Secure Hub

Contents

Known and fixed issues

November 3, 2025

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

Secure Hub for Android 25.10.0

Fixed issues

Secure Hub reports deployment failure to the CEM server when the required app is not installed to unblock policy deployment. [XMHELP-4752]

Known issues

There are no known issues in this release.

Secure Hub for iOS 25.8.0

Fixed issues

- When you switch the Mobile Application Management (MAM) app data sharing feature flag on and off, some MAM apps might display a popup alert stating "App was removed".
- When you unenroll Secure Hub, some MAM apps might remain available for use.
- when you change log settings for MAM apps from Secure Hub, the changes might not be effective.

Known issues

There are no known issues in this release.

Secure Hub for Android 25.7.0

Fixed issues

This version addresses areas that improve overall performance and stability.

Known issues

There are no known issues in this release.

Secure Hub for iOS 25.6.0

Fixed issues

- When you use the Secure Hub app, you might experience occasional crashes or receive the following error message when accessing the store, even after several retry attempts: "Could not load store. Please try again."
- When you use the Device Enrollment Program (DEP) or Return To Service (RTS) in Mobile Device Management (MDM) only mode , the process might not be supported. [XMHELP-4740]
- You might encounter failures during Azure Active Directory (AAD) registration for devices enrolled by on-premises Active Directory.

Known issues

There are no known issues in this release.

Secure Hub for Android 25.4.0

Fixed issues

When a user re-enrolls the same device without first wiping it and deleting it from the CEM console, they can't manually refresh the policy if the service is disabled. [XMHELP-4741]

Known issues

There are no known issues in this release.

Secure Hub for iOS 25.1.0

Fixed issues

This version addresses areas that improve overall performance and stability.

Known issues

There are no known issues in this release.

Secure Hub for Android 25.1.0

Fixed issues

This version addresses areas that improve overall performance and stability.

Known issues

There are no known issues in this release.

Secure Hub for iOS 24.11.0

Fixed issues

The iOS devices are prompting users to enter their User Principal Name (UPN) when opening Secure Hub, despite the devices already being enrolled in the Device Enrollment Program (DEP). [XMHELP-4439]

Known issues

There are no known issues in this release.

Secure Hub for Android 24.10.0

Fixed issues

There are no fixed issues in this release.

Known issues

There are no known issues in this release.

Secure Hub for iOS 24.9.0

Fixed issues

There are no fixed issues in this release.

Known issues

There are no known issues in this release.

Secure Hub for Android 24.8.0

Fixed issues

There are no fixed issues in this release.

Known issues

There are no known issues in this release.

Secure Hub for Android 24.6.0

Fixed issues

There are no fixed issues in this release.

Known issues

There are no known issues in this release.

Secure Hub for iOS 24.5.0

Fixed issues

There are no fixed issues in this release.

Known issues

There are no known issues in this release.

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]
- 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]

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.

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.

Secure Hub for Android and iOS - Preview

November 3, 2025

Look forward to the upcoming release, which includes exciting new features that enhance functionality and user experience.

The generally available version of Secure Hub Android is 25.10.0. For more information on the current release, see What's new.

Feature flag management

November 25, 2024

Administrators can manage feature flags to access preview features and dynamically control features in production. To ensure optimal functioning of features which are under feature flags, you need to enable traffic to the URL `features.netscalergateway.net`. For more information, see Feature flag management.

Authentication prompt scenarios

September 7, 2025

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.

