Secure Hub

Contents

Citrix Secure Hub 3

Known and fixed issues 30

Authentication prompt scenarios 32

Enrolling devices by using derived credentials 36

Citrix Secure Hub

November 10, 2021

Citrix Secure Hub is the launchpad for the mobile productivity apps. Users enroll their devices in Secure Hub to gain access to the app store. From the app store, they can add Citrix-developed mobile productivity apps and third-party apps.

You can download Secure Hub and other components from the Citrix Endpoint Management downloads page.

For Secure Hub and other system requirements for the mobile productivity apps, see System requirements.

For latest information on mobile productivity apps, see the article Recent announcements.

The following sections list the new features in current and earlier releases of Secure Hub.

> **Note:**
>
> Support ended for the Android 6.x and iOS 11.x versions of Secure Hub, Secure Mail, Secure Web, and Citrix Workspace app in June 2020.

What's new in the current version

Secure Hub 21.11.0

Secure Hub for Android

This release includes bug fixes.

What's new in earlier versions

Secure Hub 21.10.0

Secure Hub for iOS

This release includes bug fixes.

Secure Hub for Android

Support for Android 12. From this release onward, Secure Hub is supported on devices running Android 12.

Secure Hub 21.8.0

Secure Hub for iOS

This release includes bug fixes.

Secure Hub 21.7.1

Secure Hub for Android

Support for Android 12 on already enrolled devices. If you are considering upgrading to Android 12, ensure that you update Secure Hub to version 21.7.1 first. Secure Hub 21.7.1 is the minimum version required to upgrade to Android 12. This release ensures a seamless upgrade from Android 11 to Android 12 for already enrolled users.

> **Note:**
>
> If Secure Hub is not updated to version 21.7.1 before you upgrade to Android 12, your device might require a re-enrollment or a factory reset to recover prior functionality.
>
> Citrix is committed to providing Day 1 support for Android 12 and will add further updates to subsequent versions of Secure Hub to fully support Android 12.

Secure Hub 21.7.0

Secure Hub for iOS

This release includes bug fixes.

Secure Hub for Android

This release includes bug fixes.

Secure Hub 21.6.0

Secure Hub for iOS

This release includes bug fixes.

Secure Hub for Android

This release includes bug fixes.

Secure Hub 21.5.1

Secure Hub for iOS

This release includes bug fixes.

Secure Hub for Android

This release includes bug fixes.

Secure Hub 21.5.0

Secure Hub for iOS

With this release, apps wrapped with MDX Toolkit version 19.8.0 or earlier will no longer work. Ensure that you wrap your apps with the latest MDX Toolkit to resume proper functionality.

Secure Hub 21.4.0

Color revamp for Secure Hub. Secure Hub is compliant with Citrix brand color updates.

Secure Hub 21.3.2

Secure Hub for iOS

This release includes bug fixes.

Secure Hub 21.3.0

This release includes bug fixes.

Secure Hub 21.2.0

Secure Hub for Android

This release includes bug fixes.

Secure Hub 21.1.0

This release includes bug fixes.

Secure Hub 20.12.0

Secure Hub for iOS

This release includes bug fixes.

Secure Hub for Android

Secure Hub for Android supports Direct Boot mode. For more information about Direct Boot mode, see the Android documentation at *Developer.android.com.*

Secure Hub 20.11.0

Secure Hub for Android

Secure Hub supports Google Play's current target API requirements for Android 10.

Secure Hub 20.10.5

This release includes bug fixes.

Secure Hub 20.9.0

Secure Hub for iOS

Secure Hub for iOS supports iOS 14.

Secure Hub for Android

This release includes bug fixes.

Secure Hub 20.7.5

Secure Hub for Android

- Secure Hub for Android supports Android 11.
- **Transition from Secure Hub 32-bit to 64-bit for apps**. In Secure Hub version 20.7.5, support ends for 32-bit architecture for apps, and Secure Hub has been updated to 64-bit. Citrix recommends customers to upgrade to version 20.7.5 from 20.6.5. If users skip the upgrade to Secure Hub version 20.6.5, and instead update from 20.1.5 to 20.7.5 directly, they must reauthenticate. Reauthentication involves entering credentials and resetting the Secure Hub PIN. Secure Hub version 20.6.5 is available in the Google Play Store.

- **Install updates from the App Store.** In Secure Hub for Android, if there are updates available for apps, the app is highlighted and the **Updates available** feature appears on the App Store screen.

  When you tap **Updates available**, you navigate to the store that shows the list of apps with pending updates. Tap **Details** against the app to install the updates. When the app is updated, the down arrow in **Details** is changed to a check mark.

Secure Hub 20.6.5

Secure Hub for Android

Transition from 32-bit to 64-bit for apps. The Secure Hub 20.6.5 release is the final release that supports a 32-bit architecture for Android mobile apps. In subsequent releases, Secure Hub supports the 64-bit architecture. Citrix recommends that users upgrade to Secure Hub version 20.6.5, so that users can upgrade to later versions without reauthentication. If users skip the upgrade to Secure Hub version 20.6.5, and instead update to 20.7.5 directly, they need to reauthenticate. Reauthentication involves entering credentials and resetting the Secure Hub PIN.

> **Note:**
>
> The 20.6.5 release does not block the enrollment of devices running Android 10 in device administrator mode.

Secure Hub for iOS

Enable a proxy configured on iOS devices. Secure Hub for iOS requires that you enable a new client property, `ALLOW_CLIENTSIDE_PROXY`, if you want to allow users to use proxy servers that they configure in **Settings > Wi-Fi**. For more information, see `ALLOW_CLIENTSIDE_PROXY` in Client property reference.

Secure Hub 20.3.0

> **Note:**
>
> Support is ending for the Android 6.x and iOS 11.x versions of Secure Hub, Secure Mail, Secure Web, and Citrix Workspace app in June 2020.

Secure Hub for iOS

- **Network Extension disabled.** Due to recent changes on App Store Review Guidelines, from release 20.3.0 onward, Secure Hub does not support Network Extension (NE) on devices running iOS. NE has no impact on Citrix-developed mobile productivity apps. However, the removal of NE has some impact on deployed enterprise MDX wrapped apps. End-users might experience extra flips to Secure Hub while synchronizing components such as authorization tokens, timers, and PIN retries. For more information, see https://support.citrix.com/article/CTX270296.

> **Note:**
>
> New users are not prompted to install VPN.

- **Support for enhanced enrollment profiles.** Secure Hub supports the enhanced enrollment profile features announced for Citrix Endpoint Management in Enrollment profile support.

Secure Hub 20.2.0

Secure Hub for iOS

This release includes bug fixes.

Secure Hub 20.1.5

This release includes:

- Update to user privacy policy formatting and display. This feature update changes the Secure Hub enrollment flow.
- Bug fixes.

Secure Hub 19.12.5

This release includes bug fixes.

Secure Hub 19.11.5

This release includes bug fixes.

Secure Hub 19.10.5

Secure Hub for Android

Enroll Secure Hub in COPE mode. In Android Enterprise devices, enroll Secure Hub in the Corporate Owned Personally Enabled (COPE) mode when Citrix Endpoint Management is configured in the COPE enrollment profile.

Secure Hub 19.10.0

This release includes bug fixes.

Secure Hub 19.9.5

Secure Hub for iOS

This release includes bug fixes.

Secure Hub for Android

Support for 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 in Citrix Endpoint Management to control keyguard management on work profile devices and Keyguard management on fully managed and dedicated devices. With keyguard management, you can specify the features available to users, such as trust agents and secure camera, before they unlock the keyguard screen. Or, you can choose to disable all keyguard features.

For more information about the feature settings and how to configure the device policy, see Keyguard Management device policy.

Secure Hub 19.9.0

Secure Hub for iOS

Secure Hub for iOS supports iOS 13.

Secure Hub for Android

This release includes bug fixes.

Secure Hub for Android 19.8.5

This release includes bug fixes.

Secure Hub 19.8.0

Secure Hub for iOS

This release includes performance enhancements and bug fixes.

Secure Hub for Android

Support for Android Q. This release includes support for Android Q. Before upgrading to the Android Q platform: See Migrate from device administration to Android Enterprise for information about how the deprecation of Google Device Administration APIs impacts devices running Android Q. Also see the blog, Citrix Endpoint Management and Android Enterprise - a Season of Change.

Secure Hub 19.7.5

Secure Hub for iOS

This release includes performance enhancements and bug fixes.

Secure Hub for Android

Support for Samsung Knox SDK 3.x. Secure Hub for Android supports Samsung Knox SDK 3.x. For more information about migrating to Samsung Knox 3.x, see the Samsung Knox developer documentation. This release also includes support for the new Samsung Knox namespaces. For more information about changes to old Samsung Knox namespaces, see Changes to old Samsung Knox namespaces.

> **Note:**
>
> Secure Hub for Android does not support Samsung Knox 3.x on devices running Android 5.

Secure Hub 19.3.5 to 19.6.6

These releases include performance enhancements and bug fixes.

Secure Hub 19.3.0

Support for Samsung Knox Platform for Enterprise. Secure Hub for Android supports Knox Platform for Enterprise (KPE) on Android Enterprise devices.

Secure Hub 19.2.0

This release includes performance enhancements and bug fixes.

Secure Hub 19.1.5

Secure Hub for Android Enterprise now supports the following policies:

- **WiFi device policy.** The Wi-Fi device policy now supports Android Enterprise. For more information about this policy, see Wi-Fi device policy.
- **Custom XML device policy.** The custom XML device policy now supports Android Enterprise. For more information about this policy, see Custom XML device policy.
- **Files device policy.** You can add script files in Citrix Endpoint Management to perform functions on Android Enterprise devices. For more information about this policy, see Files device policy.

Secure Hub 19.1.0

Secure Hub has revamped fonts, colors, and other UI improvements. This facelift gives you an enriched user experience while closely aligning with the Citrix brand aesthetics across our full suite of mobile productivity apps.

Secure Hub 18.12.0

This release includes performance enhancements and bug fixes.

Secure Hub 18.11.5

- **Restrictions device policy settings for Android Enterprise.** New settings for the Restrictions device policy allow users access to these features on Android Enterprise devices: status bar, lock screen keyguard, account management, location sharing, and keeping the device screen on for Android Enterprise devices. For information, see Restrictions device policy.

Secure Hub 18.10.5 to 18.11.0 include performance enhancements and bug fixes.

Secure Hub 18.10.0

- **Support for Samsung DeX mode:** Samsung DeX enables users to connect KNOX-enabled devices to an external display to use apps, review documents, and watch videos on a PC-like interface. For information about Samsung DeX device requirements and setting up Samsung DeX, see How Samsung DeX works.

  To configure Samsung DeX mode features in Citrix Endpoint Management, update the Restrictions device policy for Samsung Knox. For information, see **Samsung KNOX settings** in Restrictions device policy.

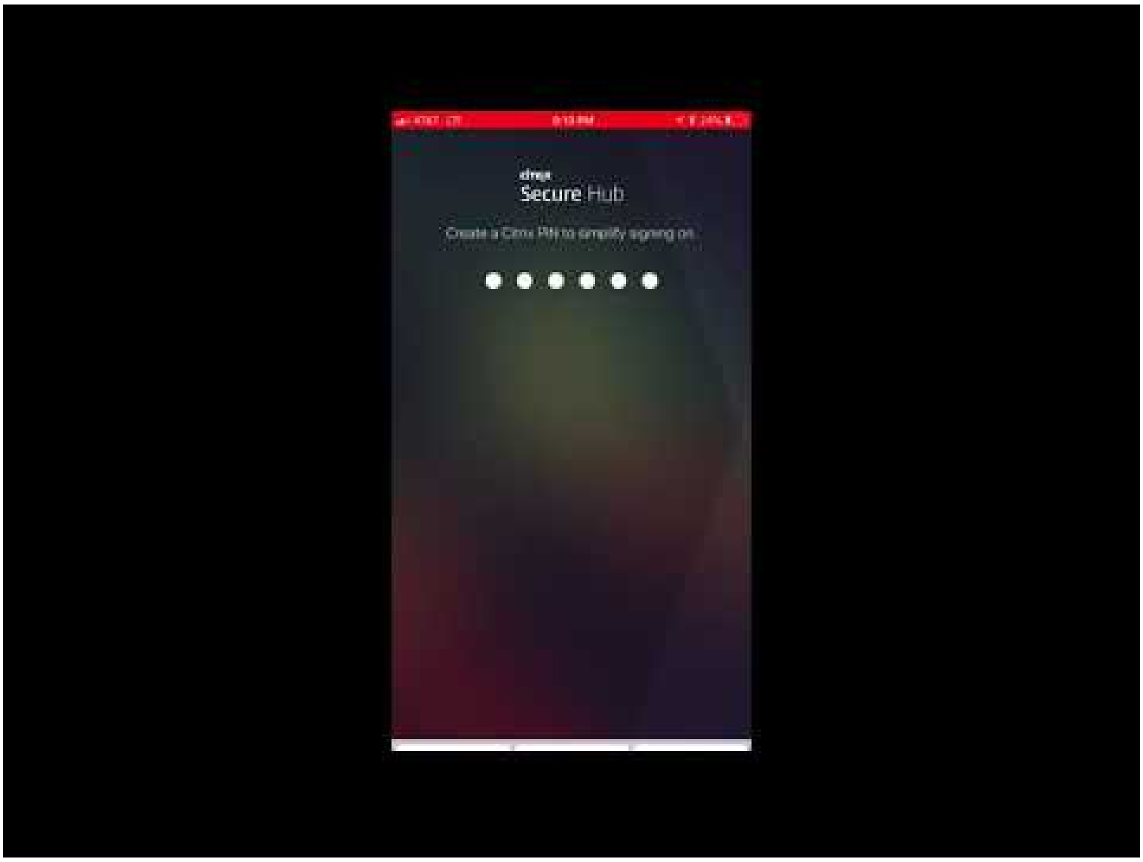
- **Support for Android SafetyNet:** You can configure Endpoint Management to use the **Android SafetyNet** feature to assess the compatibility and security of Android devices that have Secure Hub installed. The results can be used to trigger automated actions on the devices. For information, see Android SafetyNet.
- **Prevent camera use for Android Enterprise devices:** The new **Allow use of camera** setting for the Restrictions device policy lets you prevent users from using the camera on their Android Enterprise devices. For information, see Restrictions device policy.

