CITRIX

Secure Hub

Contents

Citrix Secure Hub

January 23, 2019

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.

What's new in this release

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 performace 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.

What's new in earlier releases

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

Secure Hub 18.10.0

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

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

- **Support for Android SafetyNet:** You can configure Endpoint Management to use the **Android SafetyNet** feature to assess the compatibility and security of Android devices that have Secure Hub installed. The results can be used to trigger automated actions on the devices. For information, see Android SafetyNet.

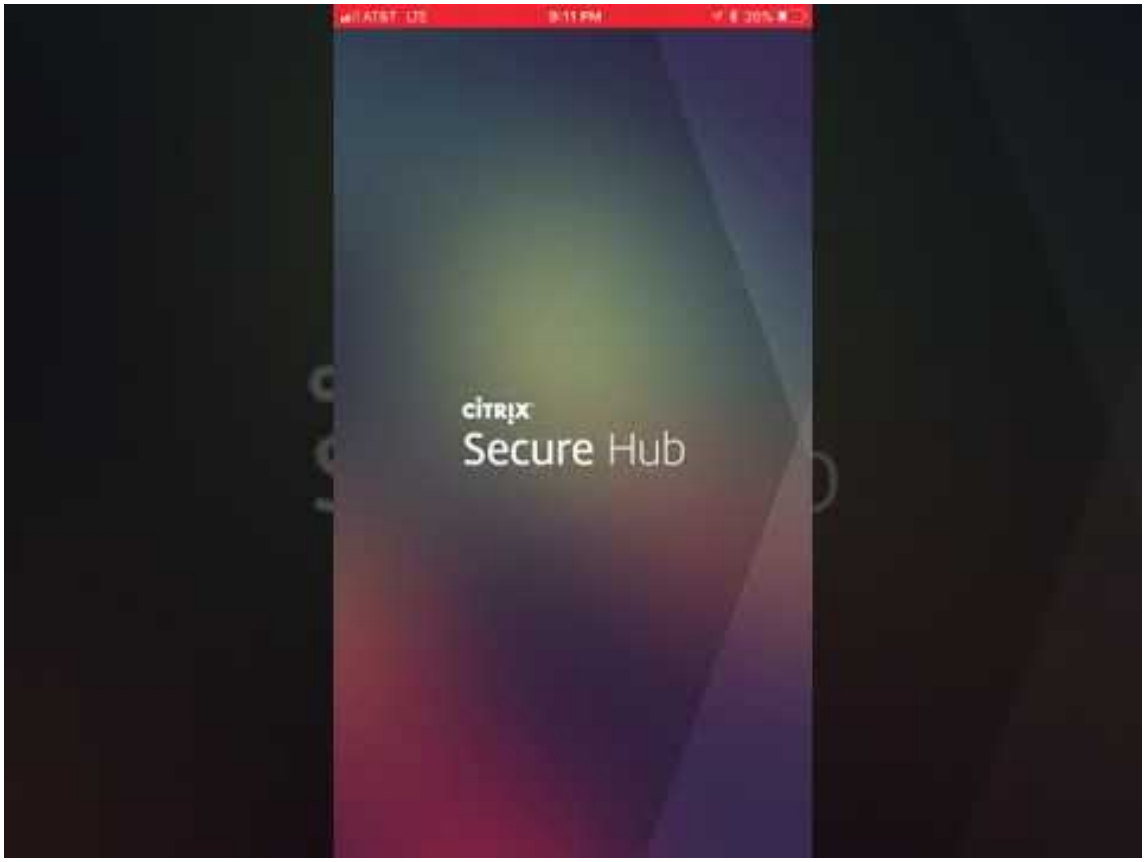
- **Prevent camera use for Android Enterprise devices:** The new **Allow use of camera** setting for the Restrictions device policy lets you prevent users from using the camera on their Android Enterprise devices. For information, see Restrictions device policy.

Secure Hub 10.8.60 to 18.9.0

Bug fixes and performance enhancements.

