



Secure Hub

Contents

Citrix Secure Hub™	19
Administering Secure Hub	19
Citrix PIN	19
Certificate pinning	20
Configuring certificate + one-time-password authentication for Secure Hub	21
Port requirement for ADS connectivity for Android devices	26
Secure Hub features	28
Citrix Secure Hub™	35
What's new in the current version	35
Secure Hub for iOS 26.8.1	35
Secure Hub for Android 26.8.0	35
Set an auto-launch app in the Launcher Configuration policy in COSU mode	35
Automatic detection and renewal of the MDM device certificate	36
What's new in earlier versions	36
Secure Hub for iOS 26.8.0	36
Support for iOS/iPadOS 27	36
Secure Hub for Android 26.5.0	36
Support for Android 17	36
Secure Hub for Android 26.2.0	36
Device Certificate troubleshooting enhancement	36
Secure Hub for iOS 25.8.0	37
Support for iOS 26	37
Secure Hub for Android 25.10.0	37
Support for 16KB memory page size	37
Secure Hub for Android 25.7.0	37
Secure Hub for iOS 25.6.0	38

Secure Hub for Android 25.4.0	38
Support for Android 16	38
Support for TLS 1.3 protocol	38
Secure Hub for Android 25.1.0	38
Secure Hub for iOS 25.1.0	38
Secure Hub for iOS 24.11.0	38
Secure Hub for Android 24.10.0	39
Support for Android 15	39
Secure Hub for iOS 24.9.0	39
Displays Terms and Conditions on Device Enrolment Program	39
Secure Hub for Android 24.8.0	39
Compliance check on Android devices (Technical Preview)	39
Secure Hub for Android 24.6.0	40
Improved log collection and reporting	40
Secure Hub for iOS 24.5.0	41
Supports iOS 17 Return to Service	41
Secure Hub for Android 24.3.0	41
Supports Samsung Knox Enhanced Attestation v3	41
Secure Hub for Android 23.12.0	42
Enhanced Security with Samsung Knox	42
Access Secure Mail from user's personal profile	42
Secure Hub for iOS 24.1.0	43
Secure Hub for Android 23.12.0	43
Add a hint about authentication PIN on the sign-in page	43
nFactor authentication supports single sign-on feature	44
Support full wipe in direct boot mode	44
Optimized the loading speed of Secure Hub's App Store	44
Secure Hub for iOS 23.11.0	44

Add a hint about authentication PIN on the sign-in page	44
nFactor authentication supports single sign-on feature	44
Secure Hub 23.10.0	45
Secure Hub for Android	45
Secure Hub 23.9.0	45
Secure Hub for Android	45
Secure Hub 23.8.1	45
Secure Hub for iOS	45
Secure Hub 23.8.0	45
Secure Hub for iOS	45
Secure Hub 23.7.0	45
Secure Hub for Android	45
Secure Hub 23.4.0	46
Secure Hub for iOS	46
Secure Hub 23.4.1	47
Secure Hub for Android	47
Secure Hub 23.4.0	47
Secure Hub for Android	47
Secure Hub 23.2.0	47
Secure Hub for Android	47
Secure Hub 22.11.0	48
Secure Hub for Android	48
Secure Hub 22.9.0	48
Secure Hub for Android	48
Secure Hub 22.7.0	49
Secure Hub for Android	49
Secure Hub 22.6.0	50
Secure Hub for Android	50

Secure Hub 22.5.0	50
Secure Hub for iOS	50
Secure Hub 22.4.0	50
Secure Hub for Android	50
Secure Hub 22.2.0	50
Secure Hub for iOS	50
Secure Hub for Android	50
Secure Hub 21.11.0	50
Secure Hub for Android	50
Secure Hub 21.10.0	50
Secure Hub for iOS	50
Secure Hub for Android	51
Secure Hub 21.8.0	51
Secure Hub for iOS	51
Secure Hub 21.7.1	51
Secure Hub for Android	51
Secure Hub 21.7.0	51
Secure Hub for iOS	51
Secure Hub for Android	51
Secure Hub 21.6.0	51
Secure Hub for iOS	51
Secure Hub for Android	52
Secure Hub 21.5.1	52
Secure Hub for iOS	52
Secure Hub for Android	52
Secure Hub 21.5.0	52
Secure Hub for iOS	52
Secure Hub 21.4.0	52

Secure Hub 21.3.2	52
Secure Hub for iOS	52
Secure Hub 21.3.0	52
Secure Hub 21.2.0	52
Secure Hub for Android	52
Secure Hub 21.1.0	52
Secure Hub for iOS	52
Secure Hub for Android	53
Secure Hub 20.12.0	53
Secure Hub for iOS	53
Secure Hub for Android	53
Secure Hub 20.11.0	53
Secure Hub for Android	53
Secure Hub 20.10.5	53
Secure Hub 20.9.0	53
Secure Hub for iOS	53
Secure Hub for Android	53
Secure Hub 20.7.5	53
Secure Hub for Android	53
Secure Hub 20.6.5	54
Secure Hub for Android	54
Secure Hub for iOS	54
Secure Hub 20.3.0	54
Secure Hub for iOS	55
Secure Hub 20.2.0	55
Secure Hub for iOS	55
Secure Hub 20.1.5	55
Secure Hub 19.12.5	55

