectors only.

XenMobile 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 XenMobile integration with storage zone connectors only. Some of these articles are in the storage zones controller documentation.

1. Configure Citrix ADC for storage zones controller

   You can use Citrix ADC 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 controllers console enables you to specify a proxy server for storage zones controllers. 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

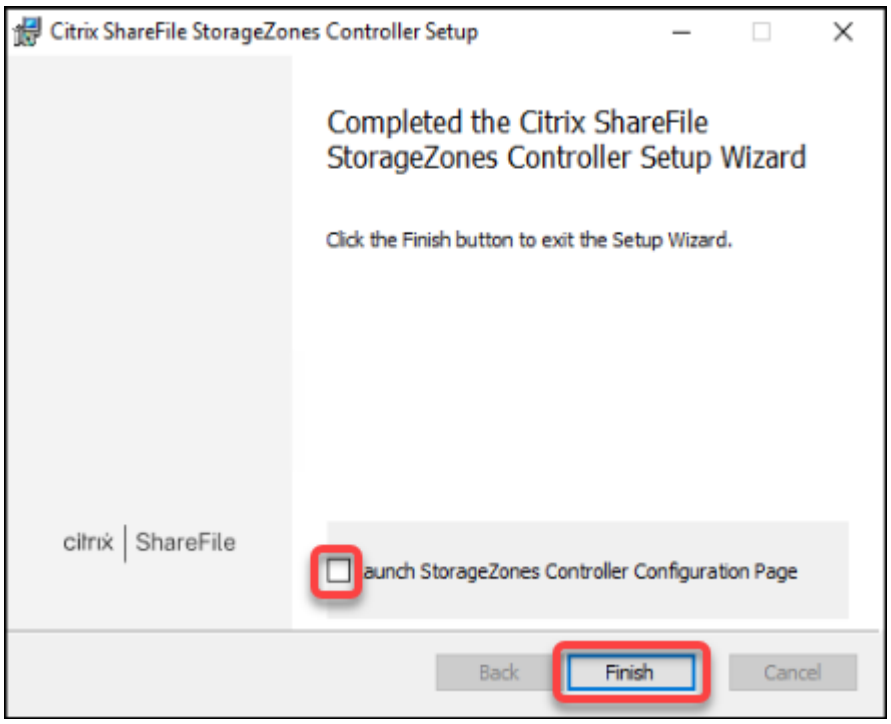
   To configure a storage zone for high availability, connect at least two storage zones controllers to it.

Install storage zones controller

1. Download and install the storage zones controller software:
   a) Go to https://www.citrix.com/downloads. Search for **ShareFile** and then 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 the installation is successful, the Citrix Files logo appears.

   If the Citrix Files logo does not appear, clear the browser cache and try again.

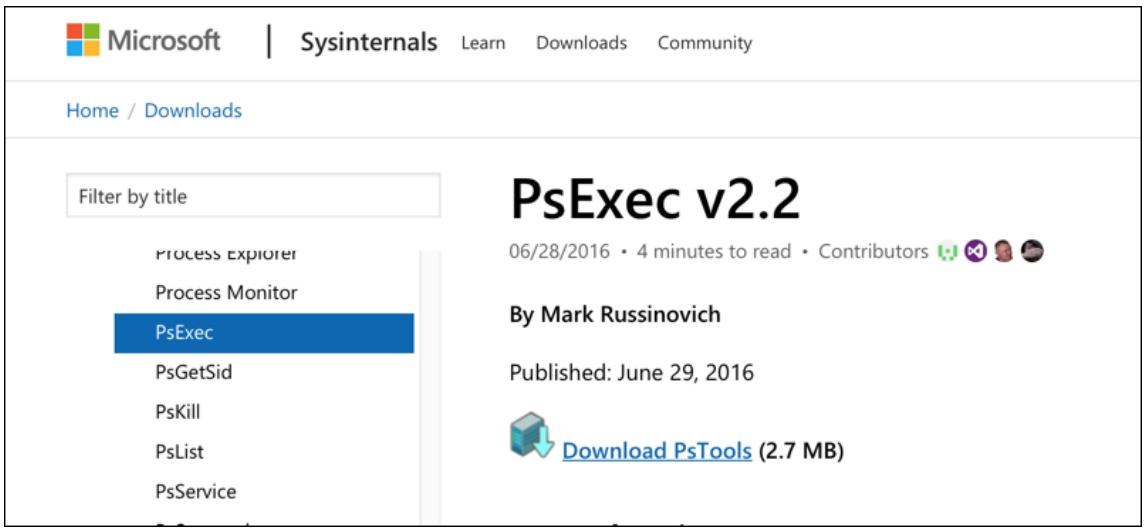
   > **Important:**
   >
   > If you plan to clone the storage zones controller, capture the disk image before you proceed with configuring the storage zones controller.

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:

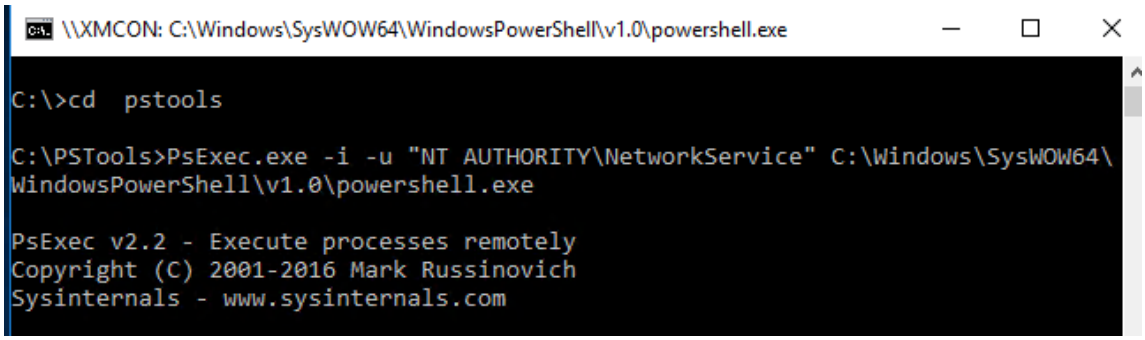
- Registers the current storage zones controller as a primary storage zones controller. You can later join secondary storage zones controllers to the primary controller.
- Creates a zone and sets the passphrase for it.

1. From your storage zone 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.

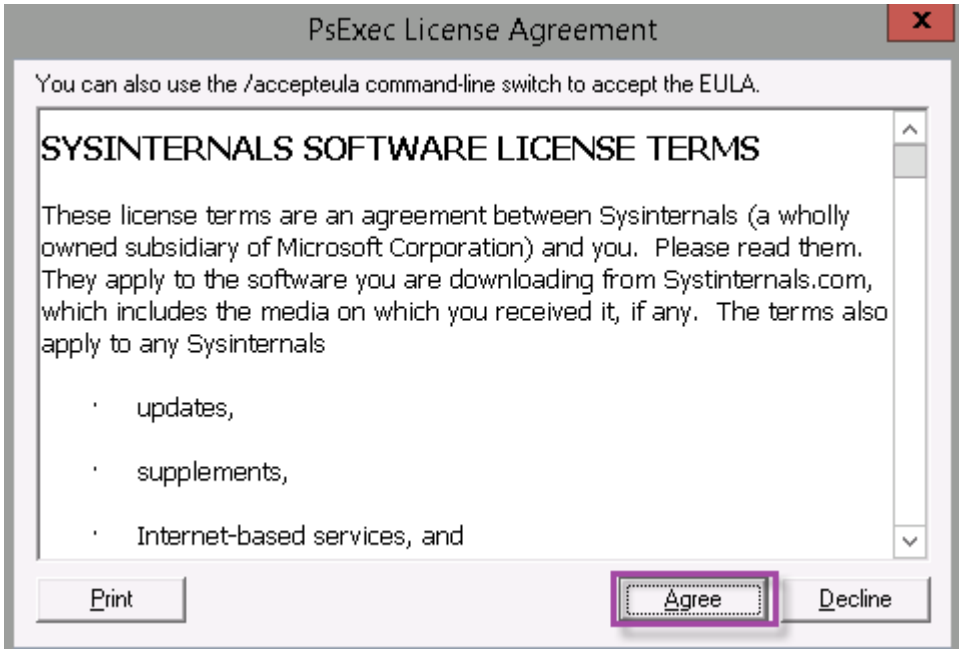


2. Run the PsExec tool: Open the Command Prompt as the Administrator User and then type the following:

```
cd c:\pstools
PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
<!--NeedCopy-->
```



3. When prompted, click **Agree** to run the Sysinternals tool.



A PowerShell widow opens.

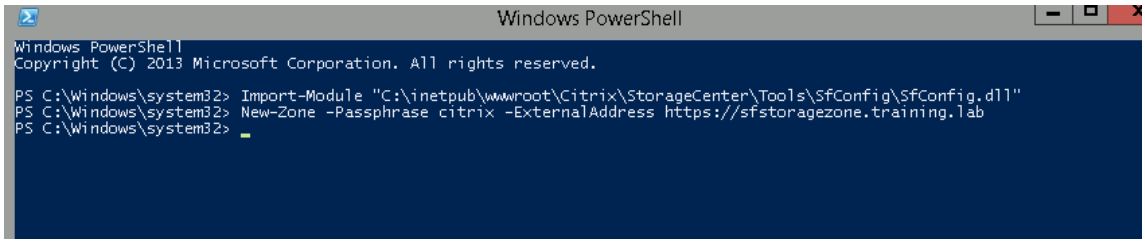
4. In the PowerShell window, type the following:

```
Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
    SfConfig\SfConfig.dll"
New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
    com
<!--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 controller. 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 XenMobile 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 XenMobile.

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>
   ```

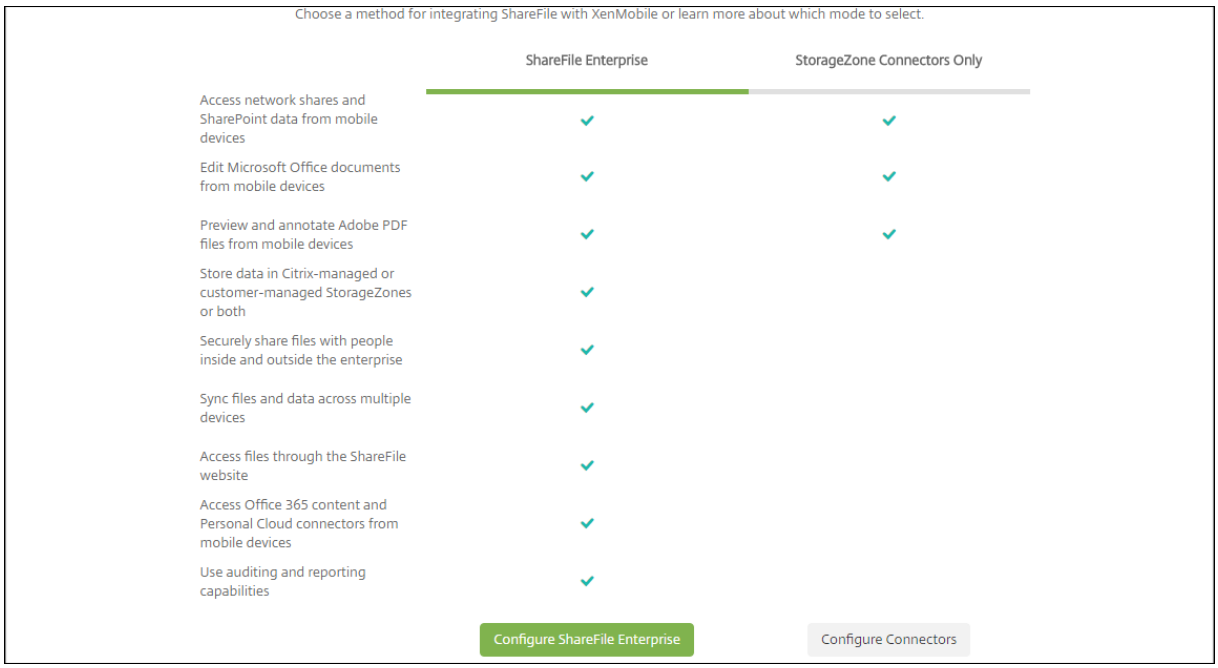
   For example:

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

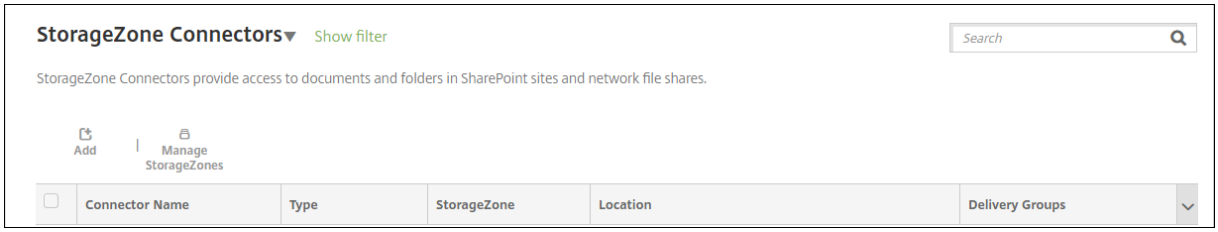
Define storage zones controller connections in XenMobile

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.

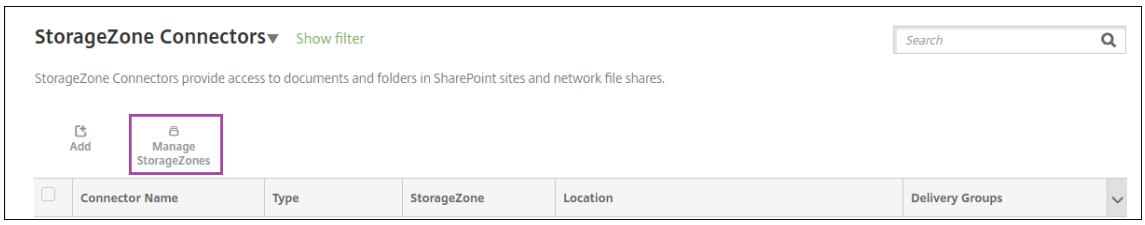
On your first visit to the **Configure > ShareFile** page, the page summarizes the differences between using XenMobile for Enterprise accounts and storage zone connectors.



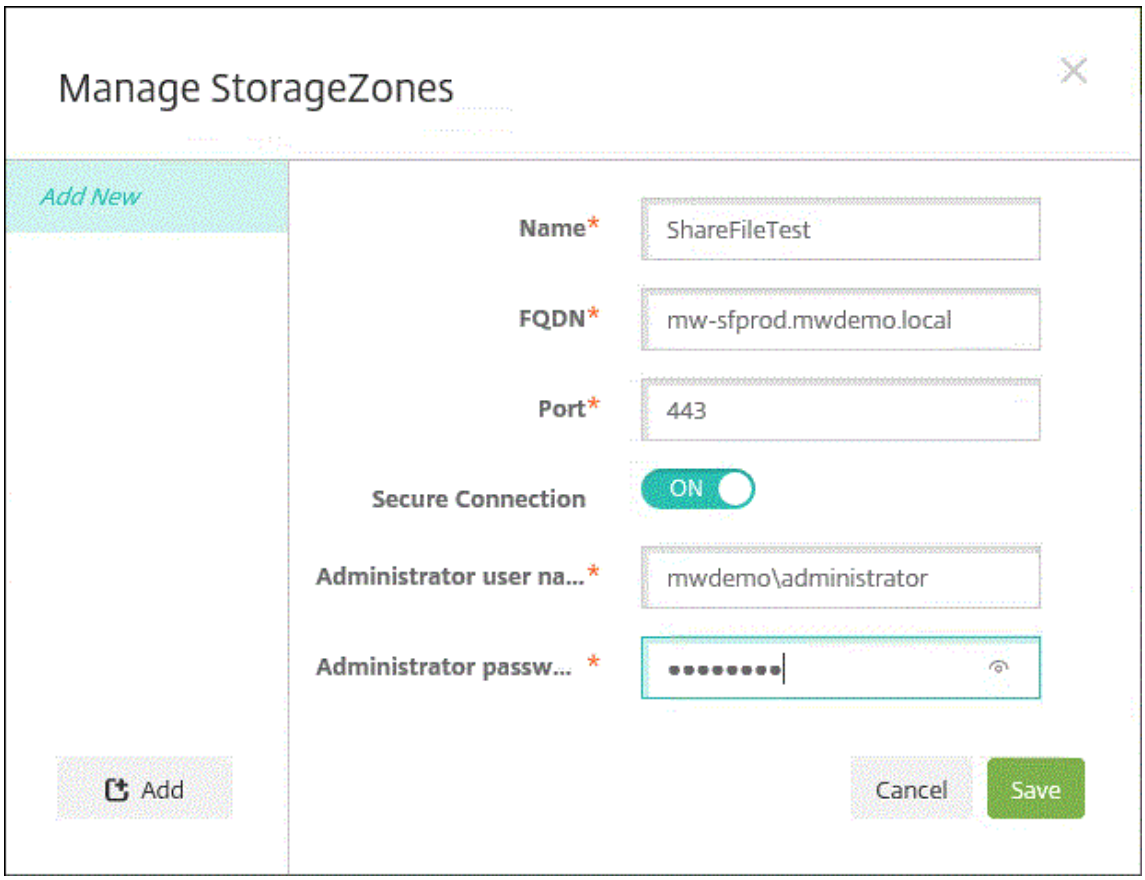
Click **Configure Connectors** to continue with the configuration steps in this article.



1. In **Configure > ShareFile**, click **Manage StorageZones**.



2. In **Manage StorageZones**, add the connection information.



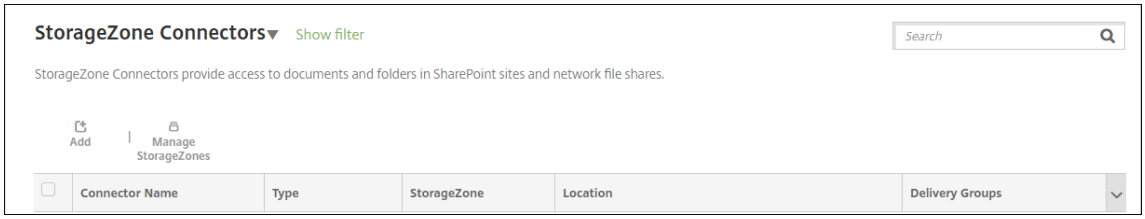
- **Name:** A descriptive name for the StorageZone, used to identify the StorageZone in XenMobile. Don't include a space or special characters in the name.
- **FQDN and Port:** The fully qualified domain name and port number for a storage zones controller that is reachable from the XenMobile Server.
- **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 XenMobile 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 StorageZones**.

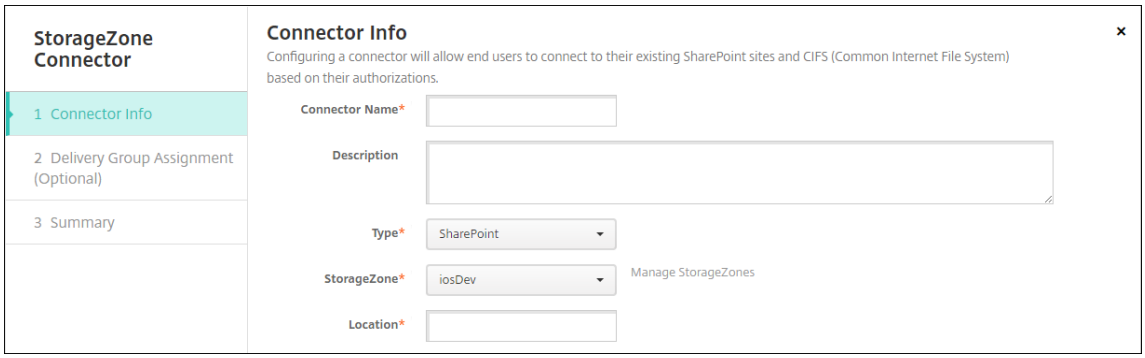
   To edit or delete the information for a storage zones controller connection, select the connection name in **Manage StorageZones**. Then, click **Edit** or **Delete**.

Add a storage zone connector in XenMobile

1. Go to **Configure > ShareFile** and then click **Add**.

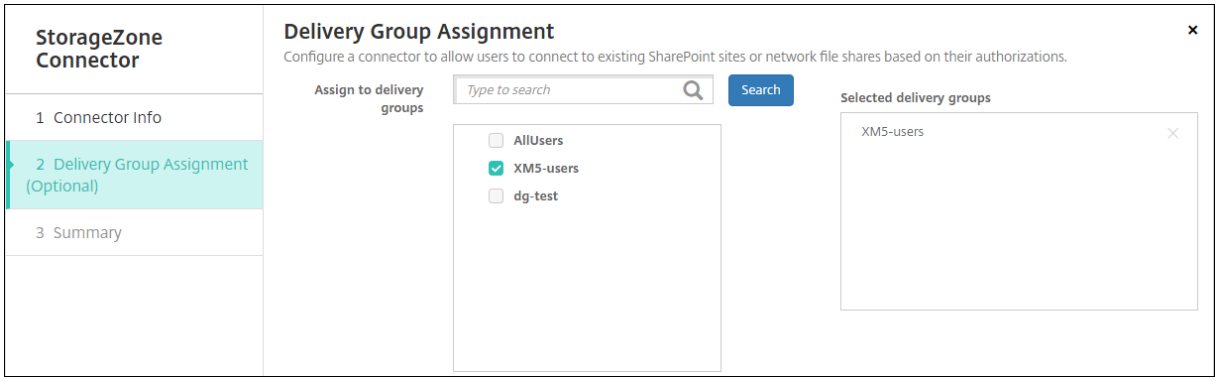


2. On the **Connector Info** page, configure these settings:



   - **Connector Name:** A name that identifies the storage zone connector in XenMobile.
   - **Description:** Optional notes about this Connector.
   - **Type:** Choose either **SharePoint** or **Network**.
   - **StorageZone:** Choose the storage zone associated with the Connector. If the storage zone isn't listed, click **Manage StorageZones** 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**.



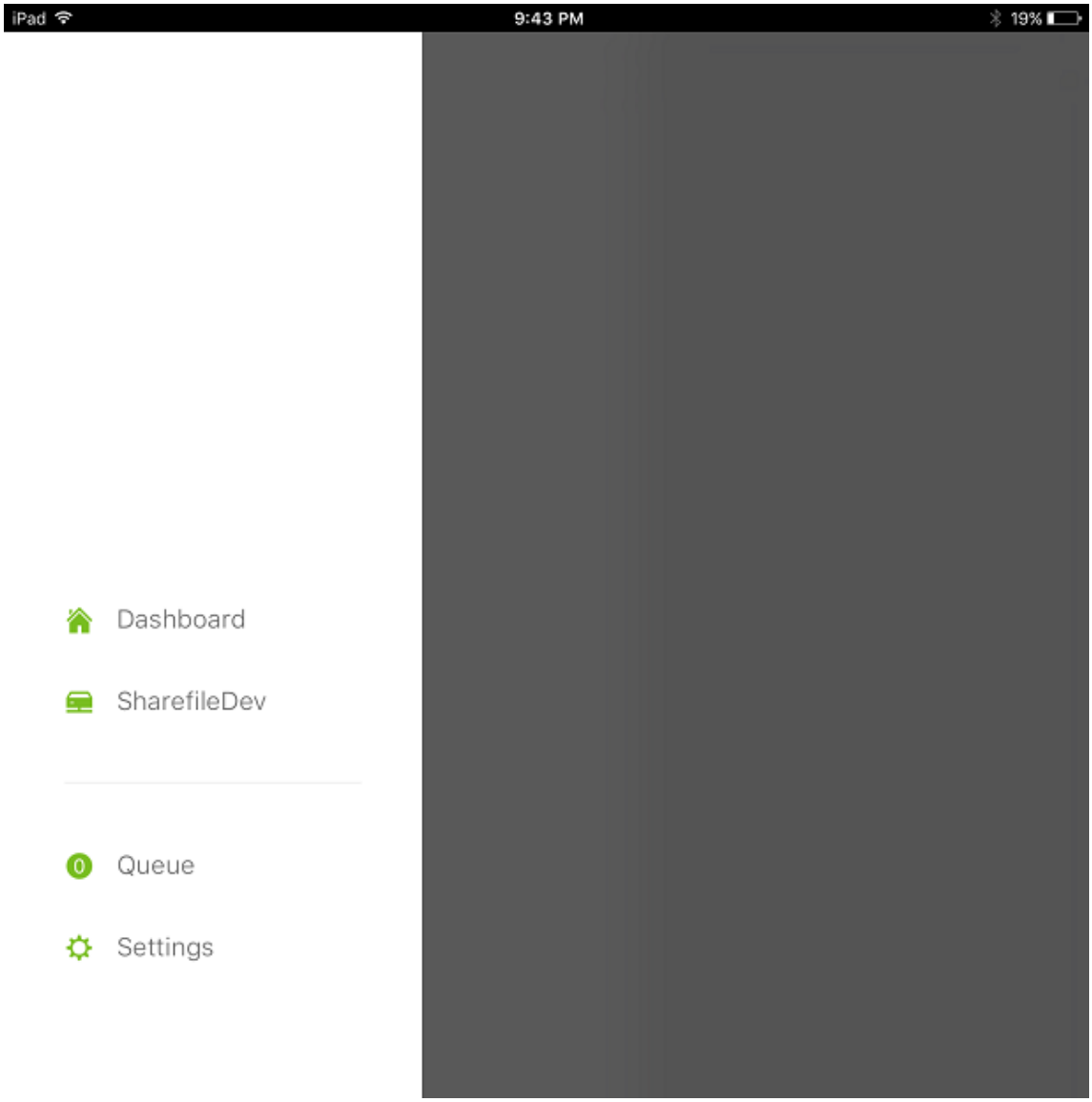
1. On the **Summary** page, you can review the options you configured. To adjust the configuration, click **Back**.
2. Click **Save** to save the Connector.
3. Test the connector:
   a) When you wrap the Citrix Files clients, do the following:
      - Set the Network access policy to **Tunneled to the internal network**.

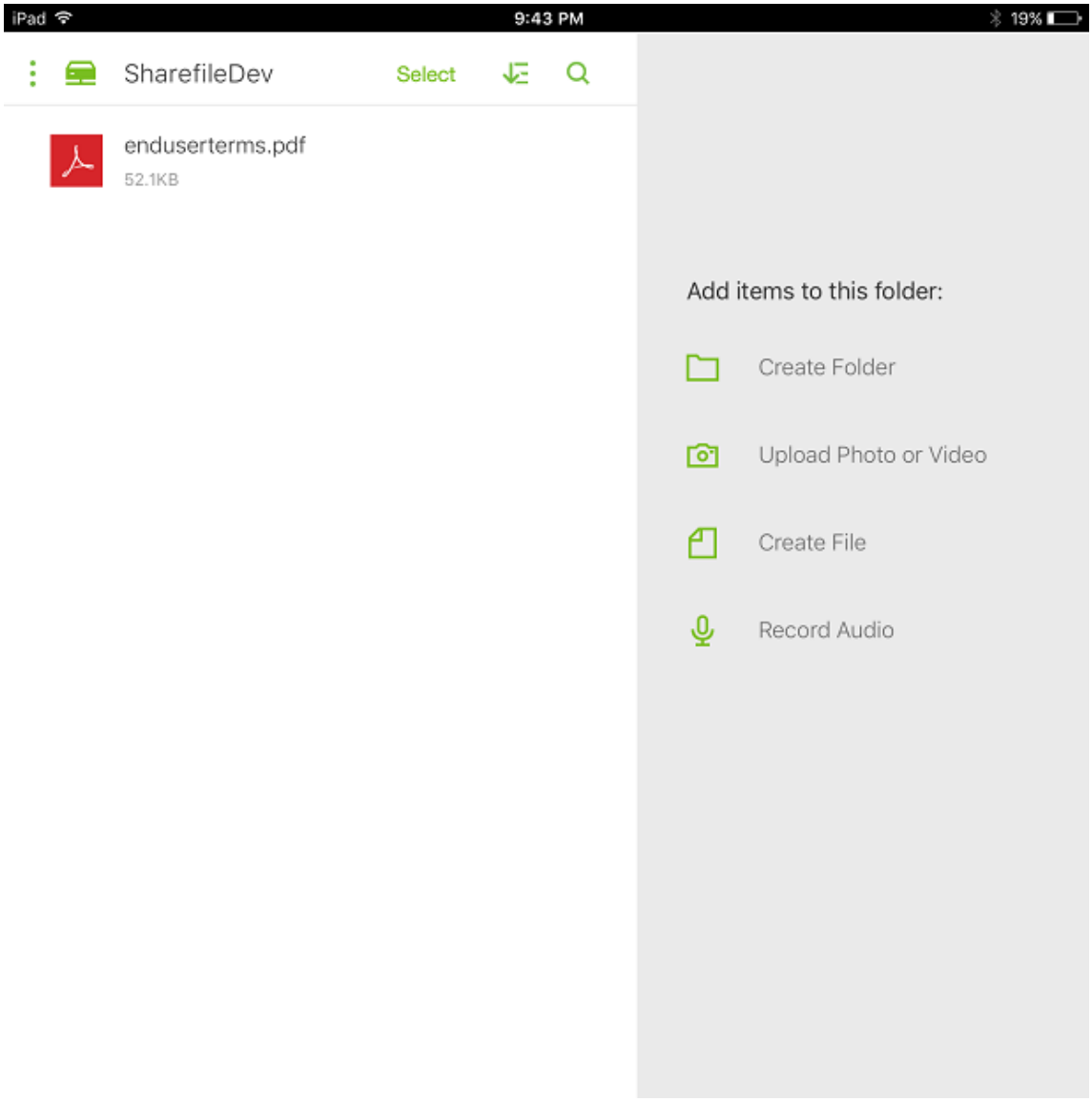
      In this mode of operation, the XenMobile MDX framework intercepts all network traffic from the Citrix Files client. The traffic redirects through Citrix Gateway by using an app-specific micro VPN.
      - Set the Preferred VPN mode policy to **Tunneled - Web SSO**.

      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 XenMobile. For details, see Integrating and delivering Citrix Files for Endpoint Management clients.
   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.

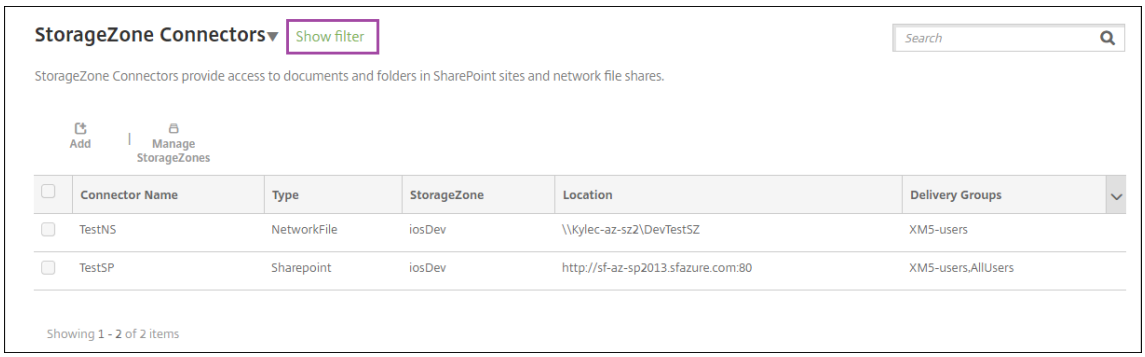




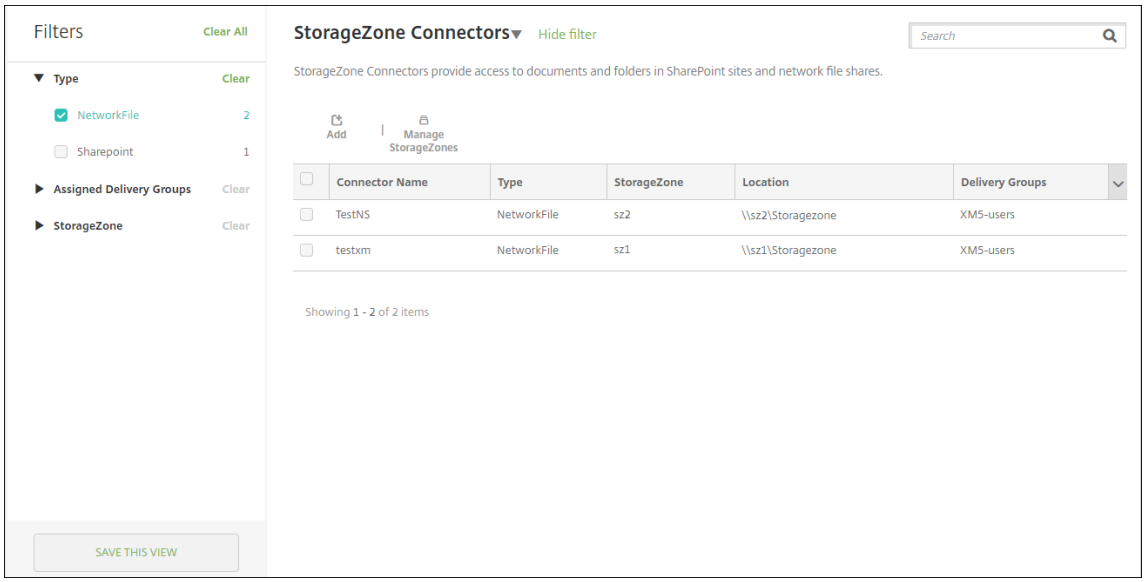
Filter the storage zone connectors list

You can filter the list of storage zone connectors by Connector type, assigned delivery groups, and storage zone.

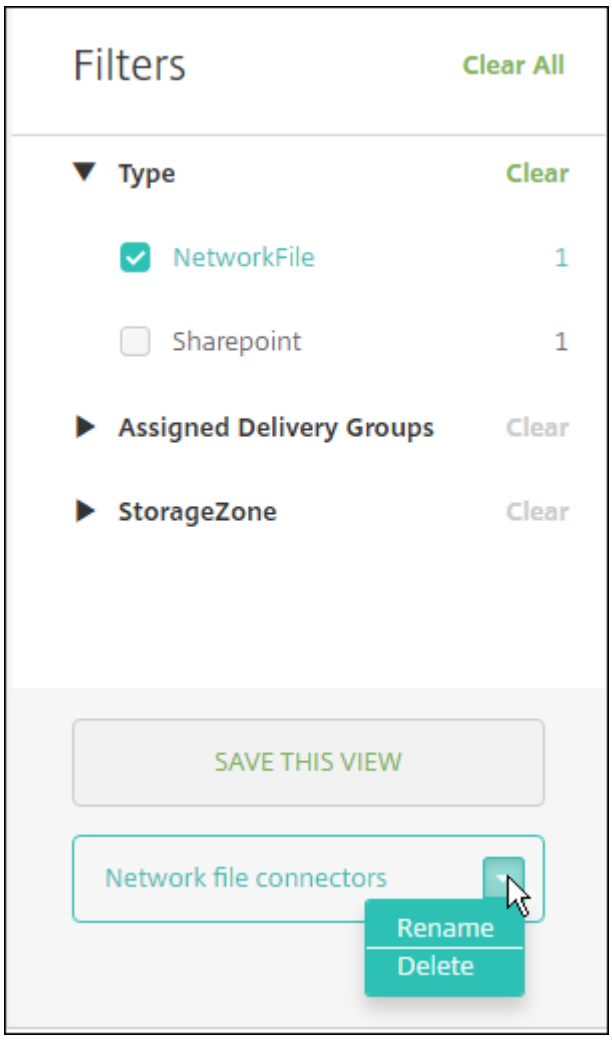
1. Go to **Configure > ShareFile** and then click **Show filter**.



2. Expand the filter headings to make selections. To save a filter, click **Save This View**, type the filter name, and click **Save**.



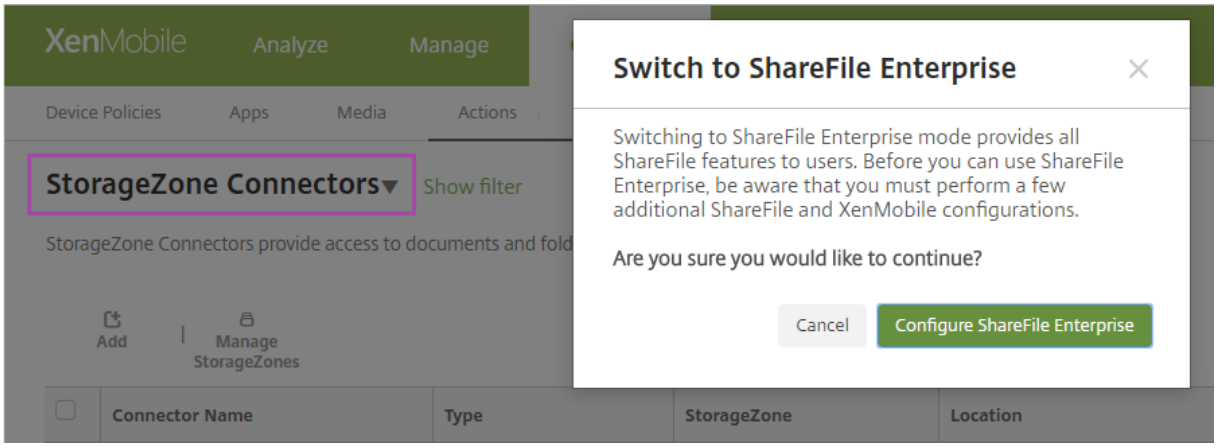
3. To rename or delete a filter, click the arrow icon beside the filter name.



Switch to Citrix Files

After integrating storage zone connectors with XenMobile, you can later switch to the full Enterprise feature set. Use of the Citrix Files feature set requires XenMobile Enterprise Edition. XenMobile retains your existing storage zone connector integration settings.

Go to **Configure > ShareFile**, click the **StorageZone Connectors** drop-down menu, and then click **Configure ShareFile Enterprise**.



For information about configuring Citrix Files, 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 Virtual Apps and Desktops by using a SmartAccess policy that denies access to out-of-compliance devices. XenMobile 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:

- Virtual Apps and Desktops 7.6
- StoreFront 3.7 or 3.8
- XenMobile Server configured to aggregate HDX apps from a StoreFront server
- XenMobile Server configured with a SAML certificate to be used for signing and encrypting tags. The same certificate without private key is uploaded on StoreFront server.

To start using this feature:

- Configure the XenMobile Server certificate to the StoreFront store
- Configure at least one Virtual Apps and Desktops delivery group with the required SmartAccess policy
- Set the automated action in XenMobile

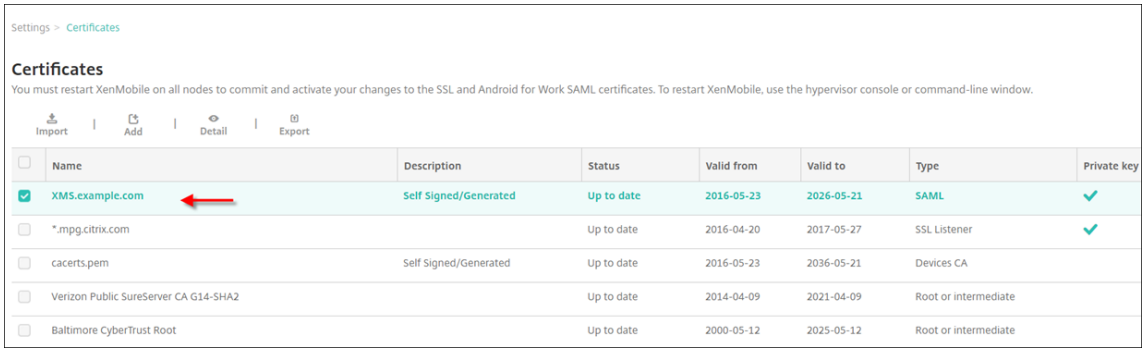
Export and configure the XenMobile Server certificate and upload it to the StoreFront store

SmartAccess uses signed and encrypted tags to communicate between the XenMobile and StoreFront servers. To enable that communication, you add the XenMobile Server certificate to the StoreFront store.

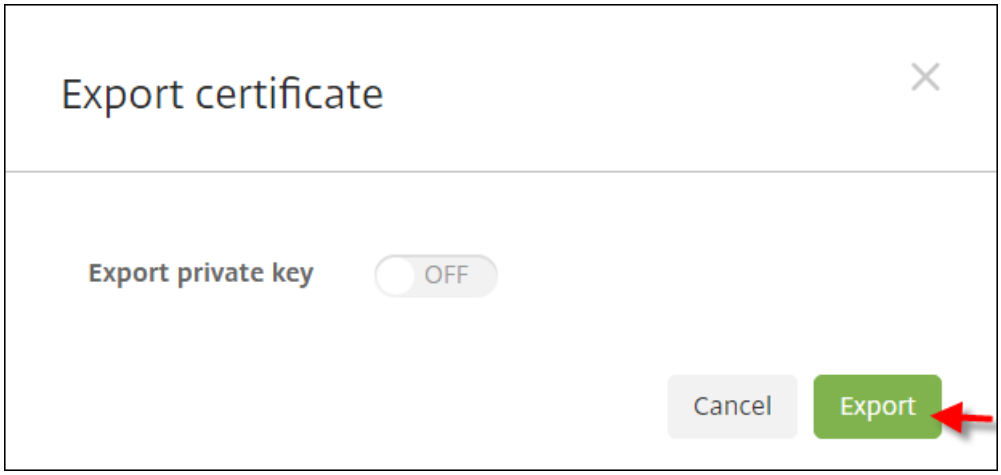
For more information about integrating StoreFront and XenMobile when XenMobile is enabled with domain and certificate-based authentication, see the Support Knowledge Center.

Export the SAML certificate from the XenMobile Server

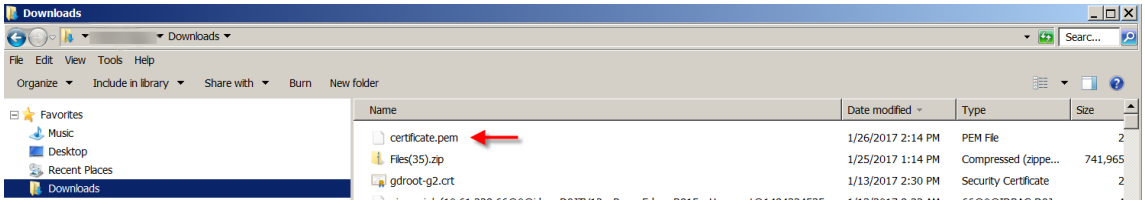
1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears. Click **Certificates**.
2. Locate the SAML certificate for XenMobile Server.



3. Ensure that **Export private key** is set to **Off**. Click **Export** to export the certificate to your download directory.

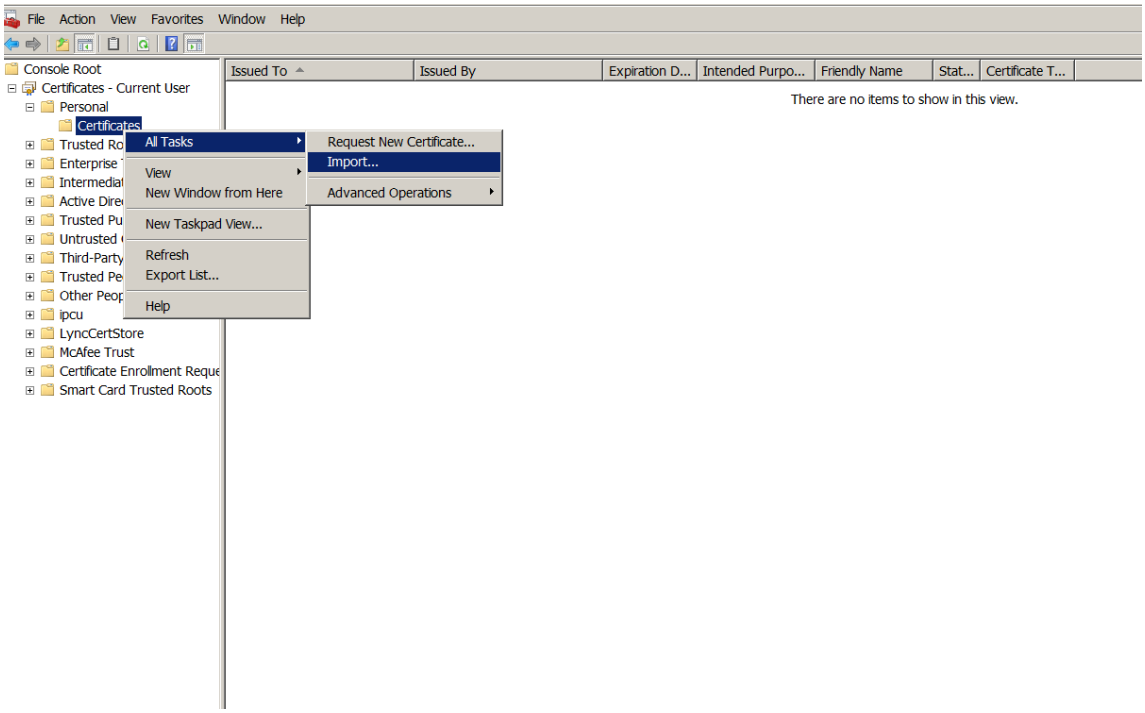


4. Locate the certificate in your download directory. The certificate is in PEM format.

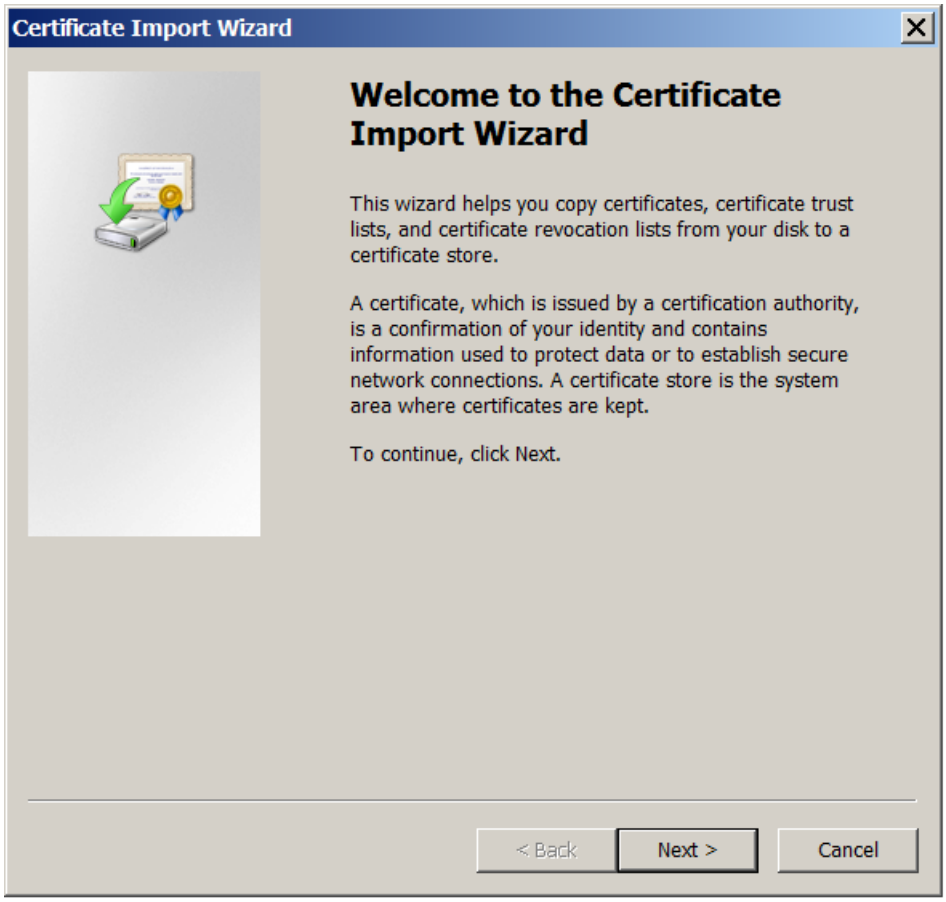


Convert the certificate from PEM to CER

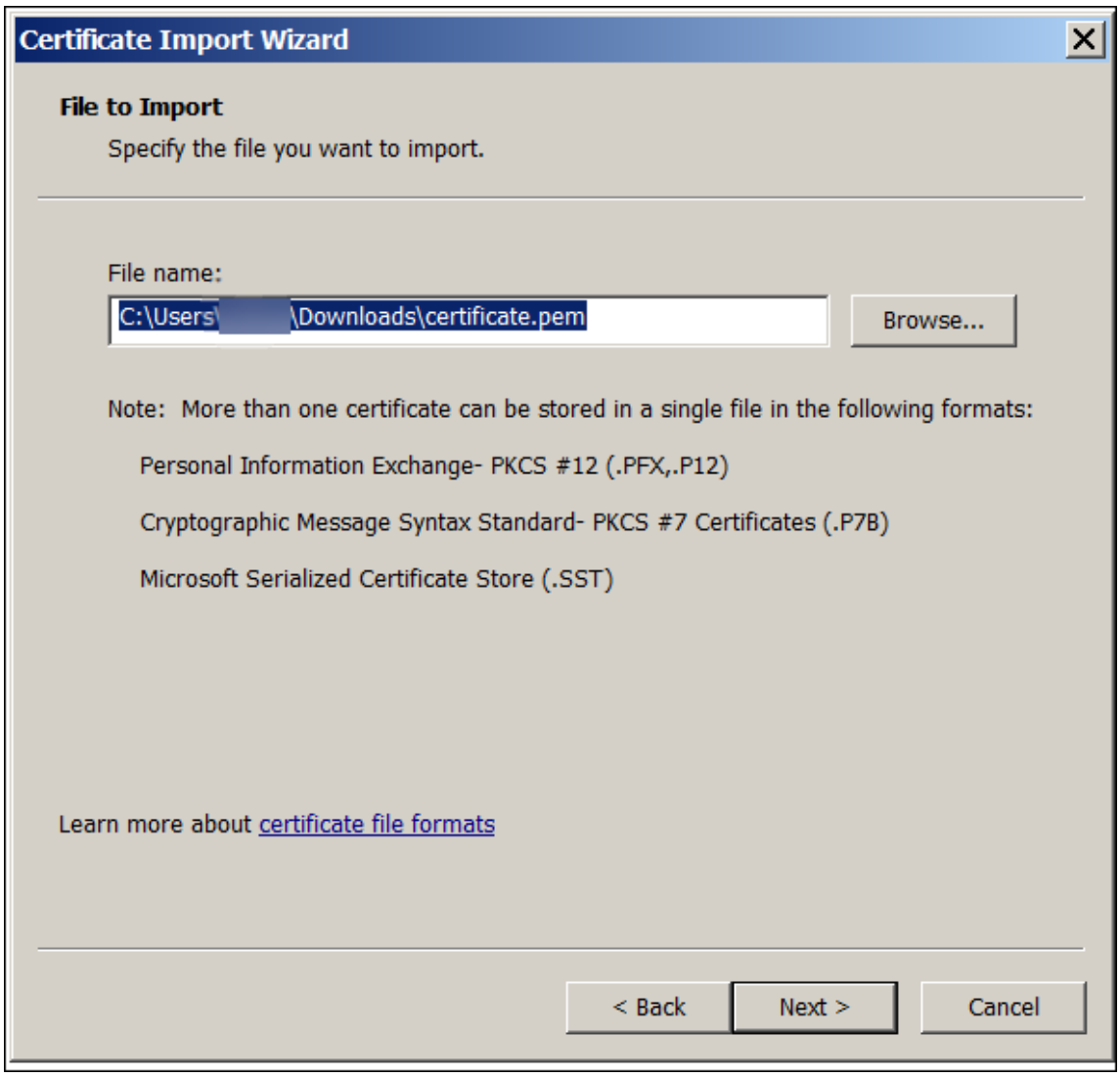
1. Open the Microsoft Management Console (MMC) and right-click **Certificates > All Tasks > Import**.



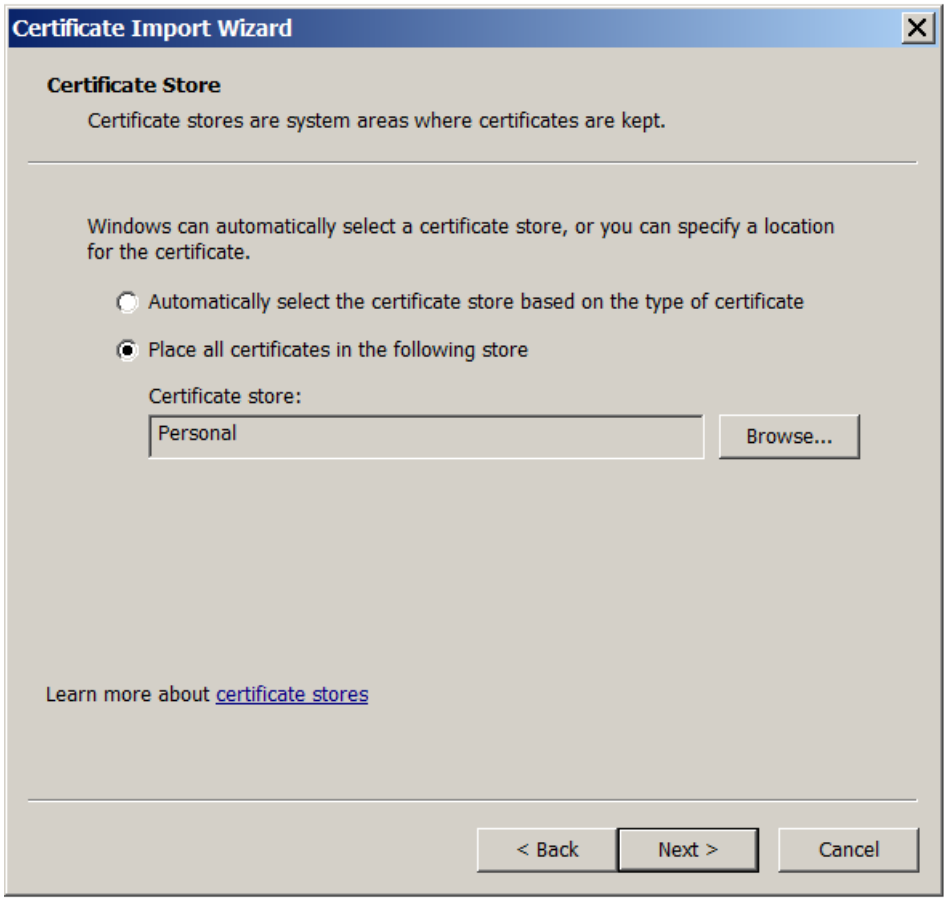
2. When the certificate import wizard appears, click **Next**.



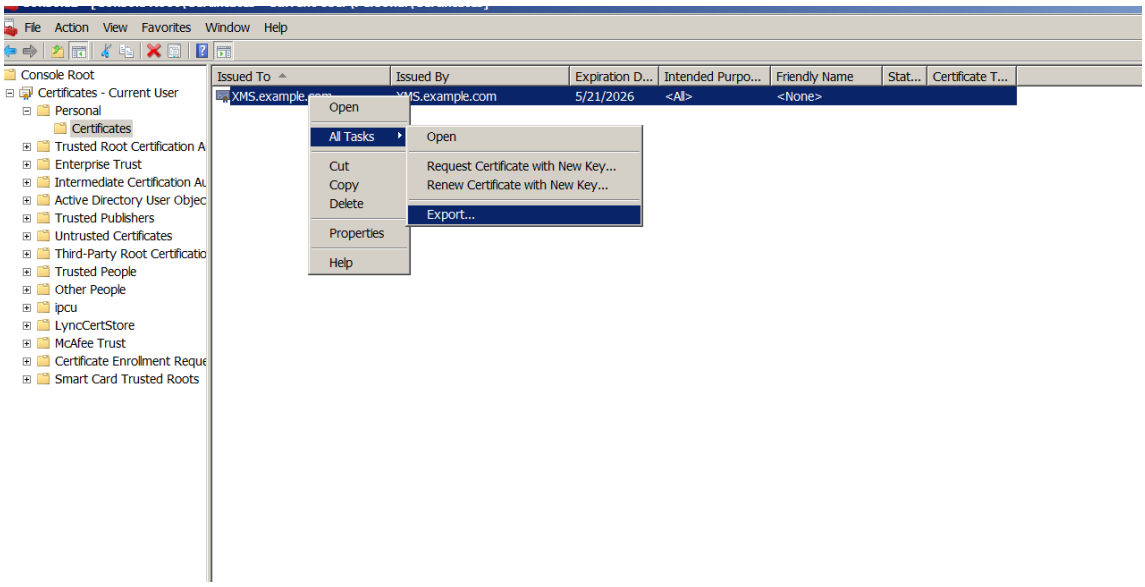
3. Browse to the certificate in the download directory.



4. Select **Place all certificates in the following store** and select **Personal** as the certificate store. Click **Next**.

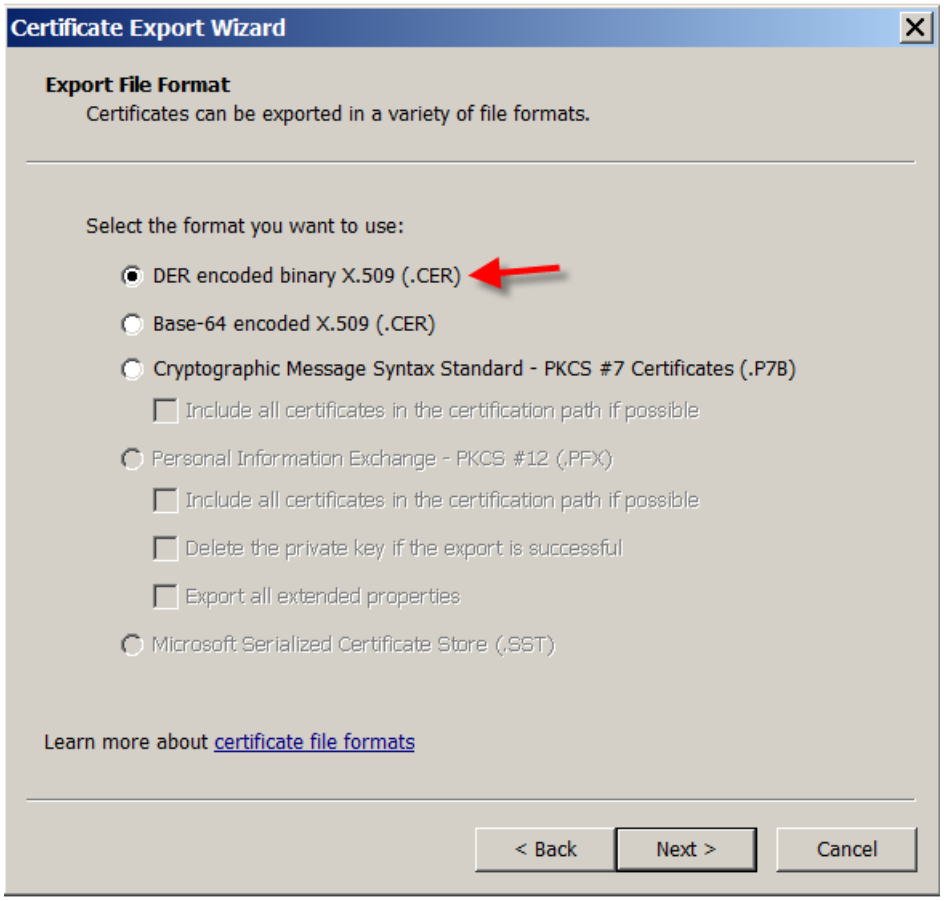


5. Review your selections and click **Finish**. Click **OK** to dismiss the confirmation window.
6. In the MMC, right-click the certificate and then choose **All Tasks > Export**.

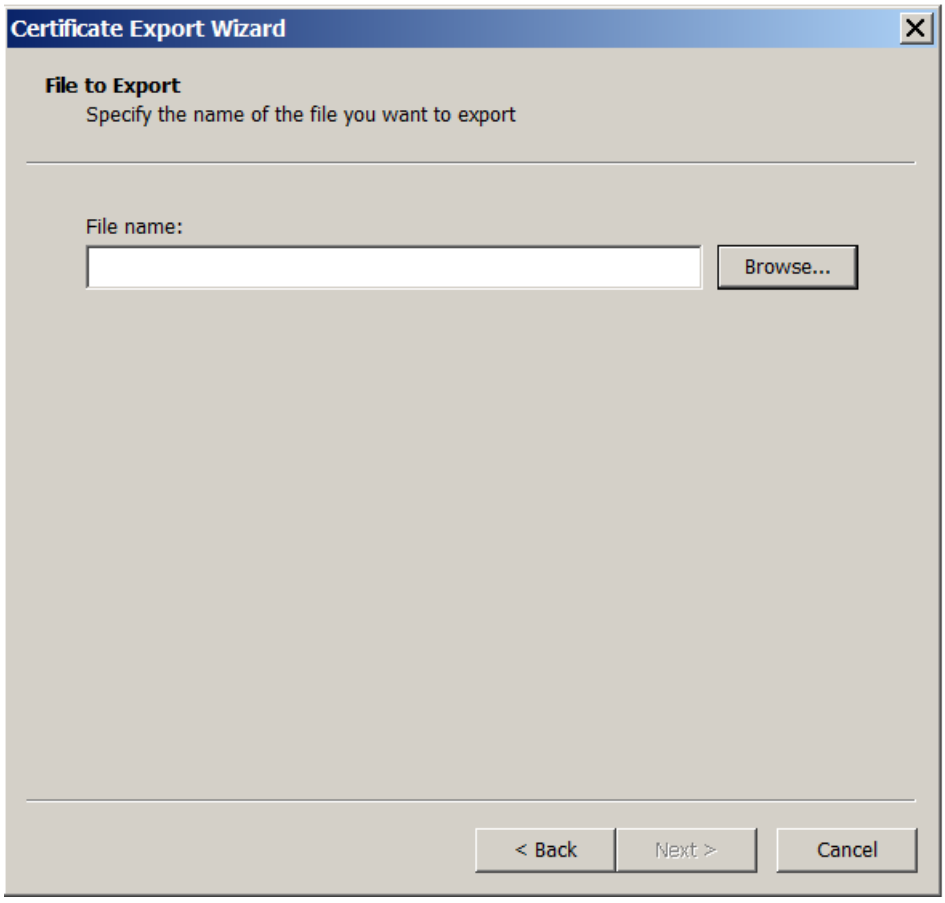


7. When the certificate export wizard appears, click **Next**.

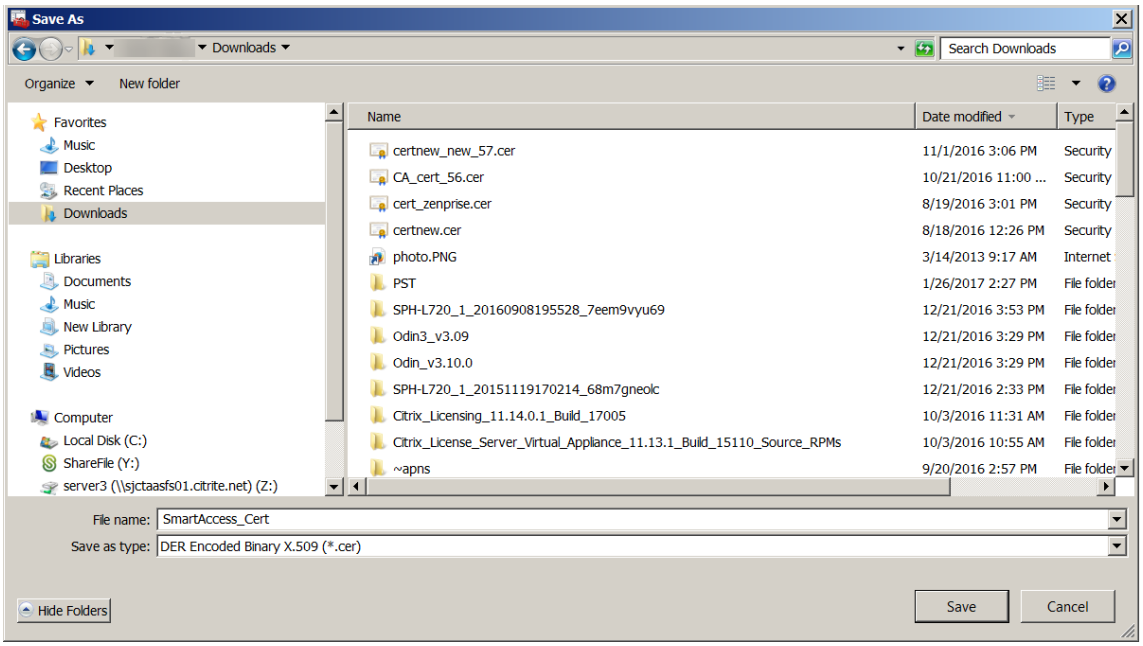
8. Choose the format **DER encoded binary X.509 (.CER)**. Click **Next**.



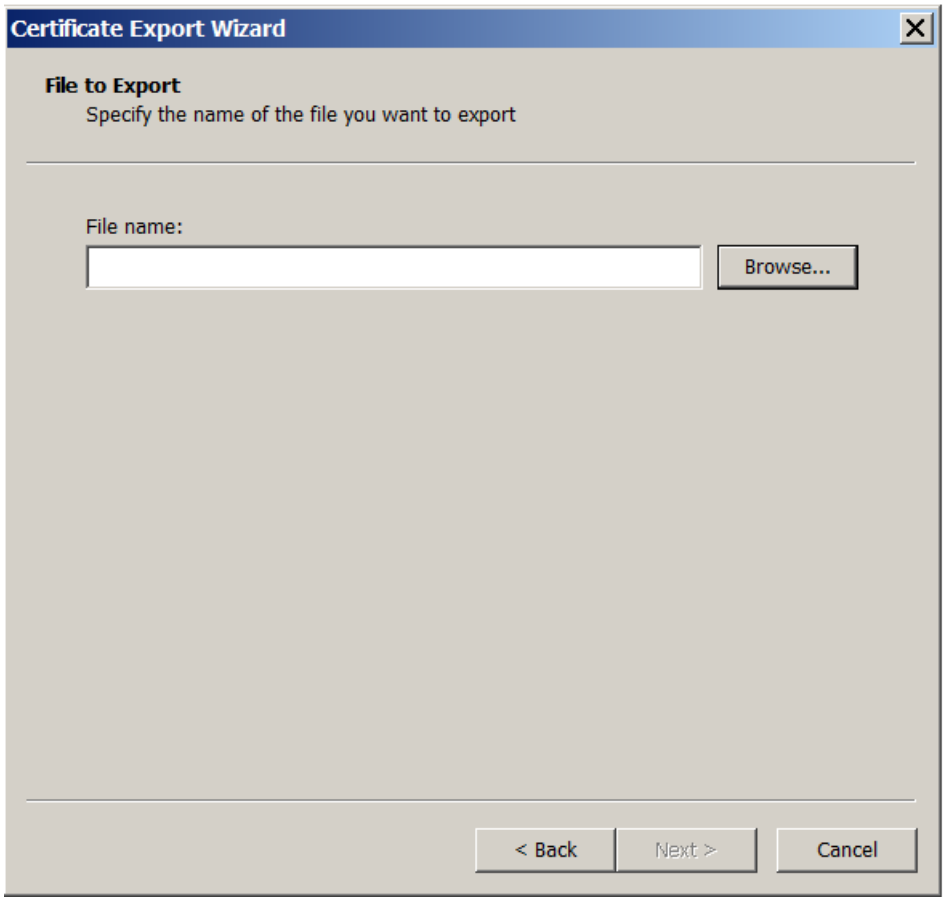
9. Browse to the certificate. Type a name for the certificate and then click **Next**.



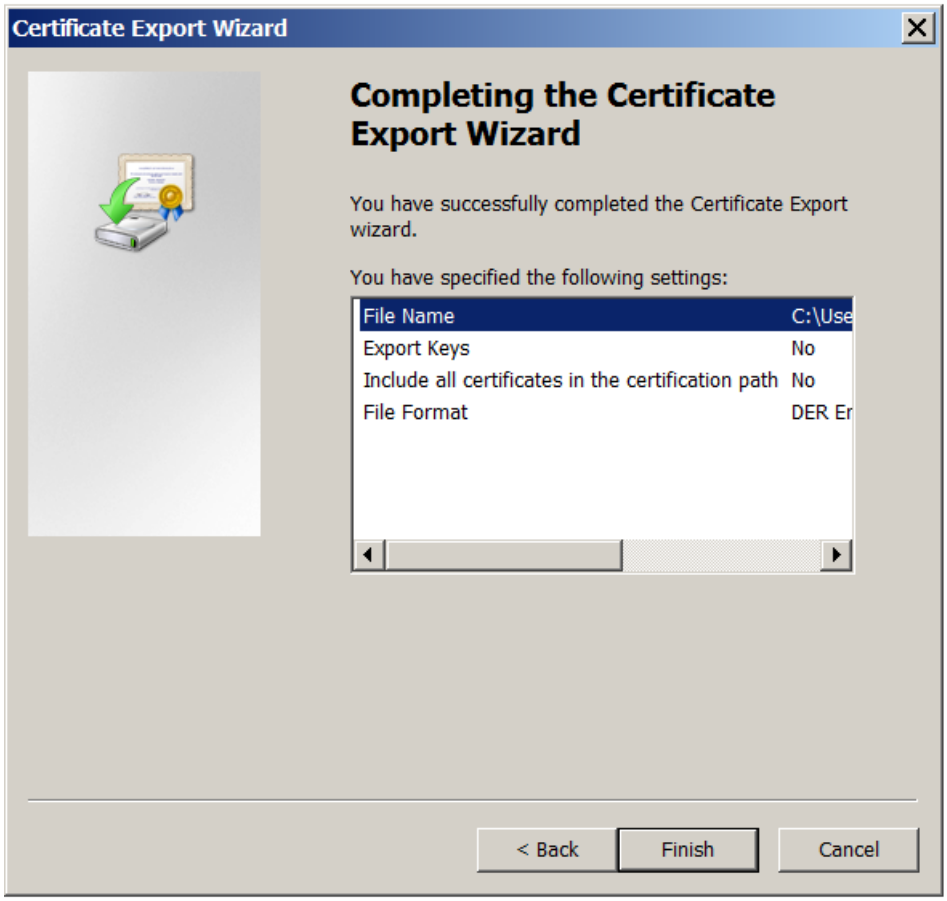
10. Save the certificate.



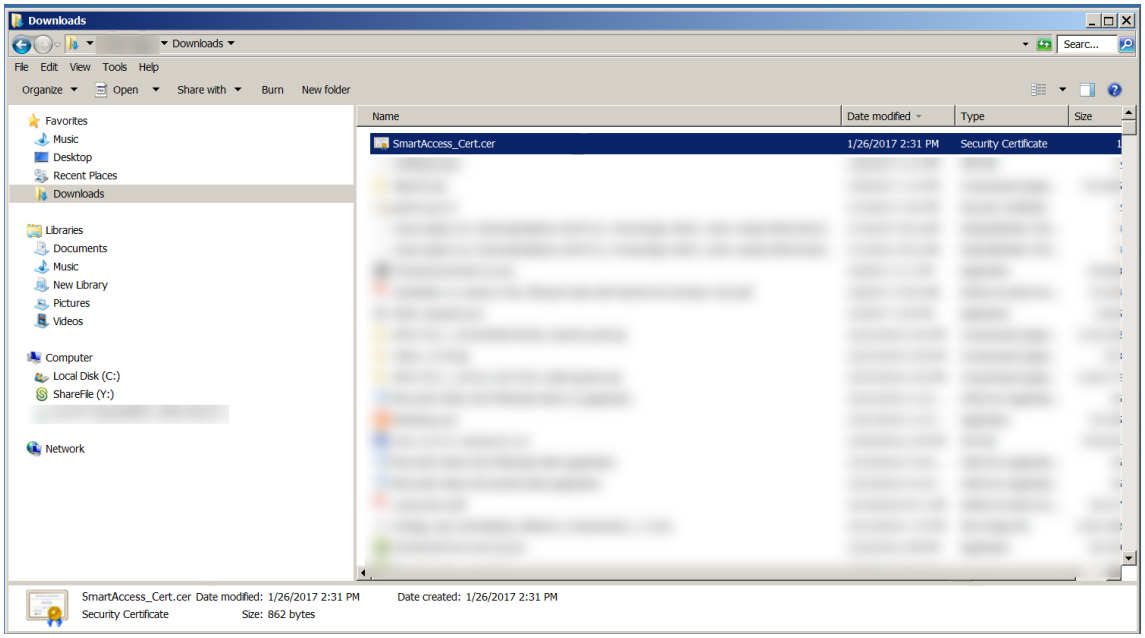
11. Browse to the certificate and click **Next**.



12. Review your selections and click **Finish**. Click **OK** to dismiss the confirmation window.

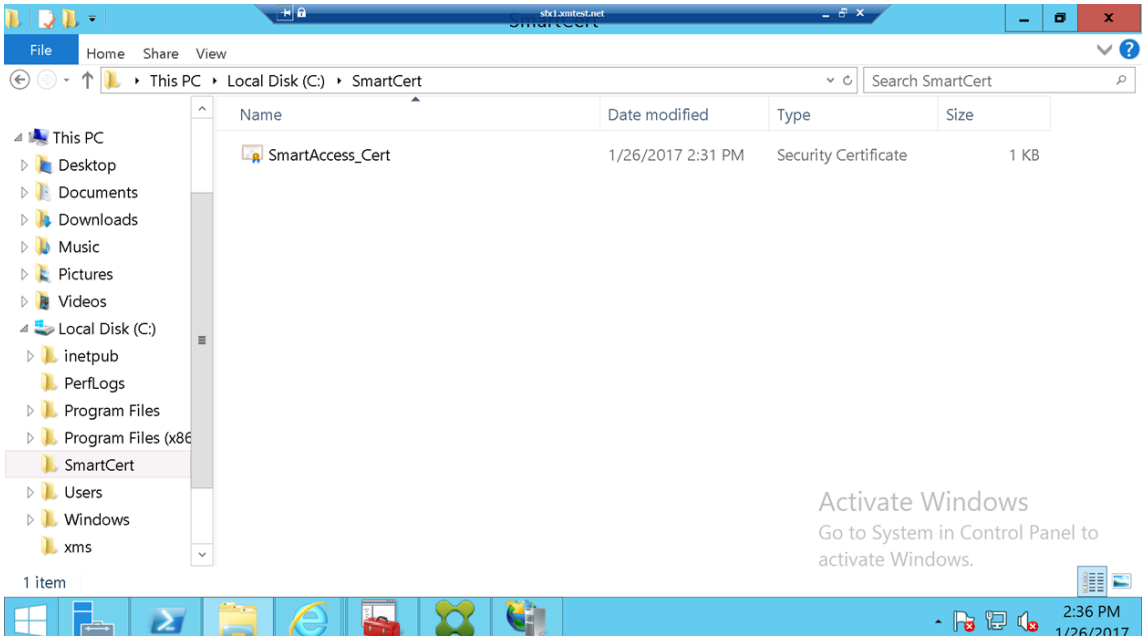


13. Locate the certificate in your download directory. Note that the certificate is in CER format.



Copy the certificate to the StoreFront Server

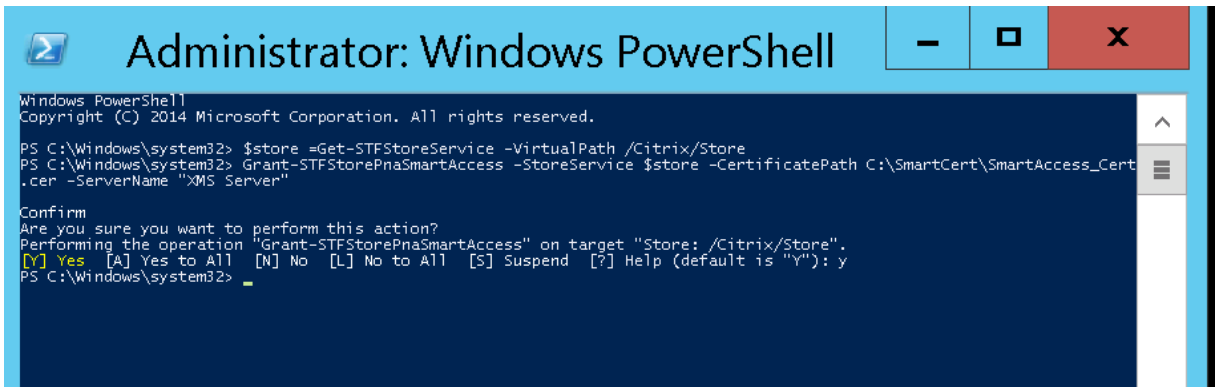
1. On the StoreFront server, create a folder called **SmartCert**.
2. Copy the certificate to the **SmartCert** folder.



Configure the certificate on the StoreFront store

On the StoreFront server, run this PowerShell command to configure the converted XenMobile 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:


```
    Revoke-STFStorePnaSmartAccess -StoreService $store -All
<!--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:

```
    $store = Get-STFStoreService -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess -StoreService $store -ServerName "
       My XM Server"
<!--NeedCopy-->
```

- Revoke by thumbprint:

```
    $store = Get-STFStoreService -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess -StoreService $store -
       CertificateThumbprint "ReplaceWithThumbprint"
<!--NeedCopy-->
```

- Revoke by server object:

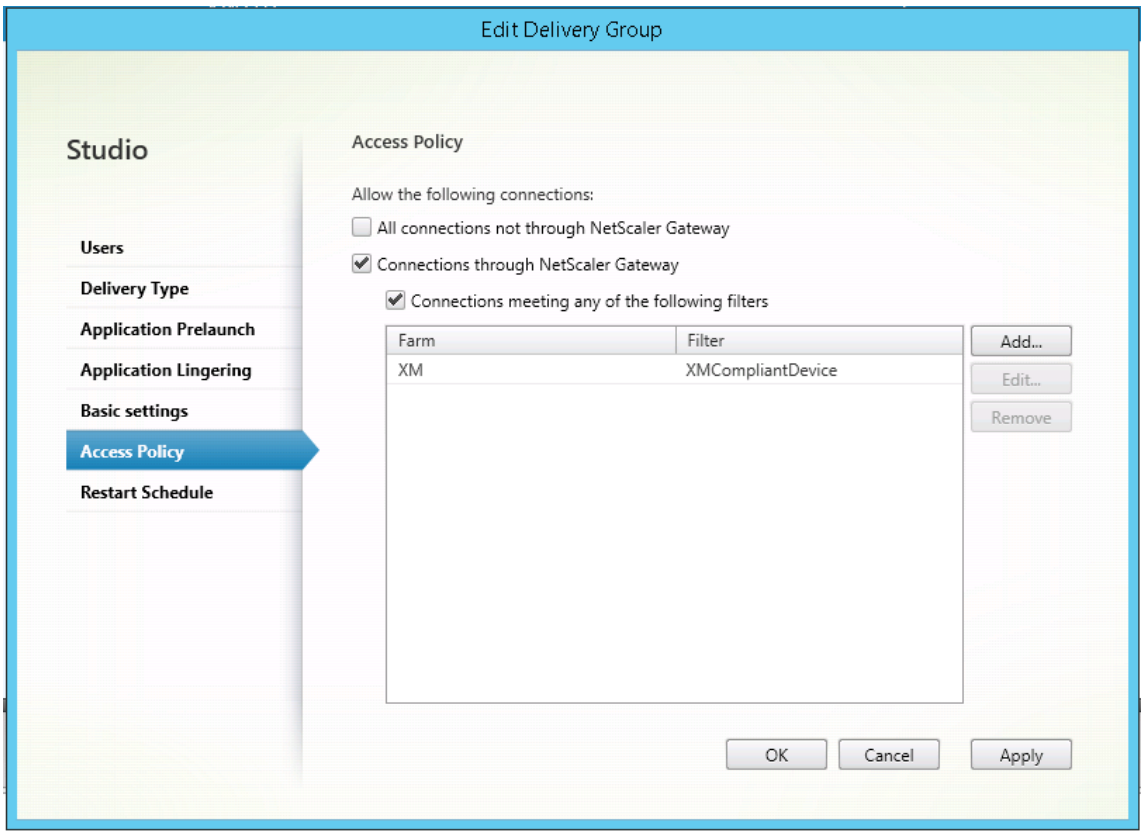
```
    $store = Get-STFStoreService -VirtualPath /Citrix/Store