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.



> **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 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 Workspace Configuration.

> **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 hostname 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 site article on Android P behavior changes.

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

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

Administering Secure Hub

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

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

> **Important:**
>
> Changes to any of the following 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 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. Fingerprint authentication is supported for iOS 9 and iOS 10.3 devices and some Android devices. For information about enabling fingerprint authentication, see the **ENABLE_TOUCH_ID_AUTH** setting in **Client** properties.

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 may 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 Endpoint Management AutoDiscovery Service.
- Private/self-signed CAs and the 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 is managed by the Endpoint Management Auto Discovery Service (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. 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.
- 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.

Configuring certificate + one-time-password authentication for Secure Hub

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 this 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**.

   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.
5. Click **Edit**.
6. On the **Virtual Servers configuration** screen, scroll down to **Policies**.
7. Click **+** to add a policy.
8. In the **Choose Policy** field, choose **Rewrite**.
9. In the **Choose Type** field, choose **Response**.
10. Click **Continue**.

    The **Policy Binding** section expands.
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.
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**.

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. Note that this com-

> munication 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 strongly discouraged from upgrading to Secure Hub 10.2. If you have any questions, please contact Citrix support.

Customers interested in enabling certificate pinning must do the following prerequisites:

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

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

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

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

Secure Hub features

Secure Hub allows you to monitor and enforce mobile policies while providing access to the Store and live support. Users begin by downloading Secure Hub on to their devices from the Apple, Android, or Windows app 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?

Note that 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.

On tablets, the Store is a separate tab.

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 be 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.

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.

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

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**.

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

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

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

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

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

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

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

Known and fixed issues

January 23, 2019

Fixed issues in version 19.1.0

Secure Hub for Android:

On Samsung Knox devices enrolled for Android For Work, when the password policy is configured to expire in one or two days, the “Password Expired” message appears repeatedly. [CXM-59250]

Known issues in version 19.1.0

Secure Hub for iOS:

In Secure Hub for iOS, when you deploy an MDX and web or SaaS apps, they appear in **My Apps** screen. When
you tap **More**, a popup appears with **Delete** and **Cancel** options that has the format of old UI branding. [CXM-60683]

Fixed issues in version 18.12.0

- On Samsung Knox devices enrolled for Android For Work, when the password policy is configured to expire in one or two days, the “Password Expired” message appears repeatedly. [CXM-59250]
- You are unable to enroll OnePlus 5T devices for Android Enterprise using QR code enrollment method. [CXM-59288]

Fixed issues in version 18.11.0

Secure Hub iOS:

- You are unable to perform single sign-on on Android devices enrolled in the Shared Device mode. The following error appears: Your corporate credentials cannot be retrieved at this time. Manual login to ShareFile is blocked due to admin policy. [CXM-58238]
- You cannot edit Android volume levels on corporate-owned, single-use (COSU) devices. [CXM-58323]

Fixed issues in version 18.10.5

- If you have FIPS mode enabled in XenMobile Server, after users update Secure Hub for iOS to version 18.10.5, an encryption-related error message appears when users open apps. For status updates on the resolution, see this Citrix Knowledge Center article. [CXM-56454]

Fixed issues in versions 10.8.25 to 18.10.6

- Secure Hub versions 10.8.25 to 18.10.6 (Android) include no known issues. The following issues are fixed in Secure Hub. The list includes issues with MDX that affect Secure Hub.