Secure Hub 19.11.5	55
Secure Hub 19.10.5	56
Secure Hub for Android	56
Secure Hub 19.10.0	56
Secure Hub 19.9.5	56
Secure Hub for iOS	56
Secure Hub for Android	56
Secure Hub 19.9.0	56
Secure Hub for iOS	56
Secure Hub for Android	56
Secure Hub for Android 19.8.5	56
Secure Hub 19.8.0	57
Secure Hub for iOS	57
Secure Hub for Android	57
Secure Hub 19.7.5	57
Secure Hub for iOS	57
Secure Hub for Android	57
Secure Hub 19.3.5 to 19.6.6	57
Secure Hub 19.3.0	57
Secure Hub 19.2.0	57
Secure Hub 19.1.5	58
Secure Hub 19.1.0	58
Secure Hub 18.12.0	58
Secure Hub 18.11.5	58
Secure Hub 18.10.0	58
Secure Hub 10.8.60 to 18.9.0	59
Secure Hub 10.8.60	59
Secure Hub 10.8.55	60

Administering Secure Hub	61
Citrix PIN	61
Certificate pinning	62
Certificate + one-time-password authentication	63
Port requirement for ADS connectivity for Android devices	68
Disabling the Delete Account option	70
Using Secure Hub	71
Automatic enrollment in Secure Mail	73
Customized Store	74
Configured Help options	75
Location policies	76
Crash collection and analysis	76
Generate device side logs for Secure Hub	76
Known and fixed issues	78
Secure Hub for iOS 26.8.1	78
Fixed issues	78
Known issues	78
Secure Hub for Android 26.8.0	78
Fixed issues	78
Known issues	78
Secure Hub for iOS 26.8.0	79
Fixed issues	79
Known issues	79
Secure Hub for Android 26.5.0	79
Fixed issues	79
Known issues	79
Secure Hub for Android 26.2.0	79
Fixed issues	79

Known issues	80
Secure Hub for Android 25.10.0	80
Fixed issues	80
Known issues	80
Secure Hub for iOS 25.8.0	80
Fixed issues	80
Known issues	80
Secure Hub for Android 25.7.0	80
Fixed issues	80
Known issues	80
Secure Hub for iOS 25.6.0	81
Fixed issues	81
Known issues	81
Secure Hub for Android 25.4.0	81
Fixed issues	81
Known issues	81
Secure Hub for iOS 25.1.0	81
Fixed issues	81
Known issues	81
Secure Hub for Android 25.1.0	82
Fixed issues	82
Known issues	82
Secure Hub for iOS 24.11.0	82
Fixed issues	82
Known issues	82
Secure Hub for Android 24.10.0	82
Fixed issues	82
Known issues	82

Secure Hub for iOS 24.9.0	82
Fixed issues	82
Known issues	82
Secure Hub for Android 24.8.0	83
Fixed issues	83
Known issues	83
Secure Hub for Android 24.6.0	83
Fixed issues	83
Known issues	83
Secure Hub for iOS 24.5.0	83
Fixed issues	83
Known issues	83
Secure Hub for Android 24.3.0	83
Fixed issues	83
Known issues	83
Secure Hub for iOS 24.1.0	84
Fixed issues	84
Secure Hub for Android 23.12.0	84
Fixed issues	84
Secure Hub for iOS 23.11.0	84
Fixed issues	84
Secure Hub for Android 23.10.0	85
Fixed issues	85
Known issues	85
Secure Hub for Android 23.9.0	85
Fixed issues	85
Known issues	85
Secure Hub for iOS 23.8.1	85

Fixed issues	85
Known issues	85
Secure Hub for iOS 23.8.0	86
Fixed issues	86
Known issues	86
Known and fixed issues in older versions	86
History of Secure Hub known and fixed issues	87
Secure Hub for Android 23.7.0	87
Fixed issues	87
Known issues	87
Secure Hub for iOS 23.4.0	88
Fixed issues	88
Known issues	88
Secure Hub for Android 23.4.1	88
Fixed issues	88
Known issues	88
Secure Hub for Android 23.4.0	88
Fixed issues	88
Known issues	88
Secure Hub for Android 23.2.0	89
Fixed issues	89
Secure Hub 22.11.0	89
Secure Hub 22.9.0	89
Secure hub 22.7.0	90
Fixed issues	90
Secure Hub 22.6.0	90
Secure Hub 22.5.0	90
Secure Hub 22.4.0	90

Secure Hub 22.2.0	90
Known issues in Secure Hub 22.2.0	90
Fixed issues in Secure Hub 22.2.0	90
Secure Hub for iOS	90
Secure Hub for Android	91
Secure Hub 21.11.0	91
Known issues in Secure Hub 21.11.0	91
Fixed issues in Secure Hub 21.11.0	91
Secure Hub for Android	91
Secure Hub 21.10.0	92
Known issues in Secure Hub 21.10.0	92
Fixed issues in Secure Hub 21.10.0	92
Secure Hub for iOS	92
Secure Hub for Android	92
Secure Hub 21.8.0	92
Secure Hub for iOS	92
Known issues in Secure Hub 21.8.0	92
Fixed issues in Secure Hub 21.8.0	92
Secure Hub 21.7.1	92
Secure Hub for Android	92
Known and fixed issues in earlier versions	93
Secure Hub 21.7.1	93
Secure Hub for Android	93
Secure Hub 21.7.0	93
Secure Hub for iOS	93
Secure Hub for Android	93
Known issues in Secure Hub 21.7.0	93
Fixed issues in Secure Hub 21.7.0	93

