Secure Hub

Contents

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Secure Hub

April 22, 2024

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 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 in Oct 2023.

What's new in the current version

Secure Hub for Android 24.3.0

Supports Samsung Knox Enhanced Attestation v3 Secure Hub now supports Samsung Enhanced Attestation v3, leveraging Knox attestation to strengthen security measures for Samsung devices managed through Citrix Endpoint Management. This advanced attestation protocol verifies the integrity and security status of the devices, ensuring they are not rooted and are running authorized firmware. The feature provides an essential layer of protection against security threats and ensures adherence to enterprise security policies.

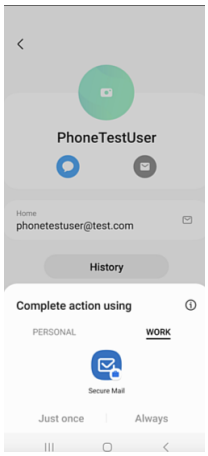
Secure Hub for Android 23.12.0

Enhanced Security with Samsung Knox The addition of the Knox Platform for Enterprise Key device policy in Citrix Endpoint Management significantly enhances the security features of Secure Hub on Samsung devices. This policy allows you to provide the required Samsung Knox Platform for Enterprise (KPE) license information and use the KPE licenses to enhance the security of your Samsung device. Samsung Knox ensures that enterprise data remains protected, while also maintaining ease of management and a smooth user experience.

For more information, see Knox Platform for Enterprise Key device policy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Access Secure Mail from user's personal profile Users can now access and use Secure Mail in their work profile from their personal profile. When users click an email address in their personal profile address book, they get an option to use Secure Mail in their work profile. This feature offers convenience, allowing users to send an email from their personal profile. This feature is applicable on BYOD or WPCOD devices.



What's new in earlier versions

Secure Hub for iOS 24.1.0

This release addresses a few issues that help to improve overall performance and stability.

Secure Hub for Android 23.12.0

Add a hint about authentication PIN on the sign-in page Starting with the 23.12.0 release, you can add a hint about the authentication PIN on the sign-in page. This feature is optional and applies to devices enrolled for two-factor authentication. The hint lets you know how to access the PIN.

You can configure a hint as text or a link. The hint text offers concise information about the PIN, while the link provides detailed information on how to access the PIN. For more information on how to configure a hint, see Configure hint through the Citrix Endpoint Management console.

nFactor authentication supports single sign-on feature Starting with Secure Hub for Android version 23.12.0, nFactor for Mobile Application Management (MAM) enrollment or login supports the single sign-on (SSO) feature. This feature allows previously entered sign-in credentials to pass through the MAM enrollment or login process, eliminating the need for users to enter them manually again. For more information on nFactor SSO property, see the Client property reference in Citrix Endpoint Management documentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Support full wipe in direct boot mode Previously, you needed to unlock the device to run a full wipe command on a rebooted device. Now, you can run a full wipe command in direct boot mode, even if the device is locked. This feature is helpful from a security viewpoint, especially when the device is in the possession of an unauthorized individual. For more information on the full wipe command, see the Security actions in Citrix Endpoint Management documentation.

Optimized the loading speed of Secure Hub's App Store The App Store in Secure Hub now loads faster than before, allowing users to access it more quickly.

Secure Hub for iOS 23.11.0

Add a hint about authentication PIN on the sign-in page Starting with the 23.11.0 release, you can add a hint about the authentication PIN on the sign-in page. This feature is optional and applies to devices enrolled for two-factor authentication. The hint lets you know how to access the PIN.

You can configure a hint as text or a link. The hint text offers concise information about the PIN, while the link provides detailed information on how to access the PIN. For more information on how to configure a hint, see the Configure hint through the Citrix Endpoint Management console article.

nFactor authentication supports single sign-on feature Starting with Secure Hub for iOS version 23.11.0, nFactor for Mobile Application Management (MAM) enrollment or sign-in supports the single sign-on (SSO) feature. This feature allows previously entered sign-in credentials to pass through the MAM enrollment or sign-in process, eliminating the need for users to enter them manually again.

For more information on nFactor SSO property, see the Client property reference in Citrix Endpoint Management documentation.

Secure Hub 23.10.0

Secure Hub for Android

Secure Hub for Android 23.10.0 supports Android 14. Upgrading the Secure Hub version to 23.10.0 ensures continuous support for devices that are updated to Android 14.

Secure Hub 23.9.0

Secure Hub for Android

This release addresses areas that improve overall performance and stability.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Hub 23.8.1

Secure Hub for iOS This release addresses a few issues that help to improve overall performance and stability.

Secure Hub 23.8.0

Secure Hub for iOS This release addresses a few issues that help to improve overall performance and stability.

Secure Hub 23.7.0

Secure Hub for Android

Play Integrity API The SafetyNet Attestation API will soon be deprecated by Google as per the deprecation timeline, and migrated to the suggested Play Integrity API.

For more information, see Play Integrity API in the Citrix Endpoint Management document.

For deprecation details, see Deprecations and removals in the Citrix Endpoint Management document.

To read about the Android SafetyNet feature, see SafetyNet

Secure Hub 23.4.0

Secure Hub for iOS

Improved user experience Starting with the 23.4.0 version, Secure Hub for iOS improves the following user experiences:

- Store experience:

  ⊠ Previously, the My Apps page appeared first. With the 23.4.0 version, the Store page appears first.

  ⊠ Previously, the Secure Hub store performed the reload action every time the user clicked the Store option.

  With the 23.4.0 version, the user experience is improved. Now, the app reloads when the user launches the app for the first time, restarts the app, or swipes down the screen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- User interface: Previously, the Sign Off option was placed at the bottom left of the screen. With the 23.4.0 version, the Sign Off option is part of the main menu and is above the About option.
- Hyperlinks: Previously, the hyperlinks on the app's detail page appeared as plain text. With the 23.4.0 version, the hyperlinks are clickable and have an underline formatting to indicate links.

MDX to MAM SDK transition experience Starting with the 23.4.0 version, the transition experience from legacy MDX to MAM SDK is enhanced for iOS dual-mode apps. This feature improves the user experience when using mobile productivity apps by reducing alert messages and switching to Secure Hub.

Use Citrix PIN to unlock apps Previously, end user entered the device passcode to unlock apps that is based on Mobile App Management (MAM).

Starting with the 23.4.0 version, end user can enter Citrix PIN as the passcode to unlock MAM based app. Administrators can configure the complexity of the passcode using the client properties on the CEM server.

Whenever the app is inactive for more than the allowed time, end users can enter the Citrix PIN to unlock the app depending upon the configuration set by the administrators.

For Secure Hub for Android, there is a separate client property to configure how to handle with inactivity timer in MAM applications. For more information, see Separate Inactivity Timer for Android.

Secure Hub 23.4.1

Secure Hub for Android This release addresses a few issues that help to improve overall performance and stability.

Secure Hub 23.4.0

Secure Hub for Android This release addresses a few issues that help to improve overall performance and stability.

Secure Hub 23.2.0

Secure Hub for Android

> **Note:**
>
> - No analytical data is collected for the users in European Union (EU), European Economic Area (EEA), Switzerland, and United Kingdom (UK).

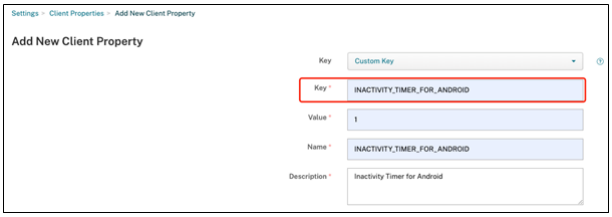
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

MDX full tunnel mode VPN The MDX Micro VPN (full tunnel mode) is deprecated.

For more information, see Deprecation in the Citrix Endpoint Management documentation.

Separate Inactivity Timer for Android Previously, the **Inactivity Timer** client property was common for Secure Hub for Android and iOS.

Starting with the 23.2.0 version, an IT administrator can use the new client property **Inactivity_Timer_For_Android** to separate the inactivity timer from iOS. An IT administrator can set the **Value** of the **Inactivity_Timer_For_Android** to 0 to disable Android inactivity timer independently. In this way, all apps in work profile, including Secure Hub, challenges work PIN only.



For more information on how to add and modify a client property, see Client properties in the XenMobile documentation.

Secure Hub 22.11.0

Secure Hub for Android This release includes bug fixes.

Secure Hub 22.9.0

Secure Hub for Android This release includes:

- Passcode complexity for device passcode (Android 12+)
- Support for SDK 31
- Bug fixes

Passcode complexity for device passcode (Android 12+) Passcode complexity is preferred than a custom password requirement. The passcode complexity level is one of the pre-defined levels. Thus, the end user is unable to set a password with a lower complexity level.

Passcode complexity for devices on Android 12+ is as follows:

- **Apply passcode complexity:** Requires a password with a complexity level defined by the platform, rather than a custom password requirement. Only for devices on Android 12+ and using Secure Hub 22.9 or later.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Complexity level:** Predefined levels of password complexity.
  - **None:** No password required.
  - **Low:** Passwords can be:
    - A pattern
    - A PIN with a minimum of four numbers
  - **Medium:** Passwords can be:
    - A PIN with no repeating sequences (4444) or ordered sequences (1234), and a minimum of four numbers
    - Alphabetic with a minimum of four characters
    - Alphanumeric with a minimum of four characters
  - **High:** Passwords can be:
    - A PIN with no repeating sequences (4444) or ordered sequences (1234), and a minimum of eight numbers
    - Alphabetic with a minimum of six characters
    - Alphanumeric with a minimum of six characters

> **Notes:**
>
> - For BYOD devices, passcode settings such as Minimum length, Required characters, Biometric recognition, and Advanced rules are not applicable on Android 12+. Use passcode complexity instead.
> - If passcode complexity for work profile is enabled, then passcode complexity for the device side must be enabled too.

For more information, see Android Enterprise settings in the Citrix Endpoint Management documentation.

Secure Hub 22.7.0

Secure Hub for Android This release includes bug fixes.

Secure Hub 22.6.0

Secure Hub for Android This release includes bug fixes.

Secure Hub 22.5.0

Secure Hub for iOS This release includes bug fixes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Hub 22.4.0

Secure Hub for Android This release includes bug fixes.

Secure Hub 22.2.0

Secure Hub for iOS This release includes bug fixes.

Secure Hub for Android This release includes bug fixes.