Fixed issues in version 18.10.0

- If the MVPN policy is turned off in the EMS console, Secure Hub displays a blank screen when trying to open Intune managed apps. [CXM-56033, CXM-56086, CXM-54393, CXM-54823]

Fixed issues in version 10.8.60

- On Samsung Galaxy Tab Active 2 SM-T395 devices, the Full Wipe security action fails for Secure Hub for Android when admins set a Disable Factory Reset restriction in XenMobile. [CXM-54452]
- Secure Hub for Android becomes unresponsive during enrollment of devices when the VPN policy is configured and Citrix SSO application is not installed on the device. It becomes responsive if you click the Back button or restart the app. [CXM-54627]
- Secure Hub for Android crashes during enrollment in the Device Owner mode in an Android Enterprise environment. [CXM-55008]
- After users enter a valid PIN for Secure Hub for iOS, Secure Hub prompts users for the PIN repeatedly. [CXM-55047]
- Secure Hub for Android crashes during enrollment in the Profile Owner mode in an Android Enterprise environment. [CXM-55076]
- Using Android Enterprise in Secure Hub for Android installs Google Chrome by default. [CXM-55232]
- Upgrading Secure Hub for iOS to version 10.8.55, doesn't allow existing or new iOS device enrollments. [CXM-55267]

Fixed issues in version 10.8.55

- Users cannot sign on to Secure Hub to enroll in Android for Work accounts when the G Suite credentials differ from the credentials in Endpoint Management. [CXM-53956]

MDX-related fixed issues in version 10.8.55

- Enterprise apps may experience connectivity issues to internal resources when Preferred VPN mode is set to SecureBrowse. [CXM-52309]
- Apps that specify android.support.multidex.MultiDexApplication or android.app.Application as their application class cannot connect to internal networks in the Secure Browse mode. [CXM-53126]
- On Android devices, multiple certificates are being generated and certificates are being revoked before their expiration date. [CXM-53428]

Known issue in version 10.8.50

- On Secure Hub for Android, users cannot add a web link shortcut. [XMHELP-952]

Fixed issues in version 10.8.35

- On Android O, shortcuts created by policies do not appear on the device home screen. This is by design in Android O. [CXM-35460]
- On Android, Secure Hub does not open on Samsung tablets after a period of inactivity. [CXM-50797]
- In Secure Hub for Android, you are unable to deploy the push policy on Samsung Knox devices. [CXM-50869]
- In Secure Hub for iOS, occasionally the following issue occurs: After users change their Active Directory password, they must keep entering their PIN in a loop. [CXM-50224]

Fixed issues in version 10.8.25

- For third-party iOS Cordova apps wrapped with the MDX Toolkit version 10.7.20, after you enable the Obscure screen contents policy, a black screen appears on iOS devices instead of a PIN screen. [CXM-48471]
- On Zebra T51 devices running Android 7, users cannot install the Citrix Launcher app. [CXM-50621]

Fixed issues in version 10.8.20

- After users update their Android devices to version 8 (Oreo): They cannot install enterprise or .apk apps from the app store that you deploy from Endpoint Management. Even when they enable installation of third-party apps, the issue persists. The issue is not limited to Samsung devices. [CXM-50401]

Fixed issues in version 10.8.15

- Secure Hub for Android crashes while fetching location details on devices running Android O. [CXM-47893]

Fixed issues in version 10.8.10

- On Android devices, when multiple apps do not install automatically or users don't click Install themselves, the apps keep downloading. As a result, high data usage occurs. [CXM-46404]
- On devices running Android 7 or later: When you send a lock security action with a password to the device from XenMobile Server, the device locks. However, the device password does not change if users have an existing lock screen password. Users can use the original passcode to unlock the device.[CXM-47908]

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.

Authentication prompt scenarios

November 1, 2018

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 needs to be an online authentication (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 frequency of authentication that you require.

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, which it is 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. If, for example, users set down their devices and walk away, if 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 in order 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 Gatewayy policies also affect when users are prompted to authenticate. In these cases, they authenticate in order 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 of time. The default is 30 minutes. If you use the Citrix Gateway wizard to configure the policy, however, the default is 1440 minutes. Users will then 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 of time. 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 Gatewaywizard 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 in order 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:**
>
> When the article refers to a *managed app*, the term refers to an app wrapped by the MDX Toolkit, in which you've left the App Passcode MDX policy enabled by default and are leveraging 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 of Secure Hub and subsequently 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. Fingerprint authentication is supported for iOS 9 and iOS 10.3 devices and some Android devices. For information about enabling fingerprint authentication, see the ENABLE_TOUCH_ID_AUTH setting in Client properties.