Secure Hub 21.6.0	93
Secure Hub for iOS	93
Known issues in Secure Hub 21.6.0	93
Fixed issues in Secure Hub 21.6.0	93
Secure Hub for Android	94
Known issues in Secure Hub 21.6.0	94
Fixed issues in Secure Hub 21.6.0	94
Secure Hub 21.5.1	94
Secure Hub for iOS	94
Secure Hub for Android	94
Secure Hub 21.5.0	94
Known issues in Secure Hub 21.5.0	94
Fixed issue in Secure Hub 21.5.0	94
Secure Hub 21.4.0	94
Secure Hub 21.3.2	95
Secure Hub for iOS	95
Known issues in Secure Hub 21.3.2	95
Fixed issue in Secure Hub 21.3.2	95
Secure Hub 21.3.0	95
Known issue in Secure Hub 21.3.0	95
Fixed issues in Secure Hub 21.3.0	95
Secure Hub 21.2.0	95
Secure Hub for Android	95
Known issues in Secure Hub 21.2.0	95
Fixed issues in Secure Hub 21.2.0	96
Secure Hub 21.1.0	96
Known issues in Secure Hub 21.1.0	96
Fixed issues in Secure Hub 21.1.0	96

Secure Hub 20.12.0	96
Known issues in Secure Hub 20.12.0	96
Fixed issues in Secure Hub 20.12.0	96
Secure Hub 20.11.0	97
Secure Hub for Android	97
Known issues in Secure Hub 20.11.0	97
Fixed issues in Secure Hub 20.11.0	97
Secure Hub 20.10.5	97
Known issues in Secure Hub 20.10.5	97
Fixed issues in Secure Hub 20.10.5	97
Secure Hub 20.9.0	97
Known issues in Secure Hub 20.9.0	97
Fixed issues in Secure Hub 20.9.0	98
Secure Hub 20.7.5	98
Known issues in Secure Hub 20.7.5	98
Fixed issues in Secure Hub 20.7.5	98
Secure Hub 20.6.5	98
Secure Hub 20.3.0	98
Secure Hub for iOS	98
Secure Hub 20.2.0	98
Secure Hub for iOS	98
Known issues in Secure Hub 20.2.0	99
Fixed issues in Secure Hub 20.2.0	99
Secure Hub 20.1.5	99
Secure Hub 19.12.5	99
Known issues in Secure Hub 19.12.5	99
Fixed issues in Secure Hub 19.12.5	99
Secure Hub 19.11.5	99

Known issues in Secure Hub 19.11.5	99
Fixed issues in Secure Hub 19.11.5	99
Secure Hub 19.10.5	100
Secure Hub for Android	100
Known issues in Secure Hub 19.10.5	100
Fixed issues in Secure Hub 19.10.5	100
Secure Hub 19.10.0	100
Known issues in Secure Hub 19.10.0	100
Fixed issues in Secure Hub 19.10.0	100
Secure Hub 19.9.5	100
Secure Hub 19.9.0	100
Known issues in Secure Hub 19.9.0	100
Fixed issues in Secure Hub 19.9.0	101
Secure Hub 19.8.5	101
Secure Hub 19.8.0	101
Known issues in Secure Hub 19.8.0	101
Fixed issues in Secure Hub 19.8.0	101
Secure Hub 19.7.5	101
Known issues in Secure Hub 19.7.5	101
Fixed issues in Secure Hub 19.7.5	101
Secure Hub 19.6.5	102
Known issues in Secure Hub 19.6.5	102
Fixed issues in Secure Hub 19.6.5	102
Secure Hub 19.5.5	102
Known issues in Secure Hub 19.5.5	102
Fixed issues in Secure Hub 19.5.5	102
Secure Hub 19.5.0	103
Known issues in Secure Hub 19.5.0	103

Fixed issues in Secure Hub 19.5.0	103
Secure Hub 19.4.5	103
Known issues in Secure Hub 19.4.5	103
Fixed issues in Secure Hub 19.4.5	103
Secure Hub 19.3.5	103
Known issues in Secure Hub 19.3.5	103
Fixed issues in Secure Hub 19.3.5	104
Secure Hub 19.3.0	104
Known issues in Secure Hub 19.3.0	104
Fixed issues in Secure Hub 19.3.0	104
Secure Hub 19.2.0	105
Known issues in Secure Hub 19.2.0	105
Fixed issues in Secure Hub 19.2.0	105
Secure Hub 19.1.5	105
Known issues in Secure Hub 19.1.5	105
Fixed issues in Secure Hub 19.1.5	105
Secure Hub 19.1.0	106
Known issues in Secure Hub 19.1.0	106
Fixed issues in Secure Hub 18.12.0	106
Secure Hub 18.11.0	106
Fixed issues in Secure Hub 18.11.0	106
Secure Hub 18.10.5	106
Fixed issues in Secure Hub 18.10.5	106
Secure Hub versions 10.8.25 to 18.10.6	107
Fixed issues in Secure Hub versions 10.8.25 to 18.10.6	107
Secure Hub 18.10.0	107
Fixed issues in Secure Hub 18.10.0	107
Secure Hub 10.8.60	107