    $access = Get-STFStorePnaSmartAccess -StoreService $store

    Revoke-STFStorePnaSmartAccess -StoreService $store -SmartAccess
       $access.AccessConditionsTrusts[0]
<!--NeedCopy-->
```

Configure the SmartAccess policy for Virtual Apps and Desktops

To add the required SmartAccess policy to the delivery group delivering the HDX app:

1. On the Virtual Apps and Desktops server, open Citrix Studio.
2. Select **Delivery Groups** in the Studio navigation pane.

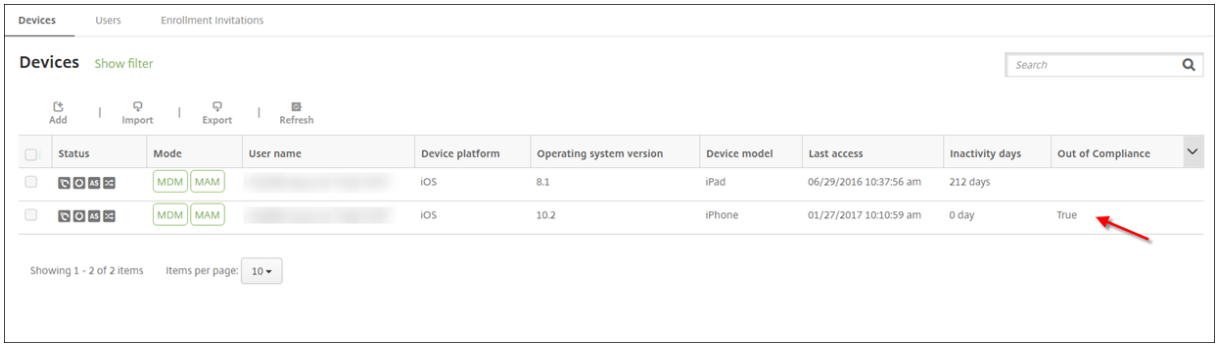
3. Select a group delivering the app or apps you want to control access to. Then select **Edit Delivery Group** in the **Actions** pane.
4. On the **Access Policy** page, select **Connections through NetScaler Gateway** and **Connection meeting any of the following**.
5. Click **Add**.
6. Add an access policy where **Farm** is **XM** and **Filter** is **XMCompliantDevice**.



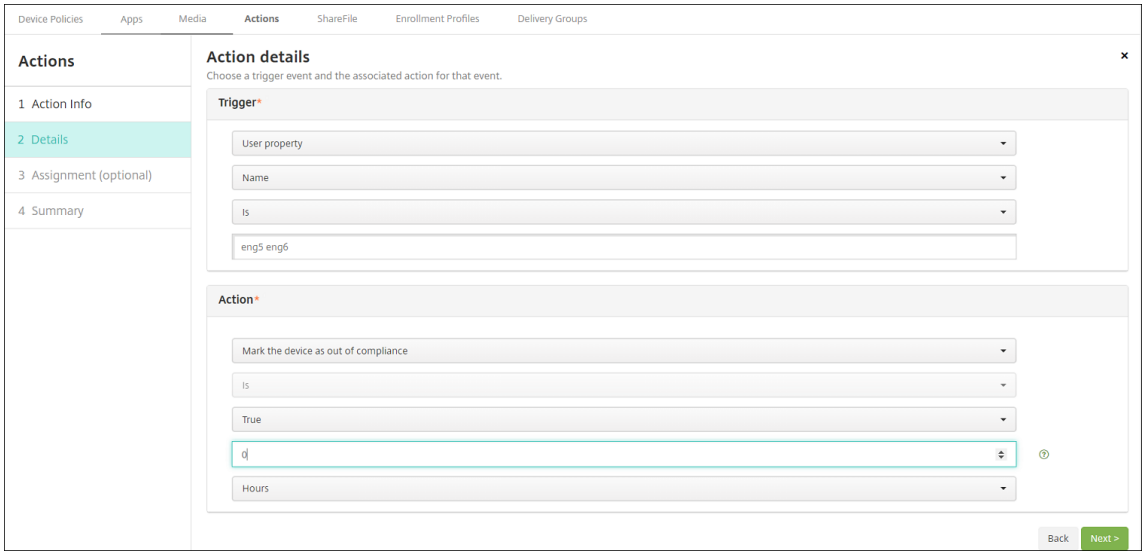
7. Click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

Set automated actions in XenMobile

The SmartAccess policy that you set in the delivery group for an HDX app denies access to a device when the device in out of compliance. Use automated actions to mark the device as out of compliance.



1. From the XenMobile 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**.



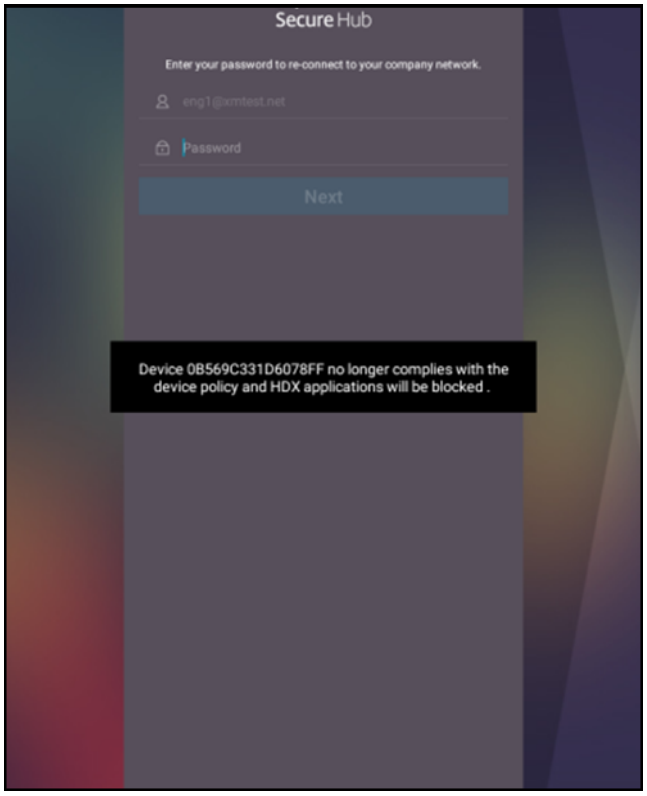
5. In the **Trigger** list, choose **Device property**, **User property**, or **Installed app name**. SmartAccess doesn't support event triggers.
6. In the **Action** list:
   - Choose **Mark the device as out of compliance.**
   - Choose **Is**.
   - Choose **True**.
   - To set the action to mark the device as out of compliance immediately when the trigger condition is met, set the time frame to **0**.
7. Choose the XenMobile 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.

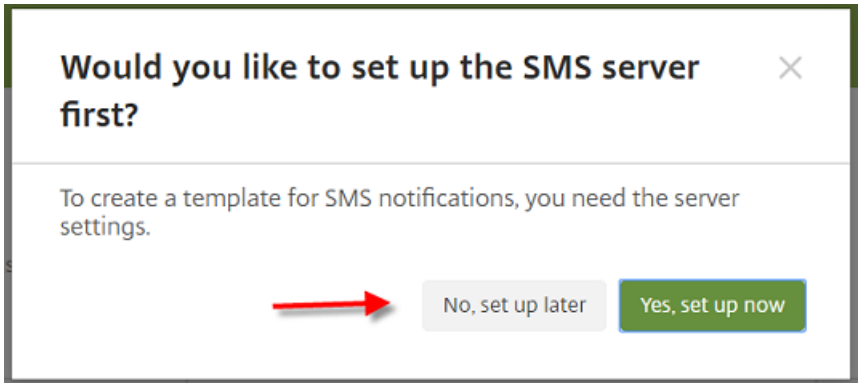
If you want users to be notified when a device is marked out of compliance, create a notification and then create an automated action to send that notification.

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.”



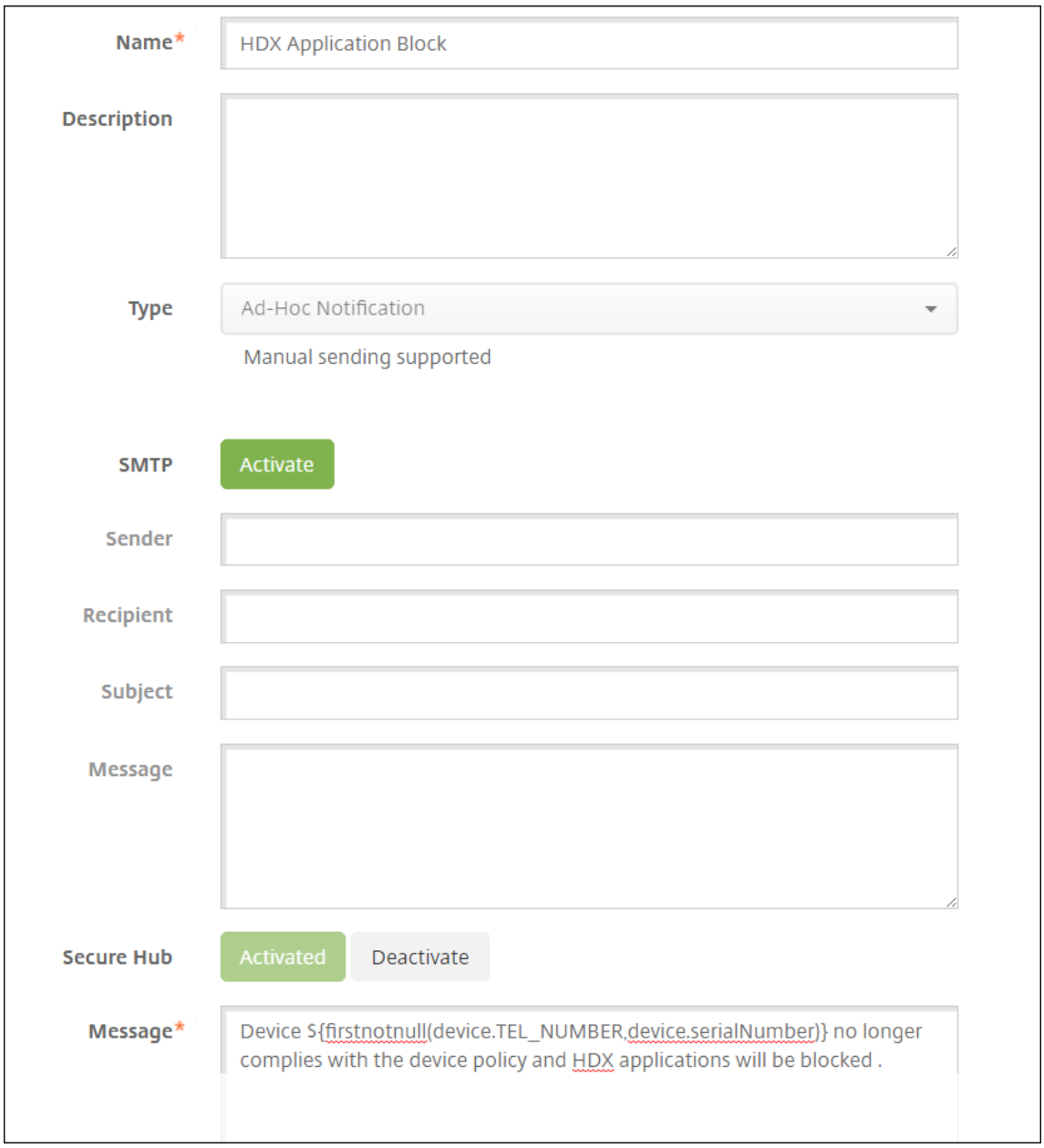
Create the notification users see when a device is marked as out of compliance

1. In the XenMobile 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.



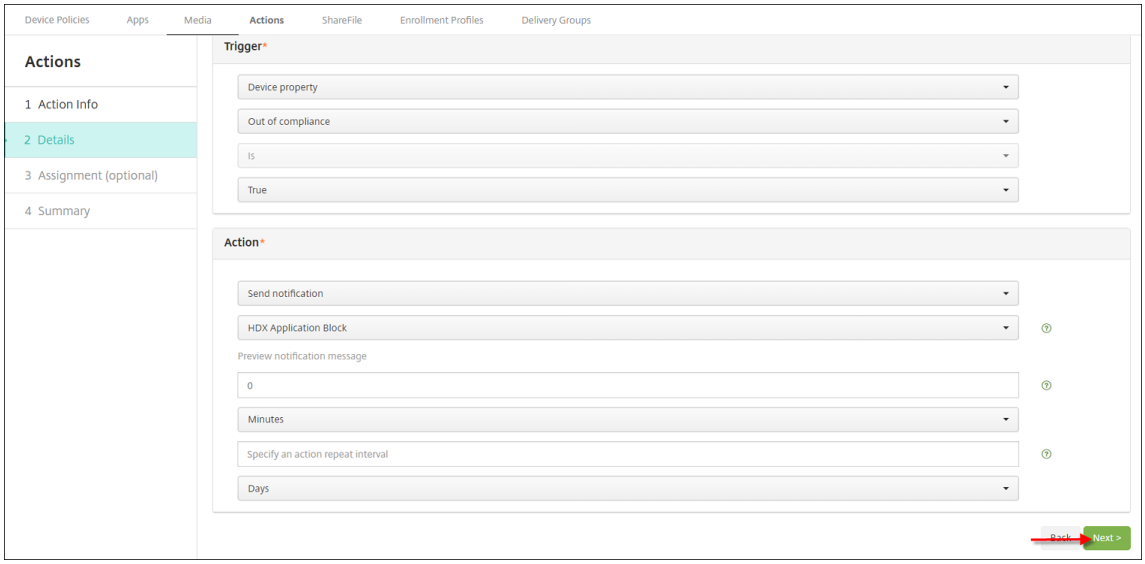
6. Click **Save**.

Create the action that sends the notification when a device is marked out of compliance

1. From the XenMobile 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**.



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 XenMobile 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**.

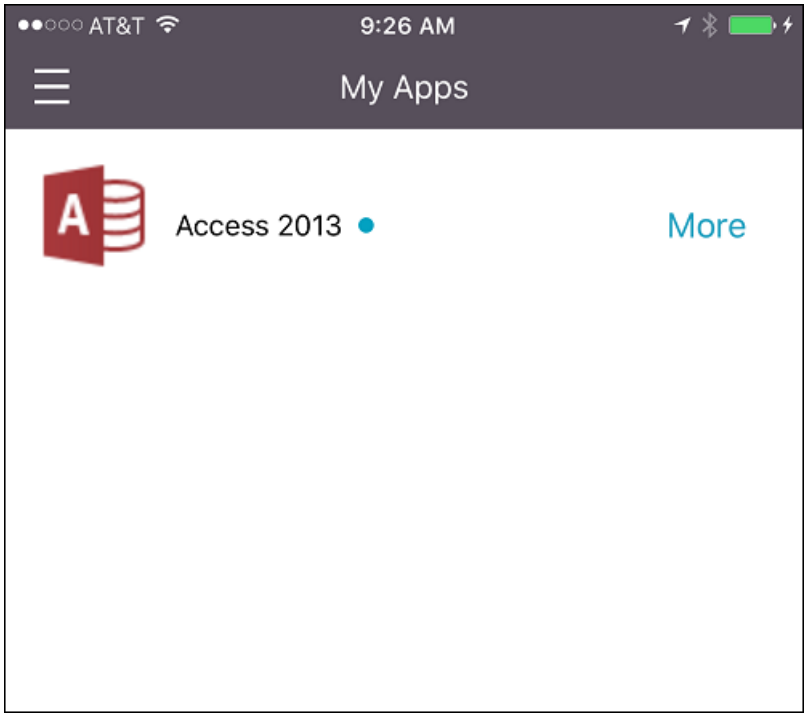
For more information on setting automated actions, see Automated actions.

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.



Add media

August 20, 2020

You add media to XenMobile so you can deploy the media to user devices. You can use XenMobile to deploy Apple Books that you obtain through Apple volume purchase.

After you configure a volume purchase account in XenMobile, 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. XenMobile 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.

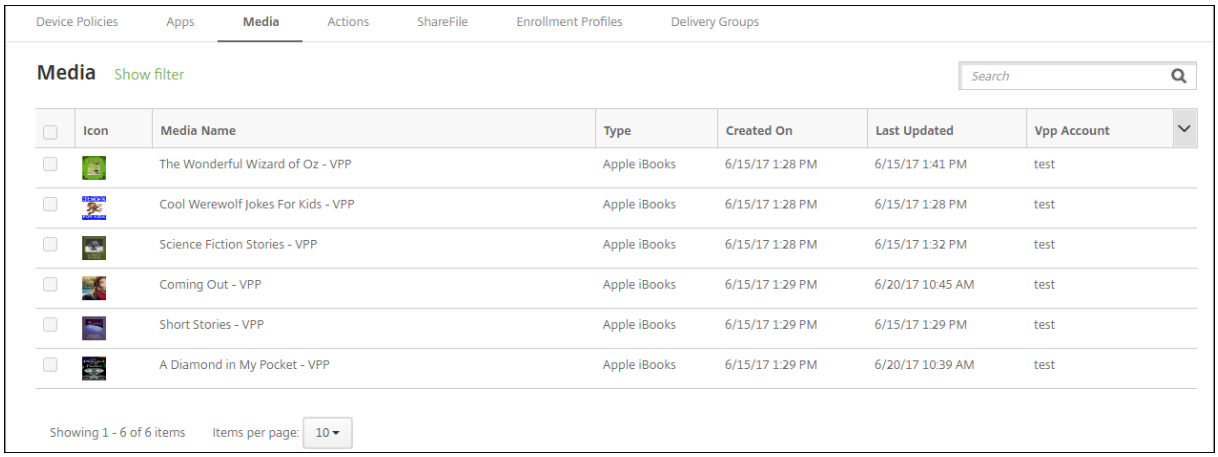
Prerequisites

- iOS devices

- Configure Apple volume purchase in XenMobile, as described in Apple Volume Purchase.

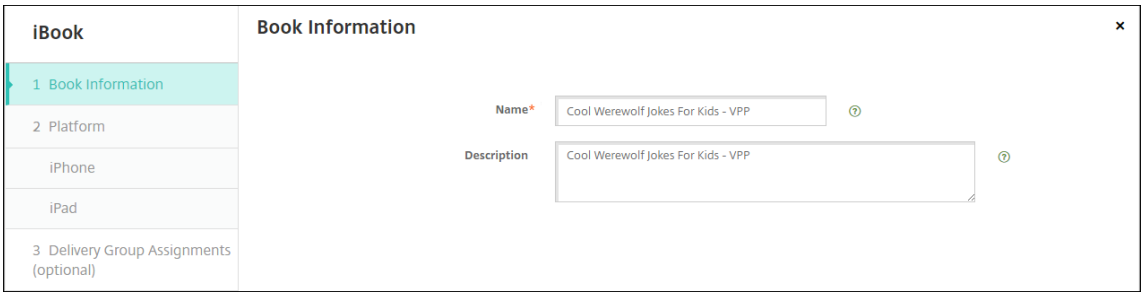
Configure books

Apple Books obtained through volume purchase appear on the **Configure > Media** page.



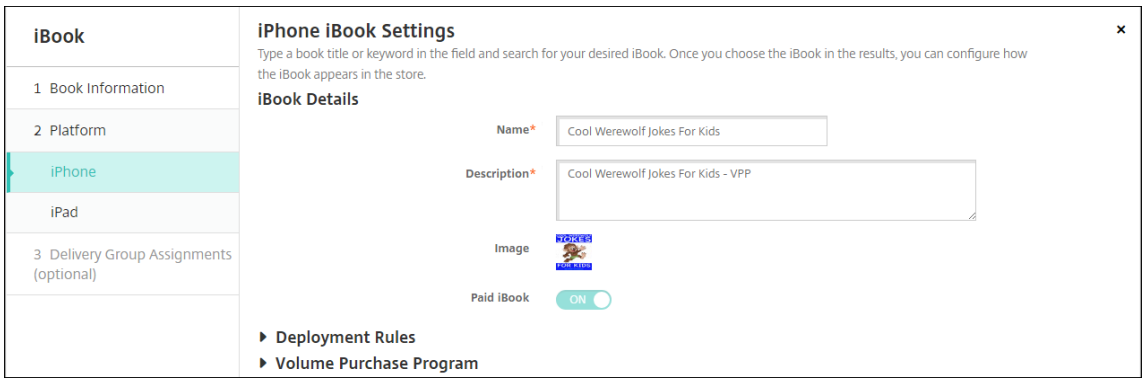
To configure an Apple Book for deployment

1. In **Configure > Media**, select a book and click **Edit**. The **Book Information** page appears.

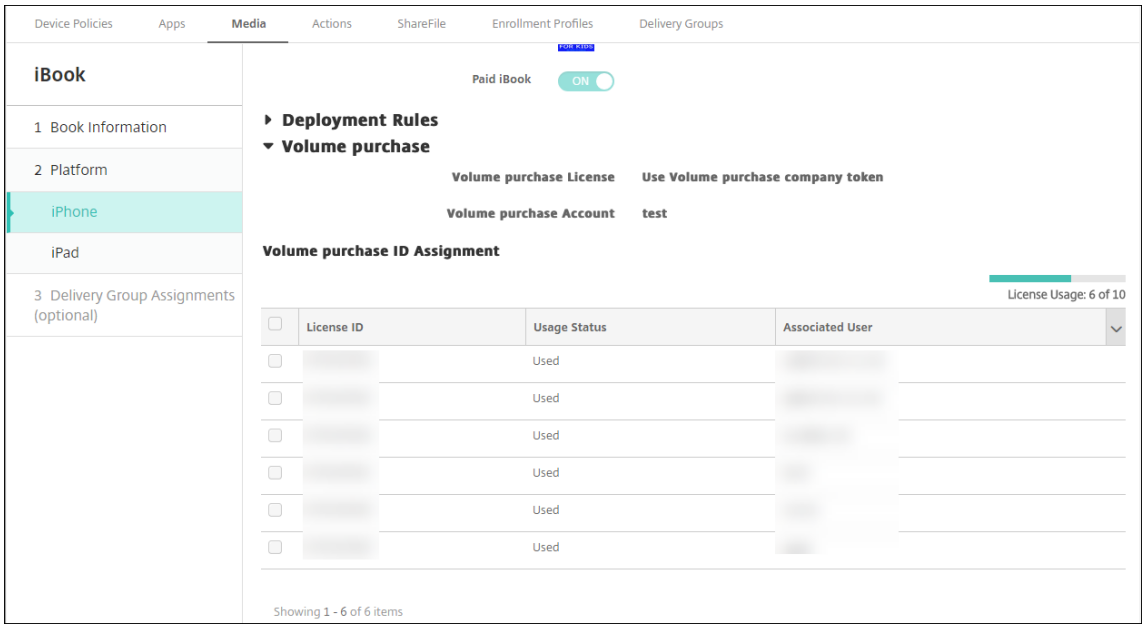


   The **Name** and **Description** appear only in the XenMobile console and logs.

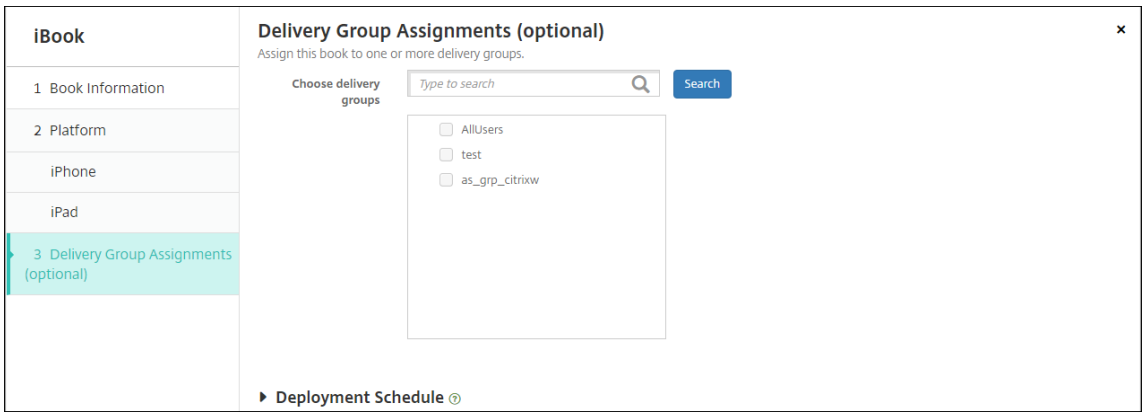
2. In the **iPhone iBook Settings** and **iPad iBook Settings** pages: While you can optionally change the book name and description, Citrix recommends that you don't change these settings. The image is for your information and isn't editable. **Paid iBook** indicates that a book is purchased through Apple volume purchase.



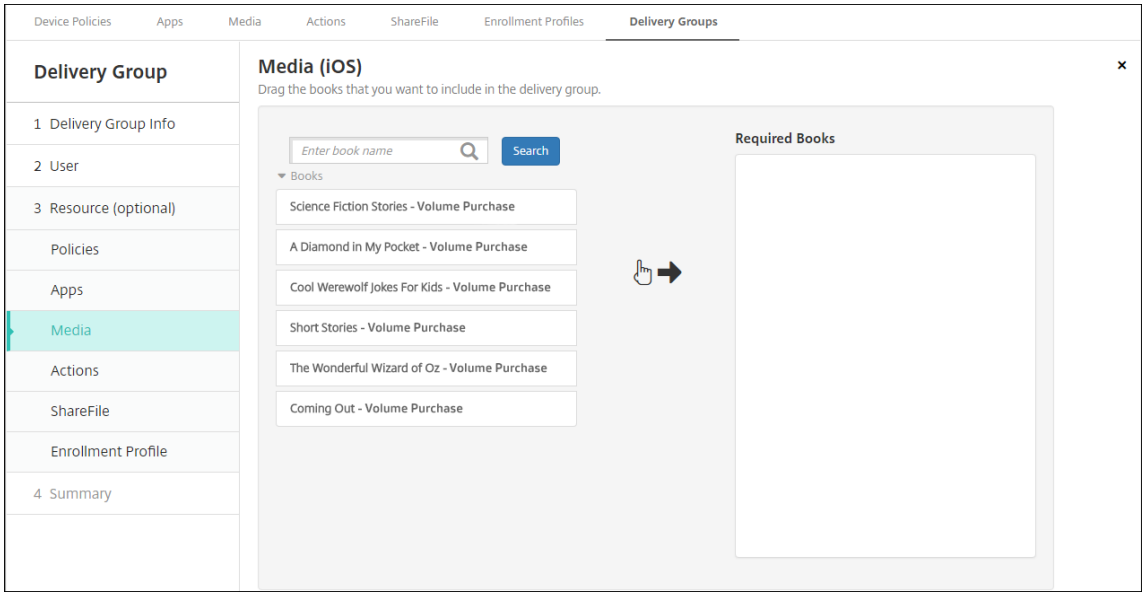
You can also specify deployment rules or view volume purchase information.



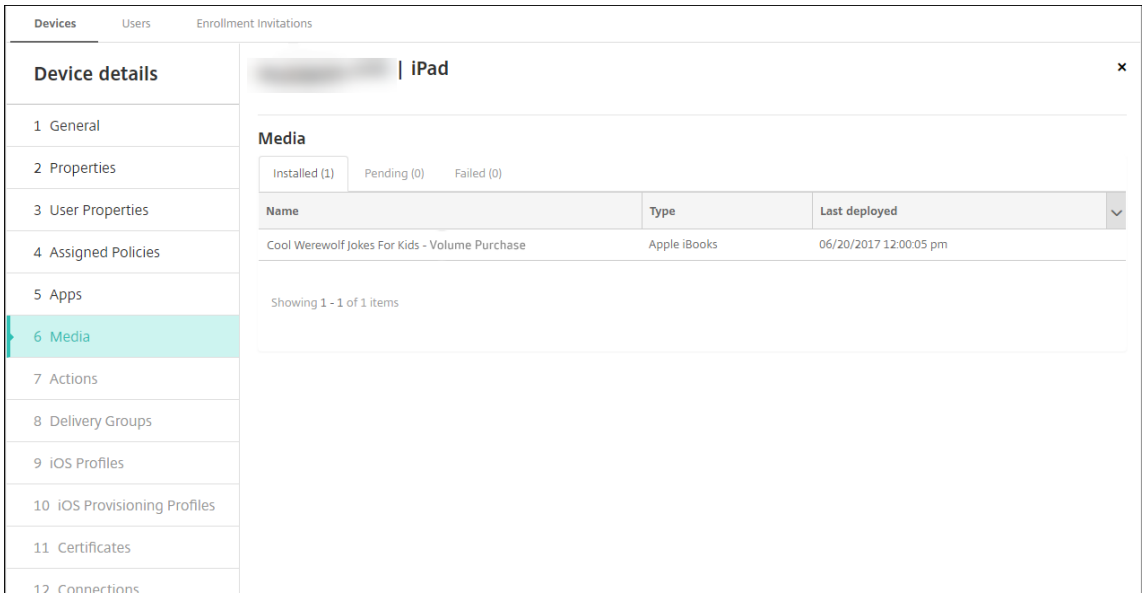
3. Optionally, assign the book to delivery groups and set a deployment schedule.



You can also assign books to delivery groups from the **Media** tab for **Configure > Delivery Groups**. XenMobile supports required book deployment only.

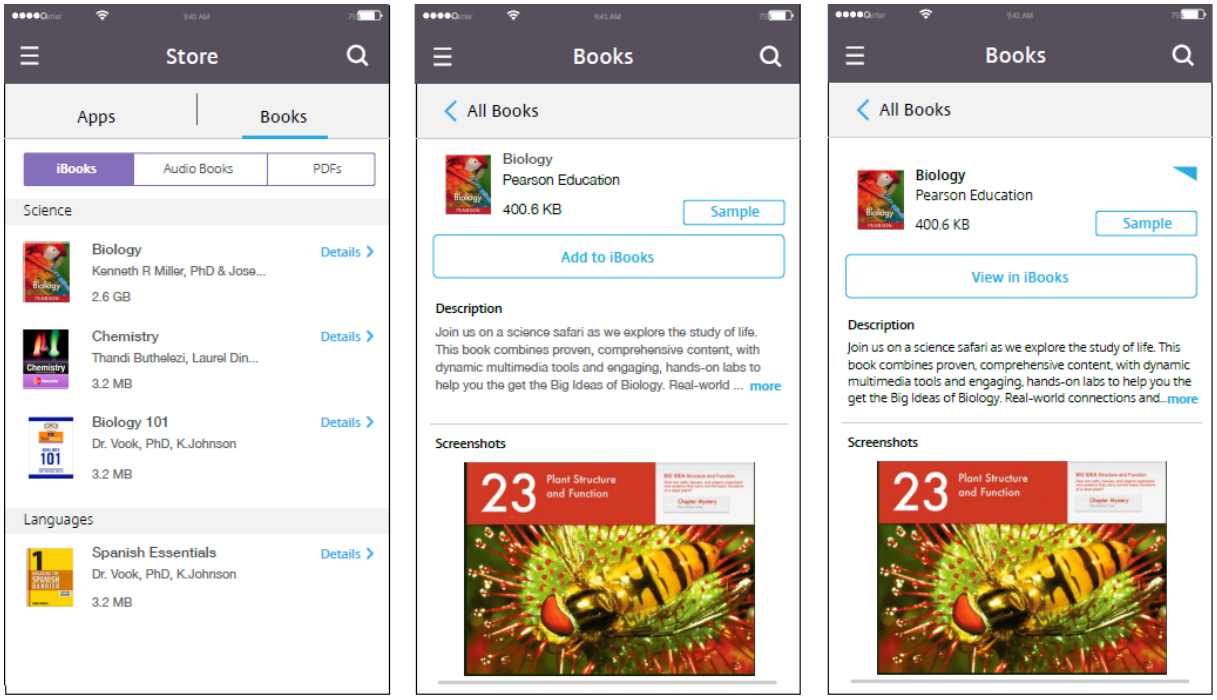


4. Use the **Media** tab for **Manage > Devices** to view deployment status.



> **Note:**
>
> On the **Configure > Media** page, if you select a book and click **Delete**, XenMobile removes the book from the list. However, the next time XenMobile 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

April 19, 2021

Device configuration and management typically involve creating resources (policies, apps, and media) and actions in the XenMobile console and then packaging them using delivery groups. The order in which XenMobile pushes resources and actions in a delivery group to devices is called the deployment order. This article describes how:

- To add, manage, and deploy delivery groups
- To change the deployment order of resources and actions in delivery groups
- XenMobile determines deployment order when a user is in multiple delivery groups that have duplicate or conflicting policies.

Delivery groups specify the category of users to whose devices you deploy combinations of policies, apps, media, and actions. 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 what resources and when they get them. You can deploy a delivery group to everyone or to a more narrowly defined group of users.

Deploying to a delivery group means sending a push notification to all users with supported iOS and Windows devices. Those users must belong to the delivery group to reconnect to XenMobile. You can reevaluate the devices and deploy policies, apps, media, and actions that are part of a delivery group.

For users with Android devices: If they are already connected, they receive the resources immediately. Otherwise, based on their scheduling policy, they receive resources the next time that they connect.

The default AllUsers delivery group is created when you install and configure XenMobile. It contains all local users and Active Directory users. You cannot delete the AllUsers group, but you can disable the group when you do not want to push resources to all users.

Deployment ordering

Deployment order is the sequence in which XenMobile pushes resources to devices. Deployment order applies only to devices in a delivery group with an enrollment profile configured for device management (MDM).

When determining deployment order, XenMobile applies filters and control criteria, such as deployment rules and deployment schedule, to resources. Resources include policies, apps, actions, and delivery groups. Before adding delivery groups, consider how the information in this section relates to your deployment goals.

Here's a summary of the main concepts related to deployment order:

- **Deployment order:** The sequence in which XenMobile pushes resources (policies. apps, and media) and actions to a device. Deployment order for some policies, such as Terms and Conditions and Software Inventory, has no effect on other resources. The order in which actions are deployed has no effect on other resources, so their position is ignored when XenMobile deploys the resources.
- **Deployment rules:** XenMobile uses the deployment rules that you specify for 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.
- **Deployment schedule:** XenMobile 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 immediately, on a particular date and time, or according to deployment conditions.

The following table shows filter and control criteria for the various object and resource types. Deployment rules are based on device properties.

Object/Resource	Device platform	Deployment rule	Deployment schedule	User/groups
Device policy	Y	Y	Y	-
App	Y	Y	Y	-
Media	Y	Y	Y	-

Object/Resource	Device platform	Deployment rule	Deployment schedule	User/groups
Action	-	Y	Y	-
Delivery group	-	Y	-	Y

It is very likely that, in a typical environment, multiple delivery groups become assigned to a single user, with the following possible results:

- Duplicate objects exist within the delivery groups.
- A specific policy is configured differently in more than one delivery group that is assigned to a user.

When either of those situations occur, XenMobile calculates a deployment order for all the objects that it must deliver to a device or act upon. The calculation steps are independent of the device platform.

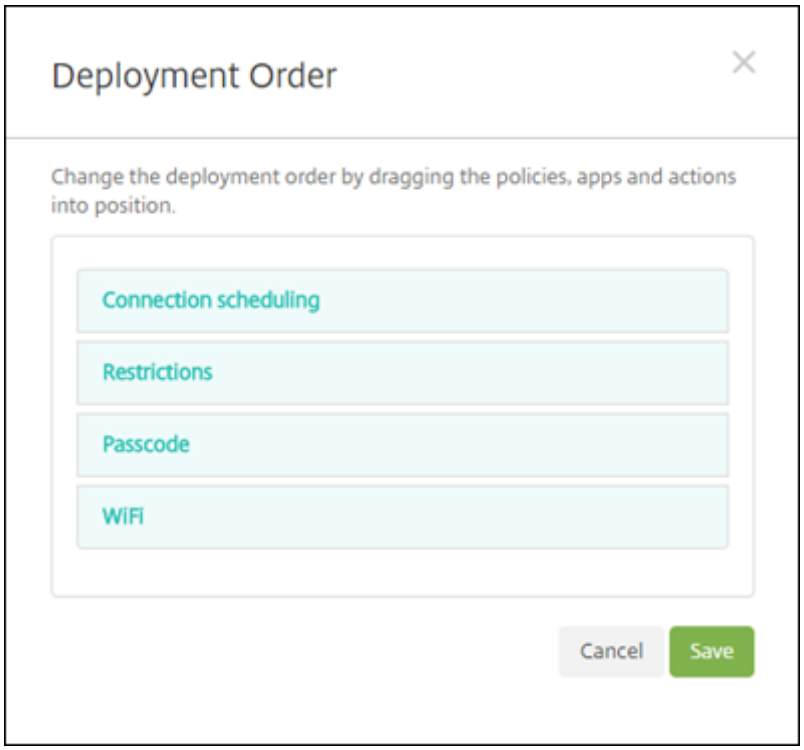
Calculation steps

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) within 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 a user-defined deployment order ahead of resources from delivery groups without one. The rationale for this placement is described after these steps.
    b) As a tie-breaker among delivery groups, order resources from delivery groups by delivery group name. For example, place resources from delivery group A ahead of resources from delivery group B.
    c) While sorting, if a user-defined deployment order is specified for the resources of a delivery group, maintain that order. Otherwise, sort the resources within that delivery group by resource name.
    d) If the same resource appears more than once, then remove the duplicate resource.

Resources that have a user-defined order associated with them deploy before resources without a user-defined order. A resource can exist in multiple delivery groups assigned to a user. As indicated in the steps above, the calculation algorithm removes redundant resources and only delivers the first resource in this list. By removing duplicate resources in that way, XenMobile enforces the order defined by the XenMobile administrator.

For example, suppose that you have two delivery groups as follows:

- Delivery group, Account Managers 1: With **unspecified** order for resources. Contains the policies **WiFi** and **Passcode**.
- Delivery group, Account Managers 2: With **specified** order for resources. Contains the policies **Connection scheduling**, **Restrictions**, **Passcode**, and **WiFi**. In this case, you want to deliver the **Passcode** policy before the **WiFi** policy.



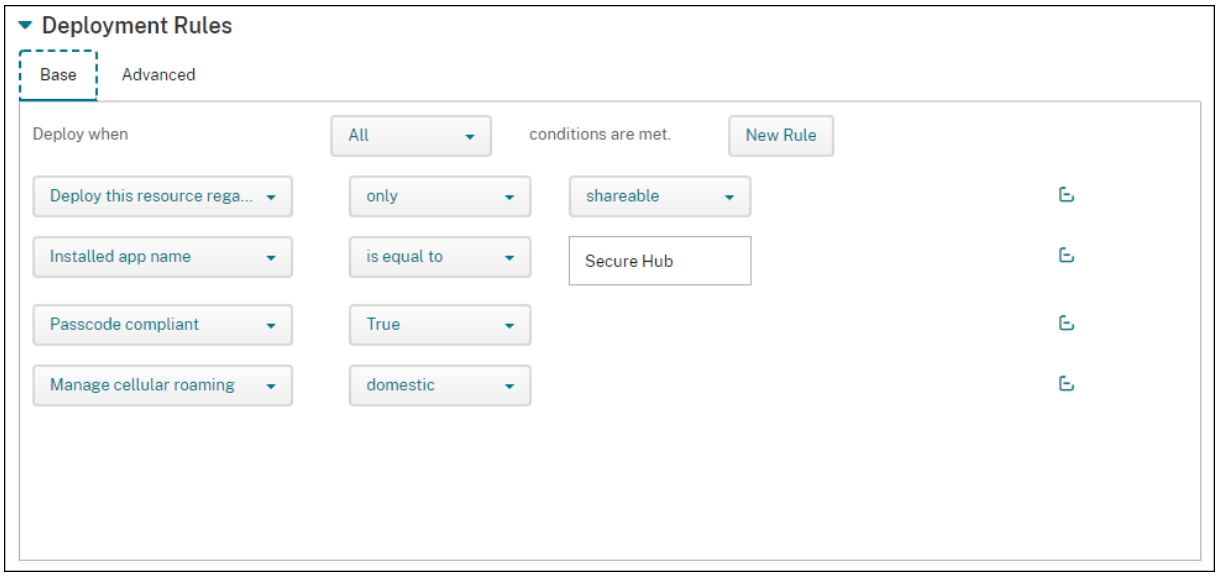
If the calculation algorithm ordered deployment groups only by name, XenMobile would perform the deployment in this order, starting with the delivery group Account Managers 1: **WiFi**, **Passcode**, **Connection scheduling**, and **Restrictions**. XenMobile would ignore **Passcode** and **WiFi**, both duplicates, from the Account Managers 2 delivery group.

However, the Account Managers 2 group has an admin-specified deployment order. Therefore, the calculation algorithm places resources from the Account Managers 2 delivery group higher in the list than the resources from the other delivery group. As a result, XenMobile deploys the policies in this order: **Connection scheduling**, **Restrictions**, **Passcode**, and **WiFi**. XenMobile ignores the policies **WiFi** and **Passcode** from the Account Managers 1 delivery group, because they are duplicates. That algorithm therefore respects the order specified by the XenMobile administrator.

Deployment rules

Configure deployment rules to deliver resources only when specific conditions exist. You can configure base or advanced deployment rules.

When adding a deployment rule using the base editor, first select when to deploy the resource.

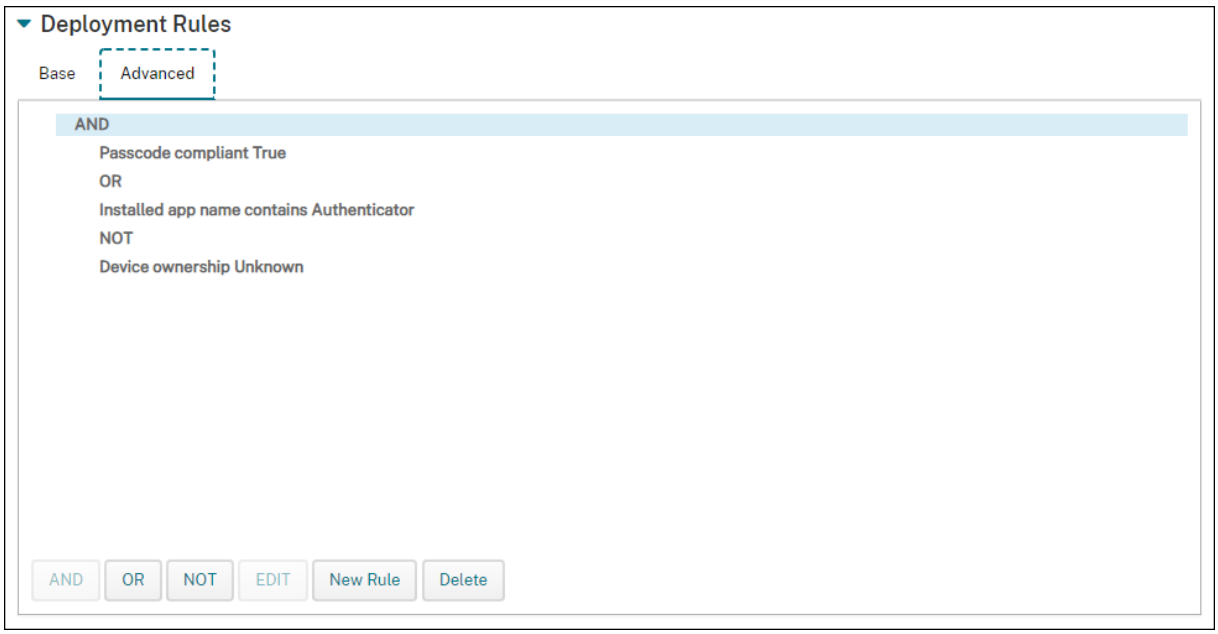


- **All:** Deliver the resource when the user or device meets all the conditions you configure.
- **Any:** Deliver the resource when the user or device meets at least one of the conditions you configure.

Click **New Rule** to add a condition. Rules vary based on the resource being deployed and the platform for which you configure the resource. Several types of rules exist. You can choose 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 the condition you select from a predefined list.

Use the advanced editor to create more complex deployment rules. More rules exist to select and you can combine different Boolean logic operators when creating an advanced rule.

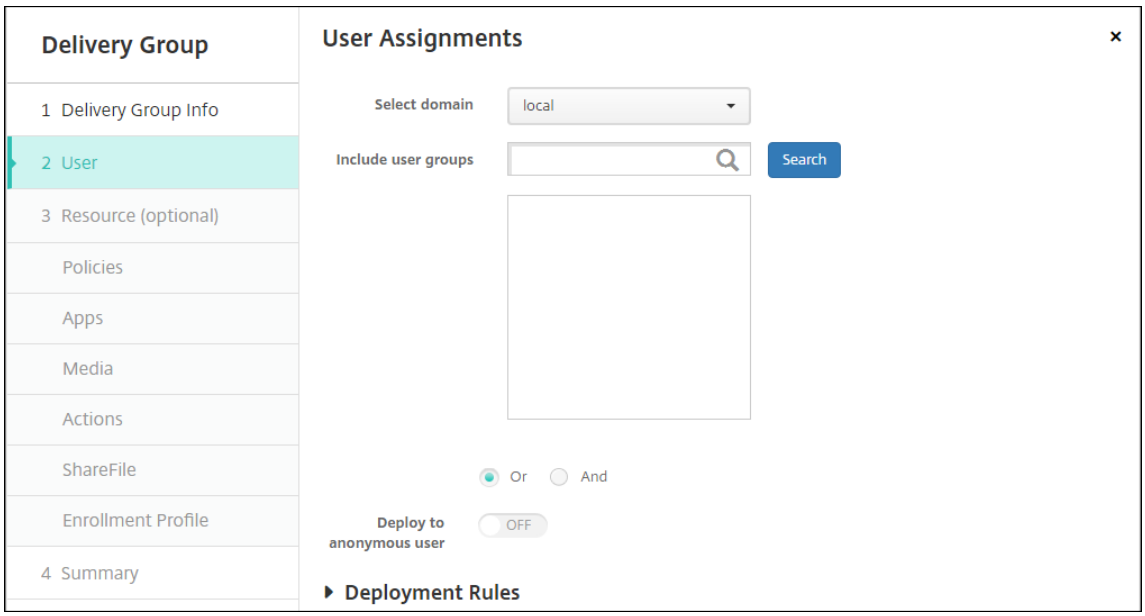


To add a delivery group

Citrix recommends creating delivery groups before you create device policies and enrollment profiles.

1. In the 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**.

   If a user belongs to multiple delivery groups that have different enrollment profiles, the name of the delivery group determines the enrollment profile used. XenMobile selects the delivery group that appears last in an alphabetized list of delivery groups. For more information, see Enrollment profiles.
4. On the **User Assignments** page, specify how to manage the delivery group user assignments.



Important:

You cannot change the **Manage user assignments** setting after the user group is created.

- **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.
- **Or/And:** Select whether users may be 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 whom you were not able to authenticate, but you allowed their devices to connect to XenMobile anyway.

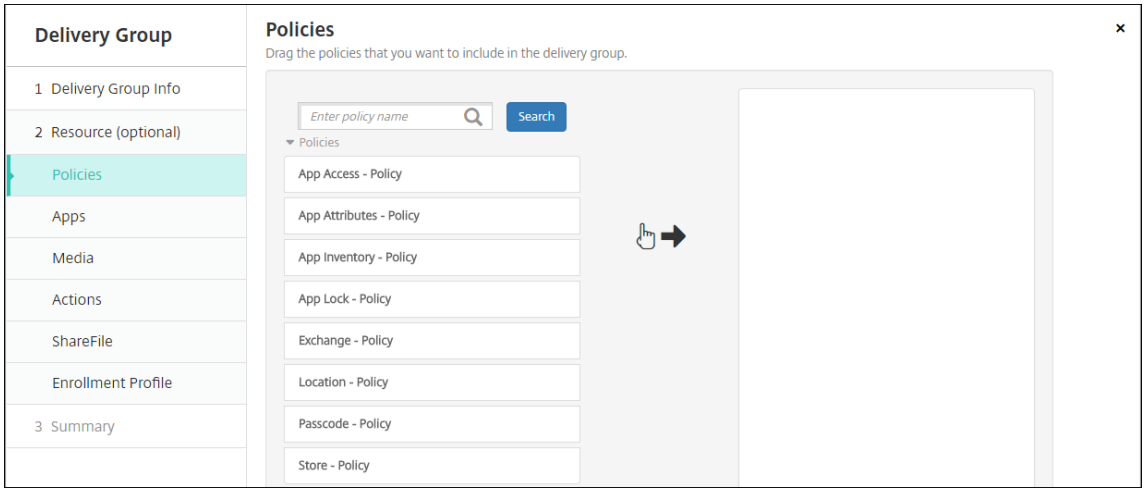
5. Configure the deployment rules.
6. Click **Next**. The **Delivery Group Resources** page appears. You optionally add policies, apps, or actions for the delivery group here. To skip this step, under **Delivery Group**, click **Summary** to see a summary the delivery group configuration.

   To skip a resource, under **Resources (optional)**, click the resource you want to add and follow the steps for that resource.

To add policies

1. 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, to limit the list of policies, type a full or partial policy name in the search box, and then click **Search**.
   - Click the policy you want to add and drag it into the box on the right.

   To remove a policy, click the **X** next to the policy name in the box on the right.



2. Click **Next**. The **Apps** page appears.

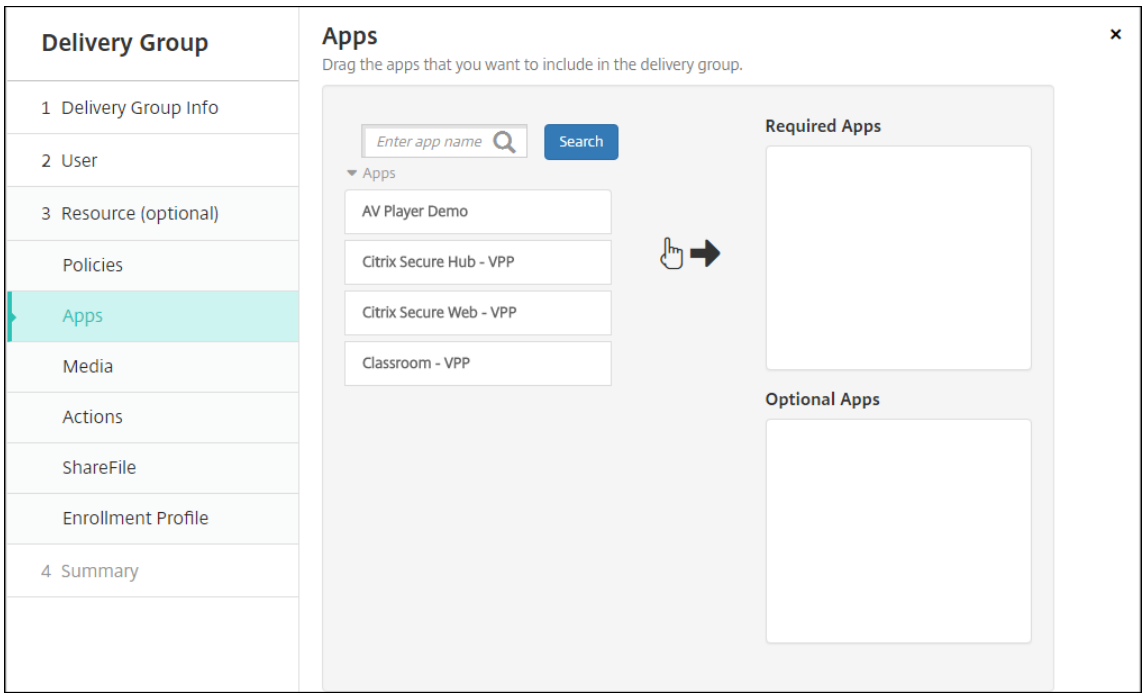
To add apps

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, to limit the list of apps, type a full or partial app name in the search box, and then click **Search**.
   - Click the app you want to add and drag it 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:

- You upload a new app and mark it as required.
- You mark an existing app as required.
- As 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.

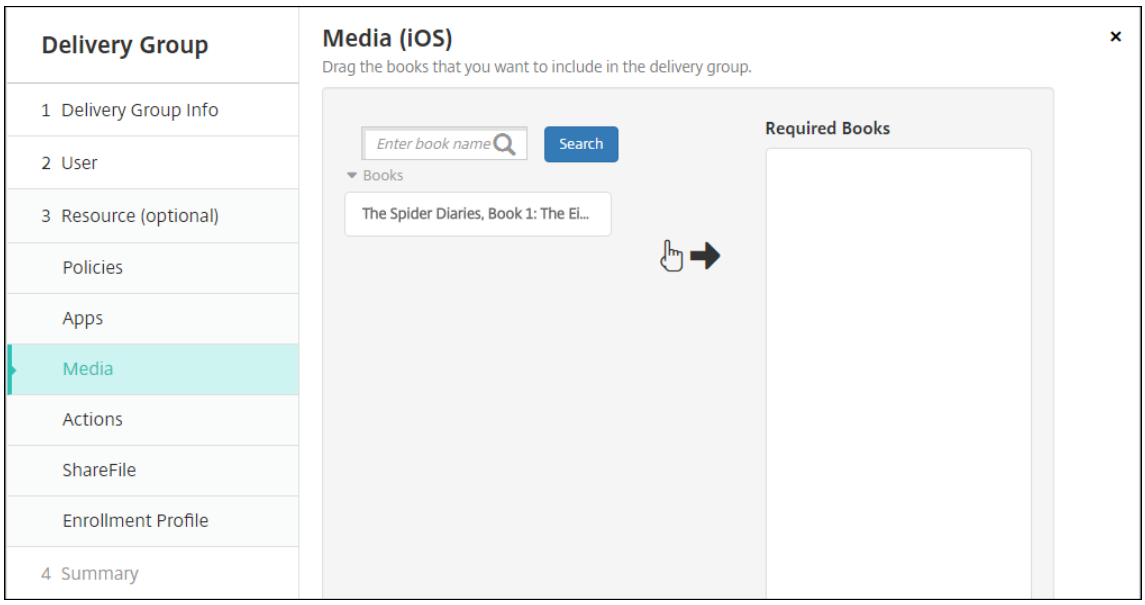


To remove an app, click the **X** next to the app name in the box on the right.

2. Click **Next**. The **Media** page appears.

To add media

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, to limit the list of books, type a full or partial book name in the search box, and then click **Search**.
   - Click the book you want to add and drag it into the **Required Books** box.



For books marked as required, users promptly receive updates in situations such as:

- You upload a new book and mark it as required.
- You mark an existing book as required.
- As user deletes a required book.
- A Secure Hub update is available.

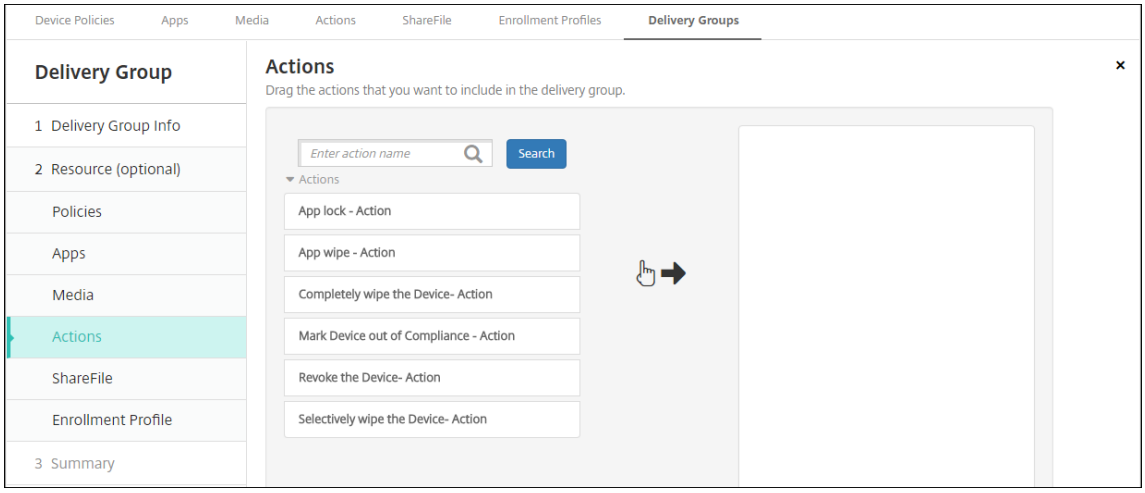
To remove a book, click the **X** next to the book name in the box on the right.

2. Click **Next**. The **Actions** page appears.

To add actions

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, to limit the list of actions, type a full or partial action name in the search box, and then click **Search**.
   - Click the action you want to add and drag it into the box on the right.

   To remove an action, click the **X** next to the action name in the box on the right.

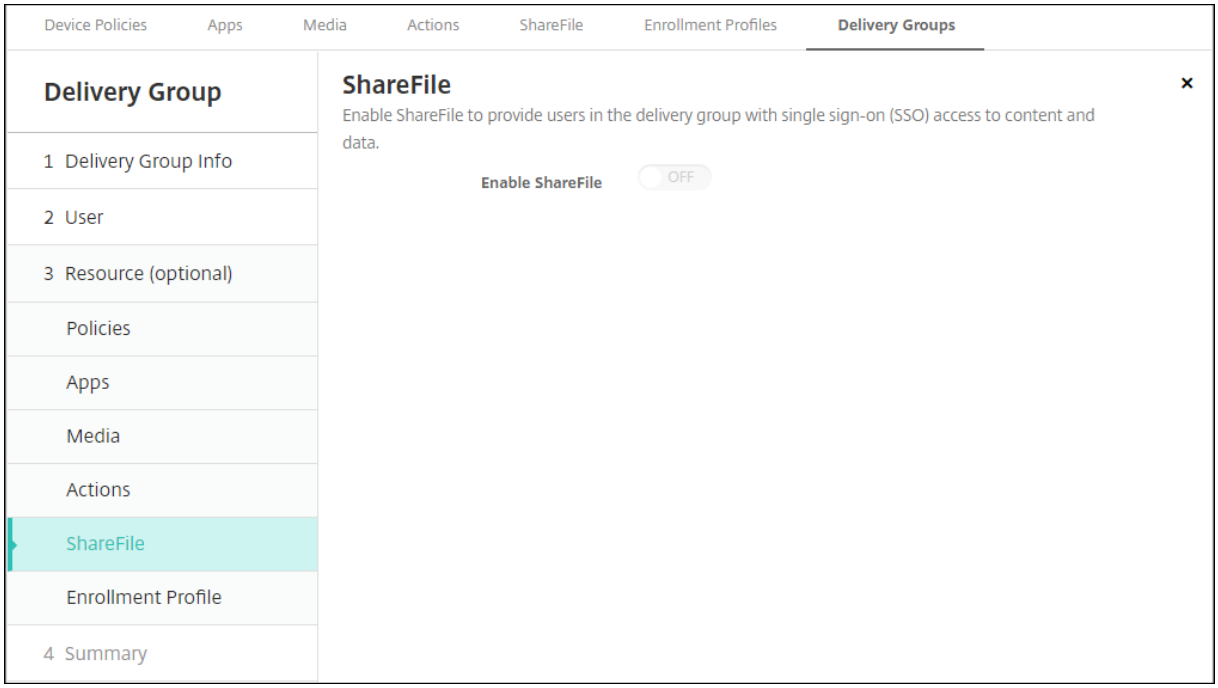


2. Click **Next**. The **ShareFile** page appears.

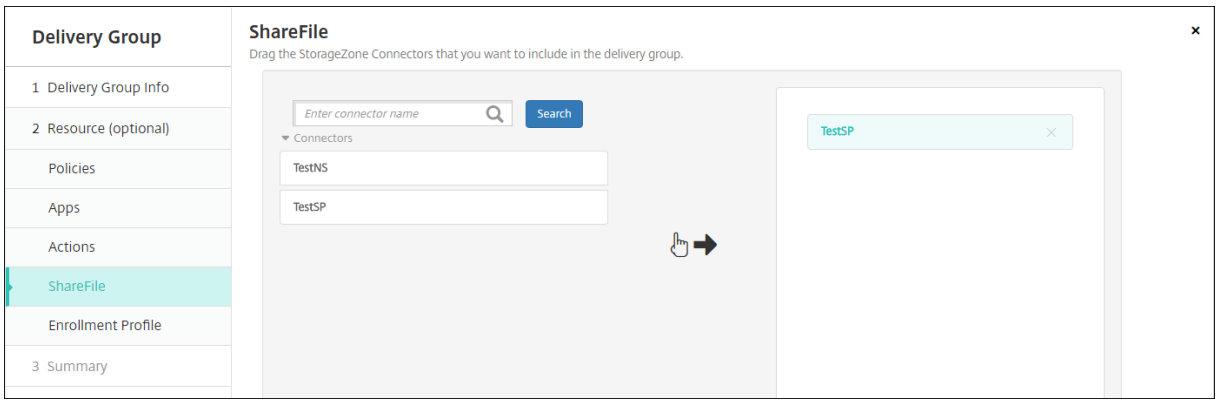
To apply the Content Collaboration configuration

The Content Collaboration page differs depending on whether you configured XenMobile (**Configure > ShareFile**) for Enterprise accounts or for storage zone connectors.

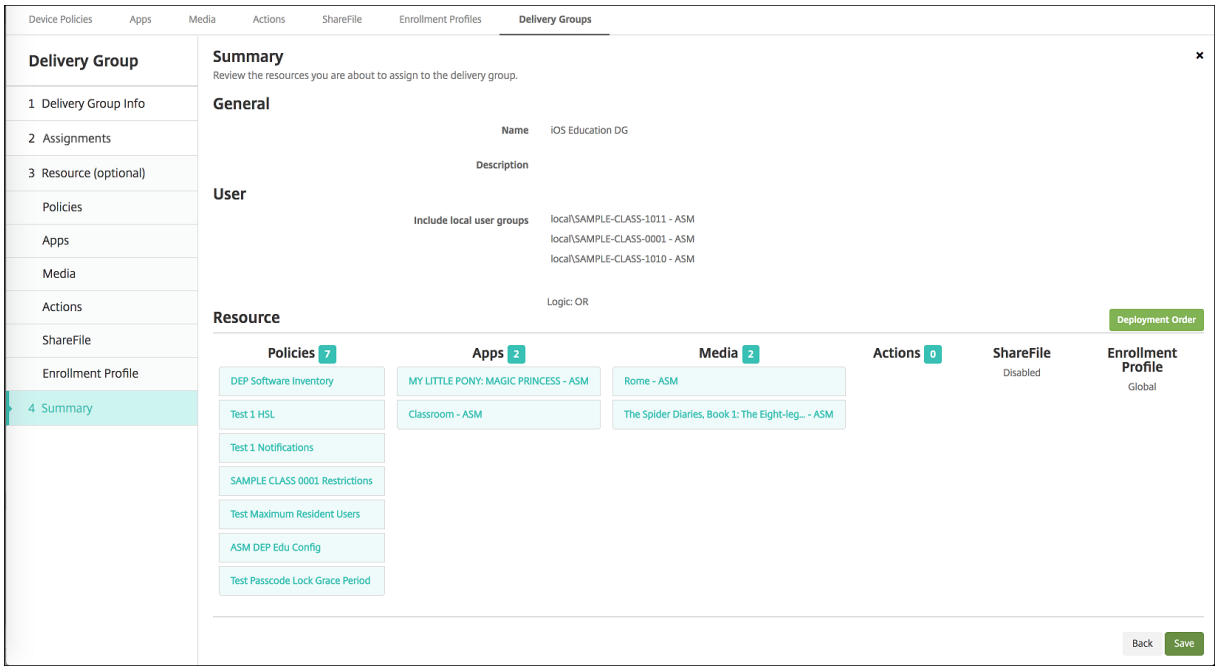
If you configured Enterprise accounts for use with XenMobile: Set **Enable ShareFile** to **ON** to provide the delivery group single sign-on access to Content Collaboration content and data.



If you configured storage zone connectors for use with XenMobile, select the storage zone connectors to include in the delivery group.

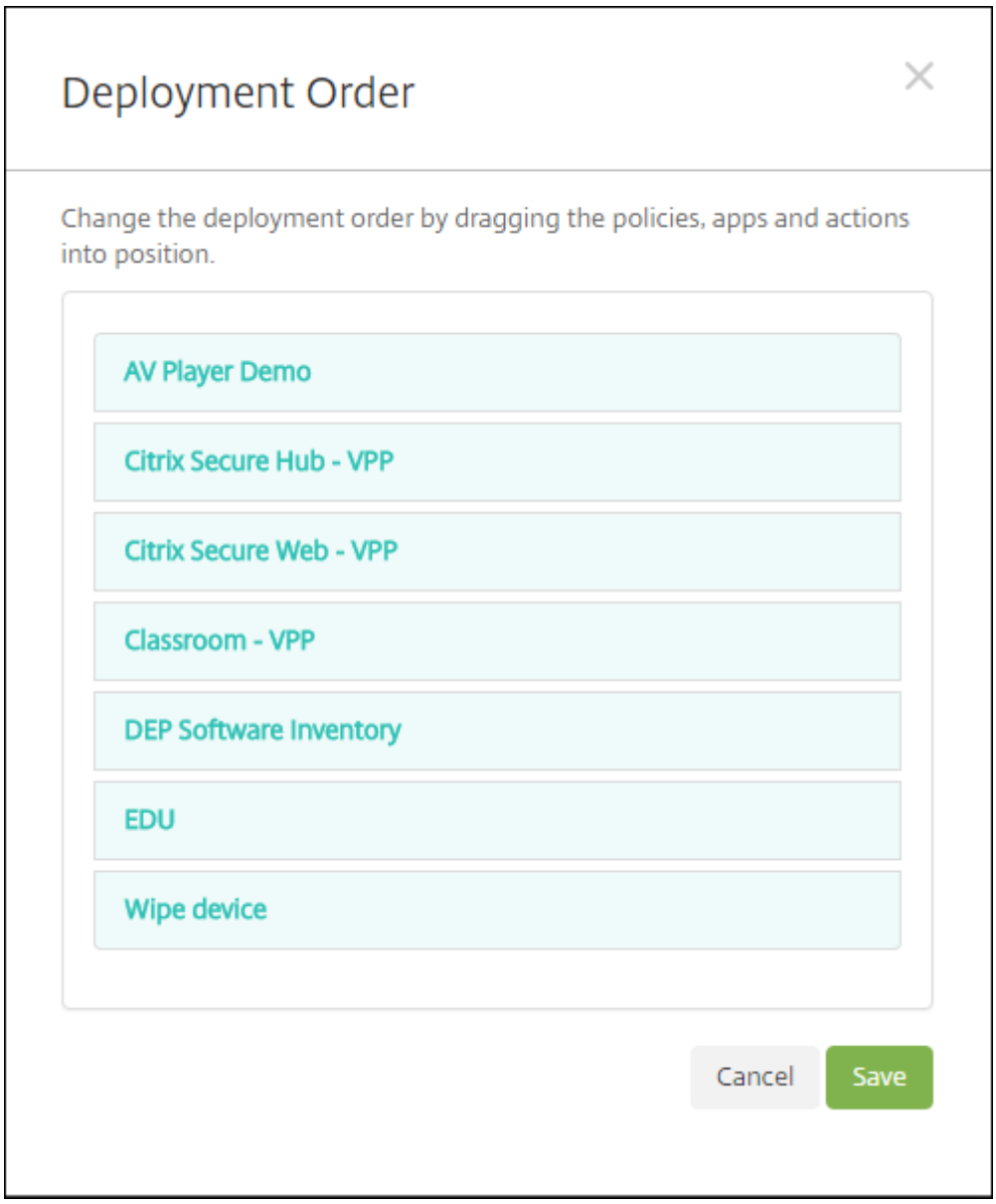


To review configured options and change deployment order



On the **Summary** page, you can review the options you have 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 reflect the deployment order.

1. Click **Back** to return to previous pages to make any necessary adjustments to the configuration.
2. Click **Deployment Order** to view the deployment order or to reorder the deployment order. The **Deployment Order** dialog box appears.



3. Click a resource and drag it to the location from which you want it deployed. After you change the deployment order, XenMobile deploys resources in the list from top to bottom.
4. Click **Save** to save the deployment order.
5. Click **Save** to save the delivery group.

To 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**.

To enable and disable the AllUsers delivery group

AllUsers is the only delivery group that you can enable or disable.

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 only available if AllUsers 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 only available if AllUsers is disabled. **Disabled** disappears from under the **Disabled** heading in the delivery group table.

To deploy to delivery groups

Deploying to a delivery group means sending a push notification to all users with iOS, Windows Phone, and Windows tablet devices. Those users must belong to the delivery group to reconnect to XenMobile. In that way, you can reevaluate the devices and deploy apps, policies, and actions.

For users with other platform devices: If those devices are already connected to XenMobile, 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 XenMobile Store on Android devices: First deploy an App Inventory policy to the user devices.

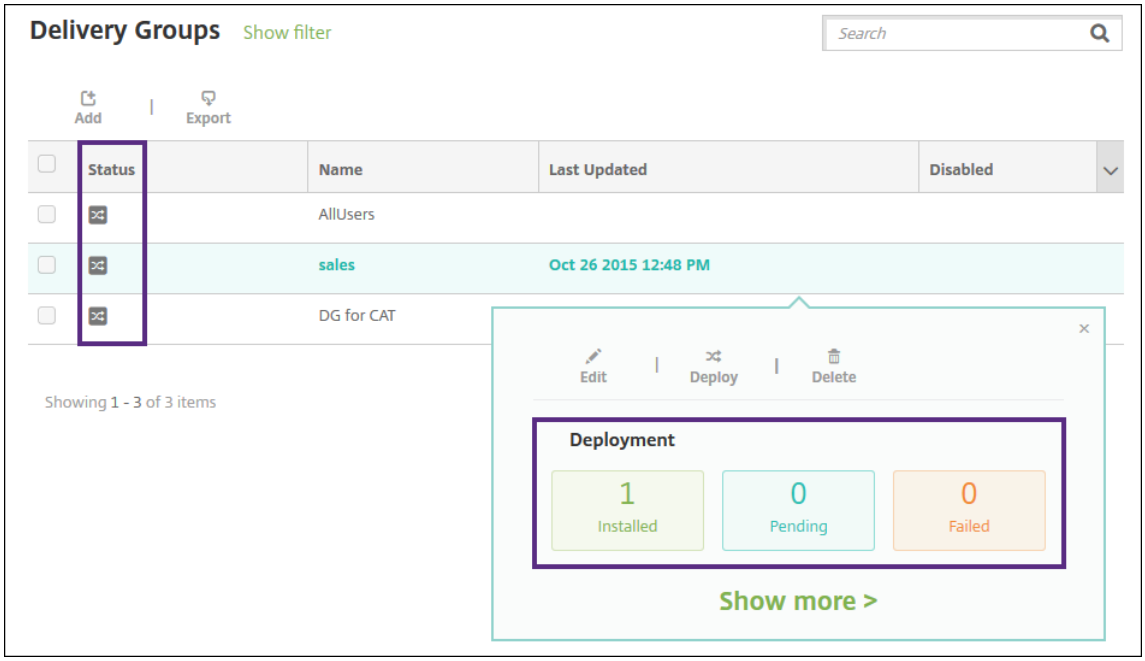
1. On the **Delivery Groups** page, do one of the following:
   - To deploy to more than one delivery group at a time, select the check boxes next to the groups you want to deploy.
   - To deploy to a single delivery group, either select the check box next to its name or click the line containing its 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 to which you want to deploy apps, policies, and actions are listed and 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 indicates **Installed**, **Pending**, and **Failed** deployments.



To delete delivery groups

You cannot delete the AllUsers delivery group, but you can disable the group when you do not want to push resources to all users.

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**. The **Delete** dialog box appears.

   Depending on how you select a single delivery group, the **Delete** command appears above or to the right of the delivery group.

   > **Important:**
   >
   > You cannot undo a delete.

3. Click **Delete**.

To export the Delivery Groups table

1. Click the **Export** button above the **Delivery Groups** table. XenMobile 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. You can also cancel the operation.

Macros

March 30, 2021

XenMobile provides macros as a way to populate user or device property data within the text field of the following items:

- Policies
- Notifications
- Enrollment templates
- Automated actions
- Credential provider Certificate Signing Requests

XenMobile 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)] }`

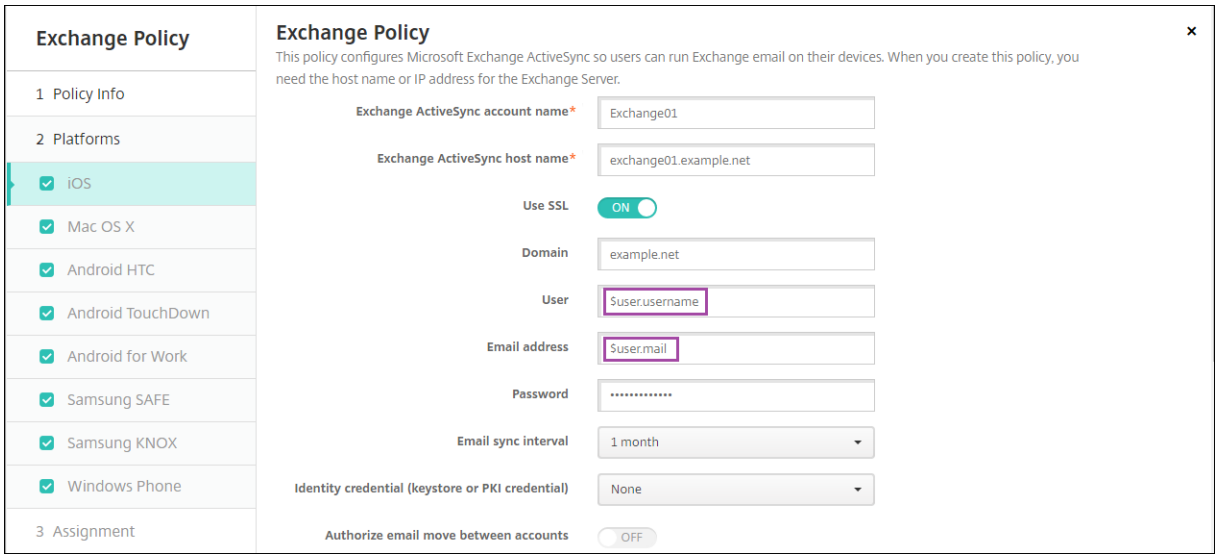
Enclose all syntax following the dollar sign ($) in curly brackets ({ }).

- 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. The following macro for a notification message includes the function **firstnotnull**.

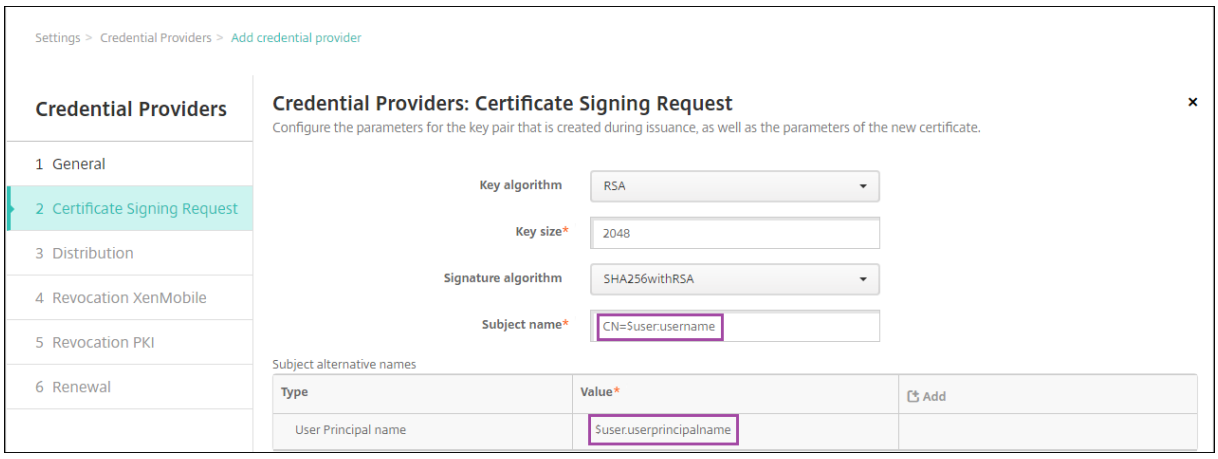
  Device `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` has been blocked…

- 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 }`**.



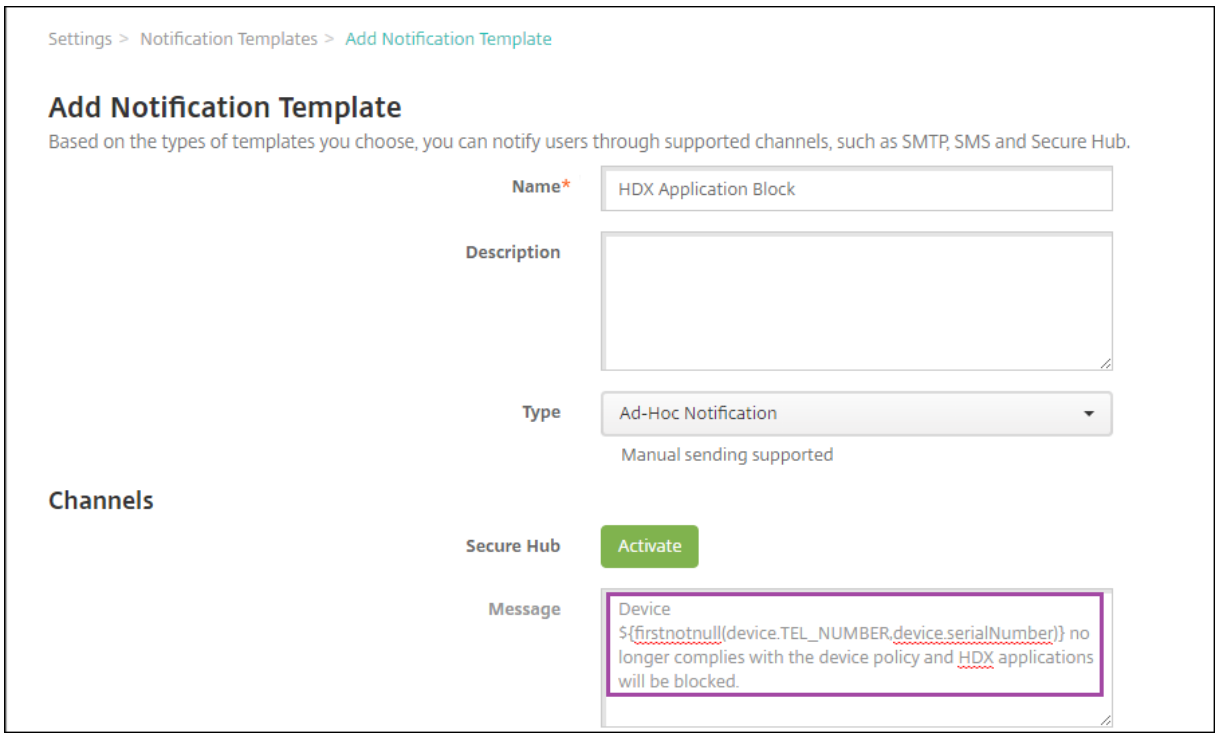
The following example shows how to use macros for a certificate signing request. The macro for **Subject name** is **`CN=$user.username`**. The macro for the **Value** of a **Subject alternative name** is **`$user.userprincipalname`**.



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:

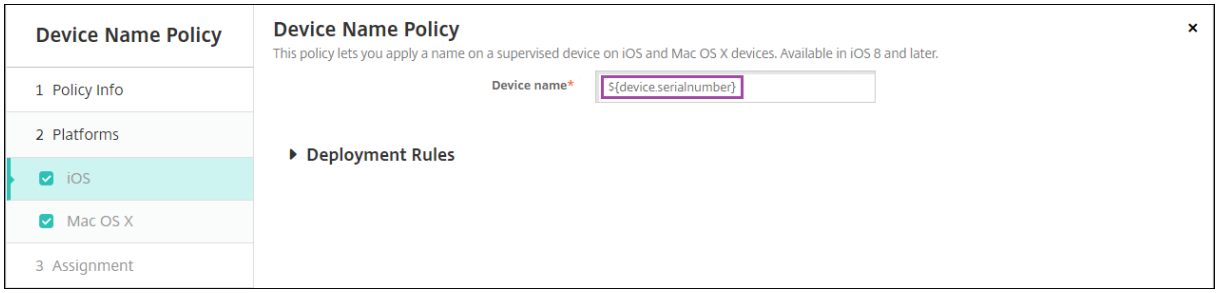
Device `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` no longer complies

with the device policy and HDX applications will be blocked.



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.



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)}

  > **Note:**
  >
  > The XenMobile Server console includes the terms “blacklist” and “whitelist”. We are changing those terms in an upcoming release to “block list” and “allow list”.

- ${ vpp.account }
- ${ vpp.appname }
- ${ vpp.url }
- ${ zdmserver.hostPath } /enroll

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 Webclip device policy, you can use this macro for the **URL**:

- `${ webeas-url }`

For the Samsung MDM License Key device policy, you can use this macro for the **ELM license key**:

- `${ elm.license.key }`

Macros to obtain built-in device properties

Display name	Macros
Device ID	`$device.id`
Device GUID	`$device.uniqueid`
Device IMEI	`$device.imei`
OS Family	`$device.OSFamily`
Serial Number	`$device.serialNumber`

Macros for all device properties

The following list gives the display name, the Web element, and the Macros.

Account Suspended?

- GOOGLE_AW_DIRECTORY_SUSPENDED
- ${device.GOOGLE_AW_DIRECTORY_SUSPENDED

Activation lock bypass code

- ACTIVATION_LOCK_BYPASS_CODE
- ${device.ACTIVATION_LOCK_BYPASS_CODE

Activation lock enabled

- ACTIVATION_LOCK_ENABLED
- ${device.ACTIVATION_LOCK_ENABLED

Active iTunes account

- ACTIVE_ITUNES
- ${device.ACTIVE_ITUNES}

ActiveSync device known by MSP

- AS_DEVICE_KNOWN_BY_ZMSP
- ${device.AS_DEVICE_KNOWN_BY_ZMSP

ActiveSync ID

- EXCHANGE_ACTIVESYNC_ID
- ${device.EXCHANGE_ACTIVESYNC_ID

Administrator disabled

- ADMIN_DISABLED
- ${device.ADMIN_DISABLED

AIK Present?

- WINDOWS_HAS_AIK_PRESENT
- ${device.WINDOWS_HAS_AIK_PRESENT

Amazon MDM API available

- AMAZON_MDM
- ${device.AMAZON_MDM

Android Enterprise Device ID

- GOOGLE_AW_DEVICE_ID
- ${device.GOOGLE_AW_DEVICE_ID

Android Enterprise Enabled Device?

- GOOGLE_AW_ENABLED_DEVICE
- ${device.GOOGLE_AW_ENABLED_DEVICE

Android Enterprise Install Type

- GOOGLE_AW_INSTALL_TYPE
- ${device.GOOGLE_AW_INSTALL_TYPE

Antispyware Signature status

- ANTI_SPYWARE_SIGNATURE_STATUS
- ${device.ANTI_SPYWARE_SIGNATURE_STATUS

Antispyware Status

- ANTI_SPYWARE_STATUS
- ${device.ANTI_SPYWARE_STATUS

Antivirus Signature Status

- ANTI_VIRUS_SIGNATURE_STATUS
- ${device.ANTI_VIRUS_SIGNATURE_STATUS

Antivirus Status

- ANTI_VIRUS_STATUS
- ${device.ANTI_VIRUS_STATUS

ASM DEP activation lock bypass code

- DEP_ACTIVATION_LOCK_BYPASS_CODE
- ${device.DEP_ACTIVATION_LOCK_BYPASS_CODE

ASM DEP escrow key

- DEP_ESCROW_KEY
- ${device.DEP_ESCROW_KEY

Asset tag

- ASSET_TAG
- ${device.ASSET_TAG

Automatically check software updates

- AutoCheckEnabled
- ${device.AutoCheckEnabled

Automatically download software updates in the background

- BackgroundDownloadEnabled
- ${device.BackgroundDownloadEnabled

Automatically install app updates

- AutomaticAppInstallationEnabled
- ${device.AutomaticAppInstallationEnabled

Automatically install OS updates

- AutomaticOSInstallationEnabled
- ${device.AutomaticOSInstallationEnabled

Automatically install security updates

- AutomaticSecurityUpdatesEnabled
- ${device.AutomaticSecurityUpdatesEnabled

Autoupdate Status

- AUTOUPDATE_STATUS
- ${device.AUTOUPDATE_STATUS

Available RAM

- MEMORY_AVAILABLE

- ${device.MEMORY_AVAILABLE

Available software updates

- AVAILABLE_OS_UPDATE_HUMAN_READABLE
- ${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE

Available storage space

- FREEDISK
- ${device.FREEDISK

Backup battery

- BACKUP_BATTERY_PERCENT
- ${device.BACKUP_BATTERY_PERCENT

Baseband firmware version

- MODEM_FIRMWARE_VERSION
- ${device.MODEM_FIRMWARE_VERSION

Battery Charging

- BATTERY_CHARGING_STATUS
- ${device.BATTERY_CHARGING_STATUS

Battery charging

- BATTERY_CHARGING
- ${device.BATTERY_CHARGING

Battery Remaining

- BATTERY_ESTIMATED_CHARGE_REMAINING
- ${device.BATTERY_ESTIMATED_CHARGE_REMAINING

Battery Runtime

- BATTERY_RUNTIME
- ${device.BATTERY_RUNTIME

Battery Status

- BATTERY_STATUS
- ${device.BATTERY_STATUS

Bes device known by MS

- BES_DEVICE_KNOWN_BY_ZMSP
- ${device.BES_DEVICE_KNOWN_BY_ZMSP

BES PIN

- BES_PIN
- ${device.BES_PIN

BES server agent ID

- AGENT_ID
- ${device.AGENT_ID

BES server name

- BES_SERVER
- ${device.BES_SERVER

BES server version

- BES_VERSION
- ${device.BES_VERSION

BIOS Info

- BIOS_INFO
- ${device.BIOS_INFO

BitLocker Status

- WINDOWS_HAS_BIT_LOCKER_STATUS
- ${device.WINDOWS_HAS_BIT_LOCKER_STATUS

Bluetooth MAC address

- BLUETOOTH_MAC
- ${device.BLUETOOTH_MAC

Boot Debugging Enabled?

- WINDOWS_HAS_BOOT_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED

Boot Manager Rev List Version

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- ${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION

Carrier Code

- CARRIER_CODE
- ${device.CARRIER_CODE

Carrier settings version

- CARRIER_SETTINGS_VERSION
- ${device.CARRIER_SETTINGS_VERSION

Catalog URL

- CatalogURL
- ${device.CatalogURL

Cellular altitude

- GPS_ALTITUDE_FROM_CELLULAR
- ${device.GPS_ALTITUDE_FROM_CELLULAR

Cellular course

- GPS_COURSE_FROM_CELLULAR
- ${device.GPS_COURSE_FROM_CELLULAR

Cellular horizontal accuracy

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR

Cellular latitude

- GPS_LATITUDE_FROM_CELLULAR
- ${device.GPS_LATITUDE_FROM_CELLULAR

Cellular longitude

- GPS_LONGITUDE_FROM_CELLULAR
- ${device.GPS_LONGITUDE_FROM_CELLULAR

Cellular speed

- GPS_SPEED_FROM_CELLULAR
- ${device.GPS_SPEED_FROM_CELLULAR

Cellular technology

- CELLULAR_TECHNOLOGY
- ${device.CELLULAR_TECHNOLOGY

Cellular timestamp

- GPS_TIMESTAMP_FROM_CELLULAR
- ${device.GPS_TIMESTAMP_FROM_CELLULAR

Cellular vertical accuracy

- GPS_VERTICAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}

Change Password at Next Login?

- GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN

- ${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

Client device ID

- CLIENT_DEVICE_ID
- ${device.CLIENT_DEVICE_ID

Cloud backup enabled

- CLOUD_BACKUP_ENABLED
- ${device.CLOUD_BACKUP_ENABLED

Code Integrity Enabled?

- WINDOWS_HAS_CODE_INTEGRITY_ENABLED
- ${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED

Code Integrity Rev List Version

- INDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION
- ${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION

Color

- COLOR
- ${device.COLOR

CPU clock speed

- CPU_CLOCK_SPEED
- ${device.CPU_CLOCK_SPEED

CPU type

- CPU_TYPE
- ${device.CPU_TYPE}

Creation Time

- GOOGLE_AW_DIRECTORY_CREATION_TIME
- ${device.GOOGLE_AW_DIRECTORY_CREATION_TIME

Critical software updates

- AVAILABLE_OS_UPDATE_IS_CRITICAL
- ${device.AVAILABLE_OS_UPDATE_IS_CRITICAL

Current carrier network

- CARRIER
- ${device.CARRIER

Current mobile country code

- CURRENT_MCC
- ${device.CURRENT_MCC

Current mobile network code

- CURRENT_MNC
- ${device.CURRENT_MNC

Data roaming allowed

- DATA_ROAMING_ENABLED
- ${device.DATA_ROAMING_ENABLED

Date of the last iCloud backup

- LAST_CLOUD_BACKUP_DATE
- ${device.LAST_CLOUD_BACKUP_DATE}

Default catalog

- IsDefaultCatalog
- ${device.IsDefaultCatalog

DEP account name

- BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- ${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME

DEP Policy

- WINDOWS_HAS_DEP_POLICY
- ${device.WINDOWS_HAS_DEP_POLICY

DEP profile assigned

- PROFILE_ASSIGN_TIME
- ${device.PROFILE_ASSIGN_TIME

DEP profile pushed

- PROFILE_PUSH_TIME
- ${device.PROFILE_PUSH_TIME

DEP profile removed

- PROFILE_REMOVE_TIME
- ${device.PROFILE_REMOVE_TIME

DEP registration by

- DEVICE_ASSIGNED_BY
- ${device.DEVICE_ASSIGNED_BY

DEP registration date

- DEVICE_ASSIGNED_DATE
- ${device.DEVICE_ASSIGNED_DATE

Description

- DESCRIPTION
- ${device.DESCRIPTION

Device identifier

- Activesyncid
- ${device.activesyncid

Device model

- SYSTEM_OEM
- ${device.SYSTEM_OEM

Device name

- DEVICE_NAME
- ${device.DEVICE_NAME

Device Type

- DEVICE_TYPE
- ${device.DEVICE_TYPE

Do Not Disturb activated

- DO_NOT_DISTURB
- ${device.DO_NOT_DISTURB

ELAM Driver Loaded?

- WINDOWS_HAS_ELAM_DRIVER_LOADED
- ${device.WINDOWS_HAS_ELAM_DRIVER_LOADED

Encryption Compliance

- ENCRYPTION_COMPLIANCE
- ${device.ENCRYPTION_COMPLIANCE

ENROLLMENT_KEY_GENERATION_DATE

- ENROLLMENT_KEY_GENERATION_DATE
- ${device.ENROLLMENT_KEY_GENERATION_DATE

Enterprise ID

- ENTERPRISEID

- ${device.ENTERPRISEID

External storage 1: available space

- EXTERNAL_STORAGE1_FREE_SPACE
- ${device.EXTERNAL_STORAGE1_FREE_SPACE

External storage 1: name

- EXTERNAL_STORAGE1_NAME
- ${device.EXTERNAL_STORAGE1_NAME

External storage 1: total space

- EXTERNAL_STORAGE1_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE1_TOTAL_SPACE

External storage 2: available space

- EXTERNAL_STORAGE2_FREE_SPACE
- ${device.EXTERNAL_STORAGE2_FREE_SPACE

External storage 2: name

- EXTERNAL_STORAGE2_NAME
- ${device.EXTERNAL_STORAGE2_NAME

External storage 2: total space

- EXTERNAL_STORAGE2_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE2_TOTAL_SPACE

External storage encrypted

- EXTERNAL_ENCRYPTION
- ${device.EXTERNAL_ENCRYPTION

FileVault Enabled

- IS_FILEVAULT_ENABLED
- ${device.IS_FILEVAULT_ENABLED

Firewall Status

- DEVICE_FIREWALL_STATUS
- ${device.DEVICE_FIREWALL_STATUS

Firewall Status

- FIREWALL_STATUS
- ${device.FIREWALL_STATUS

Firmware version

- FIRMWARE_VERSION
- ${device.FIRMWARE_VERSION

First synchronization

- ZMSP_FIRST_SYNC
- ${device.ZMSP_FIRST_SYNC

Google Directory Alias

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- ${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS

Google Directory Family Name

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- ${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME

Google Directory Name

- GOOGLE_AW_DIRECTORY_NAME
- ${device.GOOGLE_AW_DIRECTORY_NAME}

Google Directory Primary Email

- GOOGLE_AW_DIRECTORY_PRIMARY
- ${device.GOOGLE_AW_DIRECTORY_PRIMARY}

Google Directory User ID

- GOOGLE_AW_DIRECTORY_USER_ID
- ${device.GOOGLE_AW_DIRECTORY_USER_ID}

GPS altitude

- GPS_ALTITUDE_FROM_GPS
- ${device.GPS_ALTITUDE_FROM_GPS

GPS course

- GPS_COURSE_FROM_GPS
- ${device.GPS_COURSE_FROM_GPS

GPS horizontal accuracy

- GPS_HORIZONTAL_ACCURACY_FROM_GPS
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS

GPS latitude

- GPS_LATITUDE_FROM_GPS
- ${device.GPS_LATITUDE_FROM_GPS

GPS longitude

- GPS_LONGITUDE_FROM_GPS
- ${device.GPS_LONGITUDE_FROM_GPS

GPS speed

- GPS_SPEED_FROM_GPS
- ${device.GPS_SPEED_FROM_GPS

GPS timestamp

- GPS_TIMESTAMP_FROM_GPS
- ${device.GPS_TIMESTAMP_FROM_GPS

GPS vertical accuracy

- GPS_VERTICAL_ACCURACY_FROM_GPS
- ${device.GPS_VERTICAL_ACCURACY_FROM_GPS

Hardware Device ID

- HW_DEVICE_ID
- ${device.HW_DEVICE_ID

Hardware encryption capabilities

- HARDWARE_ENCRYPTION_CAPS
- ${device.HARDWARE_ENCRYPTION_CAPS

HAS_CONTAINER

- HAS_CONTAINER
- ${device.HAS_CONTAINER

Hash of the iTunes store account currently logged on

- ITUNES_STORE_ACCOUNT_HASH
- ${device.ITUNES_STORE_ACCOUNT_HASH

Home carrier network

- SIM_CARRIER_NETWORK
- ${device.SIM_CARRIER_NETWORK

Home mobile country code

- SIM_MCC
- ${device.SIM_MCC

Home mobile network code

- SIM_MNC

- ${device.SIM_MNC

ICCID

- ICCID
- ${device.ICCID

Identit

- AS_DEVICE_IDENTITY
- ${device.AS_DEVICE_IDENTITY

IMEI/MEID number

- IMEI
- ${device.IMEI

IMSI

- SIM_ID
- ${device.SIM_ID

Internal storage encrypted

- LOCAL_ENCRYPTION
- ${device.LOCAL_ENCRYPTION

IP location

- IP_LOCATION
- ${device.IP_LOCATION

IPV4 Address

- IP_ADDRESSV4
- ${device.IP_ADDRESSV4

IPV6 Address

- IP_ADDRESSV6
- ${device.IP_ADDRESSV6

Issued At

- WINDOWS_HAS_ISSUED_AT
- ${device.WINDOWS_HAS_ISSUED_AT

Jailbroken/Rooted

- ROOT_ACCESS
- ${device.ROOT_ACCESS

Kernel Debugging Enabled?

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED

Kiosk mode

- IS_KIOSK
- ${device.IS_KIOSK

Last known IP address

- LAST_IP_ADDR
- ${device.LAST_IP_ADDR

Last policy update time

- LAST_POLICY_UPDATE_TIME
- ${device.LAST_POLICY_UPDATE_TIME

Last scan date

- PreviousScanDate
- ${device.PreviousScanDate

Last scan result

- PreviousScanResult
- ${device.PreviousScanResult

Last scheduled software updates

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- ${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME

Last scheduled software updates failure message

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- ${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG

Last scheduled software updates status

- AVAILABLE_OS_UPDATE_INSTALL_STATUS
- ${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS

Last synchronization

- ZMSP_LAST_SYNC
- ${device.ZMSP_LAST_SYNC

Locator service enabled

- DEVICE_LOCATOR
- ${device.DEVICE_LOCATOR

MAC Address

- MAC_ADDRESS
- ${device.MAC_ADDRESS

MAC Address Network Connection

- MAC_NETWORK_CONNECTION
- ${device.MAC_NETWORK_CONNECTION

MAC Address Type

- MAC_ADDRESS_TYPE
- ${device.MAC_ADDRESS_TYPE

Mailbox Setup

- GOOGLE_AW_DIRECTORY_MAILBOX_SETUP
- ${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP

Main battery

- MAIN_BATTERY_PERCENT
- ${device.MAIN_BATTERY_PERCENT

MDM lost mode enabled

- IS_MDM_LOST_MODE_ENABLED
- ${device.IS_MDM_LOST_MODE_ENABLED

MDX_SHARED_ENCRYPTION_KEY

- MDX_SHARED_ENCRYPTION_KEY
- ${device.MDX_SHARED_ENCRYPTION_KEY

MEID

- MEID
- ${device.MEID

Mobile phone number

- TEL_NUMBER
- ${device.TEL_NUMBER

Model ID

- MODEL_ID
- ${device.MODEL_ID}

Model Number

- MODEL_NUMBER

- ${device.MODEL_NUMBER

Network Adapter Type

- NETWORK_ADAPTER_TYPE
- ${device.NETWORK_ADAPTER_TYPE

Operating system build

- SYSTEM_OS_BUILD
- ${device.SYSTEM_OS_BUILD

Operating System Edition

- OS_EDITION
- ${device.OS_EDITION

Operating system language (locale)

- SYSTEM_LANGUAGE
- ${device.SYSTEM_LANGUAGE

Operating system version

- SYSTEM_OS_VERSION
- ${device.SYSTEM_OS_VERSION

Organization address

- ORGANIZATION_ADDRESS
- ${device.ORGANIZATION_ADDRESS

Organization e-mail

- ORGANIZATION_EMAIL
- ${device.ORGANIZATION_EMAIL

Organization magic

- ORGANIZATION_MAGIC
- ${device.ORGANIZATION_MAGIC

Organization name

- ORGANIZATION_NAME
- ${device.ORGANIZATION_NAME

Organization phone number

- ORGANIZATION_PHONE
- ${device.ORGANIZATION_PHONE

Out of Compliance

- OUT_OF_COMPLIANCE
- ${device.OUT_OF_COMPLIANCE

Owned by

- CORPORATE_OWNED
- ${device.CORPORATE_OWNED

Passcode compliant

- PASSCODE_IS_COMPLIANT
- ${device.PASSCODE_IS_COMPLIANT

Passcode compliant with configuration

- PASSCODE_IS_COMPLIANT_WITH_CFG
- ${device.PASSCODE_IS_COMPLIANT_WITH_CFG

Passcode present

- PASSCODE_PRESENT
- ${device.PASSCODE_PRESENT

PCR0

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0

Perimeter breach

- GPS_PERIMETER_BREACH
- ${device.GPS_PERIMETER_BREACH

Periodic check

- PerformPeriodicCheck
- ${device.PerformPeriodicCheck

Personal Hotspot activated

- PERSONAL_HOTSPOT_ENABLED
- ${device.PERSONAL_HOTSPOT_ENABLED

PIN code for geofence

- PIN_CODE_FOR_GEO_FENCE
- ${device.PIN_CODE_FOR_GEO_FENCE

Platform

- SYSTEM_PLATFORM
- ${device.SYSTEM_PLATFORM}

Platform API level

- API_LEVEL
- ${device.API_LEVEL

Policy name

- POLICY_NAME
- ${device.POLICY_NAME

Primary Phone Number

- IDENTITY1_PHONENUMBER
- ${device.IDENTITY1_PHONENUMBER

Primary SIM Carrier Operator

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY1_CARRIER_NETWORK_OPERATOR

Primary SIM ICCID

- IDENTITY1_ICCID
- ${device.IDENTITY1_ICCID

Primary SIM IMEI

- IDENTITY1_IMEI
- ${device.IDENTITY1_IMEI

Primary SIM IMSI

- IDENTITY1_IMSI
- ${device.IDENTITY1_IMSI

Primary SIM Roaming

- IDENTITY1_ROAMING
- ${device.IDENTITY1_ROAMING

Primary SIM Roaming Compliance

- IDENTITY1_ROAMING_COMPLIANCE
- ${device.IDENTITY1_ROAMING_COMPLIANCE

Product name

- PRODUCT_NAME
- ${device.PRODUCT_NAME

Publisher Device ID

- PUBLISHER_DEVICE_ID

- ${device.PUBLISHER_DEVICE_ID

Reset Count

- WINDOWS_HAS_RESET_COUNT
- ${device.WINDOWS_HAS_RESET_COUNT

Restart Count

- WINDOWS_HAS_RESTART_COUNT
- ${device.WINDOWS_HAS_RESTART_COUNT

Safe Mode Enabled?

- WINDOWS_HAS_SAFE_MODE
- ${device.WINDOWS_HAS_SAFE_MODE

Samsung KNOX API available

- SAMSUNG_KNOX
- ${device.SAMSUNG_KNOX

Samsung KNOX API version

- SAMSUNG_KNOX_VERSION
- ${device.SAMSUNG_KNOX_VERSION

Samsung KNOX attestation

- SAMSUNG_KNOX_ATTESTED
- ${device.SAMSUNG_KNOX_ATTESTED

Samsung KNOX attestation updated date

- SAMSUNG_KNOX_ATT_UPDATED_TIME
- ${device.SAMSUNG_KNOX_ATT_UPDATED_TIME

Samsung SAFE API available

- SAMSUNG_MDM
- ${device.SAMSUNG_MDM

Samsung SAFE API version

- SAMSUNG_MDM_VERSION
- ${device.SAMSUNG_MDM_VERSION

SBCP Hash

- WINDOWS_HAS_SBCP_HASH
- ${device.WINDOWS_HAS_SBCP_HASH

Screen: height

- SCREEN_HEIGHT
- ${device.SCREEN_HEIGHT

Screen: number of colors

- SCREEN_NB_COLORS
- ${device.SCREEN_NB_COLORS

Screen: size

- SCREEN_SIZE
- ${device.SCREEN_SIZE

Screen: width

- SCREEN_WIDTH
- ${device.SCREEN_WIDTH

Screen: X-axis resolution

- SCREEN_XDPI
- ${device.SCREEN_XDPI

Screen: Y-axis resolution

- SCREEN_YDPI
- ${device.SCREEN_YDPI

Secondary Phone Number

- IDENTITY2_PHONENUMBER
- ${device.IDENTITY2_PHONENUMBER

Secondary SIM Carrier Operator

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY2_CARRIER_NETWORK_OPERATOR

Secondary SIM ICCID

- IDENTITY2_ICCID
- ${device.IDENTITY2_ICCID

Secondary SIM IMEI

- IDENTITY2_IMEI
- ${device.IDENTITY2_IMEI

Secondary SIM IMSI

- IDENTITY2_IMSI
- ${device.IDENTITY2_IMSI

Secondary SIM Roaming

- IDENTITY2_ROAMING
- ${device.IDENTITY2_ROAMING

Secondary SIM Roaming Compliance

- IDENTITY2_ROAMING_COMPLIANCE
- ${device.IDENTITY2_ROAMING_COMPLIANCE

Secure Boot Enabled?

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- ${device.WINDOWS_HAS_SECURE_BOOT_ENABLED

Secure Boot Status

- SECURE_BOOT_STATE
- ${device.SECURE_BOOT_STATE

SecureContainer Enabled

- DLP_ACTIVE
- ${device.DLP_ACTIVE

Security patch level

- SYSTEM_SECURITY_PATCH_LEVEL
- ${device.SYSTEM_SECURITY_PATCH_LEVEL

Serial number

- SERIAL_NUMBER
- ${device.SERIAL_NUMBER

SMS capable

- IS_SMS_CAPABLE
- ${device.IS_SMS_CAPABLE

Supervised

- SUPERVISED
- ${device.SUPERVISED

Suspension Reason

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON

Tampered Status

- TAMPERED_STATUS

- ${device.TAMPERED_STATUS

Terms & Conditions

- TERMS_AND_CONDITIONS
- ${device.TERMS_AND_CONDITIONS

Terms And Agreement Accepted?

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- ${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS

Test Signing Enabled?

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- ${device.WINDOWS_HAS_TEST_SIGNING_ENABLED

Total RAM

- MEMORY
- ${device.MEMORY

Total storage space

- TOTAL_DISK_SPACE
- ${device.TOTAL_DISK_SPACE

TPM version

- TPM_VERSION
- ${device.TPM_VERSION

UDID

- UDID
- ${device.UDID}

User Account Control Status

- UAC_STATUS
- ${device.UAC_STATUS

User agent

- USER_AGENT
- ${device.USER_AGENT

User defined #1

- USER_DEFINED_1
- ${device.USER_DEFINED_1

User defined #2

- USER_DEFINED_2
- ${device.USER_DEFINED_2

User defined #3

- USER_DEFINED_3
- ${device.USER_DEFINED_3

User language (locale)

- USER_LANGUAGE
- ${device.USER_LANGUAGE

Vendor

- VENDOR
- ${device.VENDOR

Voice capable

- IS_VOICE_CAPABLE
- ${device.IS_VOICE_CAPABLE

Voice roaming allowed

- VOICE_ROAMING_ENABLED
- ${device.VOICE_ROAMING_ENABLED

VSM Enabled?

- WINDOWS_HAS_VSM_ENABLED
- ${device.WINDOWS_HAS_VSM_ENABLED

WiFi MAC address

- WIFI_MAC
- ${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY
- ${device.WINDOWS_ENROLLMENT_KEY

WinPE Enabled?

- WINDOWS_HAS_WINPE
- ${device.WINDOWS_HAS_WINPE

WNS Notification Status

- PROPERTY_WNS_PUSH_STATUS
- ${device.PROPERTY_WNS_PUSH_STATUS

WNS Notification URL

- PROPERTY_WNS_PUSH_URL
- ${device.PROPERTY_WNS_PUSH_URL

WNS Notification URL expiry date

- PROPERTY_WNS_PUSH_URL_EXPIRY
- ${device.PROPERTY_WNS_PUSH_URL_EXPIRY

XenMobile agent ID

- ENROLLMENT_AGENT_ID
- ${device.ENROLLMENT_AGENT_ID

XenMobile agent revision

- EW_REVISION
- ${device.EW_REVISION

XenMobile agent version

- EW_VERSION
- ${device.EW_VERSION

Zebra API available

- ZEBRA_MDM
- ${device.ZEBRA_MDM

Zebra MXMF version

- ZEBRA_MDM_VERSION
- ${device.ZEBRA_MDM_VERSION

Zebra Patch version

- ZEBRA_PATCH_VERSION
- ${device.ZEBRA_PATCH_VERSION}

Macros to obtain built-in user properties

Display name	Macros
domainname (domain name; default domain)	`${ user.domainname }`
loginname (user name plus domain name)	`${ user.loginname }`
username (login name minus the domain, if any)	`${ user.username }`

Macros for all user properties

Display name	Web element	Macros
Active Directory failed logon tries	badpwdcount	`${ user.badpwdcount }`
ActiveSync user email	asuseremail	`${ user.asuseremail }`
ASM data source	asmpersonsource	`${ user.asmpersonsource }`
ASM DEP account name	asmdepaccount	`${ user.asmdepaccount }`
ASM managed Apple ID	asmpersonmanagedappleid	`${ user.asmpersonmanagedappleid }`
ASM passcode type	asmpersonpasscodetype	`${ user.asmpersonpasscodetype }`
ASM person ID	asmpersonid	`${ user.asmpersonid }`
ASM person status	asmpersonstatus	`${ user.asmpersonstatus }`
ASM person title	asmpersontitle	`${ user.asmpersontitle }`
ASM person unique ID	asmpersonuniqueid	`${ user.asmpersonuniqueid }`
ASM source system ID	asmpersonsourcesystemid	`${ user.asmpersonsourcesystemid }`
ASM student grade	asmpersongrade	`${ user.asmpersongrade }`
BES user email	besuseremail	`${ user.besuseremail }`
Company	company	`${ user.company }`
Company name	companyname	`${ user.companyname }`
Country	c	`${ user.c }`
Department	department	`${ user.department }`
Description	description	`${ user.description }`

Display name	Web element	Macros
Disabled user	disableduser	${ user.disableduser }
Display name	displayname	${ user.displayname }
Distinguished name	distinguishedname	${ user.distinguishedname }
Domain name	domainname	${ user.domainname }
Email	mail	${ user.mail }
First name	givenname	${ user.givenname }
Home address	homestreetaddress	${ user.homestreetaddress }
Home city	homecity	${ user.homecity }
Home country	homecountry	${ user.homecountry }
Home fax	homefax	${ user.homefax }
Home phone	homephone	${ user.homephone }
Home state/region	homestate	${ user.homestate }
Home zip or post code	homezip	${ user.homezip }
IP phone	ipphone	${ user.ipphone }
Middle initial	middleinitial	${ user.middleinitial }
Middle name	middlename	${ user.middlename }
Mobile	mobile	${ user.mobile }
Name	cn	${ user.cn }
Office address	physicaldeliveryofficename	${ user.physicaldeliveryofficename }
Office city	l	${ user.l }
Office fax number	facsimiletelephonenumber	${ user.facsimiletelephonenumber }
Office state/province	st	${ user.st }
Office street address	officestreetaddress	${ user.officestreetaddress }

Display name	Web element	Macros
Office telephone number	telephonenumber	${ user.telephonenumber }
Office zip or post code	postalcode	${ user.postalcode }
P.O. box	postofficebox	${ user.postofficebox }
Pager	pager	${ user.pager }
Primary group ID	primarygroupid	${ user.primarygroupid }
SAM account	samaccountname	${ user.samaccountname }
Street address	streetaddress	${ user.streetaddress }
Surname	sn	${ user.sn }
Title	title	${ user.title }
User logon name	userprincipalname	${ user.userprincipalname }

Automated actions

April 23, 2021

You create automated actions in XenMobile to program a reaction to events, user or device properties, or 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 XenMobile. 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.

> **Note:**
>
> Before you can notify users, you must configure notification servers in the XenMobile settings for SMTP and SMS so that XenMobile 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 XenMobile 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.

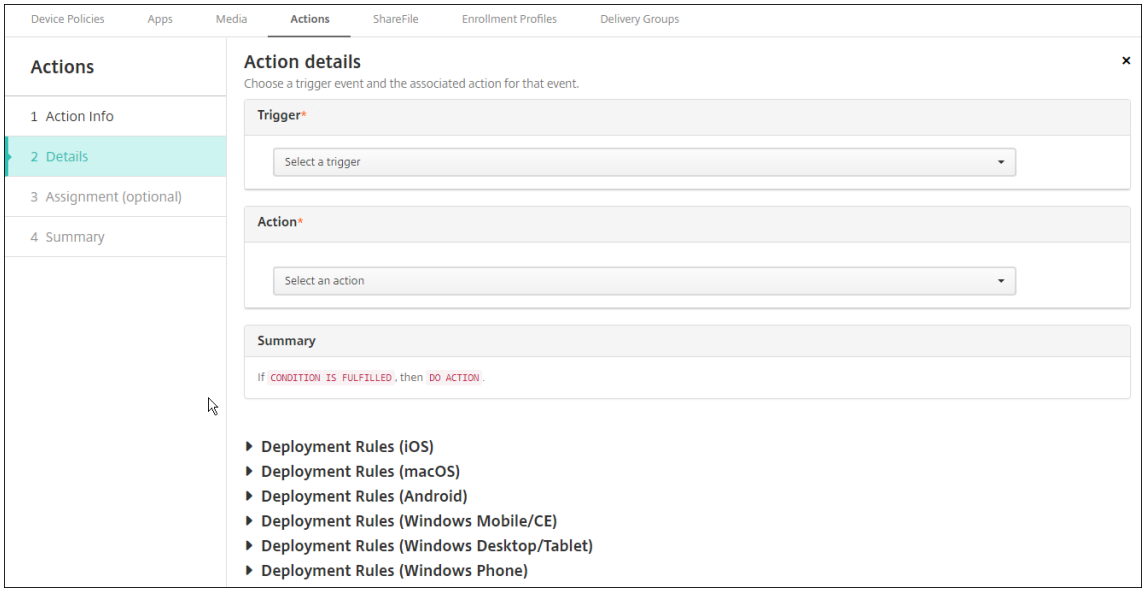
> **Tip:**
>
> To delete inactive devices in bulk, use the Public API for REST Services. You first manually obtain the device IDs for inactive devices you want to delete and then run the delete API to delete them in bulk.

Add and manage actions

To add, edit, and filter automated actions:

1. From the XenMobile 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 those 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. The meaning of each trigger is as follows:

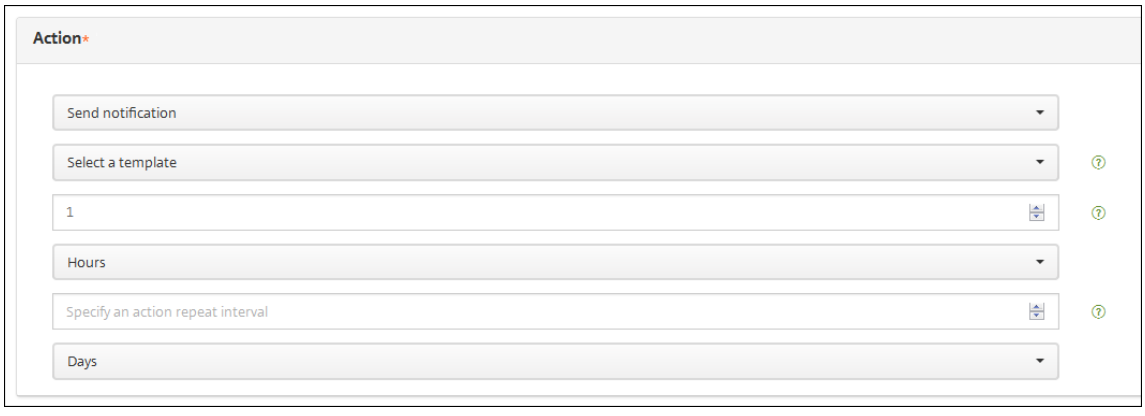
- **Event:** Reacts to a predefined event.