Secure Hub 10.8.60 to 18.9.0

These releases include performance enhancements and bug fixes.

Secure Hub 10.8.60

- Support for the Polish language.
- Support for Android P.
- Support for the use of the Workspace apps store.
  When opening Secure Hub, users no longer see the Secure Hub store. An **Add Apps** button takes users to the Workspace apps store. The following video shows an iOS device performing an enrollment to Citrix Endpoint Management using the Citrix Workspace app.

  Create a Citrix PIN to simplify signing on

  > Important:
  >
  > This feature is only available for new customers. We don't currently support migration for existing customers.

  To use this feature, configure the following:

  - Enable the Password Caching and Password Authentication policies. For more information on configuring policies, see MDX policies for mobile productivity apps at a glance.
  - Configure Active Directory authentication as AD or AD+Cert. We support these two modes. For more information on configuring authentication, see Domain or domain plus security token authentication.

  - Enable Workspace integration for Endpoint Management. For more information on workspace integration, see Configure workspaces.

> **Important:**
>
> After this feature is enabled, Citrix Files SSO occurs through Workspace and not through Endpoint Management (formerly, XenMobile). We recommend that you disable Citrix Files integration in the Endpoint Management console before you enable Workspace integration.

Secure Hub 10.8.55

- The ability to pass a user name and password for the Google zero-touch and Samsung Knox Mobile Environment (KME) portal by using the configuration JSON. For details, see Samsung Knox bulk enrollment.
- When you enable certificate pinning, users cannot enroll in Endpoint Management with a self-signed certificate. If users try to enroll to Endpoint Management with a self-signed certificate, they are warned that the certificate is not trusted.

Secure Hub 10.8.25: Secure Hub for Android includes support for Android P devices.

> **Note:**
>
> Before upgrading to the Android P platform: 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. Certificates that don't contain a SAN matching the host name are no longer trusted. For details, see the Android Developer documentation.

Secure Hub for iOS update on March 19, 2018: Secure Hub version 10.8.6 for iOS is available to fix an issue with the VPP app policy. For details, see this Citrix Knowledge Center article.

Secure Hub 10.8.5: Support in Secure Hub for Android for COSU mode for Android Work (Android for Work). For details, see the Citrix Endpoint Management documentation.

Administering Secure Hub

You perform most of the administration tasks related to Secure Hub during the initial configuration of Endpoint Management. To make Secure Hub available to users, for iOS and Android, upload Secure Hub to the iOS App Store and the Google Play Store.

Secure Hub also refreshes most MDX policies stored in Endpoint Management for the installed apps when a user's Citrix Gateway session renews after authentication using Citrix Gateway.

> **Important:**
>
> Changes to any of these policies require that a user delete and reinstall the app to apply the updated policy: Security Group, Enable encryption, and Secure Mail Exchange Server.

Citrix PIN

You can configure Secure Hub to use the Citrix PIN, a security feature enabled in the Endpoint Management console in **Settings** > **Client Properties**. The setting requires enrolled mobile device users to sign on to Secure Hub and activate any MDX wrapped apps by using a personal identification number (PIN).

The Citrix PIN feature simplifies the user authentication experience when logging on to the secured wrapped apps. Users don't have to enter another credential like their Active Directory user name and password repeatedly.

Users who sign on to Secure Hub for the first time must enter their Active Directory user name and password. During sign-on, Secure Hub saves the Active Directory credentials or a client certificate on the user device and then prompts the user to enter a PIN. When users sign on again, they enter the PIN to access their Citrix apps and the Store securely, until the next idle timeout period ends for the active user session. Related client properties enable you to encrypt secrets using the PIN, specify the passcode type for the PIN, and specify PIN strength and length requirements. For details, see Client properties.

When fingerprint (touch ID) authentication is enabled, users can sign on by using a fingerprint when offline authentication is required because of app inactivity. Users still have to enter a PIN when signing on to Secure Hub for the first time, restarting the device, and after the inactivity timer expires. For information about enabling fingerprint authentication, see Fingerprint or touch ID authentication.

Certificate pinning

Secure Hub for iOS and Android supports SSL certificate pinning. This feature ensures that the certificate signed by your enterprise is used when Citrix clients communicate with Endpoint Management, thus preventing connections from clients to Endpoint Management when installation of a root certificate on the device compromises the SSL session. When Secure Hub detects any changes to the server public key, Secure Hub denies the connection.

As of Android N, the operating system no longer allows user-added certificate authorities (CAs). Citrix recommends using a public root CA in place of a user-added CA.

Users upgrading to Android N might experience problems if they use private or self-signed CAs. Connections on Android N devices break under the following scenarios:

- Private/self-signed CAs and the Required Trusted CA for Endpoint Management option is set **ON.** For details, see Device management.
- Private/self-signed CAs and the Endpoint Management AutoDiscovery Service (ADS) are not reachable. Due to security concerns, when ADS is not reachable, Required Trusted CA turns **ON** even it was set as **OFF** initially.

Before you enroll devices or upgrade Secure Hub, consider enabling certificate pinning. The option is **Off** by default and managed by the ADS. When you enable certificate pinning, users cannot enroll in Endpoint Management with a self-signed certificate. If users try to enroll with a self-signed certificate, they are warned that the certificate is not trusted. Enrollment fails if users do not accept the certificate.

To use certificate pinning, request that Citrix upload certificates to the Citrix ADS server. Open a technical support case using the Citrix Support portal. Ensure that you don't send the private key to Citrix. Then, provide the following information:

- The domain containing the accounts with which users enroll.
- The Endpoint Management fully qualified domain name (FQDN).
- The Endpoint Management instance name. By default, the instance name is zdm and is case-sensitive.
- User ID Type, which can be either UPN or Email. By default, the type is UPN.
- The port used for iOS enrollment if you changed the port number from the default port 8443.
- The port through which Endpoint Management accepts connections if you changed the port number from the default port 443.
- The full URL of your Citrix Gateway.
- Optionally, an email address for your administrator.
- The PEM-formatted certificates you want added to the domain, which must be public certificates and not the private key.
- How to handle any existing server certificates: Whether to remove the old server certificate immediately (because it is compromised) or to continue to support the old server certificate until it expires.

Your technical support case is updated when your details and certificate have been added to the Citrix servers.

Certificate + one-time-password authentication

You can configure Citrix ADC so that Secure Hub authenticates using a certificate plus a security token that serves as a one-time password. This configuration provides a strong security option that doesn't leave an Active Directory footprint on devices.

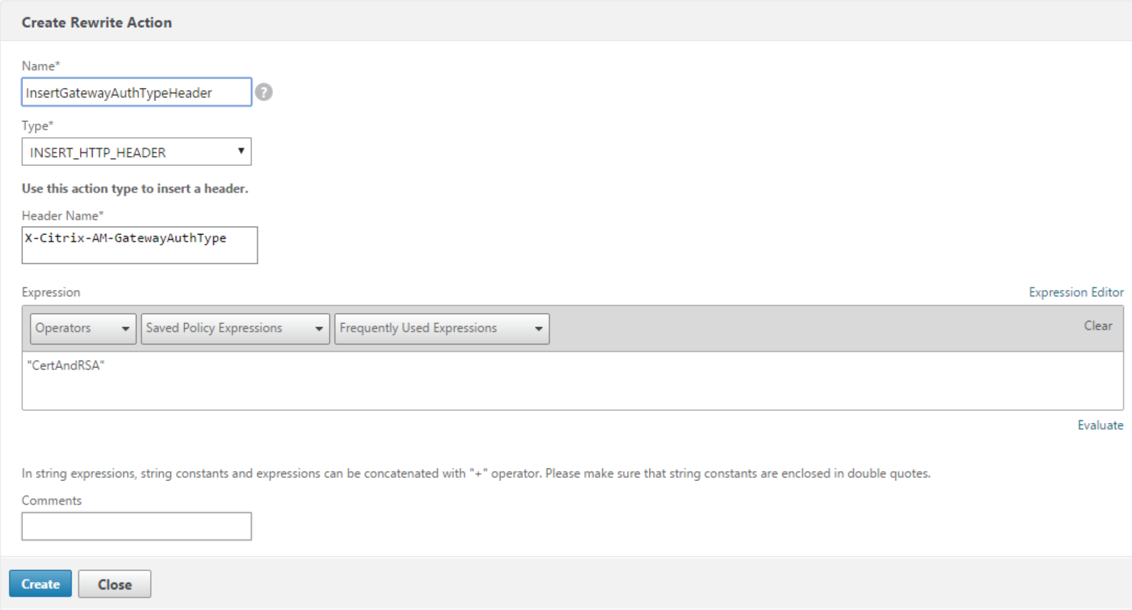
To enable Secure Hub to use the certificate + one-time-password type of authentication, do the following: Add a rewrite action and a rewrite policy in Citrix ADC that inserts a custom response header of the form **X-Citrix-AM-GatewayAuthType: CertAndRSA** to indicate the Citrix Gateway logon type.

Ordinarily, Secure Hub uses the Citrix Gateway logon type configured in the Endpoint Management console. However, this information isn't available to Secure Hub until Secure Hub completes logon for the first time. Therefore, the custom header is required.

> **Note:**
>
> If different logon types are set for Endpoint Management and Citrix ADC, the Citrix ADC configuration overrides. For details, see Citrix Gateway and Endpoint Management.

1. In Citrix ADC, navigate to **Configuration > AppExpert > Rewrite > Actions**.
2. Click **Add**.

   The **Create Rewrite Action** screen appears.
3. Fill in each field as shown in the following figure and then click **Create**.



Create Rewrite Action

Name*: InsertGatewayAuthTypeHeader

Type*: INSERT_HTTP_HEADER

Use this action type to insert a header.

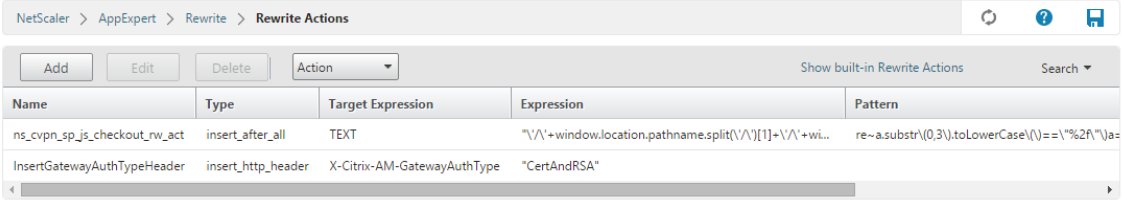
Header Name*: X-Citrix-AM-GatewayAuthType

Expression: "CertAndRSA"

In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string constants are enclosed in double quotes.