Secure Hub 21.11.0

Secure Hub for Android

Support for Work profile for company-owned devices In Android Enterprise devices, you can now enroll Secure Hub in the Work profile for company-owned devices mode. This feature is available on devices running Android 11 or later. Devices previously enrolled in the Corporate Owned Personally Enabled (COPE) mode automatically migrate to the Work profile for company-owned devices mode, when the device upgrades from Android 10 to Android 11 or later.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Secure Hub for iOS This release includes bug fixes.

Secure Hub for Android 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

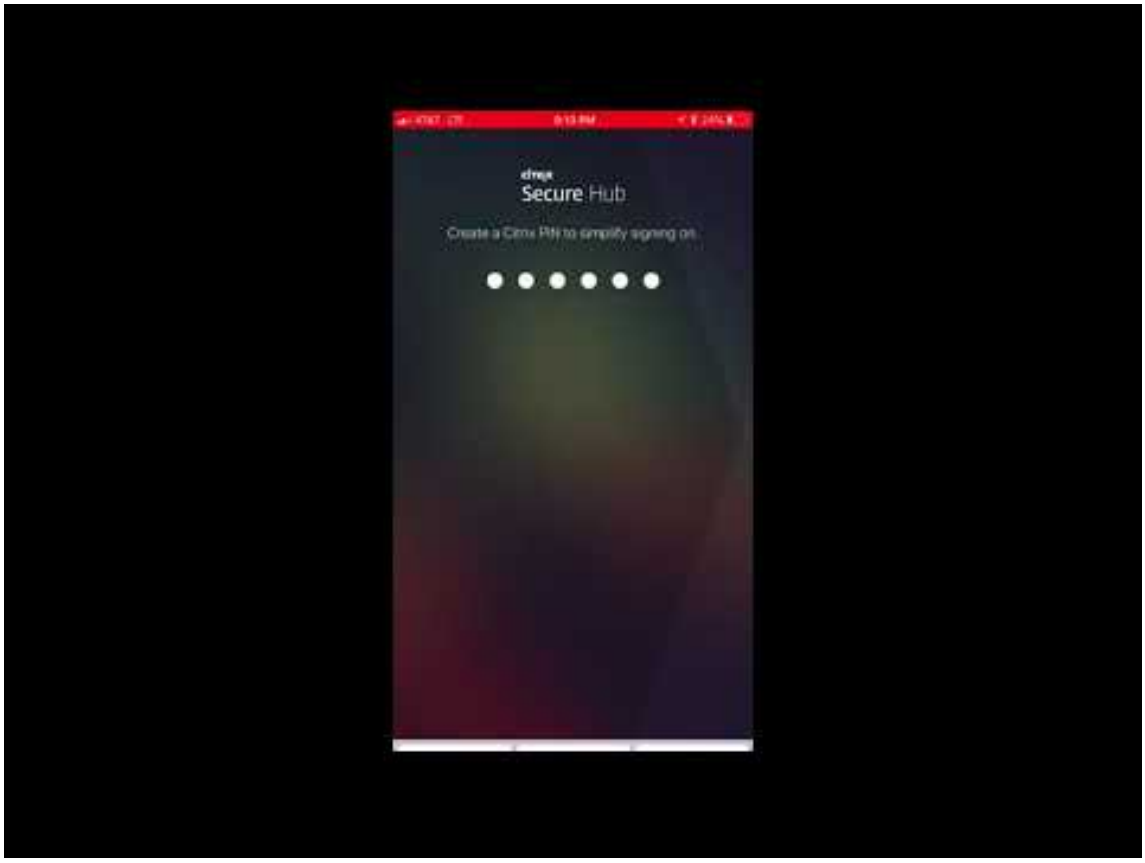
- **Prevent camera use for Android Enterprise devices:** The new **Allow use of camera** setting for the Restrictions device policy lets you prevent users from using the camera on their Android Enterprise devices. For information, see Restrictions device policy.

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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

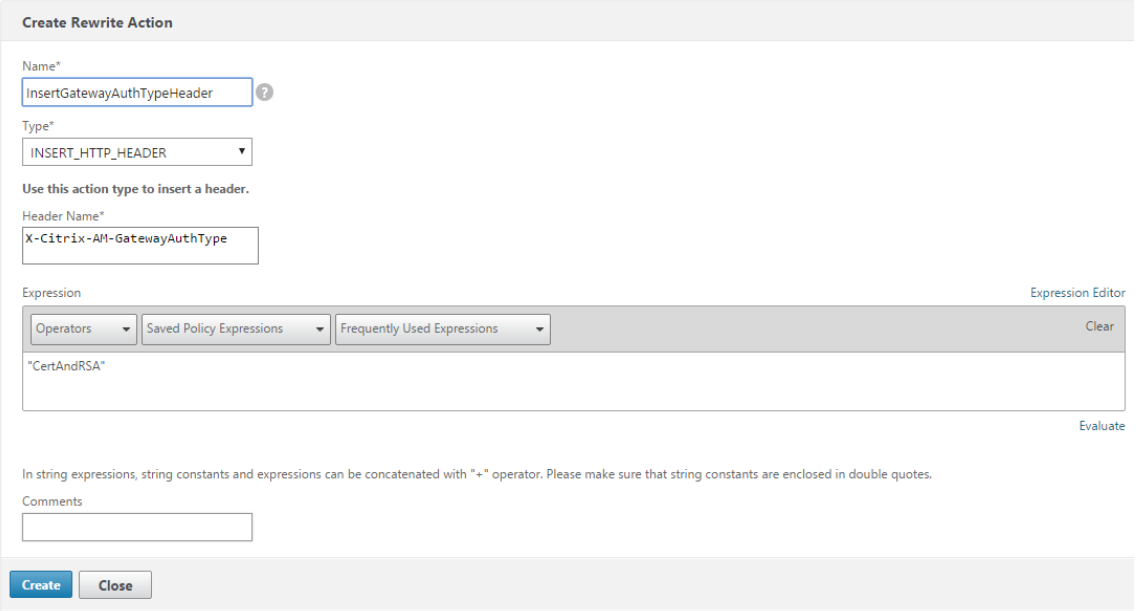
Ordinarily, Secure Hub uses the Citrix Gateway logon type configured in the Endpoint Management console. However, this information isn't available to Secure Hub until Secure Hub completes logon for the first time. Therefore, the custom header is required.

> **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.

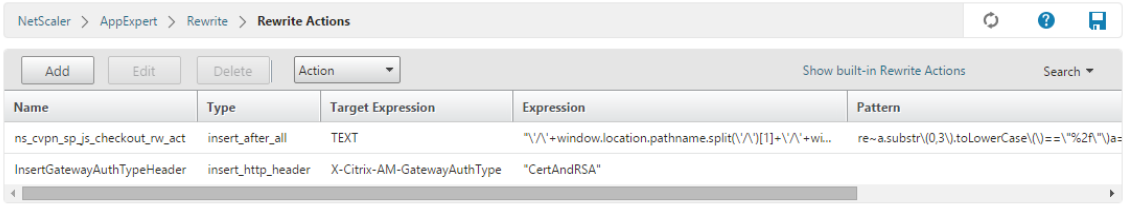
1. In Citrix ADC, navigate to **Configuration > AppExpert > Rewrite > Actions**.
2. Click **Add**.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

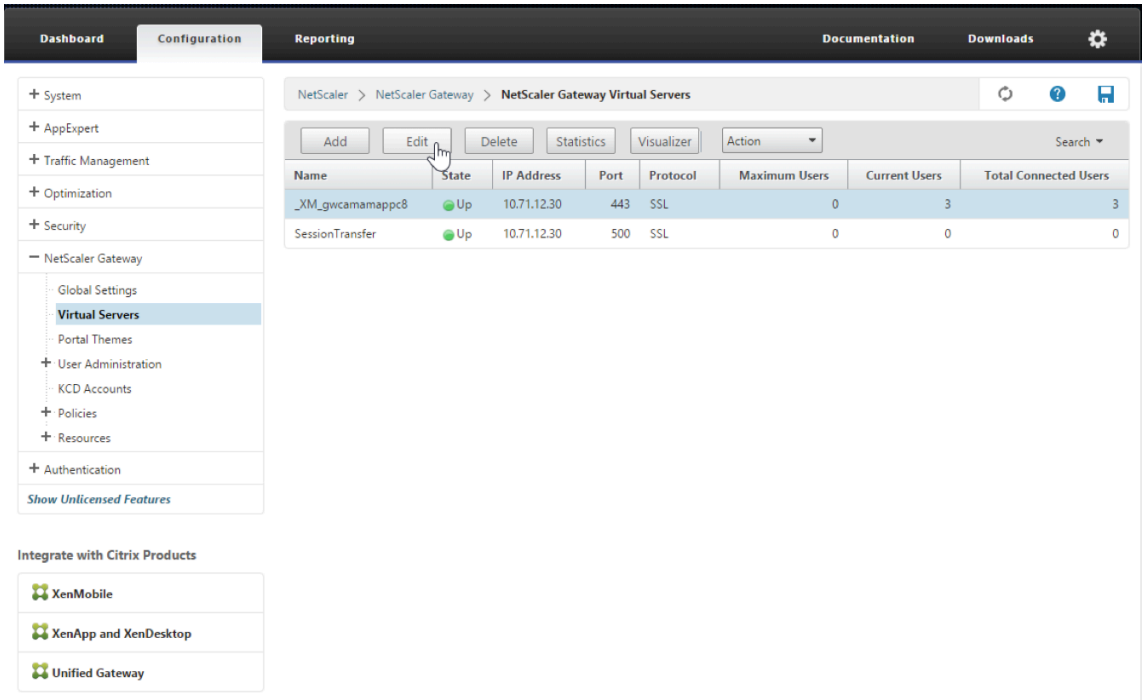


The following result appears on the main **Rewrite Actions** screen.