- **Device property:** Checks for a device attribute on a device that is MDM-managed, then reacts to it. For more information, see Device property names and values.
- **User property:** Reacts to a user attribute, usually from Active Directory.
- **Installed 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.

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 **Send notification**, 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.

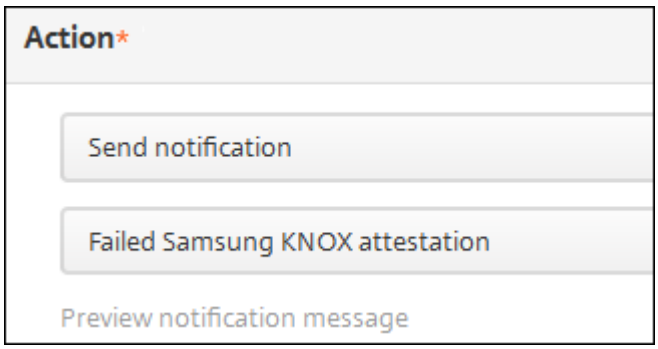
   If you pick **Send notification**, use the following steps to send a notification action.

9. In the next list, select the template to use for the notification. Notification templates relevant to the selected event appear, unless a template doesn't yet exist for the notification type. In that case, you are prompted to configure a template with the message: No template for this event type. Create template using **Notification Template** in **Settings**.

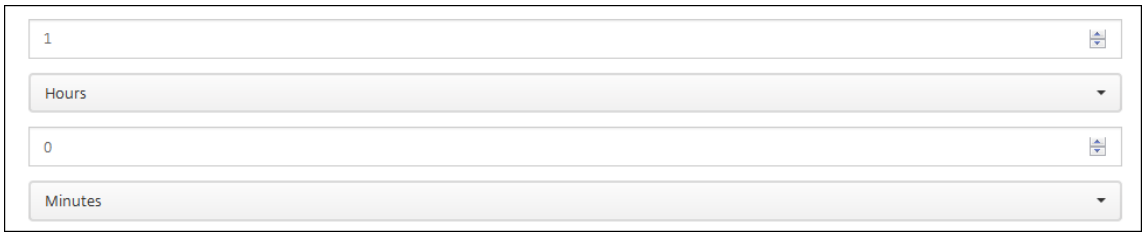
   Before you can notify users, you must have configured notification servers in Settings for SMTP and SMS so that XenMobile can send the messages, see Notifications. Also, set up any notification templates you plan to use before proceeding. For details on setting up notification templates, see Create and update notification templates.



   After you select the template, you can preview the notification by clicking **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 local encryption must be **True**.
    - 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**. The always-on option is not available for iOS devices.

    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**, which does not apply to iOS.
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 in response to all four categories of triggers listed in the XenMobile console: event, device property, user property, and installed app name.

To configure automatic app wipe or app lock

1. In the XenMobile 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.

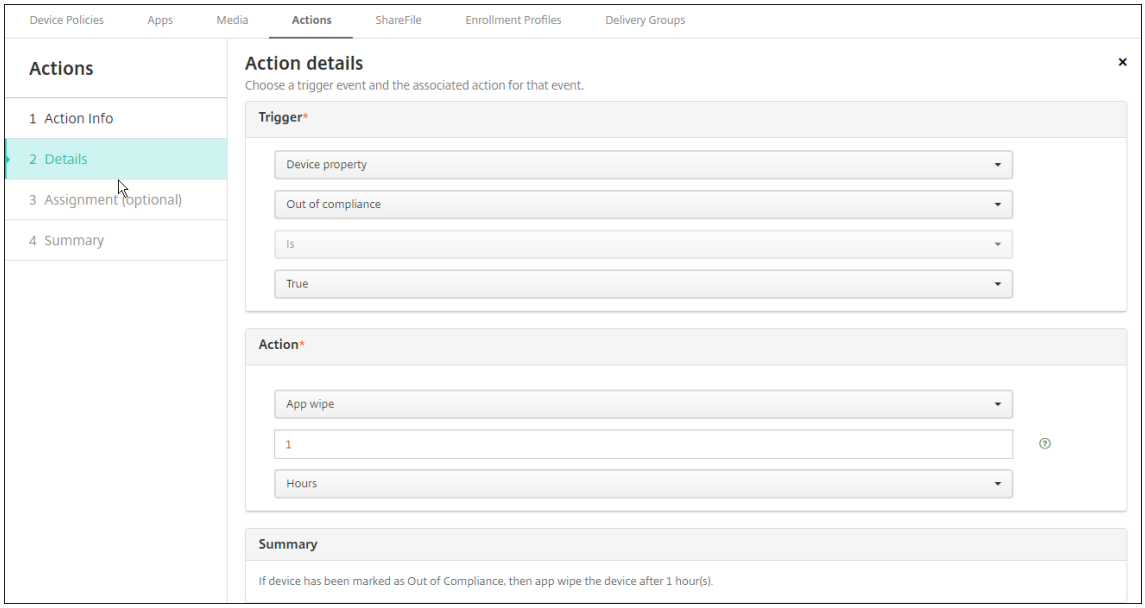
   When the trigger type is **Device property** and the value is **MDM lost mode enabled**, the following actions don't appear:

   - 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.

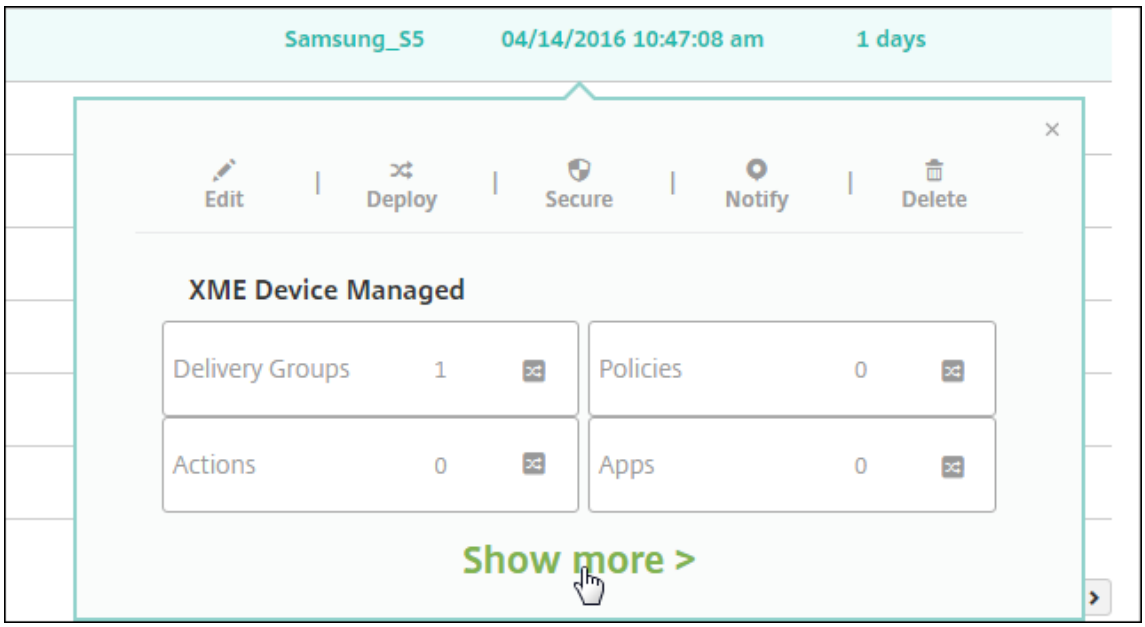
> **Note:**
>
> If you set the trigger to **event**, the repeat interval is automatically a minimum of 1 hour. The device must carry out a refresh of the policies to synchronize with the server for the notification to come in. Typically, a device synchronizes with the server when users sign on or manually refresh their policies through Secure Hub.
>
> An extra delay of approximately 1 hour may occur before any action is carried out, to allow the Active Directory database to synchronize with XenMobile.



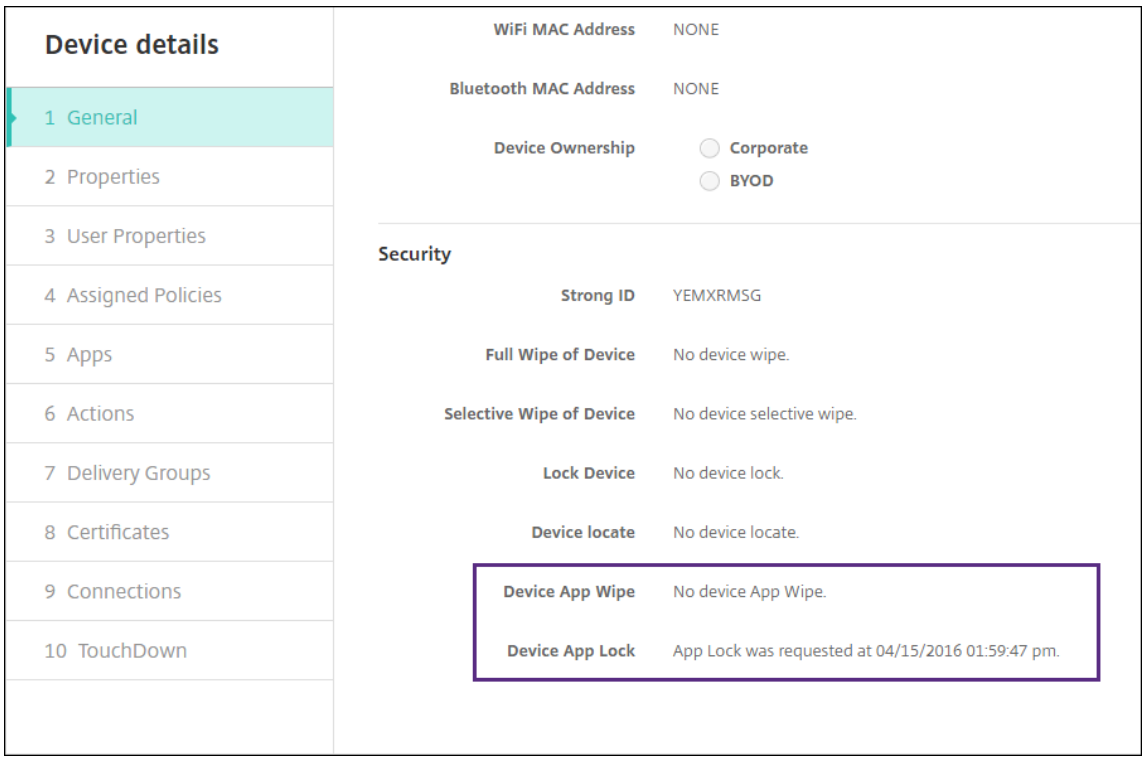
6. Configure deployment rules and then click **Next**.
7. Configure delivery group assignments and a deployment schedule and then click **Next**.
8. Click **Save**.

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.

Monitor and support

January 6, 2021

You can use the XenMobile Dashboard and the XenMobile Support page to monitor and troubleshoot your XenMobile Server. Use the XenMobile Support page to access support-related information and tools.

For an on-premises XenMobile Server, you can also perform actions from the XenMobile CLI. For details, see Command-line interface options.

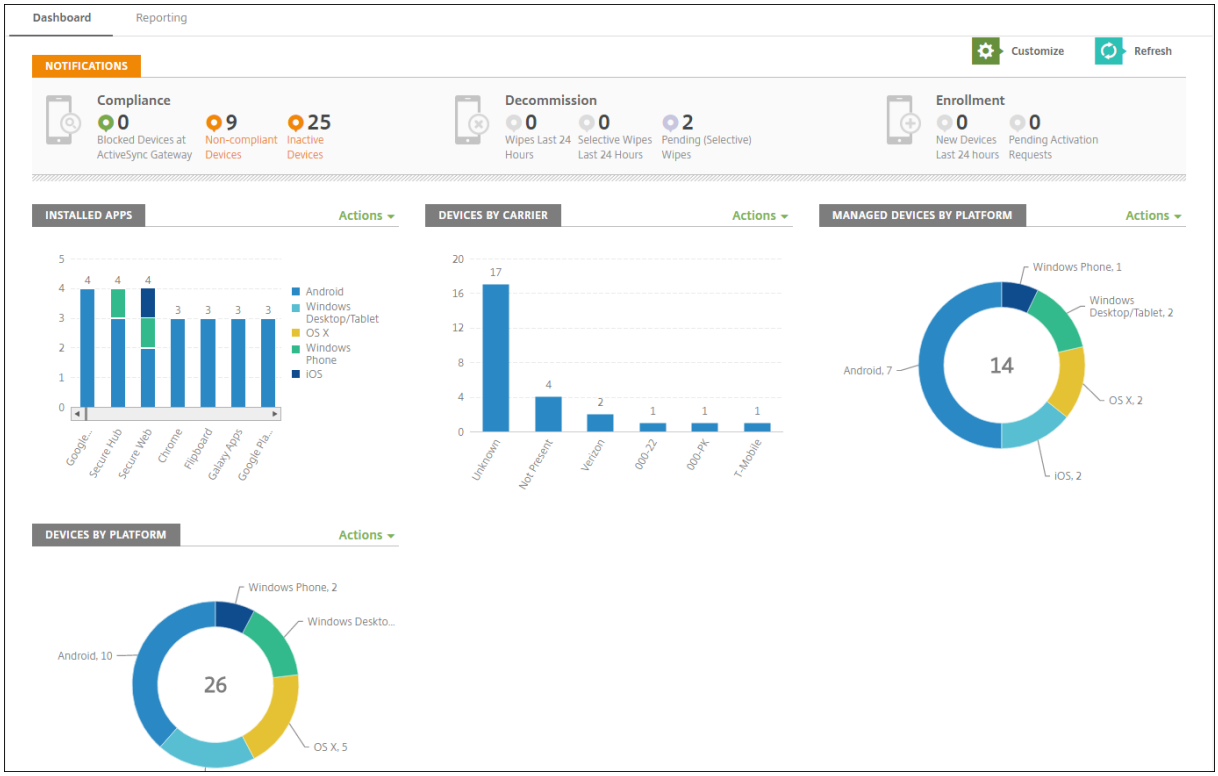
In the XenMobile console, click the wrench icon in the upper-right corner.

The Troubleshooting and Support page appears.

Use the XenMobile **Support** page to:

- Access diagnostics.
- Create support bundles (on-premises installations only).
- 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 XenMobile console dashboard. With this information, you can see issues and successes quickly by using widgets.



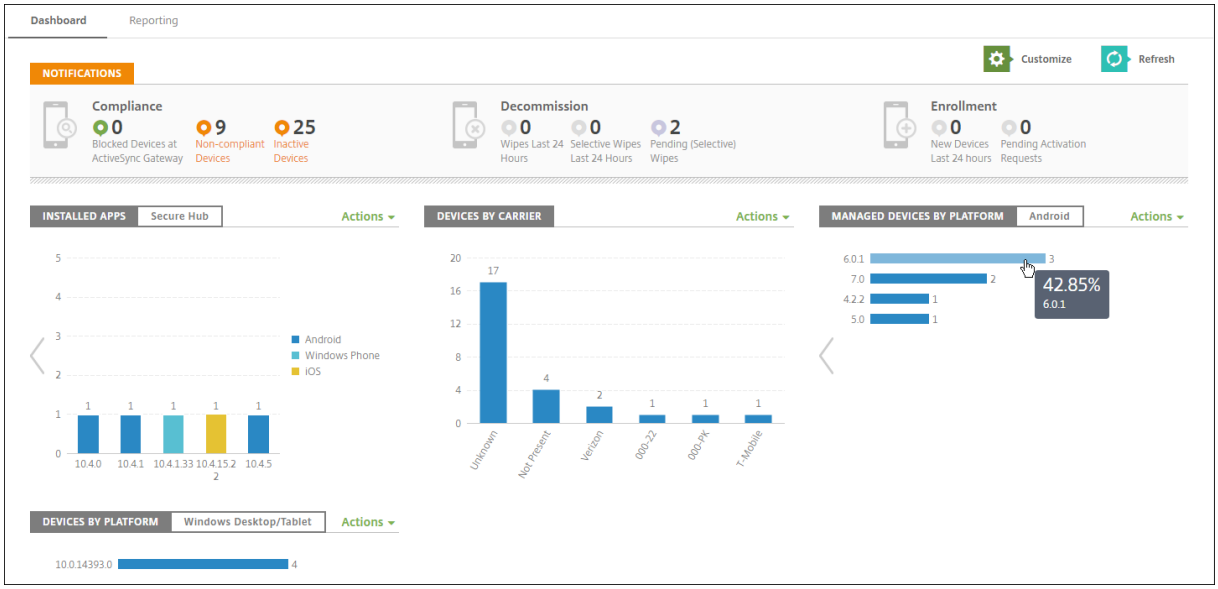
The dashboard is usually the page that first appears when you sign on to the XenMobile console. To access the dashboard from elsewhere in the console, click **Analyze**. Click **Customize** on the dashboard to edit the layout of the page and to edit the widgets that appear.

- **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 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.

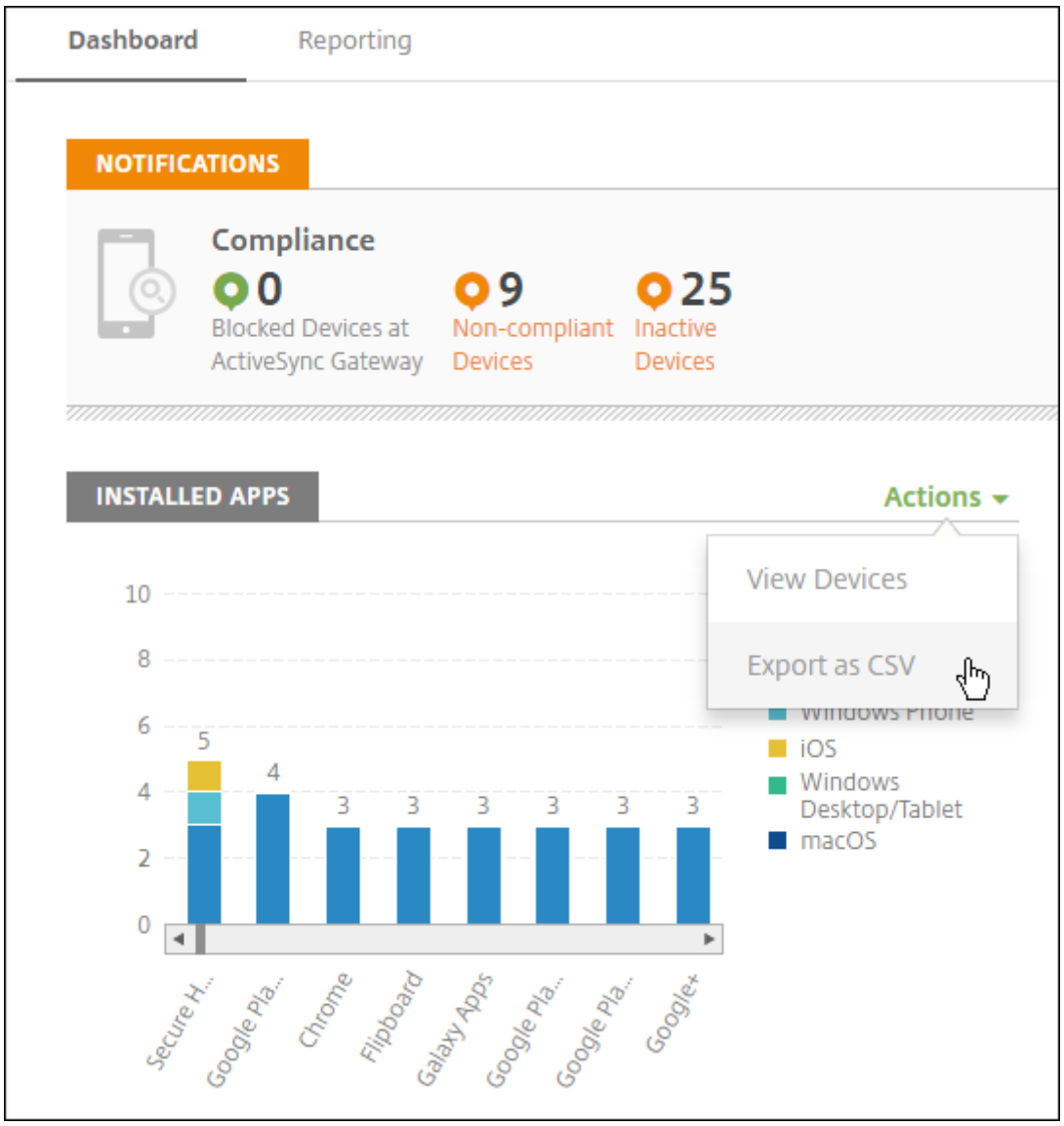
You can click each bar to break down the data by platform.

- **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:** 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.



You can also export the information as a .csv file by clicking the **Action** drop-down.



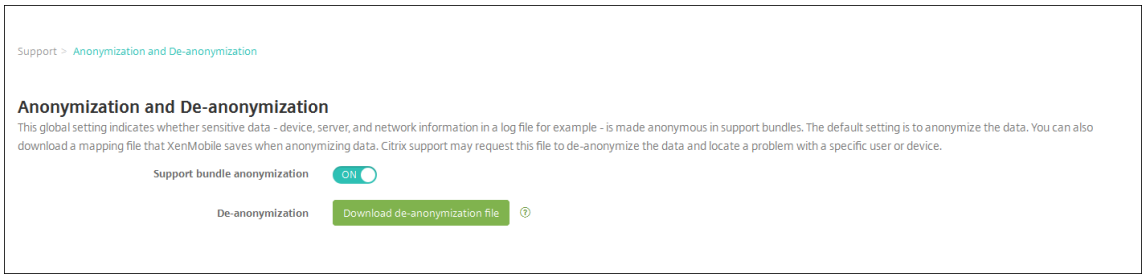
Anonymize data in support bundles

July 3, 2018

When you create support bundles in XenMobile, sensitive user, server, and network data is made anonymous by default. You can change this behavior on the Anonymization and De-anonymization page. You can also download a mapping file that XenMobile saves when anonymizing data. Citrix support may request this file to de-anonymize the data and locate a problem with a specific user or device.

1. In the XenMobile console, click the wrench icon in the right upper-hand corner. The **Support** page appears.

2. On the **Support** page, under **Advanced**, click **Anonymization and De-anonymization**. The **Anonymization and De-anonymization** page appears.



3. In **Support bundle anonymization**, select whether data is anonymized. The default is **ON**.
4. Next to **De-anonymization**, click **Download de-anonymization file** to download the mapping file to send to Citrix support when they need specific device or user information to diagnose an issue.

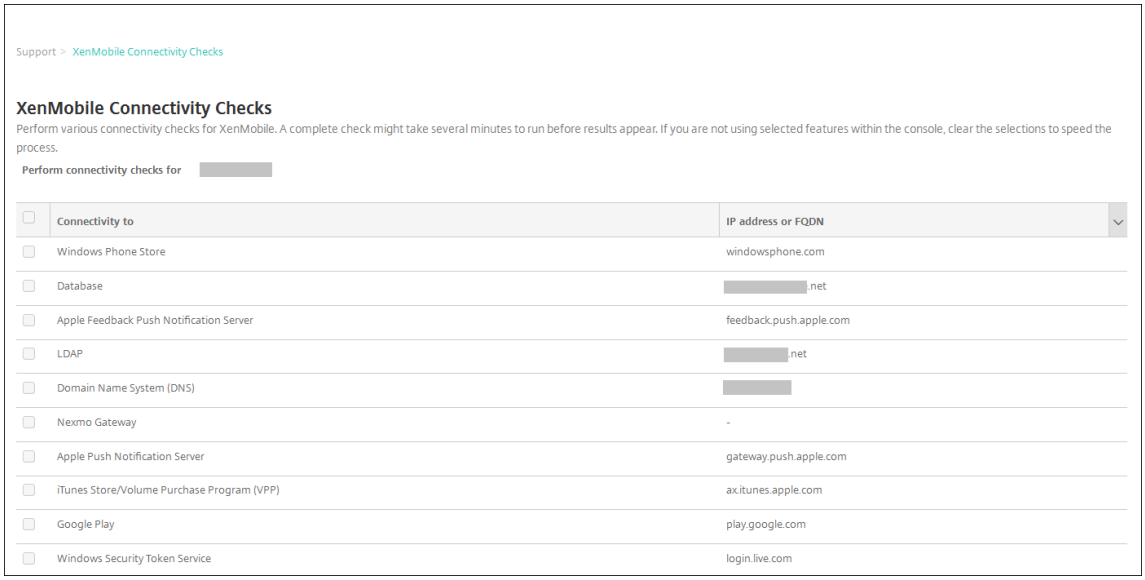
Connectivity checks

August 31, 2020

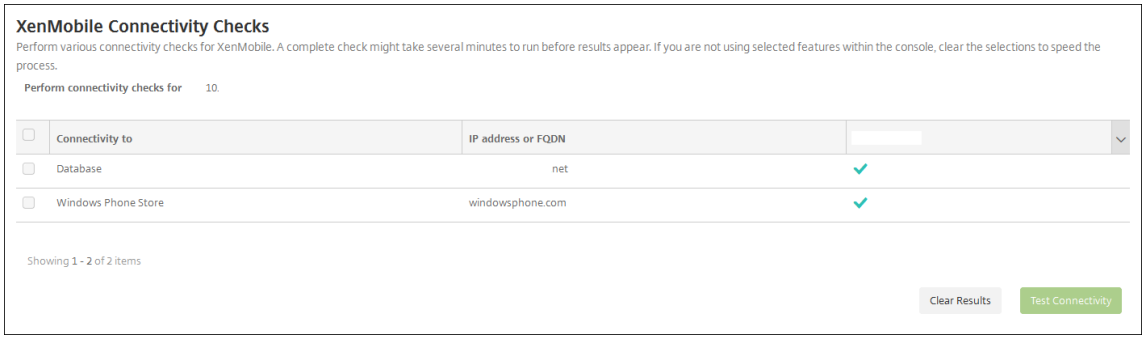
From the XenMobile **Support** page, you can check the XenMobile connection to Citrix Gateway and to other servers and locations.

Conducting XenMobile Connectivity Checks

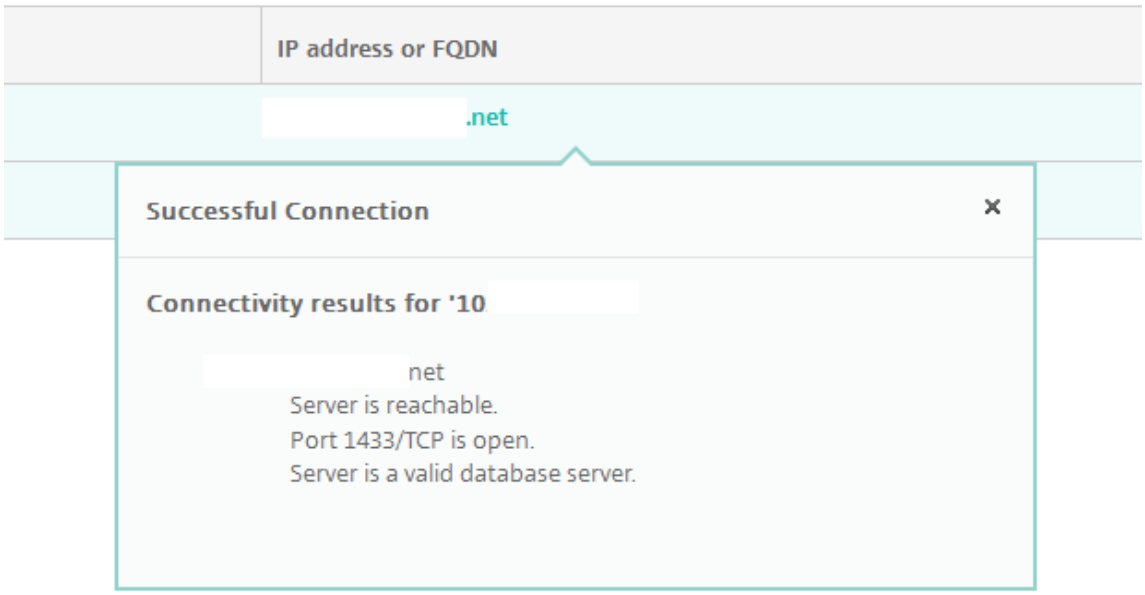
1. In the XenMobile console, click the wrench icon in the upper-right corner of the console. The **Support** page appears.
2. Under **Diagnostics**, click **XenMobile Connectivity Checks**. The **XenMobile Connectivity Checks** page appears. If your XenMobile environment contains clustered nodes, all nodes are shown.



3. Select the servers you want to include in the connectivity test and then click **Test Connectivity**. The test results page appears.

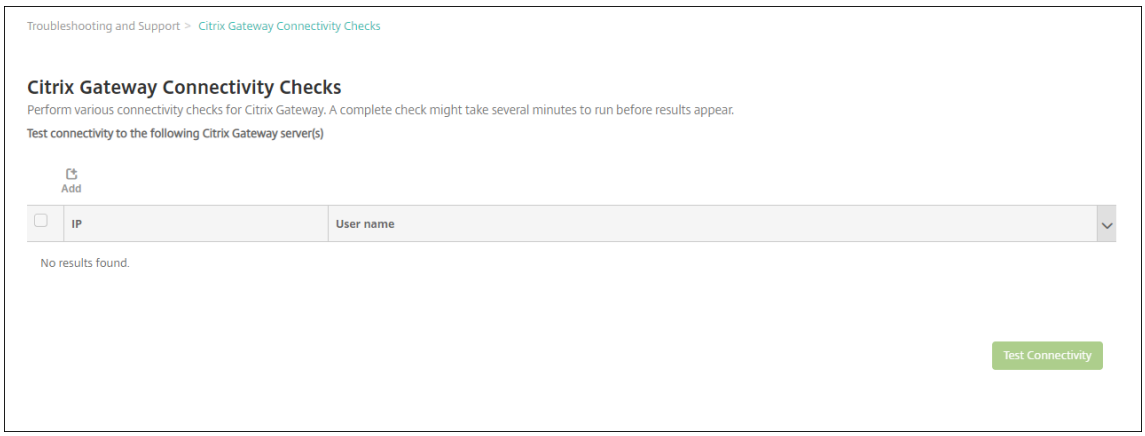


4. Select a server in the test results table to see detailed results for that server.

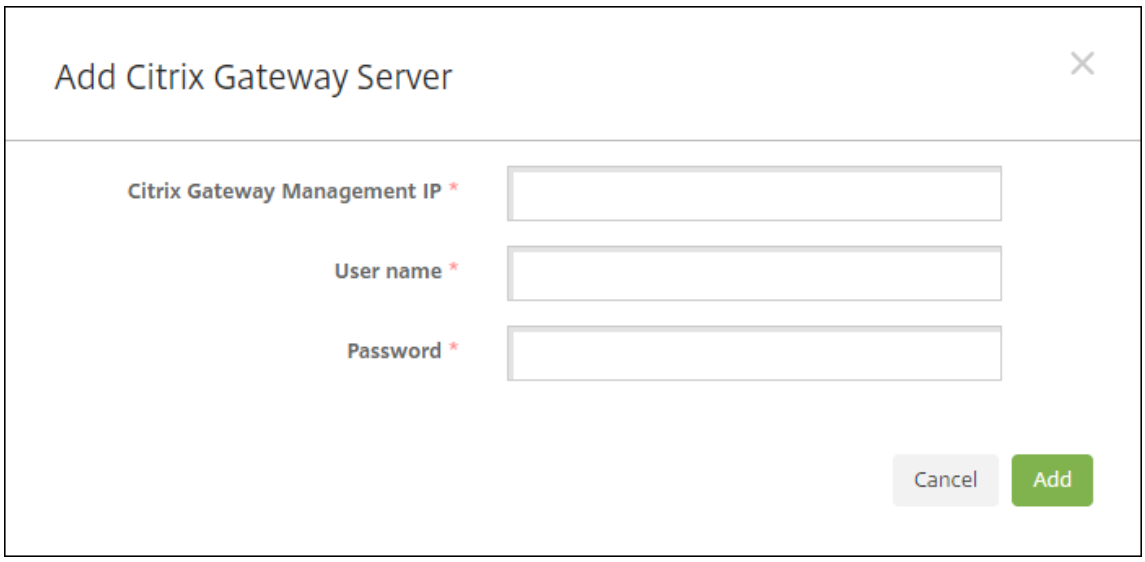


Conducting Citrix Gateway Connectivity Checks

1. On the **Support** page, under **Diagnostics**, click **Citrix Gateway Connectivity Checks**. The **Citrix Gateway Connectivity Checks** page appears. The table is empty if you haven't added any Citrix Gateway servers.



2. Click **Add**. The **Add Citrix Gateway Server** dialog box appears.



3. In **Citrix Gateway Management IP**, type the management IP address for the server running Citrix Gateway that you want to test.

   > **Note:**
   >
   > 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.

   > **Note:**
   >
   > 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.

Customer Experience Improvement Program

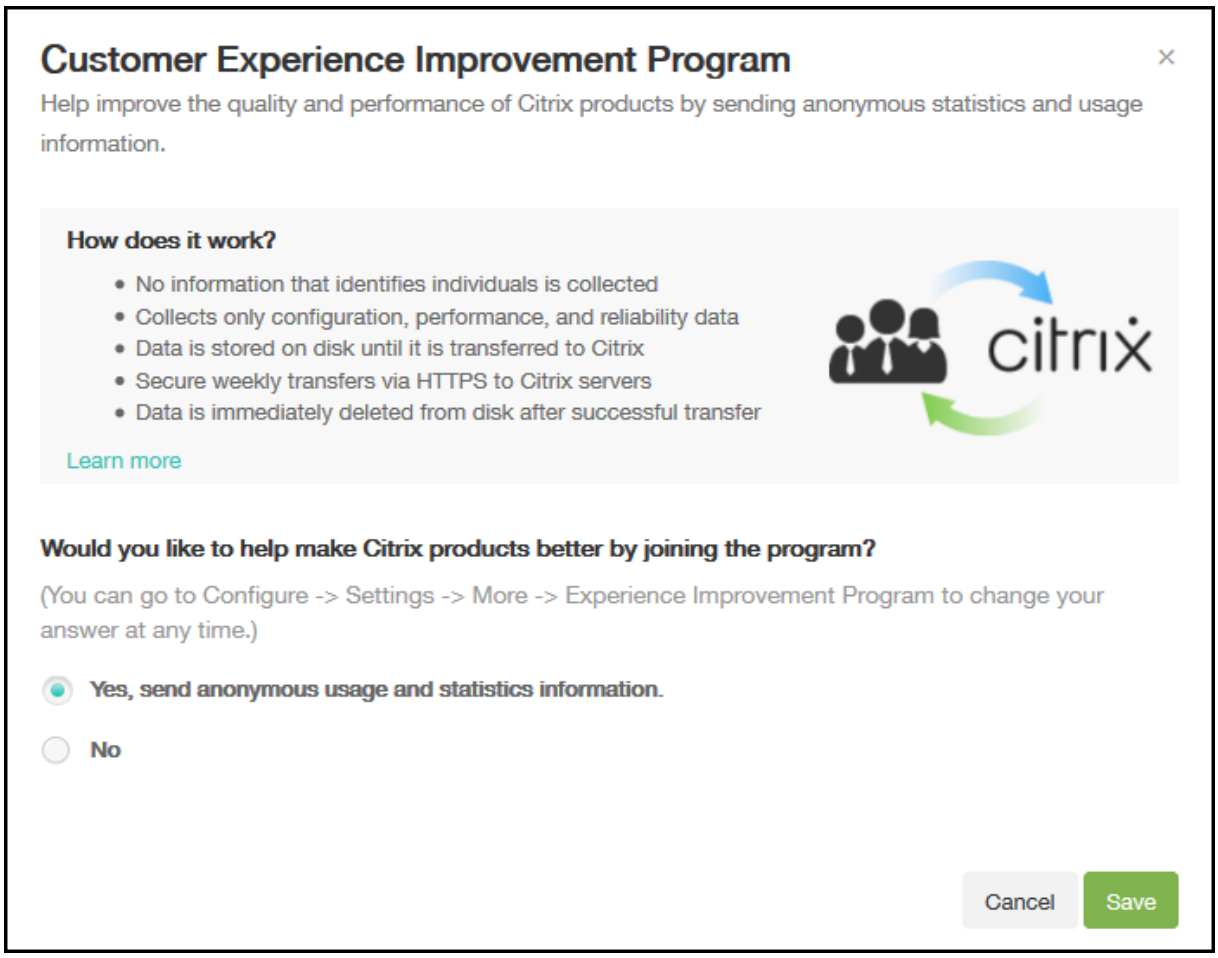
October 4, 2018

The Citrix Customer Experience Improvement Program (CEIP) gathers anonymous configuration and usage data from XenMobile and automatically sends the data to Citrix. This data helps Citrix improve

the quality, reliability, and performance of XenMobile. Participation in the CEIP is completely voluntary. When you first install XenMobile, or when you install an update, you have the option to participate in the CEIP. When you opt-in, data is typically collected on a weekly basis, and performance and usage data is collected hourly. The data is stored on disk and transferred securely via HTTPS to Citrix weekly. You can change whether you participate in the CEIP in the XenMobile console. For more information on the CEIP, see About the Citrix Customer Experience Improvement Program (CEIP).

Choosing to participate in the CEIP

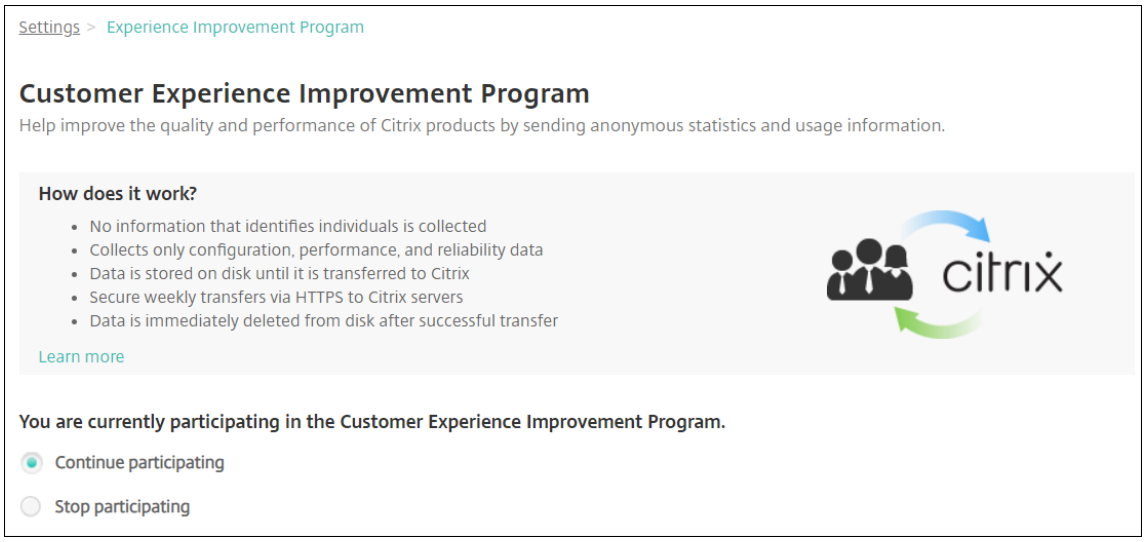
The first time you install XenMobile or when you do an update, you see the following dialog box that prompts you to participate.



Changing your CEIP participation setting

1. To change your CEIP participation setting, in the XenMobile console, click the gear icon in the upper-right corner of the console to open the **Settings** page.

2. Under **Server**, click **Experience Improvement Program**. The **Customer Experience Improvement Program** page appears. The exact page you see depends on whether you are currently participating in the CEIP.



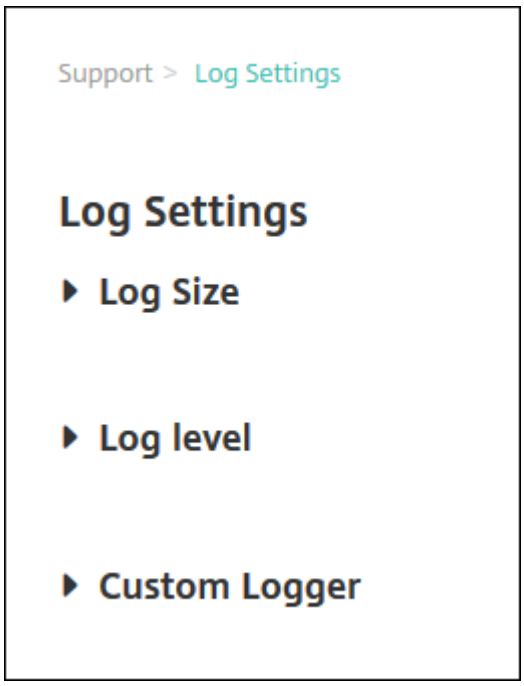
3. If you are currently participating in the CEIP and want to stop, click **Stop participating**.
4. If you are not currently participating in the CEIP and want to start, click **Start participating**.
5. Click **Save**.

Logs

April 25, 2019

You can configure log settings to customize the output of logs that XenMobile generates. If you have clustered XenMobile servers, when you configure log settings in the XenMobile console, those settings are shared with all other servers in the cluster.

1. In the XenMobile console, click the wrench icon in the upper-right corner of the console. The **Support** page appears.
2. Under **Log Operations**, click **Log Settings**. The **Log Settings** page appears.

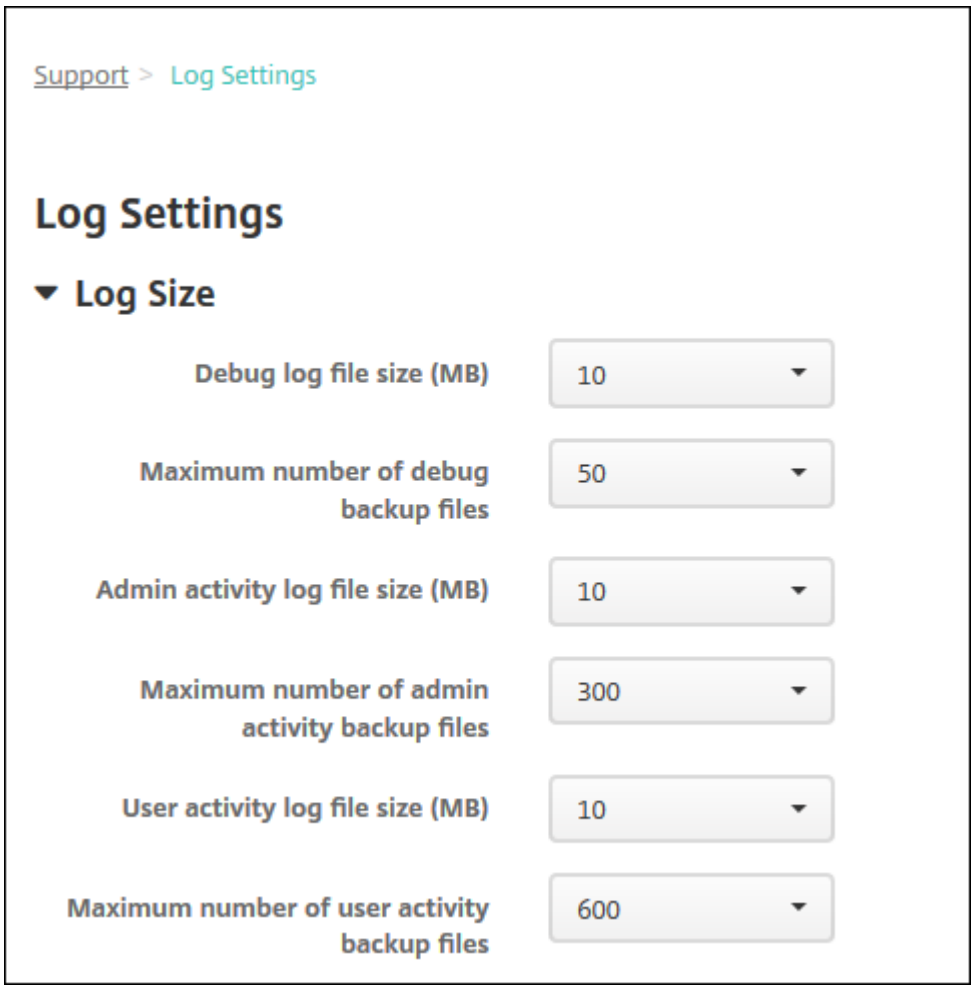


On the **Log Settings** page you can access the following options:

- **Log Size**. Use this option to control the size of the log file and the maximum number of log backup files retained in the database. Log size applies to each of the logs supported by XenMobile (debug log, Admin activity log, and user activity log).
- **Log level**. Use this option to change the log level or to persist settings.
- **Custom Logger**. Use this option to create a custom logger; custom logs require a class name and the log level.

To configure the Log Size options

1. On the **Log Settings** page, expand **Log Size**.



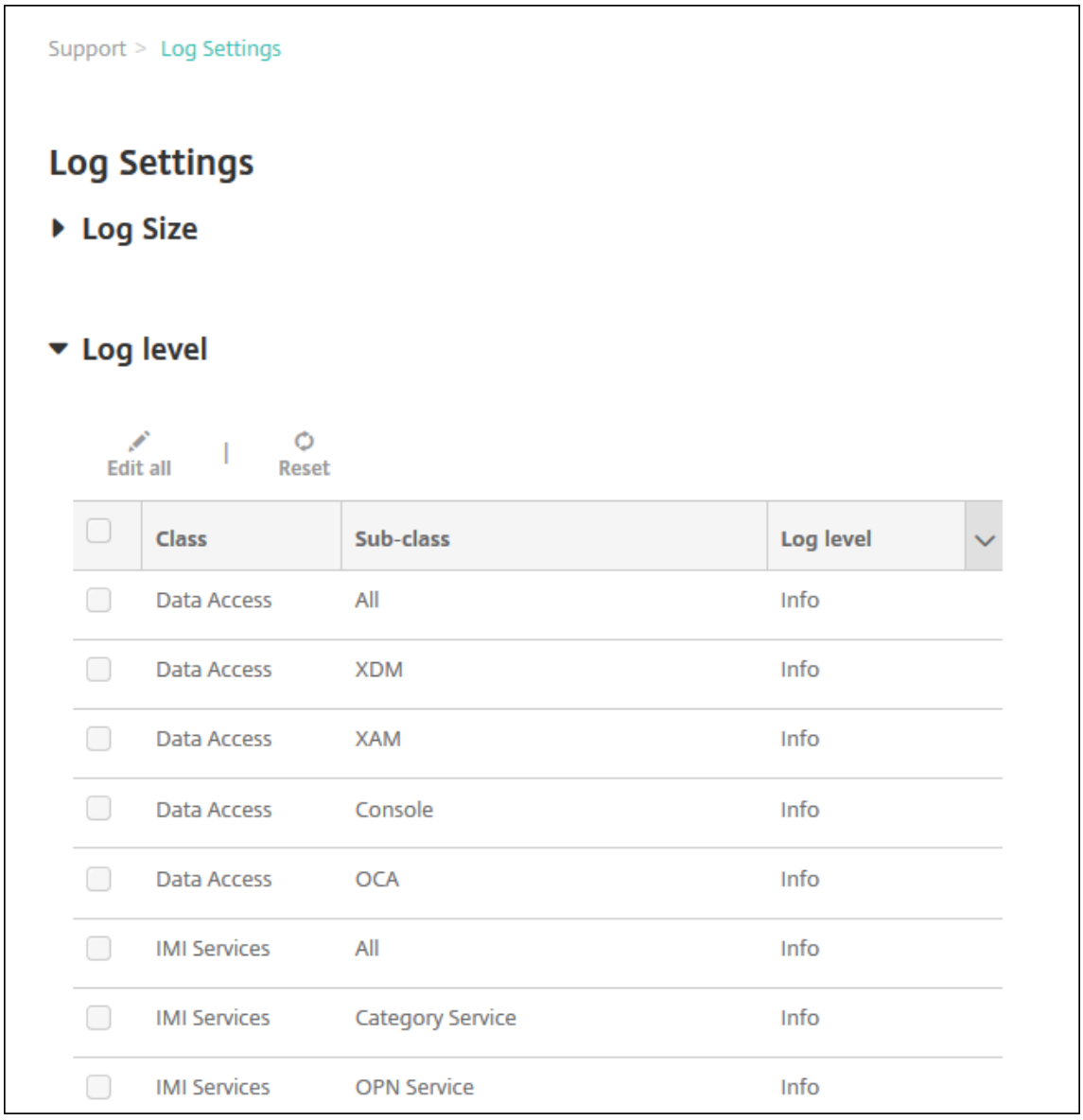
2. Configure these settings:

- **Debug log file size (MB):** In the list, click a size between 5 MB and 20 MB to change the maximum size of the debug file. The default file size is **10 MB**.
- **Maximum number of debug backup files:** In the list, click the maximum number of debug files retained by the server. By default, XenMobile retains 50 backup files on the server.
- **Admin activity log file size (MB):** in the list, click a size between 5 MB and 20 MB to change the maximum size of the admin activity file. The default file size is **10 MB**.
- **Maximum number of admin activity backup files:** In the list, click the maximum number of admin activity files retained by the server. By default, XenMobile retains 300 backup files on the server.
- **User activity log file size (MB):** In the list, click a size between 5 MB and 20 MB to change the maximum size of the user activity file. The default file size is **10 MB**.
- **Maximum number of user activity backup files:** In the list, click the maximum number of user activity files retained by the server. By default, XenMobile retains 300 backup files on the server.

To configure Log Level options

Log level lets you specify what type of information XenMobile collects in the log. You can set the same level for all classes or you can set individual classes to specific levels.

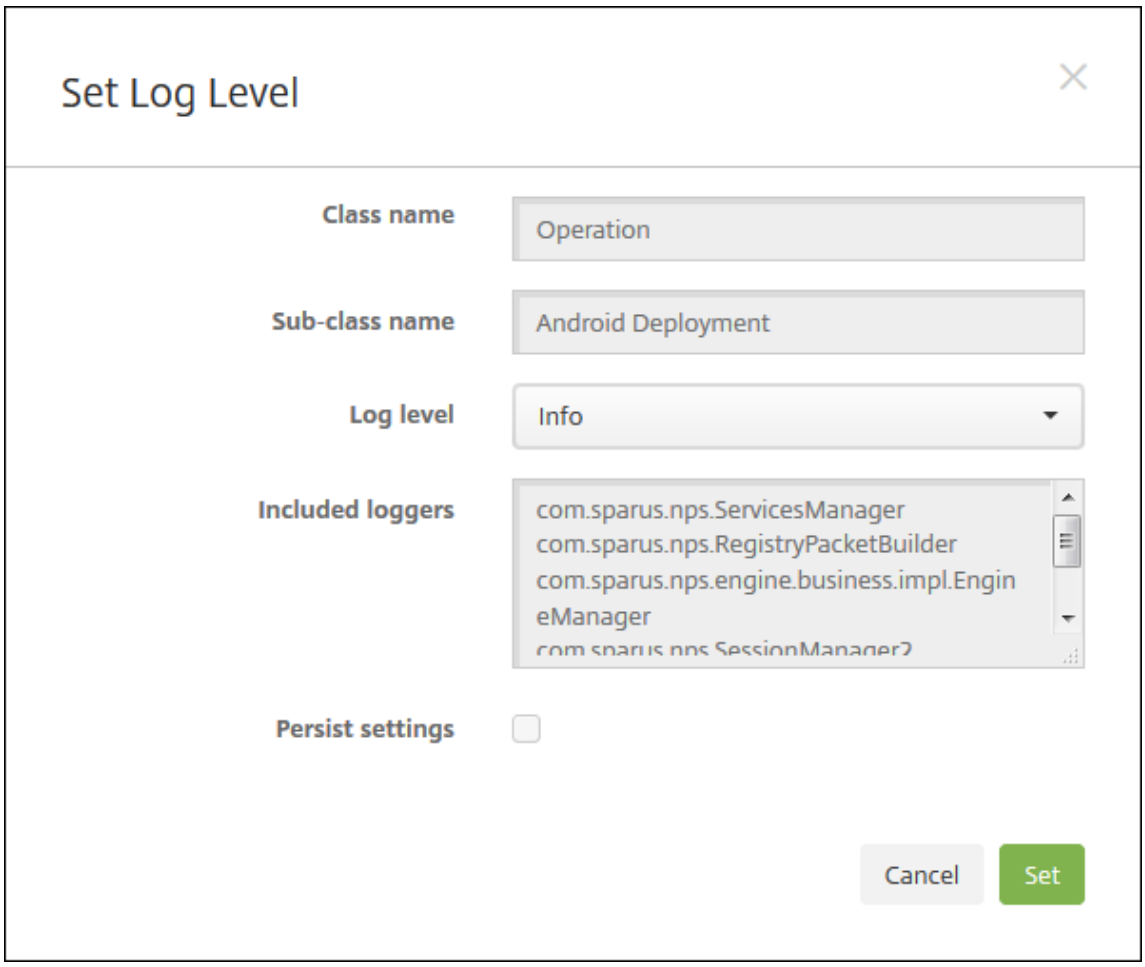
1. On the **Log Settings** page, expand **Log level**. The table of all log classes appears.



2. Do one of the following:

   - Click the check box next to one Class and then, click **Set Level** to change just this class's log level.
   - Click **Edit** all to apply the log level change to all classes in the table.

   The **Set Log Level** dialog box appears where you can set the log level and select whether to have log level settings persist when you reboot the XenMobile server.

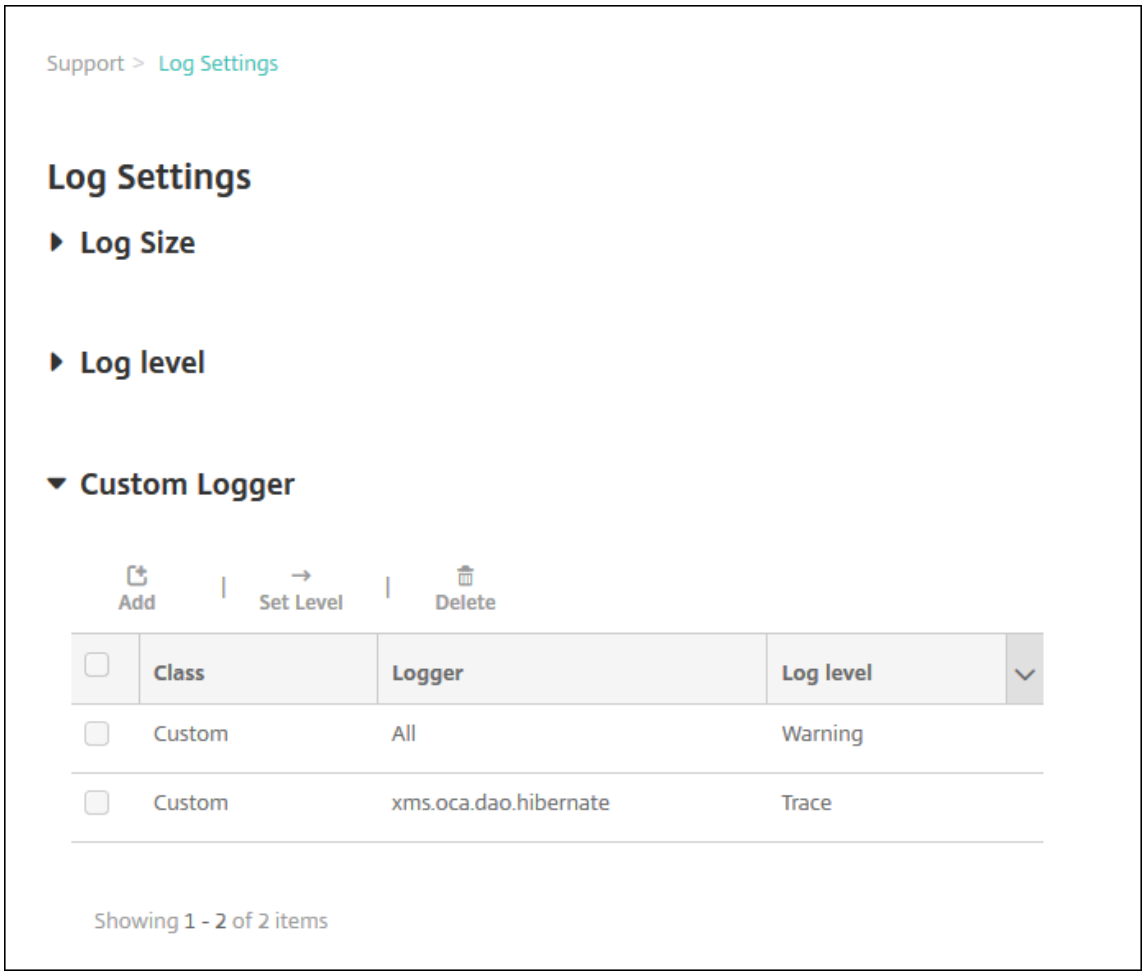


- **Class Name:** This field displays All when you are changing the log level for all classes or it displays the individual class name; it is not editable.
- **Sub-class name:** This field displays All when you are changing the log level for all classes or it displays the individual class sub-class name; it is not editable.
- **Log level:** In the list, click a log level. The supported log levels include:
  - Fatal
  - Error
  - Warning
  - Info
  - Debug
  - Trace
  - Off
- **Included Loggers:** This field is blank when you are changing the log level for all classes or it displays the currently configured loggers for an individual class; it is not editable.
- **Persist settings:** If you want the log level settings to persist when you reboot the server, select this check box. Not selecting this check box means that the log level settings revert to their defaults when you reboot the server.

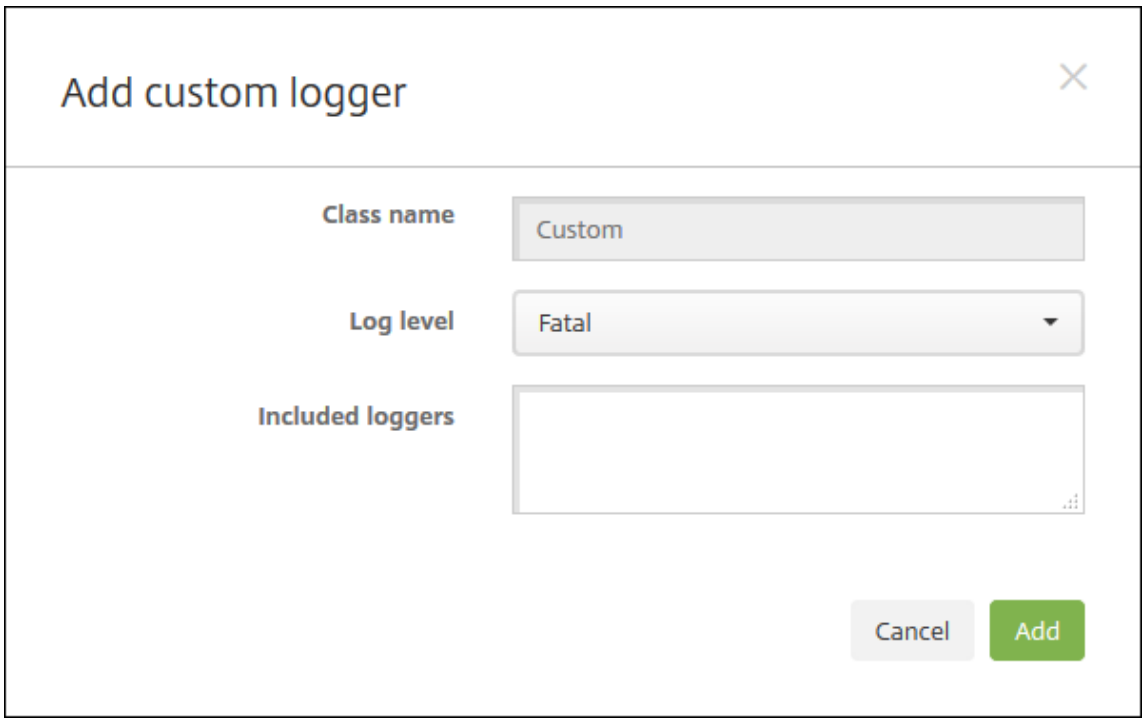
3. Click **Set** to commit your changes.

To add a Custom Logger

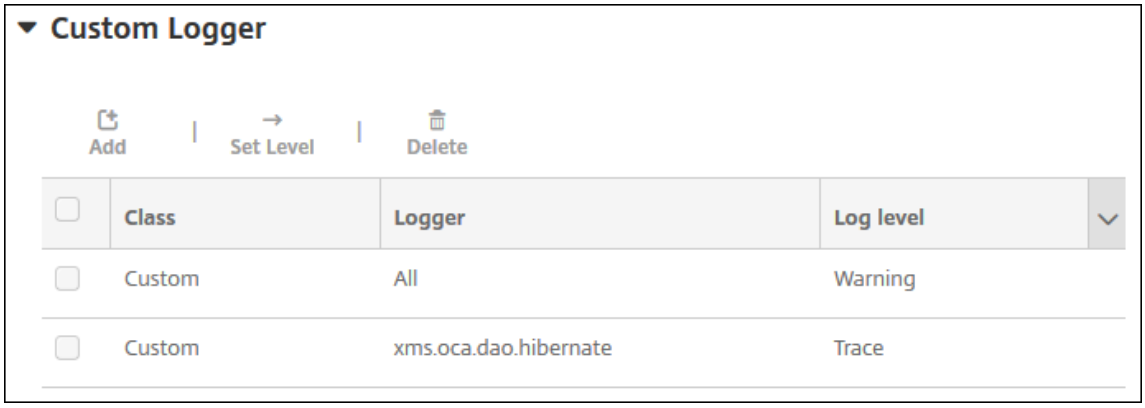
1. On the **Log Settings** page, expand **Custom Logger**. The **Custom Logger** table appears. If you haven't added any custom loggers, the table is initially empty.



2. Click **Add**. The **Add custom logger** dialog box appears.



3. Configure these settings:
   - **Class Name:** This field displays **Custom**; it is not editable.
   - **Log level:** In the list, click a log level. The supported log levels include:
     - Fatal
     - Error
     - Warning
     - Info
     - Debug
     - Trace
     - Off
   - **Included Loggers:** Type the specific loggers you want to include in the custom logger or leave the field blank to include all loggers.
4. Click **Add**. The custom logger is added to the **Custom Logger** table.



To delete a Custom Logger

1. On the **Log Settings** page, expand **Custom Logger**.
2. Select the custom logger you want to delete.
3. Click **Delete**. A dialog box appears asking whether you want to delete the custom logger. Click **OK**.

   > **Important:**
   >
   > You cannot undo this operation.

Mobile Service Provider

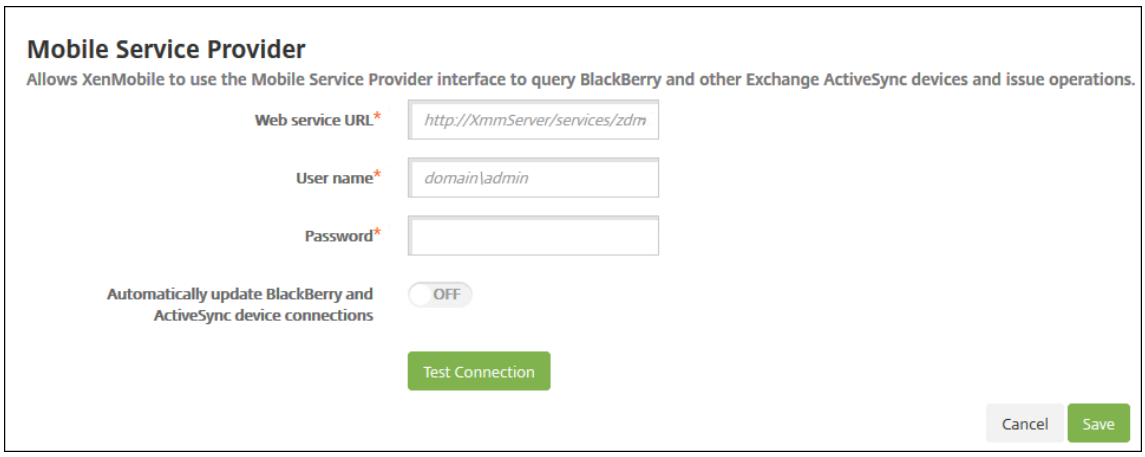
October 4, 2018

You can enable XenMobile to use the Mobile Service Provider interface to query BlackBerry and Exchange ActiveSync devices and issue operations.

For example, your organization may have 1,000 users and each user may use one or more devices. After you communicate to every user that he or she must enroll their devices with XenMobile for management, the XenMobile 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 XenMobile 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.



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

July 23, 2020

XenMobile 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 XenMobile 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 Apps:** Failed Deployment - Lists up to 10 apps that have failed to deploy.
- **Blacklisted Apps by Device & User:** Lists blocked apps that users have on their devices.

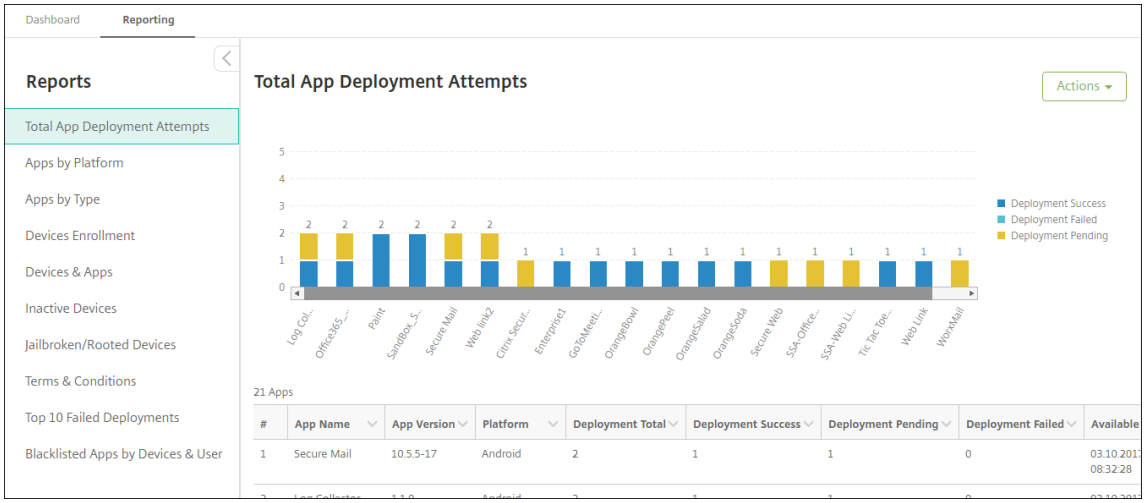
  > **Note:**
  >
  > The XenMobile Server console includes the terms “blacklist” and “whitelist”. We are changing those terms in an upcoming release to “block list” and “allow list”.

- **Non-Compliant Devices:** Lists devices that don’t meet compliance criteria such as whether the device is jailbroken, the OS version running, and if the device has a passcode.

You can export the data in each table in .csv format, which you can open by using programs like Microsoft Excel. You can export the chart for each report in PDF format.

To generate a report

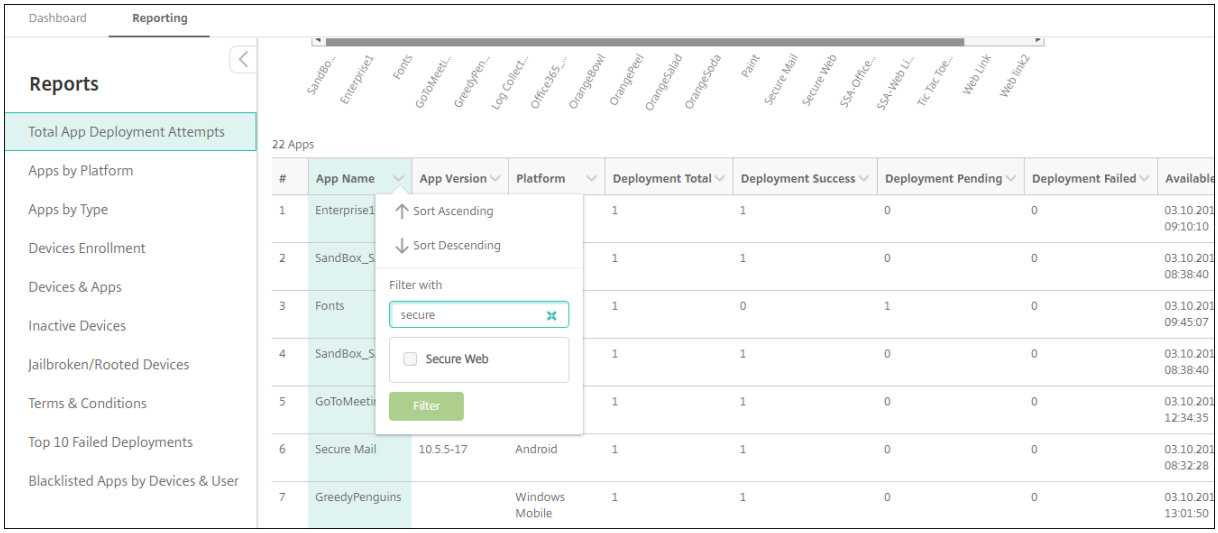
1. In the XenMobile console, click **Analyze > Reporting**. The **Reporting** page appears.
2. Click the report you want to generate.



To view more details of a report

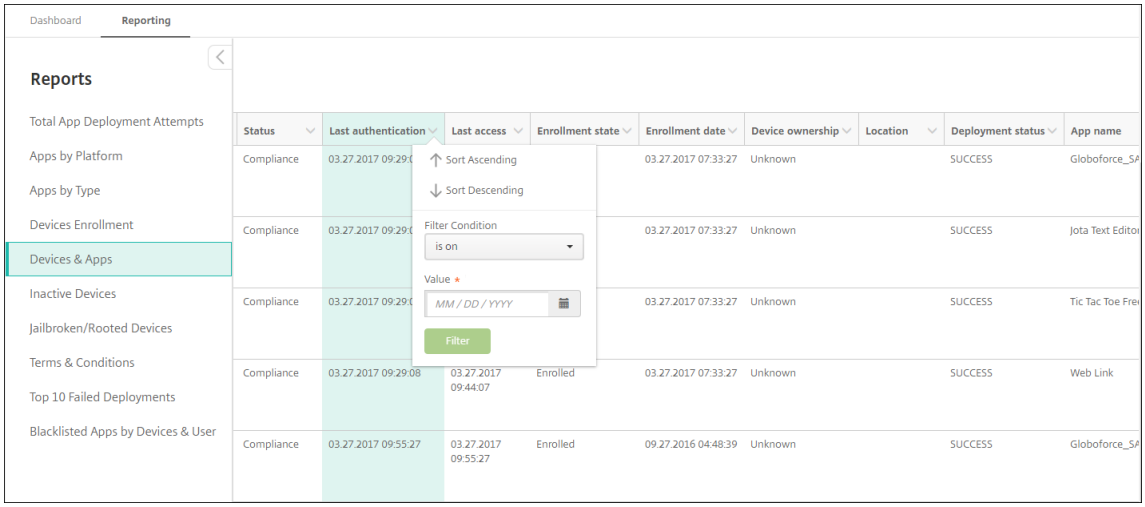
1. Click areas of the chart to drill down and see more details information.

To sort, filter, or search a table column, click the column heading

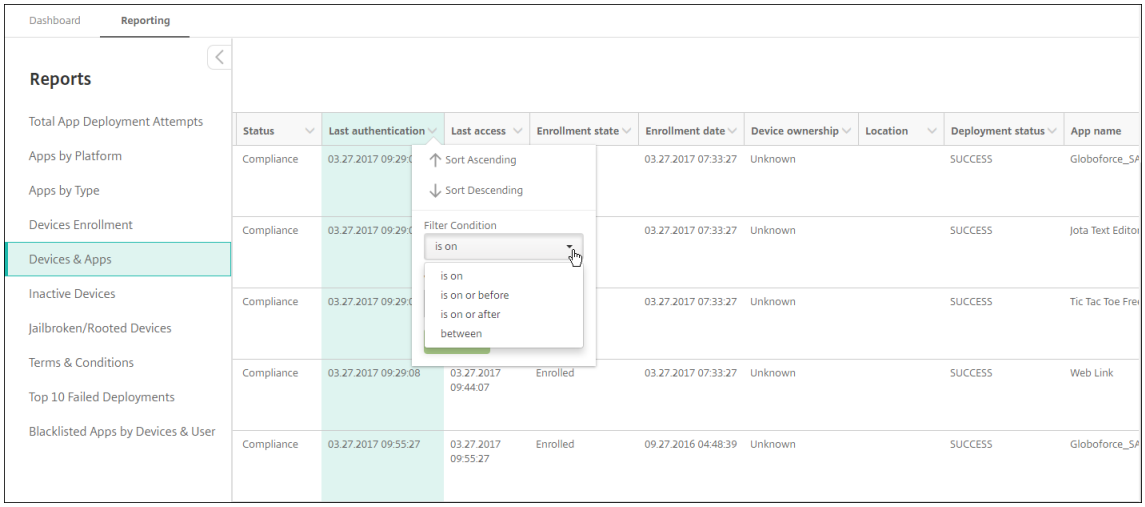


To filter the report by date

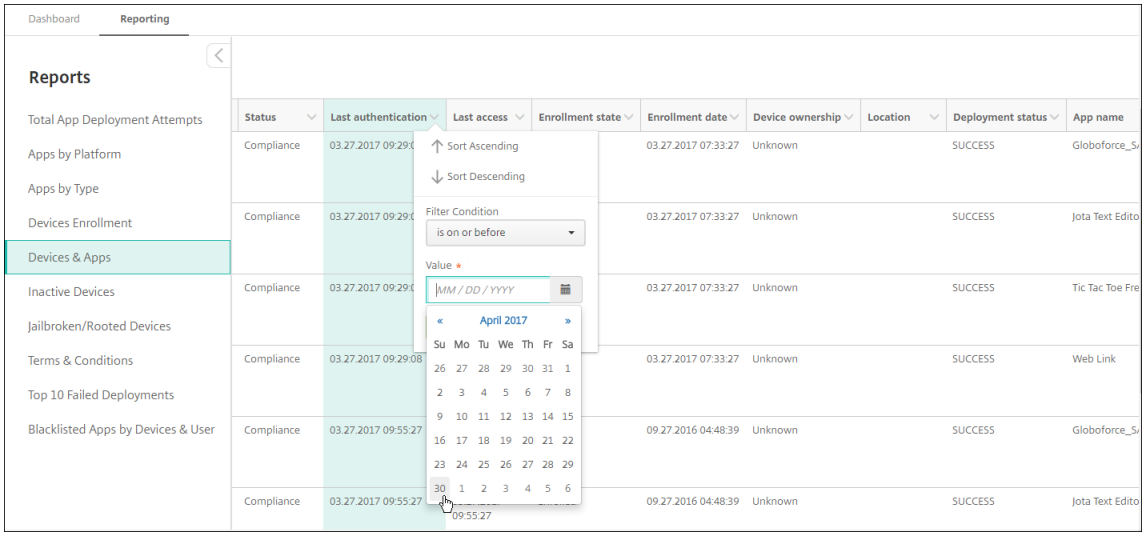
1. Click a column heading to view the filter settings.



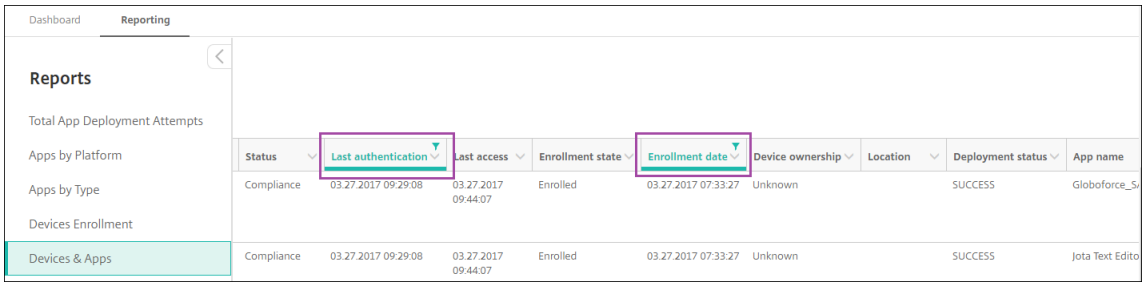
2. From **Filter Condition**, choose how you want to restrict the dates reported.



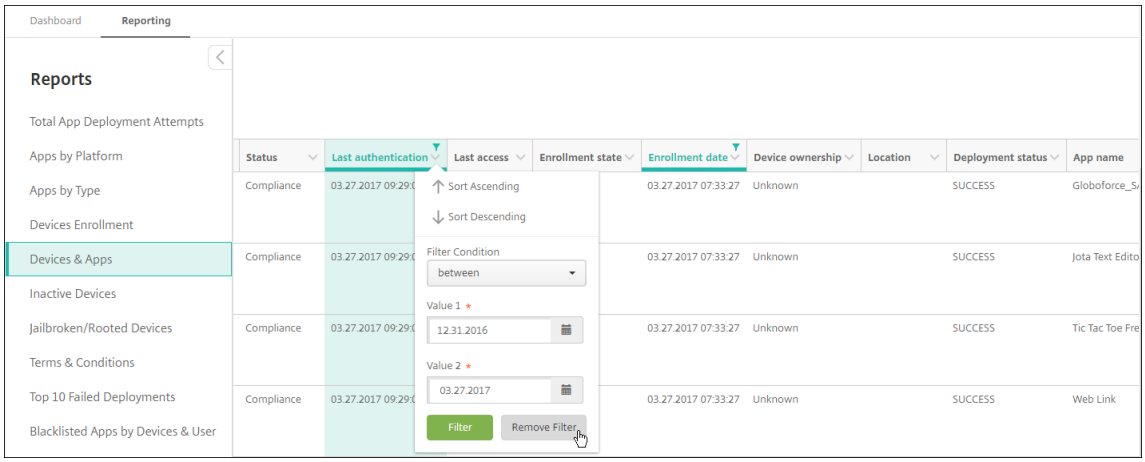
3. Use the date chooser to specify dates.



4. A column with a date filter displays as shown the following example.

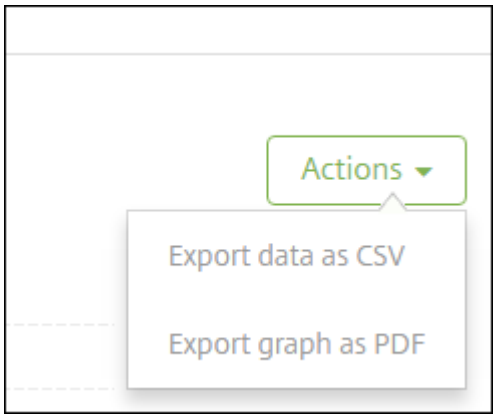


5. To remove a filter, click the column heading and then click **Remove Filter**



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**.



> **Important:**
>
> Although it is possible to use SQL Server to create custom reports, Citrix does not recommend this method. Citrix doesn't publish the schema and can change the schema without notification.

> If you do decide to pursue this method of reporting, ensure that SQL queries are run using a read-only account. Be aware that a query with multiple JOINs that takes some time to run will impact XenMobile Server performance during that time.

SNMP monitoring

April 9, 2020

You can enable SNMP monitoring in XenMobile Server to allow monitoring systems to query and obtain information on your XenMobile nodes. The queries use parameters, such as Processor Load, Load Average, Memory Usage, and Connectivity. For more information about SNMP v3, such as authentication and encryption specifications, see the official SNMP documentation for RFC 3414.

> **Note:**
>
> SNMP v3 monitoring is supported with XenMobile Server 10.8 and later.

You can use various monitoring applications that support SNMP monitoring, such as SCOM. For details about configuring SCOM, see this Citrix Support Knowledge Center article.

Prerequisites

Configure the following TCP ports:

- **Port 161 (UDP):** Used for SNMP traffic using UDP protocol. The source is the SNMP manager and the destination is XenMobile.
- **Port 162 (UDP):** Used for sending SNMP trap alerts to SNMP manager from XenMobile. The source is XenMobile and the destination is the SNMP Manager.

For more information about XenMobile ports configuration, see Port requirements.

To see an architectural diagram of an on-premises XenMobile deployment that includes SNMP, see Reference Architecture for On-Premises Deployments.

The general steps for setting up SNMP are as follows.

1. **Add users:** The users inherit the permission to receive traps and monitor the XenMobile Server.
2. **Add an SNMP Manager to receive traps:** Traps are alerts that XenMobile generates when your XenMobile node exceeds the maximum user-defined threshold.
3. **Configure the SNMP manager to interact with XenMobile:** XenMobile Server uses certain management information bases (MIBs) to perform operations. You download the MIBs from the **Settings > SNMP Configuration** page in the XenMobile console. You then import the MIBs into the SNMP manager by using a MIB importer.

> **Note:**
>
> Every SNMP manager has its own MIB importer.

4. **Enable traps:** You enable traps within the XenMobile console and define the intervals and thresholds based on your environment.
5. **View traps within the third-party SNMP manager:** To view traps, check the SNMP manager. In some managers, however, you can configure settings to enable notifications outside of the manager. You can configure notifications to appear, for example, in email.

You can generate the following traps from XenMobile.

Trap name: Processor load

- **Monitoring object ID (OID):** .1.3.6.1.2.1.25.3.3.1.2
- **Description:** Monitors the CPU load of the system for the user-defined interval. If the load exceeds the custom threshold value, XenMobile generates the SNMP trap.

Trap name: Load average for one minute

- **Monitoring object ID (OID):** .1.3.6.1.4.1.2021.10.1.5.1
- **Description:** Monitors the average system load over a period of one minute for the user-defined interval. If the load average exceeds the custom threshold value, XenMobile generates the SNMP trap.

Trap name: Load average for five minutes

- **Monitoring object ID (OID):** .1.3.6.1.4.1.2021.10.1.5.2
- **Description:** Monitors the average system load over a period of five minutes for the user-defined interval. If the load average exceeds the custom threshold value, XenMobile generates the SNMP trap.

Trap name: Load average for 15 minutes

- **Monitoring object ID (OID):** .1.3.6.1.4.1.2021.10.1.5.3
- **Description:** Monitors the average system load over a period of 15 minutes for every user-defined interval. If the load average exceeds the custom threshold value, XenMobile generates the SNMP trap.

Trap name: Total available memory

- **Monitoring object ID (OID):** .1.3.6.1.4.1.2021.4.11
- **Description:** Monitors the available memory for every user-defined interval. If the available memory falls below the custom threshold value, XenMobile generates the SNMP trap. Note: The total available memory includes both RAM and swap memory (virtual memory). To retrieve total swap memory, you can query using SNMP OID .1.3.6.1.4.1.2021.4.3. To retrieve available swap memory, you can query using SNMP OID .1.3.6.1.4.1.2021.4.4

Trap name: Total used disk storage

- **Monitoring object ID (OID):** .1.3.6.1.4.1.2021.9.1.9.1
- **Description:** Monitors the system disk storage for every user-defined interval. If disk storage exceeds the custom threshold value, XenMobile generates the SNMP trap.

Trap name: Java heap memory usage

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.2.4.0
- **Description:** Monitors the Java virtual machine (JVM) heap memory usage of XenMobile for every user-defined interval. If the usage exceeds the custom threshold value, XenMobile generates the SNMP trap.

Trap name: Java metaspace usage

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.2.5.0
- **Description:** Monitors the Java metaspace usage of XenMobile for every user-defined interval. If the usage exceeds the threshold value, XenMobile generates the SNMP trap.

Trap name: LDAP connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.1.0
- **Description:** Monitors the connectivity between LDAP server and the XenMobile node for every user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: DNS connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.2.0
- **Description:** Monitors the connectivity between DNS server and the XenMobile node for every user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: Google Store server connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.3.0
- **Description:** Monitors the connectivity between Google Store server and the XenMobile node for every user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: Windows Phone Store connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.4.0
- **Description:** Monitors the connectivity between Windows Phone Store server and the XenMobile node for every user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: Windows Tab Store connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.5.0
- **Description:** Monitors the connectivity between Windows Tab Store server and the XenMobile nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: Windows Security Token server connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.6.0
- **Description:** Monitors the connectivity between Windows Security Token server and the XenMobile nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: Windows Notification server connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.7.0
- **Description:** Monitors the connectivity between Windows Notification server and the XenMobile nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: Apple Push Notification server (APNs) connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.8.0
- **Description:** Monitors the connectivity between APNs and the XenMobile nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: Apple Feedback server connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.9.0
- **Description:** Monitors the connectivity between Apple Feedback server and the XenMobile nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: Apple Store server connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.10.0
- **Description:** Monitors the connectivity between Apple Store server and the XenMobile nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: XenMobile database connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.11.0
- **Description:** Monitors the connectivity between XenMobile Database and the XenMobile nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: Firebase Cloud Messaging server connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.12.0
- **Description:** Monitors the connectivity between Firebase Cloud Messaging server and the XenMobile nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: Citrix License Server connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- **Description:** Monitors the connectivity between Citrix License Server and the XenMobile nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: Citrix Gateway connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.15.0
- **Description:** Monitors the connectivity between the Citrix Gateway and XenMobile nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: XenMobile inter-node connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.16.0
- **Description:** Monitors the connectivity between the XenMobile cluster nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

Trap name: XenMobile Tomcat node service connectivity

- **Monitoring object ID (OID):** .1.3.6.1.4.1.3845.5.1.1.18.17.0
- **Description:** Monitors the connectivity between XenMobile Tomcat node service and the XenMobile nodes for the user-defined interval. If connectivity fails, XenMobile generates the SNMP trap.

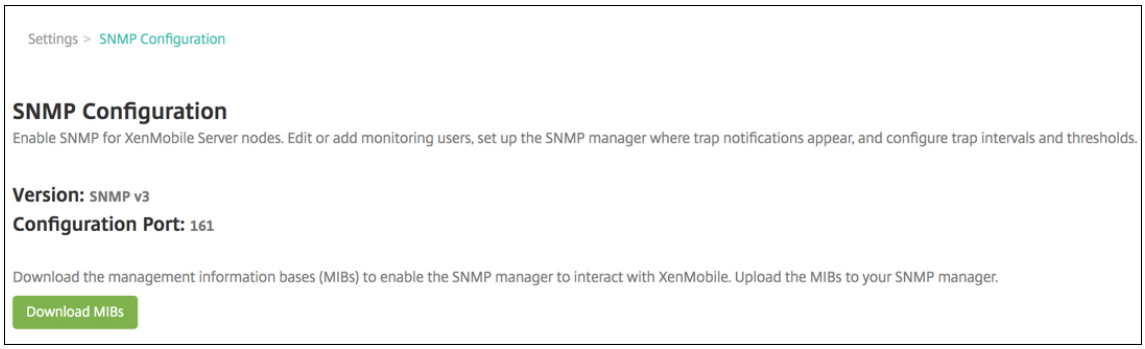
For the best server performance when configuring SNMP thresholds, keep in mind the following factors:

- Frequency of calls
- Trap data to be collected and the threshold checks
- The inter-node communication mechanism
- Frequency of connectivity checks
- Timeouts on any failure during the checks

To add SNMP users

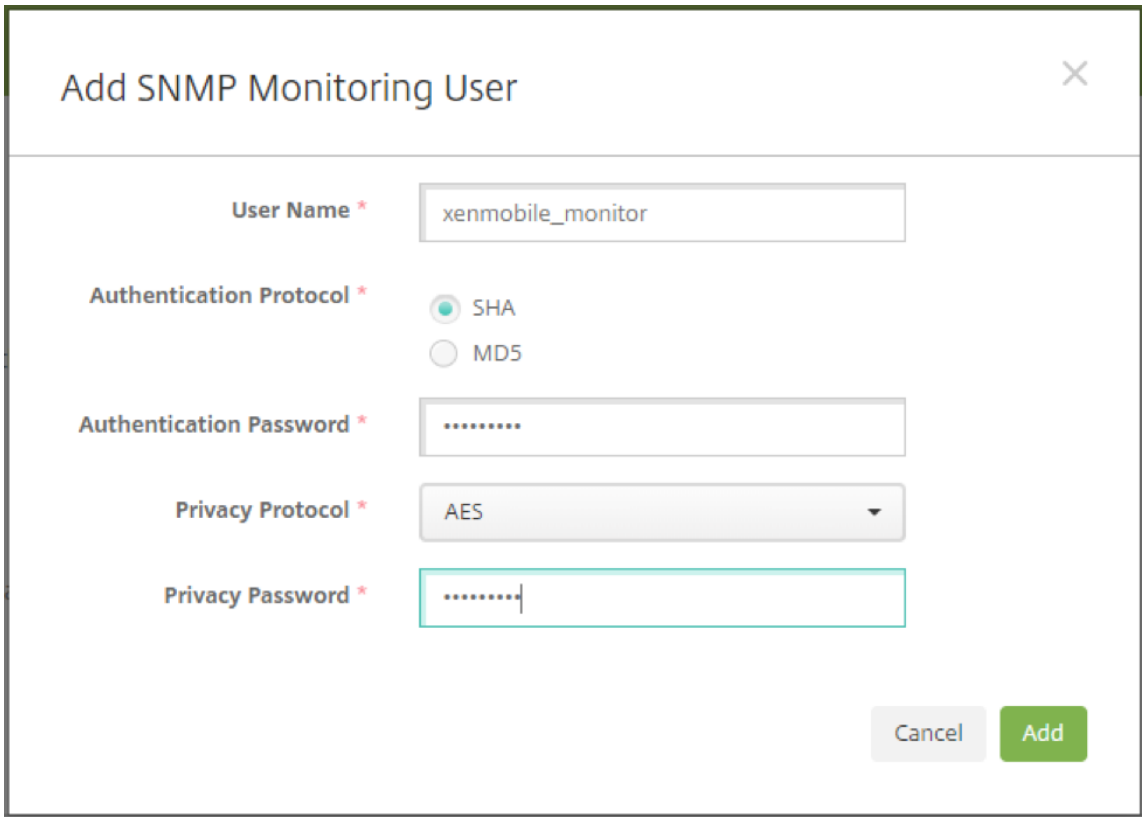
SNMP users interact with SNMP managers and receive traps.

1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Monitoring**, click **SNMP Configuration**. The **SNMP Configuration** page appears.



3. Under **SNMP Monitoring Users**, click **Add**.

4. In the **Add SNMP Monitoring User** dialog box, configure the following settings:



User Name: The user name used to log on to the SNMP manager. Although you can use alphanumeric characters, underscore and hyphens, you cannot use spaces and other special characters for your user name.

> **Note:**
>
> You cannot add the user name “xmsmonitor” because XenMobile reserves the name for internal use.

Authentication Protocol:

- **SHA** (Recommended)
- **MD5**

Authentication Password: Type an 8- to 18-character password. You can include alphanumeric and special characters.

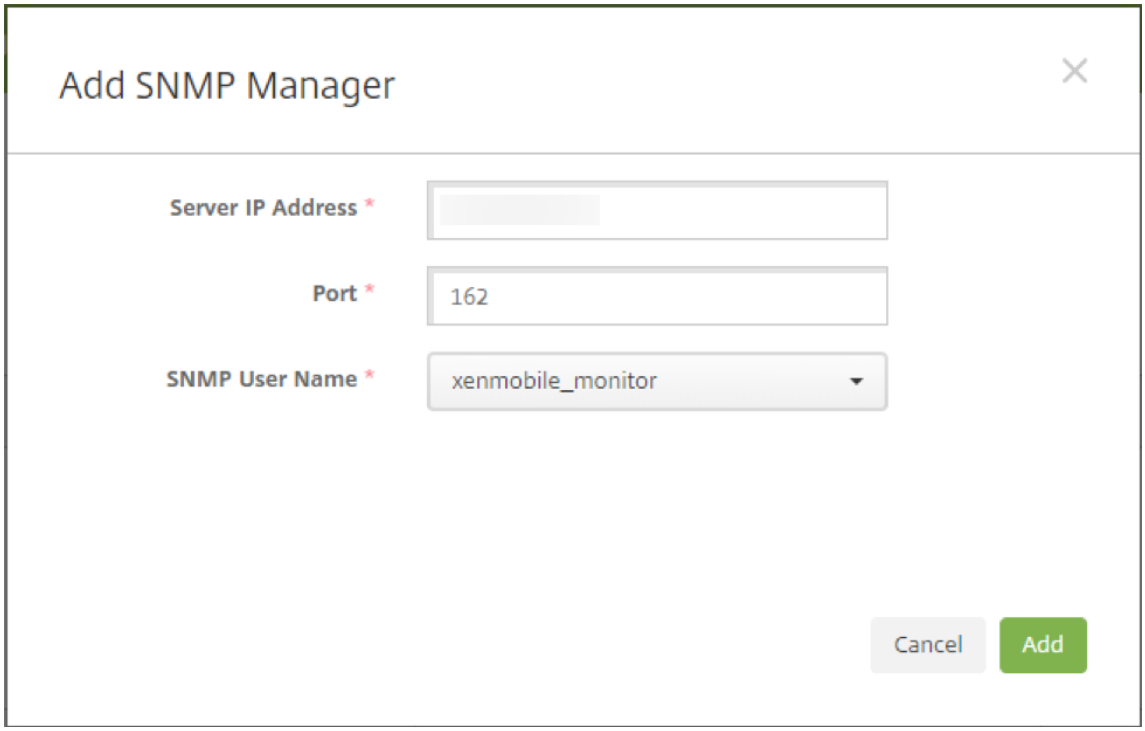
Privacy Protocol:

- **DES**
- **AES 128** (Recommended)

Privacy Password: Type an 8- to 18-character password. You can include alphanumeric and special characters.

To add an SNMP manager

1. Under **SNMP Managers**, click **Add**.
2. In the **Add SNMP Manager** dialog box, configure the following settings:



Server IP Address: Type the IP address of the SNMP manager.

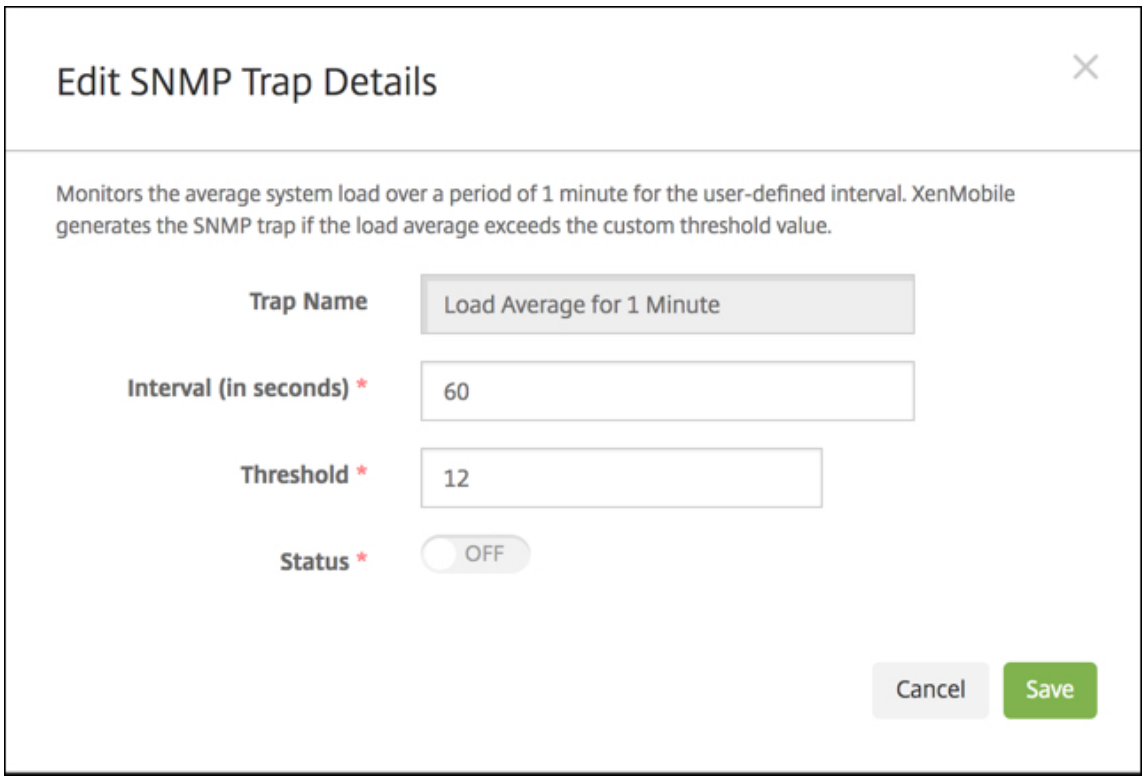
Port: Change the port number if needed. Default is 162.

SNMP User Name: Select the name of a user with access to the manager.

To enable and configure SNMP traps

To help determine the appropriate trap settings for your environment, see Scalability and performance. For example, to monitor the XenMobile Load Average for one minute, you can enable Load Average for 1 Minute and provide a threshold value. If the XenMobile Server Load Average for 1 Minute exceeds the specified threshold, you receive a trap in the configured SNMP managers.

1. To enable individual traps, do one of the following:
   - Select the check box next to the parameter and then, click **Enable**.
   - To enable all the traps in the list, select the check box at the top and then click **Enable**.
2. To edit a trap, select the parameter and then click **Edit**.
3. In the **Edit SNMP Trap Details** dialog box, you can edit the threshold values for individual traps.



Trap Name: The name of the trap. You cannot edit this field.

Interval (in seconds): The range allowed is from 60 to 86400 (24 hours).

Threshold: You can change the threshold only for the following traps:

- Processor Load
- Load Average for 1 Minute
- Load Average for 5 Minutes
- Load Average for 15 Minutes
- Total Available Memory
- Total Used Disk Storage
- Java Heap Memory Usage
- Java Metaspace Usage

Status: Select **ON** to enable SNMP monitoring for the trap. Select **OFF** to disable monitoring.

For more helpful information on monitoring XenMobile using SNMP, see this blog post.

Support bundles

November 19, 2020

To report an issue to Citrix or troubleshoot a problem, create a support bundle. Then, upload the support bundle to Citrix Insight Services (CIS).

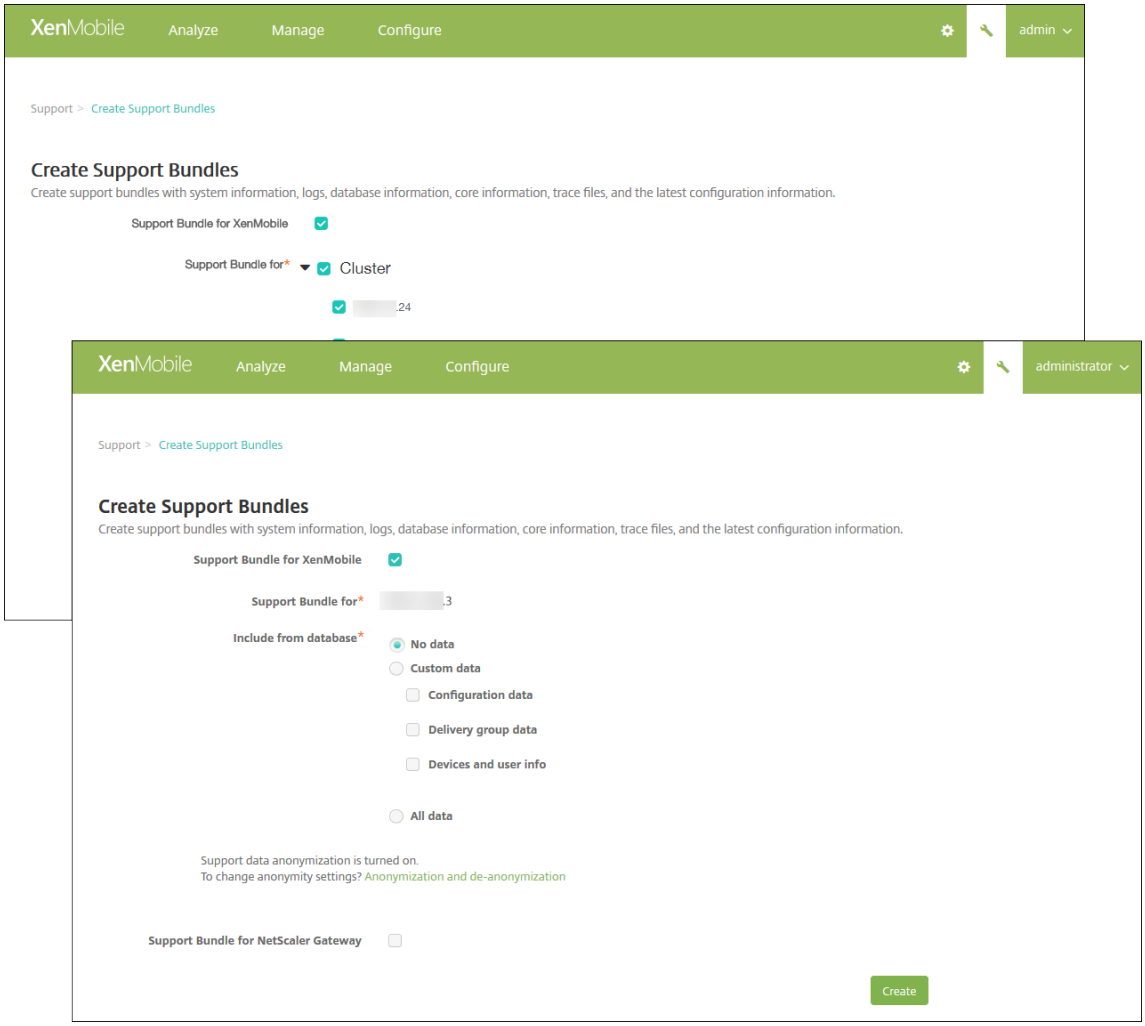
By default, a support bundle includes a maximum of 100 backup archives of the following files. The default file size for these files is 10 MB.

- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

When the support bundle includes 100 log archive files for each of those categories, the log file rolls over. If you configure a lower maximum number of log files, XenMobile immediately deletes the extraneous log files for that node. To configure the number of log files, go to **Troubleshooting and Support > Log Settings**.

To create a support bundle:

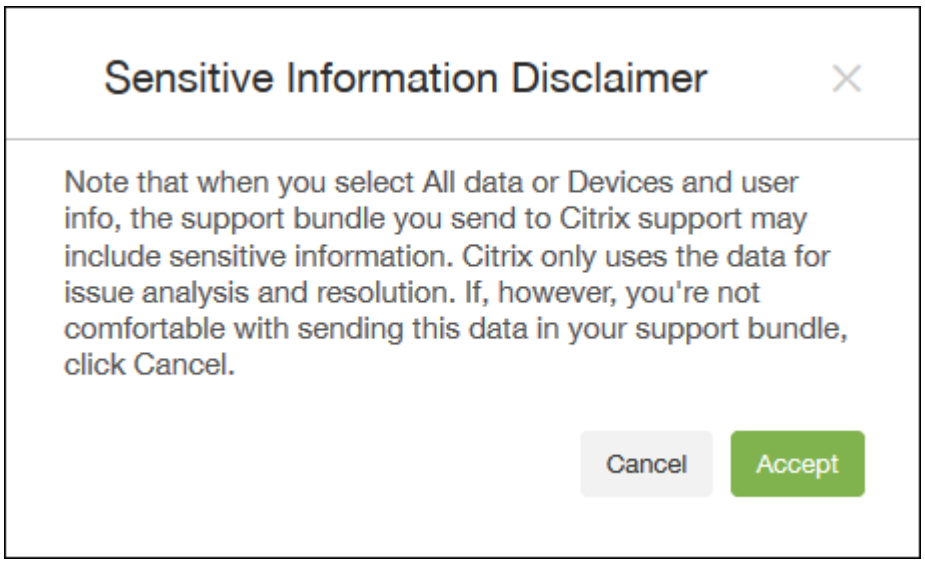
1. In the XenMobile console, click the wrench icon in the upper right corner. The **Support** page appears.
2. On the **Support** page, click **Create Support Bundles**. The **Create Support Bundles** page appears. If your XenMobile environment contains clustered nodes, all nodes are shown.



3. Ensure that the **Support Bundle for XenMobile** check box is selected.
4. If your XenMobile environment contains clustered nodes, in **Support Bundle for**, you can select all the nodes or any combination of nodes from which to draw data.
5. In **Include from database**, do one of the following:
   - Click **No data**.
   - Click **Custom data**. By default, all these options are selected.
     - **Configuration data:** Includes certificate configurations and device manager policies.
     - **Delivery group data:** Includes app delivery group information, containing app types and app delivery policy details.
     - **Devices and user info:** Includes device policies, apps, actions, and delivery groups.
   - Click **All data**.

> **Note:**
>
> If you choose **Devices and user info** or **All data**, and this is the first support bundle you

> have created, the **Sensitive Information Disclaimer** dialog box appears. Read the disclaimer and then click **Accept** or **Cancel**. If you click **Cancel**, the support bundle cannot be uploaded to Citrix. If you click **Accept**, you can upload the support bundle to Citrix and you will not see the disclaimer the next time you create a support bundle that includes device or user data.

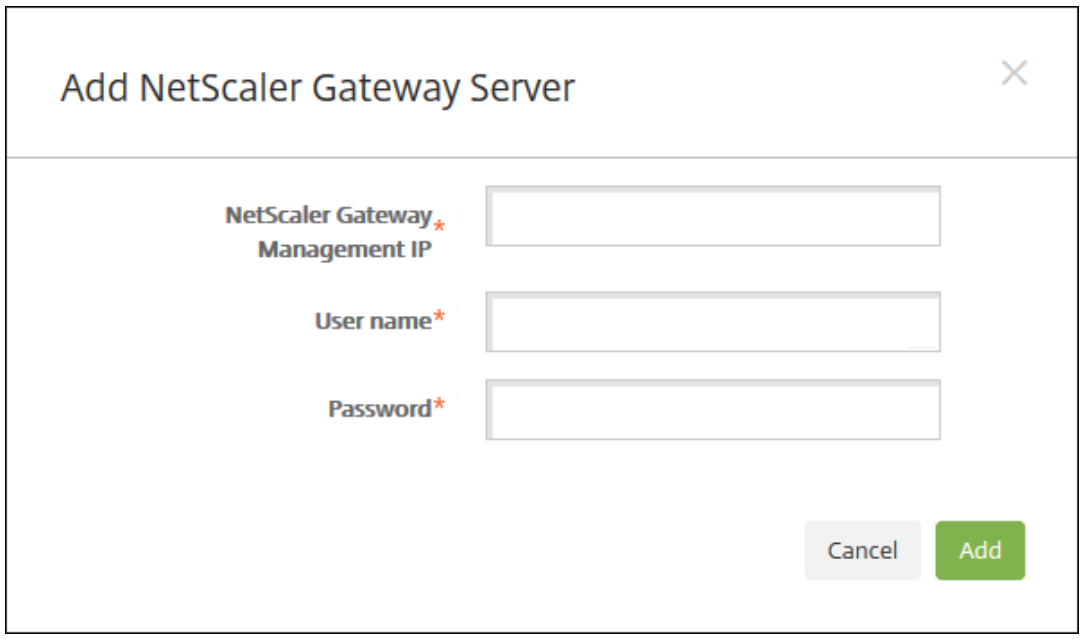


6. The option, **Support data anonymization is turned on**, indicates that the default setting is to anonymize the data. Data anonymization means that sensitive user, server, and network data is made anonymous in support bundles.

   To change this setting, click **Anonymization and de-anonymization**. For more information about data anonymization, see Anonymizing data in support bundles.

7. To include support bundles from Citrix Gateway: Select the **Support Bundle for Citrix Gateway** check box and then do the following:

   a) Click **Add**. The **Add Citrix Gateway Server** dialog box appears.



b) In **Citrix Gateway Management IP**, type the Citrix ADC management IP address for the Citrix Gateway from which you want to draw your support bundle data.

> **Note:**
>
> If you are creating a bundle from a Citrix Gateway server that is already added, the IP address is provided.

c) In **User name** and **Password**, type the user credentials required to access the server running Citrix Gateway.

> **Note:**
>
> If you are creating a bundle from a Citrix Gateway server that is already added, the user name is provided.

8. Click **Add**. The new Citrix Gateway support bundle is added to the table.
9. Repeat Step 7 to add more Citrix Gateway support bundles.
10. Click **Create**. The support bundle is created and two new buttons, **Upload to CIS** and **Download to Client**, appear.

Uploading Support Bundles to Citrix Insight Services

After creating a support bundle, you can upload the bundle to Citrix Insight Services (CIS) or download the bundle to your computer.

The upload from XenMobile to CIS is through an SSL outbound connection. Open port 443 to the CIS server IP address (52.88.24.76, 52.88.118.220, 52.11.72.119). If you have a proxy for HTTPS traffic,

verify that the proxy can reach the CIS server IP address.

These steps show you how to upload the bundle to CIS. You need a My Citrix ID and password to upload to CIS.

1. On the **Create Support Bundles** page, click **Upload to CIS**. The **Upload to Citrix Insight Services (CIS)** dialog box appears.
2. In **User Name**, type your My Citrix ID.
3. In **Password**, type your My Citrix password.
4. If you want to connect this bundle with an existing service request number, select the **Associate with SR#** check box and in the two new fields that appear, do the following:
   - In **SR#**, type the eight-digit service request number you want to associate this bundle with.
   - In **SR Description**, type a description of the SR.
5. Click **Upload**.

   If this is the first time you have uploaded a support bundle to CIS, and you haven't created an account on CIS through another product and accepted the Data Collection and Privacy agreement, the following dialog box appears; you must accept the agreement before the upload can begin. If you have an account on CIS and have previously accepted the agreement, the support bundle is uploaded immediately.

6. Read the agreement and then click **Agree and upload**. The support bundle is uploaded.

Downloading support bundles to your computer

After you create a support bundle, you can upload the bundle to CIS or download the bundle to your computer. If you would like to troubleshoot the problem on your own, download the support bundle to your computer.

On the Create Support Bundles page, click Download to Client. The bundle is downloaded to your computer.

The support bundle contains files of varying analytical value. See the following table for a list of files and their analytical value.

File Name	Type	Description	Value
DbDump.json	JSON Database Dump	Users/Devices/Applicat information	High
Garbage.html	HTML file	Java garbage collector	Low
MemoryInfo.html	HTML file	Memory usage- java related memory usage	High
MultiNodeClusterInfo.html	HTML file	Cluster configuration	High
Patches.html	HTML file	Patch information. Better to xmspatches.txt	High
pg_dump0.sql	PG Dump	Default Postgress instance dump	Medium
rt_db/*	DB Copy (redundent, this is a binary representation of pg_dump0.sql)		N/A
sas_config/c3p0.properties	Properties file	C3P0 DB Config properties	Medium
sas_config/catalina.pol	policy file	Web Server Catalina policies - Files don’t change	Low
sas_config/catalina.properties	Properties file	Web Server Catalina properties - Files don’t change	Low

File Name	Type	Description	Value
sas_config/ew-config.properties	Properties file	Information on the configuration of the XM server	High
sas_config/ew-config-reloadable.properties	Properties file	Security model information	High
sas_config/hazelcast.xr	XML File	Hazelcast logs - Don’t think would be much use.	Low
sas_config/pki.xml	XML File	Could be used to determine if 3rd party PKI server in use.	High
sas_config/push_servic	XML File	Push Services - Files don’t change	Low
sas_config/server.xml	XML File	Cipher information in here - Security related	High
sas_config/sftu_config/	Properties file	AppC Properties - Files don’t change	Low
sas_config/sftu_config/catalina.policy	catalina.policy	Catalina Policies - Files don’t change	Low
sas_config/sftu_config/	Properties file	Catalina Properties - Files don’t change	Low
sas_config/sftu_config/logging.properties	Properties file	Logging Properties - Files don’t change	Low
sas_config/sftu_config/	XML File	Cipher information in here - Security related	High
sas_config/sftu_config/sftu_migration.xml	XML File	Migration information	High
sas_config/sftu_config/	XML File	First time user settings	High
sas_config/sftu_config/tomcat-users.xml	XML File	TomCat Users - Files don’t change	Low
sas_config/sftu_config/	XML File	Web - Files don’t change	Low
sas_config/sftu.properties	Properties file	SFTU config properties	High

File Name	Type	Description	Value
sas_config/variables.xn	XML File	Variables - Files don’t change	Low
sas_config/web.xml	XML File	Webserver related information	Medium
sas_log/AdminAuditLo	Linux Log File	Any configuration changes	High
sas_log/create_sb_output.sh	Linux Log File	Support generation command output	Low
sas_log/DebugLogFile.l	Linux Log File	All features log	High
sas_log/HibernateStats.log	Linux Log File	Hibernatestats log	Low
sas_log/kafka-consumer.log	Linux Log File	Kafka log	Low
sas_log/kafka-server.log	Linux Log File	Kafka log	Low
sas_log/kafka-topics.log	Linux Log File	Kafka log	Low
sas_log/LPE.log	Linux Log File	LPE log	Low
sas_log/migration.log	Linux Log File	Migration process output	Medium
sas_log/PlatformAuditLogFile.log	Linux Log File	Backend audit level information	High
sas_log/PlatformDebu	Text file	Backend server related logs	High
sas_log/postgres.log	Linux Log File	PostGres logs	Medium
sas_log/SFTU.log	Linux Log File	SFTU log	Medium
sas_log/tc1/catalina.log	Linux Log File	Catalina log	Low
sas_log/tc1/console	Linux Log File	Console	Low
sas_log/tc1/host-manager.log	Linux Log File	Host Manager	Low
sas_log/tc1/localhost.l	Linux Log File	LocalHost	Low
sas_log/updates.log	Linux Log File	Patching process output	Medium

File Name	Type	Description	Value
sas_log/UserAuditLogF	Linux Log File	User actions	High
sas_log/zookeeper.txt	Text file	Zookeeper log	Low
snmp/snmpd_etc_nets	Properties file	SNMP config properties	Low
snmp/snmpd_privileges.conf	Properties file	SNMP config properties	Low
sys_info/arp_entries.txt	Text file	ARP entris in the XMS Server	Medium
sys_info/chrony.txt	Text file	Chrony log	Low
sys_info/diskspace_usa	Text file	Disk space usage	High
sys_info/firewall_rules.txt	Text file	Firewall rules defined in XMS	Medium
sys_info/interface_conf	Text file	System command output	Medium
sys_info/net_connections.txt	Text file	System command output	Medium
sys_info/root_account_	Text file	System command output	Medium
sys_info/routing_table.txt	Text file	High value	High
sys_info/running_proce	Text file	High value	High
sys_info/top.txt	Text file	System command output	Medium
ThreadDump.html	HTML file	No longer used.	Low
ThreadDumpV2.html	HTML file	Thread stack traces etc	Medium
var_log/auth.log	Linux Log File	OS Level log	Medium
var_log/boot.log	Linux Log File	OS Level log	Medium
var_log/btmp	Linux Log File	OS Level log	Medium
var_log/daemon.log	Linux Log File	OS Level log	Medium
var_log/kern.log	Linux Log File	OS Level log	Medium
var_log/lastlog	Linux Log File	OS Level log	Medium

File Name	Type	Description	Value
var_log/mail.log	Linux Log File	OS Level log	Medium
var_log/sys.log	Linux Log File	OS Level log	Medium
var_log/user.log	Linux Log File	OS Level log	Medium
var_log/wtmp	Linux Log File	OS Level log	Medium
version.txt	text file	Version of XM server	Medium
XENMOBILE-<IP Address>-ConnectivityCheckResults.xml	XML file	Connectivity Check results on XMS server	Medium
xmspatches.txt	Text file	Patch information.	High

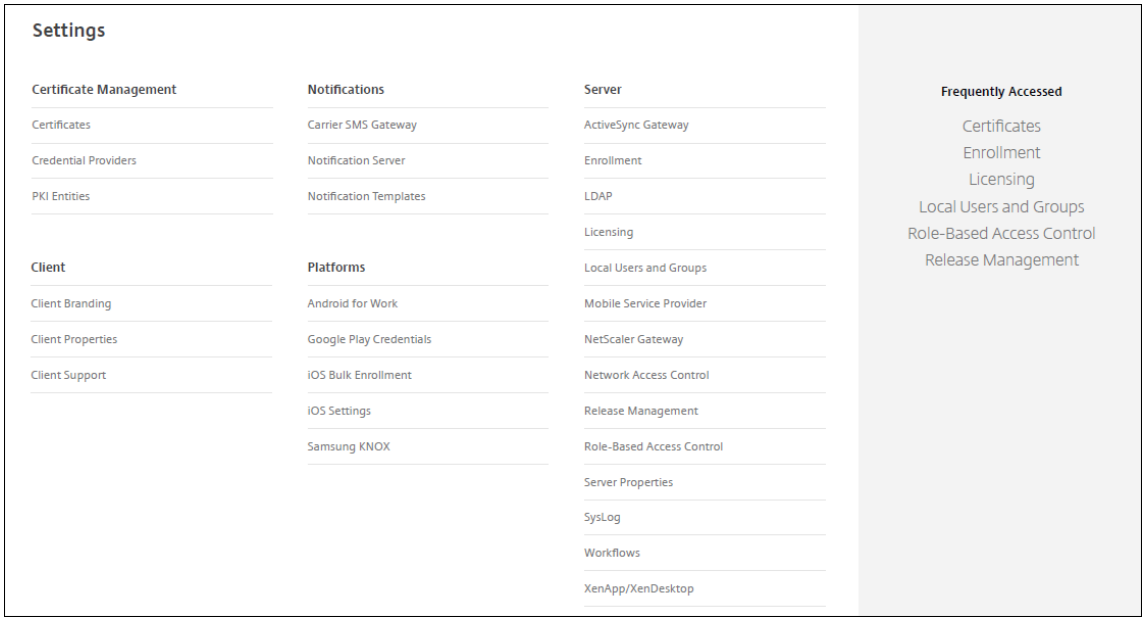
Support options and Remote Support

April 7, 2020

You can provide an email address for users to contact support staff. When users request assistance from their devices, they see the email address.

You can also configure how users send logs to the help desk from their devices. You can configure the logs to be sent directly or by email.

1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.



2. Under **Client**, click **Client Support**. The **Client Support** page appears.
3. Configure the following settings:
   - **Support email (IT help desk):** Type the email address for your IT help desk contact.
   - **Send device logs to IT help desk:** Select whether device logs are sent **directly** or **by email**. The default is **by email**.
     - When you enable **directly**, settings for Store logs on ShareFile (now called Citrix Content Collaboration) appear. If you enable Store logs on Citrix Content Collaboration, logs are sent directly to Citrix Files. Otherwise, the logs are sent to XenMobile and then emailed to the help desk. In addition, the **If sending directly fails, use email** option appears, which is enabled by default. You can disable this option when you do not want to use the client email to send the logs for a server problem. When, however, you disable this option and a server problem occurs, the logs are not sent.
     - When you enable **by email**, the client email is always used to send the logs.
4. Click **Save**.

Remote Support

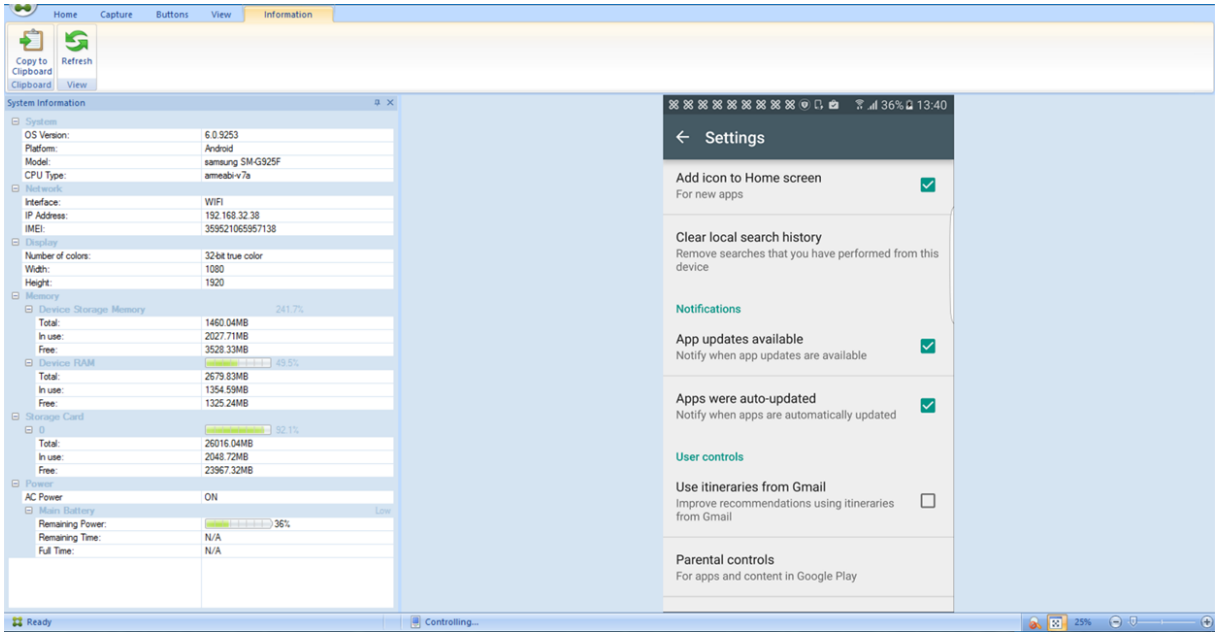
> **Note:**
>
> Remote Support is no longer available for new customers as of January 1, 2019. Existing customers can continue to use the product, however Citrix won't provide enhancements or fixes.

For on-premises XenMobile Server deployments: Remote support enables your help desk representatives to take remote control of managed Windows CE and Android mobile devices. Screen cast is supported on Samsung Knox devices only.

Remote support isn't available for clustered on-premises XenMobile Server deployments.

During a remote control session:

- Users see on their mobile device an icon indicating a remote control session is active.
- Remote Support users see the Remote Support application window and a Remote Control window that shows a rendering of the controlled device.



By using Remote Support, you can do the following:

- Remotely sign on to a user device and control the screen. Users can watch you navigate their screen, which can also be helpful for training purposes.
- Navigate and repair a remote device in real time. You can change configurations, troubleshoot operating system issues, and disable or stop problematic apps or processes.
- Isolate and contain threats before they spread to other mobile devices by remotely disabling network access, stopping rogue processes, and removing apps or malware.
- Remotely enable the device ringer and call the phone, to help the user to locate the device. When a user can't find the device, you can wipe it to ensure that your sensitive data is not compromised.

Remote Support also enables support personnel to:

- Display a list of all connected devices within one or more instances of XenMobile.
- Display system information including device model, operating system level, International Mobile Station Equipment Identity (IMEI), serial number, memory and battery status, and connectivity.
- Display the users and groups for XenMobile.
- Run the device task manager where you can display active processes, end active processes, and restart the mobile device.

- Run remote file transfer that includes bidirectional file transfer between mobile devices and a central file server.
- Download and install software programs as a batch to one or more mobile devices.
- Configure remote registry key settings on the device.
- Optimize response time over low-bandwidth cellular networks by using real-time device screen remote control.
- Display the device skin for most mobile device brands and models. Display a skin editor to add new device models and map physical keys.
- Enable device screen capture, record, and replay with the ability to capture a sequence of interactions on the device that creates a video AVI file.
- Conduct live meetings by using a shared whiteboard, VoIP-based voice communications and chat among mobile users and support personnel.

Remote Support System Requirements

The Remote Support software installs on Windows-based computers which meet the following requirements. For port requirements, see Port Requirements.

Supported platforms:

- Intel Xeon/Pentium 4 -1 GHz minimum Workstation class
- 512-MB RAM minimum
- 100-MB free disk space minimum

Supported operating systems:

- Microsoft Windows 2003 Server Standard Edition or Enterprise Edition SP1 or later
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 or later
- Microsoft Windows Vista SP1 or later
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

To install Remote Support from the command line

Run the following command:

```
1 *RemoteSupport*.exe /S
```

RemoteSupport is the name of the installation program. For example:

```
1 XenMobileRemoteSupport-9.0.0.35265.exe /S
```

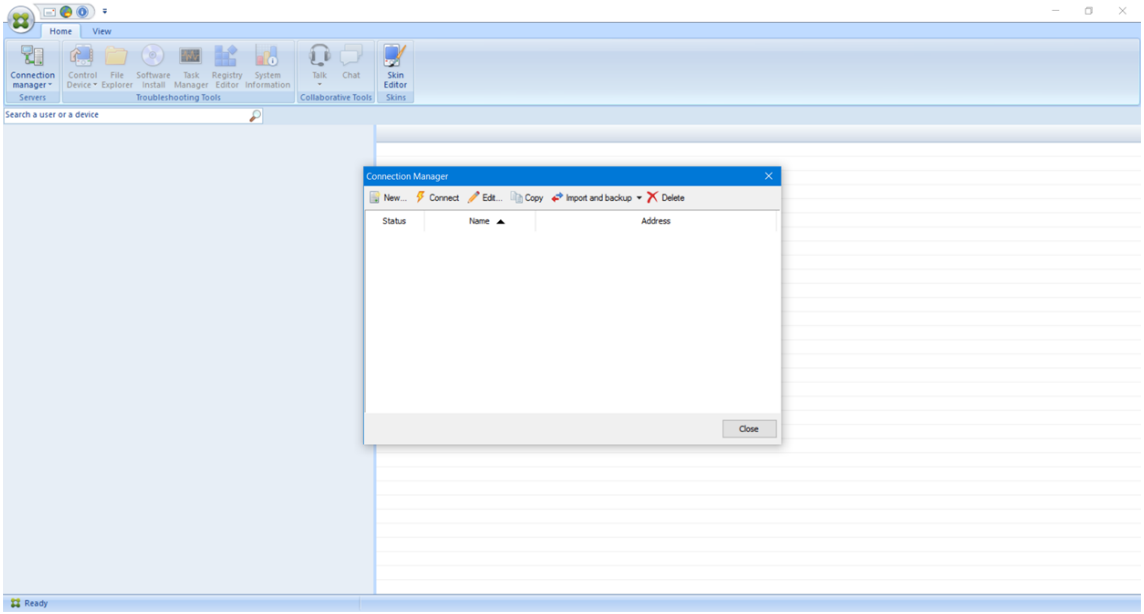

You can use the following variables when installing the Remote Support software:

- /S: to install the Remote Support software silently with the default parameters.
- /D=dir: to specify a custom installation directory.

To connect Remote Support to XenMobile

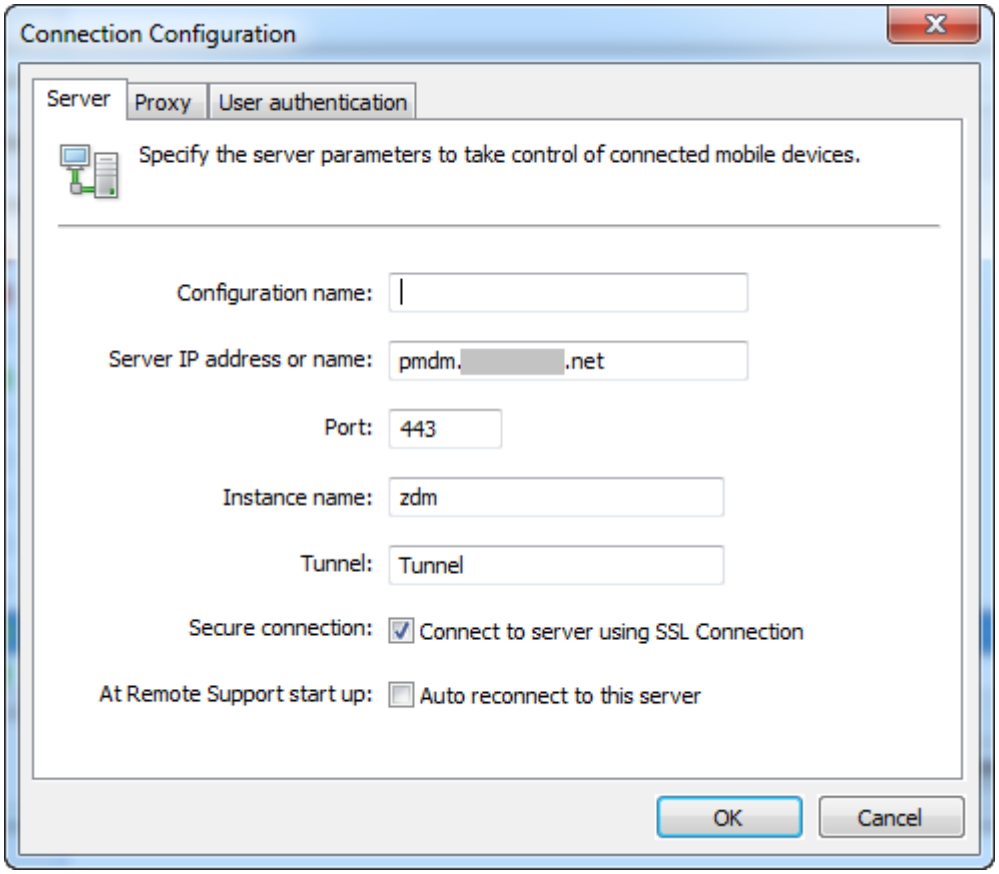
To establish remote support connections to managed devices, you must add a connection from Remote Support to one or more XenMobile Servers that manage the devices. That connection runs over an app tunnel that you define in the Tunnel MDM policy, a device policy for Android and Windows Mobile/CE devices. Define the app tunnel before you can connect Remote Support to XenMobile. For details, see App tunneling device policies.

1. Start the Remote Support software and use your XenMobile credentials to sign on.
2. In **Connection Manager**, click **New**.



3. In the **Connection Configuration** dialog box, on the **Server** tab, type the following values:
   a) In **Configuration name**, type a name for the configuration entry.
   b) In **Server IP address or name**, type the IP address or the DNS name of the XenMobile Server.
   c) In **Port**, type a TCP port number, as defined in the XenMobile Server configuration.
   d) In **Instance name**, when XenMobile is part of a multitenant deployment, type an instance name.
   e) In **Tunnel**, type the name of the Tunnel policy.
   f) Select the **Connect to server using SSL Connection** check box.

g) Select the **Auto reconnect to this server** check box to connect to the configured XenMobile Server each time the Remote Support application starts.



4. On the **Proxy** tab, select **Use an http proxy server** and then type the following information:

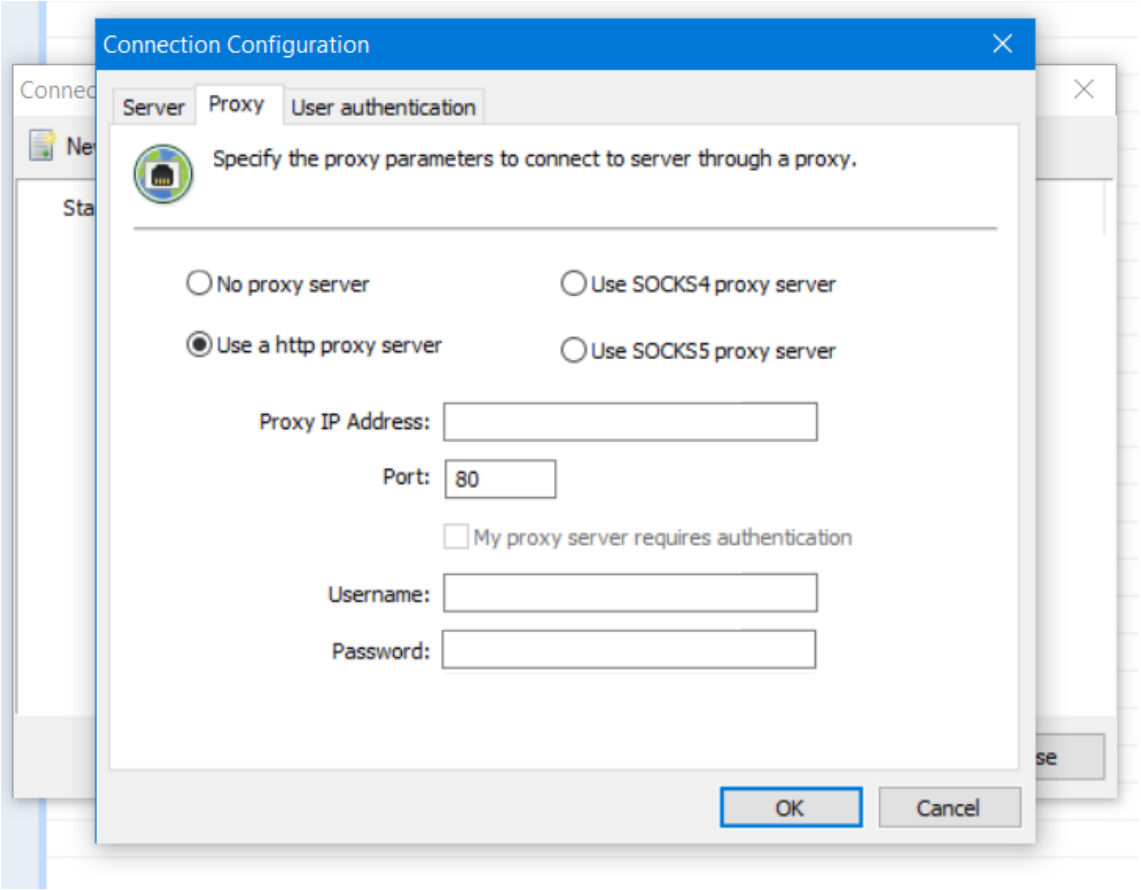
   a) In **Proxy IP Address**, type the IP address of the proxy server.

   b) In **Port**, type a TCP port number used by the proxy.

   c) Select the **My proxy server requires authentication** check box when the proxy server requires authentication to allow traffic.

   d) In **Username**, type the user name to be authenticated on the proxy server.

   e) In **Password**, type the password to be authenticated on the proxy server.



5. On the **User Authentication** tab, select the **Remember my login and password** check box and enter the credentials.
6. Click **OK**.

To connect to XenMobile, double-click the connection you created and then enter the user name and password you configured for the connection.

To enable remote support for Samsung Knox devices

You create a Remote Support policy in XenMobile to give you remote access to Samsung Knox devices. You can configure two types of support:

- **Basic:** Lets you view diagnostic information about the device. For example, system information, processes that are running, task manager (memory and CPU usage), and installed software folder contents.
- **Premium:** Lets you remotely control the device screen. For example, control window colors, establish a VoIP session between the help desk and user, and establish a chat session between the help desk and user.

  Premium support requires that you configure the Samsung MDM License Key device policy in the

XenMobile console. When you configure this policy, select the **Samsung KNOX** platform only. For the Samsung SAFE platform, the ELM key automatically deploys on Samsung devices when they enroll in XenMobile. Therefore, don't select the Samsung SAFE platform for this policy. For details, see Samsung MDM license key.

For information about configuring the Remote Support Policy, see Remote support device policy.

To use a Remote Support session

After you start Remote Support, the left-side of the Remote Support application window presents XenMobile user groups as you defined in the XenMobile console. By default, only groups containing users who are currently connected appear. You can see the device for each user next to the user entry.

1. To see all users, expand each group from the left column.
   Those users currently connected to the XenMobile Server are indicated with a green icon.
2. To display all users, including those not currently connected, click **View** and select **Non-connected devices**.
   Non-connected users appear without the small green icon.

Devices connected to the XenMobile Server but not assigned to a user appear in Anonymous mode. (The string **Anonymous** appears in the list.) You can control these devices just like the device of a logged-in user.

To control a device, select the device by clicking its row and then clicking **Control Device**. A rendering of the device appears in the Remote Control window. You can interact with a controlled device in the following ways:

- Control the device screen, including control with colors, in either the main window, or in a separate, floating window.
- Establish a VoIP session between the help desk and the user. Configure VoIP settings.
- Establish a chat session with the user.
- Access the device task manager, to manage items such as memory usage, CPU usage, and running apps.
- Explore the mobile device local directories. Transfer files.
- Edit the device registry on Windows mobile devices.
- Display device system information and all installed software.
- Update the mobile device connection status with the XenMobile Server.

SysLog

September 17, 2020

You can configure XenMobile Server (on-premises only) to send log files to a systems log (syslog) server. You need the server host name or IP address.

Syslog is a standard logging protocol with two components: an auditing module (which runs on the appliance) and a server, which can run on a remote system. The Syslog protocol uses the user data protocol (UDP) for data transfer. Admin events and User events are recorded.

You can configure the server to collect the following types of information:

- System logs that contain a record of actions taken by XenMobile.
- Audit logs that contain a chronological record of system activities for XenMobile.

The log information that a syslog server collects from an appliance is stored in a log file in the form of messages. These messages typically contain the following information:

- The IP address of the appliance that generated the log message
- A time stamp
- The message type
- The log level associated with an event (Critical, Error, Notice, Warning, Informational, Debug, Alert, or Emergency)
- The message information

XenMobile uses the log4j syslog appender to send RFC5424 formatted syslog messages. The syslog message data is plain text with no specific format.

You can use this information to analyze the source of the alert and take corrective action if necessary.

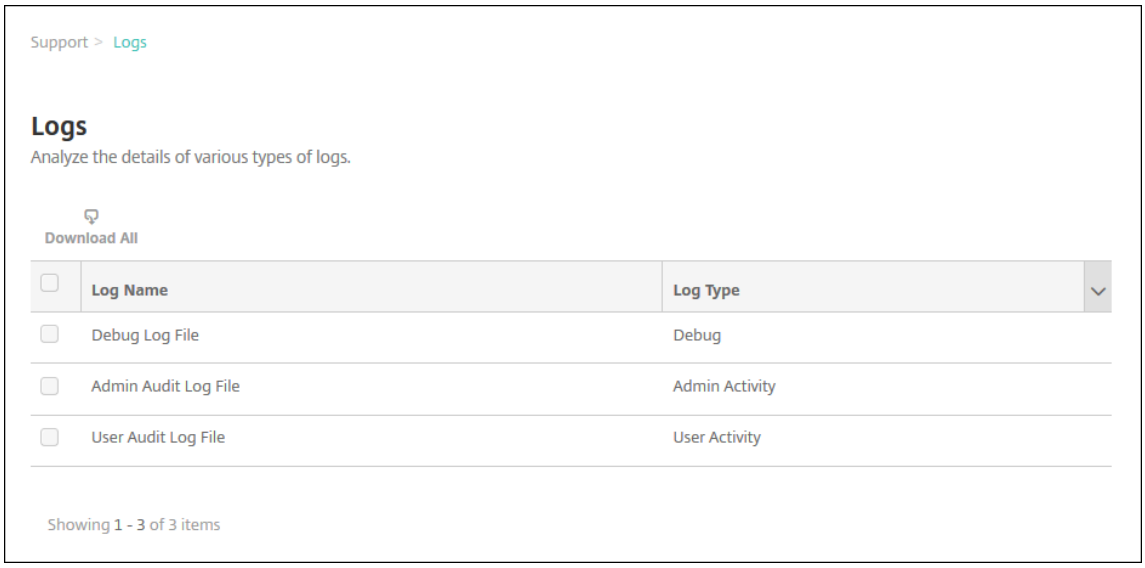
1. In the XenMobile console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **Syslog**. The **Syslog** page appears.
3. Configure these settings:
    - **Server:** Type either the IP address or the fully qualified domain name (FQDN) of your syslog server.
    - **Port:** Type the port number. By default, the port is set to 514.
    - **Information to log:** Select or clear **System Logs** and **Audit**.
        - System logs contain actions taken by XenMobile.
        - Audit logs contain a chronological record of system activities for XenMobile.
        - Debug logs for XenMobile.
4. Click **Save**.

View log files in XenMobile

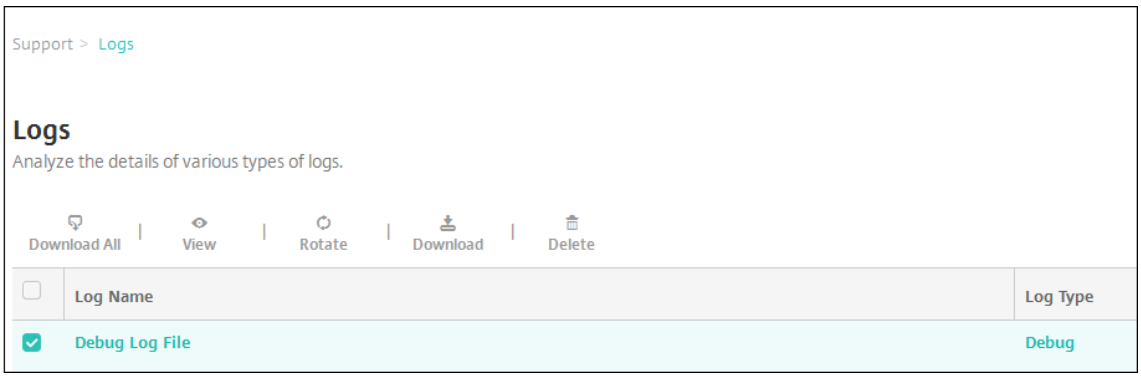
December 10, 2019

View, manipulate, and download logs to help manage with XenMobile.

1. In the XenMobile console, click the wrench icon in the upper-right corner of the console. The **Support** page opens.
2. Under **Log Operations**, click **Logs**. The **Logs** page appears. Individual logs appear in a table.



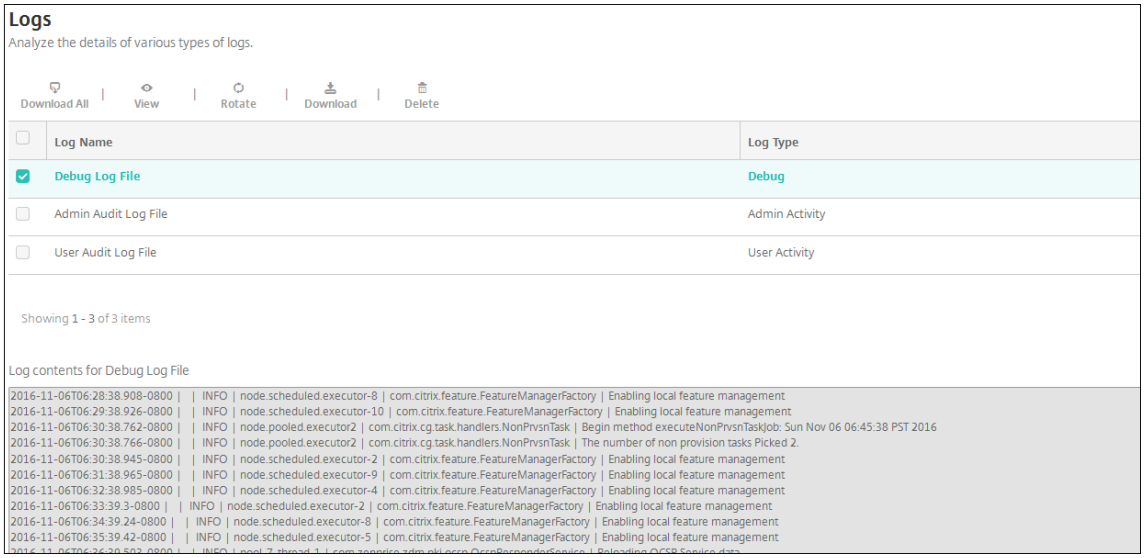
3. Select the log you want to view:
   - Debug Log Files contain information useful for Citrix Support, such as error messages and server-related actions.
   - Admin Audit Log Files contain audit information about activity on the XenMobile console.
   - User Audit Log Files contain information related to configured users.
4. Use the actions at the top of the table to download all, view, rotate, download a single log, or delete the selected log.



> **Note:**
>
> - If you select more than one log file, only **Download All** and **Rotate** are available.
> - If you have clustered XenMobile servers, you can only view the logs for the server to which you are connected. To see logs for other servers, use one of the download options.

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.
   - **Rotate:** Archives the current log file and creates a new file to capture log entries. A dialog box appears when archiving a log file; click Rotate to continue.
   - **Download:** The console downloads only the single log file type selected; it also downloads any archived logs for that same type.
   - **Delete:** Permanently removes the selected log files.



XenMobile Analyzer Tool

December 16, 2020

XenMobile Analyzer is a cloud-based tool that you can use to diagnose and troubleshoot XenMobile-related issues with configuration and other features. The tool checks for device or user enrollment and authentication issues within your XenMobile environment.

Configure the tool to point to your XenMobile 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 XenMobile Analyzer discovers issues, the tool provides recommendations to correct the issues.

Key features

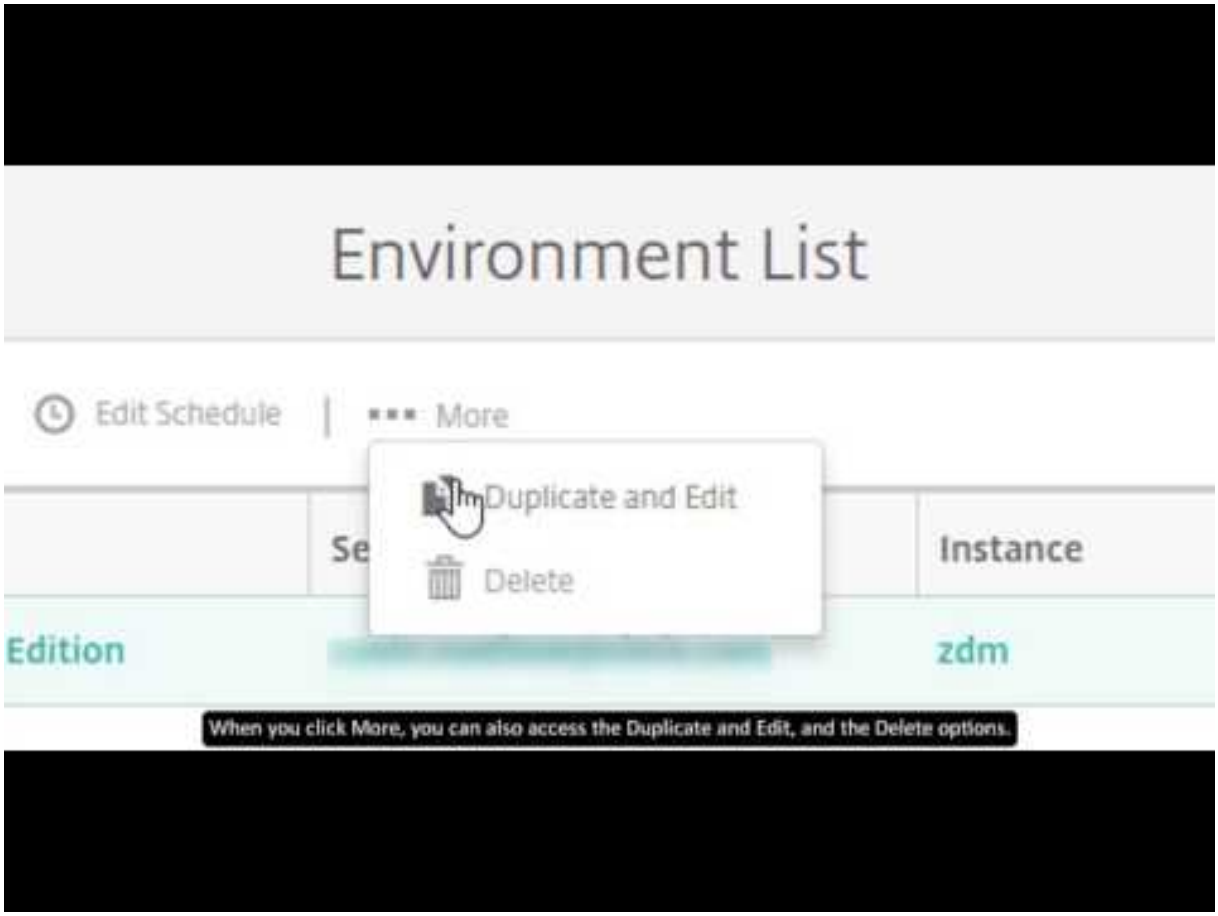
- Secure, cloud-based micro-service to troubleshoot all XenMobile related issues.
- Accurate recommendations to resolve XenMobile configuration issues.
- Reduced support calls and accelerated troubleshooting of XenMobile environments.
- Zero-day support for XenMobile Server releases.
- Health check scheduling on a daily or weekly cadence.
- Citrix ADC configuration checks.
- Secure Web tests for reachability to intranet sites.
- Secure Mail autodiscovery service checks.
- Citrix Files single sign-on (SSO) checks.

What's new

- The Citrix ADC Configuration Report displays a badge notification indicating the number of recommendations. The recommendations are based on the Essential Configuration checks on a particular Citrix Gateway.
- The icons within the global navigation bar on the Test Environment List page have now been reordered for better user experience.

The following video highlights the navigation changes in the user interface.

Citrix XenMobile Analyzer: New Environment List UI



> **Note:**
>
> This video contains no audio sound. It is best viewed in full screen mode.

Accessing and starting the XenMobile Analyzer

Prerequisites

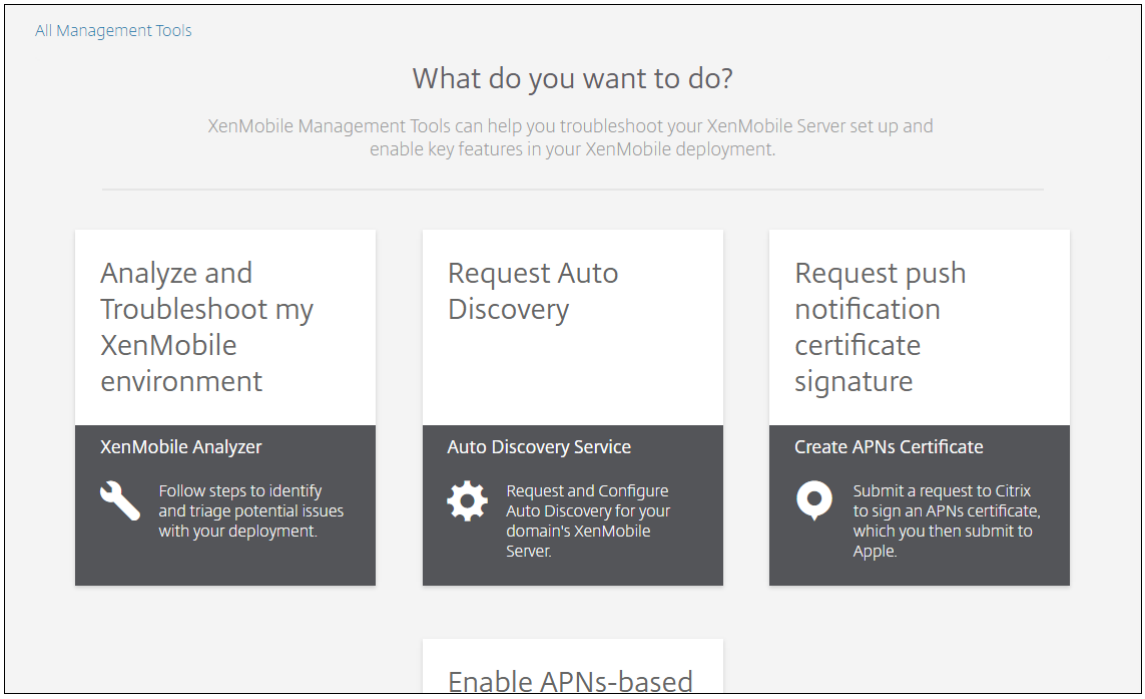
Product	Supported Version
XenMobile Server	10.1.0 and later
Citrix Gateway	10.5 and later
Client Enrollment Simulation	iOS and Android

Access the XenMobile Analyzer by using either of these methods:

- In the XenMobile console, click the wrench icon in the upper-right corner to open the **Trou-**

bleshooting and Support page.

- Use your My Citrix credentials to access the tool from https://tools.xm.cloud.com/. On the XenMobile Management Tools page that appears, to start XenMobile Analyzer, click **Analyze and Troubleshoot my XenMobile Environment**.



XenMobile Analyzer contains five options designed to lead you through the triage process and reduce the number of support tickets. The options can lower costs for everyone.

The options are as follows:

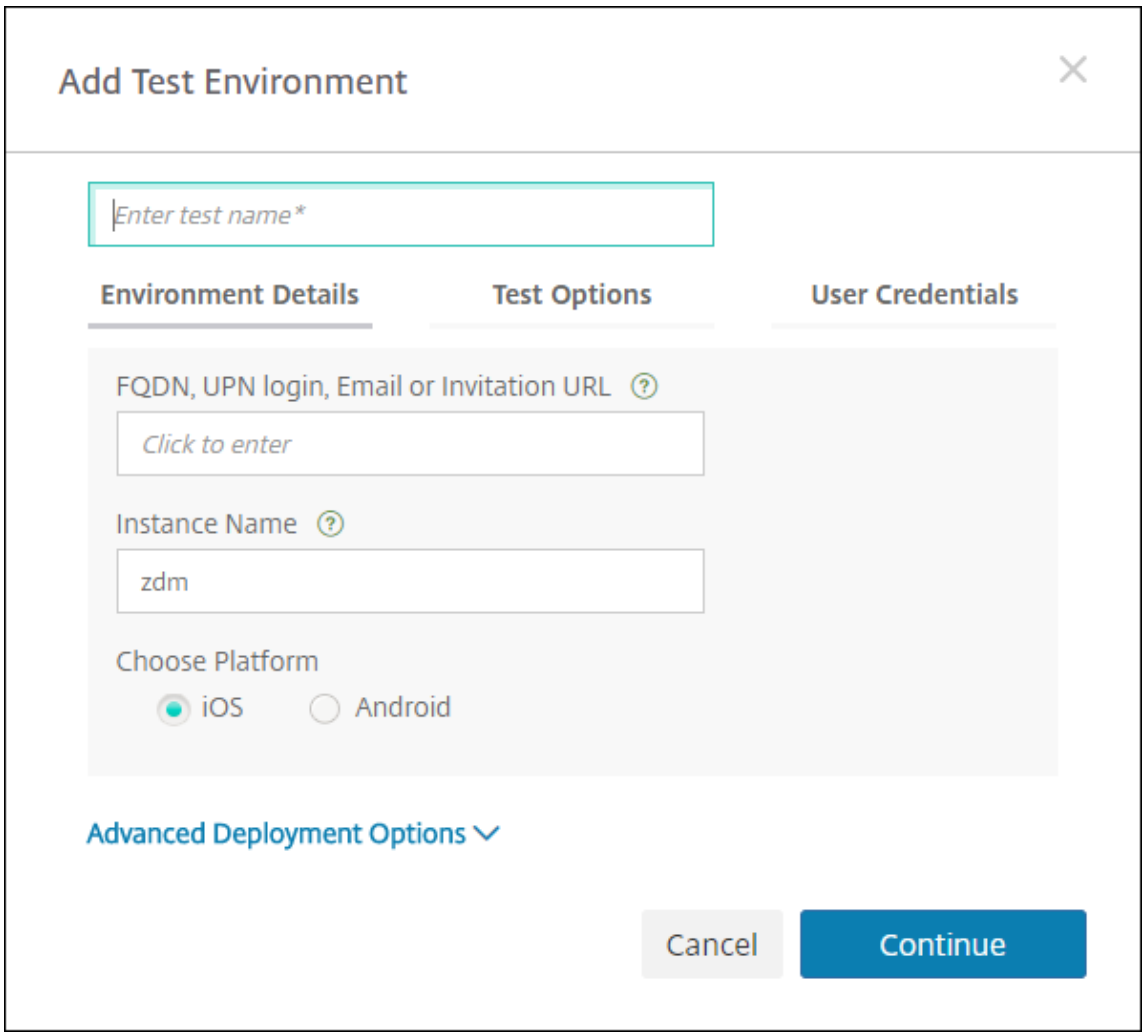
- **Environment Check:** This step guides you in setting up tests to check your setup for issues. The step also provides recommendations and solutions on device, user enrollment, and authentication issues.
- **Citrix ADC Check:** This step guides you in checking your Citrix ADC configurations for XenMobile deployment readiness.
- **Advanced Diagnostics:** This step provides information on using Citrix Insight Services to find further issues that the environment check might have missed.
- **Server Connectivity Checks:** This step instructs you to test the connectivity of your servers.
- **Contact Citrix support:** If you are still having issues, this step links you to the site where you can create a Citrix support case.

The following sections describe each option in more detail.

Performing an environment check

1. Log on to XenMobile Analyzer and click **XenMobile Environment**.

2. Click **Add Test Environment**.
3. In the new **Add Test Environment** dialog box, do the following:



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**, enter the information that is used to access the server.

c) In **Instance Name**, if you use a custom instance, you can provide that value.

d) In **Choose Platform**, select either **iOS** or **Android** as the platform for testing.

e) If you expand **Advanced Deployment Options**, in the **Deployment Mode** list, you can select your XenMobile deployment mod 1. Available options are **Enterprise (MDM + MAM)**, **App Management (MAM)**, or **Device Management (MDM)**.

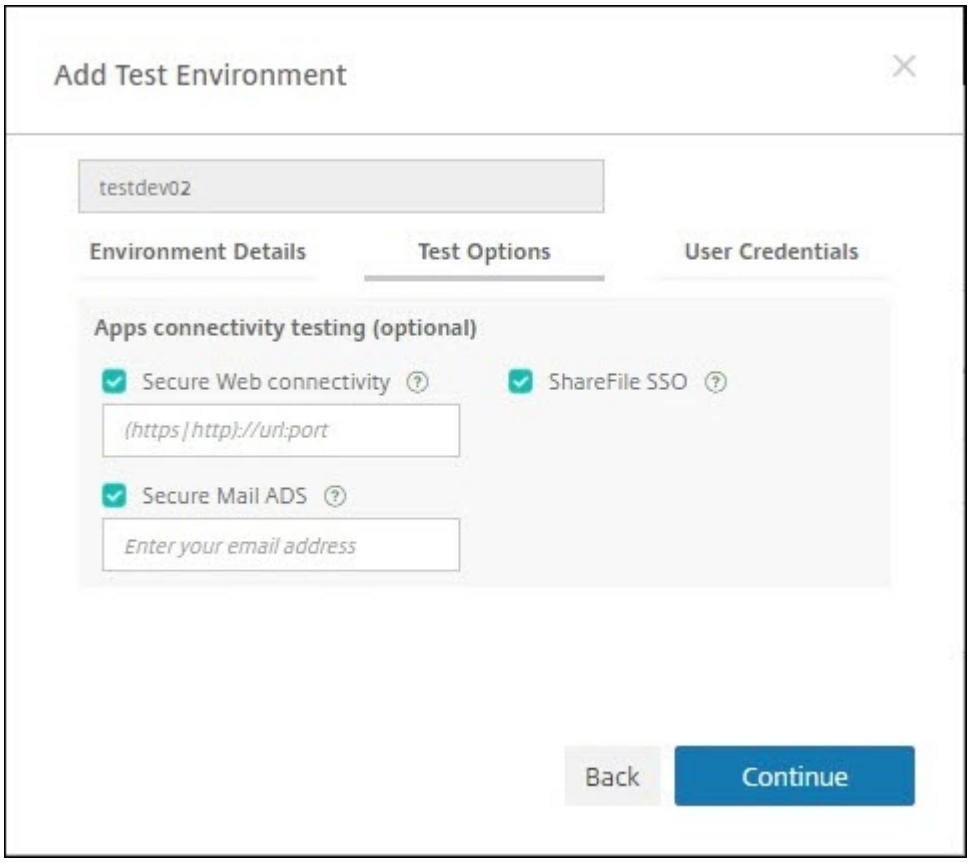
f) Click **Continue**.

4. On the **Test Options** tab, choose one or more of the following tests and then click **Continue**.

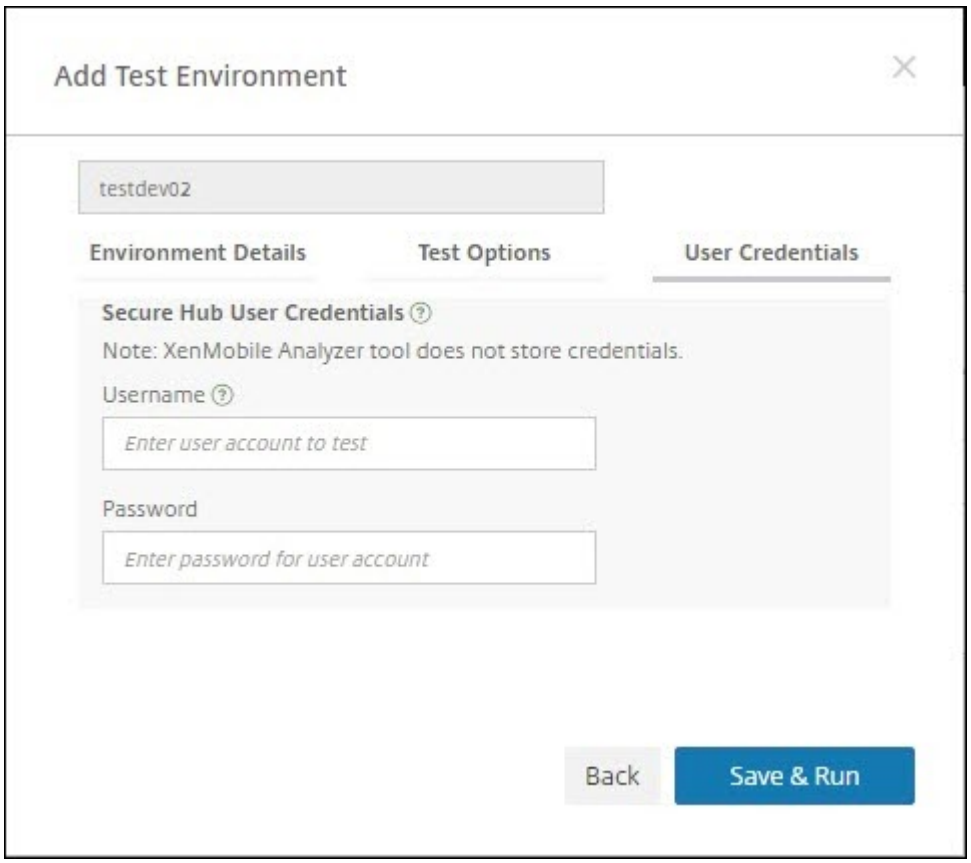
   a) **Secure Web Connectivity**. Provide an intranet URL. The tool tests for the reachability of the URL. This test detects if there are any connectivity issues that may potentially occur in the Secure Web app while trying to reach intranet URLs.

b) **Secure Mail ADS**. Provide a user email ID. This ID is used to test the autodiscovery of the Microsoft Exchange Server in your XenMobile environment. It detects if there are any issues related to Secure Mail autodiscovery.

c) **ShareFile SSO**. If selected, XenMobile Analyzer tests if the Citrix Files DNS resolution happens successfully. The tool also checks if Citrix Files single sign-on (SSO) is compatible with the provided user credentials.



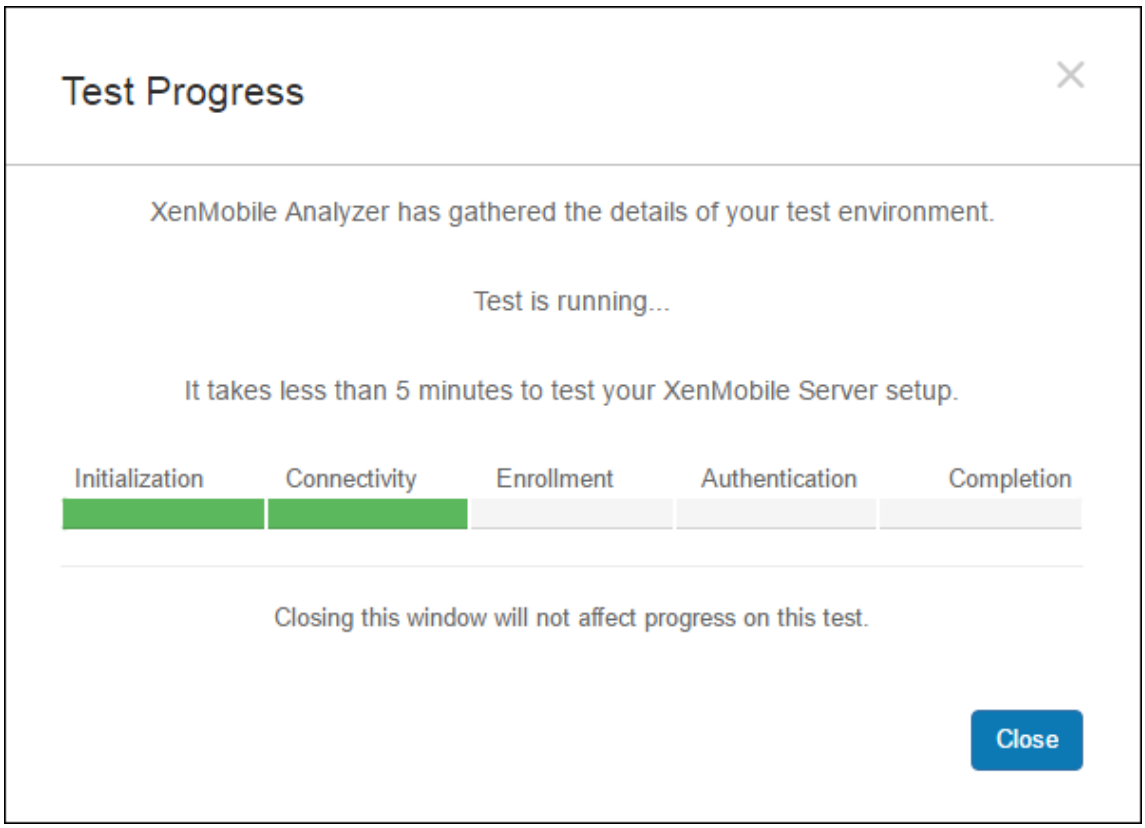
5. On the **User Credentials** tab, depending on your server setup, you see different fields. The possible fields are **Username**, **Username and Password**, or **Username, Password**, and **Enrollment PIN**.



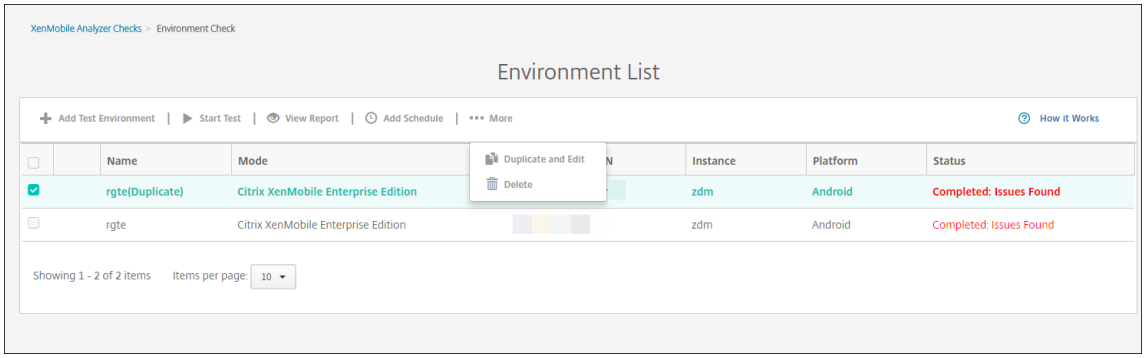
6. Click **Save & Run** to start the tests.

   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 have passed appear in green. Tests that fail appear as red.



After closing the progress dialog box, you return to the **Environments List** page.



The **Results** page shows Test Details, Recommendations, and Results.

7. Click the **View Report** icon to see test results.

   If recommendations have Citrix Knowledge Base articles associated with them, the articles are listed on this page.

8. Click the **Results** tab to display the individual Category and Tests that the tool performed, with their results.

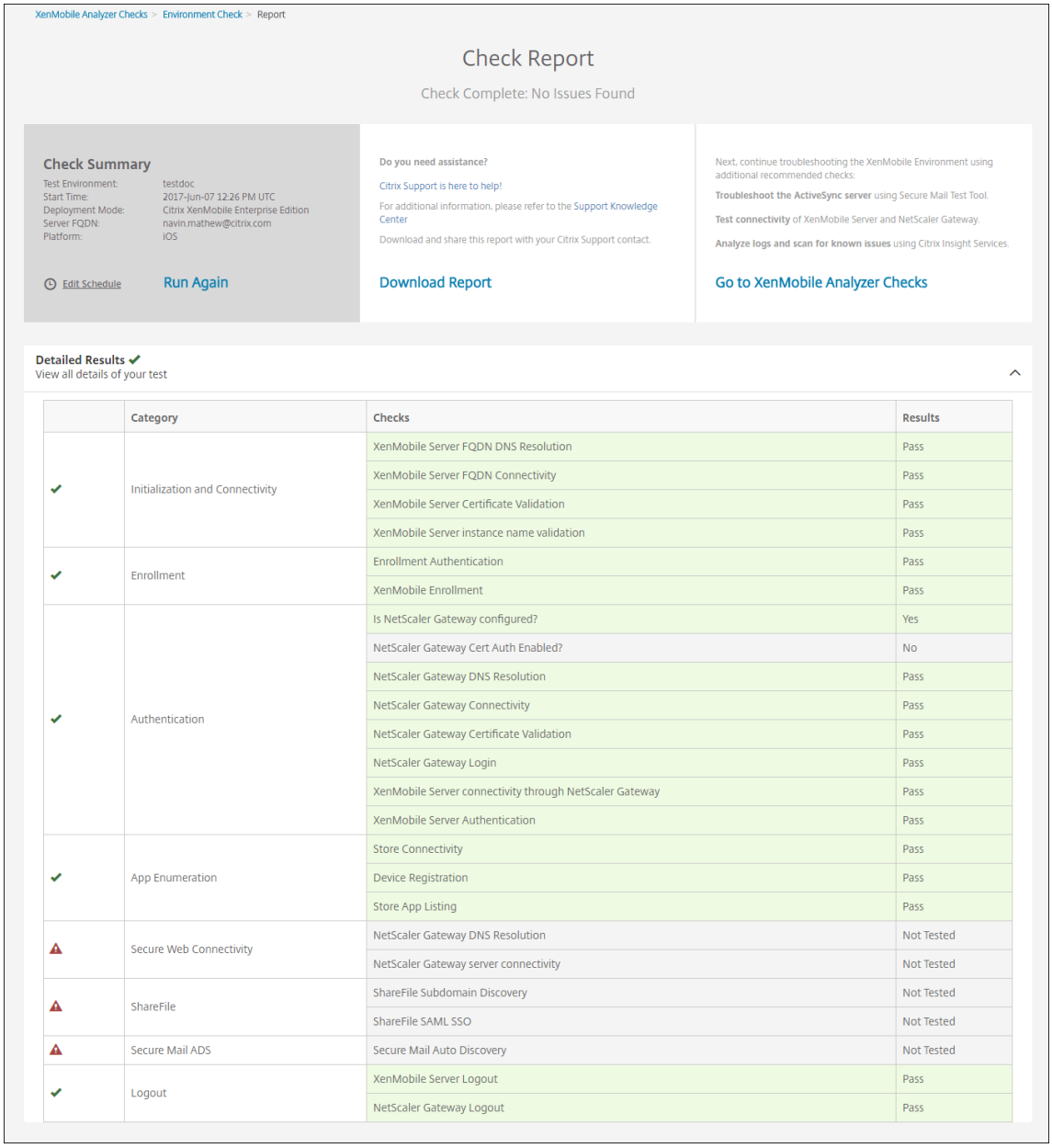
   a) To download the report, click **Download Report**.

   b) To return to the list of test environments, click **Environment Check**.

c) To rerun the same test, click **Run Again**.

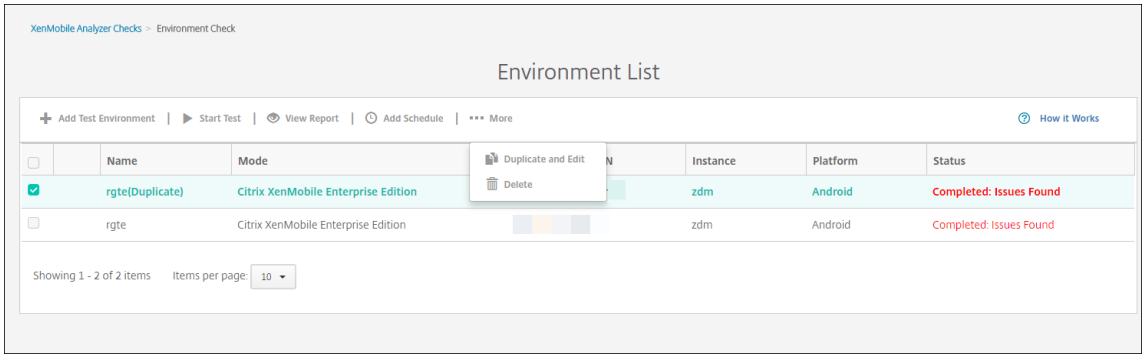
d) If you want to rerun another test, go back to **Test Environments**, select the test, and click **Start Test**.

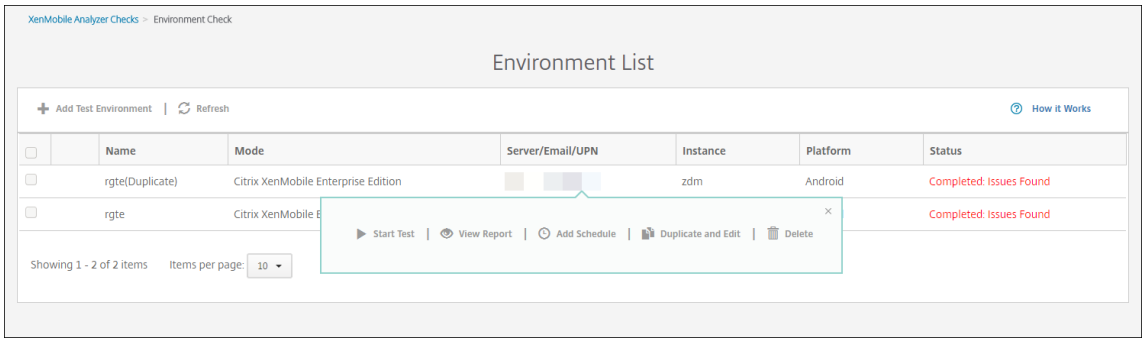
e) To select another XenMobile Analyzer option, click **Go To XenMobile Analyzer Checks**.

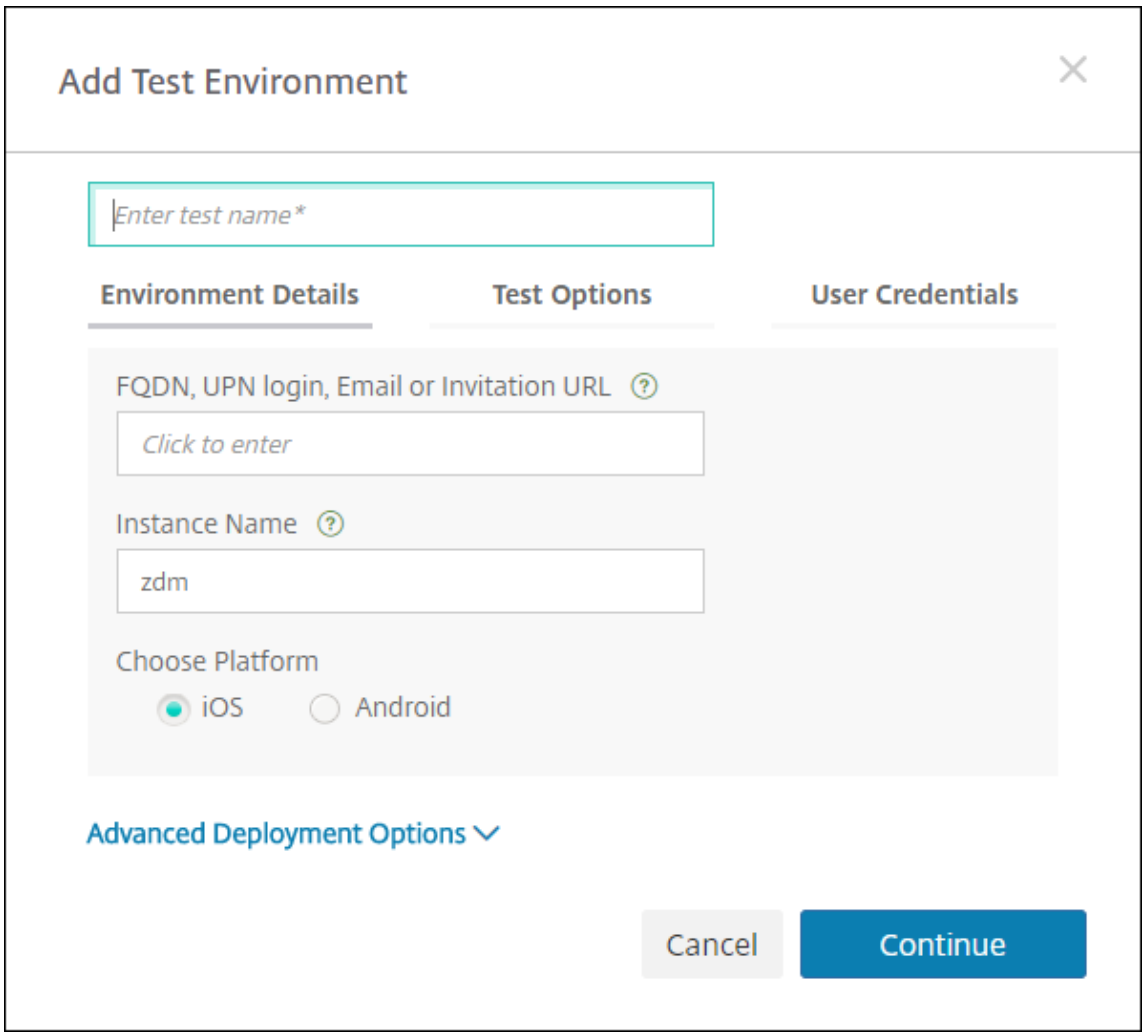


9. From the Test Environments page, you can copy and edit tests. To do so, select a test and then click **More** and select **Duplicate and Edit**.

   A copy of the selected test is created and the Add Test Environment dialog opens, allowing you to modify the new test.



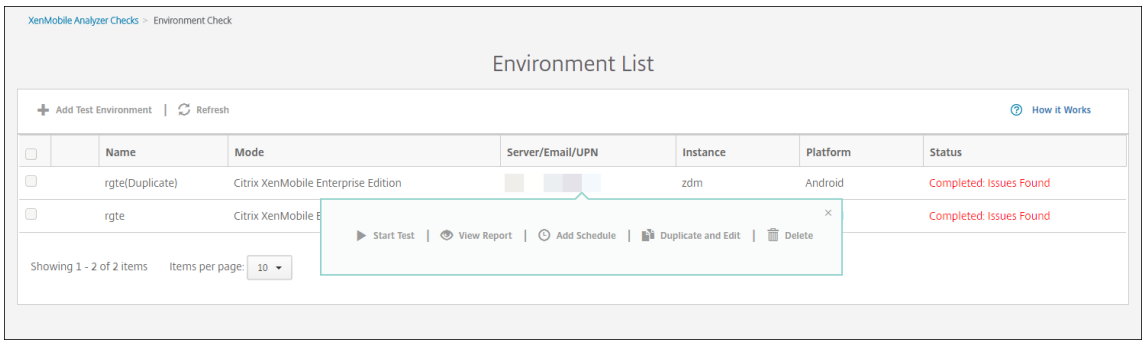




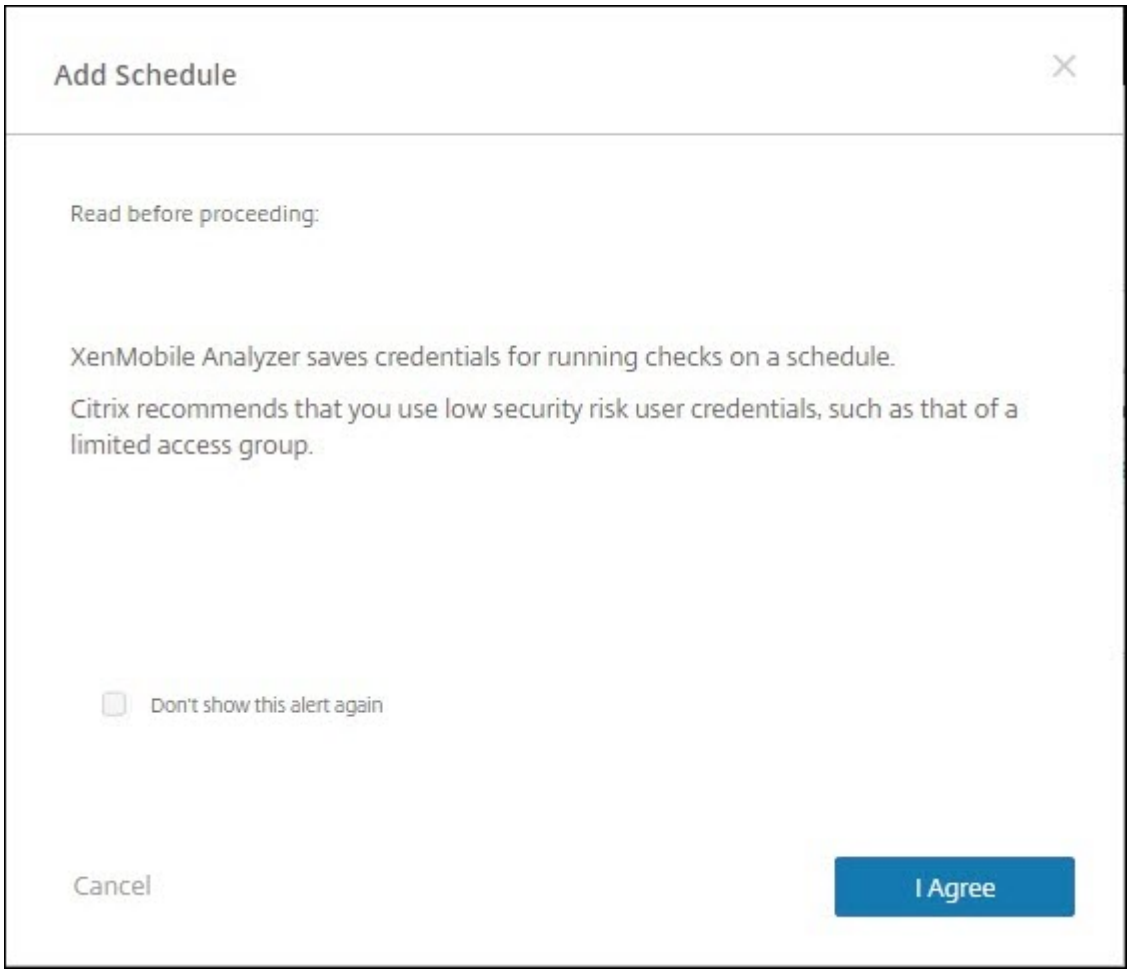
Adding a schedule to environment checks

You can configure tests to run on an automatic schedule with results sent to a list of users you configure.

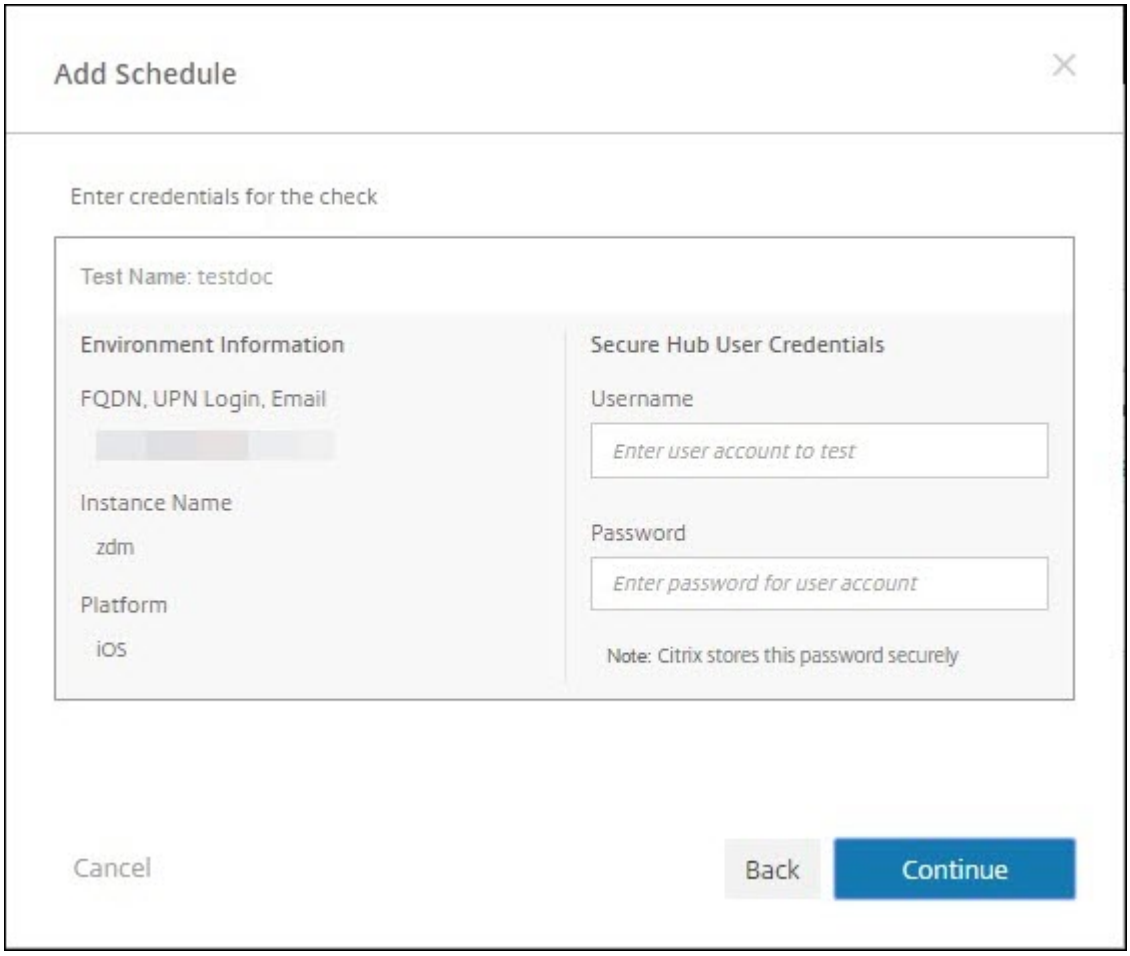
1. On the **Environment List** page, select the environment for which you want to set up a schedule and click **Add Schedule**.



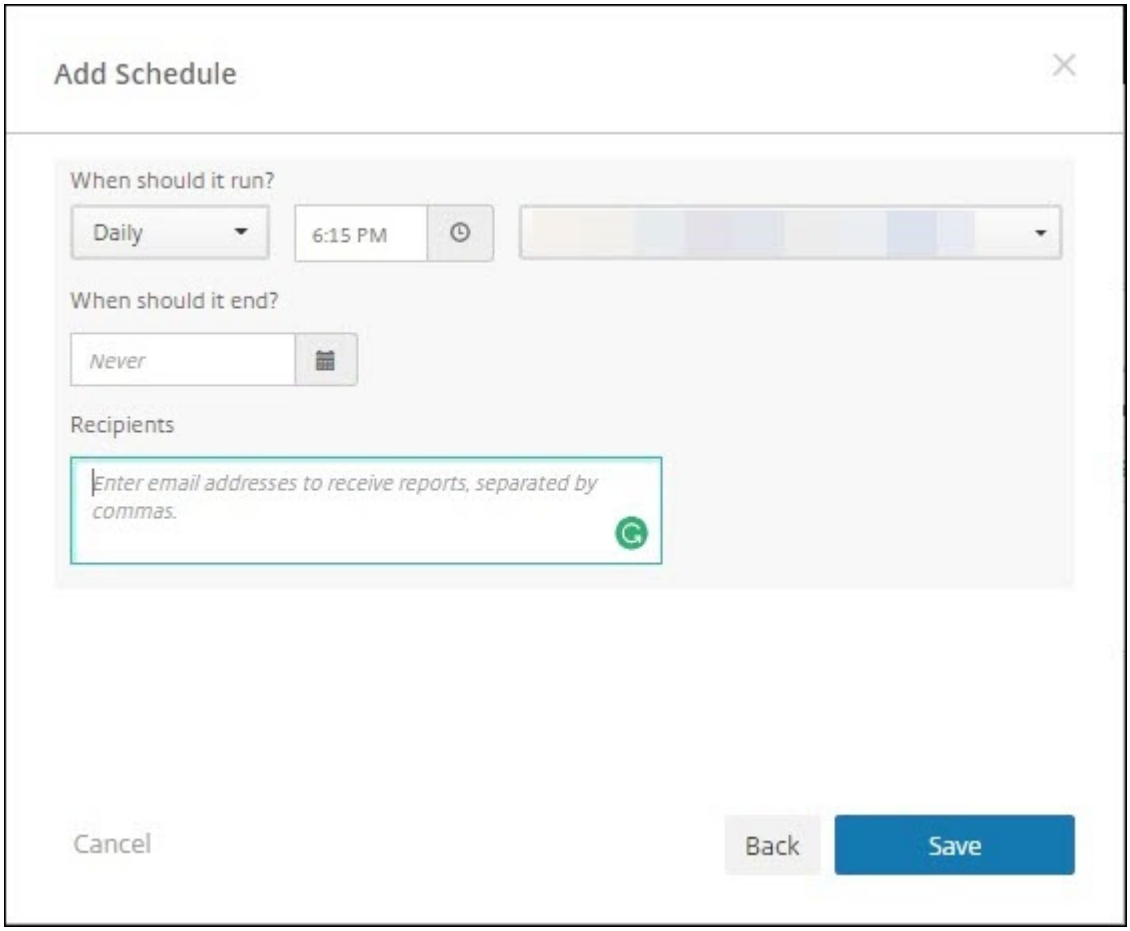
2. The **Add Schedule** window displays a message warning you that XenMobile Analyzer saves credentials for running tests on a schedule. Citrix recommends that you use an account with limited access for running scheduled tests. Click **I Agree** to continue.



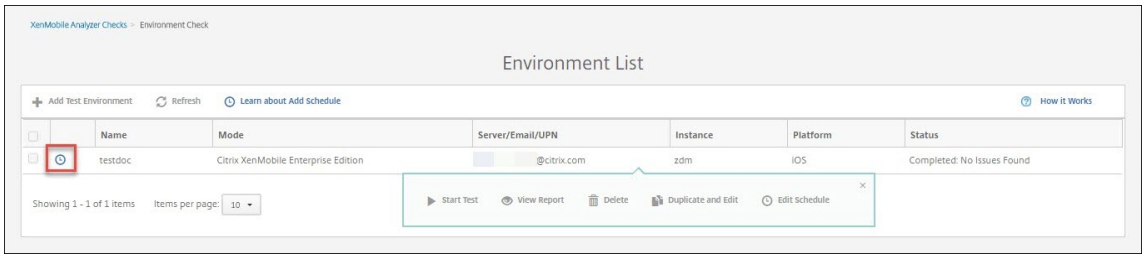
3. Enter a **Username** and **Password** for running the test.



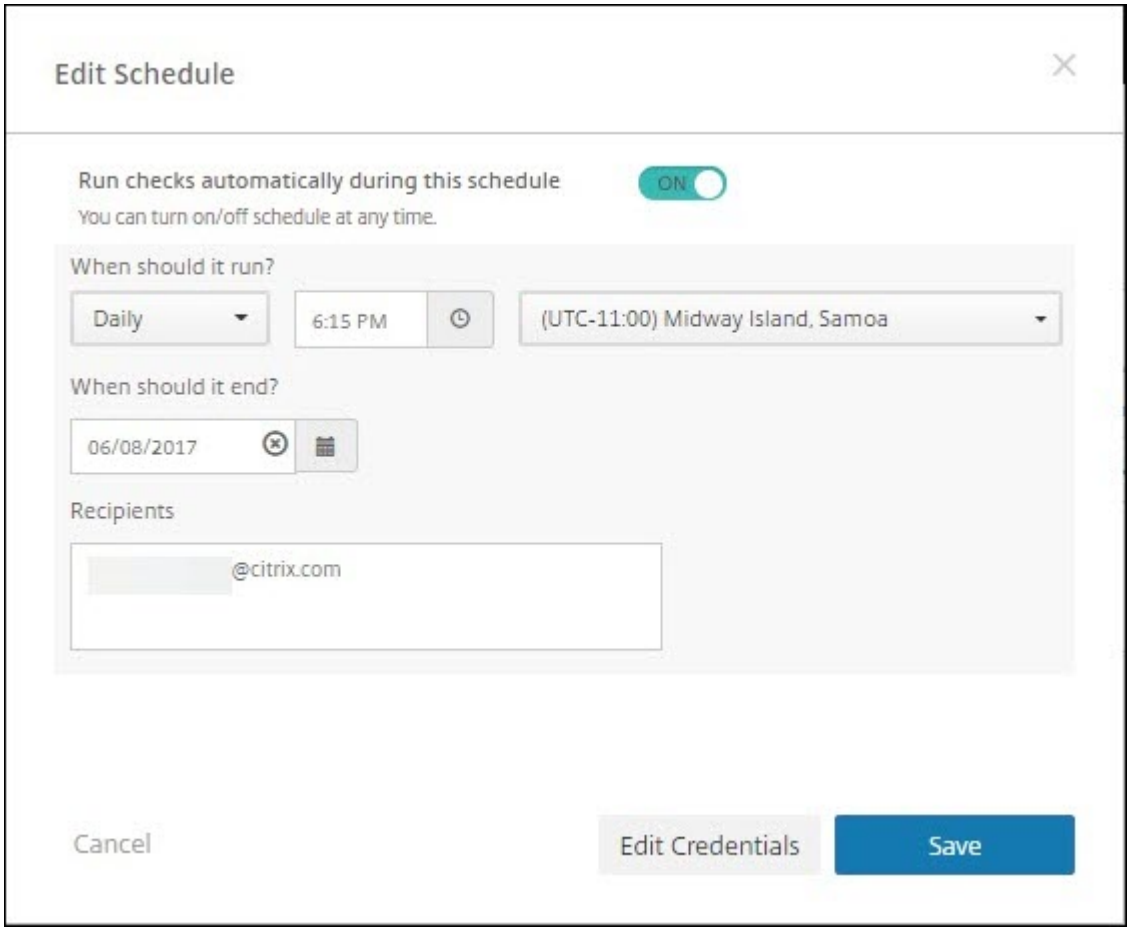
4. Configure a schedule for the test to run. You can select **Daily** or **Weekly** from the drop-down. Select a time of day for the test to run and a time zone. Use the date picker to select a date for the scheduled test to stop running or leave it blank for the test to run indefinitely. Enter a list of email addresses to receive reports, separated by commas. Click **Save**.



5. A clock symbol to the left of your test indicates that a schedule is configured. If you select your test, you can click **Edit Schedule** to change when the test runs.



6. In this window, you can change when the test runs. You can also disable it, by clicking the switch at the top. Click **Save** when you're done.



Performing other informative checks

You interact with the Environment Check step of XenMobile Analyzer directly to perform tests, whereas the other options are informative. Each of these options provides information concerning other support tools you can use to ensure that your XenMobile environment is set up correctly.

- **Advanced Diagnostics:** Instructs you to collect information on your environment and then upload the information to Citrix Insight Services. The tool analyzes your data and provides a personalized report with recommended resolutions.
- **Secure Mail Readiness:** Directs you to download and run the XenMobile Exchange ActiveSync Test application. The application troubleshoots ActiveSync servers for their readiness to be deployed with XenMobile environments. After the application runs, you can view reports or share them with others.
- **Server Connectivity Checks:** Provides you with instructions for checking your connections to XenMobile, Authentication, and Content Collaboration servers.
- **Contact Citrix support:** If all else fails, you can create a support ticket with Citrix support.

Known Issues

The following issues are known in the XenMobile 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.

Fixed Issues

The following issues with XenMobile Analyzer have been fixed:

- When performing a check using enrollment invitation, the test passes but the enrollment invitation is not redeemed.

REST APIs

August 30, 2019

> **Note:**
>
> This article covers the REST APIs for XenMobile Server. For the REST APIs for Endpoint Management, see REST APIs.

With the XenMobile REST API, you can call services that are exposed through the XenMobile console. You can call REST services by using any REST client. The API does not require you to sign on to the XenMobile console to call the services.

For the complete current set of available APIs, download the Public API for REST Services PDF.

Permissions required to access the REST API

Access to the REST API requires one of the following permissions:

- Public API access permission set as part of role-based access configuration. For information, see Configuring roles with RBAC.
- Super user permission

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.

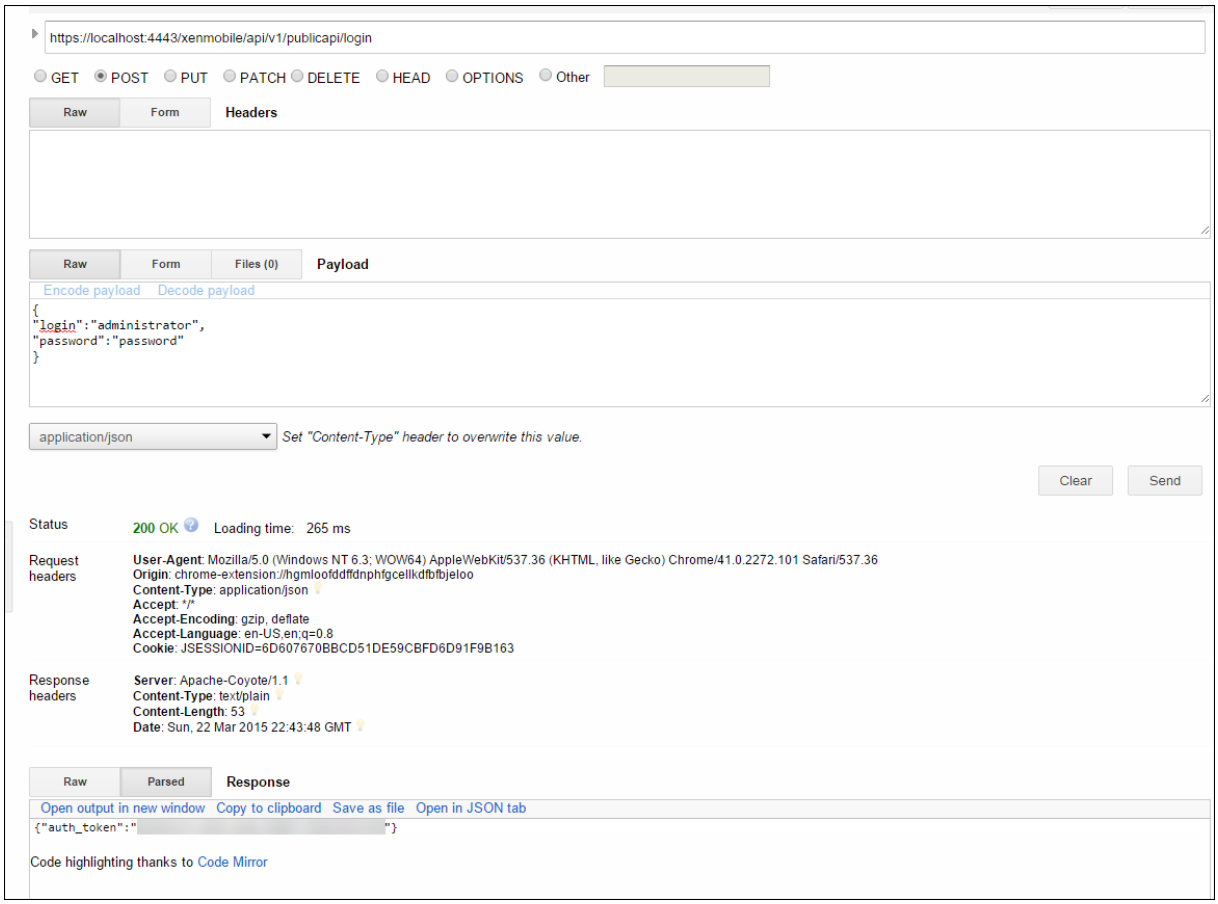
Log in

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

Request: `{ "login":"administrator", "password":"password"}`

Method type: POST

Content type: application/json



Related information

- XenMobile REST API

Endpoint Management connector for Exchange ActiveSync

January 6, 2021

XenMobile Mail Manager is now Endpoint Management connector for Exchange ActiveSync. For more detail about the Citrix unified portfolio, see the Citrix product guide.

The connector extends the capabilities of XenMobile 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 XenMobile to access EAS device partnership information provided by Exchange.
- The ability for XenMobile to wipe a mobile device based on EAS status.
- The ability for XenMobile 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.

To download the Endpoint Management connector for Exchange ActiveSync:

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 Endpoint Management connector for Exchange ActiveSync** tile, click **Download File**.

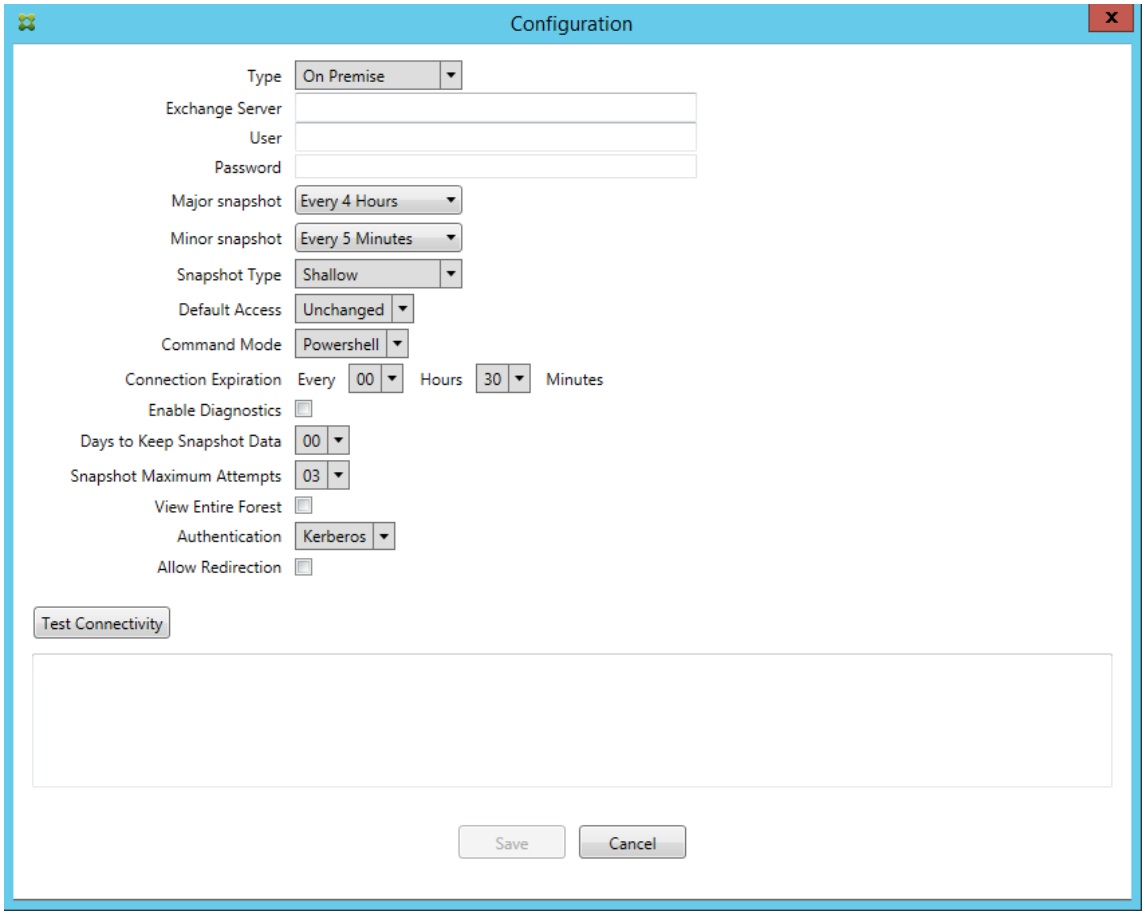
What's new

The following sections list what's new in the Endpoint Management connector for Exchange ActiveSync, formerly XenMobile Mail Manager.

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]



- 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 new 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]

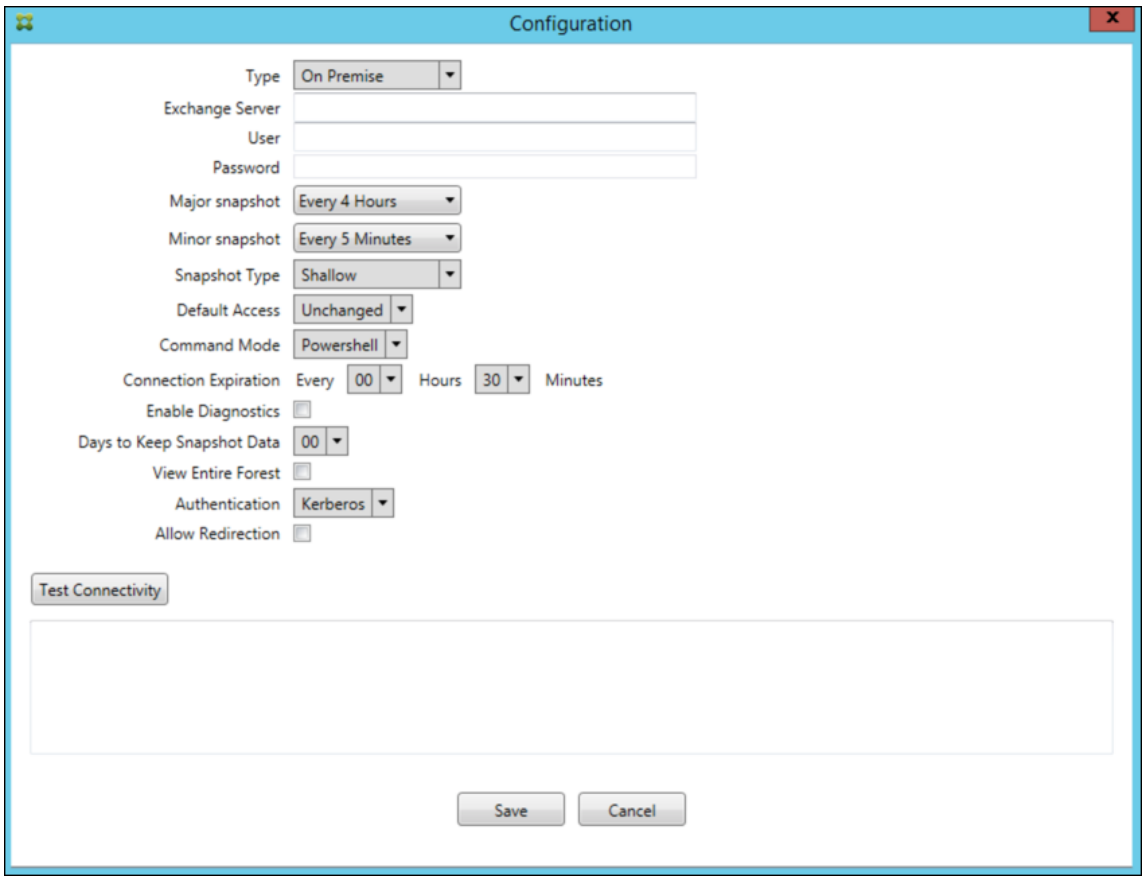
What's new in earlier versions

The following section lists the features and fixed issues in earlier versions of Endpoint Management connector for Exchange ActiveSync.

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 executing 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]



What's new in version 10.1.8

The following issues are fixed 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 is common in connections to Office 365. The effect of throttling requires that the service pause for a specified period of time 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" 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. Consequently, 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, and/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 vice versa. The result could be that some devices and/or mailboxes are rejected during the snapshot reconciliation. [CXM-56088]

> **Note:**
>
> The following 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 could 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 of time. 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 a period of 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. Consequently, if permissions were restricted, the behavior could 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 elapsed before executing 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. In order 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 all of the policies for those devices of the mailbox to be set. The error reported, which will appear 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 Allowed or Blocked could 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:

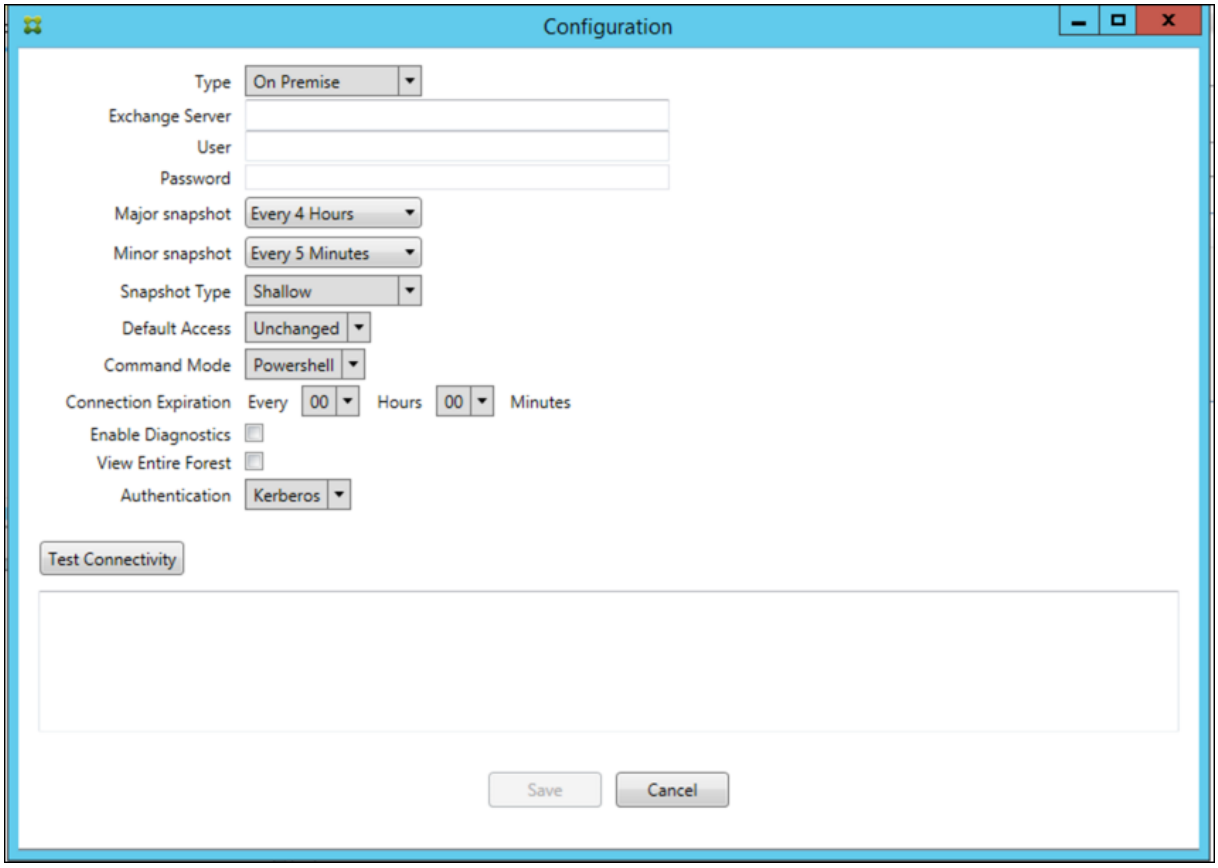
- Due to its weakening security, TLS 1.0 is being deprecated by the PCI Council. Support for TLS 1.1 and 1.2 is added to XenMobile Mail Manager. [CXM-38573, CXM-32560]
- XenMobile Mail Manager includes a new diagnostic file. When **Enable Diagnostics** is selected in the Exchange specification, a new 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: The error message is overridden by an incorrect 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]

- In some cases, 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.



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 could 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 for Microsoft .NET Framework is now version 4.6.

Fixed issues

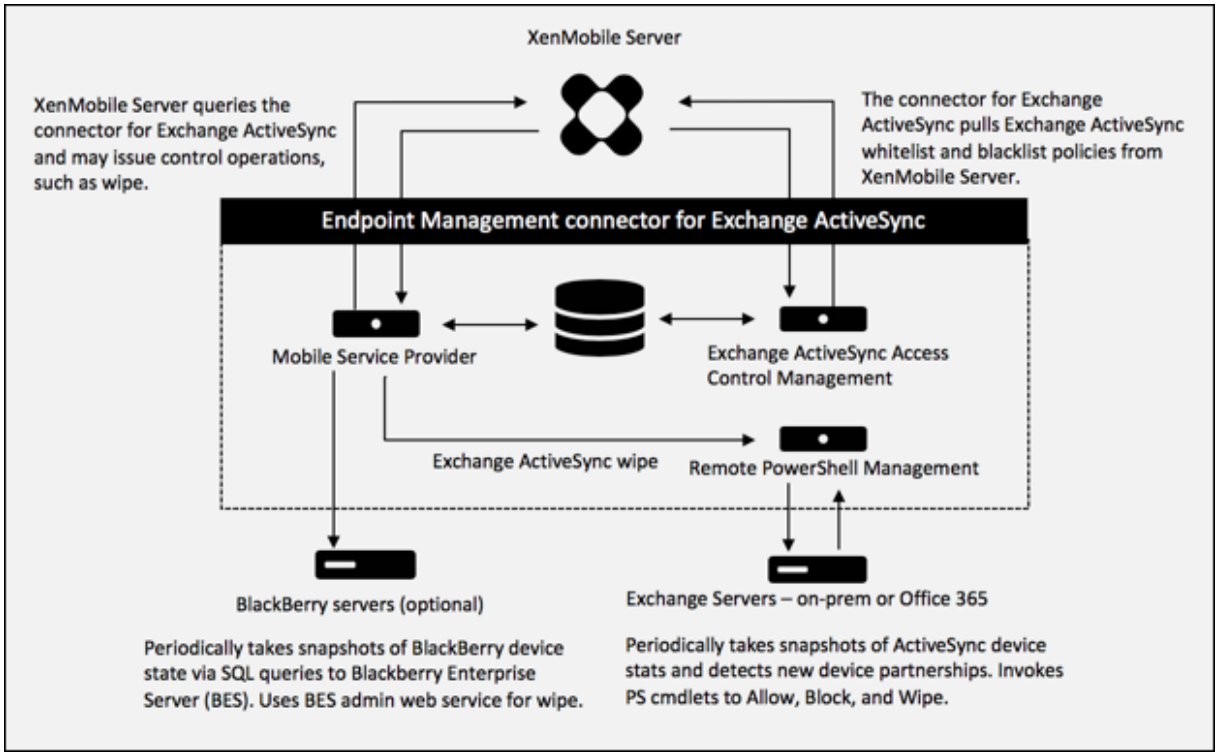
- Prompt for credentials error: Office 365 session instability often caused this error. The Improved

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 figure 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 XenMobile to retrieve an Exchange ActiveSync policy from XenMobile, 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 XenMobile 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 or SQL Server 2014 Service Pack 3.
- 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 Endpoint Management 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 Endpoint Management 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 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 Endpoint Management 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, Endpoint Management 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

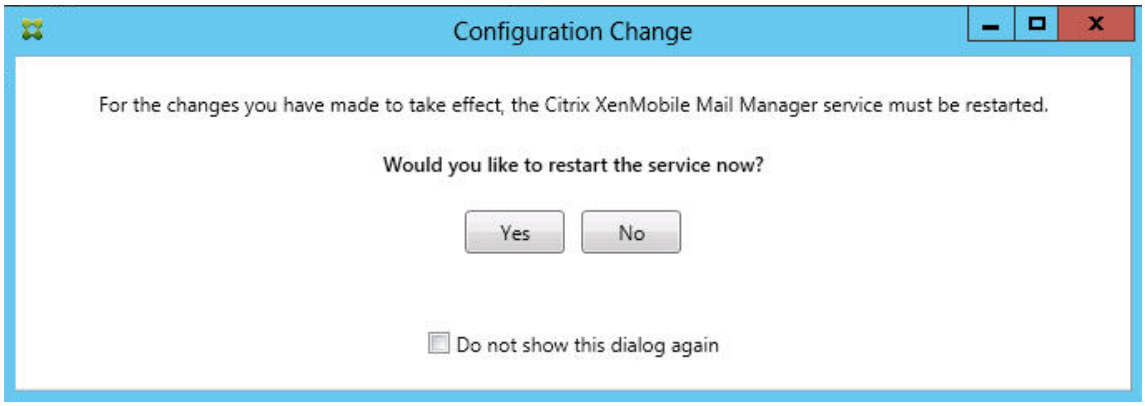
- **Permissions:** The credentials specified in the Exchange Configuration UI must be able to connect to Office 365 and be given full access to execute the following Exchange-specific PowerShell cmdlets:
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - 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, Endpoint Management 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

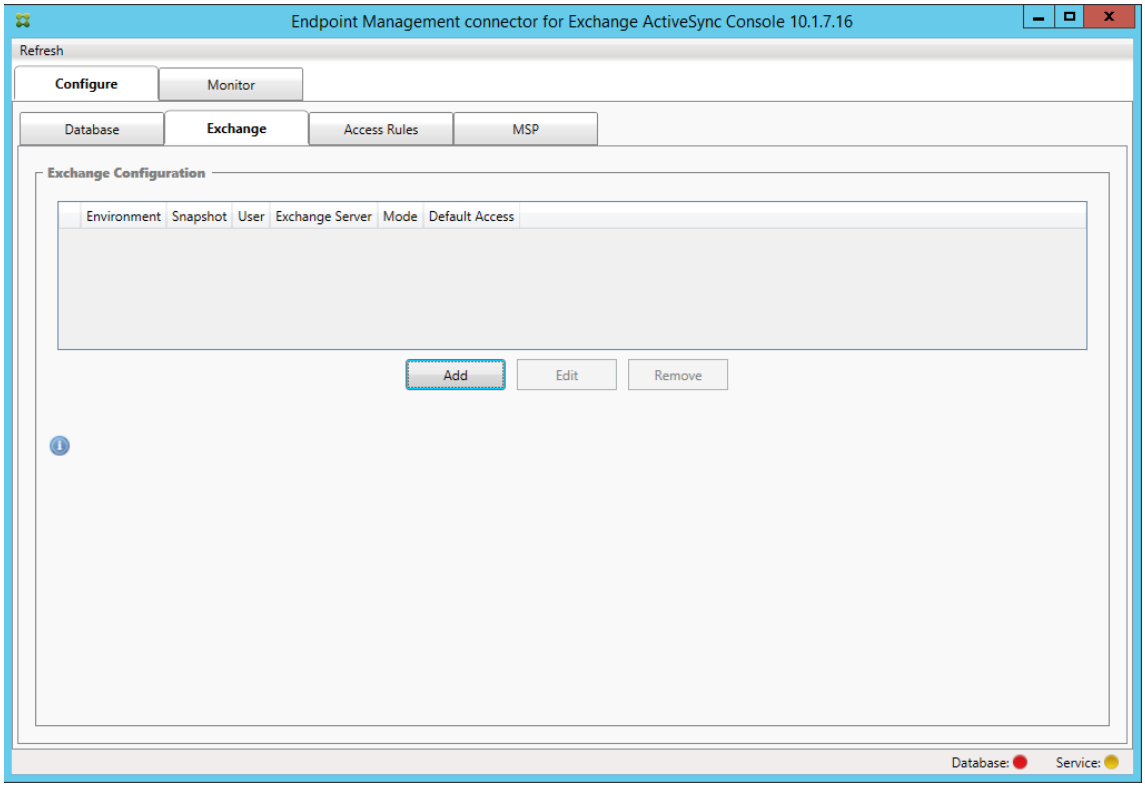
1. Click the XmmSetup.msi file and then follow the prompts in the installer to install Endpoint Management connector for Exchange ActiveSync.
2. Leave **Launch the Configure utility** selected in the last screen of the setup wizard. Or, from the **Start** menu, open Endpoint Management connector for 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 Endpoint Management connector for Exchange ActiveSync 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 Endpoint Management connector for Exchange ActiveSync 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**.



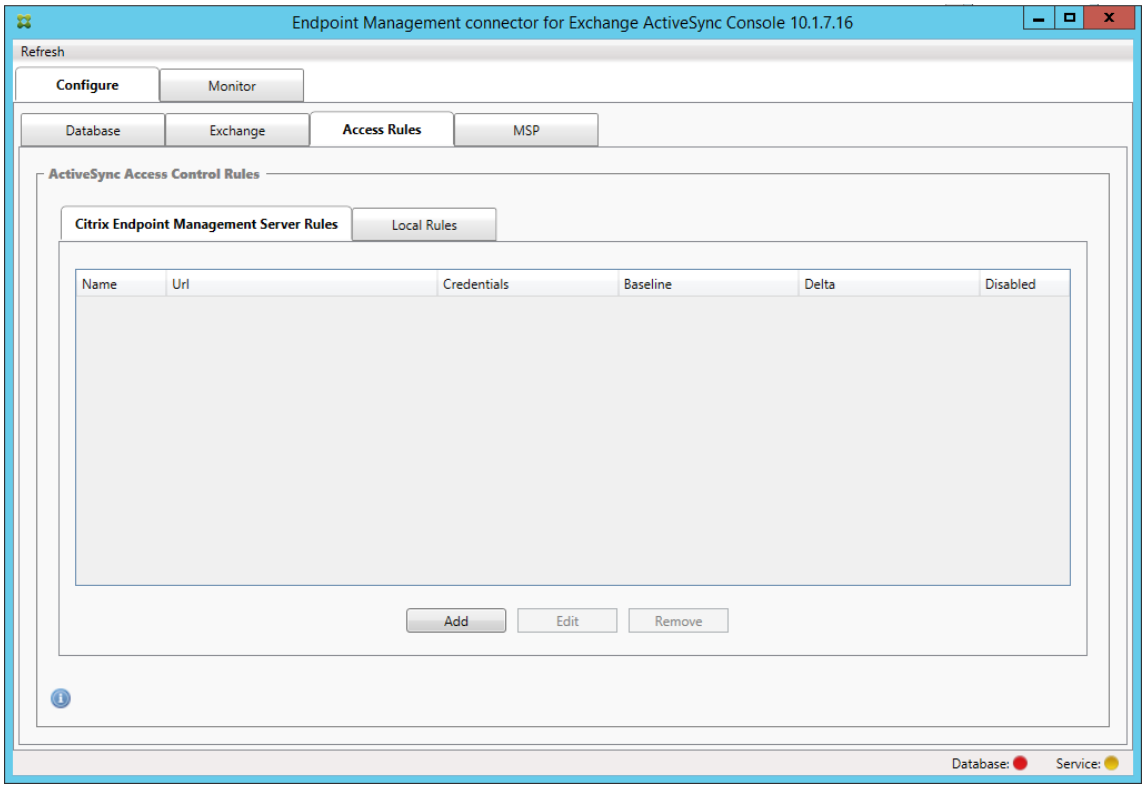
8. Select the type of Exchange Server environment: **On Premise** or **Office 365**.

   - 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 Endpoint Management 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 XenMobile 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 XenMobile 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, Endpoint Management connector for Exchange ActiveSync issues

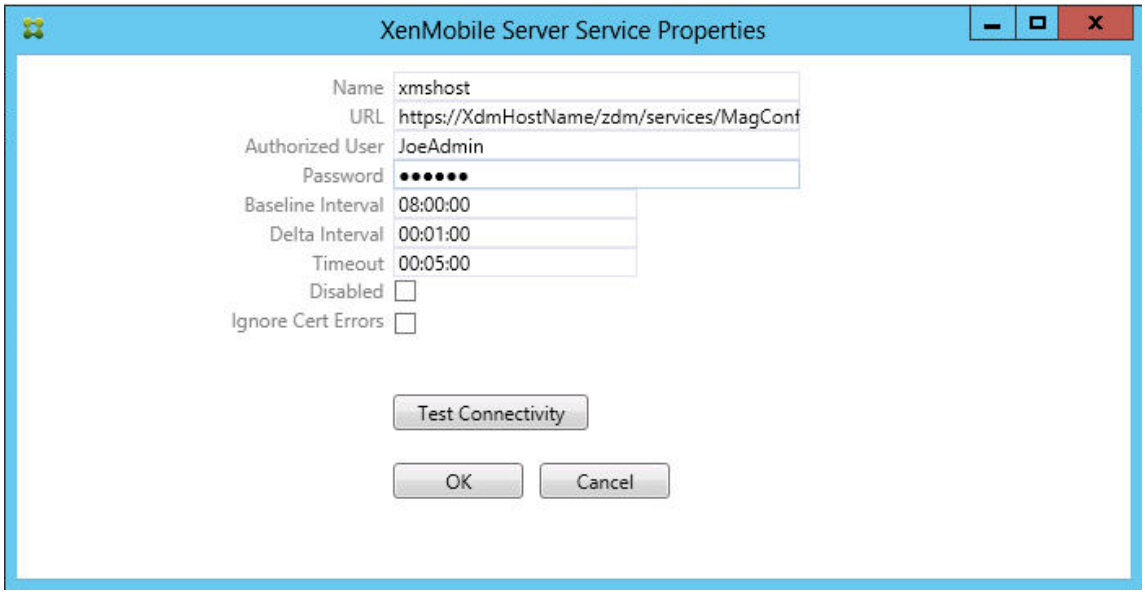
PowerShell commands to enact the desired access control. In Simulation mode, Endpoint Management connector for Exchange ActiveSync does not issue PowerShell commands, but logs the intended command and intended outcomes to the database. In Simulation mode, the user can then use the **Monitor** tab to 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, Endpoint Management 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 Endpoint Management connector for Exchange ActiveSync to view the entire Active Directory forest in the Exchange environment.
- Select the authentication protocol: **Kerberos** or **Basic**. Endpoint Management connector for Exchange ActiveSync supports Basic authentication for on-premises deployments. This enables Endpoint Management connector for Exchange ActiveSync to be used when the Endpoint Management connector for Exchange ActiveSync 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 **XMS Rules** tab, and then click **Add**.



10. On the **XenMobile server Service Properties** page, modify the URL string to point to the XenMobile 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 XenMobile Server.

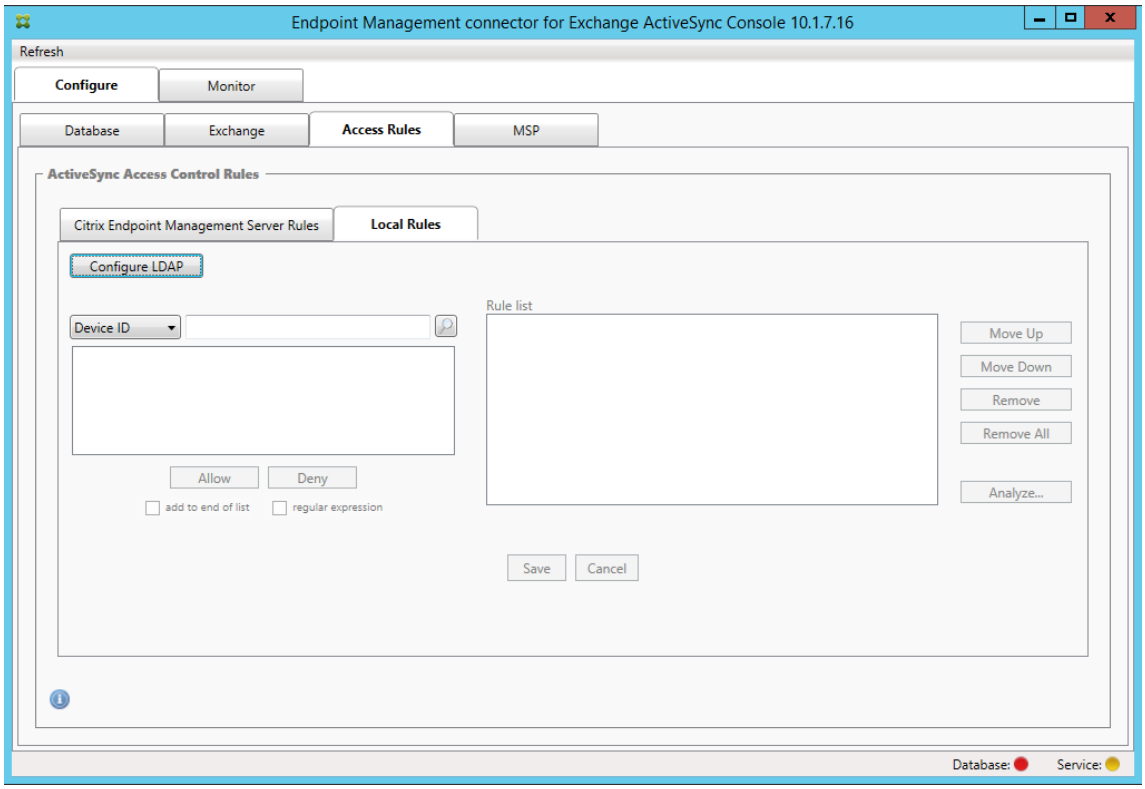


- Enter an authorized user of the server.
- Enter the password of the user.
- Keep the default values for the **Baseline Interval**, **Delta Interval**, and **Timeout** values.

- Click **Test Connectivity** to check the connection to the server and then click **OK**.

If the **Disabled** check box is selected, the XenMobile Mail Service doesn't collect policies from XenMobile.

11. Click the **Local Rules** tab.

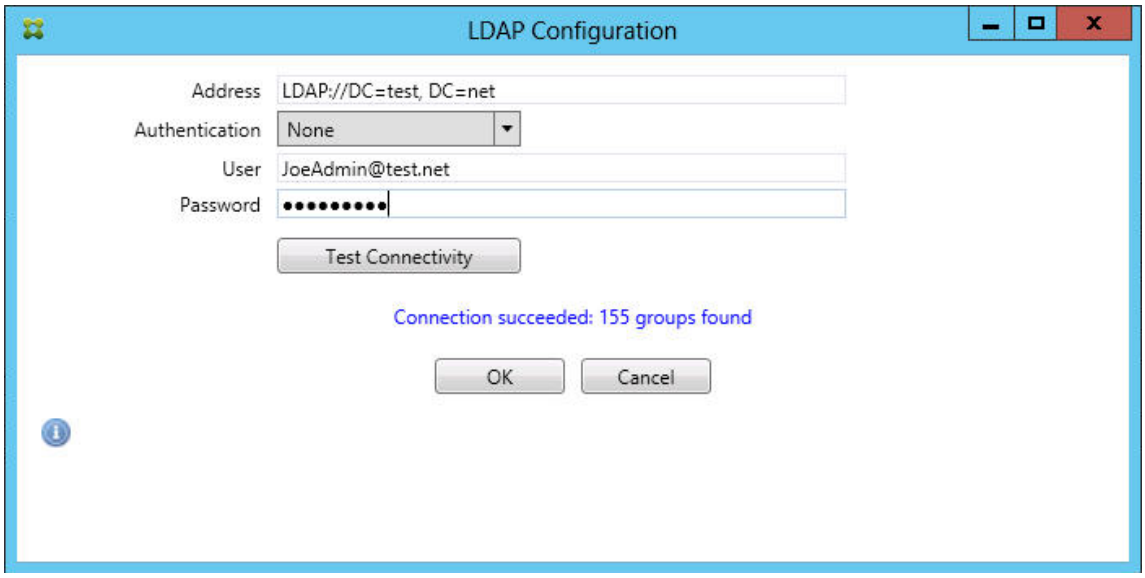


- You can add local rules based on ActiveSync Device ID, Device Type, AD Group, User, or device UserAgent. In the list, select the appropriate type.
- Enter text or text fragments in the text box. Optionally, click the query button to view the entities that match the fragment.

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**.

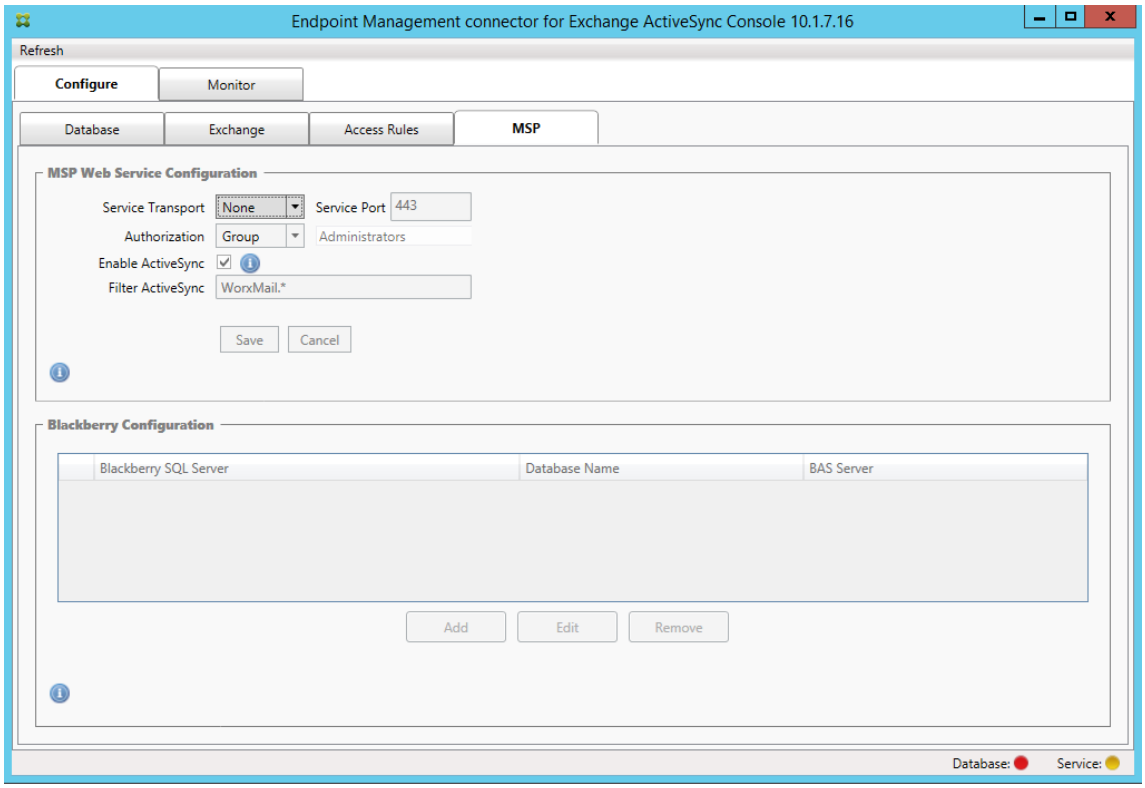
12. If you want to construct local rules that operate on Active Directory Groups, click **Configure LDAP** and then configure the LDAP connection properties.



13. Configure the Mobile Service Provider.

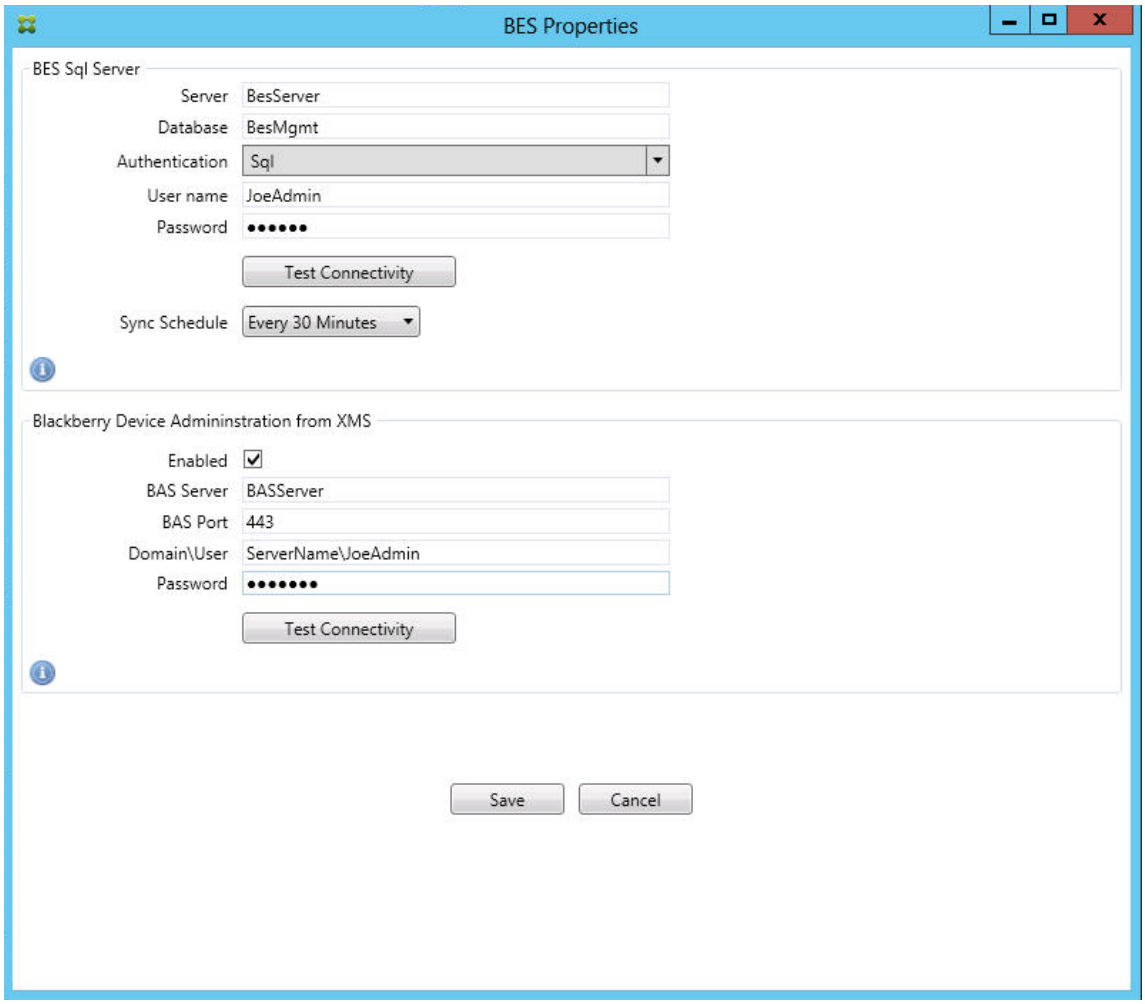
    The Mobile Service Provider is optional. That setting is necessary only if XenMobile is also configured to use the Mobile Service Provider interface to query unmanaged devices.

    - Click the **Configure > MSP** tab.



- 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 XenMobile.
- Set whether ActiveSync queries are enabled or not. If ActiveSync queries are enabled for the XenMobile 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 XenMobile. To change this behavior, alter the **Filter ActiveSync** field as necessary. Blank means that all devices are forwarded to XenMobile.
- 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



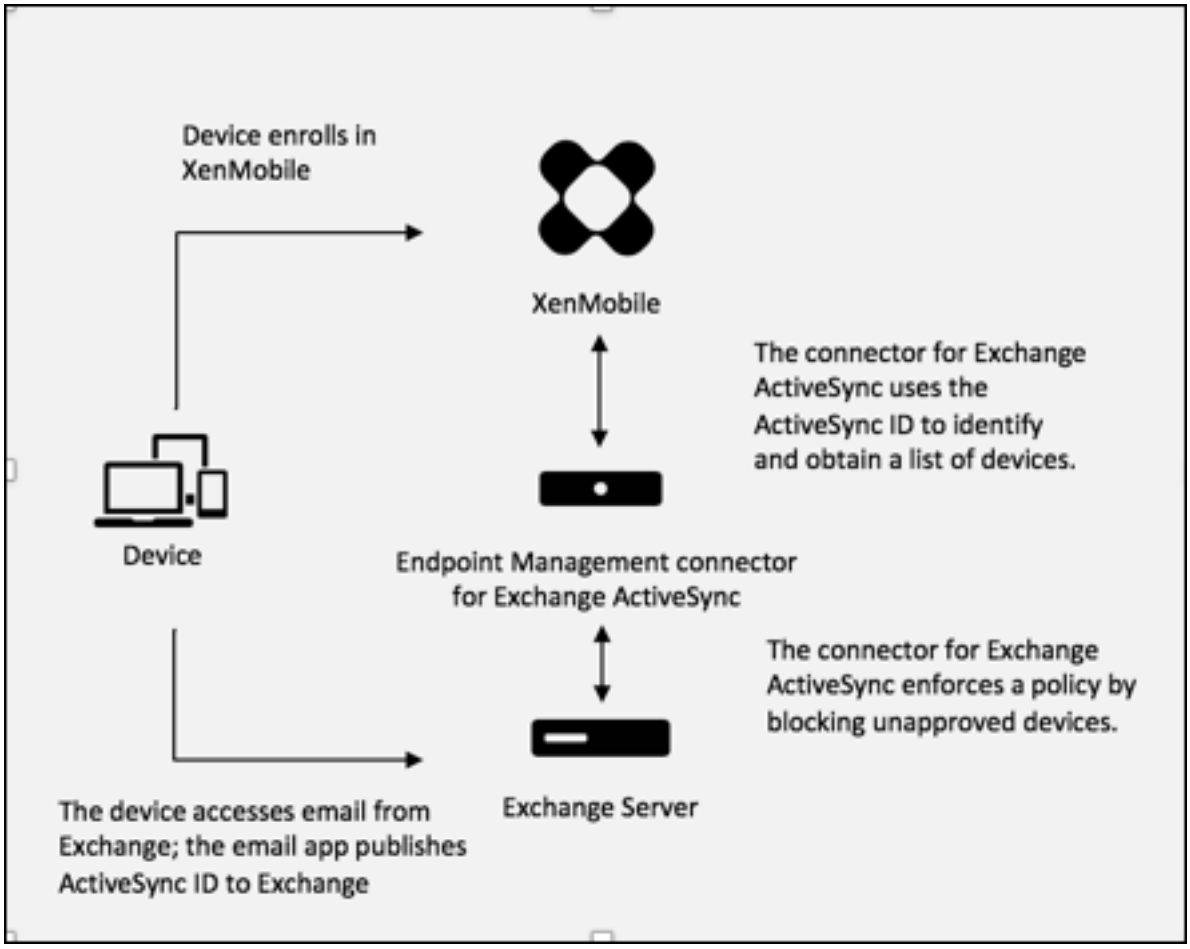
- Enter the database name of the BES management database.

- Select the **Authentication** mode. If you select Windows Integrated authentication, the user account of the Endpoint Management 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 Endpoint Management connector for Exchange ActiveSync database connection, the Windows account specified here must also be given access to the Endpoint Management connector for Exchange ActiveSync 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 Endpoint Management connector for Exchange ActiveSync service user and therefore does not accurately test SQL authentication.
- To support remote Wipe and ResetPassword of BlackBerry devices from XenMobile, 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.
- 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 XenMobile work together to enforce such an email policy. XenMobile sets the policy for corporate email access and, when an unapproved device enrolls with XenMobile, Endpoint Management 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 XenMobile when the device is enrolled. By comparing the two device IDs, Endpoint Management connector for Exchange ActiveSync can determine whether a specific device should have corporate email access. The following figure illustrates this concept:



If XenMobile sends Endpoint Management connector for Exchange ActiveSync an ActiveSync ID that is different from the ID the device publishes to Exchange, Endpoint Management connector for Exchange ActiveSync 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 XenMobile.

To guarantee that your corporate email access policy is enforced properly, you can adopt a defensive security stance and 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 an email client on an Android device and if ActiveSync ID detection does not work properly, the employee is denied corporate email access.

Access control rules

Endpoint Management connector for Exchange ActiveSync provides a rule-based approach for dynamically configuring access control for Exchange ActiveSync devices. An Endpoint Management connector for Exchange ActiveSync 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, XenMobile 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 XenMobile Server rules nor the default access rule will be consulted. Local rules are configured locally to Endpoint Management 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.

XenMobile server rules: XenMobile Server rules are references to an external XenMobile Server that provides rules about managed devices. The XenMobile Server can be configured with its own high-level rules that identify the devices to be allowed or blocked based on properties known to XenMobile, such as whether the device is jailbroken or whether the device contains forbidden apps. XenMobile evaluates the high-level rules and produces a set of allowed or blocked ActiveSync Device IDs, which are then delivered to Endpoint Management connector for Exchange ActiveSync.

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 XenMobile 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 XenMobile Server

rule will be allowed.

- **Default Access – Block:** Any device that is not matched by either a local or XenMobile Server rule will be blocked.
- **Default Access - Unchanged:** Any device that is not matched by either a local or XenMobile Server rule will not have its access state modified in any way by Endpoint Management 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 Endpoint Management connector for Exchange ActiveSync, the rules are evaluated in sequence, from highest to lowest priority as follows:

- Local rules
- XenMobile 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 XenMobile 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.

Endpoint Management 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 Endpoint Management connector for Exchange ActiveSync. Exchange may be configured with three levels of rules: personal exemptions, device rules, and organization settings. Endpoint Management 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, Endpoint Management connector for Exchange ActiveSync effectively takes over management of the exemption lists capability within Exchange. For details, see the Microsoft article, Controlling Device Access.

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.

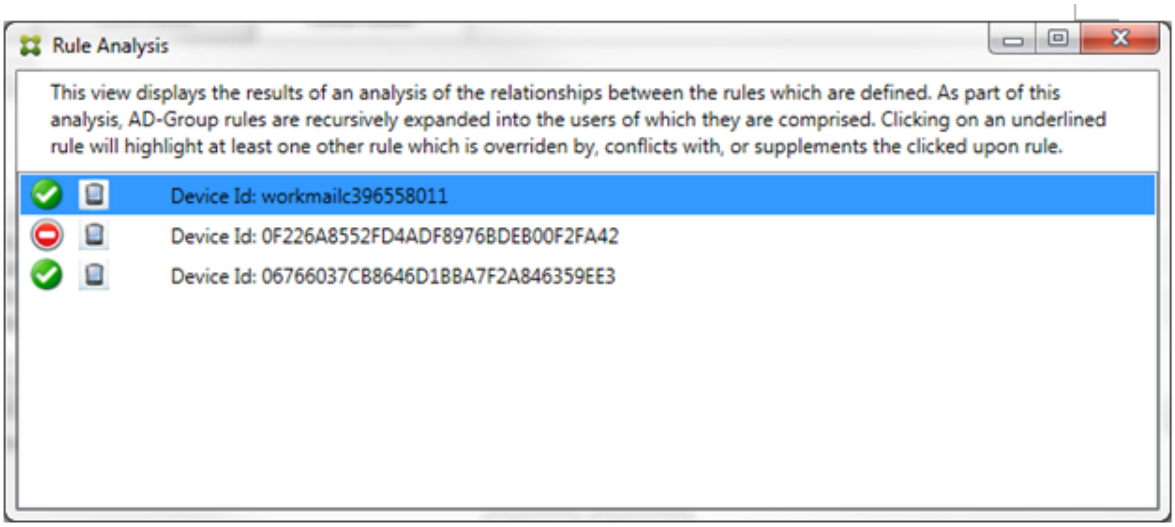
Rule terminology

- **Overriding rule:** An override occurs when more than a single rule could 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 could 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 one to 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, and/or the ancillary rule will conflict in its access with the primary rule, and/or the ancillary rule will supplement the primary rule.

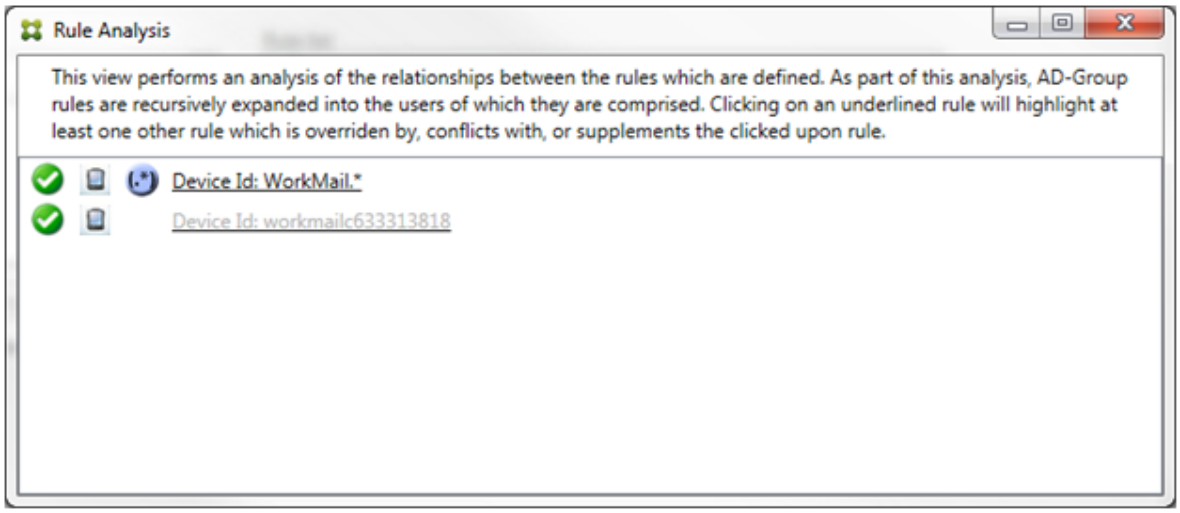
How types of rules appear in the Rule Analysis dialog box

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.

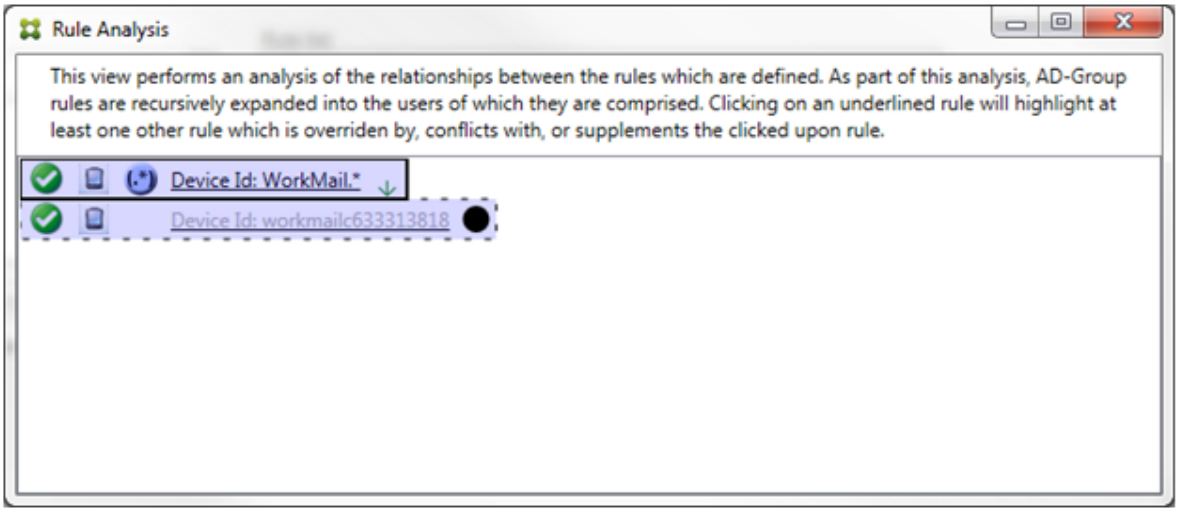
The Rule Analysis window has a check box which, when selected, displays only those rules which are conflicts, overrides, redundancies, or supplements.



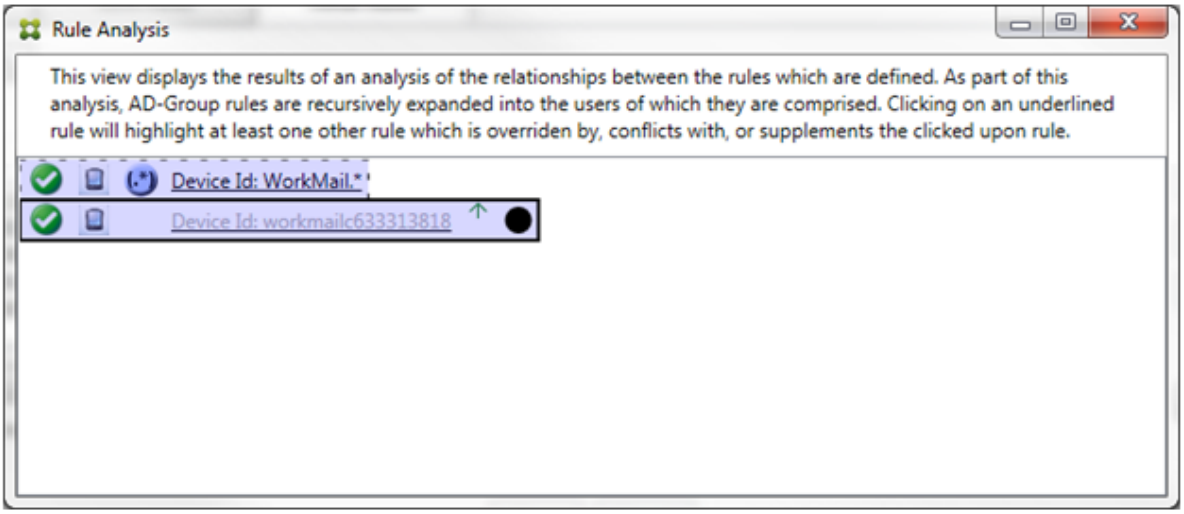
When an override occurs, at least two rules will be underlined: the primary rule and the ancillary rule or rules. At least one ancillary rule appears in a lighter font to indicate that the rule has been overridden by a higher priority rule. You can click the overridden rule to find out which rule or 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:



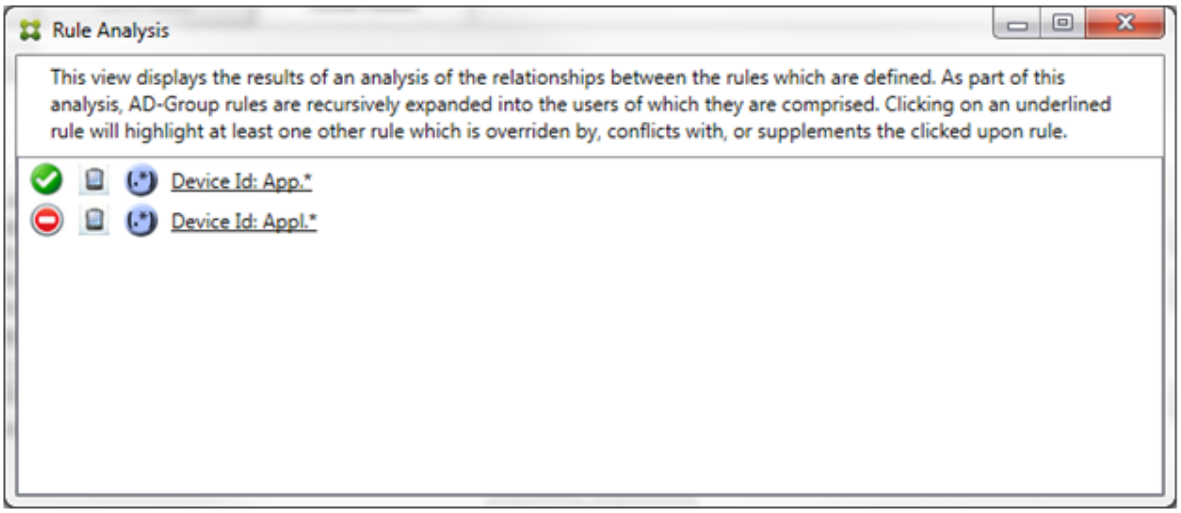
In this example, the regular expression rule `WorkMail.*` is the primary rule (indicated by the solid border) and the normal rule `workmailc633313818` is an ancillary rule (indicated by the dashed border). The black dot next to the ancillary rule is a visual cue that further indicates that the rule is 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:



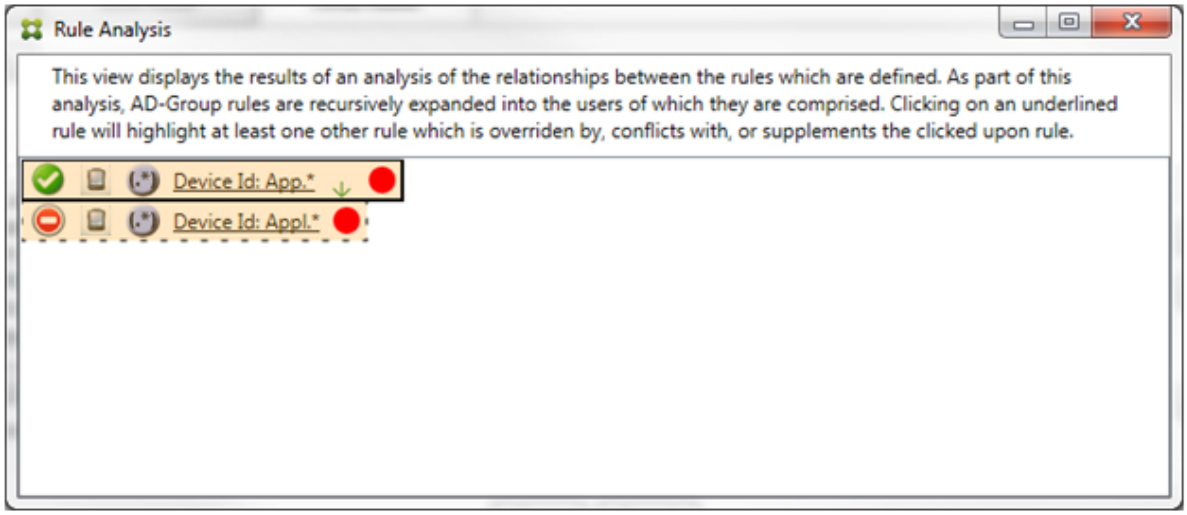
In the preceding example, the regular expression rule `WorkMail.*` is the ancillary rule (indicated by the dashed border) and the normal rule `workmailc633313818` is a primary rule (indicated by the solid border). For this simple example, there's not much difference. For a more complicated example, see 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:



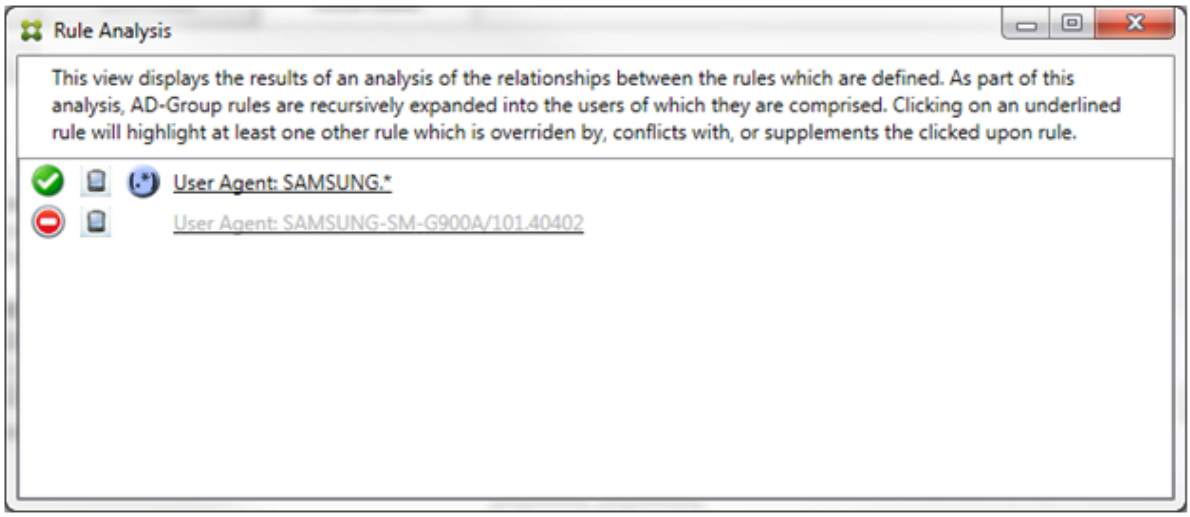
By inspecting the two regular expression rules, it's evident that the first rule allows all devices with a device ID that contains "App" and that the second rule denies all devices with a device ID that contains "Appl". In addition, even though the second rule denies all devices with a device ID that 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.

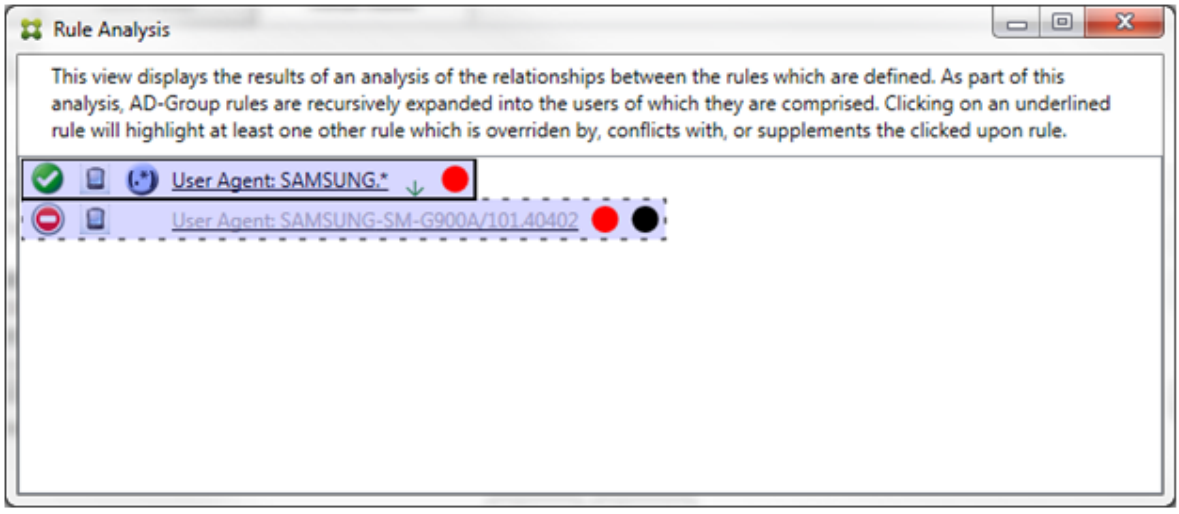
In a scenario with both a conflict and override, both the primary rule (regular expression rule `App.*`) and the ancillary rule (regular expression rule `Appl.*`) are highlighted in yellow. This is simply a visual warning to alert you to the fact that you have applied more than a single regular expression

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.

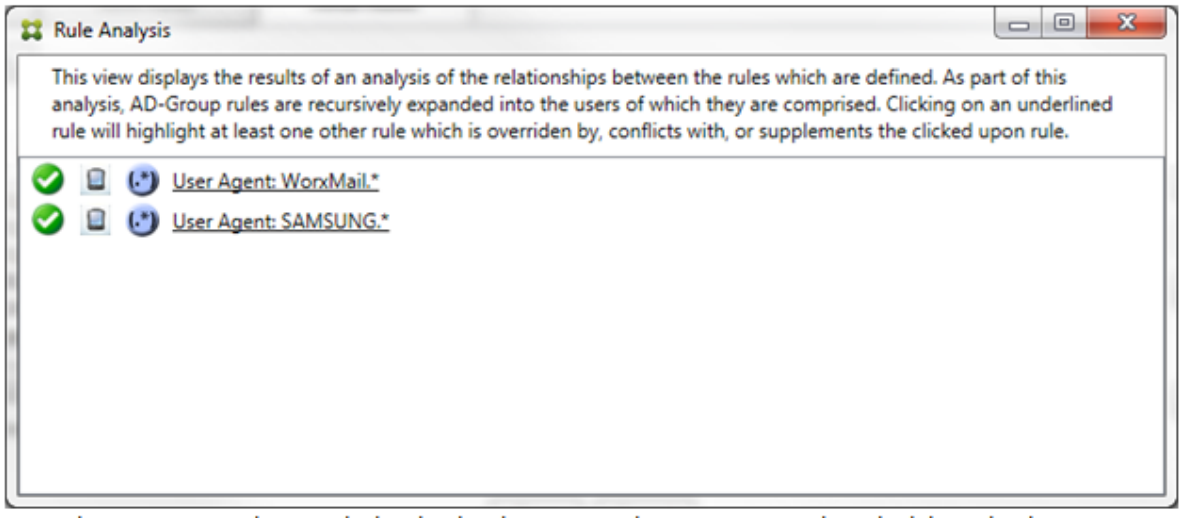
After clicking the regular expression rule, the dialog box appears as follows:



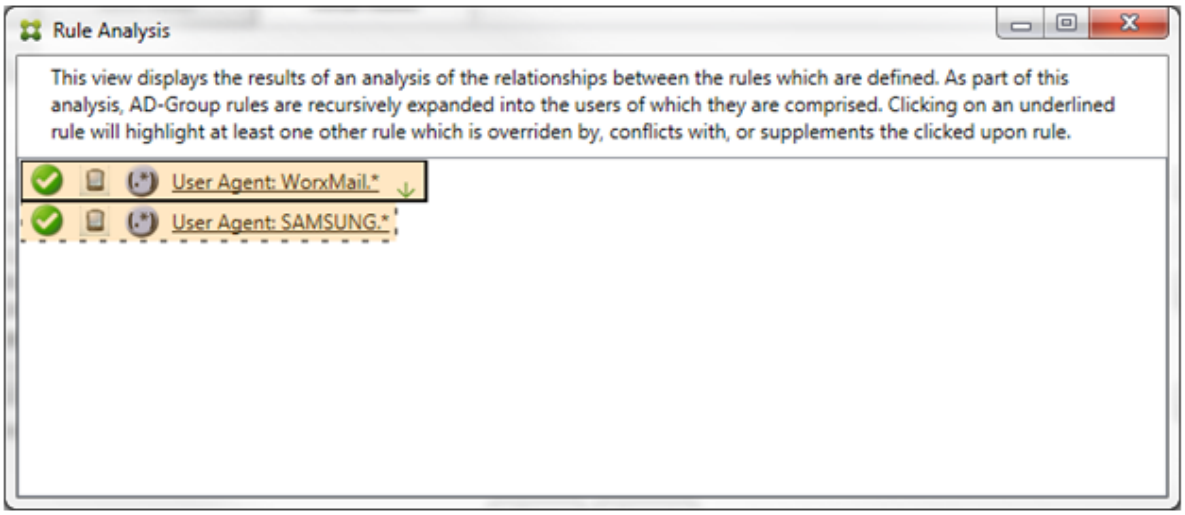
The primary rule (regular expression rule `SAMSUNG.*`) is followed by a red dot to indicate that its access state conflicts with one or more ancillary rules. The ancillary rule (normal rule `SAMSUNG-SM-G900A/101.40402`) is followed by a red dot to indicate that its access state conflicts with the primary 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 rules supplement one an-

other, they are indicated with a yellow overlay. Prior to clicking either of the rules, in a simple example, the dialog box appears as follows:



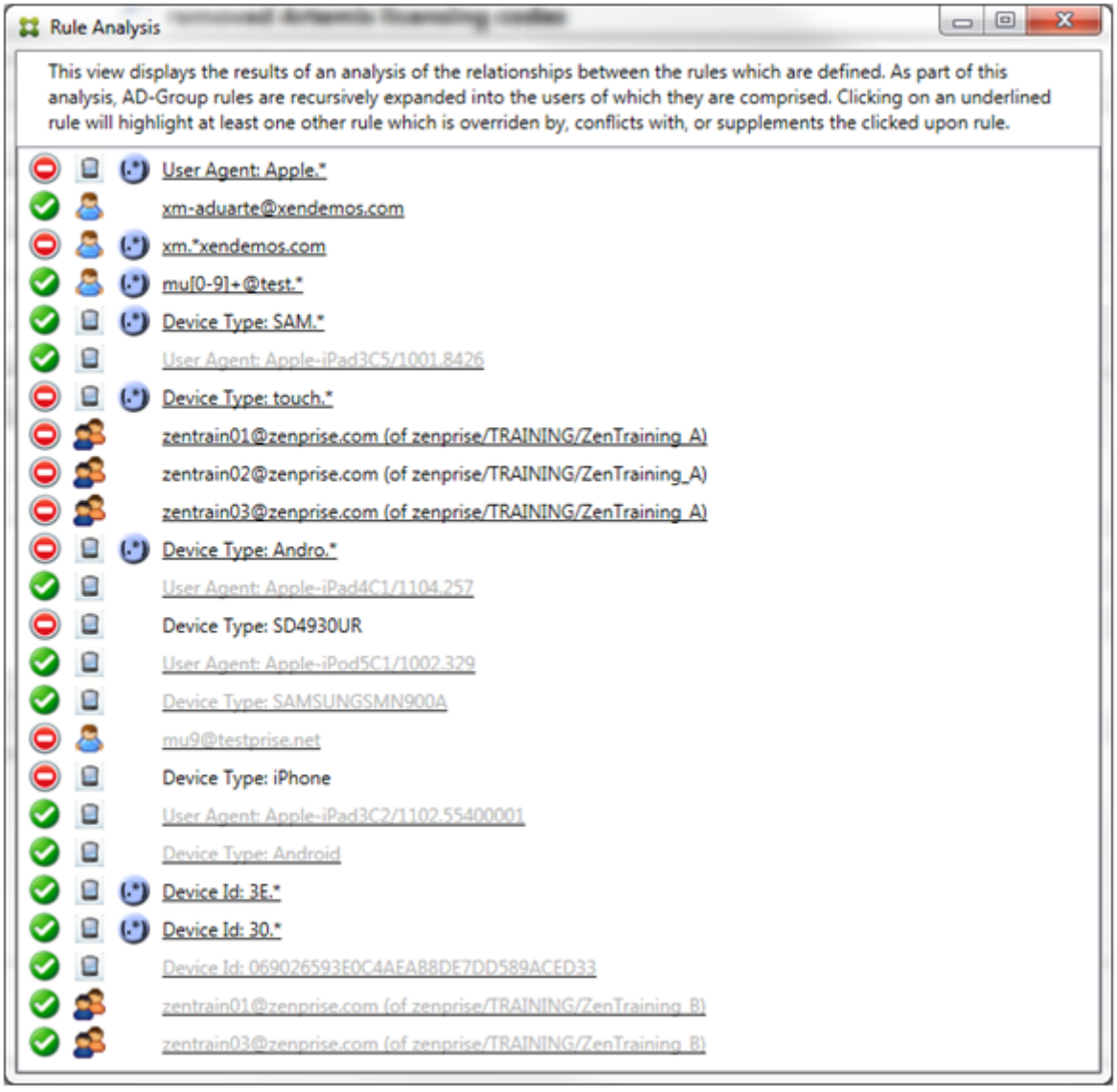
Visual inspection easily reveals that both rules are regular expression rules which have both been applied to the ActiveSync device ID field in Endpoint Management connector for Exchange ActiveSync. After clicking the first rule, the dialog box looks as follows:



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 Endpoint Management 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

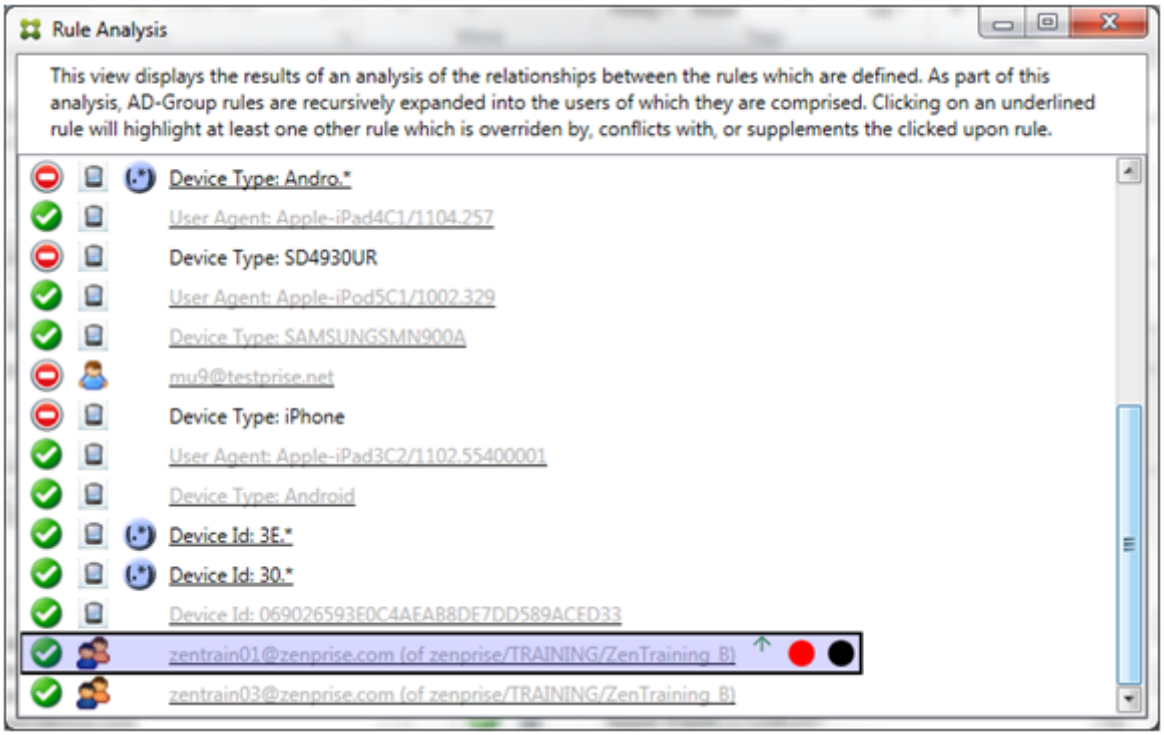
Many potential overrides, conflicts, or supplements can occur, making it impossible to give an example of all possible scenarios. The following example discusses what not to do, while also serving to illustrate the full power of the rule analysis visual construct. Most of the items are underlined in 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.

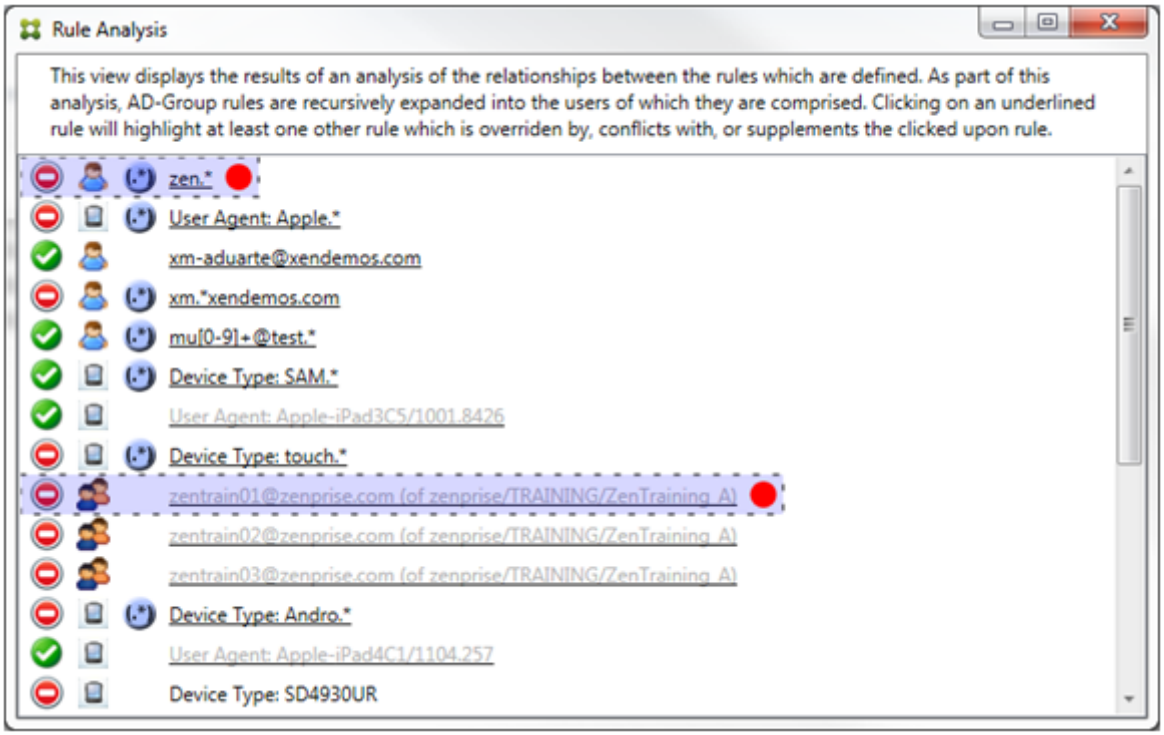
Example 1: This example examines why `zentrain01@zenprise.com` has been overridden.



The primary rule (AD-Group rule `zenprise/TRAINING/ZenTraining B`, of which `zentrain01@zenprise.com` is a member) has the following characteristics:

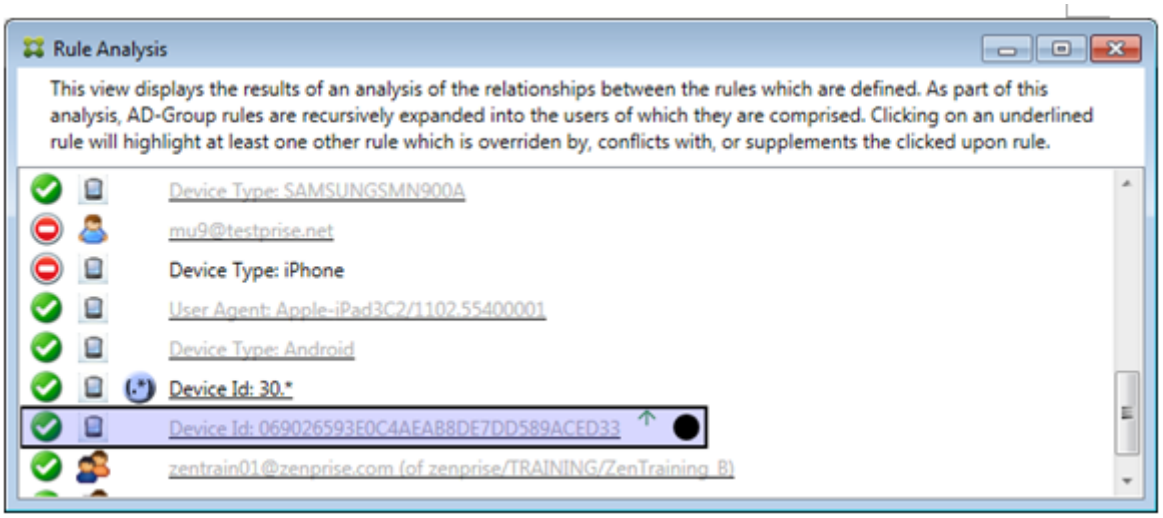
- Is highlighted in blue and has a solid border.
- Has an upwards pointing green arrow (to indicate that the ancillary rule or rules are all to be found above it).
- Is followed by both a red circle and black circle to indicate respectively that one or more ancillary rule conflicts with its access and that the primary rule has been overridden and is hence inactive.

When you scroll up, you see the following:



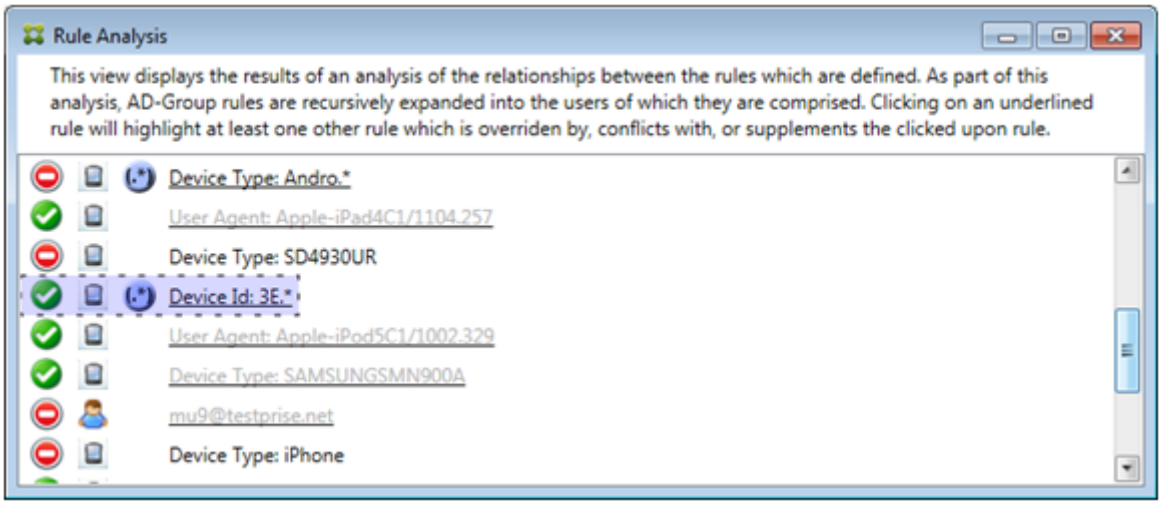
In this case, there are two ancillary rules that override the primary rule: the regular expression rule `zen.*` and the normal rule `zentrain01@zenprise.com` (of `zenprise/TRAINING/ZenTraining A`). In the case of the latter ancillary rule, what has occurred is that the Active Directory Group rule `ZenTraining 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.

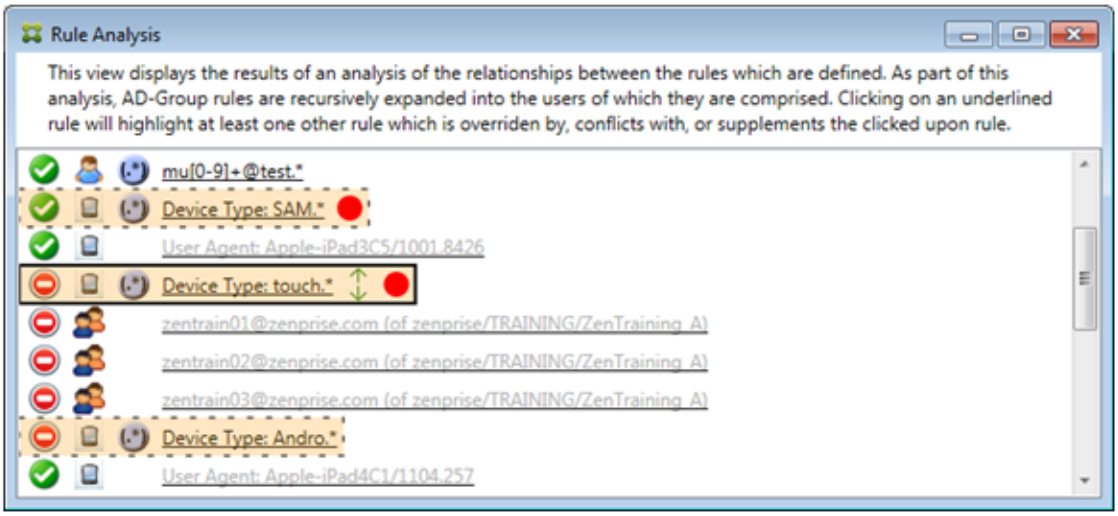


In this case, a single ancillary rule overrides the primary rule: The regular expression ActiveSync device ID rule is `3E.*` Because the regular expression `3E.*` would match `069026593E0C4AEAB8DE7DD589ACED33`, the primary rule will never be evaluated.

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 ActiveSync device type.
- You should ensure in such scenarios that their regular expression rules are not redundant.



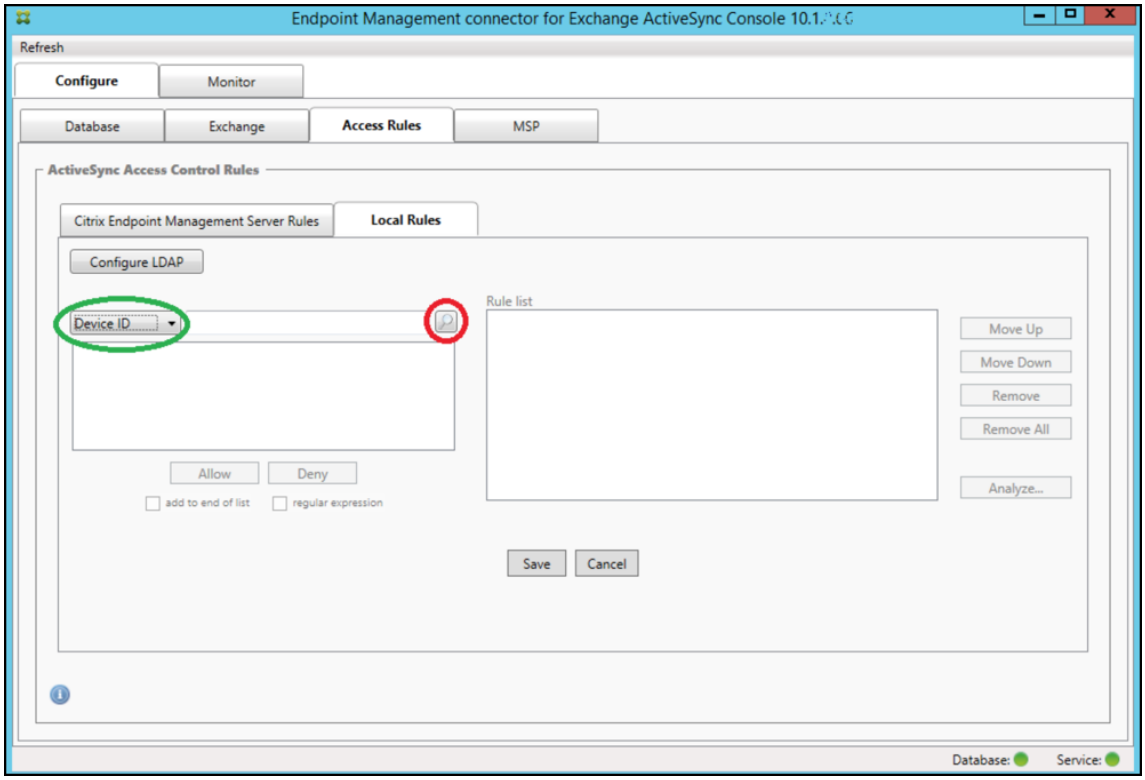
How to further analyze the rules

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.

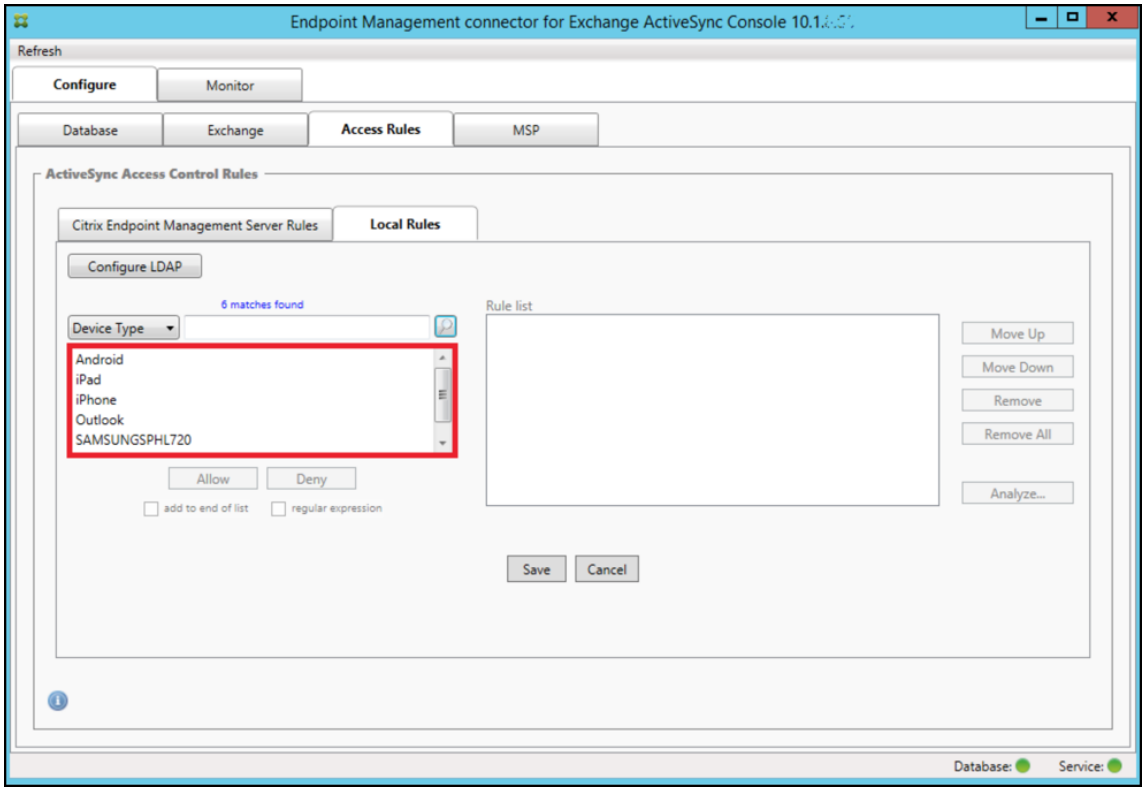
The example shows an overridden rule that is included in the rule relationship. This rule is the normal ActiveSync device type rule `Android`, which is overridden (indicated by the lightened font and the black circle next to it) and also conflicts in its access with the primary rule regular expression 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 Rule**s tab.



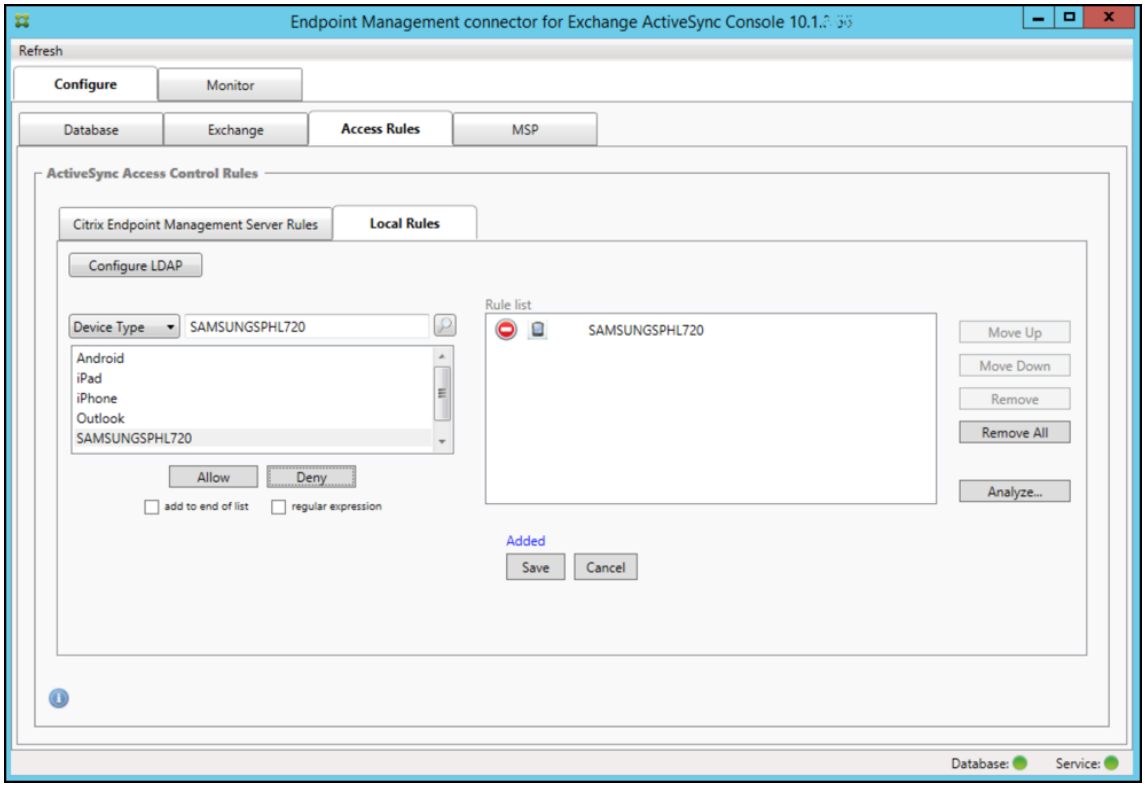
2. In the **Device ID** list, select the field for which you want to create a Local Rule.
3. Click the magnifying glass icon to display all of the unique matches for the chosen field. In this example, the field **Device Type** has been chosen and the choices are shown below in the list box.



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.



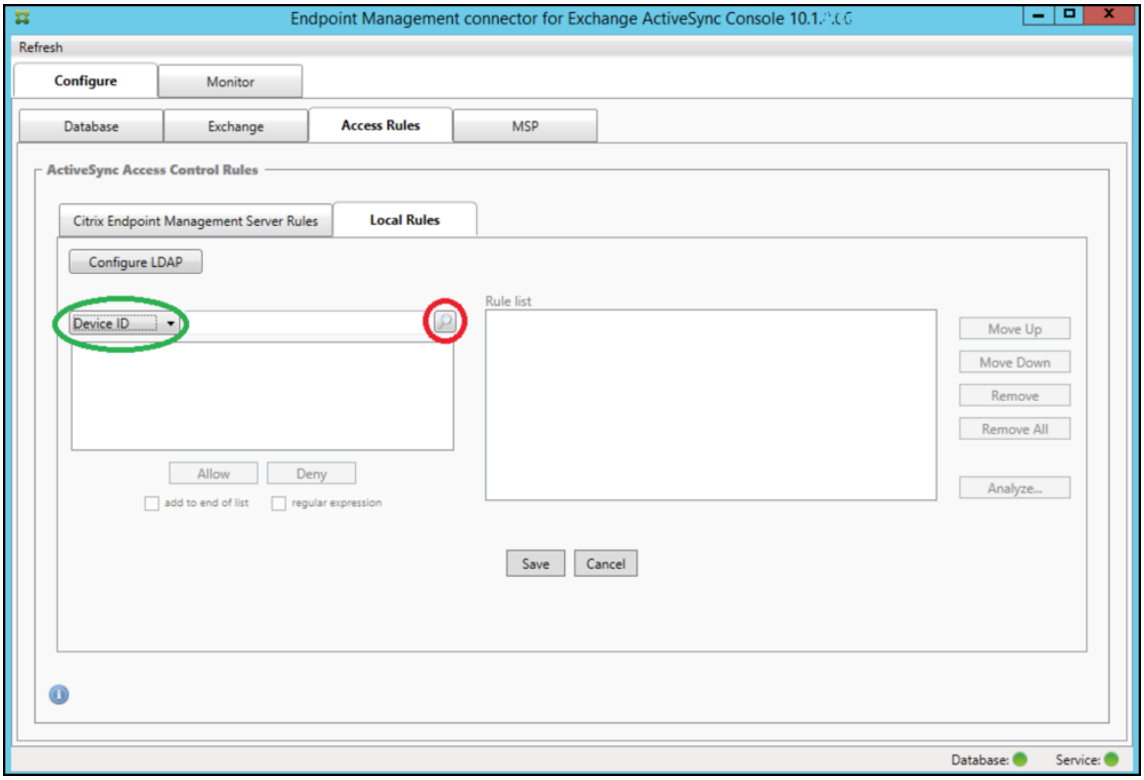
To add a regular expression

Regular expression local rules can be distinguished by the icon which appears next to them -  .

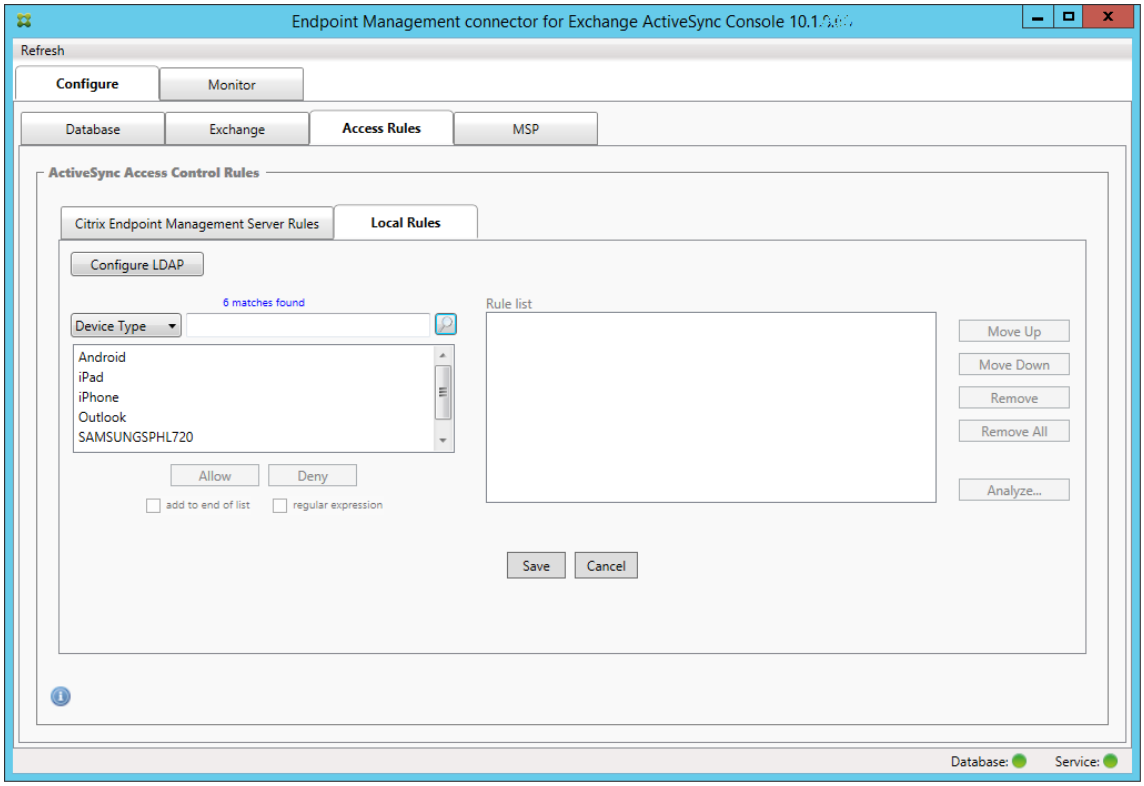
To add a regular expression rule, you can either build a regular expression rule from an existing value from the results list for a given field (as long as a major snapshot has completed), or you can simply type in the regular expression that you want.

To build a regular expression from an existing field value

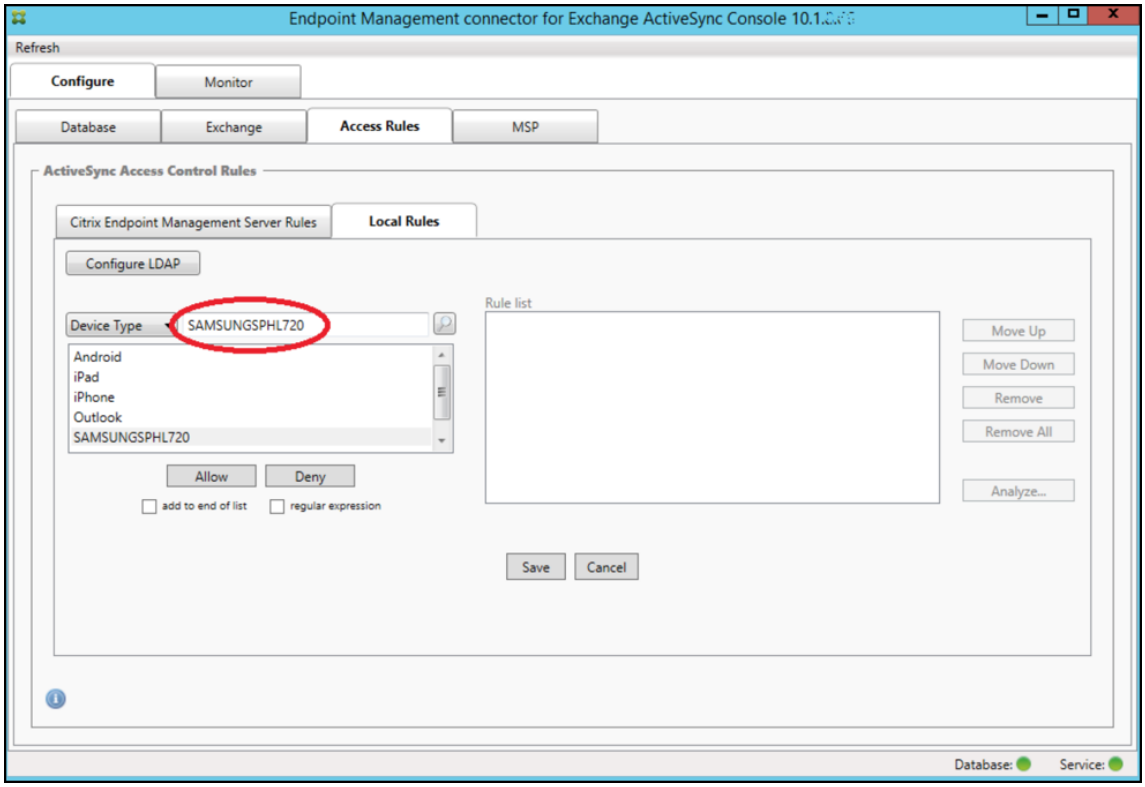
1. Click the **Access Rules** tab.



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**.



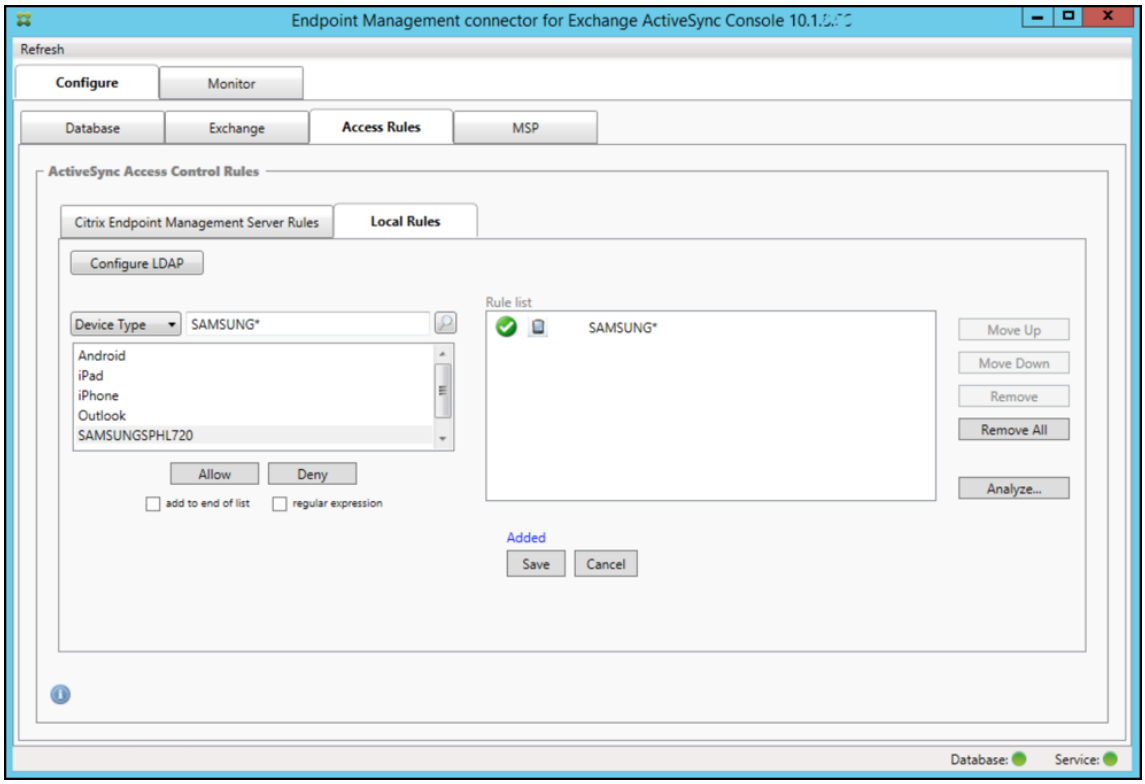
5. To allow all device types that have “Samsung” in their device type value, add a regular expression rule by following these steps:

   a) Click within the selected item text box.

   b) Change the text from **SAMSUNGSPHL720** to **SAMSUNG.***.

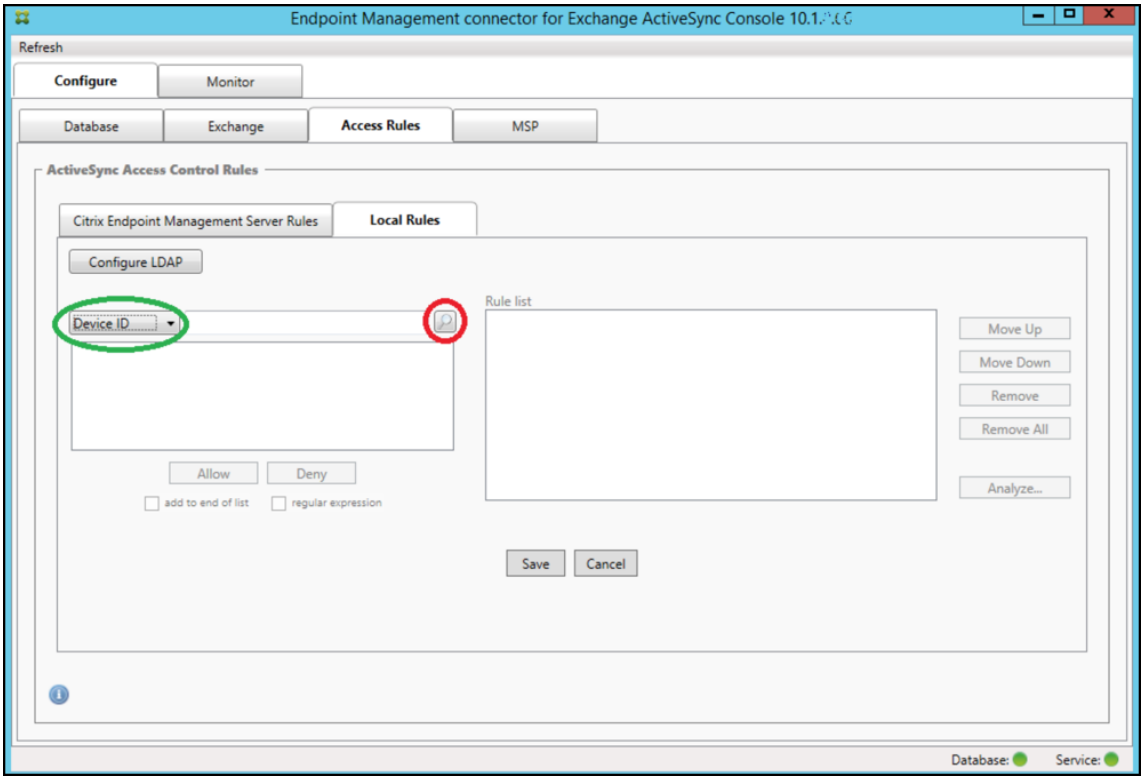
   c) Ensure that the regular expression check box is selected.

   d) Click **Allow**.

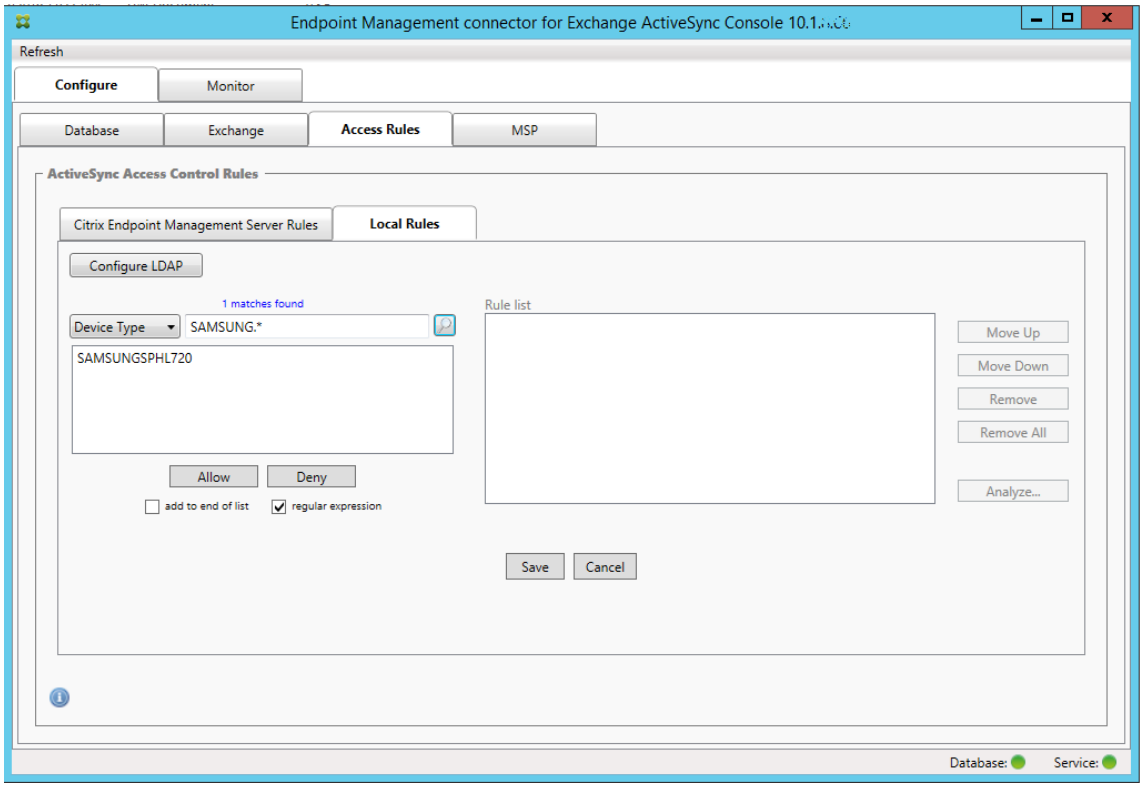


To build an access rule

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.



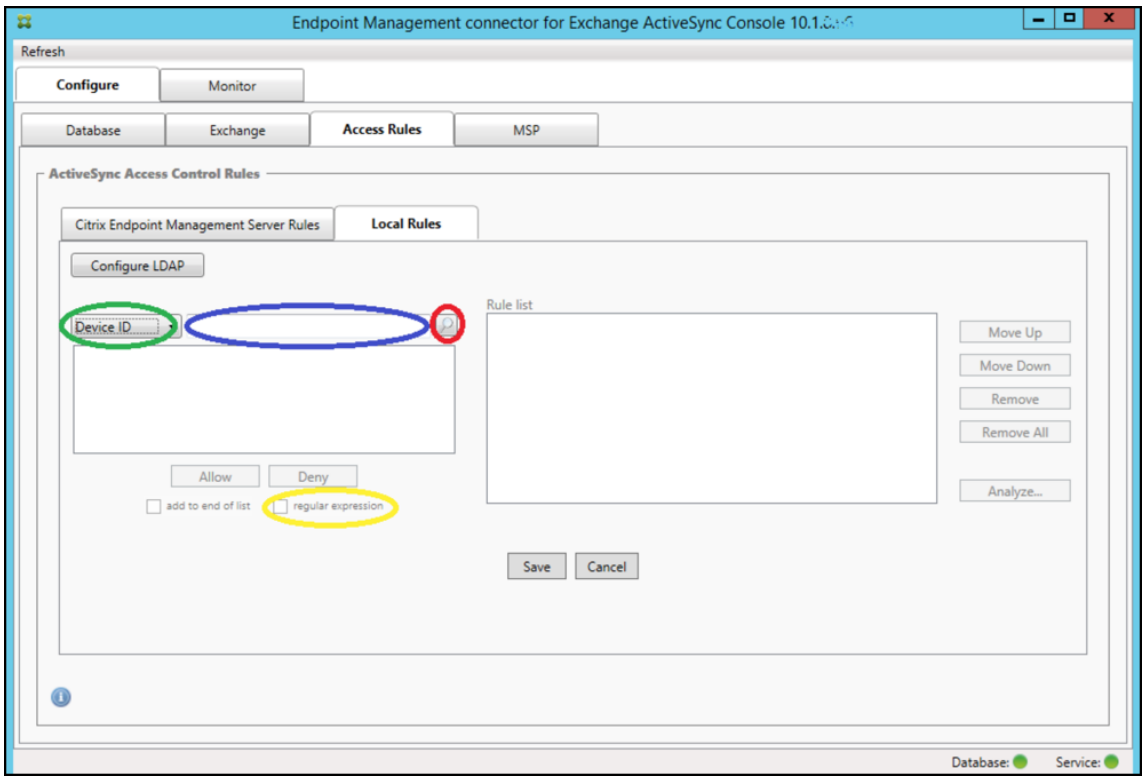
3. Select the field you want to match against. This example uses Device Type.
4. Type in the regular expression. This example uses `samsung.*`
5. Ensure that the regular expression check box is selected and then click **Allow** or **Deny**. In this example, the choice is **Allow**. The final result is as follows:



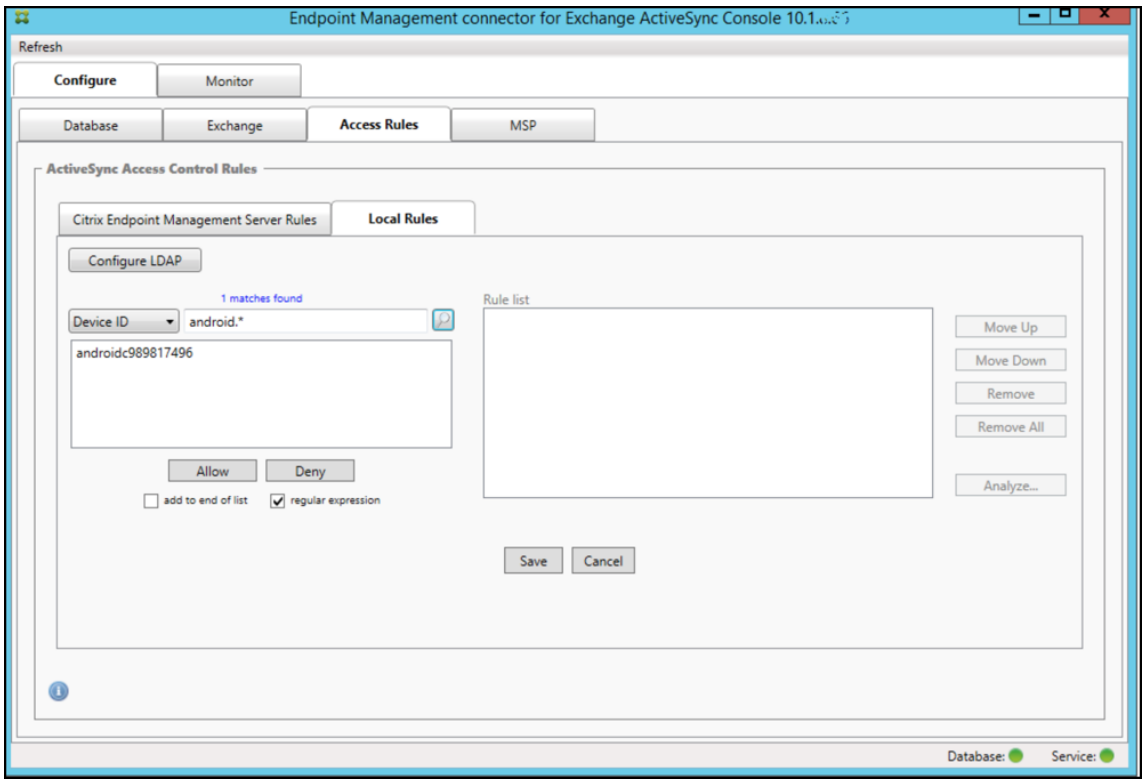
To find devices

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 matches as shown in the following figure.

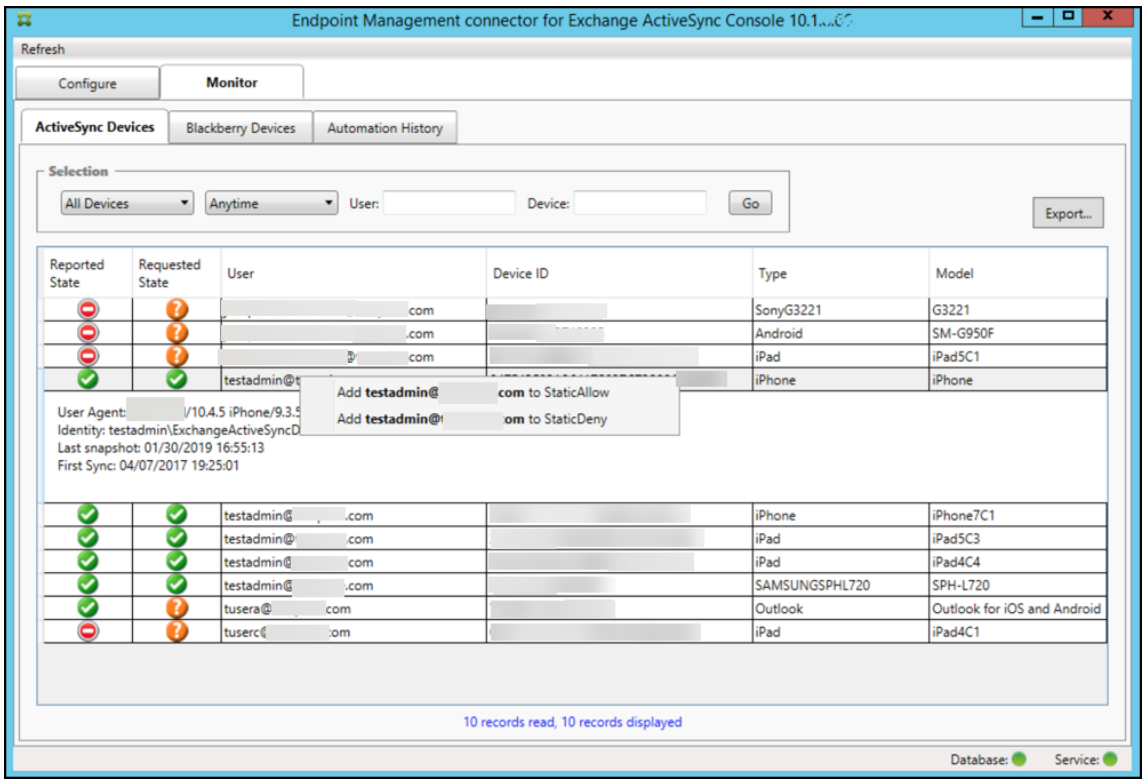


To add an individual user, device, or device type to a static rule

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. Endpoint Management 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 *minilevel* 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:

- Endpoint Management 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 Endpoint Management 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 Endpoint Management connector for Exchange ActiveSync service must be an allowed SQL logon. The account of the Endpoint Management 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.

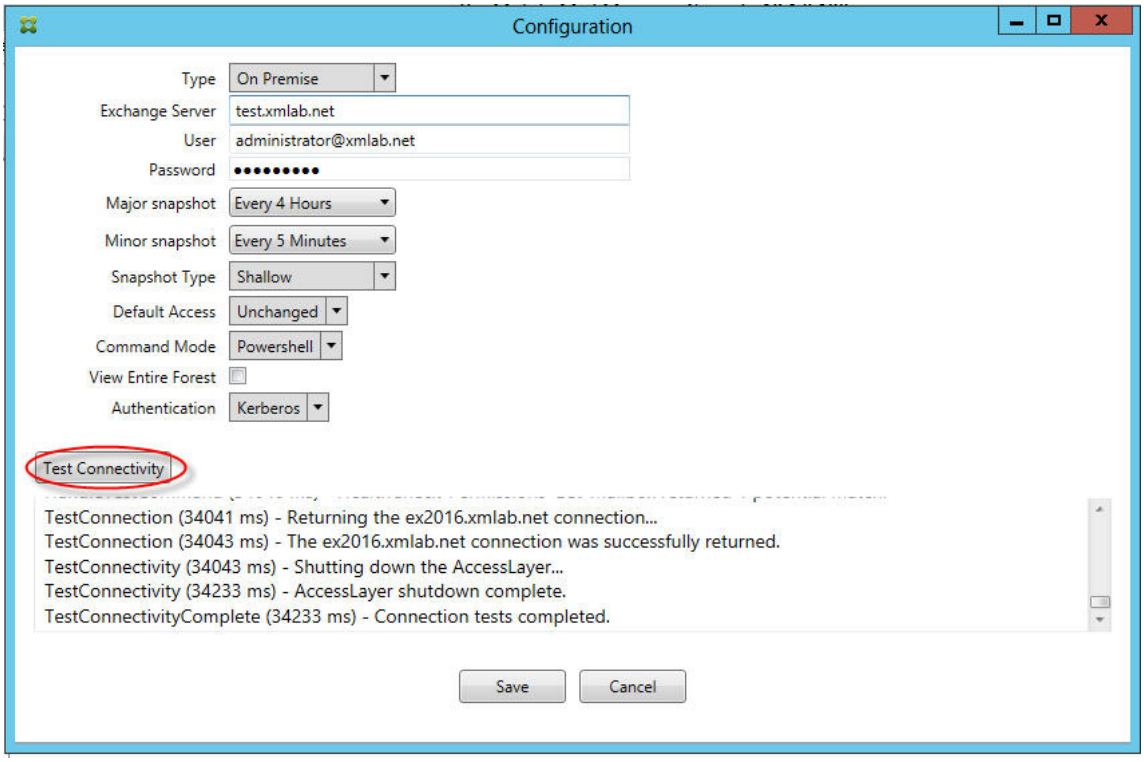
- XenMobile cannot connect to the MSP

  Check that the MSP service port and transport is properly configured in the **Configure > MSP** tab of the Endpoint Management 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, IIS Manager can be used to install the certificate. If IIS is not installed, see How to configure a port with an SSL certificate for details on installing certificates.

  Endpoint Management connector for Exchange ActiveSync 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 XenMobile and then click **Test Connectivity**. This simulates the web service requests that XenMobile Server issues. Note that 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 raw output of all cmdlets to a text file.

Citrix Gateway connector for Exchange ActiveSync

January 6, 2021

XenMobile Citrix ADC Connector is now 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 ADC acting as a reverse proxy for the Exchange ActiveSync protocol. Authorization is controlled by a combination of policies that you define within XenMobile and by rules defined locally by Citrix Gateway connector for Exchange ActiveSync.

For more information, see ActiveSync Gateway.

For a detailed reference architecture diagram, see Architecture.

The current release of Citrix Gateway connector for Exchange ActiveSync is version 8.5.2.

What's new

The following sections list what's new in the current and earlier versions of Citrix Gateway connector for Exchange ActiveSync, formerly XenMobile Citrix ADC Connector.

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 version 8.5.2

- XenMobile Citrix ADC Connector is now 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 one of the criteria involves the user ID, the following issue may occur: If a user has more aliases, the aliases are not also checked when applying the rule. [CXM-55355]

> **Note:**
>
> The following What's New section refers to Citrix Gateway connector for Exchange ActiveSync by its former name of XenMobile Citrix ADC Connector. The name changed as of version 8.5.2.

What's new in version 8.5.1.11

- **System requirement change:** The current version of Citrix ADC Connector requires Microsoft .NET Framework 4.5.
- **Google Analytics support:** We want to know how you use XenMobile Citrix ADC 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, TLS 1.0 is being deprecated by the PCI Council. Support for TLS 1.1 and 1.2 is added to XenMobile Citrix ADC Connector.

Monitoring Citrix Gateway connector for Exchange ActiveSync

The Citrix Gateway connector for Exchange ActiveSync configuration utility provides detailed logging that you can use to view all traffic passing through your Exchange Server that is either allowed or blocked by Secure Mobile Gateway.

Use the **Log** tab to view the history of the ActiveSync requests forwarded to the connector for Exchange ActiveSync by Citrix ADC for authorization.

Also, to ensure that the Citrix Gateway connector for 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 Citrix Gateway connector for Exchange ActiveSync

You can use the Citrix Gateway connector for Exchange ActiveSync to simulate what ActiveSync traffic will look like in conjunction with your policies. In the connector configuration utility, select the **Simulator** tab. The results show you how your policies will apply according to the rules you have configured.

Choosing filters for Citrix Gateway 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 within XenMobile. The two options for each filter are **Allow** or **Deny**.

- **Anonymous Devices:** Allows or denies devices that are enrolled in XenMobile but the user's identity is unknown. For example, this could be a user who was enrolled, but the user's Active Directory password is expired, or a user who enrolled with unknown credentials.
- **Failed Samsung KNOX attestation:** Samsung devices have functionality for security and diagnostics. This filter provides confirmation that the device is setup for KNOX. For details, see Samsung Knox.
- **Forbidden Apps:** Allows or denies devices based on the Device List defined by block list policies and the presence of blocked apps.
- **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 Citrix Gateway 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 of the other connector filters that have not been selected. For example, the connector denies blocked apps yet 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 XenMobile within a specified period of 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 they should 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 if the device does or does not meet 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 XenMobile database. The Mobile Application Gateway needs to be deployed in a Block Mode.

To configure a connection to Citrix Gateway connector for Exchange ActiveSync

Citrix Gateway connector for Exchange ActiveSync communicates with XenMobile and other remote configuration providers through secure web services.

1. In the connector 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 XenMobile Server.
3. In **Url**, enter the web address of the XenMobile GCS, typically in the format `https://<FQDN>/<instanceName>/services/<MagConfigService>`. The *MagConfigService* name is case-sensitive.
4. In **Password**, enter the password that will be used for basic HTTP authorization with the XenMobile Server.
5. In **Managing Host**, enter the connector server name.
6. In **Baseline Interval**, specify a time period for when a new refreshed dynamic ruleset is pulled from Device Manager.
7. In **Delta interval**, specify a time period for when an update of dynamic rules is pulled.

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 to notify XenMobile when a device is blocked. This option is required if you are using the connector rules in any of your XenMobile 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 new configuration provider, Citrix Gateway connector for Exchange ActiveSync automatically creates one or more policies associated with the provider. These policies are defined by a template definition contained in config\policyTemplates.xml in the NewPolicyTemplate section. For each Policy element defined within this section, a new policy is created.

The operator may 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 XenMobile

1. In the Citrix Gateway 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 will be used for basic HTTP authorization with the XenMobile Server and that has administrative privileges.
3. In **Url**, enter the web address of the XenMobile 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 XenMobile 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 XenMobile 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

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. No other filtering rules are used.
- **Deny All**. This policy mode blocks access for all traffic passing through the connector. No other filtering rules are used.
- **Static Rules: Block Mode**. This policy mode executes static rules with an implicit deny or block statement at the end. The connector blocks devices that are not allowed or permitted via other filter rules.
- **Static Rules: Permit Mode**. This policy mode executes 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.