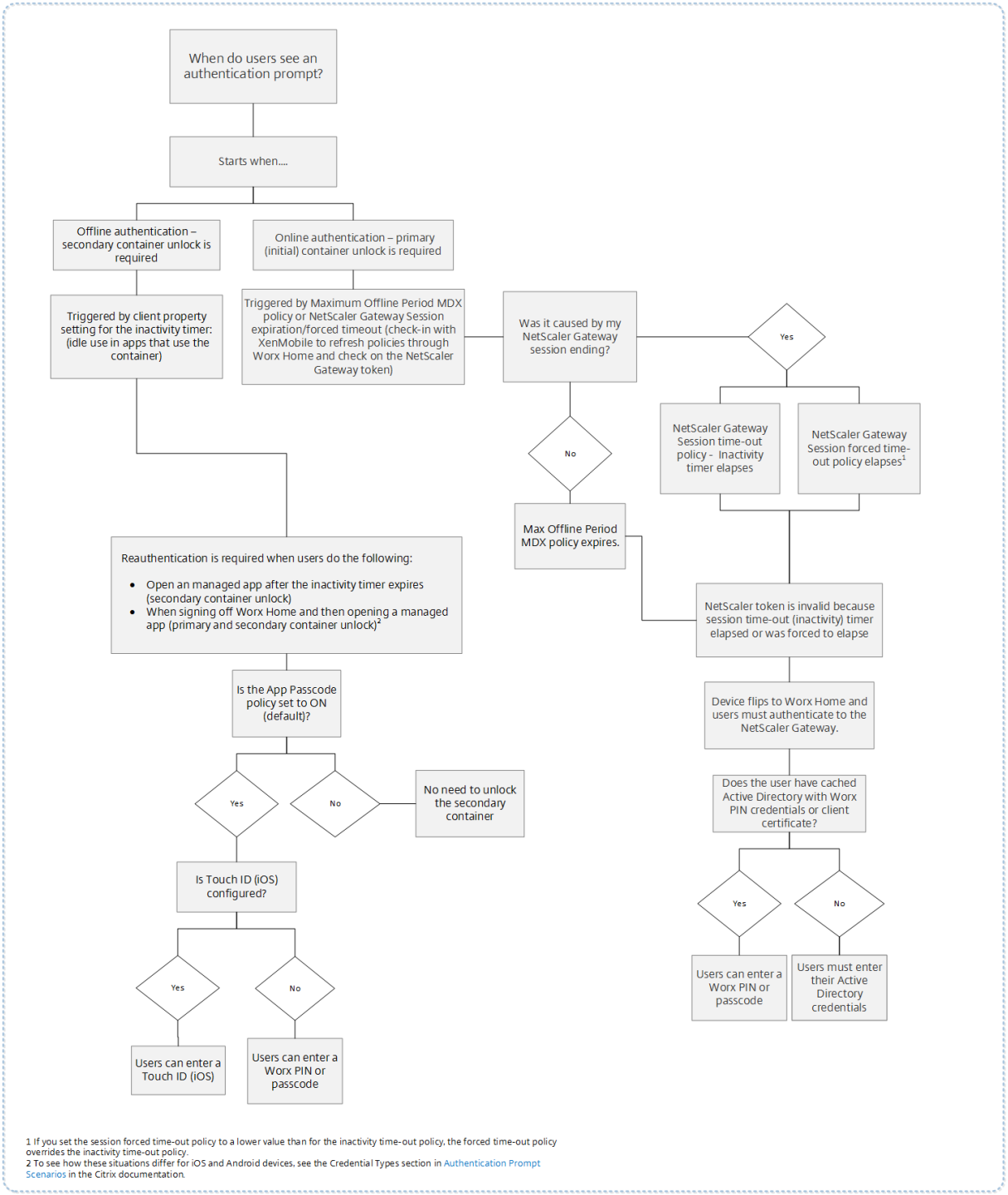
Active Directory credentials are required for either container unlock circumstance when the following conditions are true:

- 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.



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.

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.

Enrolling devices by using derived credentials

September 7, 2025

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).