Comments:

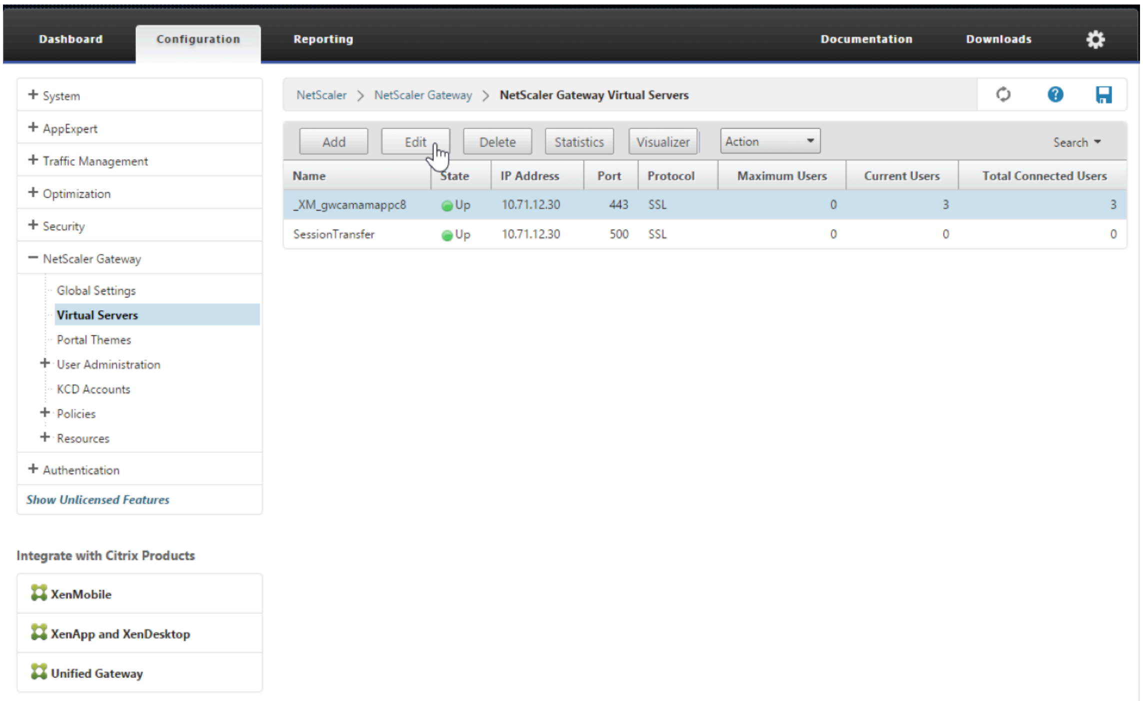
The following result appears on the main **Rewrite Actions** screen.



NetScaler > AppExpert > Rewrite > Rewrite Actions

Name	Type	Target Expression	Expression	Pattern
ns_cvpn_sp_js_checkout_rw_act	insert_after_all	TEXT	"\'/\'+window.location.pathname.split(\'/\')[1]+\'/\'+wi...	re~a.substr\(0,3\).toLowerCase\(\)==\"%2f\"\)a=
InsertGatewayAuthTypeHeader	insert_http_header	X-Citrix-AM-GatewayAuthType	"CertAndRSA"	

4. Bind the rewrite action to the virtual server as a rewrite policy. Go to **Configuration > NetScaler Gateway > Virtual Servers** and then select your virtual server.

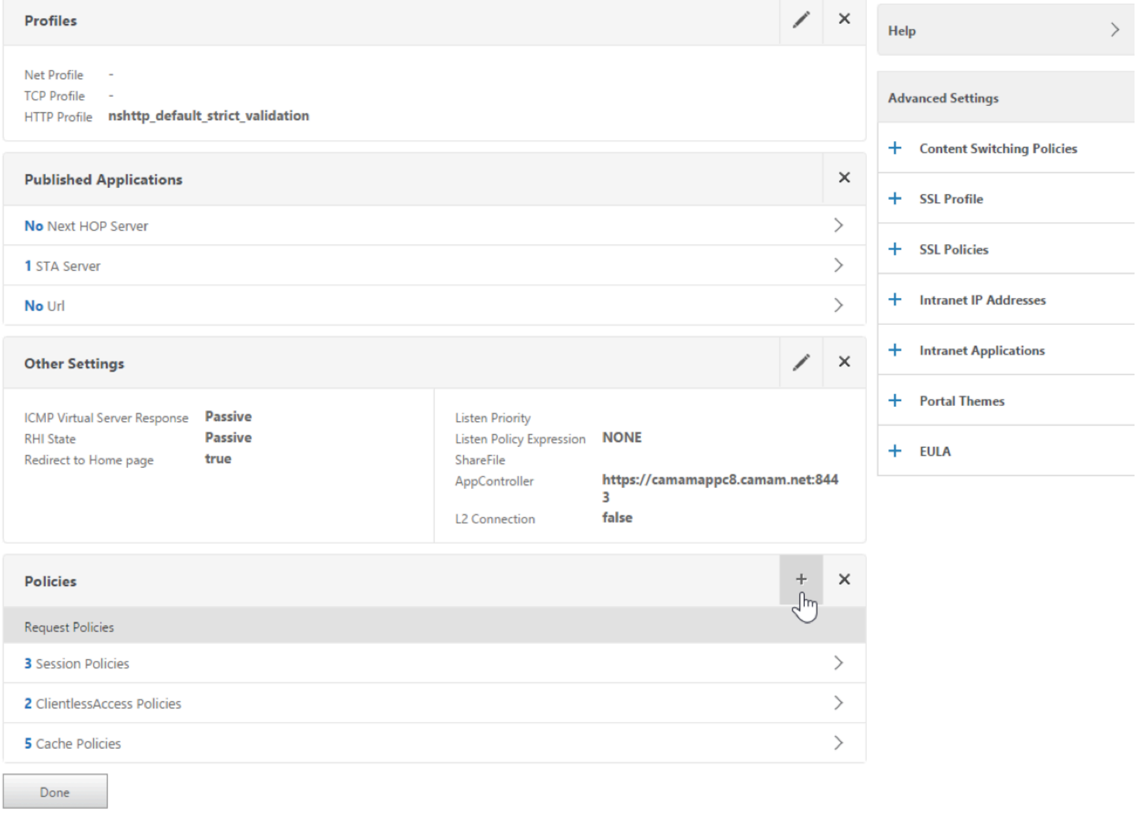


Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
_XM_gwcamamappc8	● Up	10.71.12.30	443	SSL	0	3	3
SessionTransfer	● Up	10.71.12.30	500	SSL	0	0	0

5. Click **Edit**.

6. On the **Virtual Servers configuration** screen, scroll down to **Policies**.

7. Click **+** to add a policy.



Net Profile -
TCP Profile -
HTTP Profile nshttp_default_strict_validation

No Next HOP Server

1 STA Server

No Url

ICMP Virtual Server Response **Passive**
RHI State **Passive**
Redirect to Home page **true**

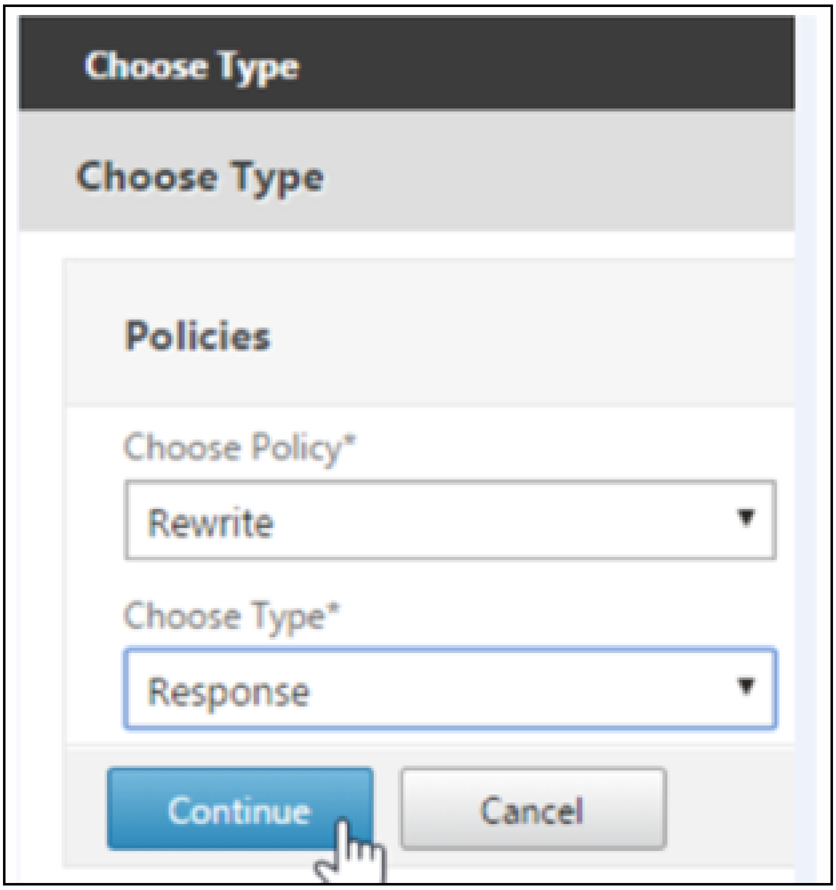
Listen Priority
Listen Policy Expression **NONE**
ShareFile
AppController **https://camamappc8.camam.net:8443**
L2 Connection **false**

3 Session Policies

2 ClientlessAccess Policies

5 Cache Policies

8. In the **Choose Policy** field, choose **Rewrite**.
9. In the **Choose Type** field, choose **Response**.



Choose Type

Choose Type

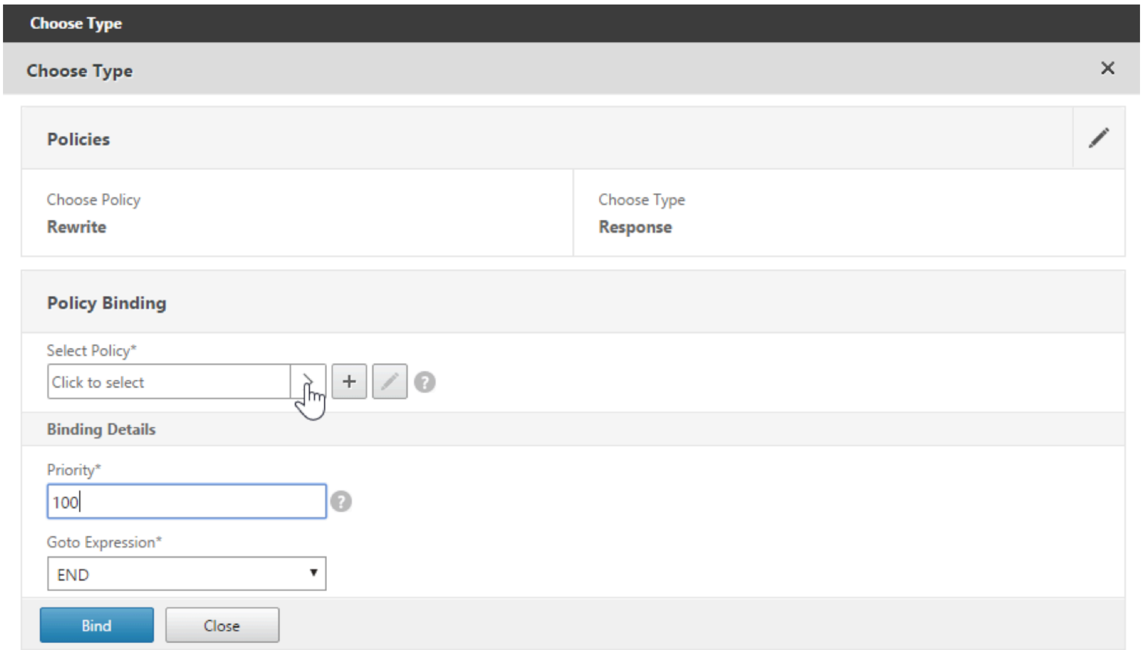
Policies

Choose Policy*
Rewrite

Choose Type*
Response

10. Click **Continue**.

    The **Policy Binding** section expands.