- **Static + ZDM Rule**s: Block Mode. This policy mode executes static rules first, followed by dynamic rules from XenMobile with an implicit deny or block statement at the end. Devices are permitted or denied based on defined filters and Device Manager rules. Any devices that do not match on defined filters and rules are blocked.
- **Static + ZDM Rule**s: Permit Mode. This policy mode executes static rules first, followed by dynamic rules from XenMobile with an implicit permit or allow statement at the end. Devices are permitted or denied based on defined filters and XenMobile rules. Any devices that do not match on defined filters and rules are allowed.

The Citrix Gateway 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 XenMobile. Android devices differ in their behavior based on the manufacturer and some do not readily expose a unique ActiveSync ID. To compensate, XenMobile 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 rules on the **Policies** tab of the configuration utility. The rules are processed on Citrix Gateway connector for Exchange ActiveSync from top to bottom. The Allow policies are displayed with 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 rules, click the **Simulator** tab. Specify values in the fields. These can also be obtained from the logs. A result message will appear specifying 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 Citrix Gateway connector for Exchange ActiveSync to permit or block traffic by the following criteria:

- **User**. Citrix Gateway connector for Exchange ActiveSync uses the authorized user value and name structure that was captured during device enrollment. This is commonly found as domain\username as referenced by the server running XenMobile connected to Active Directory via LDAP. The **Log** tab within the connector configuration utility shows the values that are passed through the connector. The values are passed if the value structure needs to be determined or is different.
- **Deviceid (ActiveSyncID)**. Also known as the ActiveSyncID of the connected device. This value is commonly found within the specific device properties page in the XenMobile console. This value can also be screened from the Log tab in the connector configuration utility.
- **DeviceType**. The connector 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. In most cases, the value specified corresponds to a specific operating system build and version for the mobile device platform.

The connector 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. Additionally, 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 XenMobile define dynamic rules and can trigger a dynamic Citrix Gateway connector for Exchange ActiveSync filter. The triggers are based on the presence of a policy violation or property setting. The connector 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.

> **Note:**
>
> You must use the XenMobile console to configure dynamic rules.

1. In the XenMobile 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 XenMobile sends Android device information to the Secure Mobile Gateway.

   When this option is enabled, XenMobile sends Android device information to the Citrix Gateway connector for Exchange ActiveSync when XenMobile does not have the ActiveSync identifier for the Android device user.

To configure custom policies by editing the Citrix Gateway connector for Exchange ActiveSync XML file

You can view the basic policies in the default configuration on the **Policies** tab of the Citrix Gateway connector for Exchange ActiveSync configuration utility. If you want to create custom policies, you can edit the connector 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 Citrix Gateway connector for Exchange ActiveSync XML file

The Citrix Gateway 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 Citrix ADC 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 will "pass." 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

Additionally, 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 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 may 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. Citrix Gateway connector for Exchange ActiveSync connects the groups on a periodic basis. XenMobile can export groups of allowed and blocked devices and users to the connector.

Dynamic groups are maintained by an external source called a Gateway Configuration Provider and collected by Citrix Gateway connector for Exchange ActiveSync on a periodic basis. XenMobile 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 may 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 may 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 will be the most logical choice.

The configuration scenarios that Citrix allows for integrating Citrix Gateway connector for Exchange ActiveSync with XenMobile 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 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 Citrix Gateway connector for Exchange ActiveSync configuration utility, you can build dynamic and static rules that enforce corporate email policies, allowing 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 and only viewable on managed devices by authorized users.

To uninstall Citrix Gateway connector for Exchange ActiveSync

1. Run XncInstaller.exe with an administrator account.
2. Follow the onscreen instructions to complete the uninstallation.

To install, upgrade, or uninstall Citrix Gateway connector for Exchange ActiveSync

1. Run XncInstaller.exe with an administrator account to install the connector 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, you must manually restart the XenMobile configuration service and the notification service.

Installing Citrix Gateway connector for Exchange ActiveSync

You install Citrix Gateway connector for Exchange ActiveSync on its own Windows Server.

The CPU load that the connector puts on a server depends on how many devices are managed. For large numbers of devices (more than 50,000), you may need to provision more than one core 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

Citrix Gateway connector for Exchange ActiveSync communicates with Citrix ADC over an SSL bridge configured on the Citrix ADC appliance. The bridge enables the appliance to bridge all secure traffic directly to XenMobile. The connector requires 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)

Component	Requirement
Citrix ADC	Citrix ADC 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 Citrix Gateway 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 Citrix Gateway 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 Citrix Gateway 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

Citrix Gateway connector for Exchange ActiveSync enables you to use Citrix ADC to proxy and load balance XenMobile Server communication with XenMobile managed devices. The connector communicates periodically with XenMobile to synchronize policies. The connector and XenMobile can be clustered, together or independently, and can be load-balanced by Citrix ADC.

Citrix Gateway connector for Exchange ActiveSync components

- **Citrix Gateway connector for Exchange ActiveSync service:** This service provides a REST web service interface that can be invoked by Citrix ADC to determine if an ActiveSync request from a device is authorized.
- **XenMobile configuration service:** This service communicates with XenMobile to synchronize XenMobile policy changes with the connector.
- **XenMobile notification service:** This service sends notifications of unauthorized device access to XenMobile. In this way, XenMobile can take appropriate measures, such as notifying the user why the device was blocked.
- **Citrix Gateway connector for Exchange ActiveSync configuration utility:** This application allows the administrator to configure and monitor the connector.

To set up listening addresses for Citrix Gateway connector for Exchange ActiveSync

For Citrix Gateway connector for Exchange ActiveSync to receive requests from Citrix ADC to authorize ActiveSync traffic, do the following. Specify the port on which the connector listens to Citrix ADC web service calls.

1. From the **Start** menu, select the Citrix Gateway 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 is co-resident with XenMobile (installed on the same server), select port values that do not conflict with XenMobile.
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 Citrix Gateway 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 XenMobile policies, select **Static + ZDM: Permit Mode or Static + ZDM: Block Mode**. These policies combine local (or, static) rules with the rules from XenMobile. 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 XenMobile

Specify the name and properties of the XenMobile Server (also known as a Config Provider) that you want to use with Citrix Gateway connector for Exchange ActiveSync and Citrix ADC.

> **Note:**
>
> This task assumes that you have already installed and configured XenMobile.

1. In the Citrix Gateway connector for Exchange ActiveSync configuration utility, click the **Config Providers** tab and then click **Add**.
2. Enter the name and URL of the XenMobile Server you are using in this deployment. If you have multiple XenMobile Servers deployed in a multitenant deployment, this name must be unique for each server instance. For example, for **Name**, you could type **XMS**.
3. In **Url**, enter the Web address of the XenMobile GlobalConfig Provider (GCP), typically in the format `https://<FQDN>/<instanceName>/services/<MagConfigService>`. The *MagConfigService* name is case-sensitive.
4. In **Password**, enter the password that will be used for basic HTTP authorization with the XenMobile web server.
5. In **Managing Host**, enter the server name where you installed Citrix Gateway connector for Exchange ActiveSync.
6. In **Baseline Interva**l, specify a time period for when a new refreshed dynamic ruleset is pulled from XenMobile.
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 XenMobile when a device is blocked. This option is required if you are using Secure Mobile Gateway rules in any of your Device Manager Automated Actions.
10. After configuring the server, click **Test Connectivity** to test the connection to XenMobile.
11. When connectivity has been established, click **Save**.

Deploying Citrix Gateway connector for Exchange ActiveSync for redundancy and scalability

If you want to scale your Citrix Gateway connector for Exchange ActiveSync and XenMobile deployment, you can install instances of the connector on multiple Windows Servers, all pointing to the same XenMobile instance, and then you can use Citrix ADC to load balance the servers.

There are two modes for the Citrix Gateway connector for Exchange ActiveSync configuration:

- In non-shared mode, each Citrix Gateway connector for Exchange ActiveSync instance communicates with a XenMobile Server and keeps its own private copy of the resulting policy. For example, if you had a cluster of XenMobile Servers, you could run a connector instance on each XenMobile Server and the connector would get policies from the local XenMobile instance.
- In shared mode, one connector node is designated the primary node and it communicates with XenMobile. The resulting configuration is shared among the other nodes either by a Windows network share or by Windows (or third-party) replication.

The entire connector 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. But the system can tolerate the primary server being down for a few minutes (for example, to restart) because the last known good configuration is cached in the connector process.

Advanced Concepts

April 25, 2019

> **Note:**
>
> This article covers advanced concepts for XenMobile Server. For advanced information about Endpoint Management, see Advanced concepts.

The XenMobile Advanced Concepts articles offer a deeper dive into product documentation on XenMobile. The aim is to help reduce deployment time through expert techniques. The articles may cite the technical expert or experts who have authored the content.

For decision points, recommendations, common questions, and use cases for your end-to-end XenMobile environment, see the XenMobile Deployment Handbook in this section.

For community support forums on XenMobile, see Citrix Discussions.

On-premises XenMobile interaction with Active Directory

April 25, 2019

Contributed by Siddartha Vuppala

This article explains the interaction between XenMobile Server and Active Directory. XenMobile Server interacts with Active Directory both inline and in the background. The following sections provide more information on the inline and the background operations that involve Active Directory interaction.

> **Note:**
>
> This article is an overview of the interaction and does not cover the granular details. For more information about configuring Active Directory and LDAP in the XenMobile console, see Domain or domain plus security token authentication.

Inline interactions

XenMobile Server communicates with Active Directory by using the LDAP settings that an administrator configures. The settings retrieve information about users and groups. Following are the operations that result in interaction between XenMobile Server and Active Directory.

1. **LDAP configuration.** Configuration of Active Directory itself results in an interaction with Active Directory. XenMobile Server attempts to validate the information by authenticating the information with Active Directory. The server does so by using the internet protocol, port, and service account credentials provided. A successful bind indicates that the connection is configured correctly.
2. **Group-based interactions.**
    a) Search for one or more groups during the Role-Based Access Control (RBAC) and delivery group definition creation. The XenMobile Server administrator inputs a search text string in the XenMobile console. XenMobile Server searches the selected domain for all groups that contain the substring that is provided. Then, XenMobile Server retrieves the objectGUID, sAMAccountName, and Distinguished Name attributes of the groups identified in the search.

    > **Note:**
    >
    > This information is not stored in the XenMobile Server database.

    b) RBAC and deployment group definition add or update. The XenMobile Server administrator selects the Active Directory groups of interest based on the previous search and includes them in the deployment group definition. XenMobile Server searches for the specific group, one at a time, in Active Directory. XenMobile Server searches for the

objectGUID attribute and retrieves selected attributes, including membership information. Group membership information helps determine membership between the group retrieved and existing users or groups in the XenMobile Server database. Changes to group membership result in the RBAC and deployment group derivation for the affected user members, which results in user entitlements.

> **Note:**
>
> Changes to the deployment group definition can lead to change in app or policy entitlements for affected users.

c) **One-time PIN (OTP) invitations**. The XenMobile Server administrator selects a group from the list of Active Directory groups present in the XenMobile Server database. For this group, all the users, both direct and indirect, are retrieved from Active Directory. OTP invitations are sent to the users who were identified in the preceding step.

> **Note:**
>
> The preceding three interactions imply that group-based interactions are triggered based on XenMobile Server configuration changes. When there are no changes to the configuration, the interactions imply that there are no interactions with Active Directory. They also imply that there are no requirement for background jobs to capture the group side of changes on a periodic basis.

3. **User-based interaction.**

a) User authentication. User authentication workflow results in two interactions with Active Directory:

- Used to authenticate the user with the credentials provided.
- Add or update select user attributes to the XenMobile Server database, including objectGUID, Distinguished Name, sAMAccountName, and direct membership to groups. Changes to group membership result in the re-evaluation of the app, policy, and access entitlements.

The user can authenticate either from the device or from the XenMobile Server console. In both the scenarios, interaction with Active Directory adheres to the same behavior.

b) App Store access and refresh. A refresh of the store results in a refresh of user attributes, including direct group memberships. This action allows for a re-evaluation of user entitlements.

c) Device check-ins. Administrators can configure in the XenMobile console the device check-ins on a periodic basis. Every time a device is checked-in, the corresponding user attributes are refreshed, including direct group memberships. These check-ins allow for a re-evaluation of user entitlements.

d) OTP invitations by Group. The XenMobile Server administrator selects a group from the list of Active Directory groups present in the XenMobile Server database. User members, both direct and indirect (due to nesting), are retrieved from Active Directory and saved in XenMobile Server database. OTP invitations are sent to the user members identified in the preceding step.

e) OTP invitations by user. The administrator inputs a search text string within the XenMobile console. XenMobile Server queries Active Directory and returns user records that match the input text string. The administrator then selects the user to send the OTP invitation. XenMobile Server retrieves the user details from Active Directory and updates the same details in the database before sending out the invitation to the user.

Background interactions

One conclusion from inline communication with Active Directory is that group-based interactions are triggered upon select changes to the XenMobile Server configuration. When there are no changes to the configuration, it implies that there are no interactions with Active Directory for groups.

This interaction requires background jobs that periodically sync with Active Directory and update relevant changes to the interested groups.

Following are the background jobs that interact with Active Directory.

1. **Group sync job**. The purpose of this job is to query Active Directory, one group at a time, on interested groups for changes to distinguished name or sAMAccountName attributes. The search query to Active Directory uses the objectGUID of the interested group to get the current values of distinguished name and sAMAccountName attributes. Changes in distinguished name or sAMAccountName values for interested groups are updated to the database.

   > **Note:**
   >
   > This job does not update user to group membership information.

2. **Nested group sync job**. This job updates changes in the nesting hierarchy of interested groups. XenMobile Server allows both direct and indirect members of an interested group to get entitlements. The direct membership of the users is updated during user-based inline interactions. Running in the background, this job tracks indirect memberships. Indirect memberships are when a user is a member of a group that is a member of an interested group.

   This job gathers the list of Active Directory groups from XenMobile Server database. These groups are a part of either the deployment group or the RBAC definition. For each group in this list, XenMobile Server gets the members of the group. Members of a group are a list of distinguished names that represent both users and groups. XenMobile Server makes another query back to Active Directory to get only the user members of the interested group. The difference

between the two lists gives only the group members for the interested group. Changes in member groups are updated to the database. The same process is repeated for all the groups in the hierarchy.

Changes to nesting results in processing the affected users for entitlement changes.

3. **Disabled user check**. This job runs only when the XenMobile administrator creates an action to check for disabled users. The job runs within the scope of a group sync job. The job queries Active Directory to check for the disabled status of interested users, one user at a time.

FAQ

What is the frequency of background jobs run, by default?

- Group sync jobs run every five hours starting at 02:00. local time.
- Nested group sync jobs run one time a day at midnight local time.

Why is a group sync job required?

- The memberOf attribute of a user record in Active Directory provides the list of groups the user is a direct member of. If a group moves from one OU to another, the memberOf attribute reflects the latest value of the distinguished name. The XenMobile Server database also has the last refreshed value. Any mismatch in the distinguished names of the group can result in the user losing access to the deployment group. The user can also lose the apps and policies associated with that deployment group.
- The background job keeps the group distinguished name attribute up-to-date in XenMobile Server database to ensure that users have access to their entitlements.
- Sync jobs are scheduled every five hours because it is assumed that group changes within Active Directory are uncommon.

Can a group sync job be turned off?

- You can turn off jobs when you know that interested groups do not change from one OU to another.

Why is a nested group processing background job required?

- Changes to nesting of groups in Active Directory is not a daily occurrence. Changes to the nesting hierarchy of interested groups result in changes to entitlements of the affected users. When a group is added to the hierarchy, its member users become entitled to the respective roles. When a group moves out of nesting then the member users of the group may lose access to the role-based entitlements.
- Changes to nesting are not captured during user refresh. Since nesting changes cannot be on-demand, the changes are captured through a background job.
- Nesting changes are assumed to be uncommon and therefore the background job runs once a day to check for any changes.

Can a nested group processing job be turned off?

- You can turn off jobs when you know that nesting changes do not occur to interested groups.

XenMobile Deployment

August 19, 2020

There's a lot to consider when you're planning a XenMobile deployment:

- Which devices to choose?
- How to manage the devices?
- How to ensure that your network remains secure while still providing a great user experience?
- What hardware do you need 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 a XenMobile 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 is the top priority. What is your primary need for XenMobile? Do you need to manage every device in your environment or just the apps? Maybe you need to manage both. How secure do you need your XenMobile environment to be? 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
- XenMobile integration
- Multi-site requirements

Design and configure

Once you finish assessing your deployment needs, you can determine the design and configuration of your environment. A few things you need to plan:

- 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 ADC and Citrix Gateway
- SSO and proxy considerations for MDX apps
- Authentication
- Reference architecture for on-premises deployments
- Server properties
- Device and app policies
- User enrollment options
- Tuning XenMobile operations

Operate and monitor

After your XenMobile 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 XenMobile 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 XenMobile support
- Systems monitoring
- Disaster recovery
- Citrix support process

Management Modes

April 1, 2021

For each XenMobile instance (a single server or a cluster of nodes), you can choose whether to manage devices, apps, or both. XenMobile uses the following terms for device and app management modes:

- Mobile device management mode (MDM mode)

- Mobile app management mode (MAM mode)
- MDM+MAM mode (Enterprise mode)

Mobile device management (MDM Mode)

> **Important:**
>
> If you configure MDM mode and later change to ENT mode, be sure to use the same (Active Directory) authentication. XenMobile doesn't support changing the authentication mode after user enrollment. For more information, see Upgrade.

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. Although app management is not available with MDM mode, you can deliver mobile apps, such as public app store and enterprise apps, in this mode. Following are common use cases for MDM mode:

- MDM is a consideration for corporate-owned devices where device-level management policies or restrictions, such as full wipe, selective wipe, or geo-location are required.
- When customers require management of an actual device, but do not require MDX policies, such as app containerization, controls on app data sharing, or micro VPN.
- 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 Mode)

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 XenMobile configured for MAM mode, you can use MDX-enabled mobile apps to provide per-app containerization and control. The term MAM mode is also called MAM-only mode. This term distinguishes this mode from a legacy MAM mode.

By leveraging MDX policies, XenMobile provides app-level control over network access (such as micro VPN), app and device interaction, data encryption, 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 mobile productivity apps. This support includes secure email delivery to Citrix Secure Mail, data sharing between the secured mobile productivity apps, and 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 (Enterprise Mode)

MDM+MAM is a hybrid mode, also called Enterprise Mode, which enables all feature sets available in the XenMobile Enterprise Mobility Management (EMM) solution. Configuring XenMobile with MDM+MAM mode enables both MDM and MAM features.

XenMobile lets you specify whether users can choose to opt out of device management or whether you require device management. This flexibility is useful for environments that include a mix of use cases. These environments may or may not 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.

You specify the management mode for XenMobile Server through the Server Mode property. You configure the setting in the XenMobile console. The mode can be MDM, MAM, or ENT (for MDM+MAM).

The XenMobile edition for which you have a license determines the management modes and other features available, as shown in the following table.

XenMobile MDM Edition	XenMobile Advanced Edition	XenMobile Enterprise Edition
MDM features	MDM features	MDM features
-	MAM features	MAM features
-	MDX Toolkit	MDX Toolkit
Secure Hub	Secure Hub	Secure Hub
-	Secure Mail	Secure Mail
-	Secure Web	Secure Web

QuickEdit	QuickEdit	QuickEdit
-	-	ShareConnect
-	-	Citrix Files

Management modes and enrollment profiles

The management modes and enrollment profiles work together. You use an enrollment profile to configure device management and app management enrollment options for Android and iOS devices. For Android, the enrollment options available for the MDM+MAM server mode differ from the options for MDM mode. For more information, see Enrollment profiles.

Device Management and MDM Enrollment

A XenMobile 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 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, it is likely that users must re-enroll their devices.

> **Note:**
>
> To specify whether you require users to enroll in MDM, use the XenMobile Server property **Enrollment Required** in the XenMobile console (**Settings > Server Properties**). That global server property applies to all users and devices for the XenMobile instance. The property applies only when the XenMobile Server Mode is ENT.

Following is a summary of the advantages and disadvantages (along with mitigations) of requiring MDM enrollment in a XenMobile Enterprise mode deployment.

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 ADC, XenMobile Server, 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 holds 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 may affect user experience.
- A second XenMobile environment with MDM enrollment required is an option. When considering this option, keep in mind the additional overhead of managing two environments and the additional resources required.

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 XenMobile actually manages on their devices and what information administrators can access.
- You can use a second XenMobile environment, with a Server Mode of MAM (also called MAM-only mode), for devices that don't need MDM management. When considering this option, keep in mind the additional overhead of managing two environments and the additional resources required.

About MAM and Legacy MAM Modes

XenMobile 10.3.5 introduced a new MAM-only server mode. To distinguish the prior and new MAM modes, the documentation uses these terms. The new mode is called MAM-only or MA, the prior MAM

mode is called legacy MAM mode.

MAM-only mode is in effect when the Server Mode property of XenMobile is MAM. Devices register in MAM mode.

Legacy MAM functionality is in effect when the Server Mode property of XenMobile is ENT and users choose to opt out of device management. In that case, devices register in MAM mode. Users who opt out of MDM management continue to receive the legacy MAM functionality.

> **Note:**
>
> Previously, setting the Server Mode property to MAM had the same effect as setting it to ENT: Users who opted out of MDM management received the legacy MAM functionality.

The following table summarizes the Server Mode setting to use for a particular license type and desired device mode:

Your licenses are for this edition	You want devices to register in this mode	Set the Server Mode property to
Enterprise/ Advanced/MDM	MDM mode	MDM
Enterprise/Advanced	MAM mode (also called MAM-only mode)	MAM
Enterprise/Advanced	MDM+MAM mode	ENT (Users who opt out of device management operate under the legacy MAM mode.)

MAM-only mode supports the following features that were previously available only for ENT. These features are not available for Windows Phone.

- **Certificate-based authentication:** MAM-only mode supports certificate-based authentication. Users will experience continued access to their apps even when their Active Directory password expires. If you use certificate-based authentication for MAM devices, you must configure your Citrix Gateway. By default, in **XenMobile Settings > Citrix Gateway**, Deliver user certificate for authentication is set to **Off**, meaning that user name and password authentication is used. Change that setting to **On** to enable certificate authentication.
- **Self Help Portal:** To enable users to perform their own app lock and app wipe. Those actions apply to all apps on the device. You can configure the App Lock and App Wipe actions in **Configure > Actions**.
- **All enrollment security modes:** Including High Security, Invitation URL, and Two Factor, configured through **Manage > Enrollment Invitations**.

- **Device registration limit for Android and iOS devices:** The Server Property **Number of Devices Per User** has moved to **Configure > Enrollment Profiles** and now applies to all server modes.
- **MAM-only APIs:** For MAM-only devices, you can call REST services by using any REST client and the XenMobile REST API to call services that the XenMobile console exposes.
- The MAM-only APIs enable you to:
  - Send an invitation URL and one-time PIN.
  - Issue app lock and wipe on devices.

The following table summarizes the differences between the legacy MAM and MAM-only functionality.

Enrollment Scenarios and Other Features	Legacy MAM (server mode is ENT)	MAM-only mode (server mode is MAM)
Certificate authentication	Not supported.	Supported. For certificate authentication, Citrix Gateway is required.
Deployment requirement	XenMobile Server does not need to be directly accessible from devices.	XenMobile Server does not need to be directly accessible from devices.
Enrollment option	Use the Citrix Gateway FQDN or, when using MDM FQDN, opt not to enroll.	Use XenMobile Server FQDN.
Enrollment methods*	User name + Password	User name + Password, High Security, Invitation URL, Invitation URL+PIN, Invitation URL + Password, Two Factor, User name + PIN
App lock and wipe	Supported.	Supported.
Self Help Portal options for app lock and wipe	Not supported.	Supported.
App wipe behavior	Apps remain on the device but are not usable. XenMobile deletes the account on the client only.	Apps remain on the device but are not usable. XenMobile deletes the account on the client only.

Automated actions for MAM-only users.	Event, device property, user property actions are supported. Doesn't support installed app-based automated actions.	Supports event, device property, user property, and some app-based actions, including app wipe and app lock.
Built-in action when an Active Directory user is deleted	Supports app wipe.	Supports app wipe.
Enrollment limit	Supported; configured through an enrollment profile.	Supported; configured through an enrollment profile.
Software inventory	Supported. XenMobile lists apps installed on a device	Not supported.

*__Regarding notifications:__ SMTP is the only supported method for sending enrollment invitations.

> **Important:**
>
> For MAM-only mode, previously enrolled users must re-enroll their devices. Be sure to provide users with the XenMobile Server FQDN they need for enrollment. In MAM-only mode, like the ENT mode, devices enroll using the XenMobile Server FQDN. (In the legacy MAM mode, devices enroll using the Citrix Gateway FQDN.)

Device Requirements

March 10, 2021

An important point to consider for any deployment is the device you plan to roll out. On the iOS, Android, and Windows platforms, the options are numerous. For a list of devices that XenMobile 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, XenMobile 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

April 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 XenMobile.

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 plan to use LDAP, certificate-based authentication, or a combination of the two?
- How do you want to handle user session time-outs? 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, an app-level passcode, or both? How many logon attempts do you want to afford to users? Keep in mind how extra per-app authentication requirements implemented with MAM might impact user experience.
- What other restrictions do you want to place on users? Do you want users to access cloud services such as Siri? What can they do and not do with each app you make available to them? Do you want to deploy corporate Wi-Fi policies to prevent cellular data plans from being consumed while inside office spaces?

App vs. Device

One of the first things to consider is whether to secure only certain apps by using mobile app management (MAM). Or if you also want to manage the entire device by using mobile device management (MDM). Most commonly, if you don't require device-level control, you only manage mobile apps, especially if your organization supports Bring Your Own Device (BYOD).

Users with devices that XenMobile 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. The policies, depending on the values you set, require the device to check XenMobile routinely 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. You can 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 might 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 can have users log on every time they access the system, but that option isn't ideal for all organizations. For example, having users enter their credentials every time they want to access their email can significantly impact user experience.

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, XenMobile creates a new vault called UserEntropy. XenMobile moves the information from the generic vault into the 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, users must enter a password or PIN each time an app requires access to shared data, including certificates, in the UserEntropy vault.

You can learn more about user entropy by reading About the MDX Toolkit in the XenMobile documentation. 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. 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 various 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. The iOS keyboard mic is also reliant on cloud access and you might block access to that feature as well.

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 to assist with application delivery, software licensing, configuration, and application life cycle management.

With XenMobile, you can go a step further to secure these apps by configuring specific MAM policies and VPN settings to prevent data leak and other security threats. XenMobile provides organizations with the flexibility to deploy any of the following solutions:

- MAM-only environment
- MDM-only environment
- Unified XenMobile Enterprise environment that provides both MDM and MAM functionality in the same platform

In addition to the ability to deliver apps to mobile devices, XenMobile 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 the app, and 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, and native apps. XenMobile 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 XenMobile. 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). XenMobile 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: Citrix-developed apps that are included with the XenMobile 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: Windows-hosted apps that you publish with StoreFront. If you have a Citrix Virtual Apps and Desktops environment, you can integrate the apps with XenMobile to make the apps available to the enrolled users.

Depending on the type of mobile apps you plan to deploy and manage with XenMobile, the underlying configuration and architecture differ. For example, if multiple groups of users with different permission levels consume a single app, you might need separate delivery groups to deploy two versions of the app. In addition, you must make sure 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 will require you to register for Apple volume purchase and configure XenMobile volume purchase settings in the XenMobile console to distribute the apps with the volume purchase licenses. A variety of such use cases makes it important to assess and plan your MAM strategy prior to implementing the XenMobile 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 then categorize them. For example: public, native, mobile productivity apps, Web, in-house, ISV apps, and so on. Also, categorize the apps for different device platforms, such as iOS and Android. This categorization helps you align the XenMobile settings that are required for each type of app. For example, certain apps might not qualify for wrapping, or might require 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. Defining per-app network requirements help in finalizing your architectural decisions early on, which streamlines the overall implementation process.

Security requirements: It's critical to define the security requirements that apply to either individual apps or all the apps. That planning ensures that you create the right configurations when you install the XenMobile Server. Although settings, such as the MDX policies, apply to individual apps, the session and authentication settings apply across all apps. Some apps might have specific encryp-

tion, containerization, wrapping, encryption, authentication, geofencing, passcode, or data sharing requirements that you can outline 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 any of the following:

- 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

You might also want certain apps 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 app-related licensing requirements. These notes help you to manage license usage effectively and to decide whether to configure specific features in XenMobile to facilitate licensing. For example, if you deploy a free or paid iOS app, Apple enforces licensing requirements on the app by requiring users to sign in to their iTunes account. You can register for Apple volume purchase to distribute and manage these apps via XenMobile. Volume purchase allows users to download the apps without having to sign into their iTunes 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 preinstalled 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 XenMobile 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.
- **Secure Mail:** Email, calendar, and contact app.
- **Secure Web:** Secure web browser that provides access to the Internet and intranet sites.
- **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 XenMobile. IT pushes security settings, configurations, and mobile apps to mobile devices via the Secure Hub client. Android and iOS devices enroll in XenMobile through Secure Hub.
- **Citrix Receiver:** Mobile app that allows users to open applications hosted by Virtual Apps and Desktops on mobile devices.
- **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 and Desktops.

- **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	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Web	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Citrix Files	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Hub	Public App	NA	Yes	Yes
Citrix Receiver	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
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 XenMobile.

App Name

VPN Required

Interaction

Interaction

Device Platform-Based Encryption

(with apps outside of container)

(from apps outside of container)

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 Receiver

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

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	Geo-fencing	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
Citrix Files	Required	N/A	Not required	N/A	Enforced
Secure Hub	Not required	Volume purchase	Not required	N/A	Not enforced
Citrix Receiver	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
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

App Name	Proxy Filtering	Licensing	Geo-fencing	Mobile Apps SDK	Minimum Operating System Version
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 the users' mobile devices. Users might work from home or in remote offices using mobile devices that you provide. Or, users might use their personal mobile devices, which allows them to access tools that are subject to certain security compliance rules.

As more user communities use mobile devices, Enterprise Mobility Management (EMM) becomes critical to prevent data leaks and to enforce 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.

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. A selected set of users receives 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, either corporate-issued or 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 (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 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 XenMobile, see Deploy resources.

Active Directory Organizational Units (OUs) and Groups

For OU **=** XenMobile 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

XenMobile Local Users and Groups

For Group= Contractors, Users =

- Vendor1
- Vendor2
- Vendor 3
- … Vendor 10

XenMobile 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	XenMobile 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.

XenMobile 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		
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

XenMobile Delivery Groups	Public App: RSA SecurID	Public App: EpicCare Haiku	HDX App: Epic Hyperspace	Passcode Policy	Device Restrictions	Automatec Actions	WiFi Policy
Clinical-Nurses							X
Clinical-Physicians					X		
Clinical-Specialists							
Clinical-Outside Physicians							
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

- XenMobile 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 XenMobile.
- XenMobile 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 XenMobile, that user cannot enroll. Likewise, if a user is a member of multiple groups, XenMobile categorizes the user as only in the groups mapped to XenMobile.
- To make MDM enrollment mandatory, you must set the Enrollment Required option to True in Server Properties in the XenMobile console. For details, see Server Properties.
- You can delete a user group from a XenMobile delivery group by deleting the entry in the SQL Server database, under dbo.userlistgrps.
  Caution: Before you perform this action, create a backup of XenMobile and the database.

About Device Ownership in XenMobile

You can group users according to the owner of a users' device. Device ownership includes corporate-owned devices and user-owned devices, also known as bring your own device (BYOD). You can control

how BYOD devices connect to your network in two places in the XenMobile console: in the deployment rules for each resource type and through server properties on the **Settings** page. For details about deployment rules, see Configuring Deployment Rules in the XenMobile documentation. For details about server properties, see Server Properties.

You can require all BYOD users to accept corporate management of their devices before they can access apps. Or, you can give users access to corporate apps without also managing their devices.

When you set the server setting **wsapi.mdm.required.flag** to **true**, XenMobile manages all BYOD devices, and any user who declines enrollment is denied access to apps. Consider setting **wsapi.mdm.required.flag** to **true** in environments in which enterprise IT teams need high security along with a positive user experience when enrolling user devices in XenMobile.

If you leave **wsapi.mdm.required.flag** as **false**, which is the default setting, users can decline enrollment, but might still access apps on their devices through the XenMobile Store. Consider setting **wsapi.mdm.required.flag** to **false** in environments in which privacy, legal, or regulatory constraints require no device management, only enterprise app management.

Users with devices that XenMobile doesn't manage can install apps through the XenMobile Store. Instead of device-level controls, such as selective or full wipe, you control access to the apps through app policies. The policies, depending on the values you set, require the device to check the XenMobile Server routinely to confirm that the apps are still allowed to run.

Security Requirements

The number of security considerations when deploying a XenMobile environment can quickly become overwhelming. There are many interlocking pieces and settings. To help you get started and choose an acceptable level of protection, Citrix provides recommendations for High, Higher, and Highest Security, outlined in the following table.

Your deployment mode choice involves more than just security concerns. It is important to also review the requirements of the use case and decide if you can mitigate security concerns before choosing your deployment 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.

Deployment mode security considerations

The following table specifies the deployment modes for each security level.

High Security	Higher Security	Highest Security
MAM or MDM	MDM+MAM	MDM+MAM; plus FIPS

Notes:

- Depending on the use case, a MDM-only or MAM-only deployment can meet security requirements and provide a good user experience.
- If you don't need app containerization, micro VPN, or app specific policies, MDM is sufficient to manage and secure devices.
- For use cases like BYOD in which app containerization alone can satisfy all business and security requirements, 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. Be sure to enforce MDM enrollment.
- FIPS options for environments with the highest security needs, such as the federal government.

If you enable FIPS mode, you must configure SQL Server to encrypt SQL traffic.

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 ENT; recommended for MDM	Standard Citrix ADC for XenMobile wizard configuration with SSL bridge if XenMobile is in the DMZ. Or SSL offload if necessary to meet security standards when the XenMobile Server is in the internal network.	SSL Offload with end-to-end encryption

Notes:

- Exposing the XenMobile Server to the Internet through NAT or existing third-party proxies and load-balancers can be an option for MDM. However, that setup requires that the SSL traffic ter-

minates on the XenMobile Server, which poses a potential security risk.
- For high security environments, Citrix ADC with the default XenMobile configuration typically meets or exceeds security requirements.
- For MDM environments with the highest security needs, SSL termination at the Citrix ADC enables traffic inspection at the perimeter and maintains end-to-end SSL encryption.
- Options to define SSL/TLS ciphers.
- SSL FIPS Citrix ADC hardware is also available.
- 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 Directory groups only. That setup requires disabling the built-in All users Delivery Group.
- You can use enrollment invitations to restrict enrollment to users with an invitation only. Enrollment invitations aren't available for Android Enterprise and 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.
- For environments with the highest security requirements, you can tie enrollment invitations to a device by SN/UDID/EMEI. A two-factor authentication option is also available to require an Active Directory password and OTP. OTP isn't supported as an option 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. Enforced by using MDM. You can set high security as required for MAM-only by using the MDX policy, Non-compliant device behavior.	Enforced by using MDM, an MDX policy, or both.	Enforced by using 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 in MDM+MAM environments.