Fixed issues in Secure Hub 10.8.60	107
Secure Hub 10.8.55	108
Fixed issues in Secure Hub 10.8.55	108
MDX-related fixed issues in version 10.8.55	108
Secure Hub 10.8.55	108
Known issue in Secure Hub 10.8.55	108
Secure Hub 10.8.50	108
Known issue in Secure Hub 10.8.50	108
Secure Hub 10.8.35	108
Fixed issues in Secure Hub 10.8.35	108
Secure Hub 10.8.25	109
Fixed issues in Secure Hub 10.8.25	109
Secure Hub 10.8.20	109
Fixed issues in Secure Hub 10.8.20	109
Secure Hub 10.8.15	109
Fixed issues in Secure Hub 10.8.15	109
Secure Hub 10.8.10	109
Fixed issues in Secure Hub 10.8.10	109
Secure Hub for Android and iOS - Preview	110
Feature flag management	111
Authentication prompt scenarios	112
Credential types	114
About Secure Hub screen flips	116
Passcode complexity for device passcode (Android 12+)	117
Enrolling devices by using derived credentials	119
Device enrollment steps when using derived credentials	119
Configure hint through the Citrix Endpoint Management™ console	127
Configure hint as text	127

Configure hint text with webpage link	128
Compliance check on Android devices (Technical Preview)	131

Citrix Secure Hub™

Citrix Secure Hub is the launchpad for the Citrix Endpoint Management™ (formerly, XenMobile) experience. Users enroll their devices in Secure Hub to gain access to the Store. From the store, they can add Citrix-developed mobile productivity apps and third-party apps.

For Secure Hub and other mobile productivity apps system requirements, see [System requirements](#).

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.

In addition to providing a portal for Citrix apps, Secure Hub 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 repeatedly enter another credential like their Active Directory user name and password.

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. For information about enabling fingerprint authentication, see [Fingerprint or touch ID authentication](#).

Certificate pinning

Secure Hub for iOS and Android supports SSL certificate pinning. This feature ensures that the certificate signed by your enterprise is used when Citrix clients communicate with Endpoint Management. Certificate pinning prevents 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 in AutoDiscovery Service is set **ON**. For details, see [Endpoint Management AutoDiscovery Service](#).
- Private/self-signed CAs and the AutoDiscovery Service (ADS) is 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 will 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 Endpoint Management administrator.
- The PEM-formatted certificates you want added to the domain.

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

You can configure Citrix ADC so that Secure Hub authenticates by 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, 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 to allow Secure Hub to do this.

Note:

If different logon types are set in Endpoint Management and Citrix ADC, the Citrix ADC configuration overrides the configuration. For details, see [Citrix Gateway and Endpoint Management](#).

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

2. Click **Add**.

The **Create Rewrite Action** screen appears.

3. Fill in each field as shown in the following figure and then click **Create**.

Create Rewrite Action

Name*
InsertGatewayAuthTypeHeader ?

Type*
INSERT_HTTP_HEADER

Use this action type to insert a header.

Header Name*
X-Citrix-AM-GatewayAuthType

Expression
Expression Editor

Operators Saved Policy Expressions Frequently Used Expressions Clear

"CertAndRSA"

Evaluate

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

Comments

Create Close

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

NetScaler > AppExpert > Rewrite > Rewrite Actions

Add Edit Delete Action Show built-in Rewrite Actions Search

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

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

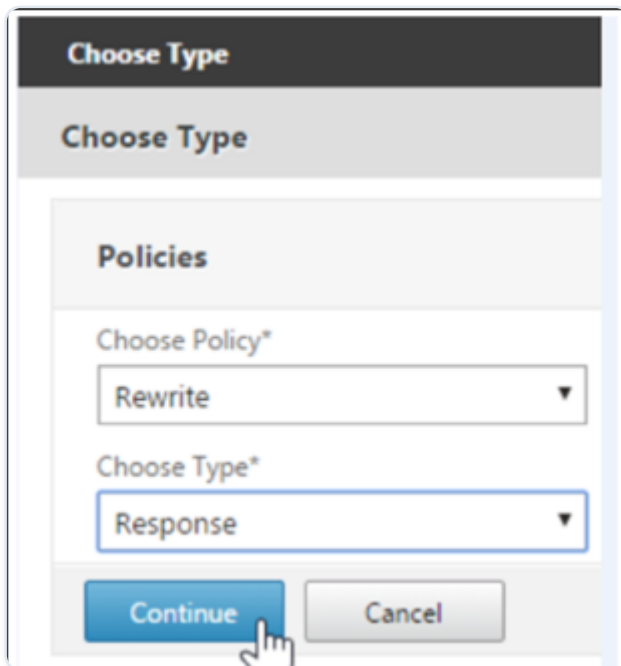
The screenshot shows the NetScaler Configuration page. The left sidebar contains a navigation menu with categories like System, AppExpert, Traffic Management, Optimization, Security, and NetScaler Gateway. The 'Virtual Servers' option under NetScaler Gateway is selected. The main content area displays the 'NetScaler Gateway Virtual Servers' configuration page. At the top, there are buttons for 'Add', 'Edit', 'Delete', 'Statistics', 'Visualizer', and an 'Action' dropdown. Below these is a table with columns: Name, State, IP Address, Port, Protocol, Maximum Users, Current Users, and Total Connected Users. The table contains two entries: '_XM_gwcamamappc8' and 'SessionTransfer', both with a state of 'Up'. The 'Edit' button is highlighted with a mouse cursor.