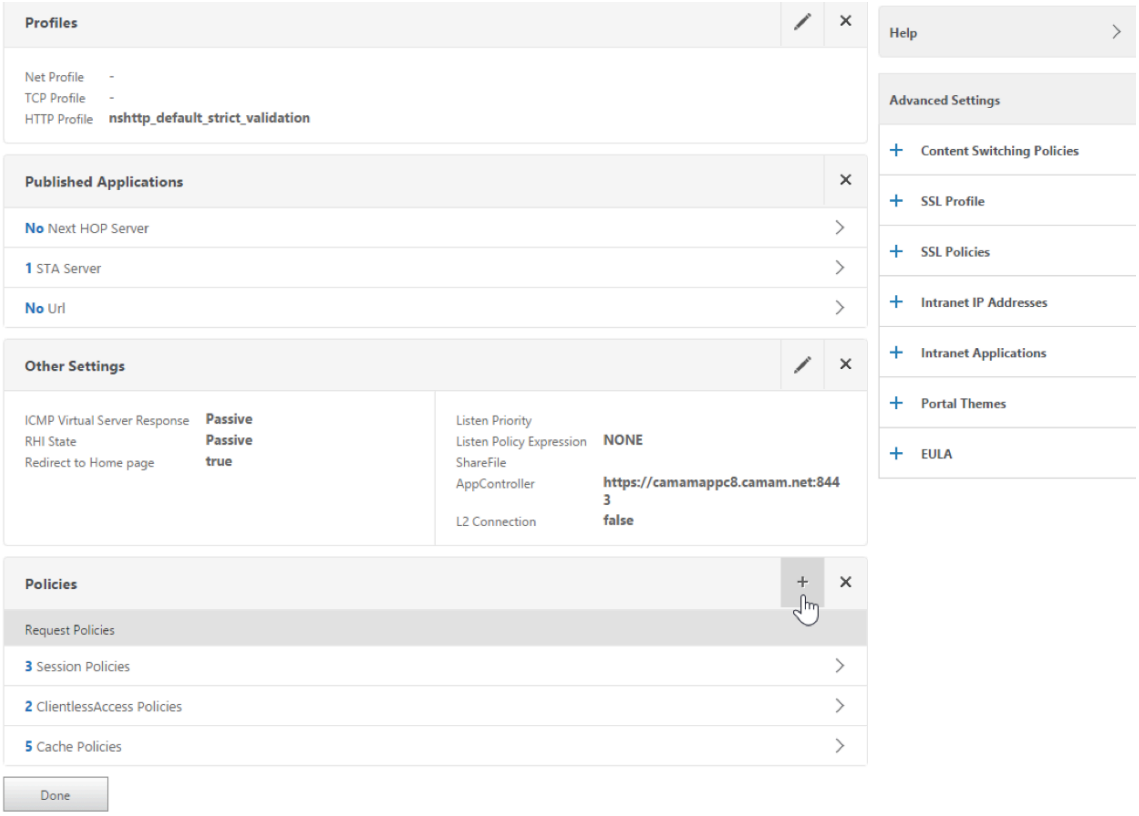


4. Bind the rewrite action to the virtual server as a rewrite policy. Go to **Configuration > NetScaler Gateway > Virtual Servers** and then select your virtual server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

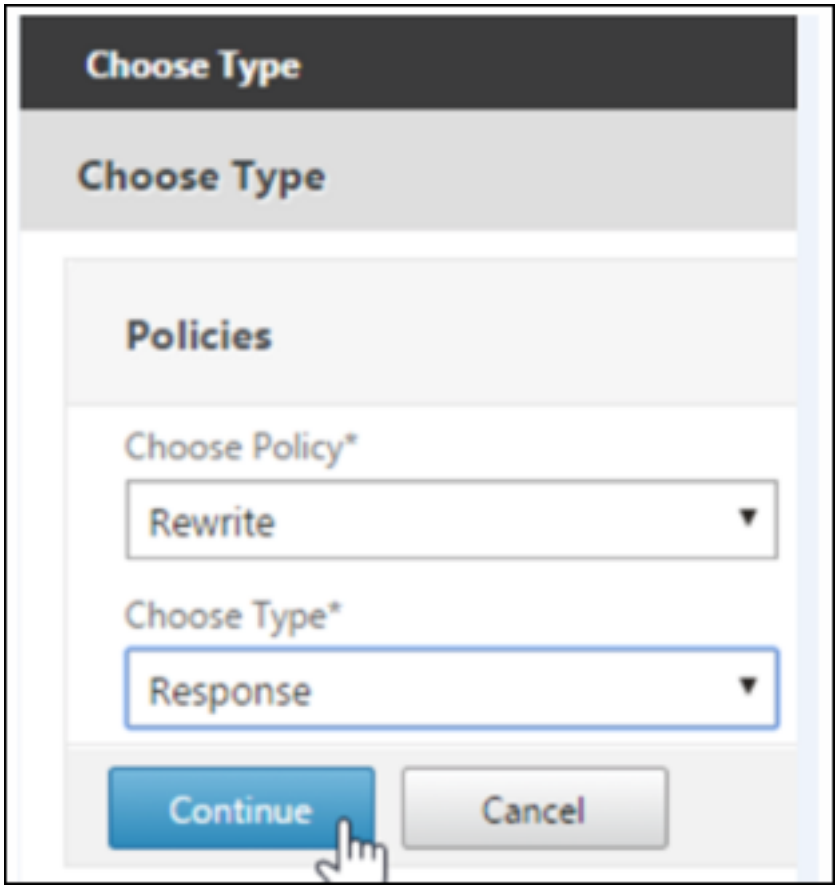


5. Click **Edit**.
6. On the **Virtual Servers configuration** screen, scroll down to **Policies**.
7. Click **+** to add a policy.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

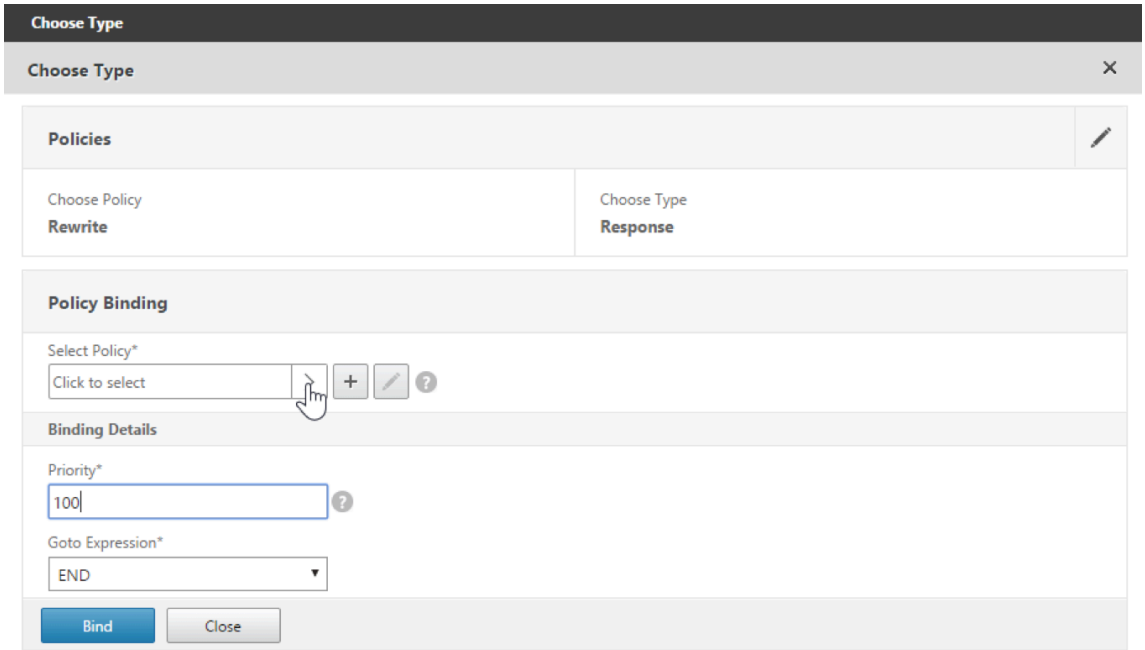
8. In the **Choose Policy** field, choose **Rewrite**.
9. In the **Choose Type** field, choose **Response**.



10. Click **Continue**.

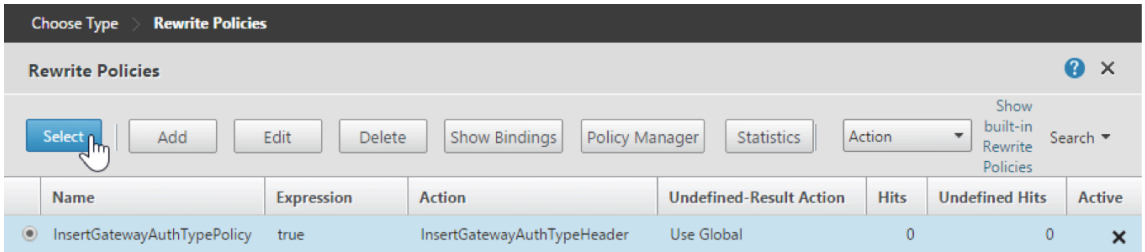
    The **Policy Binding** section expands.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



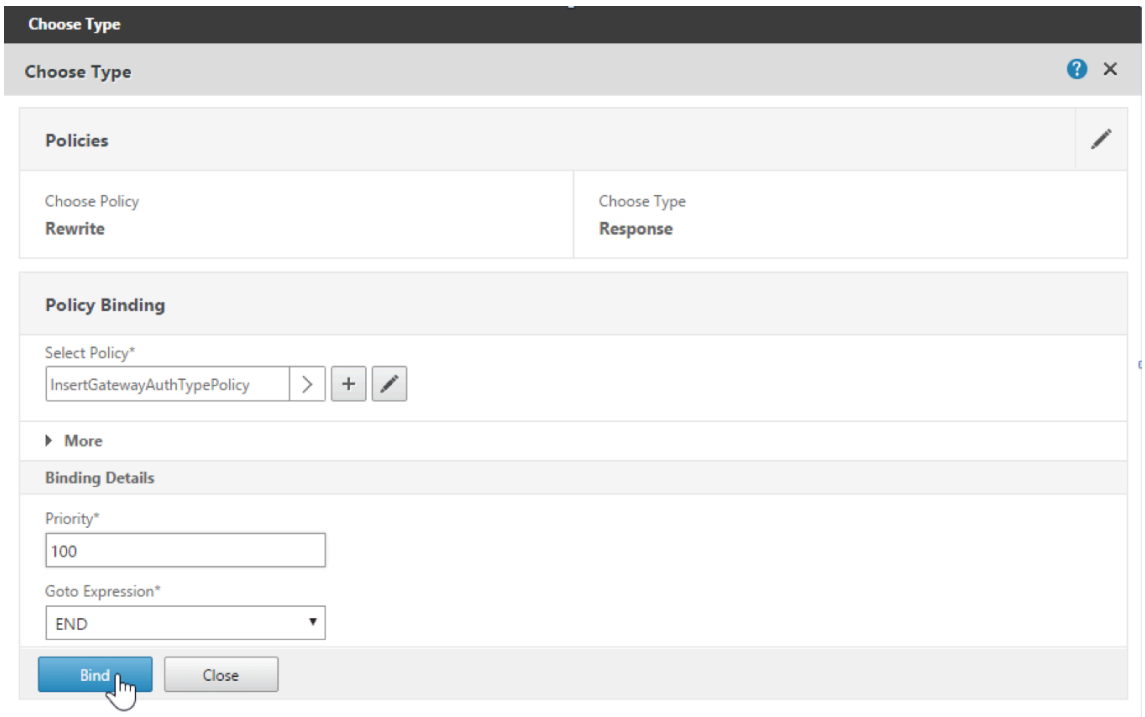
11. Click **Select Policy**.