- 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

April 1, 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. To support BYOD adoption, you can typically implement a MAM solution, such as XenMobile, to assist with the following:

- application delivery
- software licensing
- configuration
- application life cycle management

You can require or allow users to also opt into MDM management.

With XenMobile, you can go a step further to secure these apps by configuring specific MAM policies and VPN settings to prevent data leak and other security threats. XenMobile provides organizations with the flexibility to deploy their solution as a:

- MAM-only environment
- MDM-only environment
- Unified XenMobile Enterprise environment that provides both MDM and MAM functionality

In addition to the ability to deliver apps to mobile devices, XenMobile 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. XenMobile 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 Service or 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 XenMobile.

  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 Service or MDX Toolkit
- **Web and SaaS apps:** These apps include apps accessed from an internal network (web apps) or over a public network (SaaS). XenMobile 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 XenMobile 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 XenMobile, 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 XenMobile 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 XenMobile 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 XenMobile 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 may want to use a policy-based deployment to allow only compliant users to download the published apps. For example, certain apps might require that the device is managed, or that the device meets a minimum operating system version. You may 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 XenMobile 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 XenMobile. 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 XenMobile 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: Client used by all mobile devices to communicate with XenMobile. You push security settings, configurations, and mobile apps to mobile devices by using Secure Hub. Android and iOS devices enroll in XenMobile through Secure Hub.

Citrix Receiver: Mobile app that allows mobile device users to open applications 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.

- **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	MAM SDK integration or MDX Wrapping	iOS	Android
Secure Mail	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Web	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Citrix Files	XenMobile App	No for version 10.4.1 and later	Yes	Yes

Secure Hub	Public App	N/A	Yes	Yes
Citrix Receiver	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
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 XenMobile.

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Proxy Filtering	Licensing	Geofencing	Mobile Apps SDK	Minimum Operating System Version
Secure Mail	Y	Selective Allowed	Allowed	Required	N/A	Selective Required	N/A	Enforced
Secure Web	Y	Allowed	Allowed	Required	N/A	Not required	N/A	Enforced
Citrix Files	Y	Allowed	Allowed	Required	N/A	Not required	N/A	Enforced

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Proxy Filtering	Licensing	Geofencing	Mobile Apps SDK	Minimum Operating System Version
Secure Hub	Y	N/A	N/A	Not required	Volume purchase	Not required	N/A	Not enforced
Citrix Receiver	Y	N/A	N/A	Not required	Volume purchase	Not required	N/A	Not enforced
GoToMeeting	N	N/A	N/A	Not required	Volume purchase	Not required	N/A	Not enforced
SalesForc	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 Hyperspace	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

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Proxy Filtering	Licensing	Geofencing	Mobile Apps SDK	Minimum Operating System Version
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
SharePoi	Y	N/A	N/A	Required	N/A	Not required	N/A	Not enforced

User Communities

October 6, 2020

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 data leak and to enforce organizational security restrictions. In order 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 XenMobile resources.

- XenMobile local users and groups

For users who don't have an account in Active Directory, you can create the users as local XenMobile users. You can add local users to delivery groups and provision resources to them in the same manner as Active Directory users.

- XenMobile delivery groups

  If multiple groups of users with different level of permissions are to consume a single app, you might need to create separate delivery groups. With separate delivery groups, you can deploy two separate versions of the same app.

- 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 receive 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, phlebotomists, 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 health care 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 XenMobile, see Deploy resources in the XenMobile product documentation.

Active Directory Organizational Units (OUs) and Groups

For OU = XenMobile 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

XenMobile Local Users and Groups

For Group= Contractors, Users =

- Vendor1
- Vendor2
- Vendor 3
- … Vendor 10

XenMobile 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	XenMobile 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 of Apps

	Secure Mail	**Secure Web**	**ShareFil**	**Receiver**	**SalesFor**	**RSA SecurID**	**EpicCare Haiku**	**Epic Hyperspace**
Clinical-Nurses	X	X	X					
Clinical-Physician								
Clinical-Specialists								
Clinical-Outside Physicians	X		X					
Clinical-Home Health Services	X		X					

Clinical-Research Specialist	X	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	X
Non-Clinical-Philanthropic Programs	X	X				X	X
Contracto	X	X	X	X		X	X

Delivery Group and Resource Mapping of MDM Resources

	MDM: Passcode policy	MDM: Device Restrictions	MDM: Automated Actions	MDM: WiFi policy
Clinical-Nurses				X
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

- XenMobile 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 XenMobile.

- XenMobile 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 XenMobile, that user cannot enroll. Likewise, if a user is a member of multiple groups, XenMobile only categorizes the user as being in the groups mapped to XenMobile.
- To make MDM enrollment mandatory, set the **Enrollment Required** option to **True** in **Server Properties** in the XenMobile console. For details, see Server Properties.
- To delete a user group from a XenMobile delivery group, delete the entry in the SQL Server database, under dbo.userlistgrps.

  > **Caution:**
  >
  > Before you perform this action, create a backup of XenMobile and the database.

About Device Ownership in XenMobile

You can group users according to the owner of a user device. Device ownership includes corporate-owned devices and user-owned devices, also known as bring your own device (BYOD). You can control how BYOD devices connect to your network in two places in the XenMobile console: in Deployment Rules and through XenMobile server properties on the **Settings** page. For details about deployment rules, see Deploy resources in the XenMobile documentation. For details about server properties, see Server Properties in this handbook.

By setting server properties, you can require all BYOD users to accept corporate management of their devices before they can access apps. Or, you can give users access to corporate apps without also managing their devices.

When you set the server property **wsapi.mdm.required.flag** to **true**, XenMobile manages all BYOD devices, and any user who declines enrollment is denied access to apps. Consider setting **wsapi.mdm.required.flag** to **true** in environments in which enterprise IT teams need high security plus a positive user experience during enrolling.

If you leave **wsapi.mdm.required.flag** as **false**, which is the default setting, users can decline enrollment. However, they can access apps on their devices through the XenMobile Store. Consider setting **wsapi.mdm.required.flag** to **false** in environments in which privacy, legal, or regulatory constraints require no device management, only enterprise app management.

Users with devices that XenMobile doesn't manage can install apps through the XenMobile Store. Instead of device-level controls, such as selective or full wipe, you control access to the apps through app policies. Some policy settings require the device to check the XenMobile server routinely to confirm that the apps are still allowed to run.

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 XenMobile design. XenMobile 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
Minimum XenMobile Edition	Advanced	MDM	MDM
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 (with no security via MDX policies). 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 XenMobile 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 XenMobile.

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 ADC) 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 ADC (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 XenMobile, 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.

XenMobile 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 XenMobile 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 ADC 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. Citrix Gateway connector for Exchange ActiveSync acts an intermediary between Citrix ADC and the XenMobile Server. When a device communicates with Exchange through the ActiveSync virtual server on the Citrix ADC, Citrix ADC performs an HTTP callout to the connector for Exchange ActiveSync service. That service then checks the device status with XenMobile. Based on the status of the device, the connector for Exchange ActiveSync replies to Citrix ADC 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 membership, for example. If there is a requirement for Active Directory group filtering, you can use Endpoint Management connector for Exchange ActiveSync instead.
- Citrix ADC scalability: Given the requirement to proxy ActiveSync traffic via Citrix ADC: Proper sizing of the Citrix ADC instance is critical to support the added workload of all ActiveSync SSL connections.
- Citrix ADC Integrated Caching: The connector for Exchange ActiveSync configuration on the Citrix ADC uses the Integrated Caching function to cache responses from the connector for Exchange ActiveSync. As a result of that configuration, Citrix ADC doesn't need to issue a request to Citrix Gateway connector for Exchange ActiveSync 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 ADC Platinum Edition or you can license the feature separately for Enterprise Editions.
- Custom filtering policies: You might need to create custom Citrix ADC policies to restrict certain ActiveSync clients outside of the standard native mobile clients. This configuration requires knowledge on ActiveSync HTTP requests and Citrix ADC 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 ADC virtual server used for the connector for Exchange ActiveSync. You can accomplish this traffic flow via DNS and keep the connector for Exchange ActiveSync policy from affecting Secure Mail clients.

For a diagram of Citrix Gateway connector for Exchange ActiveSync in a XenMobile deployment, see Reference Architecture for On-Premises Deployments.

Endpoint Management connector for Exchange ActiveSync

Endpoint Management connector for Exchange ActiveSync is a XenMobile 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 XenMobile 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, Endpoint Management connector for Exchange ActiveSync checks the device status with XenMobile 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 ADC. You can deploy Endpoint Management connector for Exchange ActiveSync without changes routing for the existing ActiveSync traffic. Design considerations include:

- Windows Server: The Endpoint Management connector for Exchange ActiveSync component requires you to deploy Windows Server.
- Filtering rule set: Just like Citrix Gateway connector for Exchange ActiveSync, Endpoint Management connector for Exchange ActiveSync includes filtering rules to evaluate device state. Additionally, Endpoint Management connector for Exchange ActiveSync also supports static rules to filter based on Active Directory group membership.
- Exchange integration: Endpoint Management 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 Endpoint Management connector for Exchange ActiveSync is filtering at the ActiveSync service level, consider other ActiveSync clients outside the XenMobile environment. You can configure Endpoint Management connector for Exchange ActiveSync

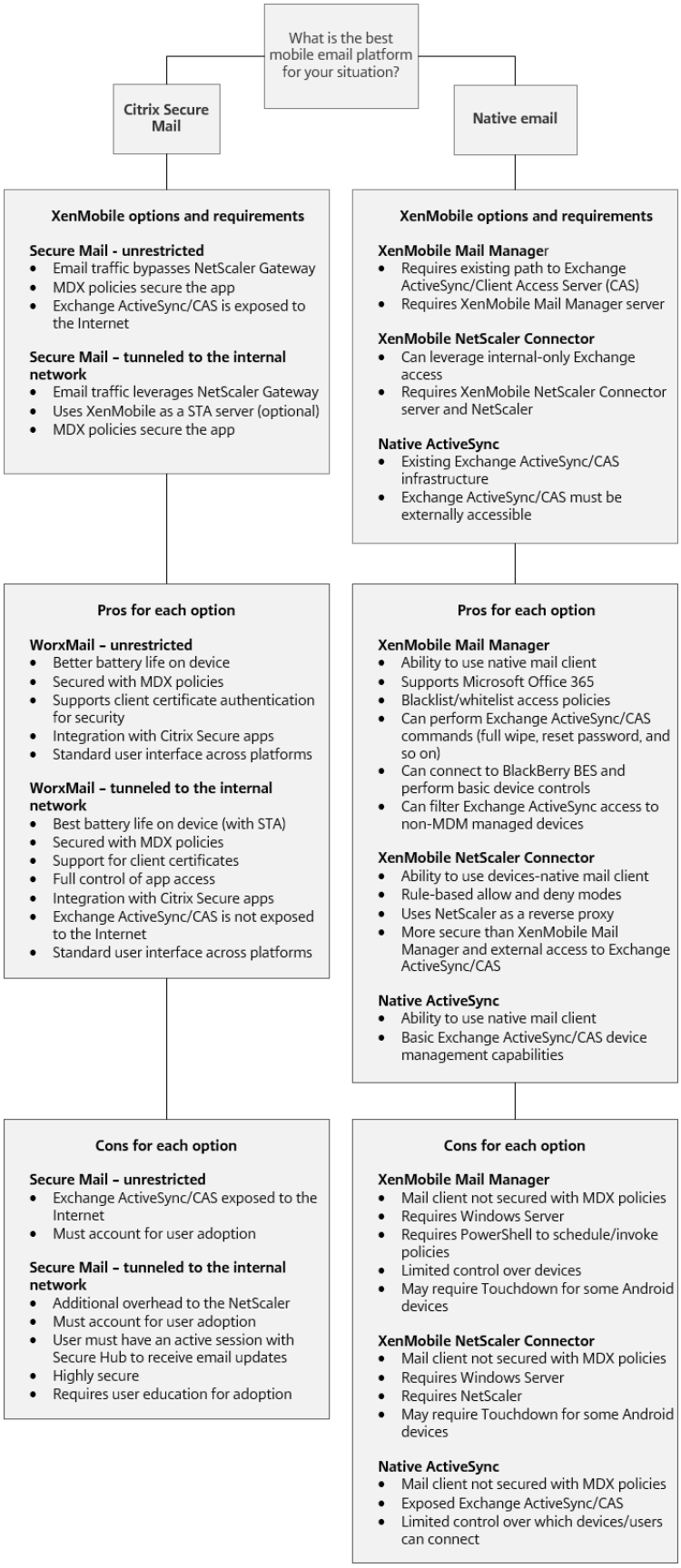
static rules to avoid unintended impact to other ActiveSync clients.

- Extended Exchange functions: Through direct integration with Exchange ActiveSync, Endpoint Management connector for Exchange ActiveSync provides the ability for XenMobile to perform an Exchange ActiveSync wipe on a mobile device. Endpoint Management connector for Exchange ActiveSync also allows XenMobile to access information about Blackberry devices and to perform other control operations.

For a diagram of Endpoint Management connector for Exchange ActiveSync in a XenMobile deployment, see Reference Architecture for On-Premises Deployments.

Email Platform Decision Tree

The following figure helps you distinguish the pros and cons between using native email or Secure Mail solutions in your XenMobile deployment. Each choice allows for associated XenMobile options and requirements to enable server, network, and database access. The pros and cons include details on security, policy, and user interface considerations.



XenMobile Integration

June 24, 2020

This article covers what to consider when planning how XenMobile is to integrate with your existing network and solutions. For example, if you're already using Citrix ADC for Virtual Apps and Desktops:

- Should you use the existing Citrix ADC instance or a new, dedicated instance?
- Do you want to integrate with XenMobile the HDX apps that are published using StoreFront?
- Do you plan to use Citrix Files with XenMobile?
- Do you have a Network Access Control solution that you want to integrate into XenMobile?
- Do you deploy web proxies for all outbound traffic from your network?

Citrix ADC and Citrix Gateway

Citrix Gateway required mandatory for XenMobile ENT and MAM modes. Citrix Gateway provides a micro VPN path for access to all corporate resources and provides strong multifactor authentication support. Citrix ADC load balancing is required for all XenMobile Server device modes:

- If you have multiple XenMobile Servers
- Or, if the XenMobile Server is inside your DMZ or internal network (and therefore traffic flows from devices to Citrix ADC to XenMobile)

You can use existing Citrix ADC instances or set up new ones for XenMobile. The following sections note the advantages and disadvantages of using existing or new, dedicated Citrix ADC instances.

Shared Citrix ADC MPX with a Citrix Gateway VIP created for XenMobile

Advantages:

- Uses a common Citrix ADC instance for all Citrix remote connections: Citrix Virtual Apps and Desktops, full VPN, and clientless VPN.
- Uses the existing Citrix ADC configurations, such as for certificate authentication and for accessing services like DNS, LDAP, and NTP.
- Uses a single Citrix ADC platform license.

Disadvantages:

- It is more difficult to plan for scale when you handle two different use cases on the same Citrix ADC.
- Sometimes you need a specific Citrix ADC version for a Citrix Virtual Apps and Desktops use case. That same version might have known issues for XenMobile. Or XenMobile might have known issues for the Citrix ADC version.

- If a Citrix Gateway exists, you cannot run the Citrix ADC for XenMobile wizard a second time to create the Citrix ADC configuration for XenMobile.
- Except when Platinum licenses are used for Citrix Gateway 11.1 or later: User access licenses installed on Citrix ADC and required for VPN connectivity are pooled. Because those licenses are available to all Citrix ADC virtual servers, services other than XenMobile can potentially consume them.

Dedicated Citrix ADC VPX/MPX instance

Advantages:

Citrix recommends using a dedicated instance of Citrix ADC.

- Easier to plan for scale and separates XenMobile traffic from a Citrix ADC instance that might already be resource constrained.
- Avoids issues when XenMobile and Citrix Virtual Apps and Desktops need different Citrix ADC software versions. The recommendation generally is to use the latest compatible Citrix ADC version and build for XenMobile.
- Allows XenMobile configuration of Citrix ADC through the built-in Citrix ADC for XenMobile wizard.
- Virtual and physical separation of services.
- Except when Platinum licenses are used for Citrix Gateway 11.1 or later: The user access licenses required for XenMobile are only available to XenMobile services on the Citrix ADC.

Disadvantages:

- Requires setup of extra services on Citrix ADC to support XenMobile configuration.
- Requires another Citrix ADC platform license. License each Citrix ADC instance for Citrix Gateway.

For information about what to consider when integrating Citrix ADC and Citrix Gateway with each XenMobile server mode, see Integrating with Citrix ADC and Citrix Gateway.

StoreFront

If you have a Citrix Virtual Apps and Desktops environment, you can integrate HDX applications with XenMobile using StoreFront. When you integrate HDX apps with XenMobile:

- The apps are available to users who are enrolled with XenMobile.
- The apps display in the XenMobile Store along with other mobile apps.
- XenMobile uses the legacy PNAgent (services) site on StoreFront.
- When Citrix Receiver is installed on a device, HDX apps start using the Receiver.

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 XenMobile.

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 XenMobile using the same Citrix Gateway.
- Use the same store or create a new one?
- Use the same or a different StoreFront server?

The following sections note the advantages and disadvantages of using separate or combined storefronts for Receiver and mobile productivity apps.

Integrate your existing StoreFront instance with XenMobile server

Advantages:

- Same store: No additional configuration of StoreFront is required for XenMobile, assuming that you use the same Citrix ADC VIP for HDX access. Suppose that you choose to use the same store and want to direct Receiver access to a new Citrix ADC 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 Virtual Apps and Desktops workloads may adversely affect XenMobile as well.
- Same StoreFront server: In large environments, consider the additional load from XenMobile usage of PNAgent for app enumeration and start-up.

Use a new, dedicated StoreFront instance for integration with XenMobile server

Advantages:

- New store: Any configuration changes of the StoreFront store for XenMobile should not affect existing Virtual Apps and Desktops workloads.
- New StoreFront server: Server configuration changes should not affect Virtual Apps and Desktops workflow. Additionally, load outside of XenMobile usage of PNAgent for app enumeration and launch should not affect scalability.

Disadvantages:

- New store: StoreFront store configuration.
- New StoreFront server: Requires new StoreFront installation and configuration.

For more information, see Virtual Apps and Desktops through Citrix Secure Hub in the XenMobile documentation.

Citrix Content Collaboration and Citrix Files

Citrix Files 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. If you integrate Citrix Content Collaboration with XenMobile Advanced Edition or Enterprise Edition, XenMobile can provide Citrix Files with:

- Single sign-on authentication for XenMobile 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 XenMobile 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 XenMobile console to configure the integration with Citrix Files or storage zones connectors. For more information, see Citrix Files use with XenMobile.

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 need 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 Citrix Files.
- 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 Content Collaboration subdomain, provision users to Citrix Files, or host Citrix Files data. Using storage zones connectors with XenMobile 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, NAT/PAT configurations, or proxy 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 ADC.

SAML integration with XenMobile Enterprise

Questions to ask:

- Is Active Directory authentication required for Citrix Files?
- Does first time use of the Citrix Files app for XenMobile 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:

XenMobile Enterprise environments may choose to use SAML as the authentication mechanism for Citrix Files. The authentication options are:

- Use XenMobile server as the Identity Provider (IdP) for SAML

This option can provide excellent user experience and automate Citrix Files account creation, as well as enable mobile app SSO features.

- XenMobile 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 may also provide SSO capabilities on the Windows client side. Be sure to evaluate use cases before choosing your Citrix FIles SAML IdP.

Additionally, to satisfy both use cases, you can configure ADFS and XenMobile as a dual IdP.

Mobile apps

Questions to ask:

- Which Citrix Files mobile app do you plan to use (public, MDM, MDX)?

Design decision:

- You distribute 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 security is low and you don't require containerization, the public Citrix Files application may not be suitable. In an MDM-only environment, you can deliver the MDM version of the Citrix Files app using XenMobile in MDM mode.
- For more information, see Apps and Citrix Files for XenMobile.

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 and device security. For information, see Employee Permissions and Managing Devices and Apps.
- Some Citrix Files device security settings and MDX policies control the same features. In those cases, XenMobile policies take precedence, followed by the Citrix Files device security settings.

Examples: If you disable external apps in Citrix Files, but enable them in XenMobile, the external apps get disabled in Citrix Files. You can configure the apps so that XenMobile 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.

Web Proxies

The most likely scenario for routing XenMobile traffic through an HTTP(S)/SOCKS proxy is as follows: When the subnet that the XenMobile server resides in doesn't have outbound Internet access to the required Apple, Google, or Microsoft IP addresses. You can specify proxy server settings in XenMobile to route all Internet traffic to the proxy server. For more information, see Enable proxy servers.

The following table describes the advantages and disadvantages of the most common proxy used with XenMobile.

Option	Advantages	Disadvantages
Use an HTTP(S)/ SOCKS Proxy with XenMobile server.	In cases where policies do not permit outbound Internet connections from the XenMobile server subnet: You can configure an HTTP(S) or SOCKS proxy to provide Internet connectivity.	If the proxy server fails, APNs (iOS) or Firebase Cloud Messaging (Android) connectivity breaks. As a result, device notifications fail for all iOS and Android devices.

Use an HTTP(S) Proxy with Secure Web.	You can monitor HTTP/HTTPS traffic to ensure that Internet activity complies with your organization's standards.	This configuration requires all Secure Web Internet traffic to tunnel back to the corporate network before they are sent back out to the Internet. If your Internet connection constrains browsing: This configuration could affect Internet browsing performance.

Your Citrix ADC session profile configuration for split tunneling affects the traffic as follows.

When Citrix ADC Split Tunneling is **off**:

- If the MDX **Network access** policy is **Tunneled to the internal network:** All traffic is forced to use the micro VPN or clientless VPN (cVPN) tunnel back to the Citrix Gateway.
- Configure Citrix ADC traffic policies/profiles for the proxy server and bind them to the Citrix Gateway VIP.

> **Important:**
>
> Be sure to exclude Secure Hub cVPN traffic from the proxy.

- For more information, see XenMobile Secure Hub Traffic Through Proxy Server in Secure Browse Mode.

When **Citrix ADC Split Tunneling** is **on**:

- When apps are configured with the MDX **Network access** policy set to **Tunneled to the internal network**: The apps first attempt to get the web resource directly. If the web resource is not publicly available, those apps then fall back to Citrix Gateway.
- Configure Citrix ADC traffic policies and profiles for the proxy server. Then, bind those policies and profiles to the Citrix Gateway VIP.

> **Important:**
>
> Be sure to exclude Secure Hub cVPN traffic from the proxy.

Your Citrix ADC session profile configuration for **Split DNS** (under **Client experience**) functions similarly to Split Tunneling.

With **Split DNS** enabled and set to **Both**:

- The client first attempts to resolve the FQDN locally and then falls back to Citrix ADC for DNS resolution during failure.

With **Split DNS** set to **Remote**:

- DNS resolution occurs only on Citrix ADC.

With **Split DNS** set to **Local**:

- The client attempts to resolve the FQDN locally. Citrix ADC isn't used for DNS resolution.

Access Control

Enterprises can manage mobile devices inside and outside of networks. Enterprise Mobility Management solutions such as XenMobile 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 XenMobile device security assessment through your NAC solution. Your NAC solution then can use the XenMobile 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 XenMobile 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 XenMobile 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 XenMobile and a configuration overview, see Network Access Control.

Multi-Site Requirements

February 11, 2020

You can architect and configure XenMobile deployments that include multiple sites for high availability and disaster recovery. This article provides an overview of the high availability and disaster recovered models used in XenMobile deployments.

High Availability

- For XenMobile cluster nodes, Citrix ADC handles the load balancing. For more information, see Configure Clustering
- XenMobile server nodes operate in an active/active configuration.
- Additional XenMobile server nodes are added to a high availability cluster as capacity is required. One node can handle up to approximately 8,500 user devices (see Scalability and performance for additional detail).
- Citrix recommends configuring "n+1" XenMobile servers: one server for every 8,500 user devices and one extra server for redundancy.
- Citrix recommends high availability for all Citrix ADC instances wherever possible to allow the configurations to sync with a second Citrix ADC.
- The standard Citrix ADC high availability pair operates in an active/passive configuration.

A typical high availability XenMobile deployment typically includes:

- Two Citrix ADC instances (VPX or MPX). If the Citrix ADC SDX platform is used, high availability should also be considered.
- Two or more XenMobile servers configured with the same database settings.

Disaster Recovery

You can configure XenMobile for disaster recovery across two data centers with one active data center and one passive data center. Citrix ADC and Global Server Load Balancing (GSLB) are used to create an active/active data path so that the user experience is that of an active/active setup.

For disaster recovery, a XenMobile deployment includes:

- Two data centers; each contains one or more Citrix ADC instances, XenMobile servers, and SQL Server databases.
- A GSLB server to direct traffic to the data centers. The GSLB server is configured for both the XenMobile enrollment URL and Citrix Gateway URL handling traffic to the site.
- When you use the Citrix ADC for XenMobile wizard to configure Citrix Gateway, by default, the GSLB is not enabled to resolve traffic to the XenMobile enrollment server and traffic to the Citrix

Gateway, en route to the MAM load-balancing server; as a result, additional steps are required. For more information on preparing for and implementing these steps, see Disaster Recovery.
- Clustered SQL Servers of Always On Availability Groups.
- Latency between the XenMobile servers and SQL Server must be less than 5 ms.

> **Note:**
>
> The disaster recovery methods described in this handbook provide only automated disaster recovery for the access layer. You must manually start all XenMobile server nodes and the SQL Server database at the failover site before devices can connect the XenMobile server.

Integrating with Citrix Gateway and Citrix ADC

November 12, 2020

When integrated with XenMobile, Citrix Gateway provides an authentication mechanism for remote device access to the internal network for MAM devices. The integration enables mobile productivity apps to connect to corporate servers in the intranet through a micro VPN. The micro VPN is created from the apps on the mobile device to Citrix Gateway. Citrix Gateway provides a micro VPN path for access to all corporate resources and provides strong multifactor authentication support.

Citrix ADC load balancing is required for all XenMobile Server device modes in these cases:

- If you have multiple XenMobile Servers
- Or if the XenMobile Server is inside your DMZ or internal network (and therefore traffic flows from devices to Citrix ADC to XenMobile)

Integration requirements for XenMobile Server modes

The integration requirements for Citrix Gateway and Citrix ADC differ based on the XenMobile Server modes: MAM, MDM, and ENT.

MAM

With XenMobile Server in MAM mode:

- **Citrix Gateway** is required. Citrix Gateway provides a micro VPN path for access to all corporate resources and provides strong multifactor authentication support.
- **Citrix ADC** is recommended for load balancing.

  Citrix recommends that you deploy XenMobile in a high availability configuration, which requires a load balancer in front of XenMobile. For details, see About MAM and Legacy MAM Modes.

MDM

With XenMobile Server in MDM mode:

- Citrix Gateway isn't required. For MDM deployments, Citrix recommends Citrix Gateway for mobile device VPN.
- Citrix ADC is recommended for security and load balancing.

  Citrix recommends that you deploy a Citrix ADC appliance in front of the XenMobile Server, for security and load balancing. For standard deployments with XenMobile in the DMZ, Citrix recommends the Citrix ADC for XenMobile wizard along with XenMobile Server load balancing in SSL Bridge mode. You can also consider SSL Offload for deployments in which:

  - The XenMobile Server resides in the internal network rather than the DMZ
  - Or your security team requires an SSL Bridge configuration

  Citrix does not recommend exposing the XenMobile Server to the Internet via NAT or existing third-party proxies or load-balancers for MDM. Those configurations pose a potential security risk, even if the SSL traffic terminates on the XenMobile Server (SSL Bridge).

  For high security environments, Citrix ADC with the default XenMobile configuration meets or exceeds security requirements.

  For MDM environments with the highest security needs, SSL termination at the Citrix ADC allows you to inspect traffic at the perimeter, while maintaining end-to-end SSL encryption. For more information, see Security Requirements. Citrix ADC offers options to define SSL/TLS ciphers and SSL FIPS Citrix ADC hardware.

ENT (MAM+MDM)

With XenMobile Server in ENT mode:

- Citrix Gateway is required. Citrix Gateway provides a micro VPN path for access to all corporate resources and provides strong multifactor authentication support.

  When the XenMobile Server mode is ENT and a user opts out of MDM enrollment, the device operates in the legacy MAM mode. In the legacy MAM mode, devices enroll using the Citrix Gateway FQDN. For details, see About MAM and Legacy MAM Modes.
- Citrix ADC is recommended for load balancing. For more information, see the Citrix ADC point earlier in this article under "MDM."

> **Important:**
>
> For initial enrollment, the traffic from user devices authenticates on the XenMobile Server whether you configure load balancing virtual servers to SSL Offload or SSL Bridge.

Design Decisions

The following sections summarize the many design decisions to consider when planning a Citrix Gateway integration with XenMobile.

Licensing and edition

Decision detail:

- What edition of Citrix ADC do you plan to use?
- Have you applied Platform licenses to Citrix ADC?
- If you require MAM functionality, have you applied the Citrix ADC Universal Access Licenses?

Design guidance:

Ensure that you apply the proper licenses to the Citrix Gateway. If you are using the Citrix Gateway connector for Exchange ActiveSync, integrated caching might be required. Therefore, you must ensure that the appropriate Citrix ADC Edition is in place.

The license requirements to enable Citrix ADC features are as follows.

- XenMobile MDM load balancing requires a Citrix ADC standard platform license at a minimum.
- Content Collaboration load balancing with storage zones controller requires a Citrix ADC standard platform license at a minimum.
- The XenMobile Enterprise edition includes the required Citrix Gateway Universal licenses for MAM.
- Exchange load balancing requires a Citrix ADC Platinum platform license or a Citrix ADC Enterprise platform license with the addition of an Integrated Caching license.

Citrix ADC version for XenMobile

Decision detail:

- What version is the Citrix ADC running in the XenMobile environment?
- Do you require a separate instance?

Design guidance:

Citrix recommends using a dedicated instance of Citrix ADC for your Citrix Gateway virtual server. Be sure that the minimum required Citrix ADC version and build is in use for the XenMobile environment. Typically, it is best to use the latest compatible Citrix ADC version and build for XenMobile. If upgrading Citrix Gateway would affect your existing environments, a second dedicated instance for XenMobile might be appropriate.

If you plan to share a Citrix ADC instance for XenMobile and other apps that use VPN connections, be sure that you have enough VPN licenses for both. Keep in mind that XenMobile test and production environments cannot share a Citrix ADC instance.

Certificates

Decision detail:

- Do you require a higher degree of security for enrollments and access to the XenMobile environment?
- Is LDAP not an option?

Design guidance:

The default configuration for XenMobile is user name and password authentication. To add another layer of security for enrollment and access to the XenMobile 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 XenMobile. Users then enroll using a unique PIN that XenMobile generates for them. After a user has access, XenMobile creates and deploys the certificate used to authenticate to the XenMobile environment.

XenMobile supports Certificate Revocation List (CRL) only for a third party Certificate Authority. If you have a Microsoft CA configured, XenMobile uses Citrix ADC to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the Citrix ADC 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. XenMobile 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.

Networking topology

Decision detail:

- What Citrix ADC topology is required?

Design guidance:

Citrix recommends using a Citrix ADC instance for XenMobile. However, you might not want traffic going from the inside network out to the DMZ. In that case, consider setting up an extra instance of Citrix ADC. Use one Citrix ADC instance for internal users and one for external users. When users switch between the internal and external networks, DNS record caching can result in an increase in Secure Hub logon prompts.

XenMobile does not support Citrix Gateway double hop.

Dedicated or shared Citrix Gateway VIPs

Decision detail:

- Do you currently use Citrix Gateway for Virtual Apps and Desktops?
- Do you plan for XenMobile to use the same Citrix Gateway as Virtual Apps and Desktops?
- What are the authentication requirements for both traffic flows?

Design guidance:

When your Citrix environment includes XenMobile, plus Virtual Apps and Desktops, you can use the same Citrix ADC instance and Citrix Gateway virtual server for both. Due to potential versioning conflicts and environment isolation, a dedicated Citrix ADC instance and Citrix Gateway are recommended for each XenMobile environment. However, if a dedicated Citrix ADC instance is not an option, Citrix recommends using a dedicated Citrix Gateway virtual server to separate the traffic flows for Secure Hub. That configuration is instead of a virtual server shared between XenMobile and Virtual Apps and Desktops.

If you use LDAP authentication, Receiver and Secure Hub can authenticate to the same Citrix Gateway with no issues. If you use certificate-based authentication, XenMobile pushes a certificate in the MDX container and Secure Hub uses the certificate to authenticate with Citrix Gateway. Receiver 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 the following work-around, which allows you to use the same FQDN for two Citrix Gateway VIPs.

- Create two Citrix Gateway VIPs with the same IP address. The VIP for Secure Hub uses the standard 443 port and the VIP for Virtual Apps and Desktops (which deploy Receiver) uses port 444.
- As a result, one FQDN resolves to the same IP address.
- For this work around, you might 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 XenMobile 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 ADC, and for accessing applications while offline.

XenMobile load balancer IP address for MAM

Decision detail:

- Are you using internal or external IP addresses for VIPs?

Design guidance:

In environments where you can use public IP addresses for Citrix Gateway VIPs, assigning the XenMobile load balancing VIP and address in this manner causes enrollment failures.

Ensure that the load balancing VIP uses an internal IP to avoid enrollment failures in this scenario. This virtual IP address must follow the RFC 1918 standard of private IP addresses. If you use a non-private IP address for this virtual server, Citrix ADC can't contact the XenMobile Server successfully during the authentication process. For details, see https://support.citrix.com/article/CTX200430.

MDM load balancing mechanism

Decision detail:

- How will Citrix Gateway load balance the XenMobile Servers?

Design guidance:

Use SSL Bridge if XenMobile is in the DMZ. Use SSL Offload, if necessary to meet security standards, when XenMobile is in the internal network.

- When you load balance XenMobile Server with Citrix ADC VIPs in SSL Bridge mode, Internet traffic flows directly to XenMobile Server, where connections terminate. SSL Bridge mode is the simplest mode to set up and troubleshoot.
- When you load balance XenMobile Server with Citrix ADC VIPs in SSL Offload mode, Internet traffic flows directly to Citrix ADC, where connections terminate. Citrix ADC then establishes new sessions from Citrix ADC to XenMobile Server. SSL Offload mode involves extra complexity during setup and troubleshooting.

Service port for MDM load balancing with SSL Offload

Decision detail:

- If you plan to use SSL Offload mode for Load Balancing, what port will the back-end service use?

Design guidance:

For SSL Offload, choose port 80 or 8443 as follows:

- Use port 80 back to XenMobile Server, for true offloading.
- End-to-end encryption, that is, re-encryption of traffic, isn't supported. For details, see the Citrix support article, Supported Architectures Between NetScaler and XenMobile Server.

Enrollment FQDN

Decision detail:

- What do you plan to use as the FQDN for enrollment and XenMobile instance/load balancing VIP?

Design guidance:

Initial configuration of the first XenMobile Server in a cluster requires that you provide the XenMobile Server FQDN. That FQDN must match your MDM VIP URL and your Internal MAM LB VIP URL. (An internal Citrix ADC address record resolves the MAM LB VIP.) For details, see “Enrollment FQDN for each management mode” later in this article.

In addition, you must use the same certificate as the following:

- XenMobile SSL listener certificate
- Internal MAM LB VIP certificate
- MDM VIP certificate (if using SSL Offload for MDM VIP)

> **Important:**
>
> After you configure the enrollment FQDN, you cannot change it. A new enrollment FQDN requires a new SQL Server database and XenMobile Server rebuild.

Secure Web traffic

Decision detail:

- Do you plan to restrict Secure Web to internal web browsing only?
- Do you plan to 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. Secure Web must 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 ADC, go through a proxy server, and then go out to the Internet. By default, Secure Web uses a per-application VPN tunnel back to the internal network for all network access. Citrix ADC uses split tunnel settings.

For a discussion of Secure Web connections, see Configuring User Connections.

Push Notifications for Secure Mail

Decision detail:

- Do you plan to use push notifications?

Design guidance for iOS:

Your Citrix Gateway configuration might include Secure Ticket Authority (STA), with split tunneling off. Citrix Gateway must allow traffic from Secure Mail to the Citrix listener service URLs 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 XenMobile. With FCM configured, any security action or deploy command triggers a push notification to Secure Hub to prompt the user to reconnect to the XenMobile Server.

HDX STAs

Decision detail:

- What STAs to use if you plan to integrate HDX application access?

Design guidance:

HDX STAs must match the STAs in StoreFront and must be valid for the Virtual Apps and Desktops farm.

Citrix Files and Citrix Content Collaboration

Decision detail:

- Do you plan to use storage zone controllers in the environment?
- What Citrix Files VIP URL do you plan to use?

Design guidance:

If you include storage zone controllers in your environment, ensure that you correctly configure the following:

- Citrix Files Switch VIP (used by the Citrix Files Control Plane to communicate with the storage zone Controller servers)
- Citrix Files Load Balancing VIPs
- All required policies and profiles

For information, see the storage zones controller documentation.

SAML IdP

Decision detail:

- If SAML is required for Citrix Files, do you want to use XenMobile as the SAML IdP?

Design guidance:

The recommended best practice is to integrate Citrix Files with XenMobile Advanced Edition or XenMobile Enterprise Edition, a simpler alternative to configuring SAML-based federation. When you use Citrix Files with those XenMobile editions, XenMobile provides Citrix Files with:

- Single sign-on (SSO) authentication of mobile productivity apps users
- User account provisioning based on Active Directory
- Comprehensive access control policies

The XenMobile 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 XenMobile clients (also referred to as wrapped Citrix Files) and Citrix Files mobile clients (also referred to as unwrapped Citrix Files). To understand the differences, see How Citrix Files for XenMobile Clients differ from Citrix Files mobile clients.

You can configure XenMobile and Citrix Content Collaboration to use SAML to provide SSO access to:

- Citrix Files mobile apps
- Non-wrapped Citrix Files clients, such as the website, Outlook plug-in, or sync clients

To use XenMobile 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:

- Must 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, XenMobile 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
Enterprise (MDM+MAM) with mandatory MDM enrollment	XenMobile Server FQDN
Enterprise (MDM+MAM) with optional MDM enrollment	XenMobile Server FQDN or Citrix Gateway FQDN
MDM only	XenMobile Server FQDN
MAM-only (legacy)	Citrix Gateway FQDN
MAM-only	XenMobile Server FQDN

Deployment Summary

Citrix recommends that you use the Citrix ADC for XenMobile wizard to ensure proper configuration. You can use the wizard only one time. If you have multiple XenMobile instances, such as for test, development, and production environments, you must configure Citrix ADC for the additional environments manually. When you have a working environment, take note of the settings before attempting to configure Citrix ADC manually for XenMobile.

The key decision you make when using the wizard is whether to use HTTPS or HTTP for communication to the XenMobile Server. HTTPS provides secure back-end communication, as traffic between Citrix ADC and XenMobile is encrypted. The re-encryption impacts XenMobile Server performance. HTTP provides better XenMobile Server performance. Traffic between Citrix ADC and XenMobile is not encrypted. The following tables show the HTTP and HTTPS port requirements for Citrix ADC and XenMobile Server.

HTTPS

Citrix typically recommends SSL Bridge for Citrix ADC MDM virtual server configurations. For Citrix ADC SSL Offload use with MDM virtual servers, XenMobile supports only port 80 as the back-end service.

Management mode	Citrix ADC load balancing method	SSL re-encryption	XenMobile server port
MDM	SSL Bridge	N/A	443, 8443
MAM	SSL Offload	Enabled	8443
Enterprise	MDM: SSL Bridge	N/A	443, 8443

Enterprise	MAM: SSL Offload	Enabled	8443

HTTP

Management mode	Citrix ADC load balancing method	SSL re-encryption	XenMobile server port
MDM	SSL Offload	Not supported	80
MAM	SSL Offload	Enabled	8443
Enterprise	MDM: SSL Offload	Not supported	80
Enterprise	MAM: SSL Offload	Enabled	8443

For diagrams of Citrix Gateway in XenMobile deployments, see Reference Architecture for On-Premises Deployments.

SSO and Proxy Considerations for MDX Apps

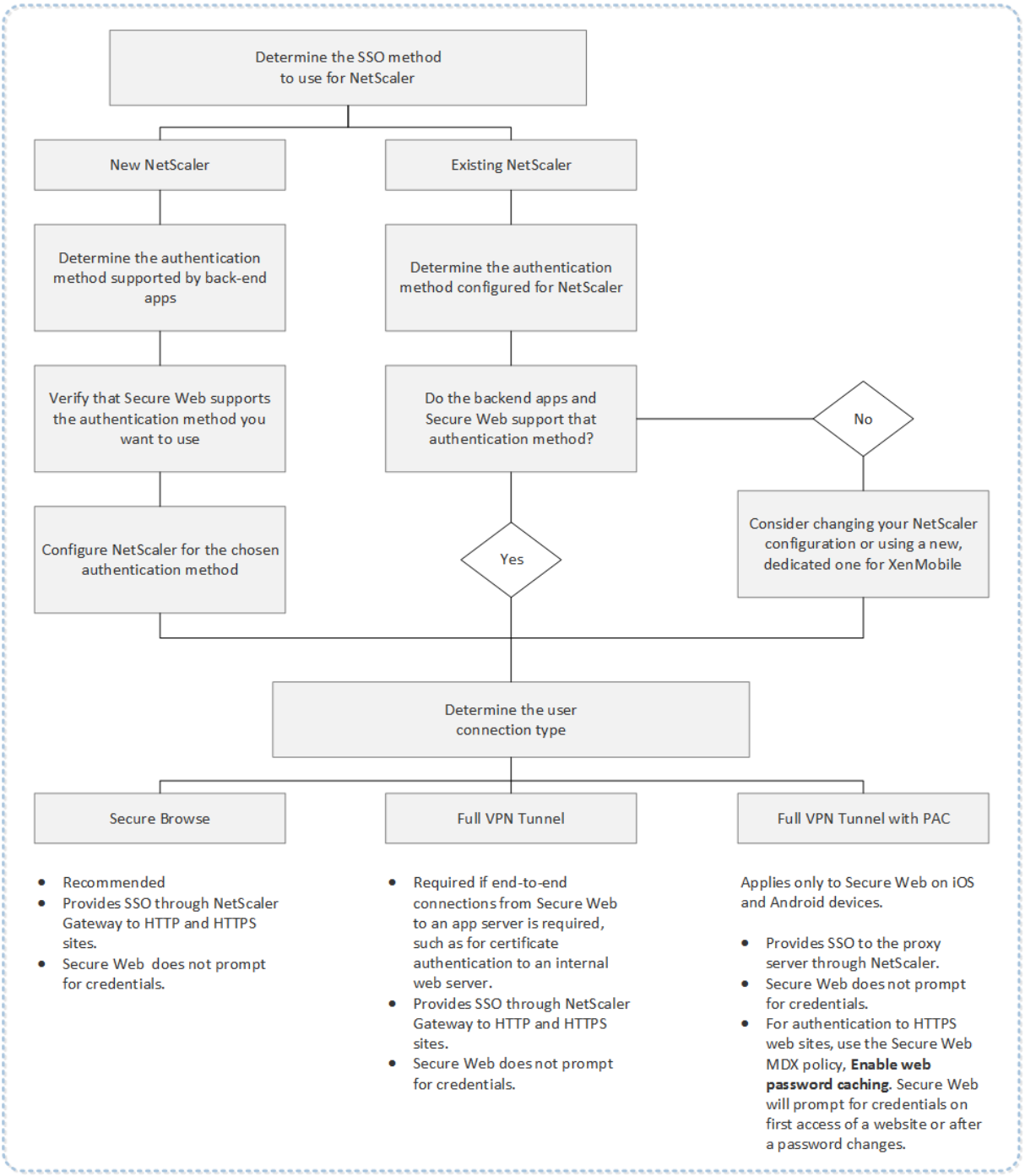
December 15, 2020

XenMobile integration with Citrix ADC 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, which is a type of clientless VPN
- Full VPN Tunnel

If Citrix ADC 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 ADC Authentication Methods

This section provides general information about the authentication methods supported by Citrix ADC.

SAML authentication

When you configure Citrix ADC 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 ADC Traffic profile.
- Configure the SAML IdP for the requested service.

NTLM authentication

If SSO to web apps is enabled in the session profile, Citrix ADC performs NTLM authentication automatically.

Required configuration:

- Enable SSO in the Citrix ADC Session or Traffic profile.

Kerberos impersonation

XenMobile supports Kerberos for Secure Web only. When you configure Citrix ADC for Kerberos SSO, Citrix ADC uses impersonation when a user password is available to Citrix ADC. Impersonation means that Citrix ADC uses user credentials to get the ticket required to gain access to services, such as Secure Web.

Required configuration:

- Configure the Citrix ADC “Worx” Session policy to allow it to identify the Kerberos Realm from your connection.
- Configure a Kerberos Constrained Delegation (KCD) account on Citrix ADC. Configure that account with no password and bind it to a traffic policy on your XenMobile gateway.
- For those and other configuration details, see the Citrix blog: WorxWeb and Kerberos Impersonation SSO.

Kerberos Constrained Delegation

XenMobile supports Kerberos for Secure Web only. When you configure Citrix ADC for Kerberos SSO, Citrix ADC uses constrained delegation when a user password is not available to Citrix ADC.

With constrained delegation, Citrix ADC 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 KCD account on Citrix ADC.
- Enable SSO in the Citrix ADC Traffic profile.
- Configure the back-end website for Kerberos authentication.

Form Fill Authentication

When you configure Citrix ADC 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 Secure Browse or Full VPN modes.

Required configuration:

- Configure Form-based SSO in the Citrix ADC Traffic profile.

Digest HTTP authentication

If you enable SSO to web apps in the session profile, Citrix ADC performs digest HTTP authentication automatically. This authentication method applies to apps that use Secure Browse or Full VPN modes.

Required configuration:

- Enable SSO in the Citrix ADC Session or Traffic profile.

Basic HTTP authentication

If you enable SSO to web apps in the session profile, Citrix ADC performs basic HTTP authentication automatically. This authentication method applies to apps that use Secure Browse or Full VPN modes.

Required configuration:

- Enable SSO in the Citrix ADC Session or Traffic profile.

Secure Browse, Full VPN Tunnel, or Full VPN Tunnel with PAC

The following sections describe the user connection types for Secure Web. For more information, see this Secure Web article in the Citrix documentation, Configuring user connections.

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 Full VPN tunnel for connections that use client certificates or end-to-end SSL to a resource in the internal network. Full VPN tunnel handles any protocol over TCP. You can use full VPN tunnel with Windows, Mac, iOS, and Android devices.