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

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

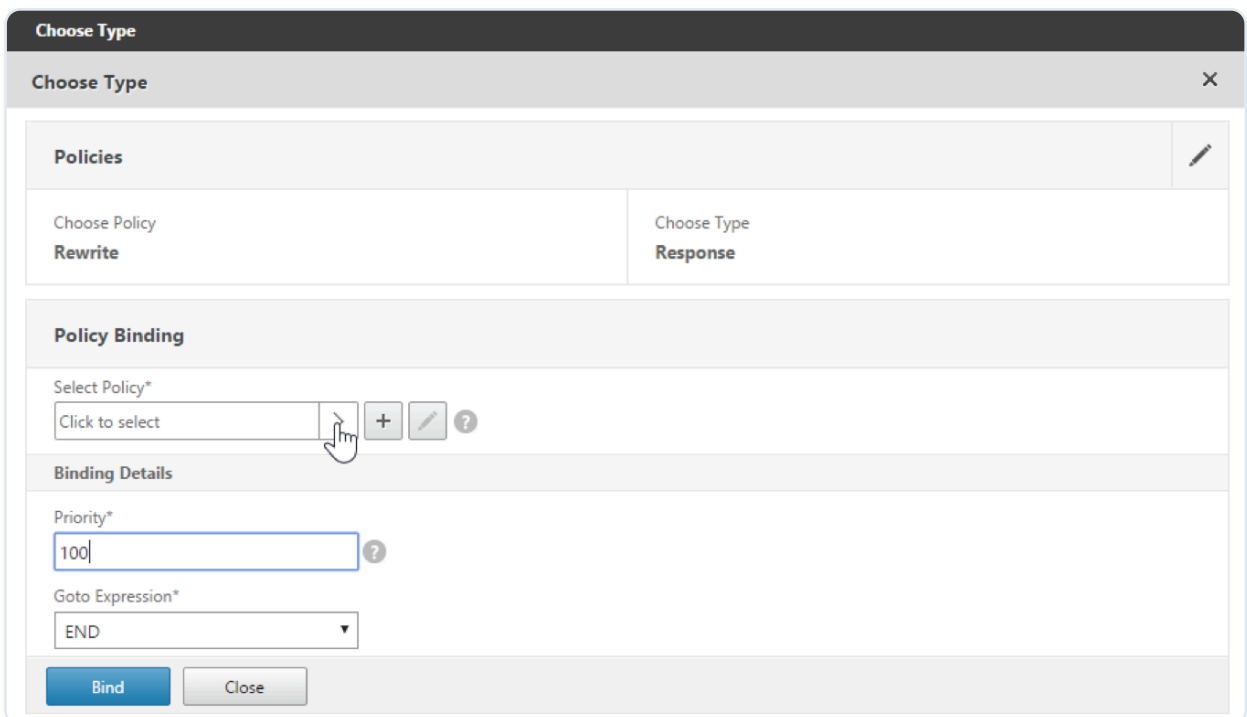
The screenshot shows the NetScaler configuration page for a specific virtual server. The 'Profiles' section shows 'Net Profile', 'TCP Profile', and 'HTTP Profile' set to 'nshttp_default_strict_validation'. The 'Published Applications' section shows 'No Next HOP Server', '1 STA Server', and 'No Url'. The 'Other Settings' section shows 'ICMP Virtual Server Response' as 'Passive', 'RHI State' as 'Passive', 'Redirect to Home page' as 'true', 'Listen Priority' as 'NONE', 'Listen Policy Expression' as 'NONE', 'ShareFile' as 'https://camamappc8.camam.net:8443', 'AppController' as '3', and 'L2 Connection' as 'false'. The 'Policies' section is expanded, showing 'Request Policies', '3 Session Policies', '2 ClientlessAccess Policies', and '5 Cache Policies'. A mouse cursor is clicking the '+' button in the 'Policies' section header to add a new policy.