Choose Policy: Rewrite

Choose Type: Response

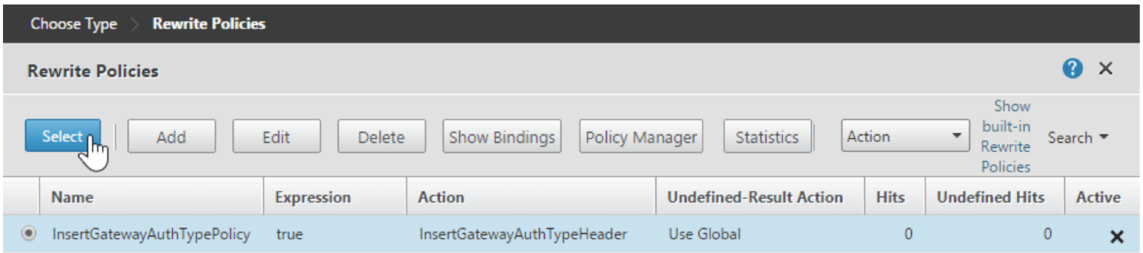
Select Policy*: Click to select

Priority*: 100

Goto Expression*: END

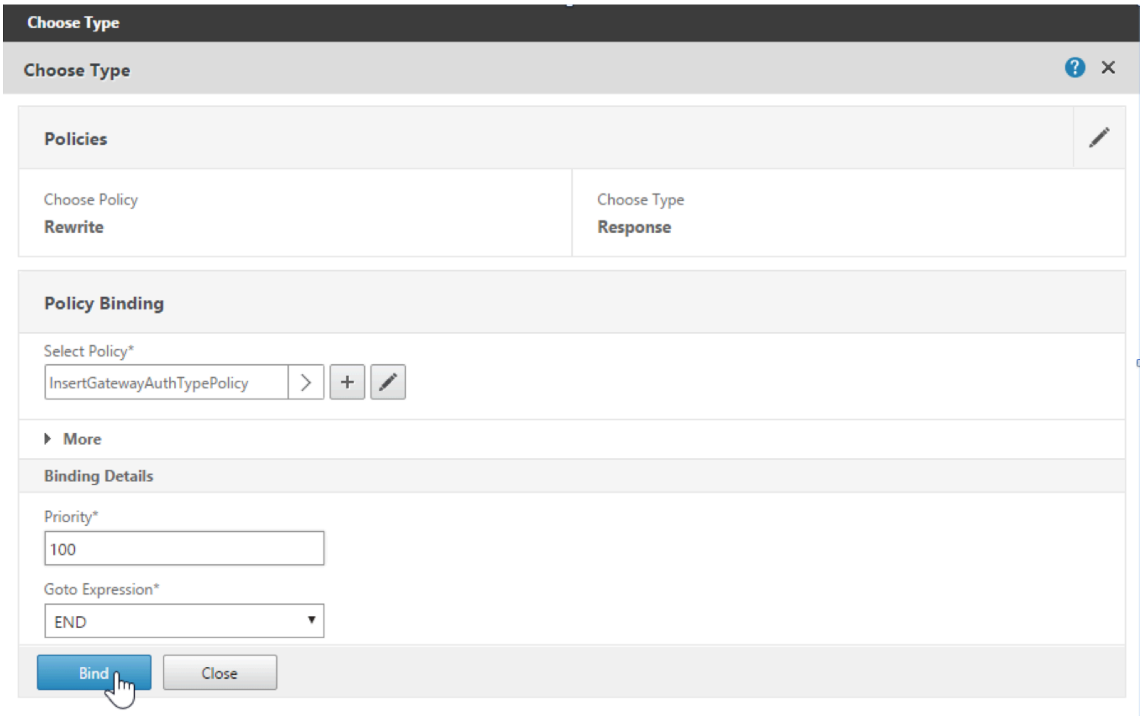
11. Click **Select Policy**.

    A screen with available policies appears.



	Name	Expression	Action	Undefined-Result Action	Hits	Undefined Hits	Active
●	InsertGatewayAuthTypePolicy	true	InsertGatewayAuthTypeHeader	Use Global	0	0	✕

12. Click the row of the policy you created and then click **Select**. The **Policy Binding** screen appears again, with your selected policy filled in.



Choose Type

Choose Type

Policies

Choose Policy	Choose Type
Rewrite	Response

Policy Binding

Select Policy*: InsertGatewayAuthTypePolicy

More

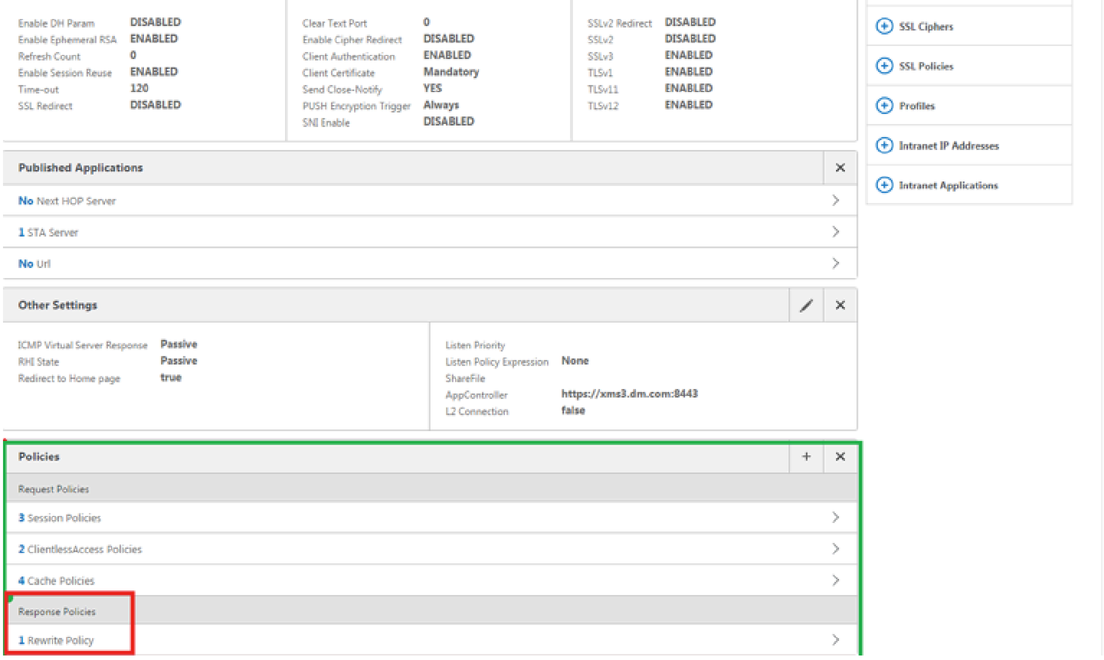
Binding Details

Priority*: 100

Goto Expression*: END

13. Click **Bind**.

    If the bind is successful, the main configuration screen appears with the completed rewrite policy shown.



Enable DH Param	DISABLED
Enable Ephemeral RSA	ENABLED
Refresh Count	0
Enable Session Reuse	ENABLED
Time-out	120
SSL Redirect	DISABLED

Clear Text Port	0
Enable Cipher Redirect	DISABLED
Client Authentication	ENABLED
Client Certificate	Mandatory
Send Close-Notify	YES
PUSH Encryption Trigger	Always
SNI Enable	DISABLED

SSLv2 Redirect	DISABLED
SSLv2	DISABLED
SSLv3	ENABLED
TLSv1	ENABLED
TLSv11	ENABLED
TLSv12	ENABLED

Published Applications

No Next HOP Server

1 STA Server

No Url

Other Settings

ICMP Virtual Server Response	Passive
RHI State	Passive
Redirect to Home page	true

Listen Priority	
Listen Policy Expression	None
ShareFile	
AppController	https://xms3.dm.com:8443
L2 Connection	false

Policies

Request Policies

3 Session Policies

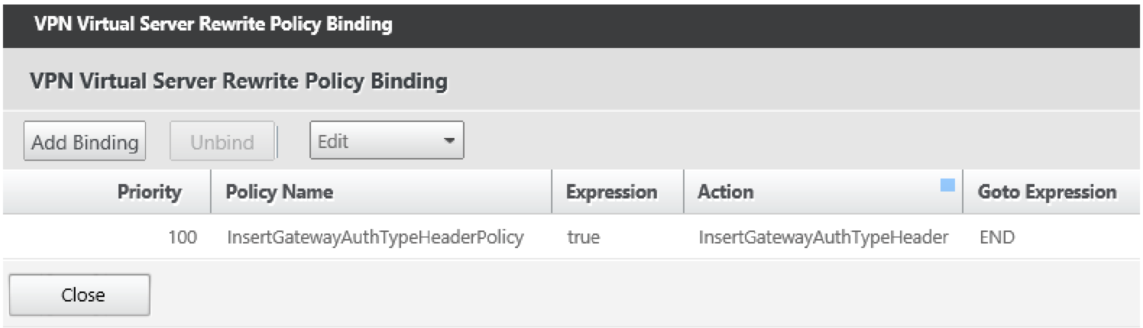
2 ClientlessAccess Policies

4 Cache Policies

Response Policies

1 Rewrite Policy

14. To view the policy details, click **Rewrite Policy**.



VPN Virtual Server Rewrite Policy Binding
VPN Virtual Server Rewrite Policy Binding
Add Binding
Unbind
Edit
Close

Priority	Policy Name	Expression	Action	Goto Expression
100	InsertGatewayAuthTypeHeaderPolicy	true	InsertGatewayAuthTypeHeader	END

Port requirement for ADS connectivity for Android devices

Port configuration ensures that Android devices connecting from Secure Hub can access the Citrix ADS from within the corporate network. The ability to access ADS is important when downloading security updates made available through ADS. ADS connections might not be compatible with your proxy server. In this scenario, allow the ADS connection to bypass the proxy server.

> **Important:**
>
> Secure Hub for Android and iOS require you to allow Android devices to access ADS. For details, see Port requirements in the Citrix Endpoint Management documentation. This communication is on outbound port 443. It's highly likely that your existing environment is designed to allow this access. Customers who cannot guarantee this communication are discouraged from upgrading to Secure Hub 10.2. If you have any questions, contact Citrix support.

Prerequisites:

- Collect Endpoint Management 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.

The new certificate pinning improvements require that devices connect to ADS before the device enrolls. This prerequisite ensures that the latest security information is available to Secure Hub for the environment in which the device is enrolling. If devices cannot reach ADS, Secure Hub does not allow enrollment of the device. Therefore, opening up ADS access within the internal network is critical to enable devices to enroll.

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

FQDN	IP address	Port	IP and port usage
`discovery.mdm.zenprise.com`	52.5.138.94	443	Secure Hub - ADS Communication

FQDN	IP address	Port	IP and port usage
discovery.mdm.zenprise.com	52.1.30.122	443	Secure Hub - ADS Communication
ads.xm.cloud.com: note that Secure Hub version 10.6.15 and later uses ads.xm.cloud.com.	34.194.83.188	443	Secure Hub - ADS Communication
ads.xm.cloud.com: note that Secure Hub version 10.6.15 and later uses ads.xm.cloud.com.	34.193.202.23	443	Secure Hub - ADS Communication

If certificate pinning is enabled:

- Secure Hub pins your enterprise certificate during device enrollment.
- During an upgrade, Secure Hub discards any currently pinned certificate and then pins the server certificate on the first connection for enrolled users.

  > **Note:**
  >
  > If you enable certificate pinning after an upgrade, users must enroll again.

- Certificate renewal does not require reenrollment, if the certificate public key did not change.

Certificate pinning supports leaf certificates, not intermediate or issuer certificates. Certificate pinning applies to Citrix servers, such as Endpoint Management and Citrix Gateway, and not third-party servers.

Disabling the Delete Account option

You can disable the **Delete Account** option in Secure Hub in environments where the Auto Discovery Services (ADS) is enabled.

Perform the following steps to disable the **Delete Account** option:

1. Configure ADS for your domain.
2. Open the **AutoDiscovery Service Information** in Citrix Endpoint Management and set the value for `displayReenrollLink` to **False**.
   By default this value is **True**.

3. If your device is enrolled in the MDM+MAM (ENT) mode, log off and log in again for the changes to take effect.
   If your device is enrolled in other modes, you must re-enroll the device.

Using Secure Hub

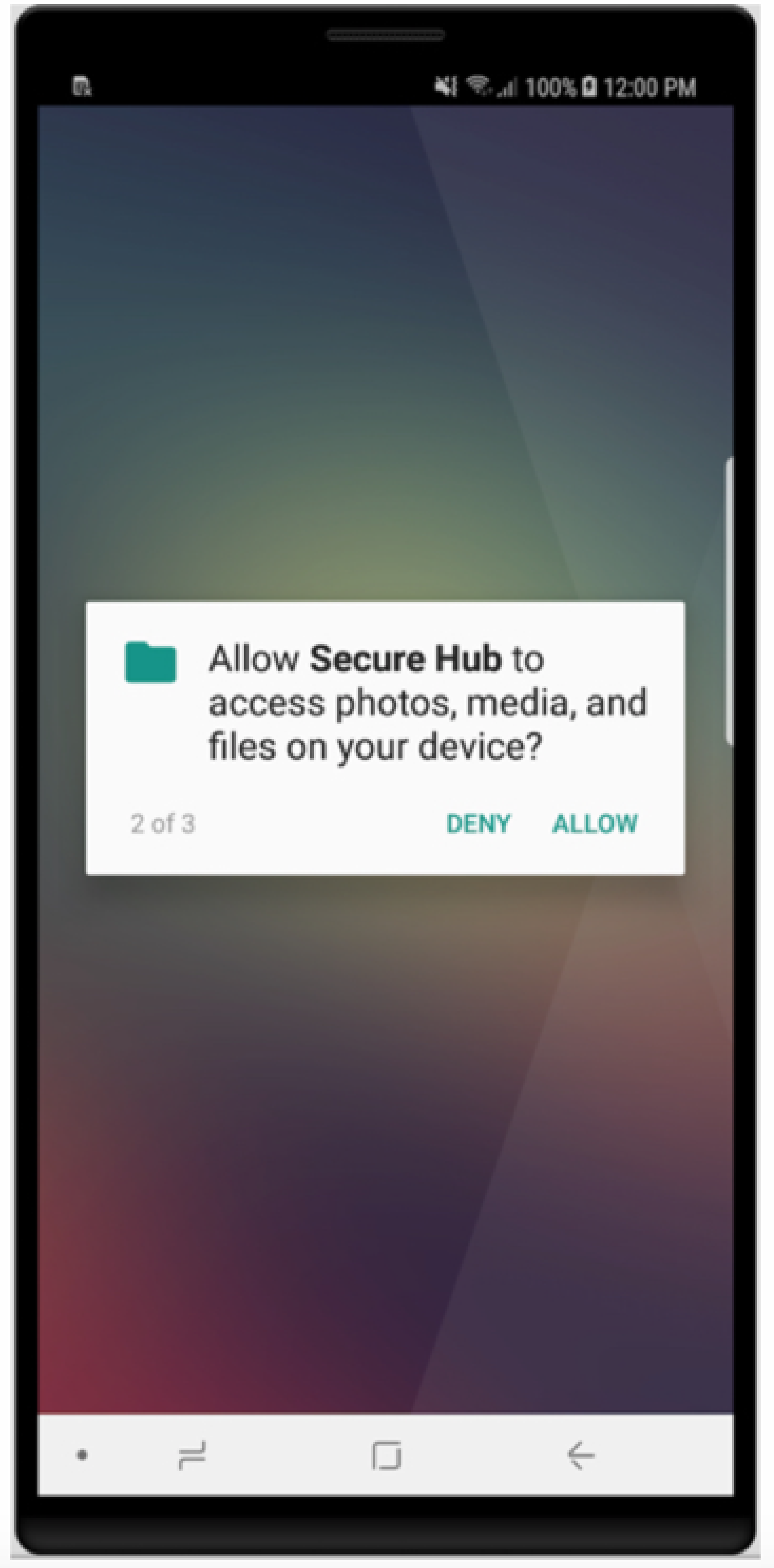
Users begin by downloading Secure Hub on to their devices from the Apple or Android store.