    A screen with available policies appears.



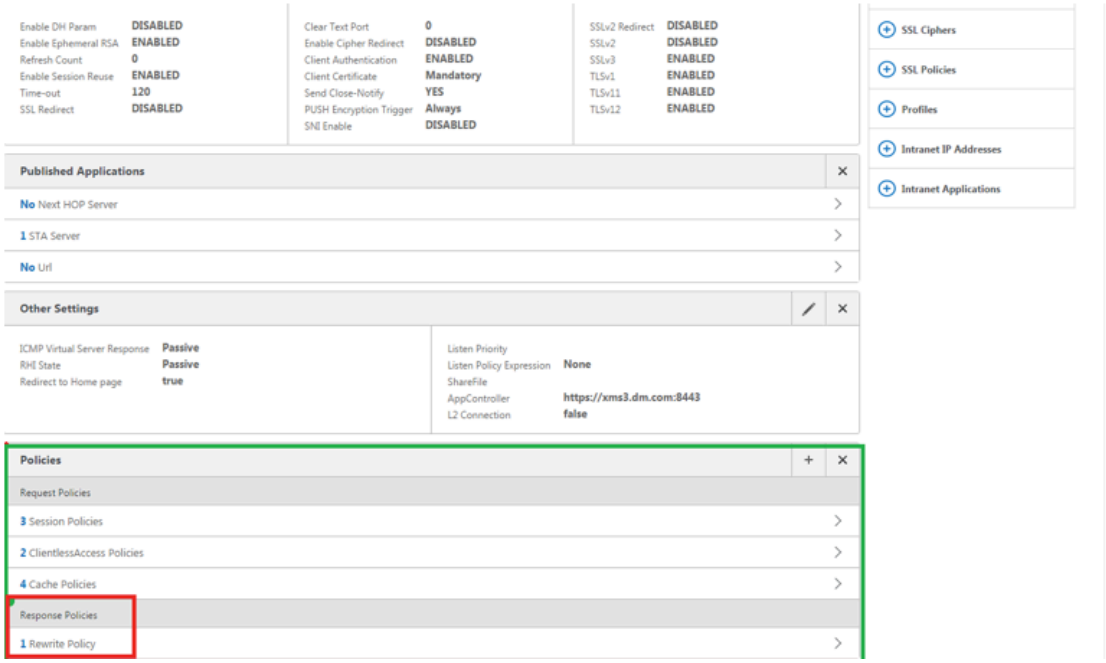
12. Click the row of the policy you created and then click **Select**. The **Policy Binding** screen appears again, with your selected policy filled in.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



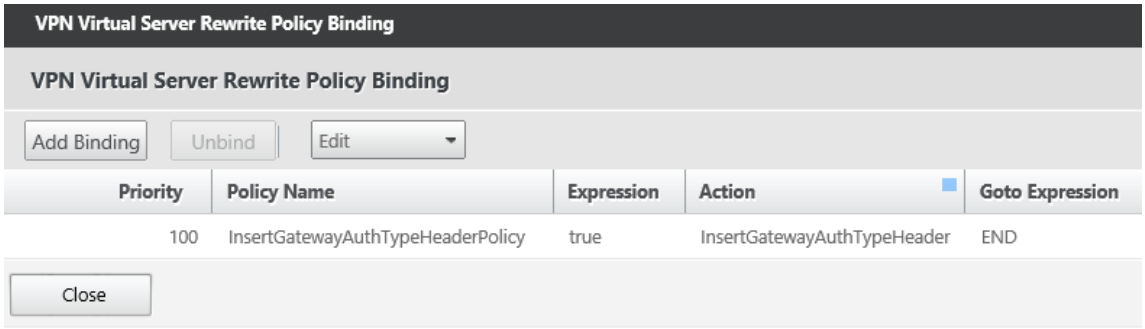
13. Click **Bind**.

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



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

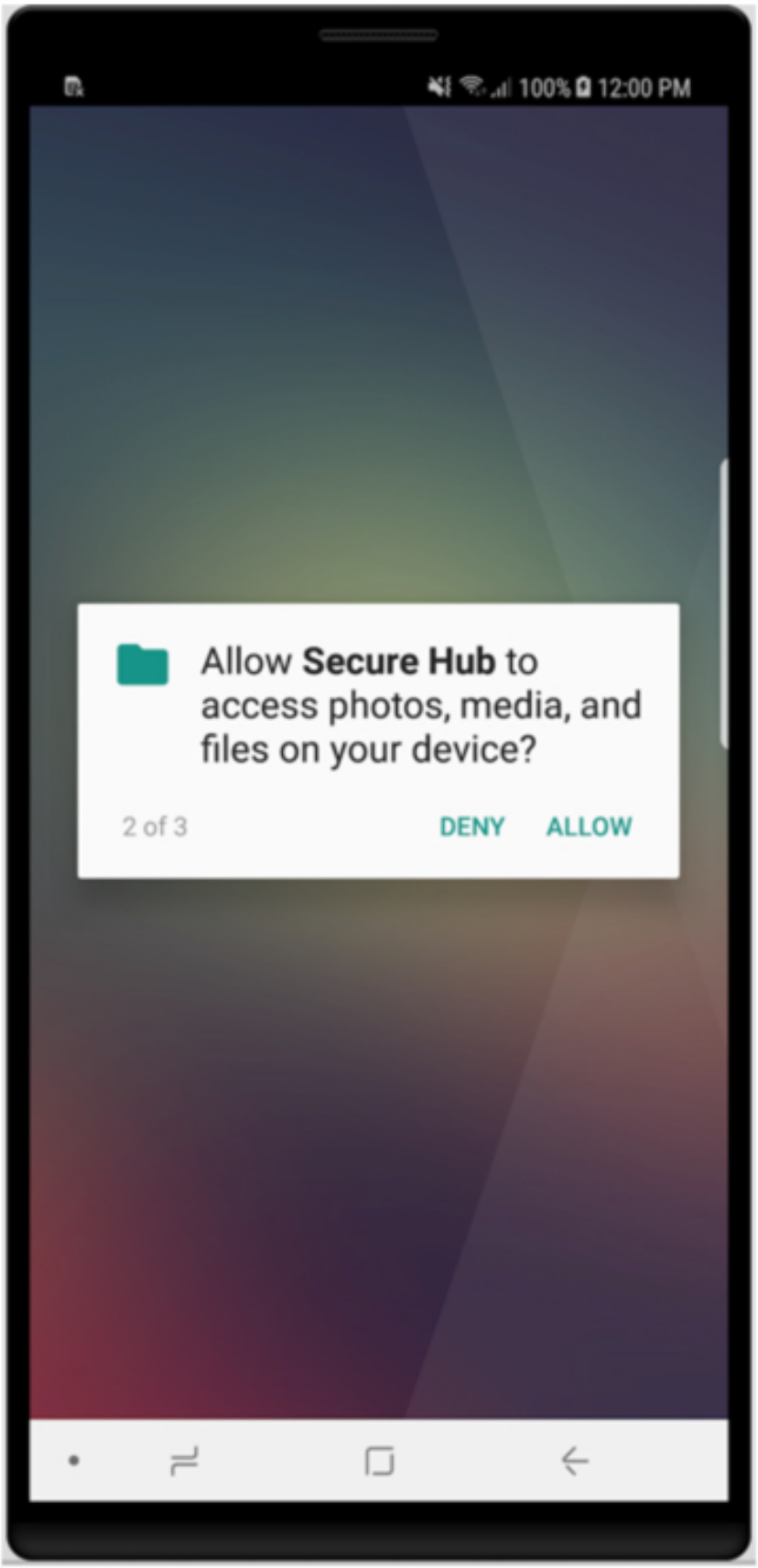
When Secure Hub opens, users enter the credentials provided by their companies to enroll their devices in Secure Hub. For more details about device enrollment, see User accounts, roles, and enrollment.

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.

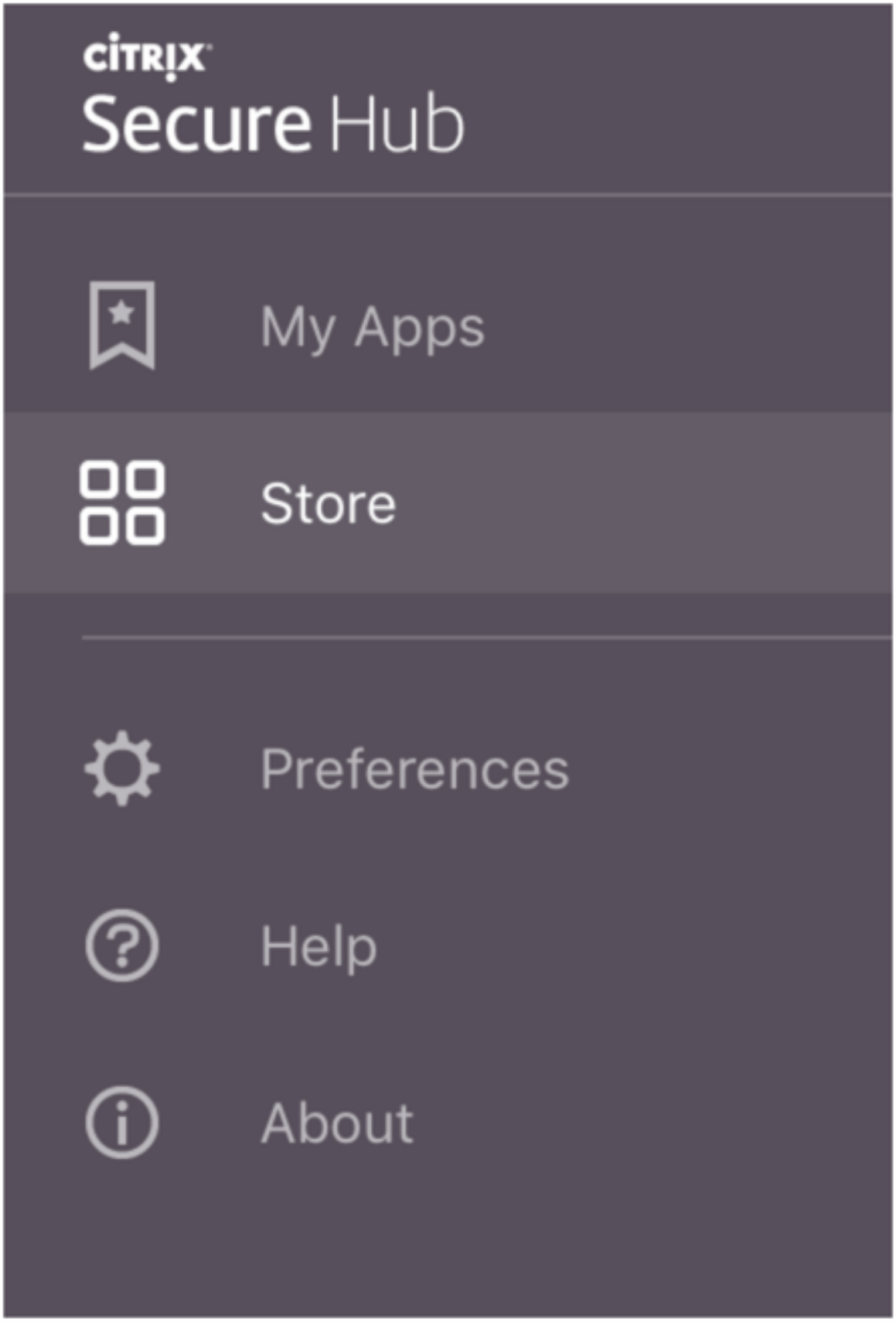
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