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



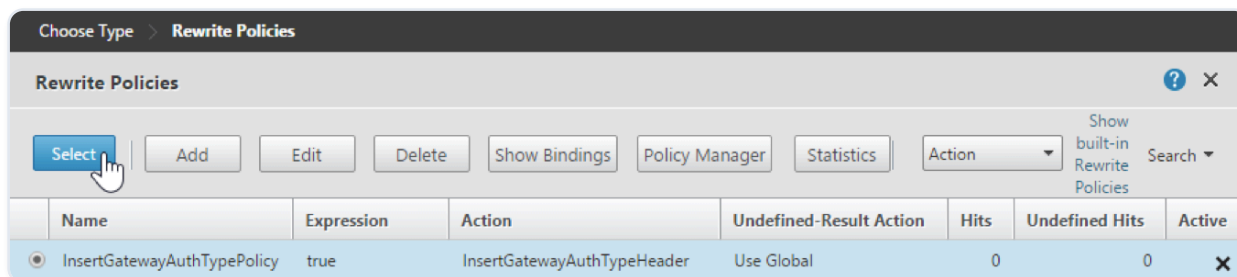
10. Click **Continue**.

The **Policy Binding** section expands.

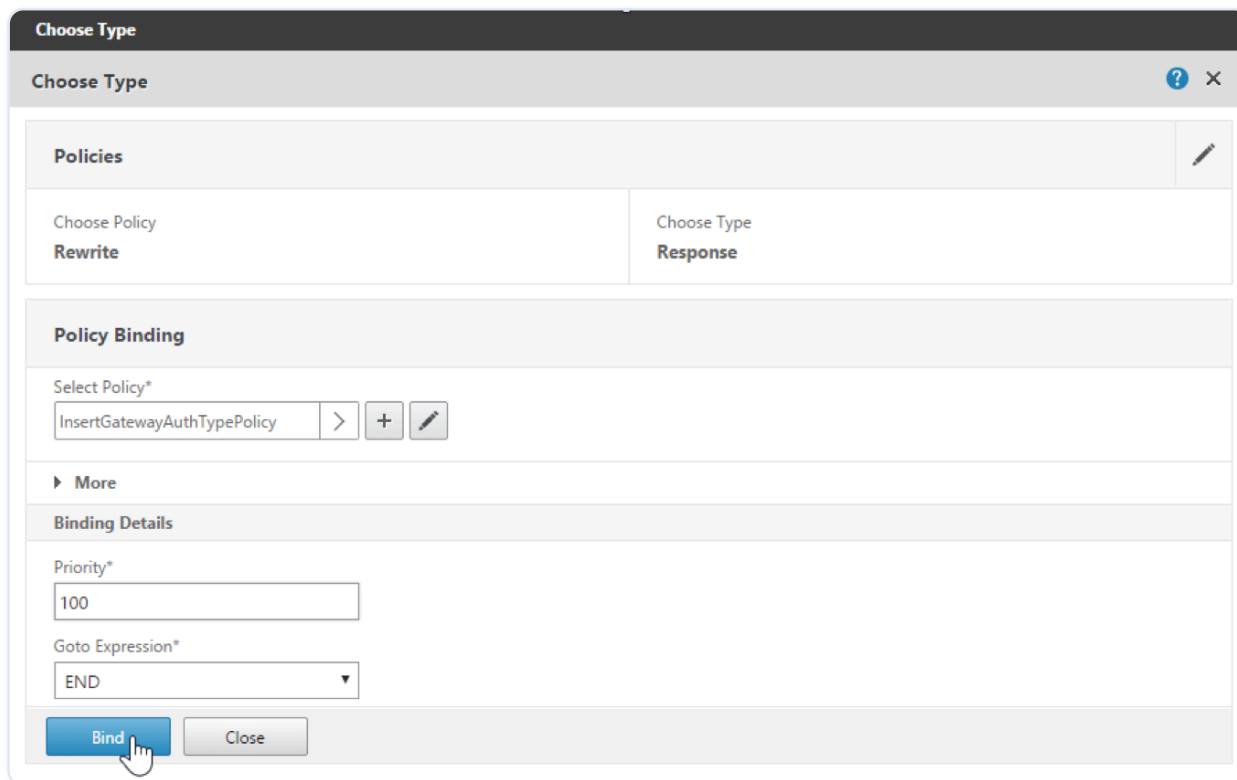


11. Click **Select Policy**.

A screen with available policies appears.



12. Click the row of the policy you just 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.

Enable DH Param DISABLED	Clear Text Port 0	SSLv2 Redirect DISABLED
Enable Ephemeral RSA ENABLED	Enable Cipher Redirect DISABLED	SSLv2 DISABLED
Refresh Count 0	Client Authentication ENABLED	SSLv3 ENABLED
Enable Session Reuse ENABLED	Client Certificate Mandatory	TLSv1 ENABLED
Time-out 120	Send Close-Notify YES	TLSv1.1 ENABLED
SSL Redirect DISABLED	PUSH Encryption Trigger Always	TLSv1.2 ENABLED
	SNI Enable DISABLED	

Published Applications	
No Next HOP Server	>
1 STA Server	>
No Uri	>

Other Settings	
ICMP Virtual Server Response Passive	Listen Priority None
RHI State Passive	Listen Policy Expression None
Redirect to Home page true	ShareFile AppController https://xms3.dm.com:8443
	L2 Connection false

Policies	
Request Policies	>
3 Session Policies	>
2 ClientlessAccess Policies	>
4 Cache Policies	>
Response Policies	>
1 Rewrite Policy	>

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

VPN Virtual Server Rewrite Policy Binding					
VPN Virtual Server Rewrite Policy Binding					
Add Binding		Unbind		Edit	
Priority	Policy Name	Expression	Action	Goto Expression	
100	InsertGatewayAuthTypeHeaderPolicy	true	InsertGatewayAuthTypeHeader	END	
Close					

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 Endpoint Management documentation. Note that 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 strongly discouraged from upgrading to Secure Hub 10.2. If you have any questions, please contact Citrix support.