When Secure Hub opens, users enter the credentials provided by their companies to enroll their devices in Secure Hub. For more details about device enrollment, see User accounts, roles, and enrollment.

On Secure Hub for Android, during initial installation and enrollment, the following message appears: Allow Secure Hub to access photos, media, and files on your device?

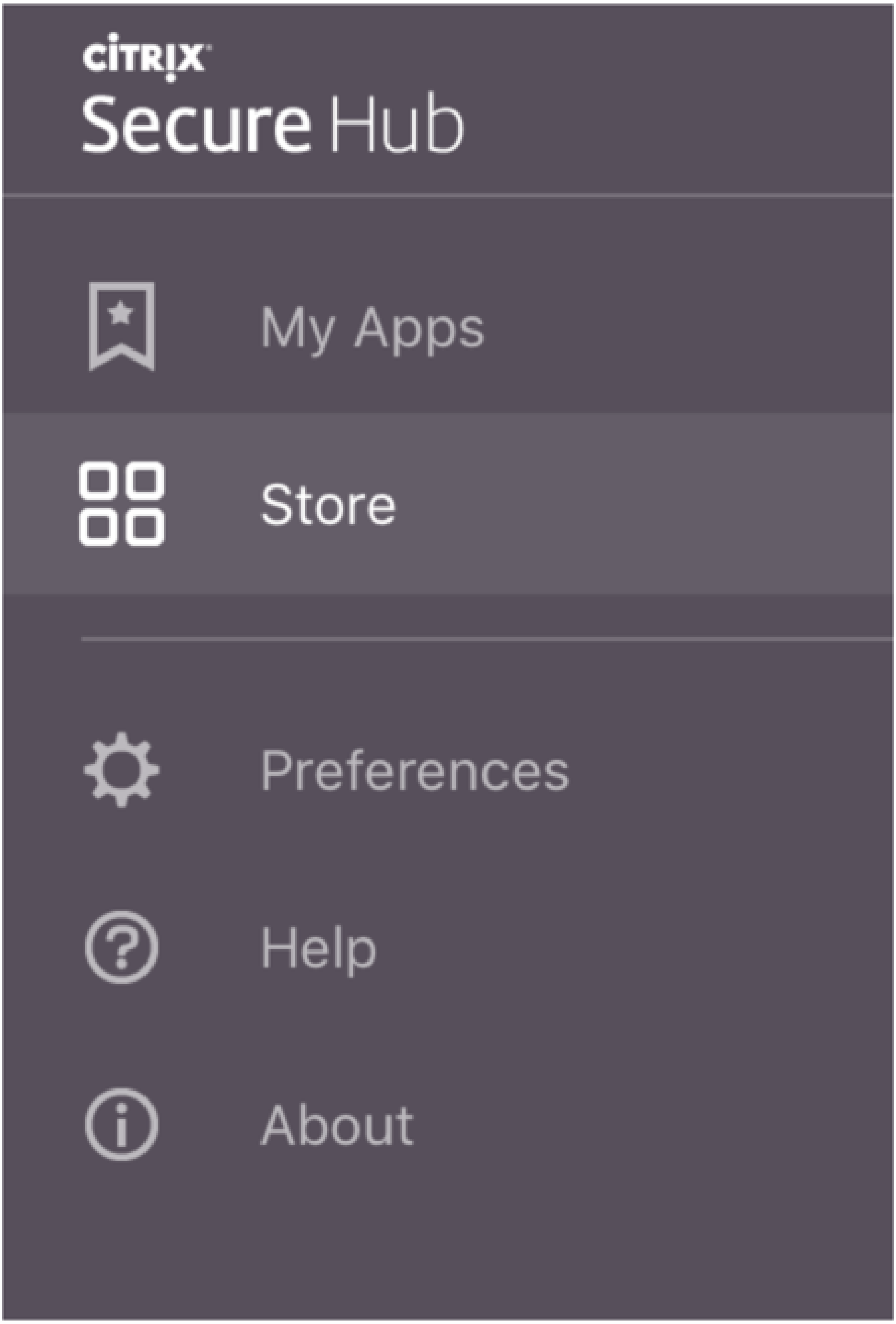
This message comes from the Android operating system and not from Citrix. When you tap **Allow**, Citrix and the admins who manage Secure Hub do not view your personal data at any time. If however, you conduct a remote support session with your admin, the admin can view your personal files within the session.

Once enrolled, users see any apps and desktops that you've pushed in their **My Apps** tab. Users can add more apps from the Store. On phones, the Store link is under the **Settings** hamburger icon in the upper left-hand corner.



Allow **Secure Hub** to access photos, media, and files on your device?

On tablets, the Store is a separate tab.


citrix
Secure Hub
My Apps
Store
Preferences
Help
About

When users with iPhones running iOS 9 or later install mobile productivity apps from the store, they see a message. The message states that the enterprise developer, Citrix, is not trusted on that iPhone. The message notes that the app is not available for use until the developer is trusted. When this message appears, Secure Hub prompts users to view a guide that coaches them through the process of trusting Citrix enterprise apps for their iPhone.

Automatic enrollment in Secure Mail

For MAM-only deployments, you can configure Endpoint Management so that users with Android or iOS devices who enroll in Secure Hub using email credentials are automatically enrolled in Secure Mail. Users do not have to enter more information or take more steps to enroll in Secure Mail.

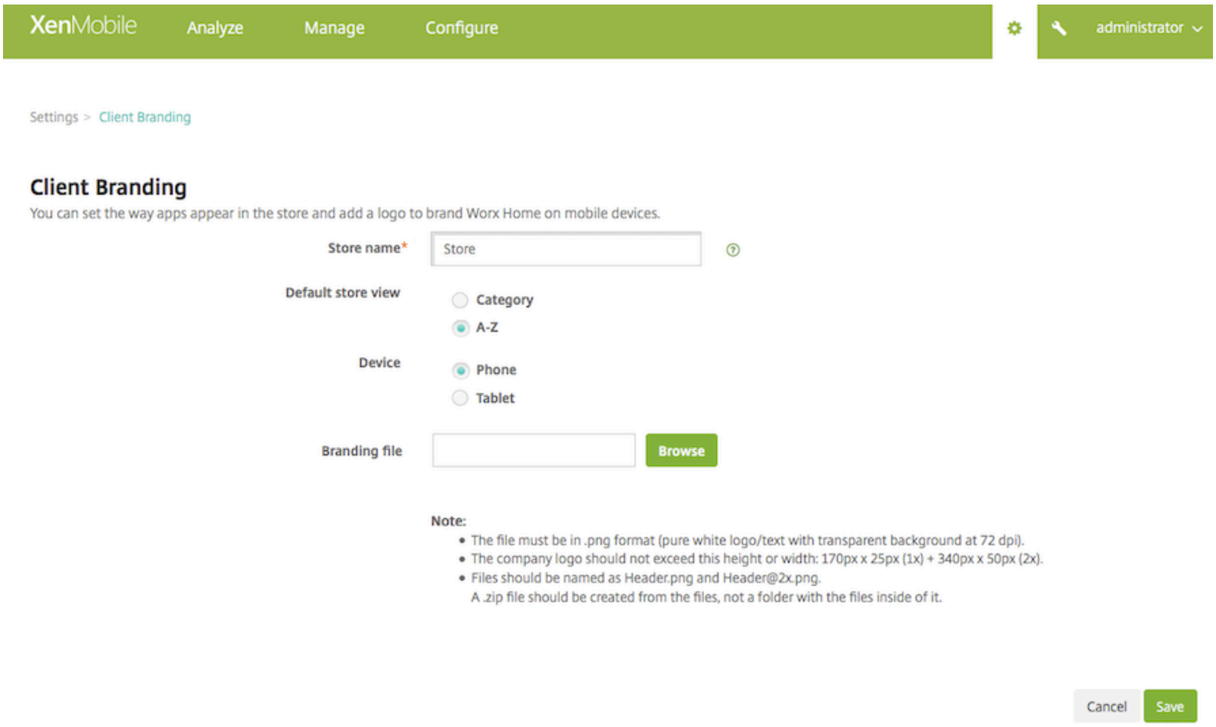
On first-time use of Secure Mail, Secure Mail obtains the user's email address, domain, and user ID from Secure Hub. Secure Mail uses the email address for AutoDiscovery. The Exchange Server is identified using the domain and user ID, which enables Secure Mail to authenticate the user automatically. The user is prompted to enter a password if the policy is set to not pass through the password. The user is not, however, required to enter more information.

To enable this feature, create three properties:

- The server property MAM_MACRO_SUPPORT. For instructions, see Server properties.
- The client properties ENABLE_CREDENTIAL_STORE and SEND_LDAP_ATTRIBUTES. For instructions, see Client properties.

Customized Store

If you want to customize your Store, go to **Settings > Client Branding** to change the name, add a logo, and specify how the apps appear.



Client Branding

You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.

Store name* Store

Default store view ○ Category ● A-Z

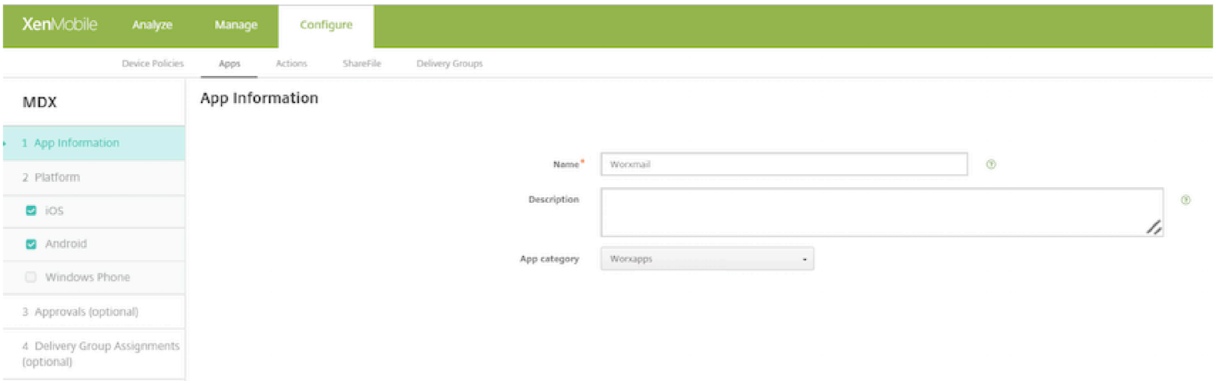
Device ● Phone ○ Tablet

Branding file Browse

Note:

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.
  A .zip file should be created from the files, not a folder with the files inside of it.

You can edit app descriptions in the Endpoint Management console. Click **Configure** then click **Apps**. Select the app from the table and then click **Edit**. Select the platforms for the app with the description you're editing and then type the text in the **Description** box.