On tablets, the Store is a separate tab.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

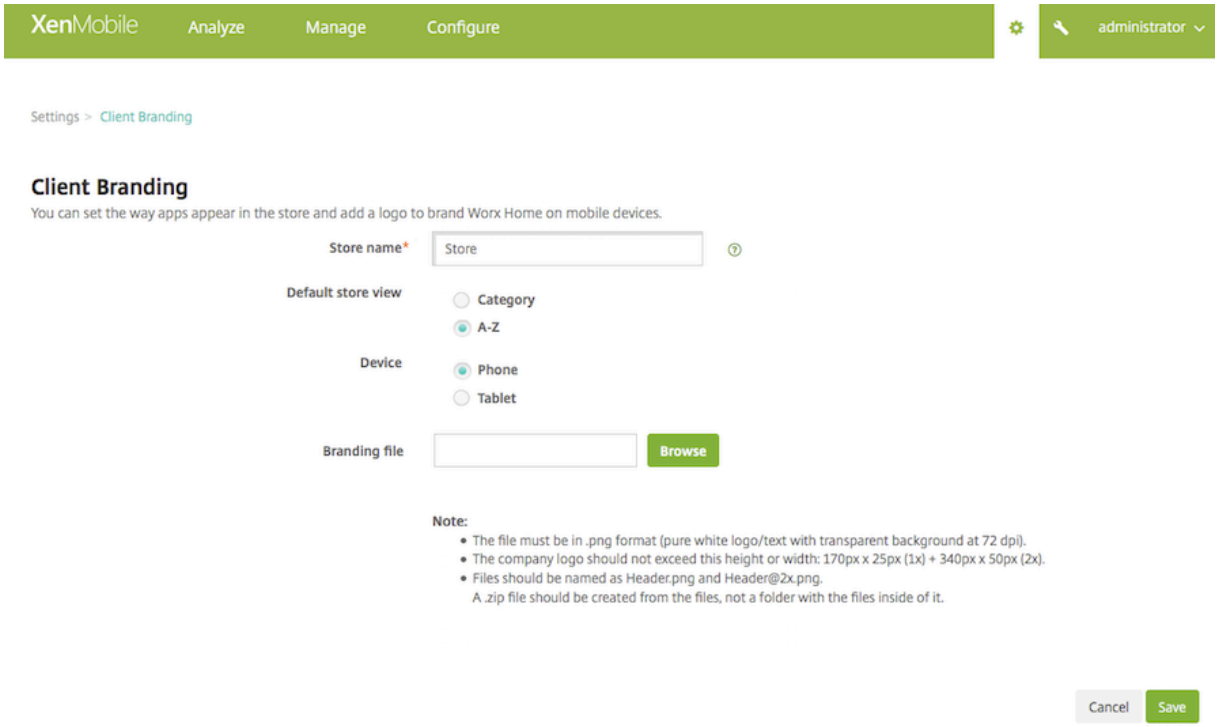
To enable this feature, create three properties:

- 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.

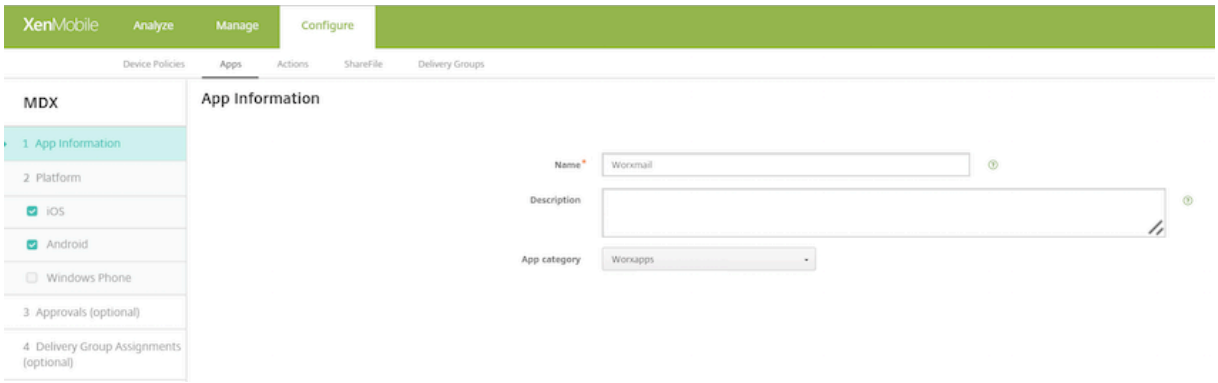
Customized Store

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

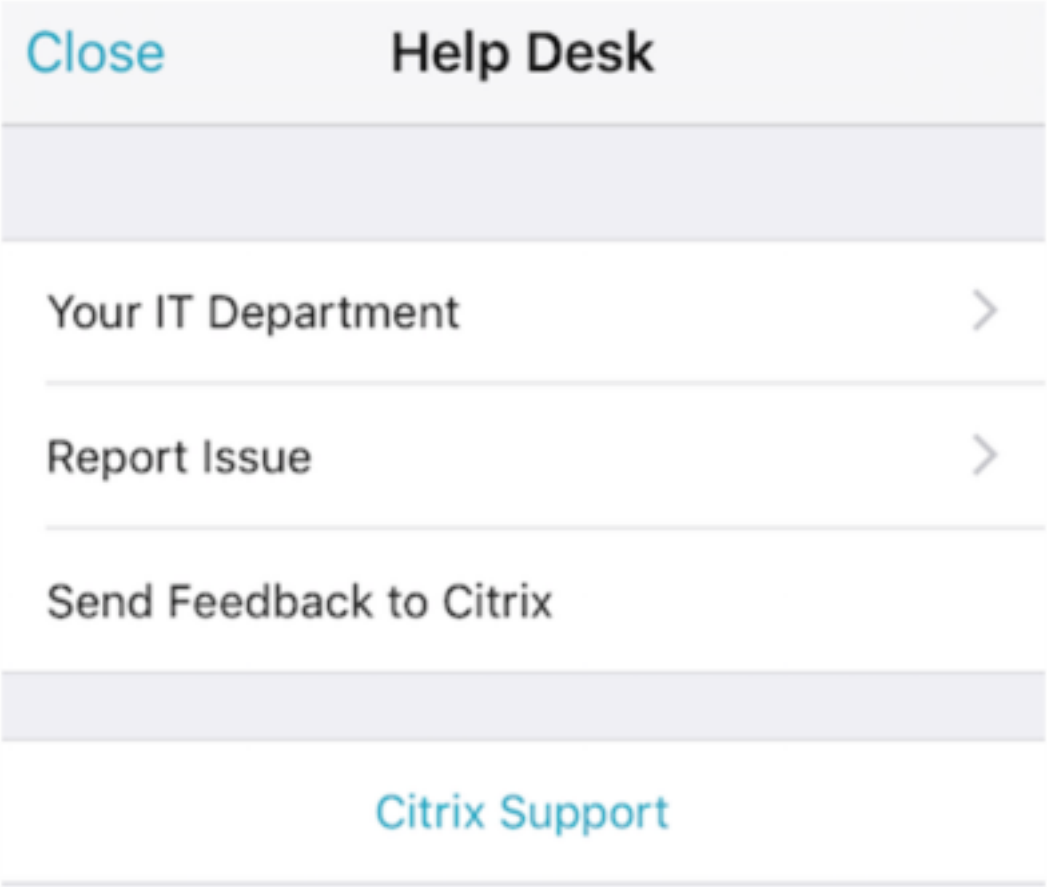


In the Store, users can browse only those apps and desktops that you've configured and secured in Endpoint Management. To add the app, users tap **Details** and then tap **Add**.

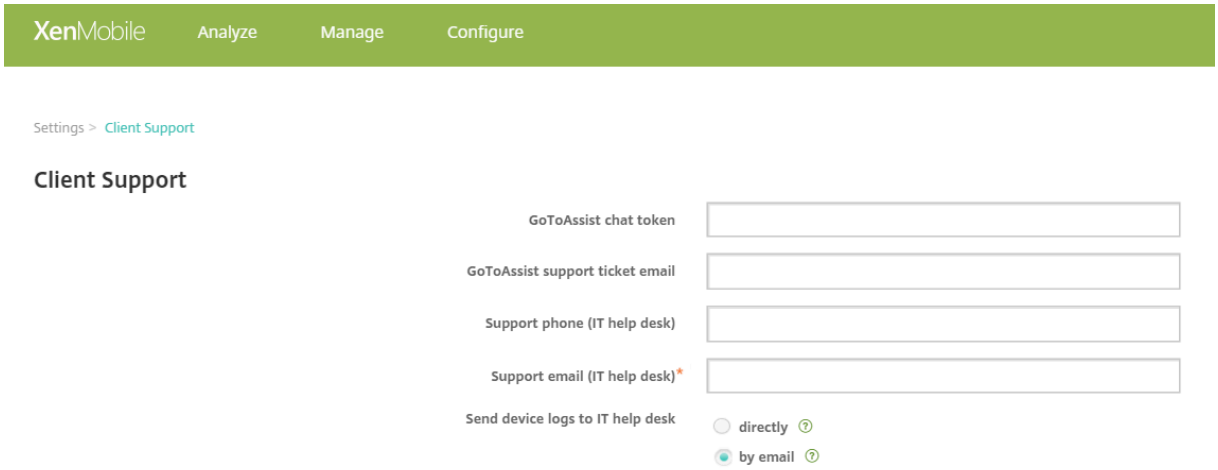
Configured Help options

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.