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

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.

iOS VPN installation

August 23, 2018

On iOS 10 and later devices, Secure Hub VPN is used for secure local data sharing between Secure Hub and MDX apps. Secure Hub VPN runs on iOS 10 and later devices. Secure Hub VPN provides an ideal user experience because Secure Hub and MDX apps can communicate seamlessly through this VPN.

Secure Hub VPN works for apps signed by Apple Enterprise developer account (“team id”) certificates, Citrix certificates, Enterprise certificates, or third-party ISV certificates.

Secure Hub VPN is used by default on iOS 10 devices. If Secure Hub VPN is not running on the iOS 10 device, MDX uses the iOS shared keychain for secure data sharing. The iOS shared keychain mechanism requires all participating apps to be signed with the same certificate to access the specific shared

keychain for that iOS "team id" certificate. If an app is not signed with the same certificate as the Citrix-signed Secure Hub app, the app might flip to Secure Hub to get the required information.

Secure Hub VPN is available only for Citrix Endpoint Management Enterprise and MAM-only deployments. Secure Hub VPN does not apply to Endpoint Management MDM-only environments, and the VPN is not installed in MDM-only enrollments. On iOS 9 and earlier versions, Secure Hub does not use Secure Hub VPN.

Secure Hub VPN is used for communication between Secure Hub and mobile productivity apps. It does not filter or monitor network traffic on the device and is independent of the MDX micro-VPN mechanism.

> **Note:**
>
> Citrix recommends that you leave Secure Hub VPN enabled in environments where it is enabled by default.
>
> Because iOS does not allow more than one VPN client to run on an iOS device simultaneously, however, be aware of the following situation. The Secure Hub VPN cannot be used if another VPN app, such as Cisco AnyConnect or Citrix VPN, needs to run on iOS devices to establish a device-level VPN. You can set up an iOS per-app VPN even if Secure Hub VPN is not disabled. The app using the iOS per-app VPN establishes a per-app VPN connection when the app is in the foreground.
>
> To disable Secure Hub VPN, see the following section in this article. When Secure Hub VPN is disabled, users might experience more flips from a managed app to Secure Hub.

Disabling or reenabling Secure Hub VPN in Endpoint Management

Secure Hub VPN is enabled by default when users start using Secure Hub 10.3.10 and later on iOS 10.

To disable Secure Hub VPN and set iOS devices in your deployment to use the shared keychain mechanism, do the following:

1. In the Endpoint Management console, go to **Settings > Client > Client Properties**.
2. On the **Client Properties** page, create a custom client property called **ENABLE_NETWORK_EXTENSION** and set the value to 0.

   To reenable Secure Hub VPN, go to the Secure Hub VPN and set the value of **ENABLE_NETWORK_EXTENSION** to 1.

Installing Secure Hub VPN on the client device

The Secure Hub VPN is installed in two cases: after Secure Hub 10.3.10 or later is installed on an iOS 10 device or when a user upgrades a device running Secure Hub 10.3.10 or later to iOS 10.

Users see this informational message.

Next, users see an iOS message asking for permission to add VPN configurations. This message is shown only one time, when the VPN is first installed. It is not shown when users open Secure Hub again.

The message on this screen is not customizable. It is a standard iOS dialog box used for all VPN installations.

On the screen asking for permission to add the VPN configuration: If users select **Don't Allow**, they see another message indicating that they must install the VPN to access Secure Hub.

Running Secure Hub VPN on the client device

When the Secure Hub VPN is running as designed, the text **Connecting** appears in the **General > VPN** screen of the iOS Settings app.

This is expected and does not mean that the MDX sharing and communication mechanisms are not functioning. There is no action required from users if they see this message.

Enrolling devices by using derived credentials

September 20, 2018

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**.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States