☑ iOS
☑ Android
□ Windows Phone

App Information

Name* Worxmail

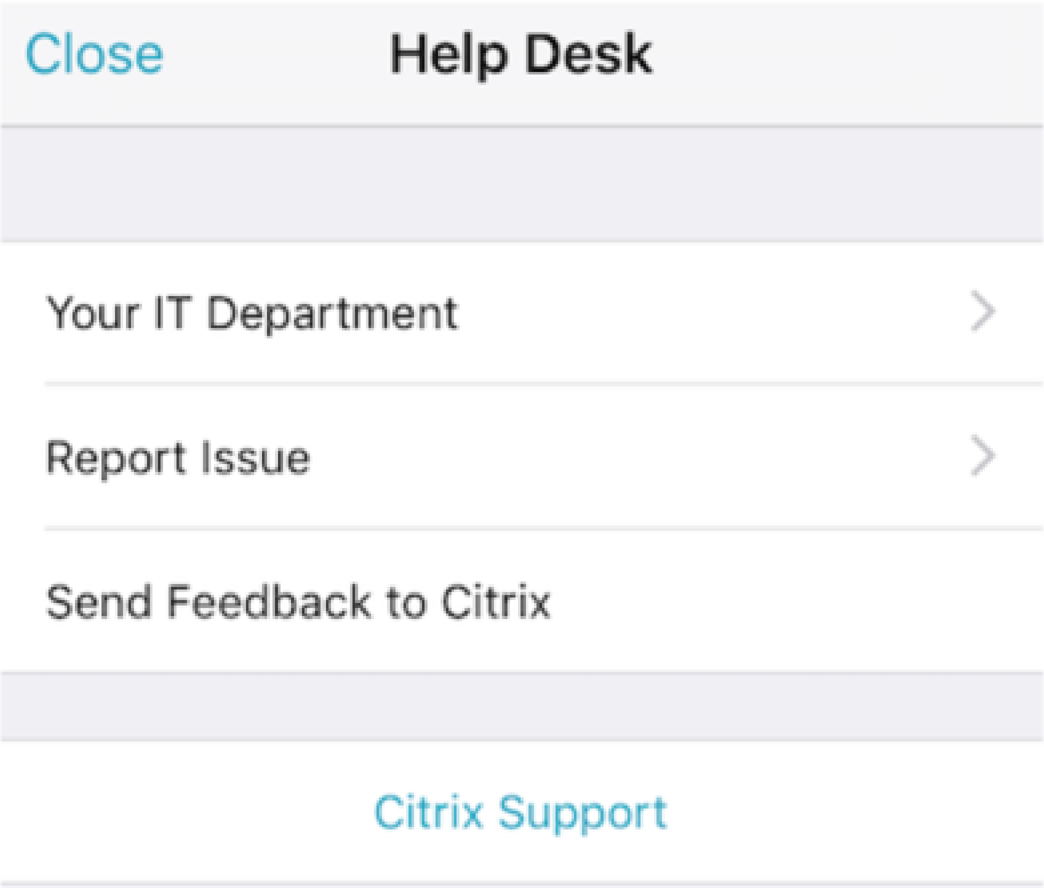
Description

App category Worxapps

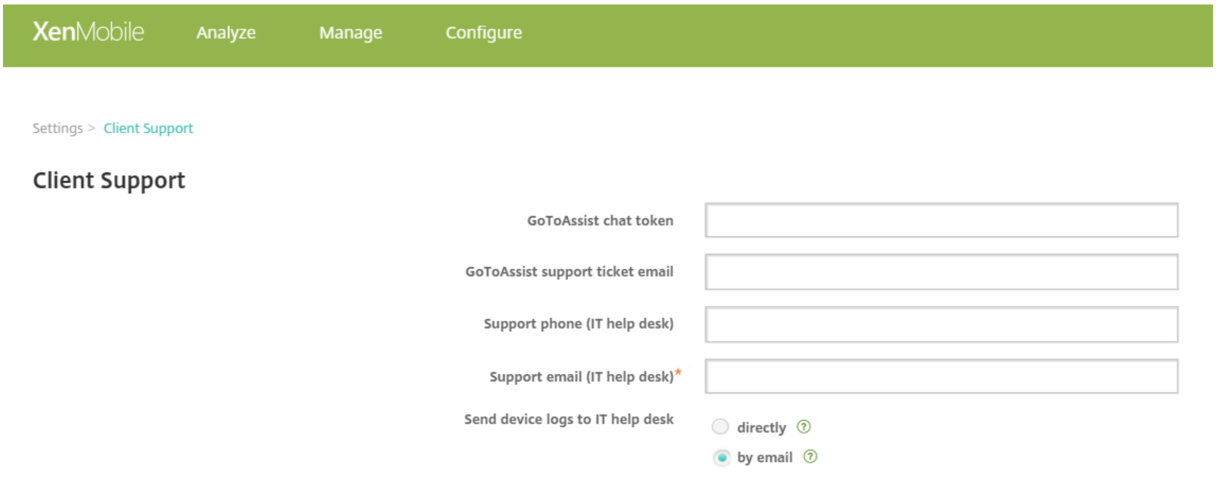
In the Store, users can browse only those apps and desktops that you've configured and secured in Endpoint Management. To add the app, users tap **Details** and then tap **Add**.

Configured Help options

Secure Hub also offers users various ways to get help. On tablets, tapping the question mark in the upper-right corner opens help options. On phones, users tap the hamburger menu icon in the upper-left corner and then tap **Help**.



Your IT Department shows the telephone and email of your company help desk, which users can access directly from the app. You enter phone numbers and email addresses in the Endpoint Management console. Click the gear icon in the upper-right corner. The **Settings** page appears. Click **More** and then click **Client Support**. The screen where you enter the information appears.



Client Support

GoToAssist chat token	
GoToAssist support ticket email	
Support phone (IT help desk)	
Support email (IT help desk)*	
Send device logs to IT help desk	○ directly ● by email

Report Issue shows a list of apps. Users select the app that has the issue. Secure Hub automatically generates logs and then opens a message in Secure Mail with the logs attached as a zip file. Users add subject lines and descriptions of the issue. They can also attach a screenshot.

Send Feedback to Citrix opens a message in Secure Mail with a Citrix support address filled in. In the body of the message, the user can enter suggestions for improving Secure Mail. If Secure Mail isn't installed on the device, the native mail program opens.

Users can also tap **Citrix Support,** which opens the Citrix Knowledge Center. From there, they can search support articles for all Citrix products.

In **Preferences**, users can find information about their accounts and devices.

Location policies

Secure Hub also provides geo-location and geo-tracking policies if, for example, you want to ensure that a corporate-owned device does not breach a certain geographic perimeter. For details, see Location device policy.

Crash collection and analysis

Secure Hub automatically collects and analyzes failure information so you can see what led to a particular failure. The software Crashlytics supports this function.

For more features available for iOS and Android, see the Features by platform matrix for Citrix Secure Hub.

Known and fixed issues

November 10, 2021

Citrix supports upgrades from the last two versions of the mobile productivity apps.

Secure Hub 21.11.0

Known issues in Secure Hub 21.11.0

There are no known issues in this release.

Fixed issues in Secure Hub 21.11.0

Secure Hub for Android

-During enrollment in Secure Hub for Android, the **No certificates found** error message appears. When you click **Install certificate**, an empty link, without any certificate, appears. If you click **Cancel**, the authentication screen appears. This issue also occurs when you sign out and sign in to Secure Hub. [CXM-101126]

Secure Hub 21.10.0

Known issues in Secure Hub 21.10.0

There are no known issues in this release.

Fixed issues in Secure Hub 21.10.0

Secure Hub for iOS

- In Secure Hub for iOS, you are prompted to enroll using a PIN on devices enrolled through the Apple Deployment Program. [CXM-99240]

Secure Hub for Android

- When creating an enrollment profile for Android devices to enroll in work profile on corporate-owned devices mode, you must enable the **BYOD work profile** setting. If you don't enable this setting, devices fail to enroll. [CXM-100418]
- While signing in to Secure Hub for Android, the email ID is auto populated. [CXM-100517]

Secure Hub 21.8.0

Secure Hub for iOS

Known issues in Secure Hub 21.8.0

There are no known issues in this release.

Fixed issues in Secure Hub 21.8.0

- When you log in to Secure Mail after your device has been idle, Secure Hub for iOS opens and attempts to log on but the logon request fails. Secure Mail continues to prompt for logon and creates a sign-on loop. [CXM-96825]
- Users with certain special characters in their user name or password can't enroll. [CXM-98778]

Secure Hub 21.7.1

Secure Hub for Android

There are no known or fixed issues in this release.

Known and fixed issues in earlier versions

For known and fixed issues in earlier versions of Secure Hub, see History of Secure Hub known and fixed issues.

Authentication prompt scenarios

June 22, 2021

Various scenarios prompt users to authenticate with Secure Hub by entering their credentials on their devices.

The scenarios change depending on these factors:

- Your MDX app policy and Client Property configuration in the Endpoint Management console settings.
- Whether the authentication occurs offline or online (the device needs a network connection to Endpoint Management).

In addition, the kind of credentials that users enter, such as the Active Directory password, Citrix PIN or passcode, one-time password, fingerprint authentication (known as Touch ID in iOS), which also change based on the type of authentication and the frequency of authentication.

Let’s start with the scenarios that result in an authentication prompt.

- **Device restart:** When users restart their device, they must reauthenticate with Secure Hub.

- **Offline inactivity (time-out):** With the App Passcode MDX policy enabled (by default), the Endpoint Management client property called Inactivity Timer comes into play. The Inactivity Timer limits the length of time that can pass without user activity in any of the apps that use the secure container.

When the Inactivity Timer expires, users must reauthenticate to the secure container on the device. For example, when users set down their devices and walk away, and the Inactivity Timer has expired, someone else can’t pick up the device and access sensitive data within the container. You set the **Inactivity Timer client** property in the Endpoint Management console. The default is 15 minutes. The combination of the App Passcode set to **ON** and the Inactivity Timer client property is responsible for probably the most common of the authentication prompt scenarios.

- **Signing off from Secure Hub:**. When users sign off from Secure Hub, they have to reauthenticate the next time they access Secure Hub or any MDX app, when the app requires a passcode as determined by the App Passcode MDX policy and the Inactivity Timer status.
- **Maximum offline period:**. This scenario is specific to individual apps because it is driven by a per-app MDX policy. The Maximum offline period MDX policy has a default setting of 3 days. If the time period for an app to run without online authentication with Secure Hub elapses, a check-in with Endpoint Management is required to confirm app entitlement and to refresh policies. When this check-in occurs, the app triggers Secure Hub for an online authentication. Users must reauthenticate before they can access the MDX app.

Note the relationship between the Maximum offline period and the Active poll period MDX policy:

- The Active poll period is the interval during which apps check in with Endpoint Management for performing security actions, such as app lock and app wipe. In addition, the app also checks for updated app policies.
- After a successful check for policies via the Active poll period policy, the Maximum offline period timer is reset and begins counting down again.

Both check-ins with Endpoint Management, for Active poll period and Maximum offline period expiry, require a valid Citrix Gateway token on the device. If the device has a valid Citrix Gateway token, the app retrieves new policies from Endpoint Management without any interruption to users. If the app needs a Citrix Gateway token, a flip to Secure Hub occurs, and users see an authentication prompt in Secure Hub.

On Android devices, the Secure Hub activity screens open directly on top of the current app screen. On iOS devices, however, Secure Hub must come to the foreground, which temporarily displaces the current app.

After users enter their credentials, Secure Hub flips back to the original app. If, in this case, you allow for cached Active Directory credentials or you have a client certificate configured, users can enter a PIN, password, or fingerprint authentication. If you do not, users must enter their complete Active Directory credentials.

The Citrix ADC token may become invalid due to Citrix Gateway session inactivity or a forced session time-out policy, as discussed in the following list of Citrix Gateway policies. When users sign on to Secure Hub again, they can continue running the app.

- **Citrix Gateway session policies:** Two Citrix Gateway policies also affect when users are prompted to authenticate. In these cases, they authenticate to create an online session with Citrix ADC for connecting to Endpoint Management.
  - **Session time-out:** The Citrix ADC session for Endpoint Management is disconnected if no network activity occurs for the set period. The default is 30 minutes. If you use the Citrix Gateway wizard to configure the policy, however, the default is 1440 minutes. Users see an authentication prompt to reconnect to their corporate network.

  - **Forced time-out:** If **On**, the Citrix ADC session for Endpoint Management is disconnected after the forced time-out period elapses. The forced time-out makes reauthentication mandatory after a set period. Users will then see an authentication prompt to reconnect to their corporate network upon the next use. The default is **Off**. If you use the Citrix Gateway wizard to configure the policy, however, the default is 1440 minutes.

Credential types

The preceding section discussed when users are prompted to authenticate. This section discusses the kinds of credentials they must enter. Authentication is necessary through various authentication methods to gain access to encrypted data on the device. To initially unlock the device, you unlock the *primary container*. After this occurs and the container is secured again, to gain access again, you unlock a *secondary container*.

> Note:
>
> The term *managed app* refers to an app wrapped by the MDX Toolkit, in which you've left the App Passcode MDX policy enabled by default and are using the Inactivity Timer client property.