Report Issue shows a list of apps. Users select the app that has the issue. Secure Hub automatically

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Generate device side logs for Secure Hub

This section explains how to generate the Secure Hub device side logs and to setup the correct debug level on them.

To obtain the Secure Mail logs do the following:

1. Go to **Secure Hub > Help > Report Issue**. Select Secure Mail from the list of apps.
   An email addressed to your organization help desk opens.
2. Change log settings only if your support team has instructed you to do so. Always confirm that the settings are properly set.
3. Return to Secure Mail and reproduce the issue. Note the time when the issue started to be reproduced, and the time when the issue happens or error message is displayed.
4. Return to **Secure Hub > Help > Report Issue**. Select Secure Mail from the list of apps.
   An email addressed to your organization help desk opens.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Fill in the subject line and body with a few words describing your issue. Include the timestamps gathered in step 3, and click **Send**.
   The completed message opens with zipped log files attached.
6. Click **Send** again.

   The zip files sent include the following logs:

   - CtxLog_AppInfo.txt (iOS), Device_And_AppInfo.txt (Android), logx.txt, and WH_logx.txt (Windows Phone)

   App info logs include information about the device and app.

Known and fixed issues

April 11, 2024

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

Secure Hub for Android 24.3.0

Fixed issues

Users can perform a factory reset on company-owned Android Enterprise devices even when the restriction policy for factory reset is set to NO. This issue occurs when a user relaunches the Secure hub. [XMHELP-4479]

Known issues

There are no known issues in this release.

Secure Hub for iOS 24.1.0

Fixed issues

- When you jailbreak an iOS device with the Palera1n app, the Citrix Endpoint Management server doesn't detect the device as jailbroken. As a result, the Endpoint Management server can't factory reset the jailbroken device. In addition, the Endpoint Management server can't clear the jailbroken device entries from the server console. [XMHELP-4397]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- When you use the MAM SDK to manage your iOS apps, the Secure Hub store comes across either one of the following issues:
  - It doesn't notify when an update is available for the apps.
  - It continuously notifies about updates even after the apps are updated.

[XMHELP-4427]

- When you use the MAM SDK to manage your iOS apps, the following compliance alert might appear:

"This app has been removed from your account. You can remove it from your device."

The issue occurs when you install both MAM SDK and MDX toolkit on the same iOS device. [XMHELP-4463]

Secure Hub for Android 23.12.0

Fixed issues

When the Citrix Gateway credential expires, Secure Hub might not generate a new certificate to connect to the Citrix Gateway server. As a result, Secure Hub fails to start with the following error message.

"An error has occurred in your connection. Try connecting again"

[XMHELP-4446]

Secure Hub for iOS 23.11.0

Fixed issues

- The Secure Hub authentication fails on iOS devices, as the Citrix Gateway client certificate doesn't auto-renew when it expires. The issue occurs when the Citrix Gateway uses the TLSv1.3 protocol. [XMHELP-4396]
- When you sign in to Secure Hub through the Citrix Gateway, you might get the following error message:

  "Could not sign on. Incorrect credentials. Ending the session"

  The issue occurs when you enroll your iOS device in Citrix Endpoint Management (CEM) with nFactor. [XMHELP-4423]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Hub for Android 23.10.0

Fixed issues

On Android version 11 and later, the Wi-Fi policy on Android Enterprise devices might not deploy. This issue occurs when the domain value isn't specified in the Anonymous field on the Wi-Fi policy. [XMHELP-4379]

Known issues

There are no known issues in this release.

Secure Hub for Android 23.9.0

Fixed issues

This release addresses areas that improve overall performance and stability.

Known issues

There are no known issues in this release.

Secure Hub for iOS 23.8.1

Fixed issues

- When a user tries to enroll the devices using Secure Hub 23.8.0, and the user name is of the format `sAMAccount`, the process might fail with the following error message:

  "Enrollment Failed, The MAM logged in user does not match enrolled user, please try enroll again."[XMHELP-4410]

Known issues

There are no known issues in this release.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Hub for iOS 23.8.0

Fixed issues

- When you enroll your iOS device in Citrix Endpoint Management (CEM) with nFactor, you might have issues establishing a micro VPN tunnel. [XMHELP-4390]

Known issues

There are no known issues in this release.

Known and fixed issues in older versions

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

Authentication prompt scenarios

October 12, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

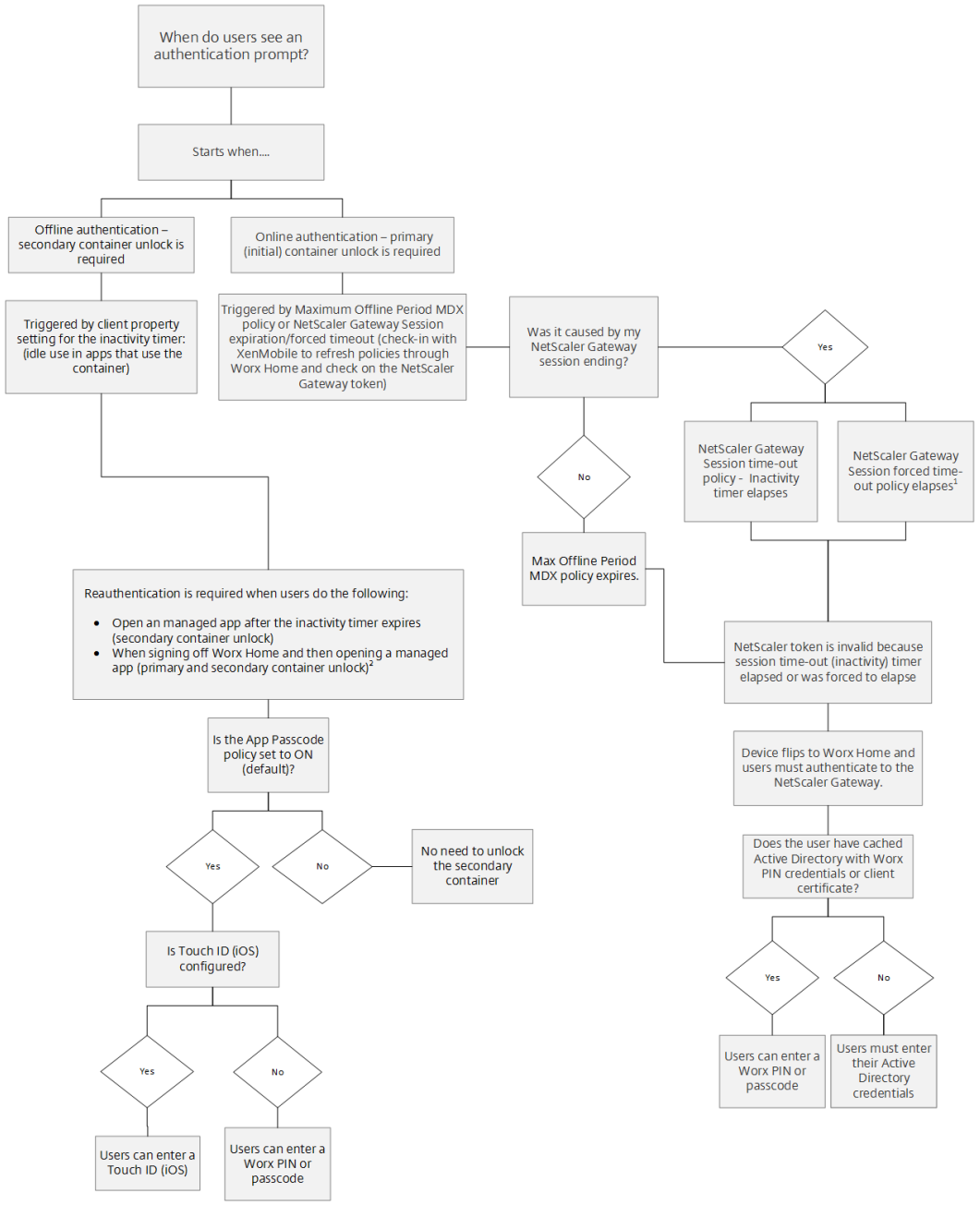
Active Directory credentials are required for either container unlock circumstance when the following conditions are true:

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Passcode complexity for device passcode (Android 12+)

Passcode complexity is preferred than a custom password requirement. The passcode complexity level is one of the pre-defined levels. Thus, the end user is unable to set a password with a lower complexity level.

Passcode complexity for devices on Android 12+ is as follows:

- **Apply passcode complexity:** Requires a password with a complexity level defined by the platform, rather than a custom password requirement. Only for devices on Android 12+ and using Secure Hub 22.9 or later.
- **Complexity level:** Predefined levels of password complexity.
  - **None:** No password required.
  - **Low:** Passwords can be:
    * A pattern
    * A PIN with a minimum of four numbers
  - **Medium:** Passwords can be:
    * A PIN with no repeating sequences (4444) or ordered sequences (1234), and a minimum of four numbers
    * Alphabetic with a minimum of four characters
    * Alphanumeric with a minimum of four characters
  - **High:** Passwords can be:
    * A PIN with no repeating sequences (4444) or ordered sequences (1234), and a minimum of eight numbers
    * Alphabetic with a minimum of six characters
    * Alphanumeric with a minimum of six characters

> **Notes:**
>
> - For BYOD devices, passcode settings such as Minimum length, Required characters, Biometric recognition, and Advanced rules are not applicable on Android 12+. Use passcode complexity instead.
> - If passcode complexity for work profile is enabled, then passcode complexity for the device side must be enabled too.