In Full VPN Tunnel mode, Citrix ADC does not have visibility inside an HTTPS session.

Secure Browse

Connections that tunnel to the internal network can use a variation of a clientless VPN, referred to as Secure Browse. Secure Browse is the default configuration specified for the Secure Web **Preferred VPN mode** policy. Citrix recommends Secure Browse for connections that require single sign-on (SSO).

In Secure Browse mode, Citrix ADC breaks the HTTPS session into two parts:

- From the client to Citrix ADC
- From Citrix ADC to the back-end resource server.

In this manner, Citrix ADC 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 secure browse mode. For details, see the blog XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode.

Full VPN Tunnel with PAC

You can use a Proxy Automatic Configuration (PAC) file with a full VPN tunnel deployment for Secure Web on iOS and Android devices. XenMobile supports proxy authentication provided by Citrix ADC. 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 ADC Split Tunneling

When planning your SSO and proxy configuration, you must also decide whether to use Citrix ADC split tunneling. Citrix recommends that you use Citrix ADC split tunneling only if needed. This section provides a high-level look at how split tunneling works: Citrix ADC determines the traffic path based on its routing table. When Citrix ADC 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 ADC 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 ADC 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 ADC split tunneling rules. A proxy server configured in a traffic policy does not override the Citrix ADC split tunneling rules.

By default, the **Network access** policy is set to **Tunneled to the internal network** for Secure Web. With that configuration, MDX apps use Citrix ADC split tunnel settings. The **Network access** policy default differs for some other mobile productivity apps.

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 ADC. Instead, those addresses are sent by using the device internet connection. For more information about reverse split tunneling, see the Citrix Gateway documentation.

XenMobile 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 Secure Browse mode with Citrix Gateway configured for reverse split tunneling.

Authentication

September 17, 2020

In a XenMobile deployment, several considerations come into play when deciding how to configure authentication. This section will help you understand the various factors that affect authentication by discussing the following:

- The main MDX policies, XenMobile 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. By reviewing the three recommended configurations, you should gain a greater understanding of the interplay of authentication measures available to you, and how to best deploy your own XenMobile environment.

Authentication Modes

Online authentication: Allows users into the XenMobile 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 XenMobile to one or more directories, such as Active Directory that are compliant with the Lightweight Directory Access Protocol (LDAP). This is a commonly used method 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 while still providing the security of complex passwords on enrollment, password expiration, and account lockout.

For more details, see Domain or domain plus STA.

Client certificate: XenMobile can integrate with industry-standard certificate authorities to use certificates as the sole method of online authentication. XenMobile 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.

XenMobile supports Certificate Revocation List (CRL) only for a third-party Certificate Authority. If you have a Microsoft CA configured, XenMobile uses Citrix ADC to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the Citrix ADC 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; XenMobile re-issues 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 if you plan to use certificate-based authentication for users or if you need to use your enterprise Certificate Authority (CA) for issuing device certificates, see Reference Architecture for On-Premises Deployments.

Two Factor

LDAP + Client Certificate: In the XenMobile environment, this configuration is the best combination of security and user experience, with the best SSO possibilities coupled with security provided by two-factor authentication at Citrix ADC. Using both LDAP and client certificate provides security with both something users know (their Active Directory passwords) and something they have (client certificates on their devices). Secure Mail (and some other mobile productivity apps) can automatically configure

and provide a seamless first-time user experience with client certificate authentication, with a properly configured Exchange client access server environment. For optimal usability, you can combine this option 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 Involved in 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 XenMobile 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.

> **Note:**
>
> If you select Secure offline for the Encryption keys policy, this policy is automatically enabled.

Online session required: If **On**, the user must have a connection to the enterprise network and an active session in order 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 XenMobile. When you set the Maximum offline period, if Secure Hub for iOS has a valid Citrix Gateway token, the app retrieves new policies for MDX apps from XenMobile without any interruption to users. If Secure Hub does not have a valid Citrix ADC token, users must authenticate through Secure Hub in order for app policies to update. The Citrix ADC token may become invalid due to a 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 may use international roaming,

> the default of 72 hours (3 days) may 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, XenMobile issues a token that Secure Mail uses 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 will discontinue.

Online session required grace period: Determines how many minutes a user can use the app offline before the Online session required policy prevents them from further use (until the online session is validated). 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 Service or MDX Toolkit: MDX Policies for iOS and MDX Policies for Android

XenMobile client properties

> **Note:**
>
> Client properties are a global setting that apply to all devices that connect to XenMobile.

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 XenMobile 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. You should enable this setting if **ENABLE_PASSWORD_CACHING** is enabled or if XenMobile 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 will still require 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 ADC Settings

Session time-out: If you enable this setting, Citrix Gateway disconnects the session if Citrix ADC detects no network activity for the specified interval. This setting is enforced for users who connect with

the Citrix Gateway Plug-in, Citrix Receiver, 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 Receiver, Secure Hub, or through a web browser. If Secure Mail is using STA, a special Citrix ADC mode, the Forced time-out setting does not apply to Secure Mail sessions. Default is **1440 minutes**. If you leave this value blank, the setting is disabled.

For more information about time-out settings in Citrix Gateway, see the Citrix ADC documentation.

For more information on the scenarios that prompt users to authenticate with XenMobile 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, MDX Service, or MDX Toolkit
- XenMobile console

Setting	Where to Find the Setting	Default Setting
Session time-out	Citrix Gateway	1440 minutes
Force time-out	Citrix Gateway	1440 minutes
Maximum offline period	MDX Policies	72 hours
Background services ticket expiration	MDX Policies	168 hours (7 days)
Online session required	MDX Policies	Off
Online session required grace period	MDX Policies	0
App passcode	MDX Policies	On
Encrypt secrets using passcode	XenMobile client properties	false
Enable Citrix PIN Authentication	XenMobile client properties	false
PIN Strength Requirement	XenMobile client properties	Medium
PIN Type	XenMobile client properties	Numeric

Setting	Where to Find the Setting	Default Setting
Enable User Password Caching	XenMobile client properties	false
Inactivity Timer	XenMobile client properties	15
Enable Touch ID Authentication	XenMobile client properties	false

Recommended Configurations

This section gives examples of three XenMobile configurations that range from lowest security and optimal user experience, to the highest security and more intrusive user experience. These examples should provide you with helpful reference points to determine where on the scale you want to place your own configuration. Be aware that modifying these settings may require you to alter other settings as well. For instance, the maximum offline period should always be less than the session time-out.

Highest Security

This configuration offers the highest level of security but contains significant usability trade-offs.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Session time-out	Citrix Gateway	1440	Users enter their Secure Hub credentials only when online authentication is required-every 24 hours.
Force time-out	Citrix Gateway	1440	Online authentication will be strictly required every 24 hours. Activity doesn't extend session life.
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. In the case of Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop without prompting the user if they don’t open the app before the session expires.
Online session required	MDX Policies	Off	Ensures a valid network connection and Citrix Gateway session to use apps.
Online session required grace period	MDX Policies	0	No grace period (if you enabled Online Session required).
App passcode	MDX Policies	On	Require passcode for application.
Encrypt secrets using passcode	XenMobile client properties	true	A key derived from user entropy protects the vault.
Enable Citrix PIN Authentication	XenMobile client properties	true	Enable Citrix PIN for simplified authentication experience.
PIN Strength Requirement	XenMobile client properties	Strong	High password complexity requirements.

PIN Type	XenMobile client properties	Alphanumeric	PIN is an alphanumeric sequence.
Enable Password Caching	XenMobile client properties	false	Active Directory password is not cached and Citrix PIN will be used for offline authentications.
Inactivity Timer	XenMobile client properties	15	If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.
Enable Touch ID Authentication	XenMobile 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

Force time-out	Citrix Gateway	No value	Sessions will be 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. In the case of Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop without prompting the user if they don't open the app before the session expires.
Online session required	MDX Policies	Off	Ensures a valid network connection and Citrix Gateway session to use apps.
Online session required grace period	MDX Policies	0	No grace period (if you enabled Online Session required).
App passcode	MDX Policies	On	Require passcode for application.

Encrypt secrets using passcode	XenMobile client properties	false	Do not require user entropy to encrypt the vault.
Enable Citrix PIN Authentication	XenMobile client properties	true	Enable Citrix PIN for simplified authentication experience.
PIN Strength Requirement	XenMobile client properties	Medium	Enforces medium password complexity rules.
PIN Type	XenMobile client properties	Numeric	PIN is a numeric sequence.
Enable Password Caching	XenMobile client properties	true	The user PIN caches and protects the Active Directory password.
Inactivity Timer	XenMobile client properties	30	If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.
Enable Touch ID Authentication	XenMobile 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
Force time-out	Citrix Gateway	No value	Sessions will be 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. In the case of Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop without prompting the user if they don't open the app before the session expires.
Online session required	MDX Policies	Off	Ensures a valid network connection and Citrix Gateway session to use apps.

Online session required grace period	MDX Policies	0	No grace period (if you enabled Online Session required).
App passcode	MDX Policies	On	Require passcode for application.
Encrypt secrets using passcode	XenMobile client properties	false	Do not require user entropy to encrypt the vault.
Enable Citrix PIN Authentication	XenMobile client properties	true	Enable Citrix PIN for simplified authentication experience.
PIN Strength Requirement	XenMobile client properties	Low	No password complexity requirements
PIN Type	XenMobile client properties	Numeric	PIN is a numeric sequence.
Enable Password Caching	XenMobile client properties	true	The user PIN caches and protects the Active Directory password.
Inactivity Timer	XenMobile client properties	90	If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.
Enable Touch ID Authentication	XenMobile client properties	true	Enables Touch ID for offline authentication use cases in iOS.

Using Step-Up Authentication

Some apps may 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 ADC 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 ADC appliance.	Allows for enhanced authentication controlled by the secondary Citrix ADC appliance authentication and session policies.

If a user opens an app that logs on to the alternate Citrix Gateway instance, all other apps will use that Citrix Gateway instance for communicating with the internal network. The session will only switch back to the lower security Citrix Gateway instance when the session times out from the Citrix Gateway instance with enhanced security.

Using Online Session Required

For certain applications, such as Secure Web, you may want to ensure that users run an app only when they have an authenticated session and while the device is connected to a network. This policy enforces that option and allows for a grace period so users can finish their work.

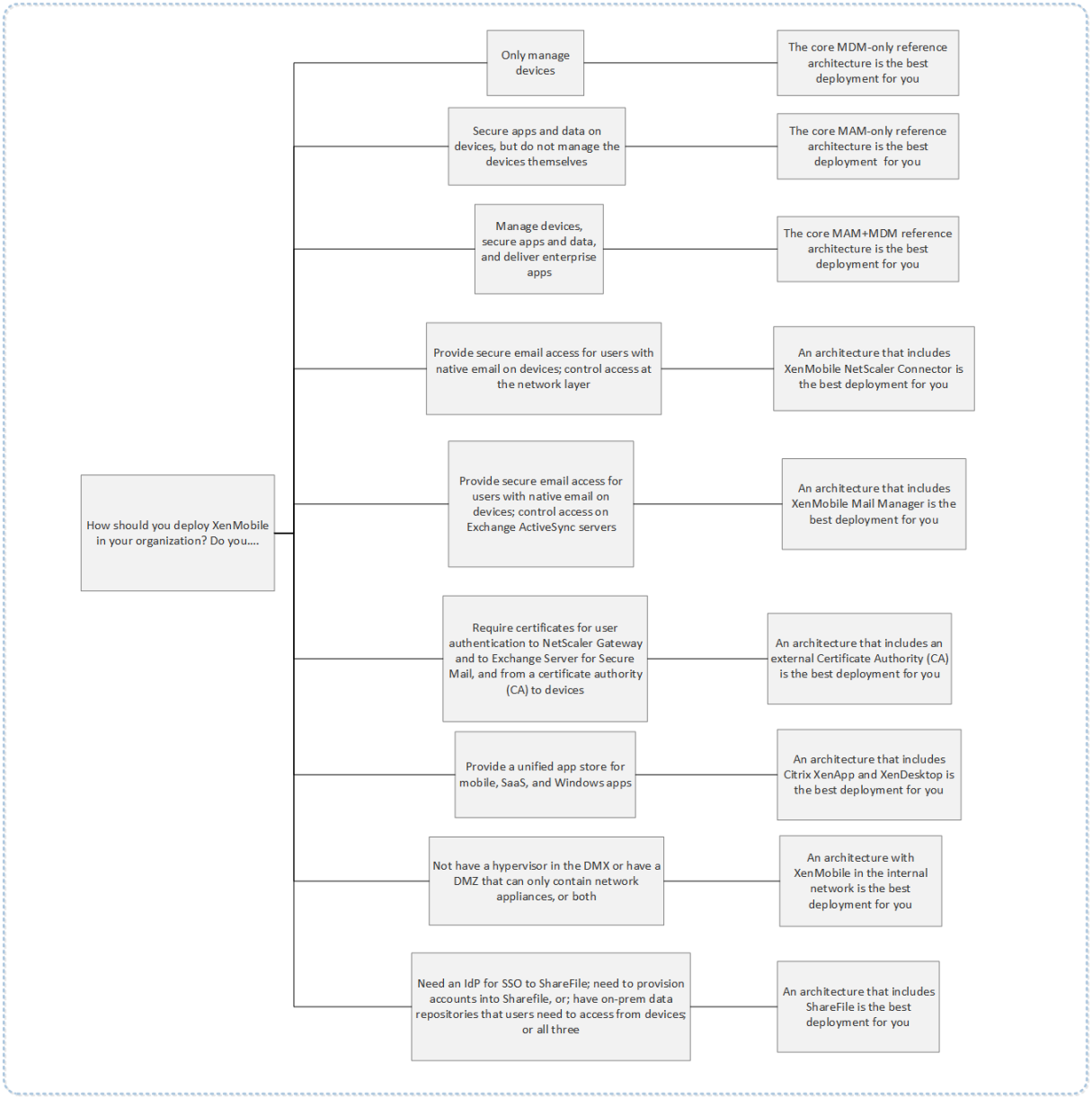
Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Online session required	MDX Policies	On	Ensures device is online and has a valid authentication token.
Online session required grace period	MDX Policies	15	Allows a 15-minute grace period before the user can no longer use apps

Reference Architecture for On-Premises Deployments

March 25, 2020

The figures in this article illustrate the reference architectures for the XenMobile deployment on premises. The deployment scenarios include MDM-only, MAM-only, and MDM+MAM as the core architectures, as well as those that include components, such as the SNMP Manager, Citrix Gateway connector for Exchange ActiveSync, Endpoint Management connector for Exchange ActiveSync, and Virtual Apps and Desktops. The figures show the minimal components required for XenMobile.

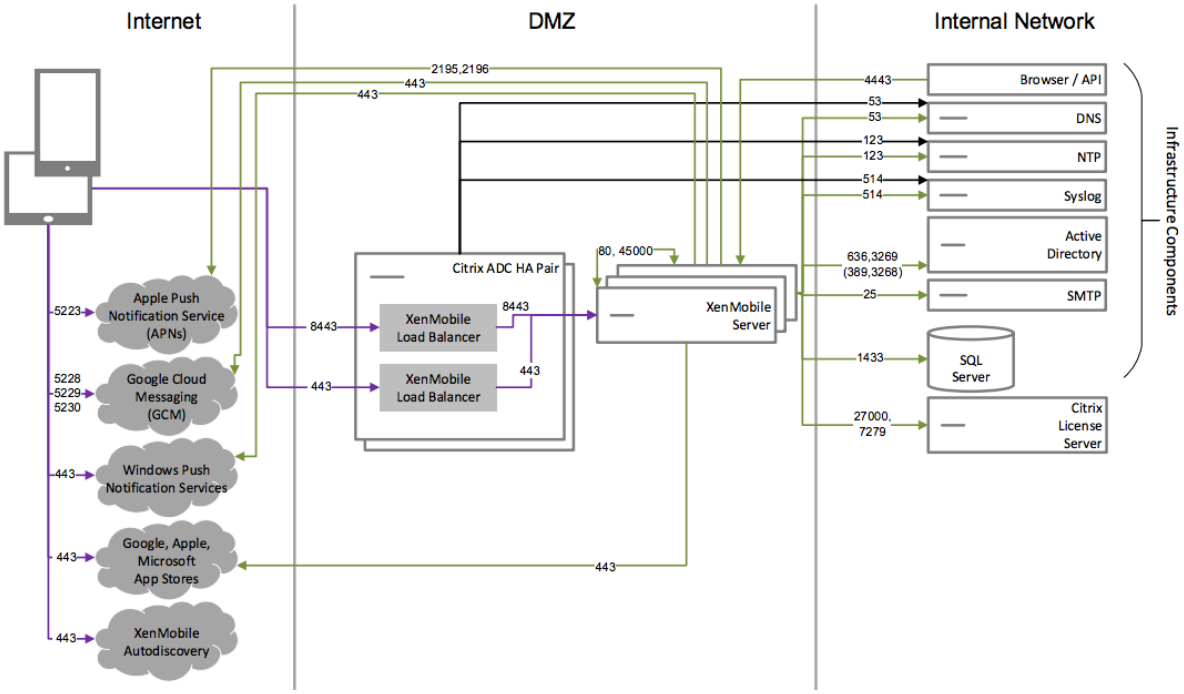
Use this chart as a general guide for your deployment decisions.



In the figures, the numbers on the connectors represent ports that you must open to allow connections between the components. For a complete list of ports, see Port requirements in the XenMobile documentation.

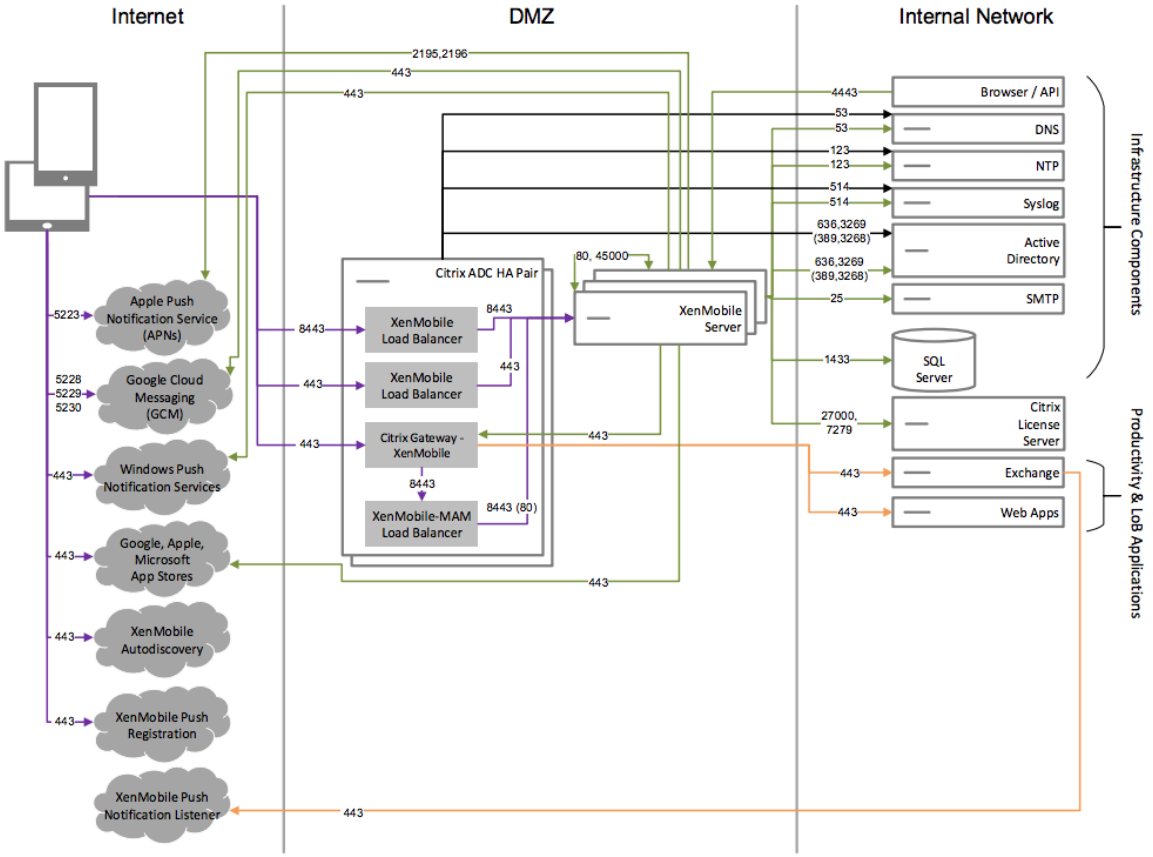
Core MDM-Only Reference Architecture

Deploy this architecture if you plan to use only the MDM features of XenMobile. For example, you need to manage a corporate-issued device through MDM in order to deploy device policies, apps and to retrieve asset inventories and be able to carry out actions on devices, such as a device wipe.



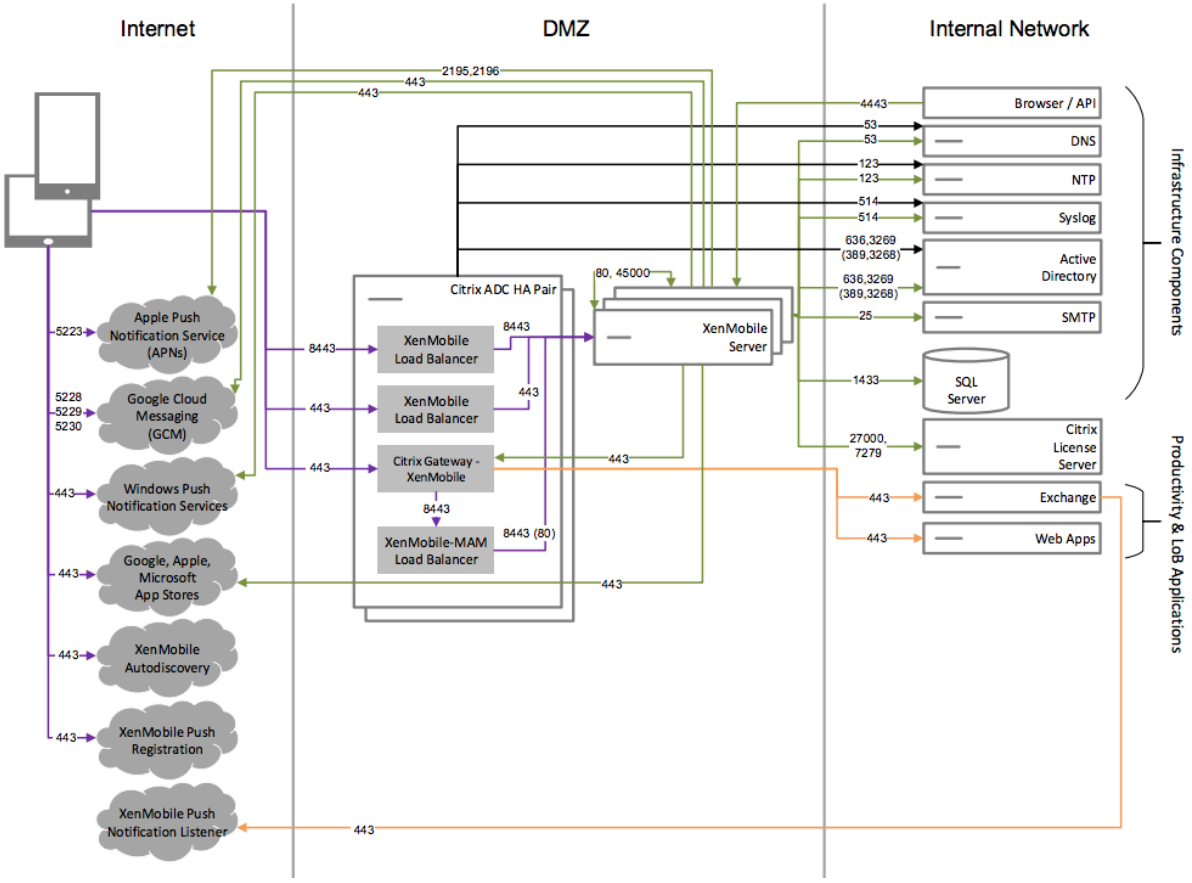
Core MAM-Only Reference Architecture

Deploy this architecture if you plan to use only the MAM features of XenMobile without having devices enroll for MDM. For example, you want to secure apps and data on BYO mobile devices; you want to deliver enterprise mobile apps and be able to lock apps and wipe their data. The devices cannot be MDM enrolled.



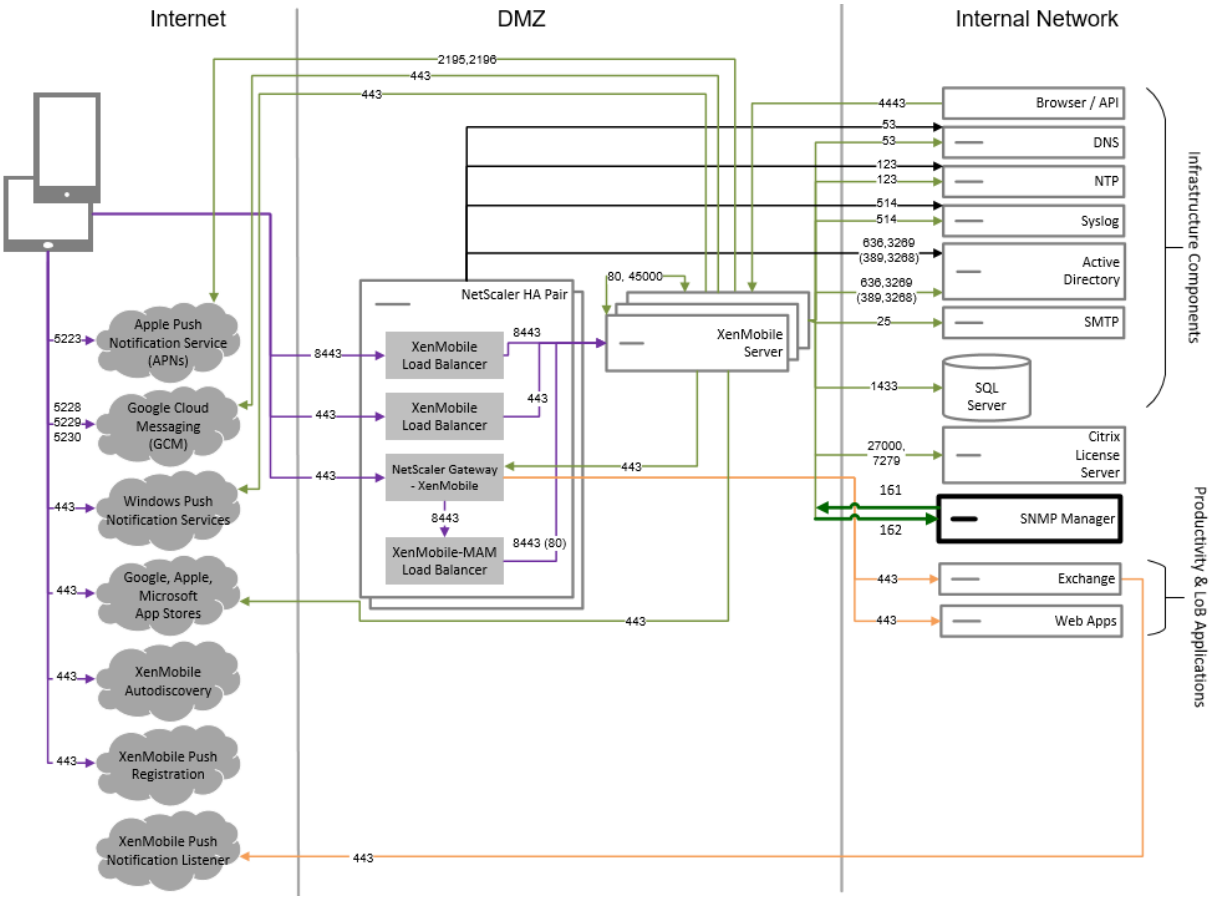
Core MAM+MDM Reference Architecture

Deploy this architecture if you plan to use MDM+MAM features of XenMobile. For example, you want to manage a corporate-issued device via MDM; you want to deploy device policies and apps, retrieve an asset inventory and be able to wipe devices. You also want to deliver enterprise mobile apps and be able to lock apps and wipe the data on devices.



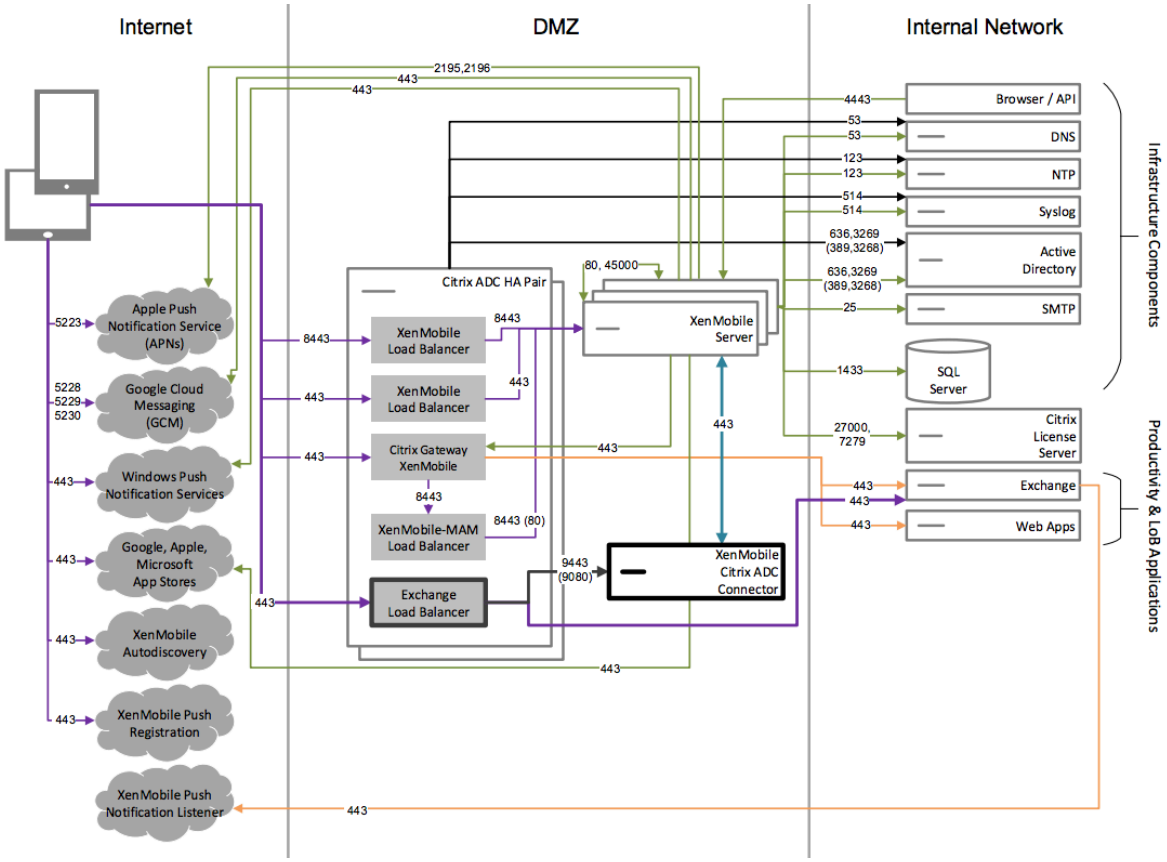
Reference Architecture with SNMP

Deploy this architecture if you plan to enable SNMP monitoring with XenMobile. For example, you want to allow monitoring systems to query and obtain information on your XenMobile nodes. For details, see SNMP monitoring.



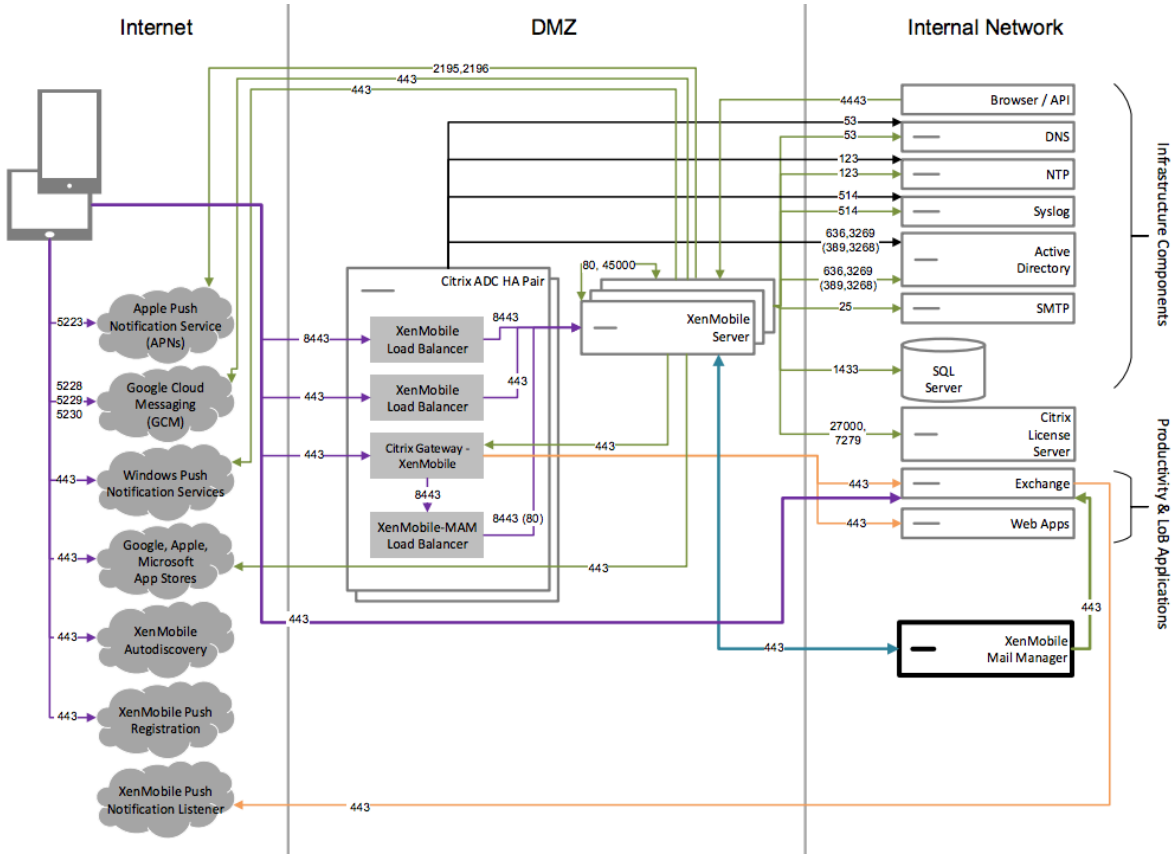
Reference Architecture with Citrix Gateway connector for Exchange ActiveSync

Deploy this architecture if you plan to use Citrix Gateway connector for Exchange ActiveSync with XenMobile. For example, you need to provide secure email access to users who use native mobile email apps. These users will continue accessing email via a native app or you may transition them over time to Citrix Secure Mail. Access control needs to occur at the network layer before traffic hits the Exchange Active Sync servers. Even though the diagram shows the connector for Exchange ActiveSync deployed in a MDM and MAM architecture, you can also deploy the connector for Exchange ActiveSync in the same manner as part of an MDM-only architecture.



Reference Architecture with Endpoint Management connector for Exchange ActiveSync

Deploy this architecture if you plan to use Endpoint Management connector for Exchange ActiveSync with XenMobile. For example, you want to provide secure email access to users who use native mobile email apps. These users will continue accessing email via a native app or you may transition users over time to Secure Mail. You can achieve access control on the Exchange ActiveSync servers. Although the diagram shows Endpoint Management connector for Exchange ActiveSync deployed in a MDM and MAM architecture, you can also deploy Endpoint Management connector for Exchange ActiveSync in the same manner as part of an MDM-only architecture.

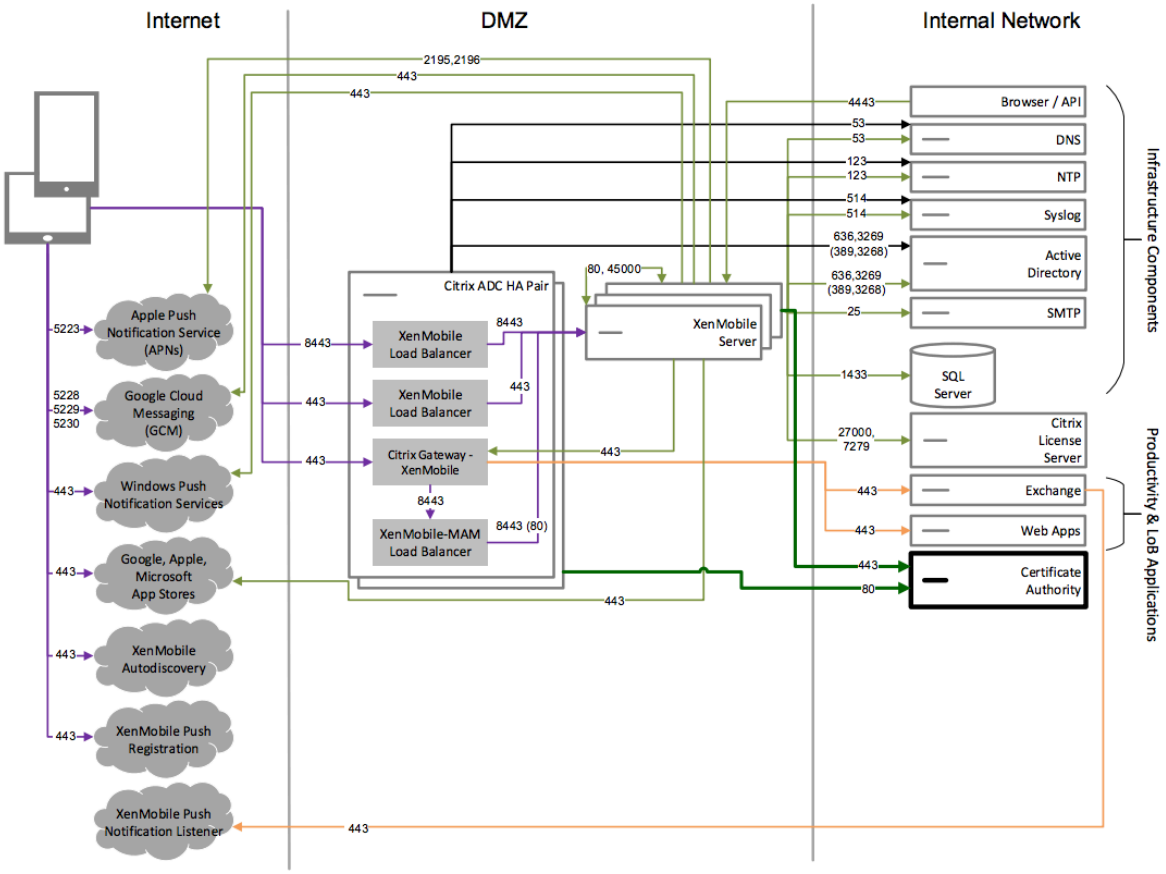


Reference Architecture with External Certificate Authority

A deployment that includes an external certificate authority is recommended to meet one or more of the following requirements:

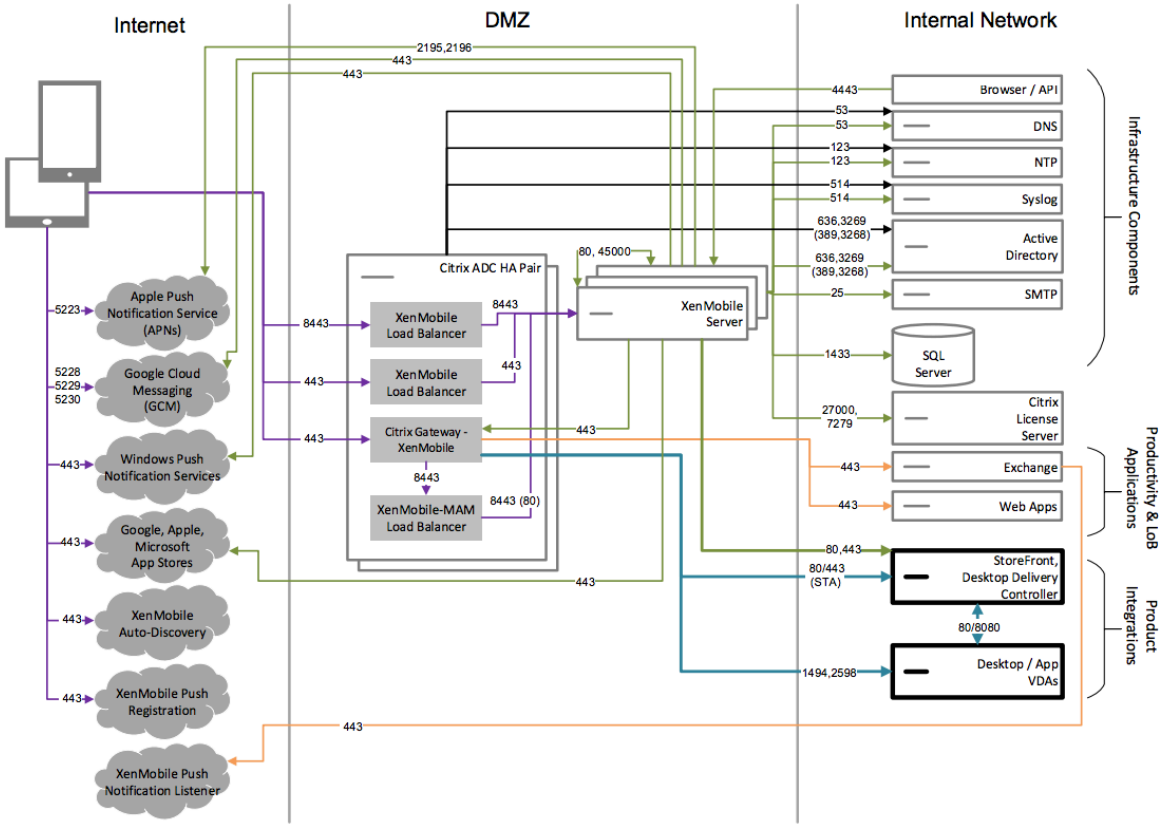
- You require user certificates for user authentication to Citrix Gateway (for intranet access).
- You require Secure Mail users to authenticate to Exchange Server by using a user certificate.
- You need to push certificates issued by your corporate Certificate Authority to mobile devices for WiFi access, for example.

Although the diagram shows an external certificate authority deployed in an MDM+MAM architecture, you can also deploy an external Certificate Authority in the same manner as part of an MDM-only or MAM-only architecture.



Reference Architecture with Virtual Apps and Desktops

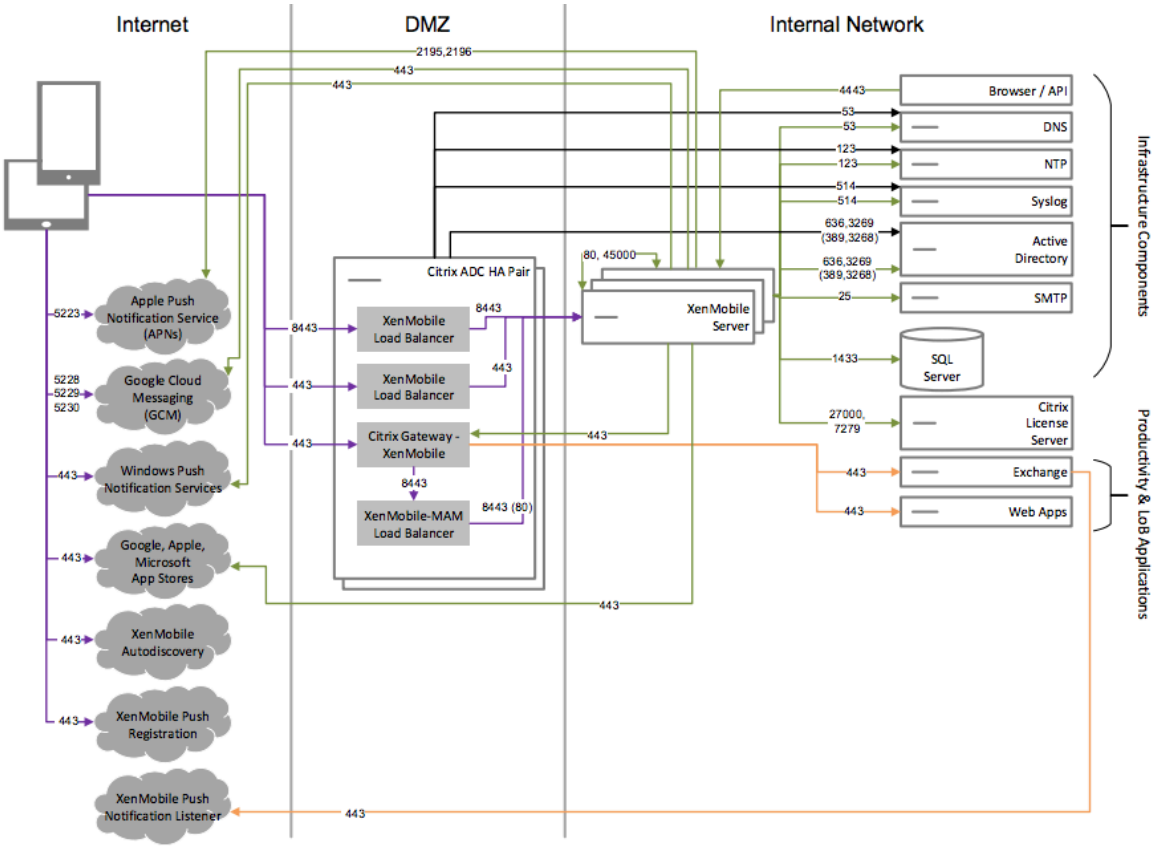
Deploy this architecture if you plan to integrate Virtual Apps and Desktops with XenMobile. For example, you need to provide a unified app store to mobile users for all types of applications (mobile, SaaS and Windows). Although the diagram shows Virtula Desktops deployed in a MDM and MAM architecture, you can also deploy those desktops in the same manner as part of a MAM-only architecture.



Reference Architecture with XenMobile in the Internal Network

You can deploy an architecture with XenMobile in the internal network to meet one or more of the following requirements:

- You do not have or are not allowed to have a hypervisor in the DMZ.
- Your DMZ can only contain network appliances.
- Your security requirements require the use of SSL Offload.



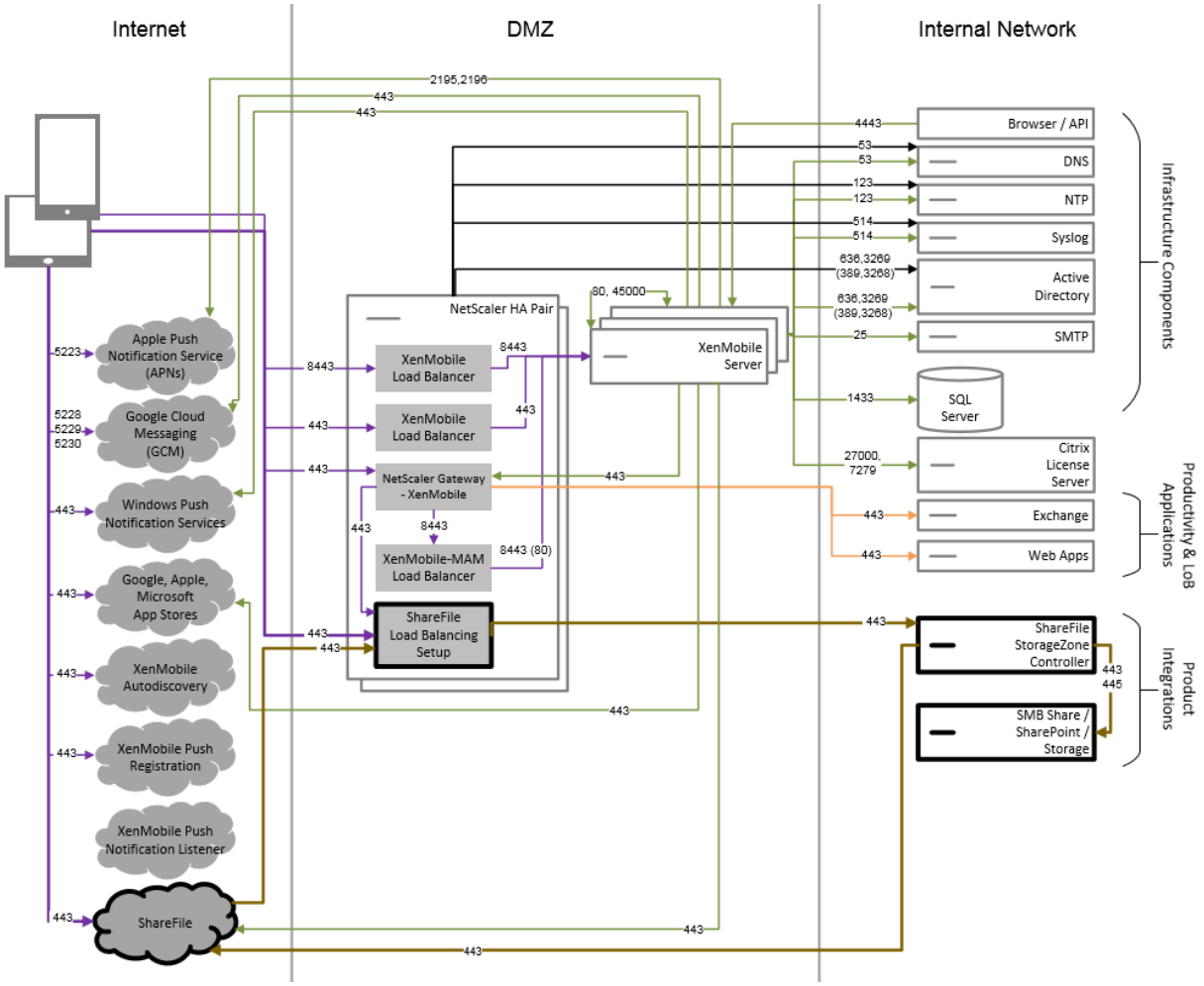
Reference Architecture with Citrix Content Collaboration

Deploy this architecture if you want to integrate Citrix Files or only storage zone connectors with XenMobile. Citrix Files integration enables you to meet one or more of the following requirements:

- You need an IDP to give users single sign-on (SSO) to ShareFile.com.
- You need a way to provision accounts into ShareFile.com.
- You have on-premises data repositories that need to be accessed from mobile devices.

An integration with only storage zone connectors gives users secure mobile access to existing on-premises storage repositories, such as SharePoint sites and network file shares. In this configuration, you don't need to set up a Citrix Content Collaboration subdomain, provision users to Citrix Files, or host Citrix Files data.

Although the diagram shows Citrix FIles deployed in a MDM+MAM architecture, you can also deploy Citrix Files in the same manner as part of a MAM-only architecture.



Server Properties

October 13, 2020

Server properties are global properties that apply to operations, users, and devices across an entire XenMobile 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.

A change to some server properties requires a restart of each XenMobile server node. XenMobile notifies you when a restart is required.

Some server properties help improve performance and stability. For details, see Tuning XenMobile Operations.

Access all apps in the managed Google Play store. If `true`, XenMobile makes all apps from the public Google Play store accessible from the managed Google Play store. Setting this property to

true allows the public Google Play store apps for all Android Enterprise users. Administrators can then use the Restrictions device policy to control access to these apps. Defaults to **false**.

Allow hostnames for iOS App Store links: The property `ios.app.store.allowed.hostnames` is a list of allowed host names used when uploading public app store apps to the server using the public APIs. If you plan on uploading public app store apps using the public APIs rather than uploading the apps through the server, configure this property. The default value is `itunes.apple.com,vpp.itunes.apple.com,apps.apple.com`.

Block Enrollment of Rooted Android and Jailbroken iOS Devices: When this property is **true**, XenMobile blocks enrollments for rooted Android devices and jailbroken iOS devices. Default is **true**. Recommended setting is **true** for all security levels.

Enrollment required: `wsapi.mdm.required.flag`, which applies only when the XenMobile Server Mode is ENT, specifies whether you require users to enroll in MDM. The property applies to all users and devices for the XenMobile instance. Requiring enrollment provides a higher level of security. However, that decision depends on whether you want to require MDM. By default, enrollment is not required.

When this property is **false**, users can decline enrollment, but can still access apps on their devices through the XenMobile Store. When this property is **true**, any user who declines enrollment is denied access to any apps.

If you change this property after users enroll, the users must re-enroll.

For a discussion about whether to require MDM enrollment, see Device Management and MDM Enrollment.

Enable multimode enrollment: The property `enable.multimode.xms` allows you to create enrollment profiles on one XenMobile Server that controls enrollment settings for both device and app management for Android and iOS devices. In addition, the new enhanced enrollment profiles feature enables enrollment of dedicated devices for Android and MAM-only enrollment for Android and iOS devices. When this property is **false**, those enrollment options aren't available when setting up enrollment profiles. The default value is **true**. Devices that enroll when this property is **true** still work if you change the property to **false**.

Enable the Self-Help Portal: If `shp.console.enable` is **false**, it prevents access to the Self-Help Portal. Users who navigate to the Self-Help Portal on port 443 get a 404 error. 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**.

Local user account lockout limit: Using the restriction policy, you can set a limit on sign-in attempts for Active Directory users. Use the key `local.user.account.lockout.limit` to do the same for local user accounts. After users attempt to sign in the number of times you specify, they can't attempt again until an amount of time passes. Configure that time with the **Local user account lockout time** property. The default value is 6.

Local user account lockout time: The property `local.user.account.lockout.time` allows you to set a number of minutes that must pass before a locked out local user account can attempt to sign in again. The default value is `30` minutes.

Maximum size of file upload restriction enabled: Enable restricting the maximum file size for uploads setting `max.file.size.upload.restriction` to **`true`**. If you enable this restriction, configure the maximum file size using `max.file.size.upload.allowed`. The default value for this property is **`true`**.

Maximum size of file upload allowed: With `max.file.size.upload.allowed`, you can specify a maximum file size for any uploads. Example values include `500 B`, `1 KB`, `1 MB`, `1 MiB`, `1 G`, or `1 GiB`. The default value is `5 MB`.

Inactivity Timeout in Minutes: The number of minutes after which XenMobile logs out an inactive user who used the XenMobile Server Public API to access the XenMobile console or any third-party app. A time-out value of `0` means an inactive user remains logged in. For third-party apps that access the API, remaining logged in is typically necessary. Default is `5`.

iOS Device Management Enrollment Install Root CA if Required: The latest enrollment workflow from Apple requires that users manually install the MDM profiles. That workflow doesn't apply to MDM enrollment to servers assigned in Apple Business Manager or Apple School Manager. However, during manual enrollment in MDM, iOS device users receive only the MDM device certificate prompt during enrollment.

To provide a better user experience during manual enrollment, Citrix recommends changing the server property `ios.mdm.enrollment.installRootCaIfRequired` to **`false`**. The default value is **`true`**. With that change, a Safari window opens during MDM enrollment to simplify the profile installation for users.

VPP baseline interval: The property `vpp.baseline` sets the minimum interval that XenMobile reimports volume purchase licenses from Apple. Refreshing license information ensures that XenMobile reflects all changes, such as when you manually delete an imported app from volume purchase. By default, XenMobile refreshes the volume purchase license baseline a minimum of every `1440` minutes.

If you have many volume purchase licenses installed (for example, over 50,000), Citrix recommends that you increase the baseline interval to reduce the overhead of importing licenses. If you expect frequent volume purchase license changes from Apple, Citrix recommends that you lower the value to keep XenMobile updated with the changes. The minimum interval between two baselines is 60 minutes. Because the cron job runs every 60 minutes, if the volume purchase baseline interval is 60 minutes, the interval between baselines can be delayed up to 119 minutes.

XenMobile MDM Self Help Portal console max inactive interval (minutes): This property name reflects the older XenMobile versions. The property controls the XenMobile console max inactive interval. That interval is the number of minutes after which XenMobile logs an inactive user out of the XenMobile console. A time-out of 0 means an inactive user remains logged in. Default is `30`.

Device and App Policies

April 1, 2021

XenMobile 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. In the event 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

XenMobile device and app policies address many situations that may pose a security risk, such as the following:

- When users try to access apps and data from untrusted devices and unpredictable locations.
- When users pass data from device to device.
- When an unauthorized user tries to access data.
- When a user who has left the company had used their own device (BYOD).
- When a user misplaces a device.
- When users need to access the network securely at all times.
- When users have their own device managed and you need to separate work data from personal data.
- When a device is idle and requires verification of user credentials again.
- When users copy and paste sensitive content into unprotected email systems.
- When 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 XenMobile protects data at rest

Data stored on mobile devices is referred to as data at rest. XenMobile uses the device encryption provided by the iOS and Android platforms. XenMobile supplements platform-based encryption with features such as compliance checking, available through the Citrix MAM SDK.

The mobile application management (MAM) capabilities in XenMobile enable complete management, security, and control over mobile productivity apps, MDX-enabled apps, and their associated data.

The Mobile Apps SDK enables apps for XenMobile 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.

XenMobile also includes app-level encryption. XenMobile 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.

Policies and the Mobile Apps SDK enable you to:

- Separate business and personal apps and data in a secure mobile container.
- Secure apps with encryption and other mobile Data Loss Prevention (DLP) technologies.

MDX policies provide many operational controls. You can enable seamless integration between apps that are MAM SDK enabled or MDX-wrapped, while also controlling all communication. In this way, you can enforce policies, such as ensuring that data only is accessible by MAM SDK enabled or MDX-wrapped apps.

Beyond device and app policy control, the best way to safeguard data at rest is encryption. XenMobile adds a layer of encryption to any data stored in an MDX-enabled app, giving you policy control over features such as public file encryption, private file encryption, and encryption exclusions. The Mobile Apps SDK uses FIPS 140-2 compliant AES 256-bit encryption with keys stored in a protected Citrix Secret Vault.

How XenMobile 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 could 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, used for authentication and for micro VPN sessions with an app. You can use an Alternate Citrix Gateway with the Online 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 XenMobile 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 XenMobile operation in sync with enterprise or industry changes, such as new corporate security policies or compliance regulations
- When a new version of MDX Service 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 XenMobile. 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 Client Properties in your XenMobile Server Settings. You can set an inactivity timer in Client Properties so that, with continued use, Secure Hub doesn't prompt the user to authenticate to the managed app again until the timer expires.

  The app passcode differs from a device passcode in that, with a device passcode policy pushed to a device, Secure Hub prompts the user to configure a passcode or PIN, which they must unlock before they can gain access to their device when they turn on the device or when the inactivity timer expires. For more information, see Authentication in XenMobile.

  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.

- **Online session required**

  Why use this policy: If an application requires access to a web app (web service) to run, enable this policy so that XenMobile 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 Online session required policy enabled, they can't use the app until they connected to the network using a cellular or Wi-Fi service.

- **Maximum offline period**

  Why use this policy: Use this policy as an additional security option, to ensure that users can't run an app offline for long time periods without reconfirming app entitlement and refreshing policies from XenMobile.

  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 XenMobile 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 those who might experience long periods offline when travelling internationally.

  User example: You load a new version of Secure Mail in the XenMobile Store and then set an app update grace period of 6 hours. All Secure Mail users will see a message asking them to update their Secure Mail app, until the 6 hours expires. When the 6 hours expire, Secure Hub routes users to the XenMobile Store.

- **Active poll period (minutes)**

  Why use this policy: The active poll period is the interval at which XenMobile 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, when you send the App Lock command from XenMobile to the device, the lock occurs within 60 minutes of when the last poll took place.

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 or from pasting data from outside of 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 but 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 Quick Edit but 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. This helps 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: If you enable the App Restriction policy to block dictation on iOS in an MDX app, the user can't use the dictate function on the iOS keyboard while the MDX app is running. Thus, data 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. For the Network access policy, set the **Tunneled to the internal network** option to automate a micro VPN from the MDX app through the Citrix ADC to a back-end web service or datastore.

User example: When a user opens an MDX app, such as Secure Web, that has tunneling enabled, the browser opens and launches an intranet site without the user needing to start a VPN. The Secure Web app automatically accesses the internal site using 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 leverage 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 Citrix ADC 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. Be aware that 2 weeks of email takes longer to sync than 3 days and prolongs the setup process for the user.

  User example: If the default sync interval is set to 3 days when the user first sets up Secure Mail, they can see any emails in their Inbox that they received from the present to 3 days in the past. If a user wants to see emails that are older than 3 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 XenMobile works with 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: Deploy the App inventory policy to a device if you need to see the apps installed by a user. If you don't deploy the App inventory policy, you can see only the apps that a user installed from the XenMobile Store and not any personally installed applications. You must use this policy if you want 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 XenMobile administrators.

- **App lock policy**

  Why use this policy: The App Lock policy, for Android, allows you to block or allow apps. For example, by allowing 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: You must use the Connection scheduling policy so that Windows Mobile devices can connect back to XenMobile Server for MDM management, app push, and policy deployment. For Android, Android Enterprise, and Chrome OS devices, use Google Firebase Cloud Messaging (FCM), instead of this policy, to control connections to XenMobile Server. The Scheduling options are as follows:

  - **Always:** Keeps the connection alive permanently. Citrix recommends this option for optimized security. When you choose **Always**, also use the Connection timer policy to ensure that the connection is not draining the battery. By keeping the connection alive, you can push security commands like wipe or lock to the device on-demand. You must also select the Deployment Schedule option **Deploy for always-on connection** in each policy you deploy to the device.
  - **Never:** Connects manually. Citrix does not recommend this option for production deployments because the **Never** option prevents you from deploying security policies to devices; thus, users never receive any new apps or policies.
  - **Every:** Connects at the designated interval. When this option is in effect and you send a security policy, such as a lock or a wipe, XenMobile processes the policy on the device the next time the device connects.
  - **Define schedule:** When enabled, XenMobile attempts to reconnect the user's device to the XenMobile server after a network connection loss and 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 in conjunction with a WiFi policy, the Credentials policy lets you deploy certificates for authentication to internal resources that require certificate authentication.

  User example: You deploy a WiFi policy that configures a wireless network on the device. The WiFi 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 XenMobile, 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 XenMobile Store.
  - **Native email app:** Use the Exchange policy to enable ActiveSync email for the native email client on the device. With the Exchange policy for native email, 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 the XenMobile server, 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 XenMobile Self-Help Portal and choose the locate option to see the location of their device on a map. Note that the user makes the choice 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, which they must unlock before they can gain access to their device when they turn on the device 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 need to remove that policy from a subset of the users. You can remove the policy for selected users by creating a Profile removal policy and using deployment rules to deploy the Profile removal policy only to specified user names.

  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 won't know that camera use is now allowed. 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, from disabling the camera or microphone on a device to enforcing roaming rules and access to third-party services like app stores.

  User example: If you deploy a restriction to an iOS device, the user may not be able to access iCloud or the Apple App store.

- **Terms and conditions policy**

  Why use this policy: You might need to advise users of the legal implications of having their device managed. In addition, you may want to ensure that users are aware of the security risks when corporate data is pushed to the device. The custom 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 backend systems using older VPN Gateway technology. The policy supports a number of VPN providers, including Cisco AnyConnect, Juniper, as well as 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.

- **Webclip policy**

  Why use this policy: Use the Webclip 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 on a web clip icon to open an internet site that provides services they need to access. Using a web link is more convenient than needing to open a browser app and type a link address.

- **WiFi policy**

  Why use this policy: The WiFi policy lets you deploy WiFi network details, such as the SSID, authentication data, and configuration data, to a managed device.

User example: When you deploy the WiFi policy, the device automatically connects to the WiFi 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 in appropriate 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.

- **XenMobile Store policy**

  Why use this policy: The XenMobile 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 XenMobile, they access the XenMobile Store through the Citrix Secure Hub app. The user can then see all the corporate apps and services available to them. Users can click on an app to install it, access the data, rate and review the app, and download app updates from the XenMobile Store.

User Enrollment Options

March 25, 2021

You can have users enroll their devices in XenMobile 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 Android Enterprise or Windows devices.

- **Self Help Portal:** Set up a portal that users can visit to download Secure Hub and enroll their devices or send themselves an enrollment invitation.
- **Manual Enrollment:** Send out an email, handbook, or some other communication to let users know that the system is available for enrollment. 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 the 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, or legacy Android devices. Enrollment invitations and URLs aren't available for Android Enterprise or Windows devices.

You can also send an installation link through SMTP or SMS to users with iOS, macOS, Android, or Windows devices. For more information, see Enroll devices.

If you choose to use the enrollment invitation method, you can:

- Choose from up to seven enrollment security modes, depending on platform.
- Use any combination of the modes.
- Enable or disable the modes from the **Settings** page.
- Select a default from User name + Password, Two Factor, and User name + PIN. For information on each enrollment security mode, see To configure enrollment security modes.

If you choose certificate-based, consider excluding User name + Password traditional authentication from the allowed options. User name + Password authentication might expose a weak onboarding vector into your environment and potentially void the mandated security quality.

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. For example, sending invitations by 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 to access email outside of Secure Hub. You can use a one-time password (OTP) enrollment security mode as an alternative to Active

Directory passwords for MDM enrollment.

Self-Help Portal

Users can request an enrollment invitation through the Self-Help Portal. The default mode is User name + Password, but you can also change that requirement to Two Factor or User name + PIN. For information about setting up the Self-Help Portal, see To configure enrollment security modes.

Manual Enrollment

With manual enrollment, users connect to XenMobile 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 XenMobile 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, server information, or both.

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 XenMobile 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. 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 Sending an enrollment invitation.

While you can use Active Directory groups to create invitations in batches, you must carry out this approach in waves.

First Contact with Users

After you decide between open enrollment or selective invitation and then set up those environments, you must make users aware of 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 XenMobile console for open enrollment as well. For details, see Sending an enrollment invitation.

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 XenMobile, sending them an invitation email would be problematic.

You can also send communications by another means outside of XenMobile 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 XenMobile Server address. To learn more about AutoDiscovery, see XenMobile AutoDiscovery Service.

Tuning XenMobile Operations

May 7, 2021

The performance and stability of XenMobile operations involves many settings across XenMobile and depends on your Citrix ADC and SQL Server database configuration. This article focuses on the settings that admins most often configure, related to the tuning and optimization of XenMobile. Citrix recommends that you evaluate each of the settings in this article before deploying XenMobile.

> **Important:**
>
> These guidelines assume that the XenMobile server CPU and RAM is adequate for the number of devices. For more information about scalability, see Scalability and performance.

The following server properties globally apply to operations, users, and devices across an entire XenMobile instance. A change to some server properties requires a restart of each XenMobile server node. XenMobile notifies you when a restart is required.

These tuning guidelines apply to both clustered and non-clustered environments.

hibernate.c3p0.idle_test_period

This XenMobile server property, a Custom Key, determines the idle time in seconds before a connection is automatically validated. Configure the key as follows. Default is **30**.

- Key: **Custom Key**
- Key: **hibernate.c3p0. idle_test_period**
- Value: **120**
- Display name: **hibernate.c3p0. idle_test_period**
- Description: **Hibernate idle test period**

hibernate.c3p0.max_size

This Custom Key determines the maximum number of connections that XenMobile can open to the SQL Server database. XenMobile uses the value you specify for this custom key as an upper limit. The connections open only if you need them. Base your settings on the capacity of your database server.

Note the following equation in a clustered configuration. Your c3p0 connection multiplied by the number of nodes equals your actual maximum number of connections that XenMobile can open to the SQL Server database.

In clustered and non-clustered configuration, setting the value too high with an undersized SQL Server can cause resource issues on the SQL side during peak load. Setting the value too low means you might not be able to take advantage of the SQL resources available.

Configure the key as follows. Default is **1000**.

- Key: **hibernate.c3p0.max_size**
- Value: **1000**
- Display name: **hibernate.c3p0.max_size**
- Description: DB connections to SQL

hibernate.c3p0.min_size

This Custom Key determines the minimum number of connections that XenMobile opens to the SQL Server database. Configure the key as follows. Default is **100**.

- Key: **hibernate.c3p0.min_size**
- Value: **100**
- Display name: **hibernate.c3p0.min_size**
- Description: DB connections to SQL

hibernate.c3p0.timeout

This Custom Key determines the idle time-out. If you use database cluster failover, Citrix recommends that you add this Custom Key and set it to reduce the idle time-out. Default is **120**.

- Key: **Custom Key**
- Key: **hibernate.c3p0.timeout**
- Value: **120**
- Display name: **hibernate.c3p0.timeout**
- Description: Database idle timeout

Push Services Heartbeat Interval

This setting determines how frequently an iOS device checks if an APNs notification is not delivered in the interim. Increasing the APNs heartbeat frequency can optimize database communications. Too large a value can add unnecessary load. This setting applies only to iOS. Default is **20** hours.

If you have many iOS devices in your environment, the heartbeat interval can lead to higher load than necessary. Security actions, such as selective wipe, lock, and full wipe, do not rely on this heartbeat. The reason is that an APNs notification is sent to the device when these actions are executed. This value governs how quickly a policy updates after Active Directory Group membership changes. As such, it is often suitable to increase this value to something between 12 and 20 hours to reduce load.

iOS MDM APNS connection pool size

An APNs connection pool that is too small can negatively affect APNs activity performance when you have more than 100 devices. Performance issues include slower deployment of apps and policies to devices and slower device registration. Default is **1**. We recommend that you increase this value by 1 for about every 400 devices.

auth.ldap.connect.timeout

To compensate for slow LDAP responses, Citrix recommends that you add server properties for the following Custom Key.

- Key: **Custom Key**
- Key: **auth.ldap.connect.timeout**
- Value: **60000**
- Display name: **auth.ldap.connect.timeout**
- Description: **LDAP connection timeout**

auth.ldap.read.timeout

To compensate for slow LDAP responses, Citrix recommends that you add server properties for the following Custom Key.

- Key: **Custom Key**
- Key: **auth.ldap.read.timeout**
- Value: **60000**
- Display name: **auth.ldap.read.timeout**
- Description: **LDAP read timeout**

Other Server Optimizations

Server Property	Default Setting	Why Change This Setting?
Background Deployment	1,440 minutes	The frequency for background policy deployments, in minutes. Applies only to always-on connections for Android devices. Increasing the frequency of policy deployments reduces server load. Recommended setting is **1440** (24 hours).

Background Hardware Inventory	1,440 minutes	The frequency for background hardware inventory, in minutes. Applies only to always-on connections for Android devices. Increasing the frequency of hardware inventory reduces server load. Recommended setting is **1440** (24 hours).
Interval for check deleted Active Directory user	15 minutes	The standard sync time for Active Directory is **15** minutes. The value **0** prevents XenMobile from checking for deleted Active Directory users. Recommended setting is **15** minutes.
MaxNumberOfWorker	3	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, be aware that with a larger number of threads, such as 6, a volume purchase import results in high CPU usage.

How to check deadlocks in a SQL DB and delete historical data

When you see deadlocks, run the following query to see the deadlocks. Then, a database administrator or Microsoft SQL team can confirm the information.

SQL Query