The circumstances that determine the credential types are as follows:

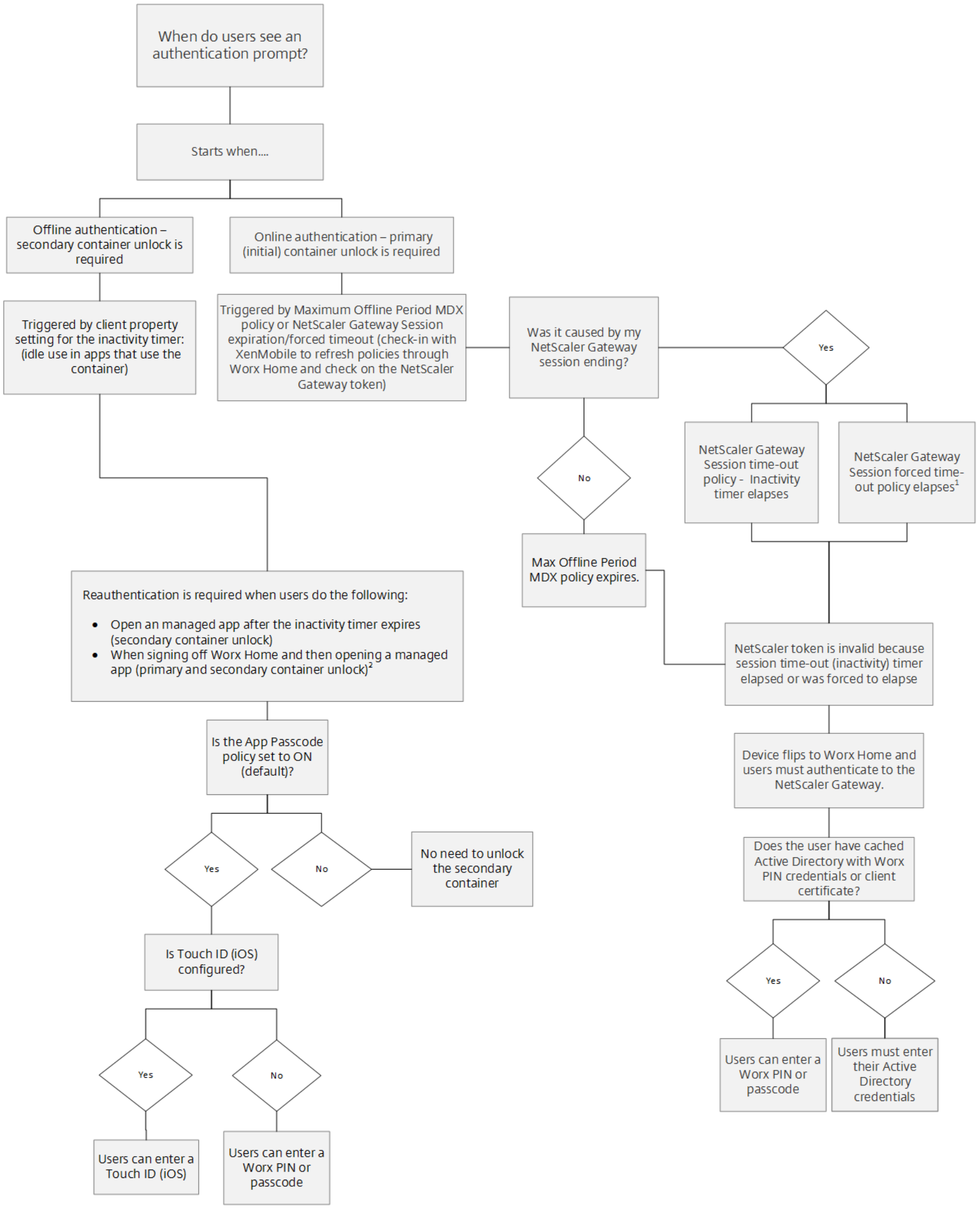
- **Primary container unlock:** An Active Directory password, Citrix PIN or passcode, one-time password, Touch ID or fingerprint ID are required to unlock the primary container.
  - On iOS, when users open Secure Hub or a managed app for the first time after the app is installed on the device.
  - On iOS, when users restart a device and then open Secure Hub.
  - On Android, when users open a managed app if Secure Hub is not running.
  - On Android, when users restart Secure Hub for any reason, including a device restart.
- **Secondary container unlock:** Fingerprint authentication (if configured), a Citrix PIN or passcode, or Active Directory credentials, to unlock the secondary container.
  - When users open a managed app after the inactivity timer expires.
  - When users sign off from Secure Hub and then open a managed app.

Active Directory credentials are required for either container unlock circumstance when the following conditions are true:

- When users change the passcode associated with their corporate account.
- When you have not set the client properties in the Endpoint Management console to enable the Citrix PIN: ENABLE_PASSCODE_AUTH and ENABLE_PASSWORD_CACHING.
- When the NetScaler Gateway session ends, which occurs in the following circumstances: when the session time-out or forced time-out policy timer expires, if the device does not cache the credentials or does not have a client certificate.

When fingerprint authentication is enabled, users can sign on by using a fingerprint when offline authentication is required because of app inactivity. Users still have to enter a PIN when signing on to Secure Hub for the first time and when restarting the device. For information about enabling fingerprint authentication, see Fingerprint or touch ID authentication.

The following flowchart summarizes the decision flow that determines which credentials a user must enter when prompted to authenticate.


When do users see an authentication prompt?
Starts when....
Offline authentication – secondary container unlock is required
Online authentication – primary (initial) container unlock is required
Triggered by client property setting for the inactivity timer: (idle use in apps that use the container)
Triggered by Maximum Offline Period MDX policy or NetScaler Gateway Session expiration/forced timeout (check-in with XenMobile to refresh policies through Worx Home and check on the NetScaler Gateway token)
Was it caused by my NetScaler Gateway session ending?
Yes
NetScaler Gateway Session time-out policy - Inactivity timer elapses
NetScaler Gateway Session forced time-out policy elapses1
No
Max Offline Period MDX policy expires.
NetScaler token is invalid because session time-out (inactivity) timer elapsed or was forced to elapse
Device flips to Worx Home and users must authenticate to the NetScaler Gateway.
Does the user have cached Active Directory with Worx PIN credentials or client certificate?
Yes
No
Users can enter a Worx PIN or passcode
Users must enter their Active Directory credentials
Reauthentication is required when users do the following:
Open an managed app after the inactivity timer expires (secondary container unlock)
When signing off Worx Home and then opening a managed app (primary and secondary container unlock)2
Is the App Passcode policy set to ON (default)?
Yes
No
No need to unlock the secondary container
Is Touch ID (iOS) configured?
Yes
No
Users can enter a Touch ID (iOS)
Users can enter a Worx PIN or passcode

1 If you set the session forced time-out policy to a lower value than for the inactivity time-out policy, the forced time-out policy overrides the inactivity time-out policy.
2 To see how these situations differ for iOS and Android devices, see the Credential Types section in Authentication Prompt Scenarios in the Citrix documentation.

About Secure Hub screen flips

Another situation to note is when a flip from an app to Secure Hub and then back to an app is required. The flip displays a notification that users must acknowledge. Authentication is not required when this occurs. The situation occurs after a check-in happens with Endpoint Management, as specified by the Maximum offline period and Active poll period MDX policies, and Endpoint Management detects updated policies that need to be pushed to the device through Secure Hub.

Enrolling devices by using derived credentials

January 25, 2019

Derived credentials provide strong authentication for mobile devices. The credentials, derived from a smart card, reside in a mobile device instead of the card. The smart card is either a Personal Identity Verification (PIV) card or Common Access Card (CAC).

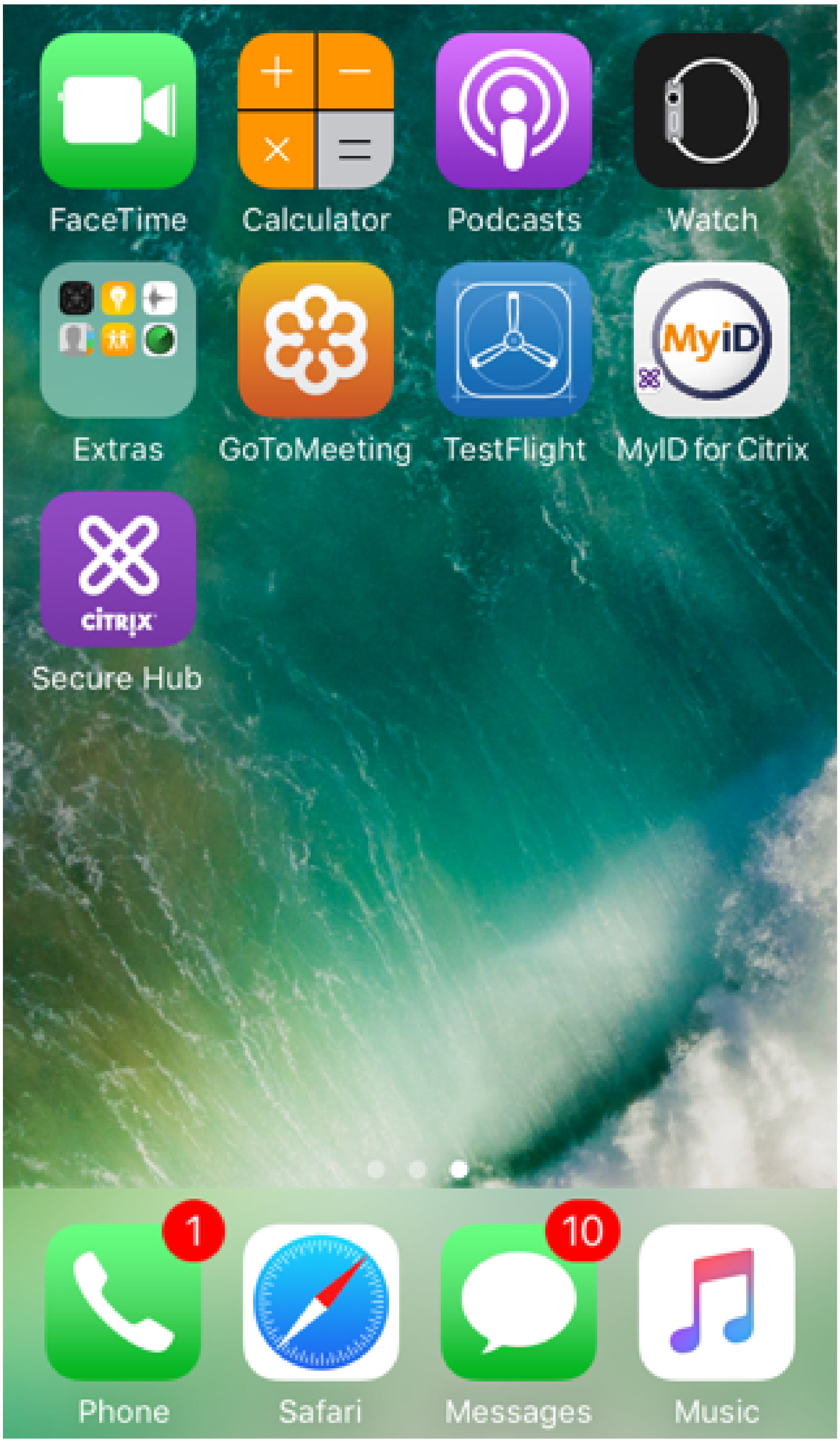
The derived credentials are an enrollment certificate that contains the user identifier, such as UPN. Endpoint Management stores the credentials obtained from the credential provider in a secure vault on the device.

Endpoint Management can use derived credentials for iOS device enrollment. If configured for derived credentials, Endpoint Management doesn't support enrollment invitations or other enrollment modes for iOS devices. However, you can use the same Endpoint Management server to enroll Android devices through enrollment invitations and other enrollment modes.

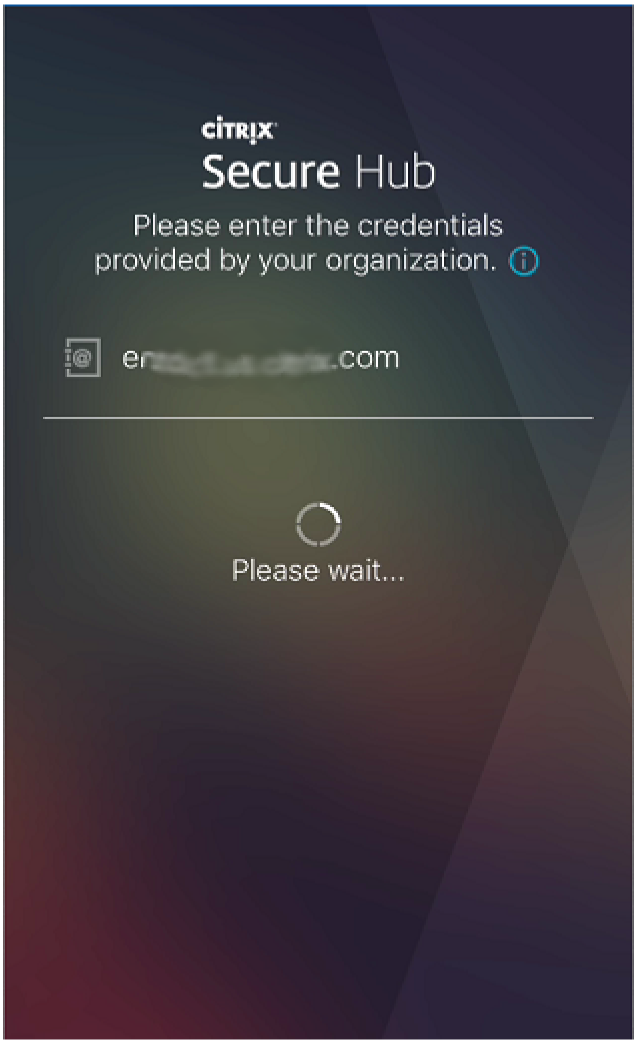
Device enrollment steps when using derived credentials

Enrollment requires that users insert their smart card to a reader attached to their desktop.