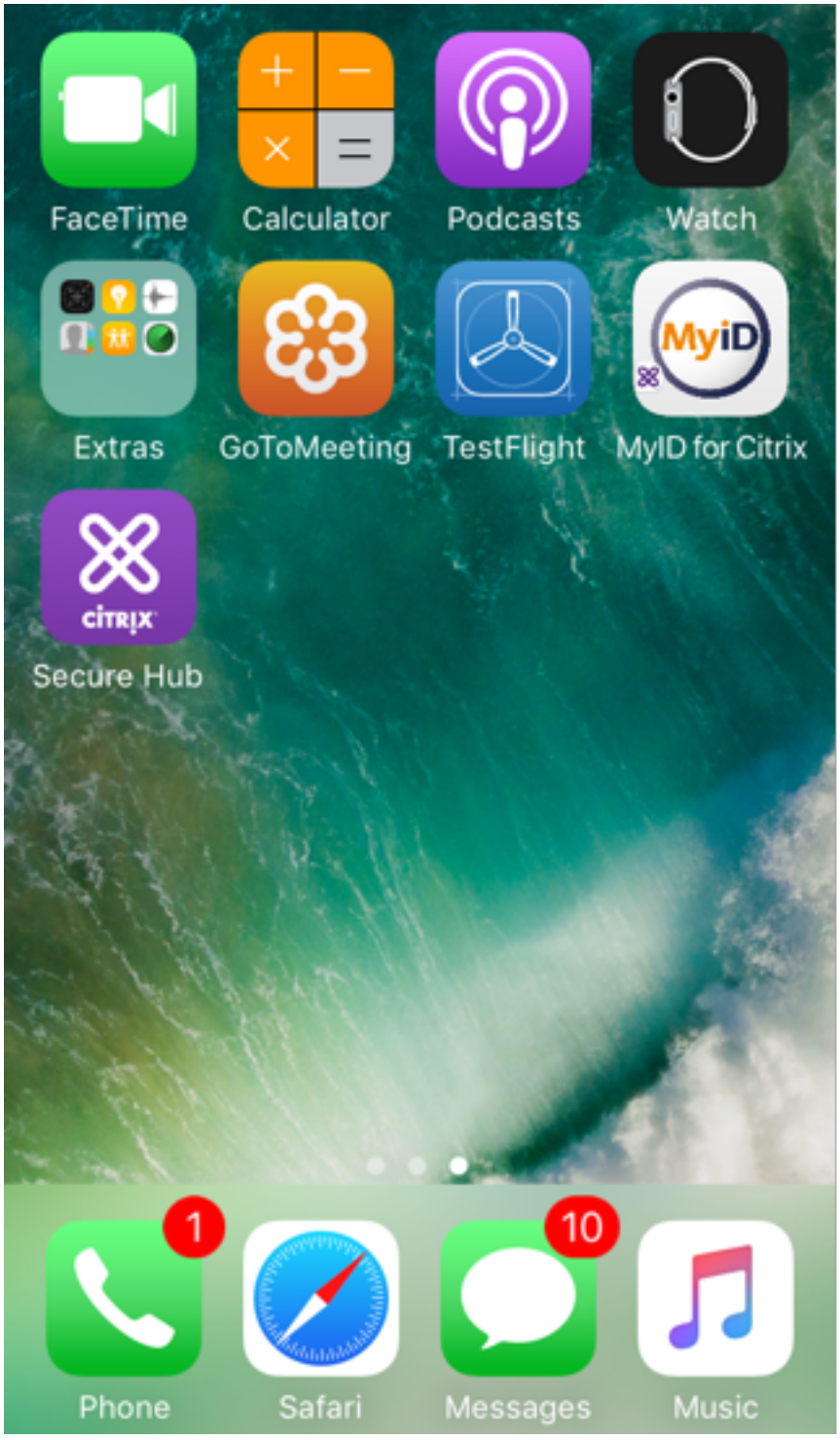
The derived credentials are an enrollment certificate that contains the user identifier, such as UPN. Endpoint Management stores the credentials obtained from the credential provider in a secure vault on the device.

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.