To enable certificate pinning, you 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 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
<code>discovery.mdm.ze nprise.com</code>	52.5.138.94	443	Secure Hub - ADS Communication
<code>discovery.mdm.ze nprise.com</code>	52.1.30.122	443	Secure Hub - ADS Communication
<code>ads.xm.cloud.com</code> : note that SecureHub version 10.6.15 and later uses	34.194.83.188	443	Secure Hub - ADS Communication

FQDN	IP ADDRESS	PORT	IP AND PORT USAGE
ads.xml.cloud.com .			
ads.xml.cloud.com : note that SecureHub version 10.6.15 and later uses ads.xml.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, provided that 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

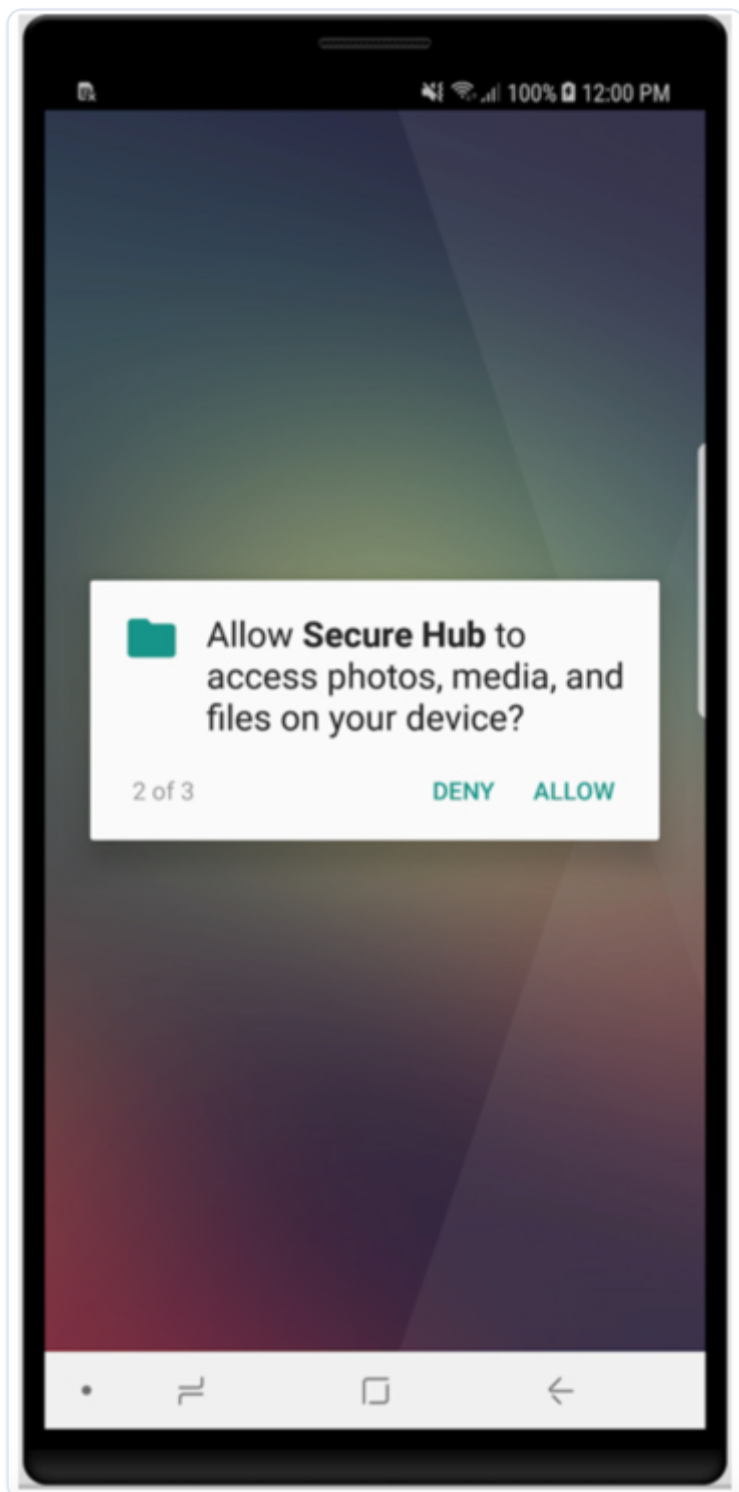
Secure Hub allows you to monitor and enforce mobile policies while providing access to the Store and live support. Users begin by downloading Secure Hub onto their devices from the Apple, Android, or Windows app store.

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 [Users, accounts, roles, and enrollment](#).