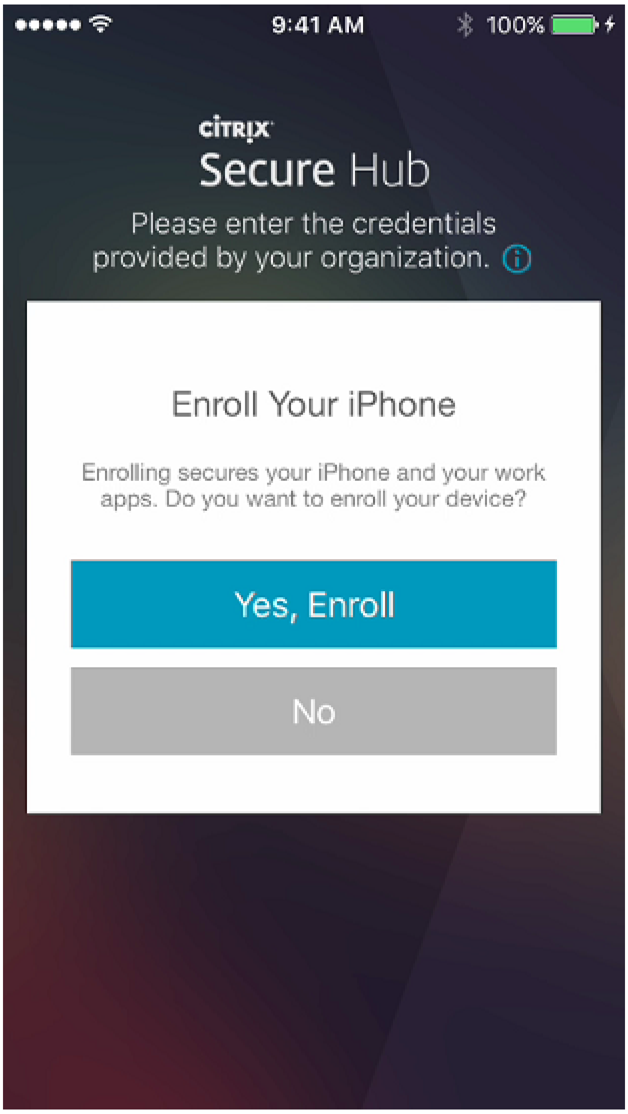
1. The user installs Secure Hub and the app from your derived credential provider. In this example, the identity provider app is the Intercede MyID Identity Agent.



2. The user starts Secure Hub. When prompted, the user types the Endpoint Management fully qualified domain name (FQDN) and then clicks **Next**. Enrollment in Secure Hub starts. If Endpoint Management supports derived credentials, Secure Hub prompts the user to create a Citrix PIN.



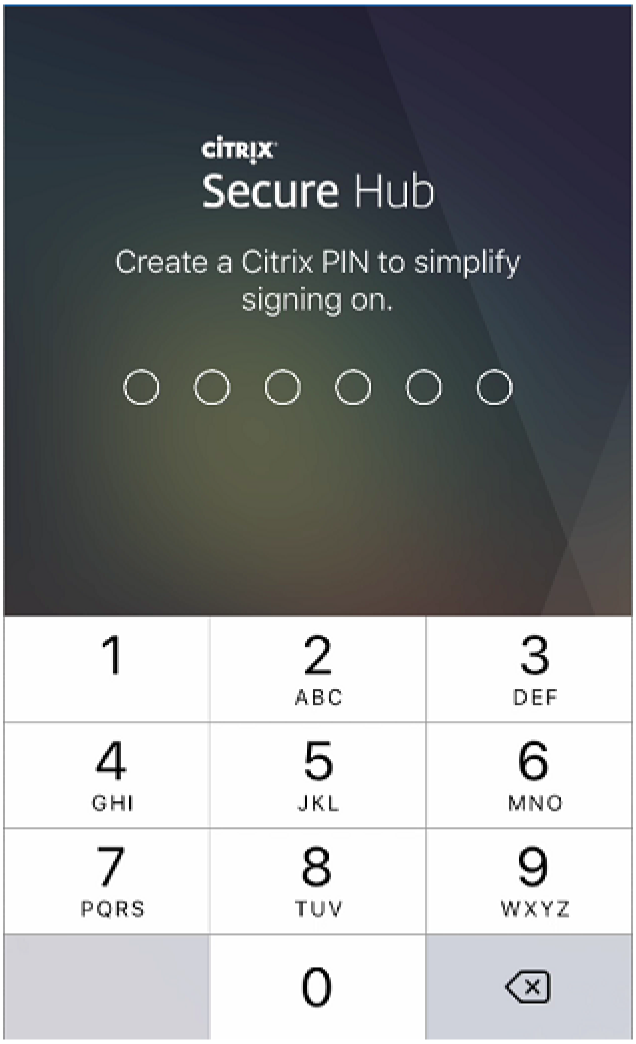
Please enter the credentials provided by your organization.



Please enter the credentials provided by your organization. ⓘ

Enroll Your iPhone

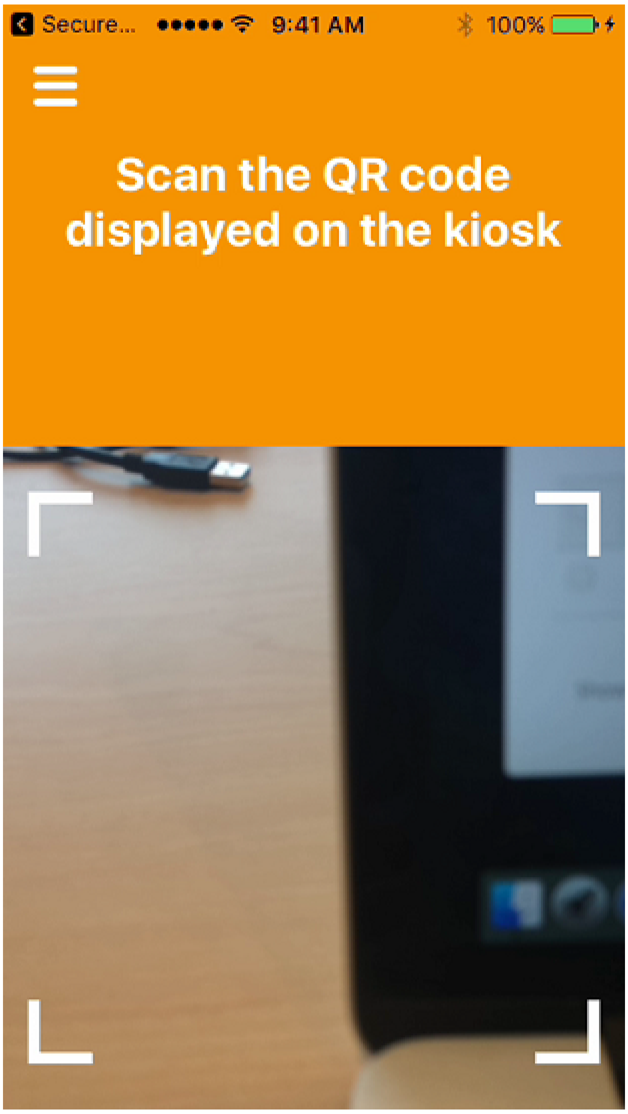
Enrolling secures your iPhone and your work apps. Do you want to enroll your device?



Secure Hub

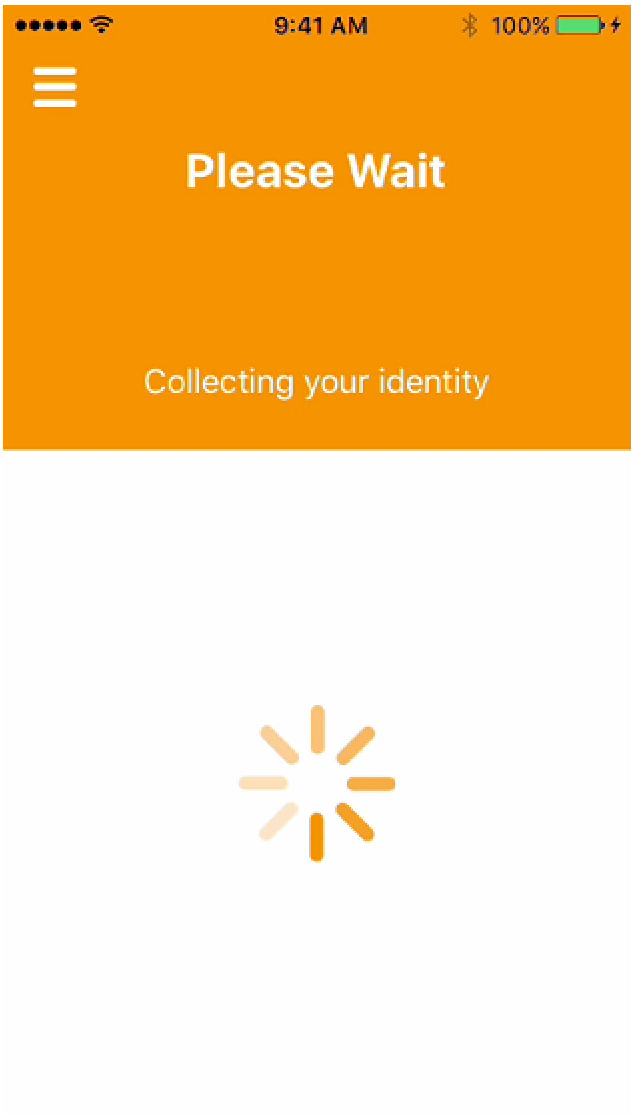
Create a Citrix PIN to simplify signing on.

3. The user follows the instructions to activate their smart credential. A splash screen appears, followed by a prompt to scan a QR code.



Scan the QR code displayed on the kiosk

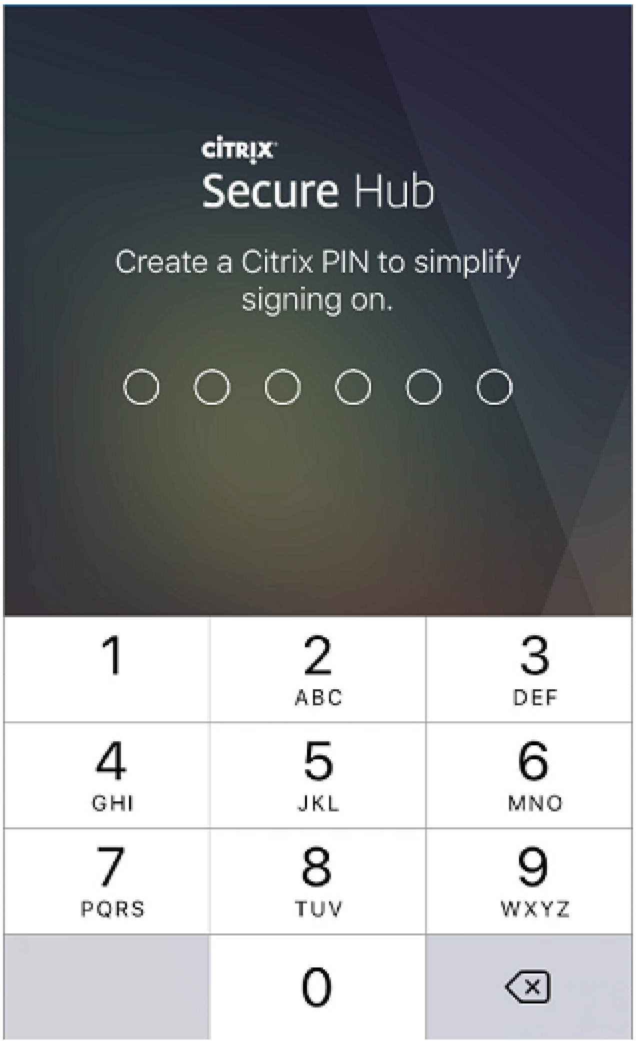
4. The user inserts their card into the smart card reader that's attached to their desktop. The desktop app then displays a QR code and prompts the user to scan the code using their mobile device.



Please Wait

Collecting your identity

The user enters their Secure Hub PIN when prompted.



Create a Citrix PIN to simplify signing on.

After authenticating the PIN, Secure Hub downloads the certificates. The user then follows the prompts to complete enrollment.

To view device information in the Endpoint Management console, do one of the following:

- Go to **Manage > Devices** and then select a device to display a command box. Click **Show more.**
- Go to **Analyze > Dashboard**.

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