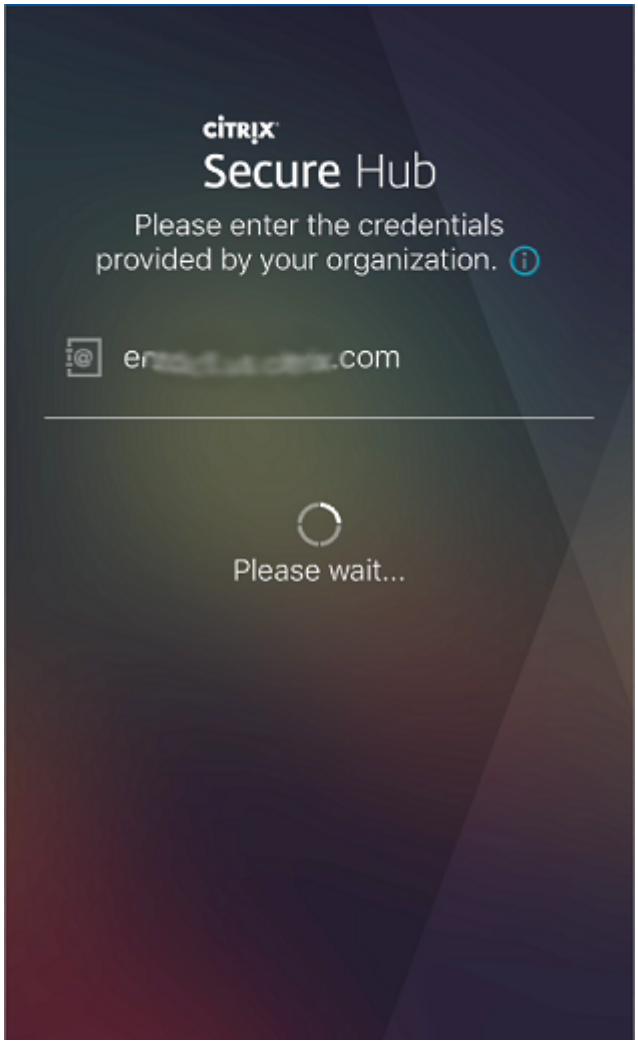
Device enrollment steps when using derived credentials

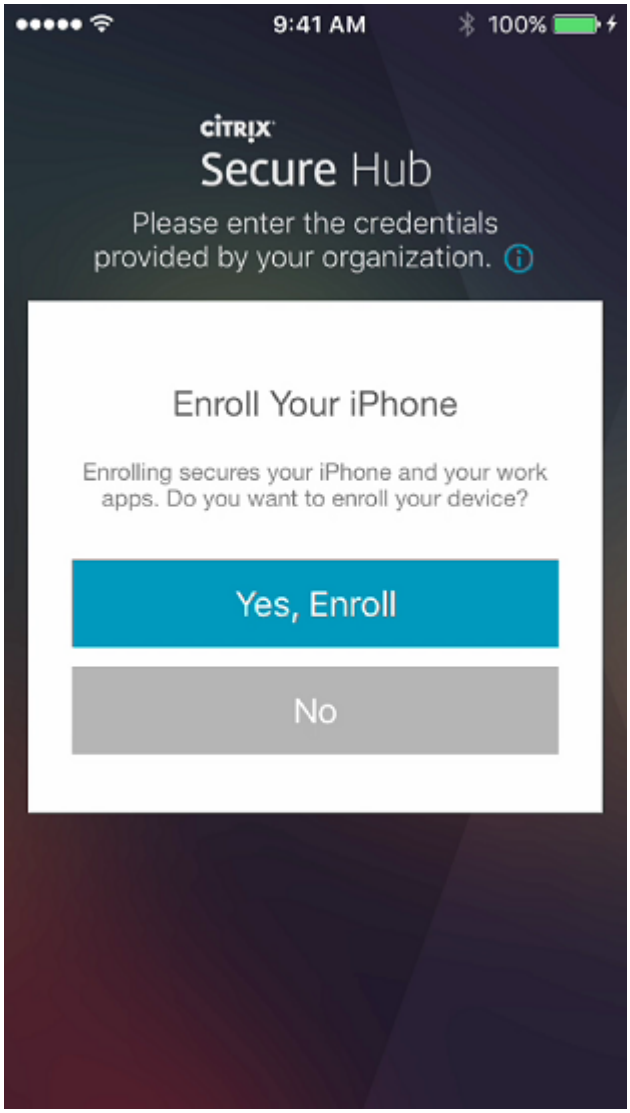
Enrollment requires that users insert their smart card to a reader attached to their desktop.