For more information, see Android Enterprise settings in the Citrix Endpoint Management documentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

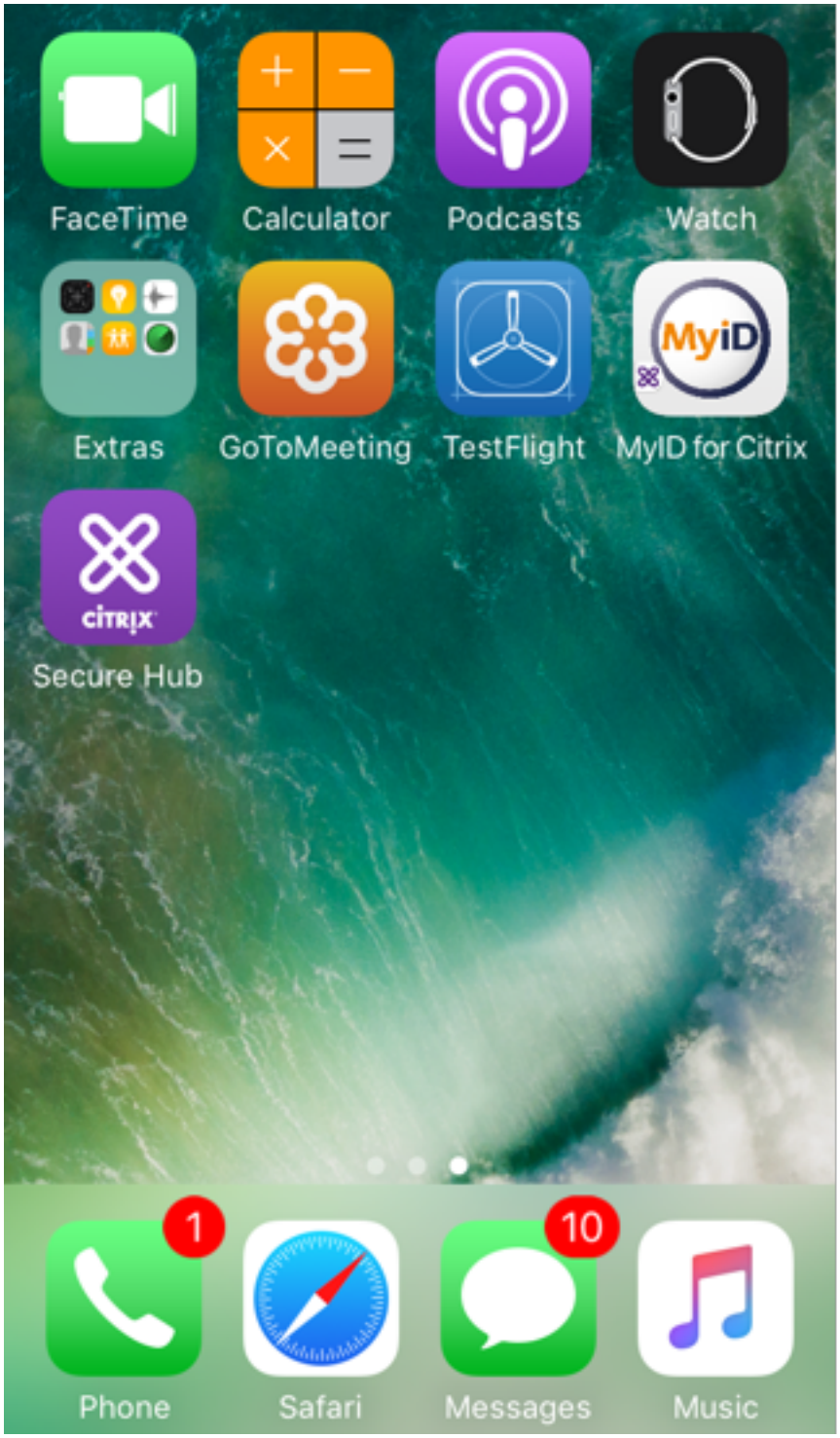
Endpoint Management can use derived credentials for iOS device enrollment. If configured for derived credentials, Endpoint Management doesn't support enrollment invitations or other enrollment modes for iOS devices. However, you can use the same Endpoint Management server to enroll Android devices through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

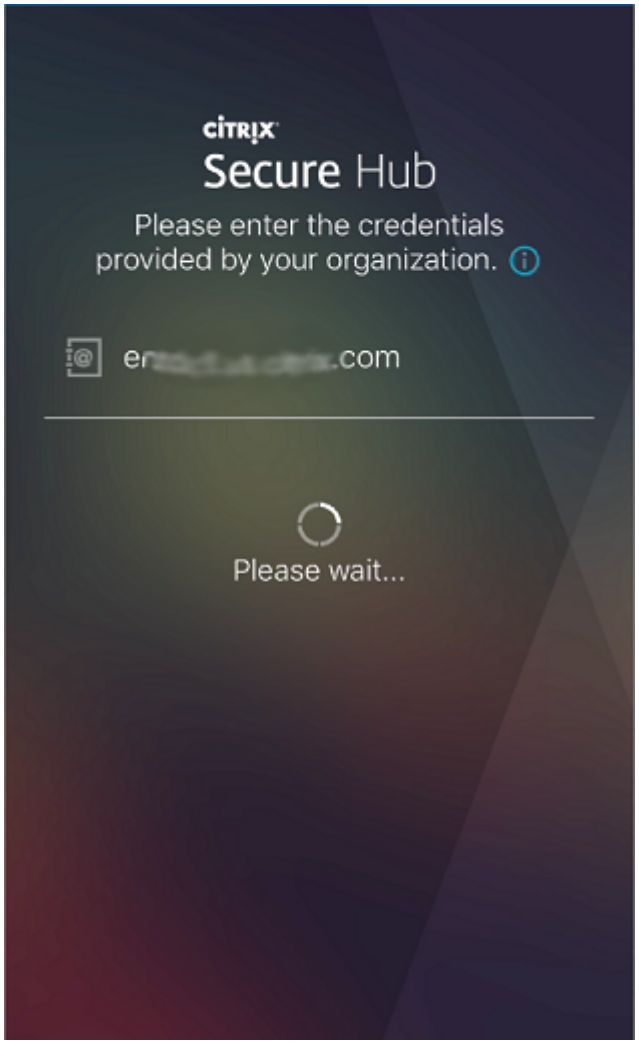
1. The user installs Secure Hub and the app from your derived credential provider. In this example, the identity provider app is the Intercede MyID Identity Agent.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

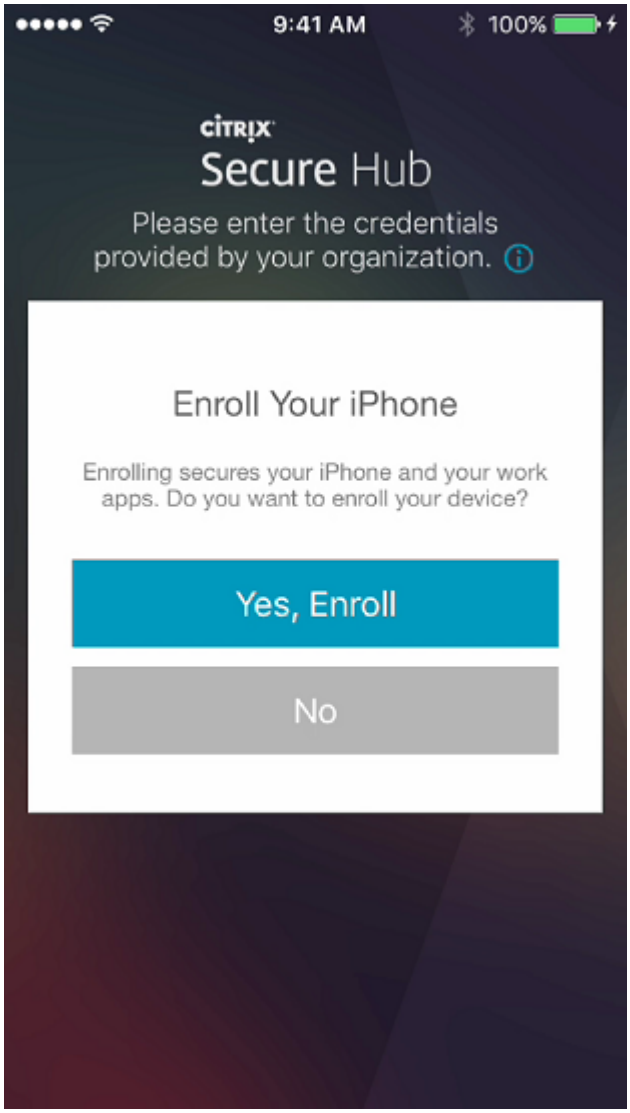


2. The user starts Secure Hub. When prompted, the user types the Endpoint Management fully qualified domain name (FQDN) and then clicks **Next**. Enrollment in Secure Hub starts. If Endpoint Management supports derived credentials, Secure Hub prompts the user to create a Citrix PIN.

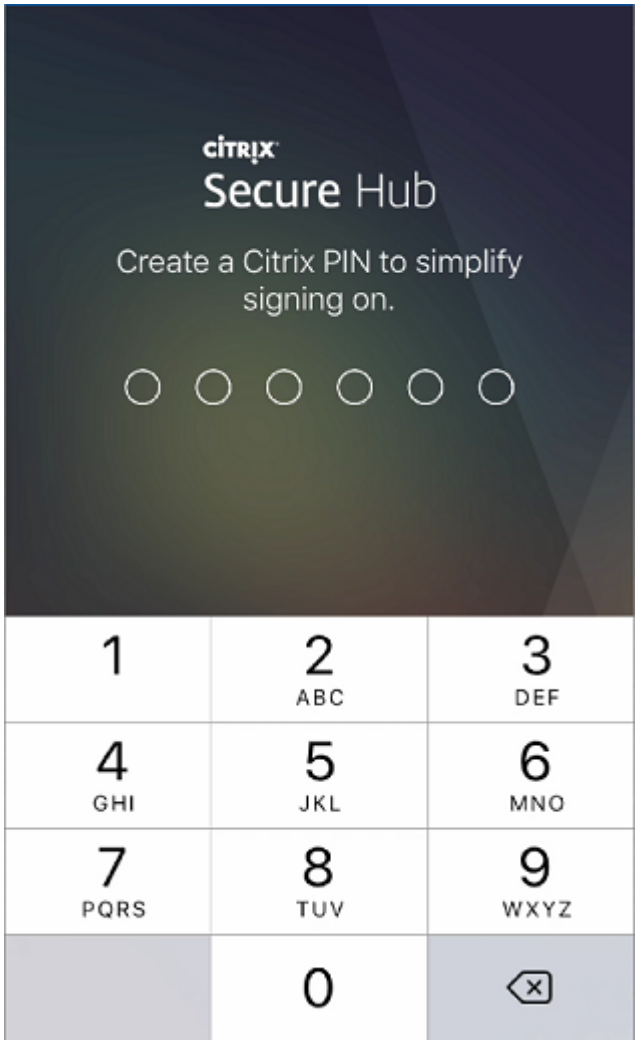
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