```
1 SELECT
2
```



```
db.name DB_Service,

tl.request_session_id,

wt.blocking_session_id,

OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,

tl.resource_type,

h1.TEXT AS RequestingText,

h2.TEXT AS BlockingTest,

tl.request_mode

FROM sys.dm_tran_locks AS tl

INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id

INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address = wt.
    resource_address

INNER JOIN sys.partitions AS p ON p.hobt_id = tl.
    resource_associated_entity_id

INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id = tl.
    request_session_id

INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id = wt.
    blocking_session_id

CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1

CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2

GO
<!--NeedCopy-->
```

Clean up the database

> **Important:**
>
> Back up your database before you make changes to tables.

1. Run the following query to check the historical data.

```
select COUNT(*) as total_record from dbo.EWDEPLOY_HISTO;
select COUNT(*) as total_record from dbo.EWSESS;
select COUNT(*) as total_record from dbo.EWAUDIT;
<!--NeedCopy-->
```

2. Delete the data from the preceding three tables.

> **Note:**
>
> You may not see historical data in a table. If so, skip running the truncate query for that particular table.

```
truncate TABLE dbo.EWDEPLOY_HISTO;
truncate TABLE dbo.EWSESS;
truncate TABLE dbo.EWAUDIT;
<!--NeedCopy-->
```

3. Unblock the SELECT queries which were blocked due to deadlocks. This step takes care of further deadlocks.

```
ALTER DATABASE <database_name> SET       READ_COMMITTED_SNAPSHOT
   ON WITH ROLLBACK IMMEDIATE
<!--NeedCopy-->
```

4. By default, database cleanup is seven days for retaining session retention and audit retention data, which is high for many users. Change the cleanup value to 1 or 2 days. In server properties, make the following change:

```
zdm.dbcleanup.sessionRetentionTimeInDays = 1 day
zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day
zdm.dbcleanup.auditRetentionTimeInDays=1 day
<!--NeedCopy-->
```

Clean up orphans in the KEYSTORE table

If XenMobile nodes have poor performance, check if the KEYSTORE table is too large. XenMobile stores enrollment certificates in the ENROLLMENT_CERTIFICATE and KEYSTORE tables. When you delete or re-enroll devices, the certificates in the ENROLLMENT_CERTIFICATE table get deleted. Entries in the KEYSTORE table remain, which can cause performance issues. Perform the following procedure to clean the orphans from the KEYSTORE table.

> **Important:**
>
> Back up your database before you make changes to tables.

1. Run the following query to check the historical data.

```
select COUNT(*) from KEYSTORE
<!--NeedCopy-->
```

2. Check for orphans in the KEYSTORE table with the following query.

```
WITH cte(KEYSTORE_ID)
AS (SELECT KEYSTORE_ID
    FROM ENROLLMENT_CERTIFICATE
    UNION
    SELECT CA_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT CLIENT_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT KEYSTORE_ID
    FROM SAML_SERVICE_PROVIDER
    UNION
    SELECT KEYSTORE_ID
    FROM SERVER_CERTIFICATE)
SELECT keystore.id
FROM keystore
    LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
WHERE KEYSTORE_ID IS NULL;
<!--NeedCopy-->
```

3. Clear the orphans using the following query.

```
WITH cte(KEYSTORE_ID)
    AS (SELECT KEYSTORE_ID
        FROM ENROLLMENT_CERTIFICATE
        UNION
        SELECT CA_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT CLIENT_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT KEYSTORE_ID
        FROM SAML_SERVICE_PROVIDER
```



```
13          UNION
14          SELECT KEYSTORE_ID
15          FROM SERVER_CERTIFICATE)
16      DELETE FROM keystore
17      WHERE id IN
18      (
19          SELECT keystore.id
20          FROM keystore
21              LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
22          WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'
23      );
24  <!--NeedCopy-->
```

4. Add an index to the KEYSTORE table to improve search efficiency.

```
1  DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";
2  ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;
3  CREATE INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE"("NAME") INCLUDE ("
       ID", "TYPE", "CONTENT", "PASSWORD", "PUBLICLY_TRUSTED", "
       DESCRIPTION", "ALIAS", "MODIFICATION_DATE");
4  <!--NeedCopy-->
```

App Provisioning and Deprovisioning

September 17, 2020

Application provisioning revolves around mobile app lifecycle management: Preparing, configuring, delivering, and managing mobile apps within a XenMobile environment. In some instances, developing or modifying application code might also be part of the provisioning process. XenMobile is equipped with various tools and processes that you can use for app provisioning.

Before you read this article on app provisioning, we recommend that you read the following articles:

- Apps - User Communities

After you finalize the type of apps your organization plans to deliver to users, you can outline the process for managing the apps throughout their lifecycle.

Consider the following points when defining your app provisioning process:

- **App profiling:** Your organization can 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 from the beginning 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 Secure Browse or full VPN

  > **Note:**
  > Tunneled Web SSO is the name for the Secure Browse in the MDX settings. The behavior is the same.

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
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 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 production impact.

It is also important to evaluate if a specific upgrade is required. App upgrades are usually of two types: One is a minor upgrade, such as a fix to a specific bug. The second is a major release, which introduces significant changes and improvements to the app. 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 Service and MDX Toolkit, which is scheduled for deprecation in September 2021. For information about app wrapping, see Endpoint Management MDX Service. 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 XenMobile environment. The changes depend on the type of security compliance that the apps require. For example, you might want the device to be encrypted to allow the use of a critical business intelligence app. Or a certain app might require end-to-end SSL encryption or geofencing.

- **App delivery:** XenMobile allows you to deliver apps as MDM apps or as MAM apps. The MDM apps appear in the XenMobile Store. This store allows you to conveniently deliver public or native apps to users. The only MDM app control you manage is to enforce device level restrictions. However, delivering apps by using MAM allows full control over app delivery and over the app itself. Delivering the apps through MAM is more suitable usually.

- **Application maintenance:**

  - Perform an initial audit: Track the app version 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. This app version is the fall-back in case an unexpected issue occurs after the upgrade. Also develop a rollback plan. Test app upgrades in a test environment before your production deployment. 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.
  - Devise a strategy to notify users: Define a strategy to notify users when app upgrades are

available. Prepare users with training before deployment. You can send multiple notifications before updating the apps. Depending on the app, the best notification method might be email notifications or websites.

App lifecycle management represents the completed 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.

Application lifecycle Example using Secure Mail

1. Requirements for specifications: As a security requirement, you require a mail app that is containerized and supports MDX security policies.
2. Development: Validate that the app meets business needs. You must be able to apply MDX policy controls to the app.
3. Testing: Assign Secure Mail to a test users group and deploy the corresponding MDX file from the XenMobile Server. The test users validate that they can successfully send and receive email, and have calendar and contact access. The test users also report issues and identify bugs. Based on the test users' feedback you optimize the Secure Mail configuration for production use.
4. Deployment: When the testing phase is complete, you assign Secure Mail to production users and deploy the corresponding MDX file from XenMobile.
5. Maintenance: A new update to Secure Mail is available. You download the new MDX file from Citrix downloads and replace the existing MDX file on the XenMobile Server. Instruct the users to perform the update. Note: Citrix recommends that you complete and test this process in a test environment. Then, upload the app to a XenMobile production environment and deploy the app to users.

For more information, see Wrapping iOS Mobile Apps and Wrapping Android Mobile Apps.

Dashboard-Based Operations

January 6, 2021

You can view information at a glance by accessing your XenMobile 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 XenMobile 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 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 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. XenMobile 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.

> **Important:**
>
> Although it is possible to use SQL Server to create custom reports, Citrix does not recommend this method. Using the SQL Server database in this manner may have unforeseen consequences in your XenMobile deployment. If you do decide to pursue this method of reporting, ensure that SQL queries are run using a read-only account.

Role-Based Access Control and XenMobile Support

March 18, 2021

XenMobile uses role-based access control (RBAC) to restrict user and group access to XenMobile system functions, such as the XenMobile console, Remote Support, and public API. This article describes the roles built in to XenMobile and includes considerations for deciding on a support model for XenMobile that leverages RBAC.

> **Note:**
>
> Remote Support is no longer available for new customers as of January 1, 2019. Existing customers can continue to use the product, however Citrix won't provide enhancements or fixes.

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 from the XenMobile documentation. For a definition of each feature, see Configure roles with RBAC in the XenMobile documentation.

Admin role

Default access granted:

- Full system access except to Remote Support.
- 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 Remote Support? 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.

Device Provisioning

Default access granted:

- Access to the XenMobile console to perform basic administration on Windows CE devices: add, change, and remove devices; use the Settings page.

Considerations:

- Applies only to Windows CE devices.

Support

Default access granted:

- Access to Remote Support.

Considerations:

- For on-premises XenMobile Server deployments: Remote support enables your help desk representatives to take remote control of managed Windows CE and Android mobile devices. Screen cast is supported on Samsung KNOX devices only.
- Remote support isn't available for clustered on-premises XenMobile Server deployments.

User

Default access granted:

- Restricted access to the XenMobile 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 XenMobile 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 XenMobile 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 XenMobile 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 XenMobile-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 XenMobile Self-Help Portal?
Use **Settings > Enrollment** to enable the Self-Help Portal for an enrollment security mode. From the Self-Help Portal users can generate enrollment links that let them enroll their devices or send themselves an enrollment invitation. See To configure enrollment security modes.

Systems Monitoring

July 7, 2020

To ensure optimal uptime for app access and connectivity, you should monitor the following core components in the XenMobile environment.

XenMobile server

XenMobile server generates and stores logs on local storage that you can also export to a systems log (syslogs) server. You can configure log settings to specify size constraints, log level, or you can create custom loggers to filter specific events. You can look at XenMobile server logs from the XenMobile console at any time. You can also export information in the logs via the syslog server to your production Splunk logging servers.

The following list describes the different types of log files available in XenMobile:

Debug log file: Contains debug level information about core web services of XenMobile, including error messages and server-related actions.

Message format:

```
<date> <timestamp> <loglevel> <class name (including the package)> - <id> <log message>
```

- where <id> is a unique identifier like sessionID.
- where <log message> is the message supplied by the application.

Admin audit log file: Contains audit information about activity on the XenMobile console.

> **Note:**
>
> The same format is used for both admin audit and user audit logs.

Message format:

With the exception of required Date and Timestamp values, all other attributes are optional. Optional fields are represented with " " in the message.

```
<date> <timestamp> "<username/id>""<sessionid>""<deviceid>""<clientip>" "<action>""<status>""<application name>""<app user id>""<user agent>""<details>"
```

The following table lists the available admin audit log events:

Admin Audit Log Messages for events	Status
Login	success/failure
Logout	success/failure
Get admin	success/failure
Update admin	success/failure
Get application	success/failure
Add application	success/failure

Admin Audit Log Messages for events	Status
Update application	success/failure
Delete application	success/failure
Bind application	success/failure
Unbind application	success/failure
Disable application	success/failure
Enable application	success/failure
Get category	success/failure
Add category	success/failure
Update category	success/failure
Delete category	success/failure
Add certificate	success/failure
Delete certificate	success/failure
Active certificate	success/failure
CSR certificate	success/failure
Export certificate	success/failure
Delete certificate chain	success/failure
Add certificate chain	success/failure
Get connector	success/failure
Add connector	success/failure
Delete connector	success/failure
Update connector	success/failure
Get device	success/failure
Lock device	success/failure
Unlock device	success/failure
Wipe device	success/failure
Unwipe device	success/failure
Delete device	success/failure
Get role	success/failure
Add role	success/failure

Admin Audit Log Messages for events	Status
Update role	success/failure
Delete role	success/failure
Bind role	success/failure
Unbind role	success/failure
Update config settings	success/failure
Update workflow email	success/failure
Add workflow	success/failure
Delete workflow	success/failure
Add Active Directory	success/failure
Update Active Directory	success/failure
Add masteruserlist	success/failure
Update masteruserlist	success/failure
Update DNS	success/failure
Update Network	success/failure
Update log server	success/failure
Transfer log from log server	success/failure
Update syslog	success/failure
Update receiver updates	success/failure
Update time server	success/failure
Update trust	success/failure
Add service record	success/failure
Update service record	success/failure
Update receiver email	success/failure
Upload patch	success/failure
Import snapshot	success/failure
Fetch app store app details	success/failure
Update MDM	success/failure
Delete MDM	success/failure
Add HDX	success/failure

Admin Audit Log Messages for events	Status
Update HDX	success/failure
Delete HDX	success/failure
Add Branding	success/failure
Delete Branding	success/failure
Update SSL offload	success/failure
Add account property	success/failure
Delete account property	success/failure
Update account property	success/failure
Add beacon	success/failure

User audit log file: Contains information related to the user activity from enrolled devices.

> **Note:**
>
> The same format is used for both user audit and admin audit logs.

Message format:

With the exception of required Date and Timestamp values, all other attributes are optional. Optional fields are represented with " " in the message. For example,

```
<date> <timestamp> "<username/id>""<sessionid>""<deviceid>""<clientip>"
"<action>""<status>""<application name>""<app user id>""<user agent>""<
details>"
```

The following table lists the available user audit log events:

User Audit Log Messages for events	Status
Login	success/failure
Session time-out	success/failure
Subscribe	success/failure
Unsubscribe	success/failure
Pre-launch	success/failure
AGEE SSO	success/failure
SAML Token for Citrix Files	success/failure

User Audit Log Messages for events	Status
Device registration	success/failure
Device check	lock/wipe
Device update	success/failure
Token refresh	success/failure
Secret saved	success/failure
Secret retrieved	success/failure
User initiated change password	success/failure
Mobile client download	success/failure
Logout	success/failure
Discovery Service	success/failure
Endpoint Service	success/failure

MDM Functions	Status
REGHIVE	success/failure
Cab inventory	success/failure
Cab	success/failure
Cab auto install	success/failure
Cab shell install	success/failure
Cab create folder	success/failure
Cab file get	success/failure
File create folder	success/failure
File get	success/failure
File sent	success/failure
Script create folder	success/failure
Script get	success/failure
Script sent	success/failure
Script shell execution	success/failure
Script auto execution	success/failure

MDM Functions	Status
APK inventory	success/failure
APK	success/failure
APK shell install	success/failure
APK auto install	success/failure
APK create folder	success/failure
APK file get	success/failure
APK App	success/failure
EXT App	success/failure
List get	success/failure
List sent	success/failure
Locate device	success/failure
CFG	success/failure
Unlock	success/failure
SharePoint wipe	success/failure
SharePoint Configuration	success/failure
Remove profile	success/failure
Remove application	success/failure
Remove unmanaged application	success/failure
Remove unmanaged profile	success/failure
IPA App	success/failure
EXT App	success/failure
Apply redemption code	success/failure
Apply settings	success/failure
Enable tracking device	success/failure
App management policy	success/failure
SD card wipe	success/failure
Encrypted email attachment	success/failure
Branding	success/failure
Secure browser	success/failure

MDM Functions	Status
Container browser	success/failure
Container unlock	success/failure
Container password reset	success/failure
AG client auth creds	success/failure

Citrix ADC also monitors the XenMobile web service state, which is configured with intelligent monitoring probes to simulate HTTP requests to each XenMobile server cluster node. The probes determine whether the service is online and then respond based on the response received. In the event that a node does not respond as expected, Citrix ADC marks the server as down. In addition, Citrix ADC takes the node out of the load-balancing pool and logs the event for use in generating alerts through the Citrix ADC monitoring solution.

You can also use standard hypervisor monitoring tools to monitor the XenMobile virtual machines and to provide relevant alerts regarding CPU, memory, and storage utilization metrics.

SQL Server and database

SQL Server and database performance directly affects XenMobile services. The XenMobile instance requires access to the database at all times and goes offline (for example, stops responding) in the event of an outage to the SQL infrastructure. The XenMobile console may continue to function for a while following any disk space issues with SQL Server. To ensure maximum database uptime and adequate performance for the XenMobile workload, you should proactively monitor the state of your SQL Servers. For more information on monitoring your SQL Servers, see Monitoring and Tuning for Performance Overview. Additionally, you should adjust resource allocation for CPU, memory, and storage to guarantee service level agreements as your XenMobile environment continues to grow.

Citrix ADC

Citrix ADC provides the ability to log metrics to internal storage or to send logs to an external logging server. You can configure the syslog server to export Citrix ADC logs to your production Splunk logging servers. The following logging levels are available in Citrix ADC:

- Emergency
- Alert
- Critical
- Error
- Warning

- Information

The log files are also stored in Citrix ADC storage in the /var/log/ns.log directory and named newnslog. Citrix ADC rolls over and compresses the files by using the GZIP algorithm. Log file names are newnslog.xx.gz, where xx represents a running number.

Citrix ADC also supports SNMP traps and alerts as a monitoring option. For a list of SNMP traps, see SNMP monitoring.

Disaster Recovery

March 25, 2020

You can architect and configure XenMobile deployments that include multiple sites for disaster recovery using an active-passive failover strategy.

The recommended disaster recovery strategy discuss in this article consists of:

- A single XenMobile active site in the datacenter of one geographical location serving all the enterprises users globally, known as the primary site.
- A second XenMobile site in the datacenter of a second geographical location, known as the disaster recovery site. This disaster recovery site provides active-passive site failover in if a site-wide datacenter failure occurs in the primary site. The primary site includes XenMobile, SQL database, Citrix ADC infrastructure in order to facilitate failover and provide users with access to XenMobile via the event of connectivity failure to the primary site.

The XenMobile servers at the disaster recovery site remains offline during normal operations and is brought online during only disaster recovery scenarios, where complete site failover from the primary site to the disaster recovery site is required. The SQL Servers at the disaster recovery site must be active and ready to service connections before you start the XenMobile servers at the disaster recovery site.

This disaster recovery strategy relies on manual failover of the Citrix ADC access tier by means of DNS changes for routing MDM and MAM connections to the disaster recovery site in the event of an outage.

> **Note:**
>
> To use this architecture, you must have a process in place for asynchronous backups of the databases and some way of ensuring high availability for the SQL infrastructure.

Disaster Recovery Failover Process

1. If you are testing your disaster recovery failover process, shut down XenMobile servers in the primary site to simulate site failure.

2. Change public DNS records for the XenMobile servers to point to the disaster recovery site's external IP addresses.
3. Change internal DNS record for the SQL Server to point to the disaster recovery site's SQL Server IP address.
4. Bring XenMobile SQL databases online at the disaster recovery site. Ensure that the SQL Server and database is active and ready to service connections from the XenMobile servers local to the site.
5. Turn on the XenMobile servers on the disaster recovery site.

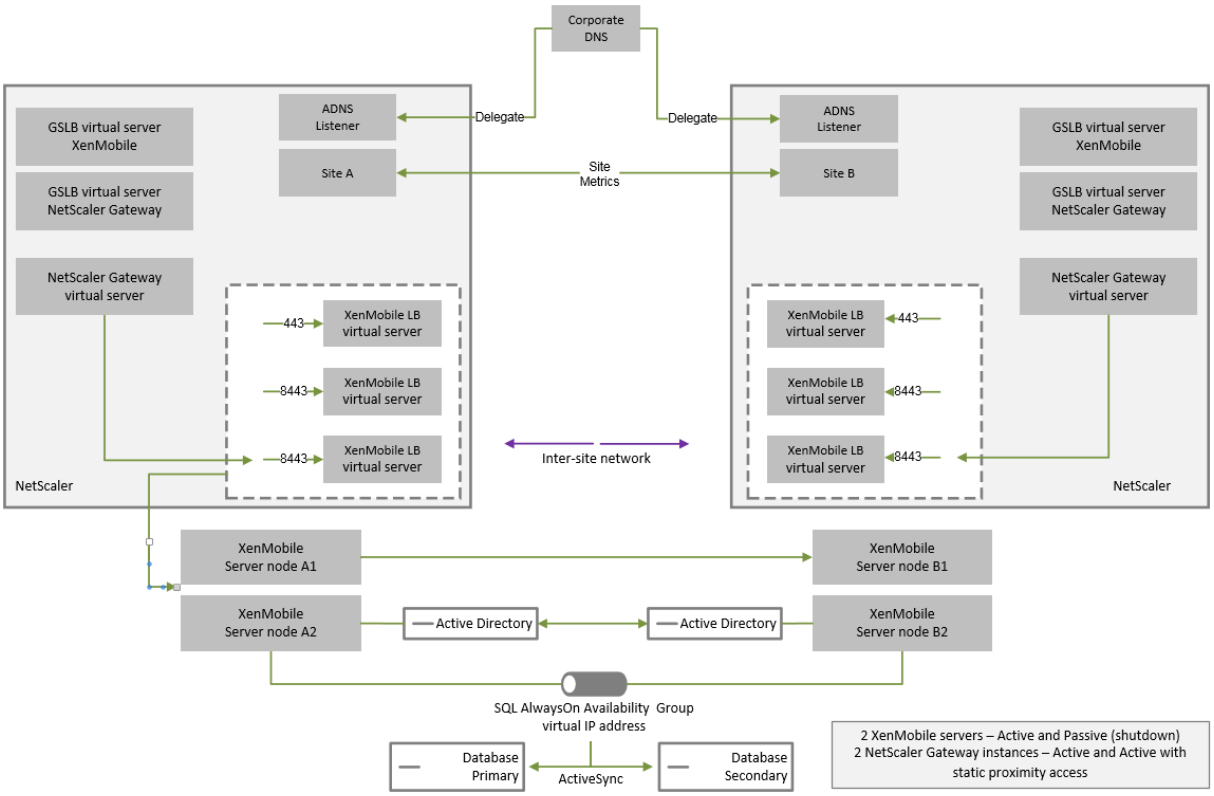
XenMobile Server Update Process

Follow these steps any time you update XenMobile with patches and releases, in order to keep the code of the primary and disaster recovery servers uniform.

1. Ensure that XenMobile servers in primary site have been patched or upgraded.
2. Ensure that DNS record for the SQL Server is resolving to the active SQL Server database in the primary site.
3. Bring the disaster recovery site's XenMobile servers online. The servers connect to the primary site's database across the WAN during the upgrade process only.
4. Apply required patches and updates to all disaster recovery site's XenMobile servers.
5. Restart the XenMobile servers and confirm that the patch or upgrade is successful.

Disaster Recovery Reference Architecture Diagram

The following diagram shows the high-level architecture for a disaster recovery deployment of XenMobile.



GSLB for Disaster Recovery

A key element of this architecture is the use of Global Server Load Balancing (GSLB) to direct traffic to the correct data center.

By default, the Citrix ADC for XenMobile wizard configures Citrix Gateway in a way that does not enable the use of GSLB for disaster recovery. Therefore, you must take additional steps.

How GSLB Works

GSLB is at its core a form of DNS. Participating Citrix ADC appliances act as authoritative DNS servers and resolve DNS records to the correct IP address (typically the VIP that is supposed to receive traffic). The Citrix ADC appliance checks the system health before responding to a DNS query directing traffic to that system.

When a record is resolved, GSLB's role in resolving the traffic is complete. The client communicates directly with the target virtual IP (VIP) address. DNS client behavior plays an important part on controlling how and when a record expires. This is largely outside the boundaries of the Citrix ADC system. As such, GSLB is subject to the same limitations as DNS name resolution. Clients cache responses; thus, load balancing in this way isn't as real-time as is traditional load balancing.

The GSLB configuration on Citrix ADC, including sites, services, and monitors, exist in order to provide the correct DNS name resolution.

The actual configuration for publishing servers (in this scenario, the configuration that the Citrix ADC for XenMobile wizard creates) is not affected by the GSLB. GSLB is a separate service on the Citrix ADC.

Challenges with Domain Delegation When Using GSLB with XenMobile

The Citrix ADC for XenMobile wizard configures Citrix Gateway for XenMobile. This wizard generates three load balancing virtual servers and a Citrix Gateway virtual server.

Two of the load balancing virtual servers handle MDM traffic, on port 443 and 8443. Citrix Gateway receives MAM traffic and forwards it to the third server, the MAM load balancing virtual server, on port 8443. All traffic to the MAM load balancing virtual server is passed through Citrix Gateway.

The MAM load balancing virtual server requires the same SSL certificate as the XenMobile servers and uses the same FQDN as used to enroll devices. The MAM load balancing server also uses the same port (8443) as one of the MDM load balancing servers. To enable traffic to be resolved, the Citrix ADC for XenMobile wizard creates a local DNS record on Citrix Gateway. The DNS record matches the FQDN used to enroll devices.

This configuration is effective when the XenMobile server URL is not a GSLB domain URL. If a GSLB domain URL is used as the XenMobile server URL, as is required for disaster recovery, the local DNS record prevents Citrix Gateway from resolving traffic to the MDM load balancing servers.

Using the CNAME Method for GSLB Disaster Recovery

To address the challenges presented by the default configuration created by the Citrix ADC for XenMobile wizard, you can create a CNAME record for the XenMobile server FQDN in the parent domain (`company.com`) and point a record in the delegated subzone (`gslb.company.com`) for which Citrix ADC is authoritative. Doing so allows for the creation of the static DNS A record for the MAM load balancing VIP address required to resolve traffic.

1. On the external DNS, create a CNAME for the XenMobile server FQDN that points to the GSLB domain FQDN on Citrix ADC GSLB. You need two GSLB domains: One for MDM traffic and another for MAM (Citrix Gateway) traffic.

   Example:

   ```
   CNAME = xms.company.com IN CNAME xms.gslb.comany.com
   ```

2. On the Citrix Gateway instance of each site, create a GSLB virtual server with a FQDN that is what the CNAME record is pointing to.

   Example:


```
bind gslb vserver xms-gslb -domainName xms.gslb.company.com
```

When using the Citrix ADC for XenMobile wizard to deploy Citrix Gatway, use the XenMobile server URL when configuring the MAM load balancing server. This creates a static DNS A record for the XenMobile server URL.

3. Test with clients enrolling on Secure Hub using the XenMobile server URL (`xms.company.com`).

   This example uses the following FQDNs:

   - `xms.company.com` is the URL that is used by the MDM traffic and is used by devices enrolling, which is configured in this example by using the Citrix ADC for XenMobile wizard.
   - `xms.gslb.company.com` is the GSLB domain FQDN for the XenMobile server.

Citrix Support Process

January 13, 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 XenMobile, 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. For information on contacting support for XenMobile issues, see How to Contact Support.

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 XenMobile

March 18, 2021

Contributed by John Bartel III

You can send enrollment invitations to groups and nested groups in XenMobile Server. Enrollment invitations aren't available for Android Enterprise and 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 XenMobile 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 authentication security that you prefer for users.

   - User name + Password
   - High Security
   - Invitation URL
   - Invitation URL + PIN
   - Invitation URL + Password
   - Two Factor
   - User name + PIN

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.

   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 Notifications.

   For these notification templates, use your configured SMTP server setup within XenMobile. 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, XenMobile 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 group.

Configuring an on-premises Device Health Attestation server

April 9, 2020

Contributed by Sanket Mishra

You can enable Device Health Attestation (DHA) for Windows 10 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 a XenMobile Server policy to enable the on-premises DHA service. For information on creating this policy, see Device Health Attestation device policy.

Prerequisites for a DHA server

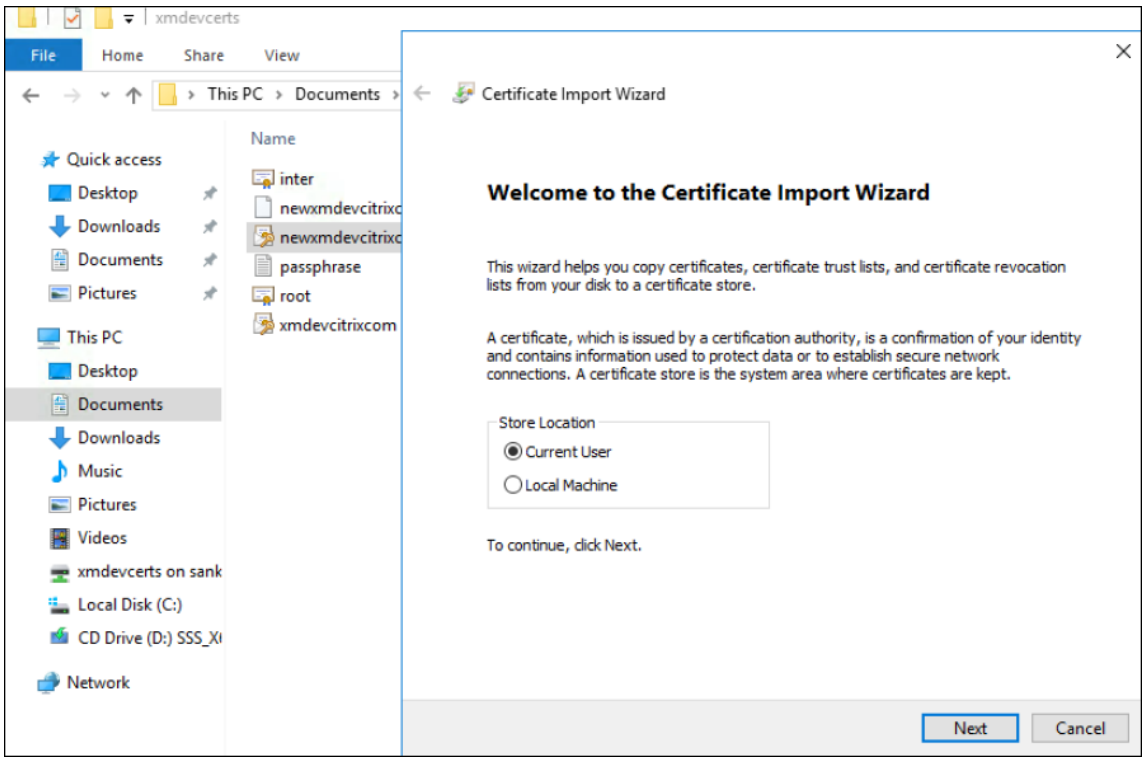
- A server running Windows Server Technical Preview 5 or later, installed using the Desktop Experience installation option.
- One or more Windows 10 client devices. These devices must be have TPM 1.2 or 2.0 running the latest version of Windows.
- These certificates:
  - **DHA SSL certificate.** An x.509 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) and server to client (DHA service and a Windows 10 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

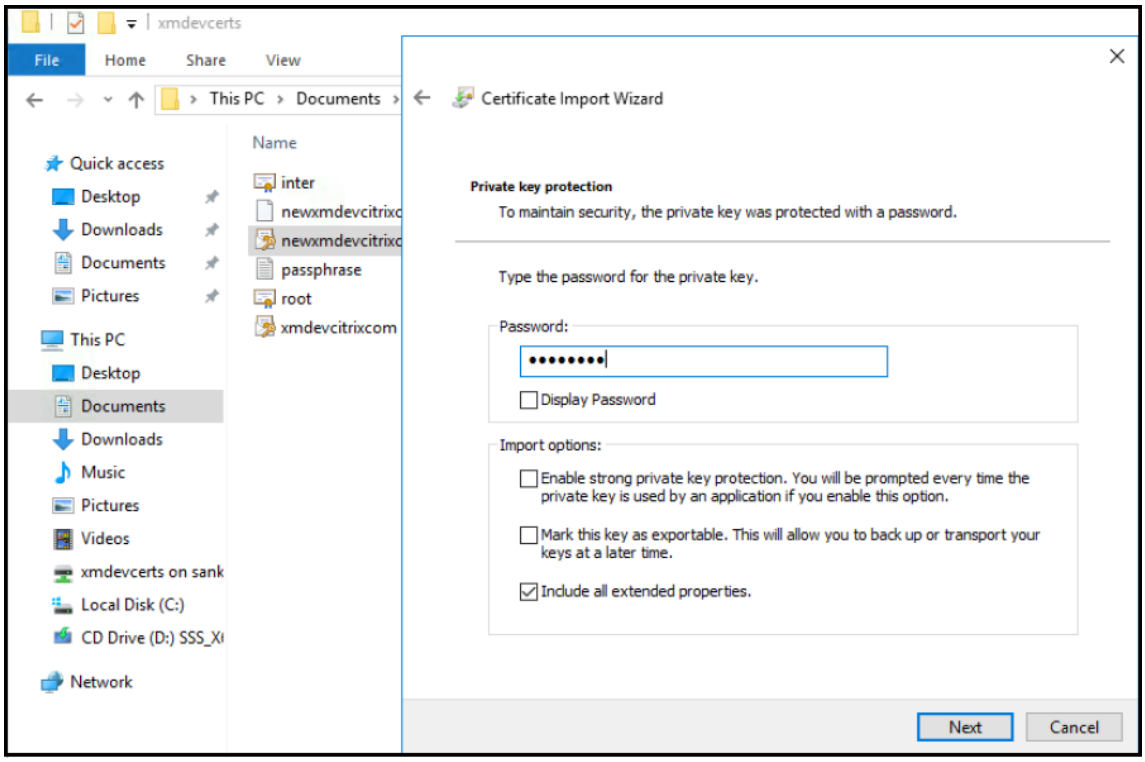
1. On the Windows server, if the Server Manager is not already open, click **Start** and then click **Server Manager**.
2. Click **Add roles and features**.
3. On the **Before you begin** page, click **Next**.
4. On the **Select installation type** page, click **Role-based or feature-based installation**, 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 role**s 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 feature**s 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

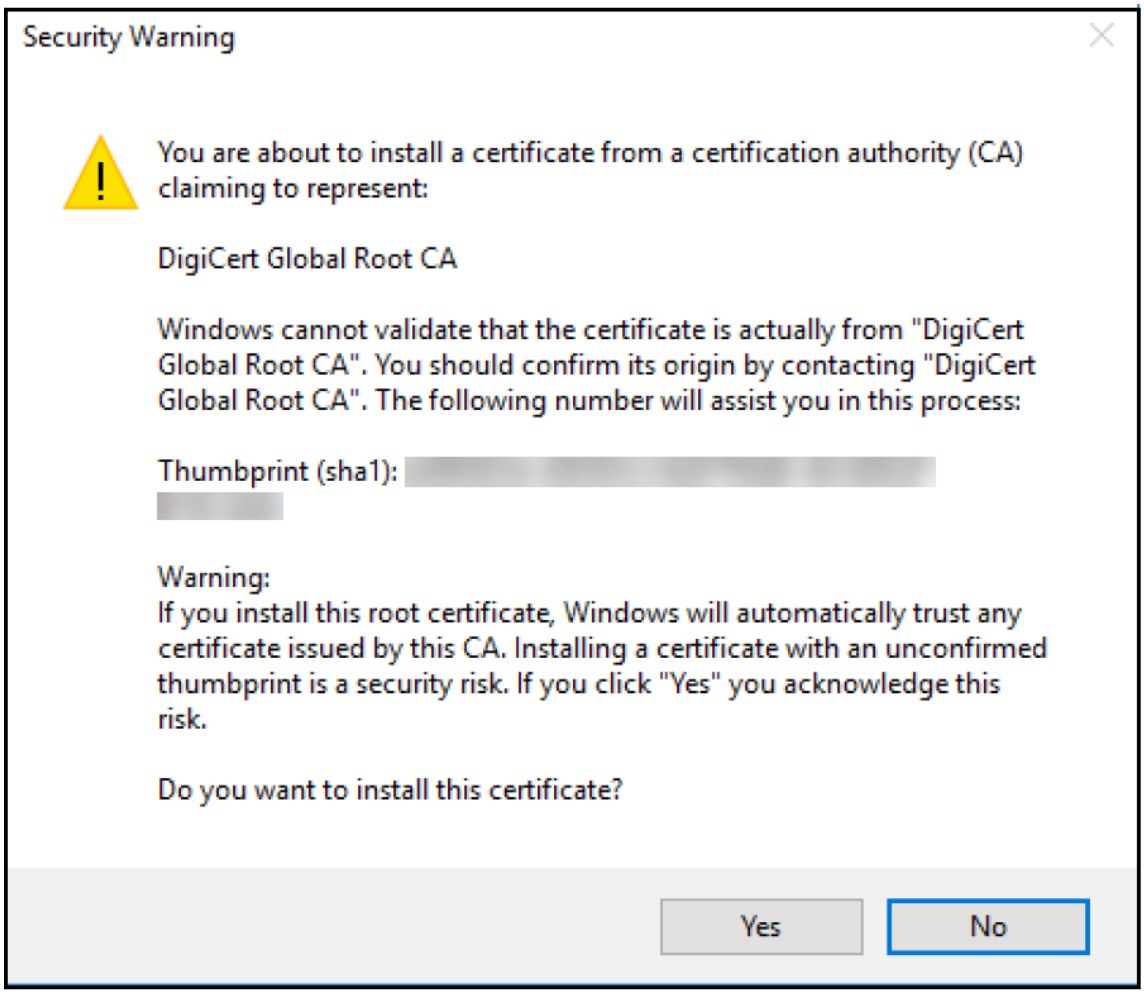
1. Go to the SSL certificate file and select it.
2. Select **Current user** as the store location and click **Next**.



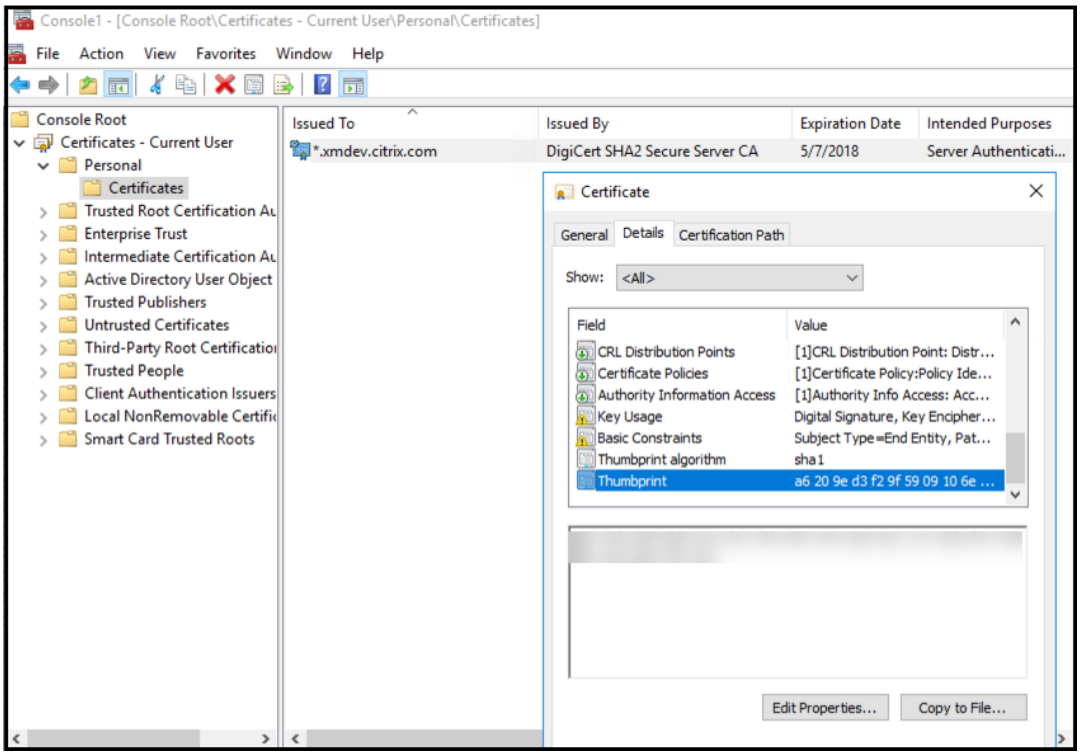
3. Type the password for the private key.
4. Ensure the import option **Include all extended properties** is selected. Click **Next**.



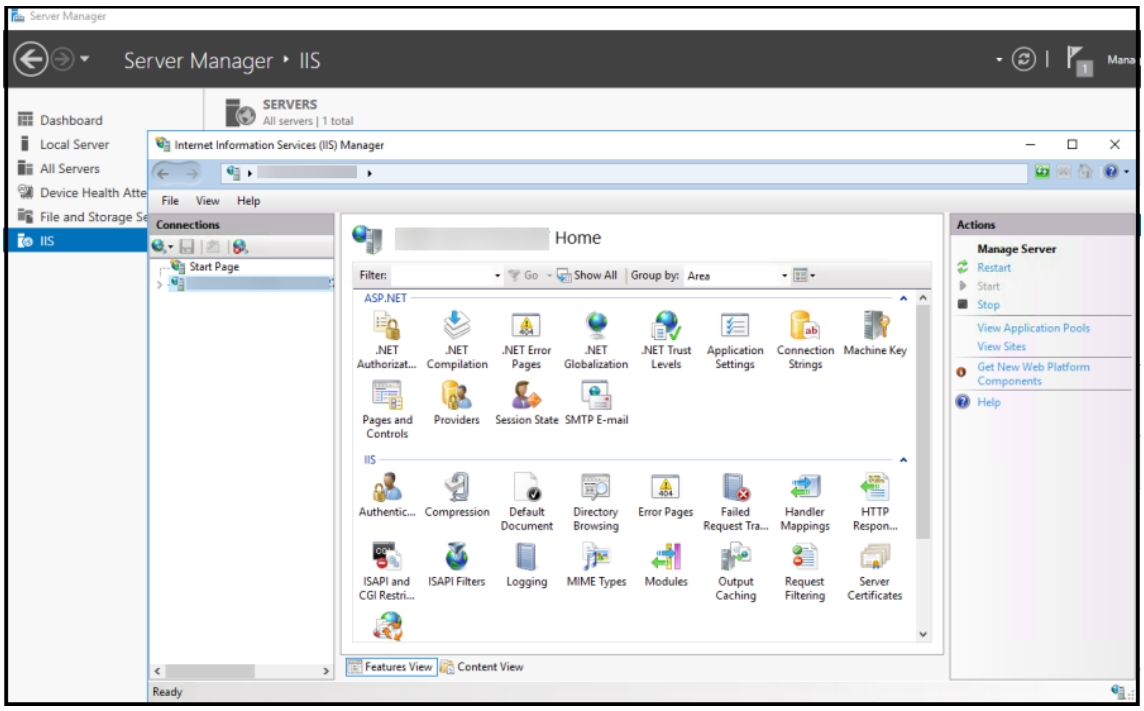
5. When this window appears, click **Yes**.



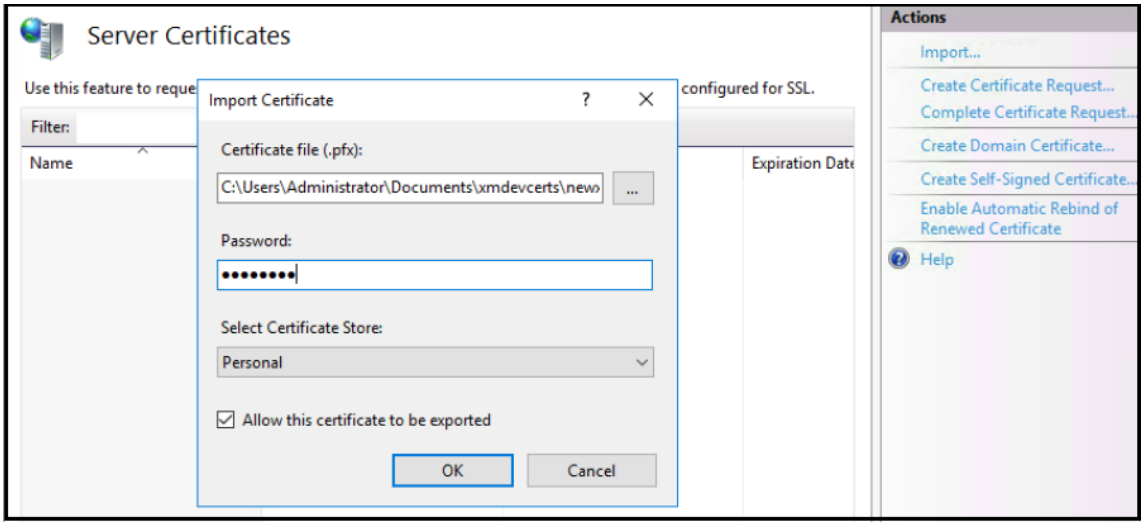
6. Confirm that the certificate is installed:
    a) Open a Command Prompt window.
    b) Type **mmc** and press the Enter key. To view certificates in the local machine store, you must be in the Administrator role.
    c) On the File menu, click **Add/Remove Snap In**.
    d) Click **Add**.
    e) In 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.

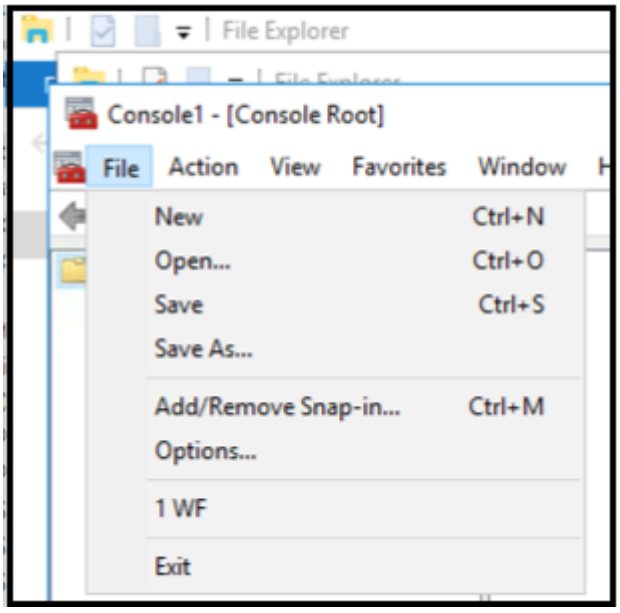


8. From the Action menu, select **Import...** to import the SSL certificate.

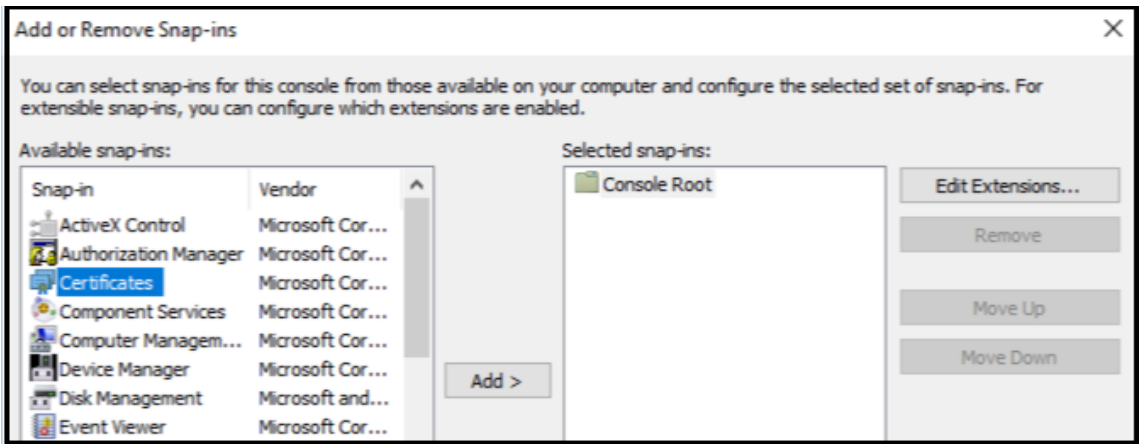


Retrieve and save the thumbprint of the certificate

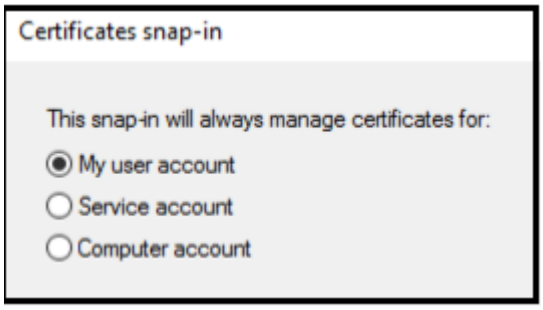
1. In the File Explorer search bar, type **mmc**.
2. In the Console Root window, click **File > Add/Remove Snap-in...**.



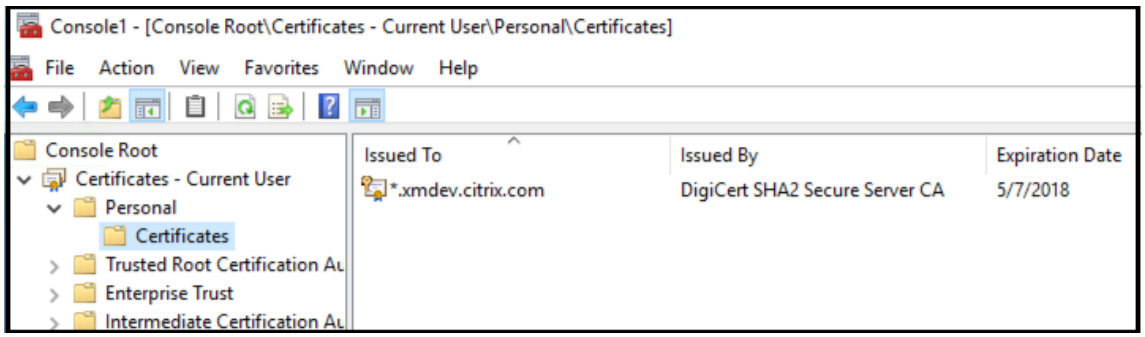
3. Select the certificate from available snap-in and add it to selected snap-ins.



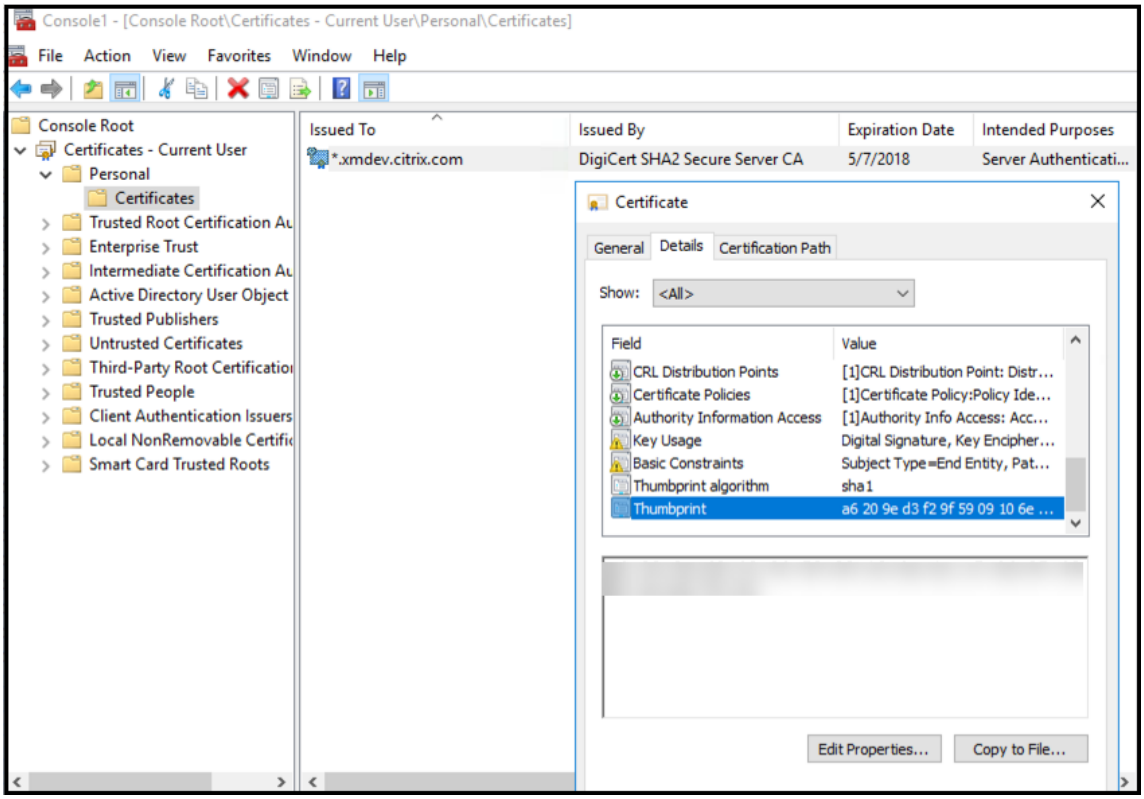
4. Select **My user account**.



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.



7. 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.

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
 $_.Thumbprint -like "ReplaceWithThumbprint" }


$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys\" +
   $keyname icacls $keypath /grant IIS_IUSRS`:R
<!--NeedCopy-->
```


Extract the TPM roots certificate and install the trusted certificate package

Run these commands on the Windows server:

```
mkdir .\TrustedTpm

expand -F:\* .\TrustedTpm.cab .\TrustedTpm

cd .\TrustedTpm

.\setup.cmd
<!--NeedCopy-->
```

Configure the DHA service

Run this command on the Windows server to configure the DHA service.

Replace the placeholder ReplaceWithThumbprint.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
    ReplaceWithThumbprint

-SigningCertificateThumbprint ReplaceWithThumbprint

-SslCertificateStoreName My -SslCertificateThumbprint
    ReplaceWithThumbprint

-SupportedAuthenticationSchema "AikCertificate"
<!--NeedCopy-->
```

Run these commands on the Windows server to set up the certificate chain policy for the DHA service:

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
<!--NeedCopy-->
```

Respond to these prompts, as follows:

```
  Confirm

    Are you sure you want to perform this action?

```



```
    Performing the operation "Install-DeviceHealthAttestation" on
       target "WIN-N27D1FKCEBT".

    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?]
       Help (default is "Y"): A

    Adding SSL binding to website 'Default Web Site'.

    Add SSL binding?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.

    Add application pool?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding web application 'DeviceHealthAttestation' to website '
       Default Web Site'.

    Add web application?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding firewall rule 'Device Health Attestation Service' to allow
       inbound connections on port(s) '443'.

    Add firewall rule?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Setting initial configuration for Device Health Attestation Service
       .

    Set initial configuration?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Registering User Access Logging.

    Register User Access Logging?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
<!--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>/DeviceHeathAttestation/ValidateHealthCertificate
/v1
```

If the DHA service is running, “Method not allowed” appears.

Configuring certificate-based authentication with EWS for Secure Mail push notifications

April 9, 2020

Contributed by Vijay Kumar Kunchakuri

To make sure that Secure Mail push notifications work, you must configure Exchange Server for certificate-based authentication. This requirement is especially necessary when Secure Hub is enrolled in XenMobile with certificate-based authentication.

You need to configure the Active Sync and Exchange Web Services (EWS) virtual directory on the Exchange Mail Server with certificate-based authentication.

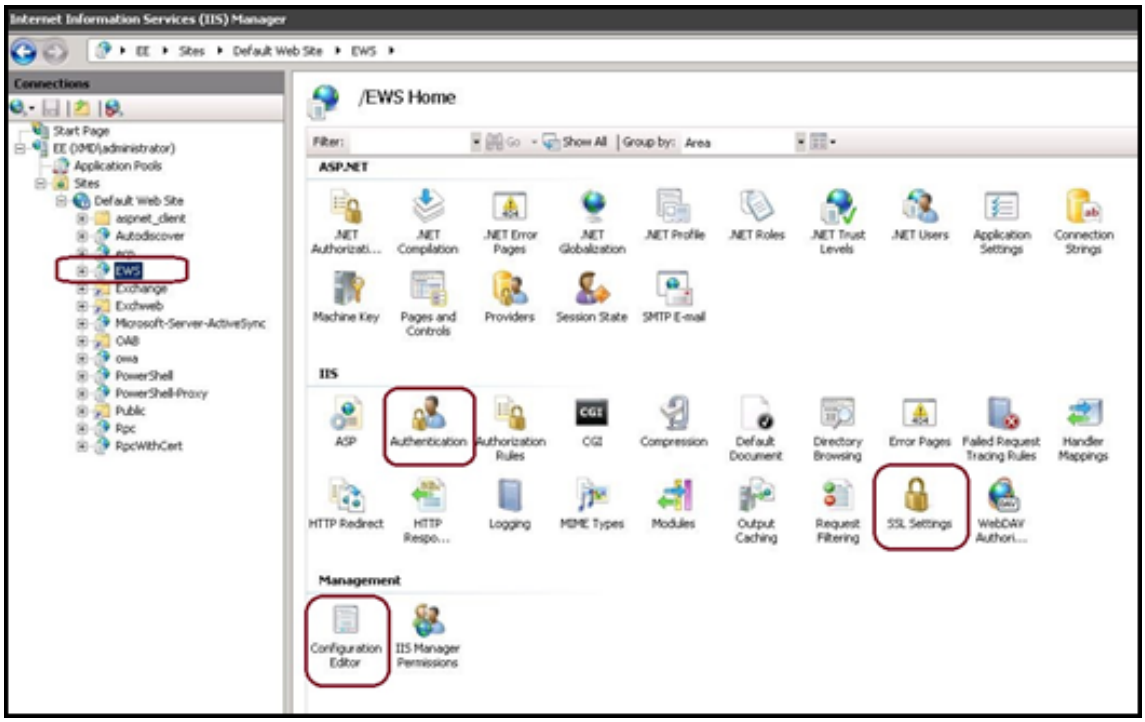
Unless you complete these configurations, the subscription to Secure Mail push notifications fails and no badge updates occur in Secure Mail.

This article describes the steps to configure certificate-based authentication. The configurations are specifically against the EWS virtual directory on Exchange Server.

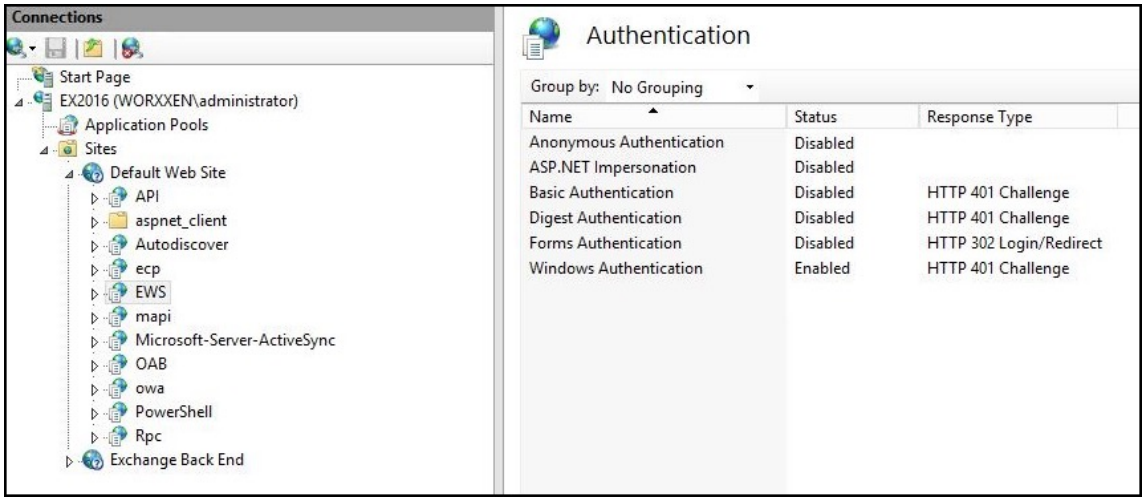
To get started with the configuration, do the following:

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



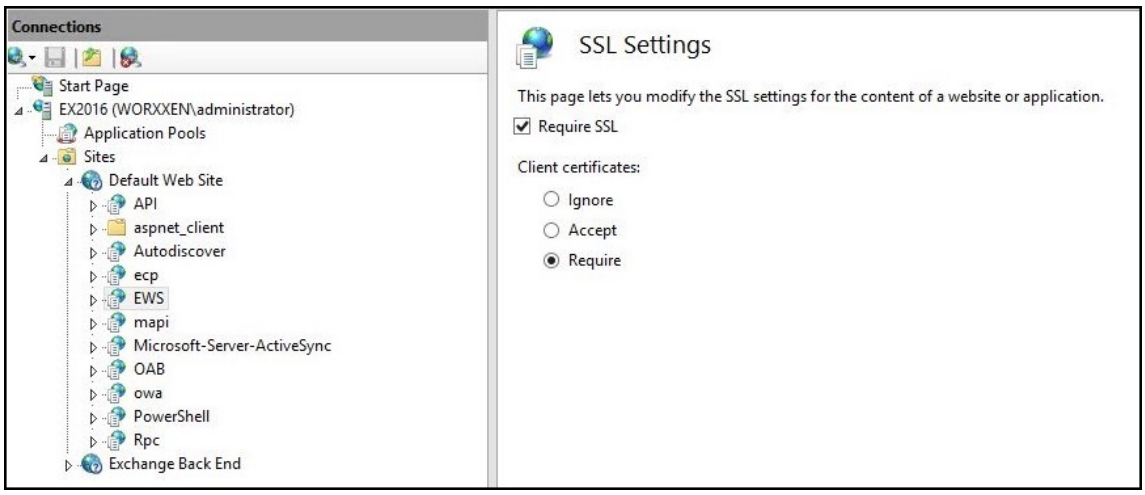
4. Ensure that the **Authentication** settings for EWS are configured as shown in the following figure.



5. Configure the **SSL Settings** for the EWS virtual directory.

   a) Select the **Require SSL** check box.

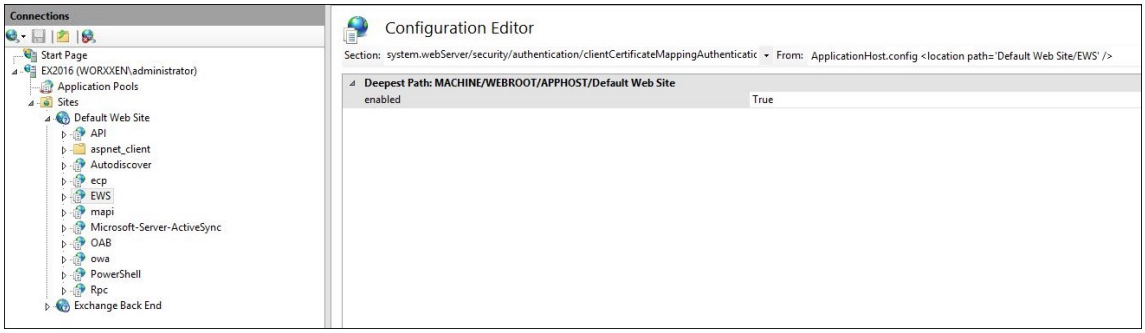
   b) Under **Client Certificates**, click **Require.** You can set this option to **Accept** if other EWS mail clients connect with username and password as credentials to authenticate and connect to the Exchange Server.



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**.

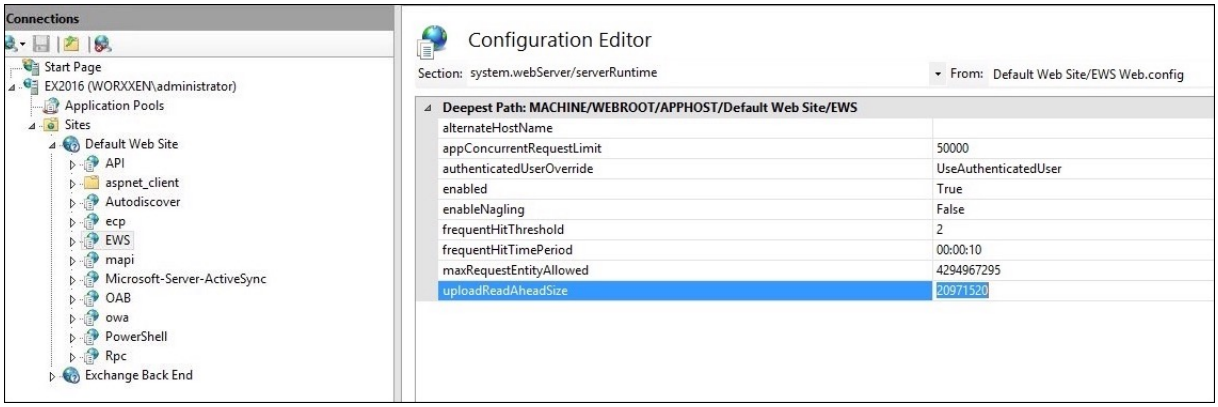


8. Click **Configuration Editor** and in the **Section** drop-down list, navigate to the following section:
   - **system.webServer/serverRuntime**
9. Set the **uploadReadAheadSize** value to **10485760** (10 MB) or **20971520** (20 MB) or to a value as required by your organization.

   > **Important:**
   >
   > If you don't set this value correctly, certificate-based authentication while subscribing to EWS push notifications may fail with an error code of 413.
   >
   > Do not set this value to **0.**

For more information, see the following third-party resources:

- Microsoft IIS server runtime
- Butsch Client Management Blog



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

Integrate XenMobile Mobile Device Management (MDM) with Cisco Identity Services Engine (ISE)

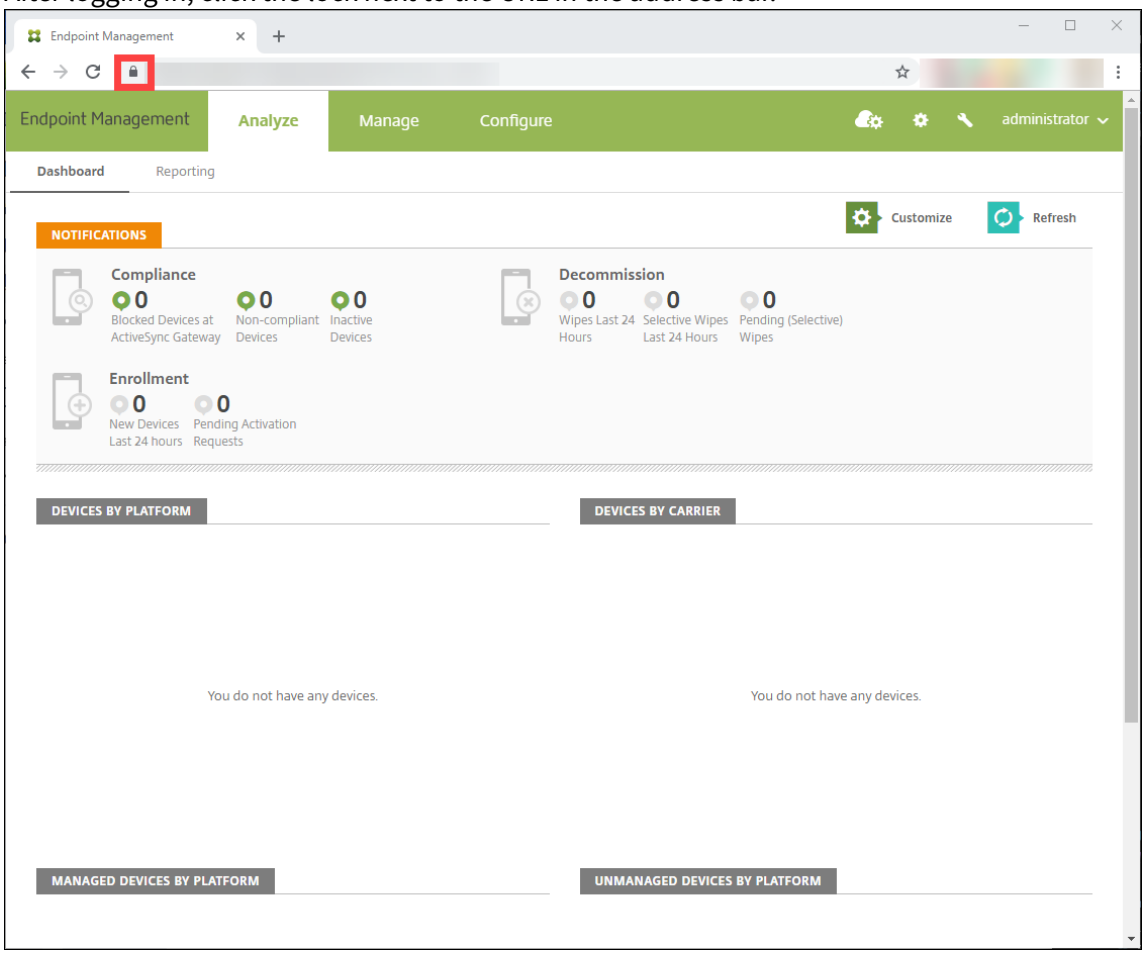
July 9, 2020

Contributed by John Bartel III

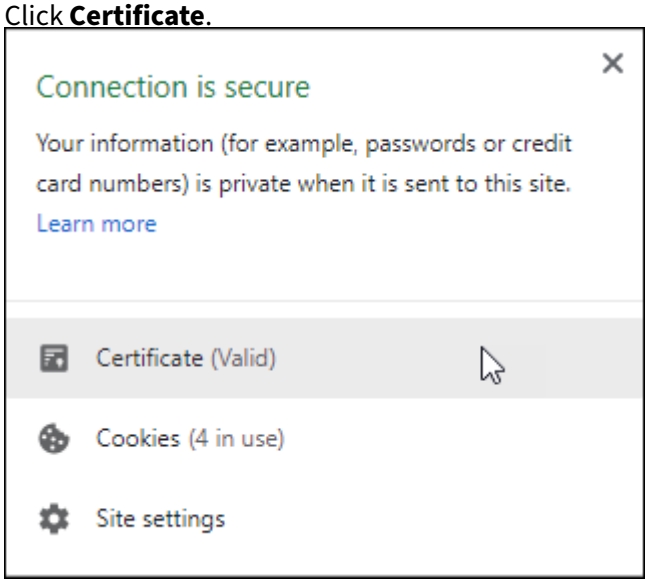
Cisco ISE is used to deploy, secure, monitor, integrate, and manage mobile devices in the workplace. The software downloaded to the mobile device controls the distribution of applications and patches and control data and configuration on the endpoint. XenMobile can integrate with Cisco ISE to manage non-compliant and unmanaged devices on the Cisco ISE console. XenMobile also allows you to selectively allow, deny, or quarantine access to corporate services.

To set up the integration with XenMobile, create a local service account on the XenMobile Server with the administrator RBAC role assigned to it. This role allows the Cisco ISE to access the XenMobile API. ISE needs to trust the XenMobile certificate. To download this certificate, open a web browser and navigate to your server URL and log in.

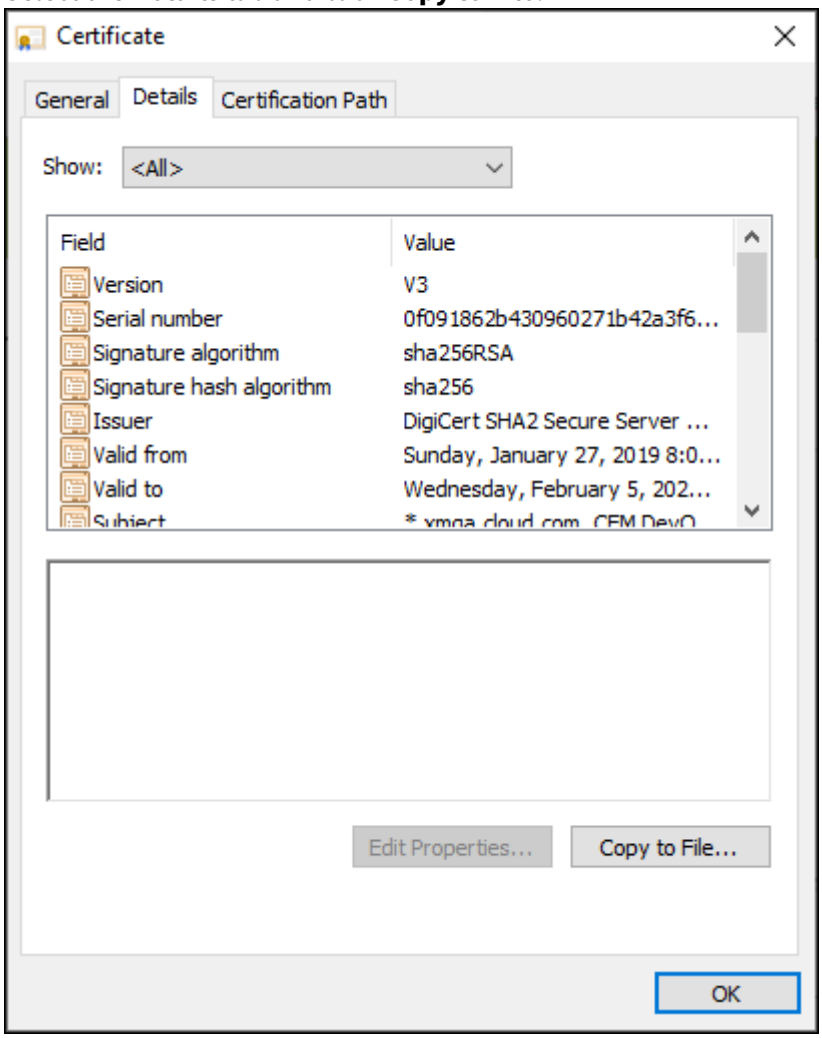
1. After logging in, click the lock next to the URL in the address bar.



2. Click **Certificate**.



3. Select the **Details** tab and click **Copy to File**.



4. Follow the wizard to save the certificate locally.

5. Log in to your Cisco ISE console and import the XenMobile certificate you previously downloaded. Import the certificate into Cisco ISE's Trusted Certificate store. This import is necessary for Cisco ISE to trust communication with the XenMobile Server.
   a) Navigate to **Administration > System > Certificates > Certificate Management > Trusted Certificates**. Click **Import**.
   b) Give the certificate a name and check the boxes for **Trust for authentication within ISE** and **Trust for authentication of Cisco Services**.
6. Add XenMobile as an external MDM inside Cisco ISE.
   a) Navigate to **Administration > Network Resource > External MDM**. Clicking **Add** and fill out the following:
      - **Server Host:** Your XenMobile FQDN
      - **Port:** 443
      - **Instance name:** The instance name of your XenMobile Server. The instance name is "zdm" by default on most deployments.
      - **User Name:** Type the name of the user you created for this task. The user should be a local administrator account in the origial admin RBAC group.
      - **Password:** The password for the user you just added.
      - Check where it says **Enable**.
7. If the test is successful, click **Submit**.

For more information about Cisco ISE, see Cisco documentation.

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