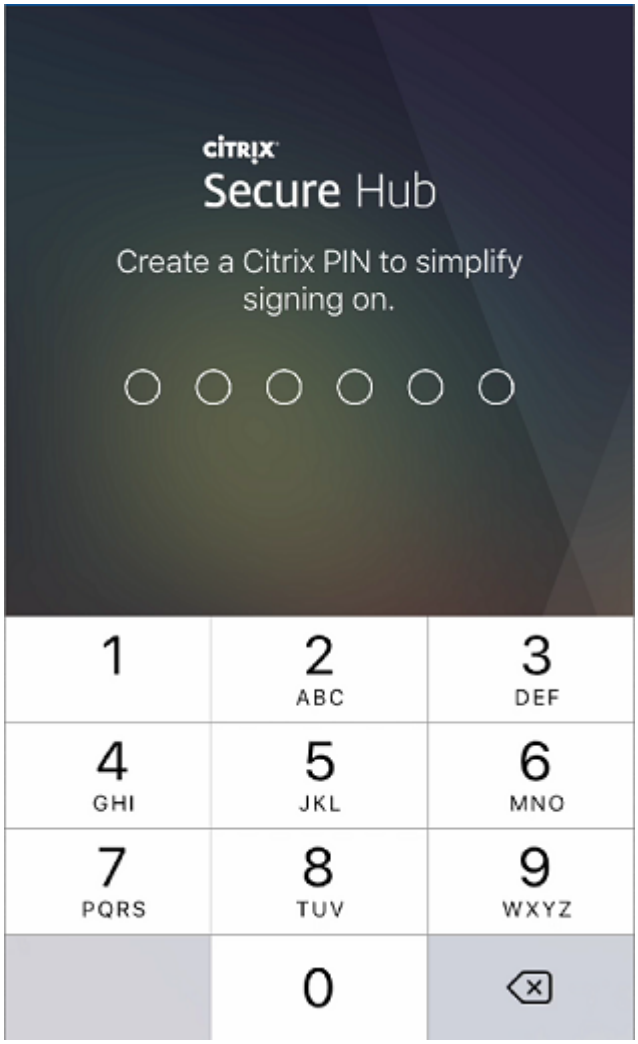
1. The user installs Secure Hub and the app from your derived credential provider. In this example, the identity provider app is the Intercede MyID Identity Agent.



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.