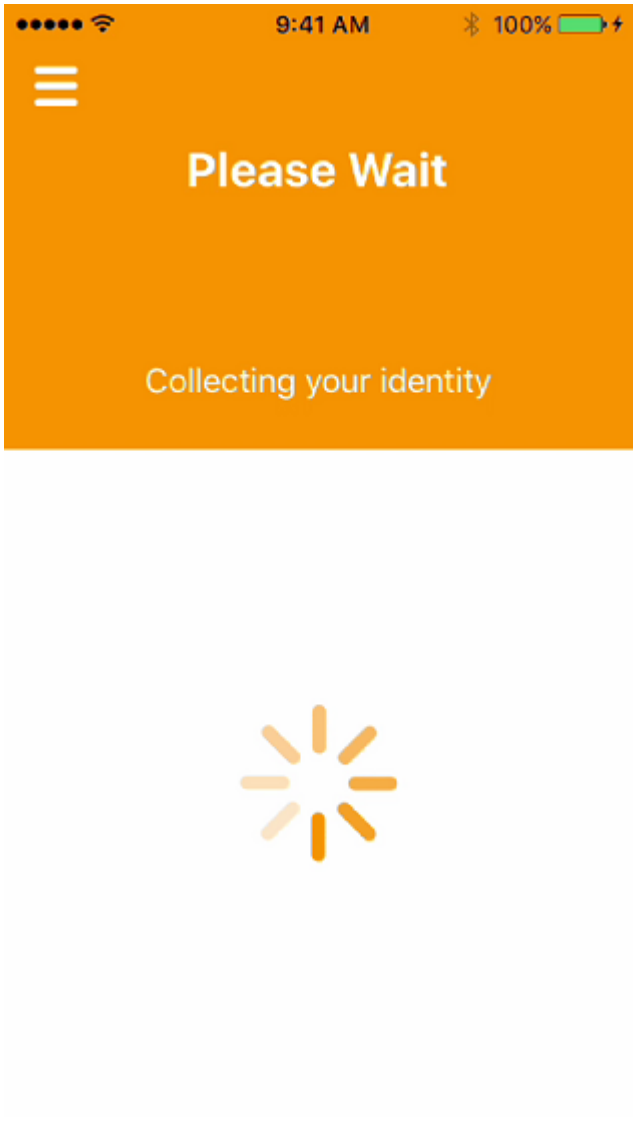


3. The user follows the instructions to activate their smart credential. A splash screen appears, followed by a prompt to scan a QR code.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

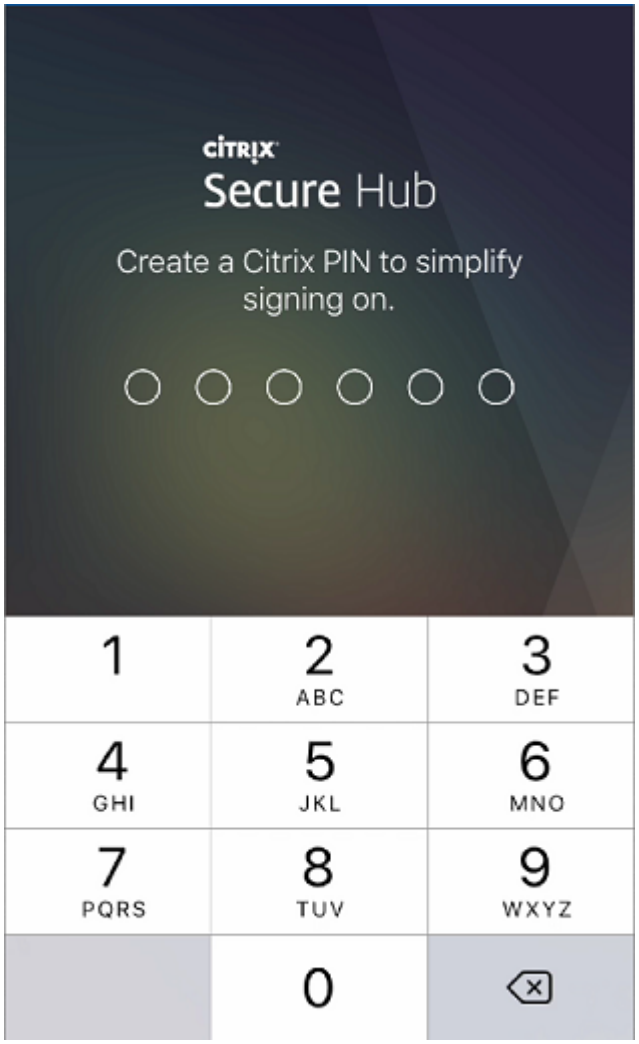
4. The user inserts their card into the smart card reader that's attached to their desktop. The desktop app then displays a QR code and prompts the user to scan the code using their mobile device.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



The user enters their Secure Hub PIN when prompted.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**.

Configure hint through the Citrix Endpoint Management console

November 28, 2023

An administrator can configure a hint on the Secure Hub sign-in page for devices with the enrollment mode set to **Two Factor**. You can configure a hint in one of the following ways:

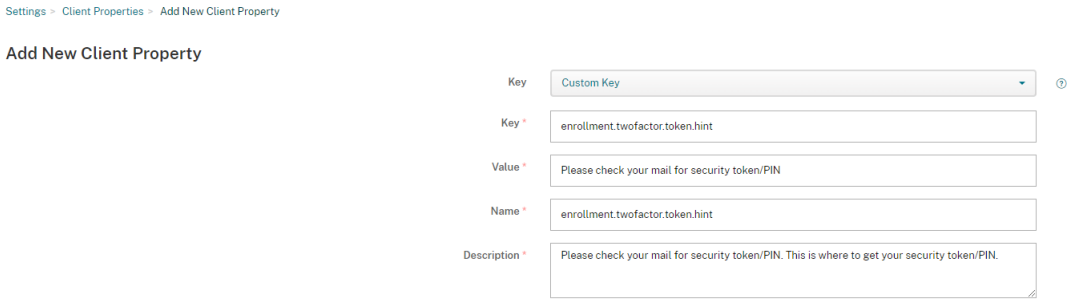
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Configure hint as text
- Configure hint text with webpage link

Configure hint as text

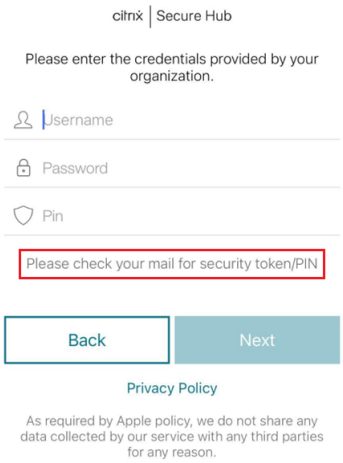
To configure a hint text, perform the following steps:

1. Sign in to the Citrix Endpoint Management console using administrator credentials.
2. Navigate to **Settings** > **Client Properties**, and click **Add New Client Property**.
3. From the **Key** drop-down list, select **Custom Key**.
4. In the **Key** field, enter **enrollment.twofactor.token.hint**.
5. In the **Value** field, you can provide text that displays as a hint on the sign-in page. The hint guides the users to locate the PIN for two-factor authentication.
6. In the **Name** field, enter **enrollment.twofactor.token.hint**.
7. In the **Description** field, you can provide remarks about the hint you configured, which will be helpful for your future reference.



8. Click **Save**.

The hint text appears on the sign-in page once you complete the configuration.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

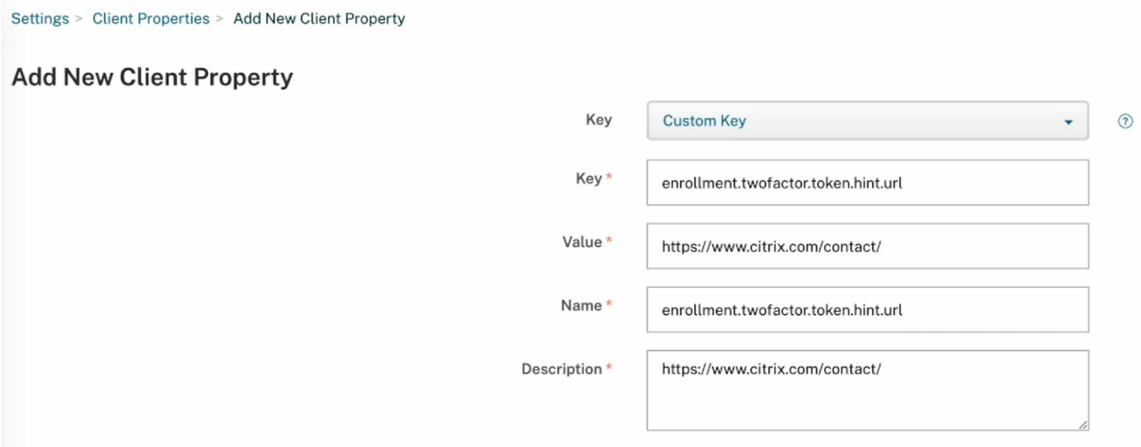
Configure hint text with webpage link

You can configure a webpage with detailed information about accessing the PIN. Later, provide the webpage link as a hyperlink in the hint text. When a user clicks the hint on the sign-in page, Secure Hub opens an embedded browser and navigates to the webpage that you already configured.

To configure hint text with a webpage link, first, you need to configure the hint text as explained in the Configure hint as text article. Once completed, continue with the following steps:

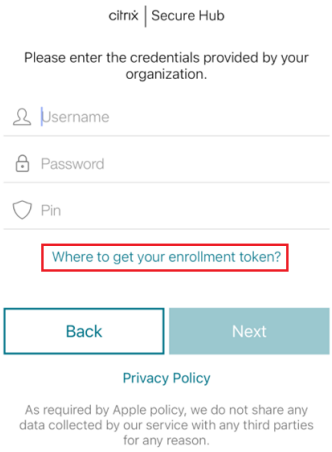
1. Sign in to the Citrix Endpoint Management console using administrator credentials.
2. Navigate to **Settings** > **Client Properties**, and click **Add New Client Property**.
3. From the **Key** drop-down list, select **Custom Key**.
4. In the **Key** field, enter **enrollment.twofactor.token.hint.url**.
5. In the **Value** field, enter the webpage URL that you configured.
6. In the **Name** field, **enter enrollment.twofactor.token.hint.url**.
7. In the **Description** field, you can provide remarks about the hint you configured, which will be helpful for your future reference.

   > **Note:**
   >
   > When a user clicks the hint link, a webpage appears in an embedded browser.



8. Click **Save**.

Once you complete the configuration, the hint text with the webpage link appears on the sign-in page.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).