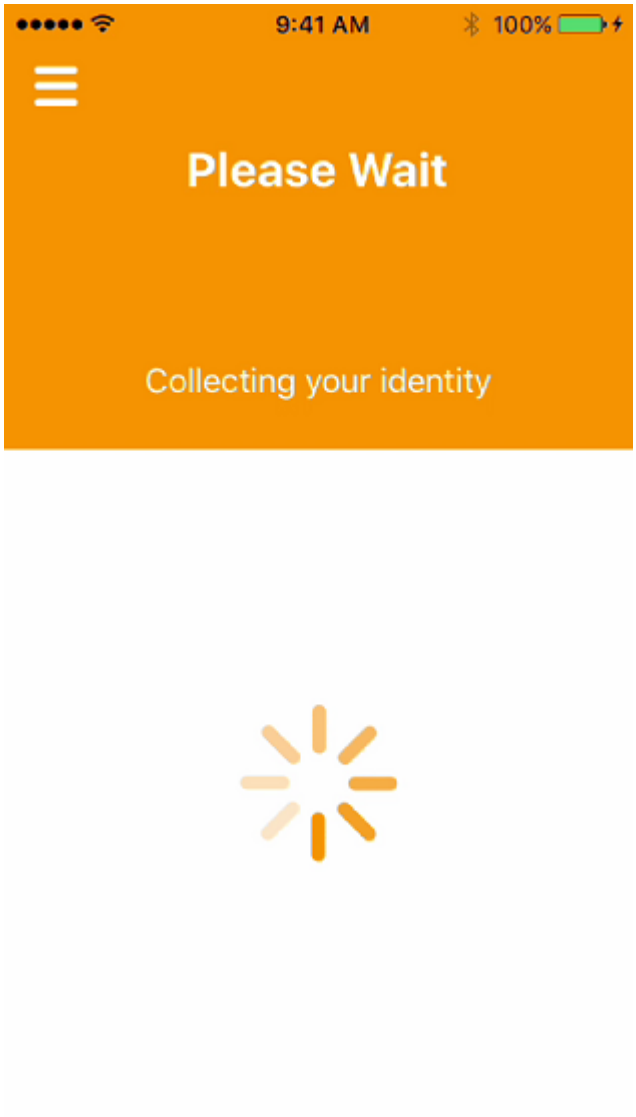




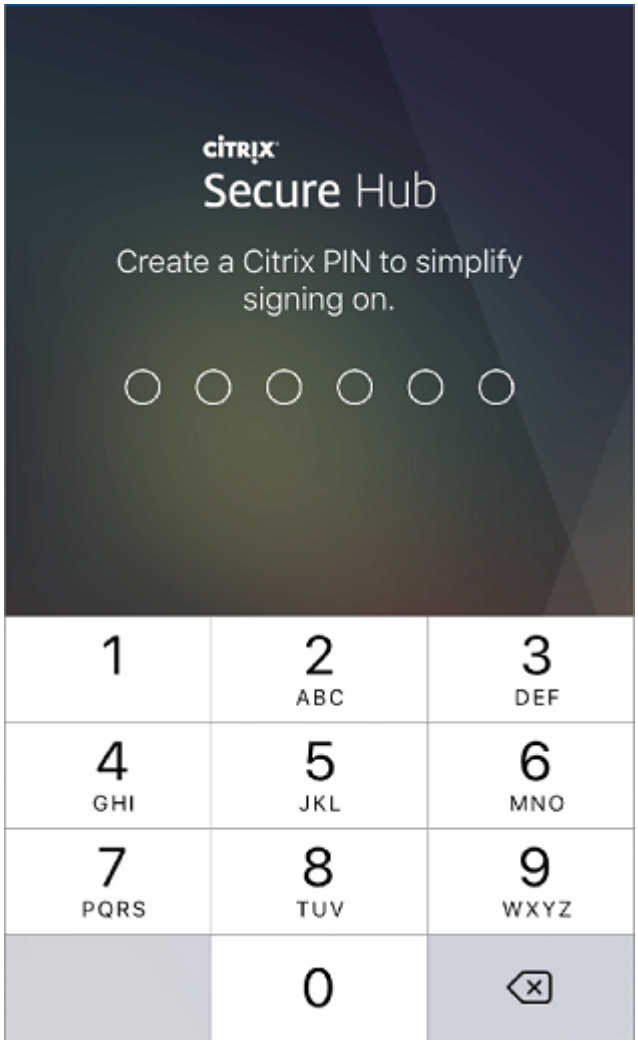


3. The user follows the instructions to activate their smart credential. A splash screen appears, followed by a prompt to scan a QR code.

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.



The user enters their Secure Hub PIN when prompted.



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

September 7, 2025

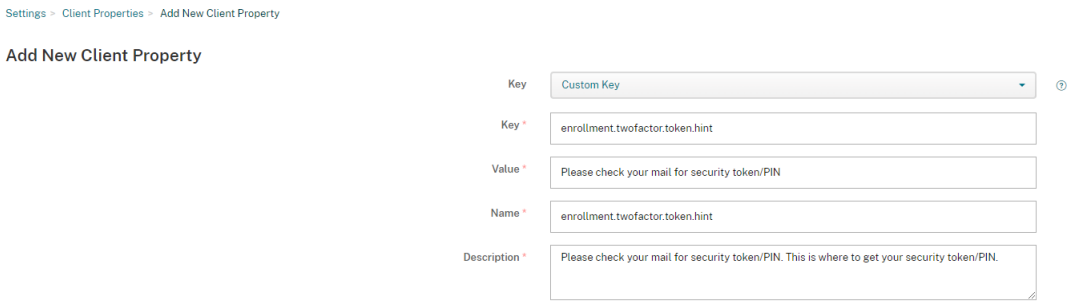
An administrator can configure a hint on the Secure Hub sign-in page for devices with the enrollment mode set to **Two Factor**. You can configure a hint in one of the following ways:

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

Configure hint as text

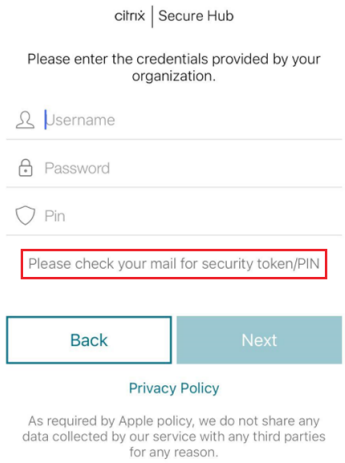
To configure a hint text, perform the following steps:

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.



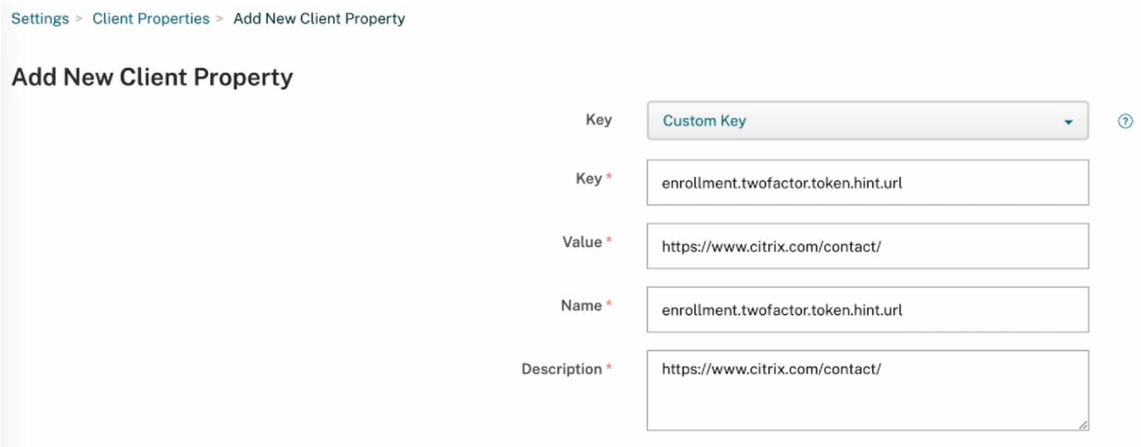
Configure hint text with webpage link

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:

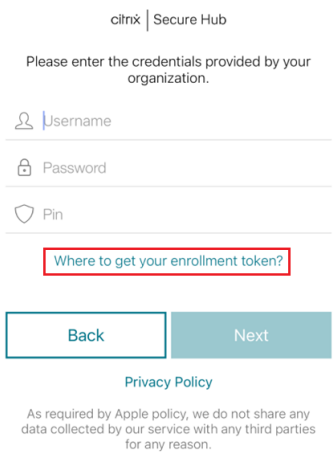
1. Sign in to the Citrix Endpoint Management console using administrator credentials.
2. Navigate to **Settings** > **Client Properties**, and click **Add New Client Property**.
3. From the **Key** drop-down list, select **Custom Key**.
4. In the **Key** field, enter **enrollment.twofactor.token.hint.url**.
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.



Compliance check on Android devices (Technical Preview)

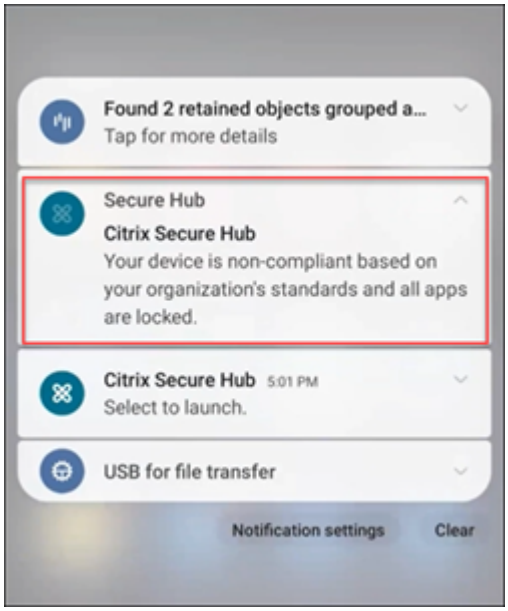
September 7, 2024

> **Note:**
>
> This feature is applicable for Android devices enrolled in *Device Owner* mode.

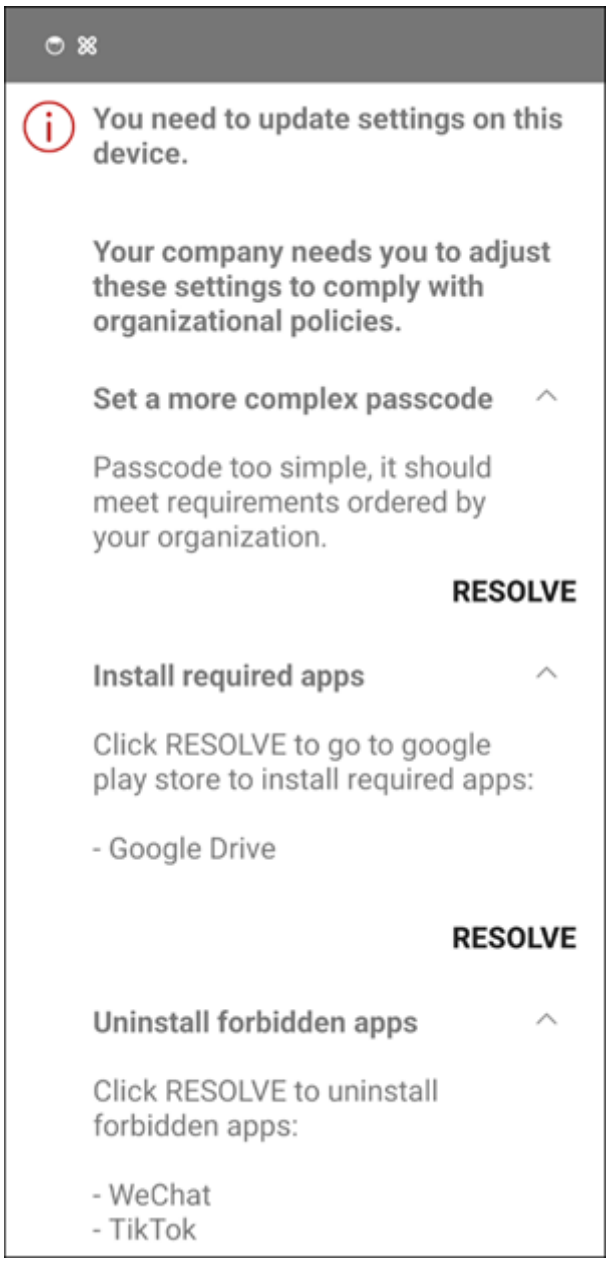
Starting from the release of Secure Hub for Android 24.8.0, Secure Hub verifies the compliance of Android devices against the policies configured by administrator through Citrix Endpoint Management. These compliance check includes:

- Ensuring device password strength
- Verifying installation of mandatory apps
- Confirming removal of prohibited apps

When a device is non-compliant, the following notification appears on the user device.



When a device is non-compliant, users see the following message when they open Secure Hub.



Users can click the **RESOLVE** button to address the respective issues.

> **Note:**
>
> - The apps remain locked until the compliance is met.
> - You have the option to unlock specific apps by adding them to Unlock apps list. For more information, see Compliance Enforcement for Android Devices (Technical Preview).

For more information on configuring policies and compliance checks, see Compliance Enforcement for Android Devices (Technical Preview) in the Citrix Endpoint Management product documentation.