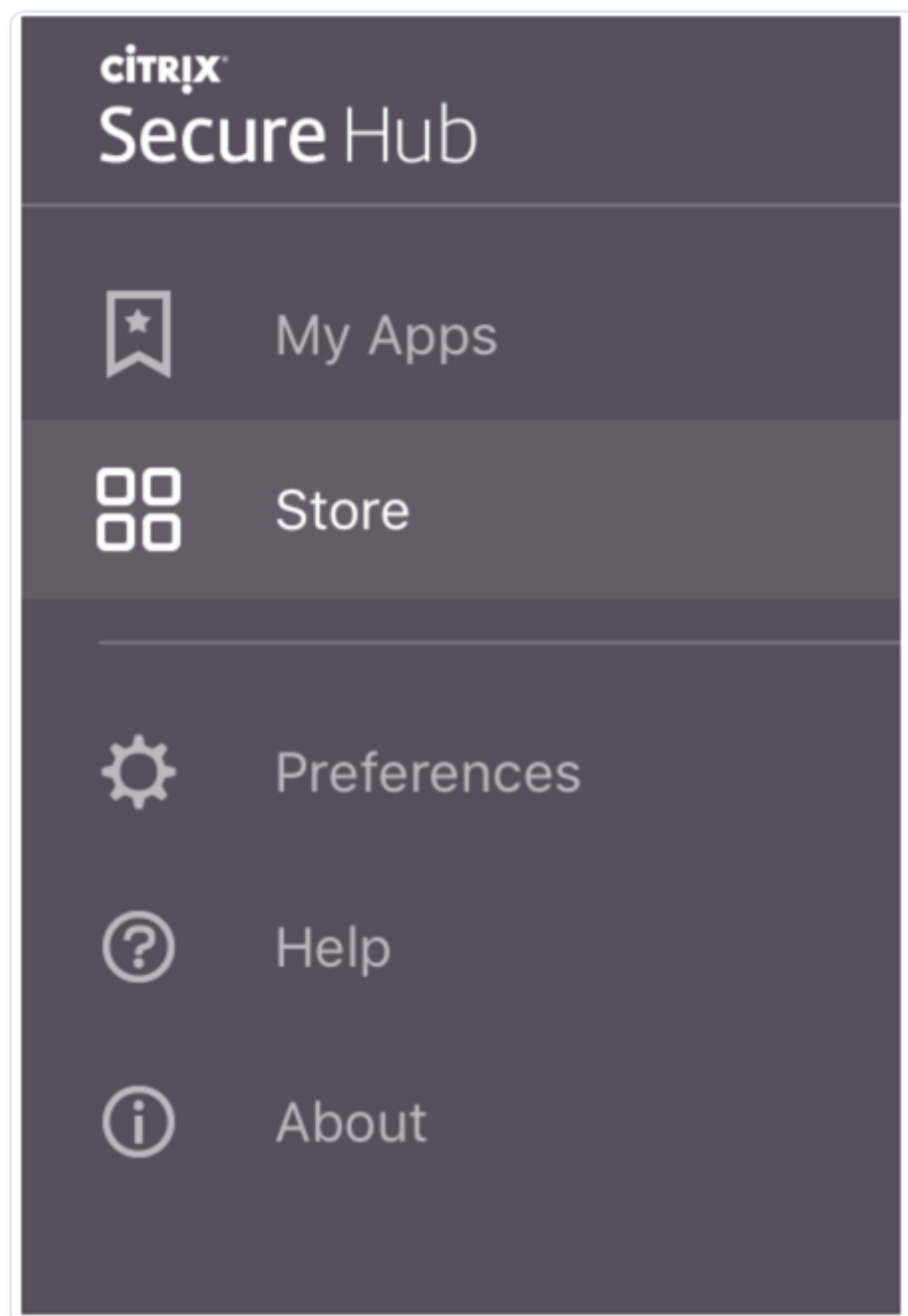
On Secure Hub for Android, during initial installation and enrollment, the following message appears: Allow Secure Hub to access photos, media, and files on your device?

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 Endpoint Management app store, they see a message stating that the enterprise developer, Citrix, is not trusted on that iPhone and the app will 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, but the user is not required to enter any 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.

The screenshot shows the XenMobile web interface. The top navigation bar is green with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. On the right, there's a gear icon and a user dropdown showing 'administrator'. The main content area has a breadcrumb 'Settings > Client Branding'. The title is 'Client Branding' with a subtitle: 'You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.' The form includes: 'Store name*' with a text box containing 'Store'; 'Default store view' with radio buttons for 'Category' and 'A-Z' (selected); 'Device' with radio buttons for 'Phone' (selected) and 'Tablet'; 'Branding file' with a text box and a green 'Browse' button. A 'Note' section lists requirements for the branding file: it must be a .png, have specific dimensions for 1x and 2x scales, be named 'Header.png' and 'Header@2x.png', and be a zip file. At the bottom right are 'Cancel' and 'Save' buttons.

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.

The screenshot shows the XenMobile 'Configure' page. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Apps' tab is selected, and the 'MDX' sidebar on the left lists steps: '1 App Information' (selected), '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. The main area is titled 'App Information' and contains the following fields:

- Name:** A text field containing 'Workmail' with a question mark icon to its right.
- Description:** A large text area that is currently empty, with a question mark icon to its right.
- App category:** A dropdown menu currently set to 'Workapps'.

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**.

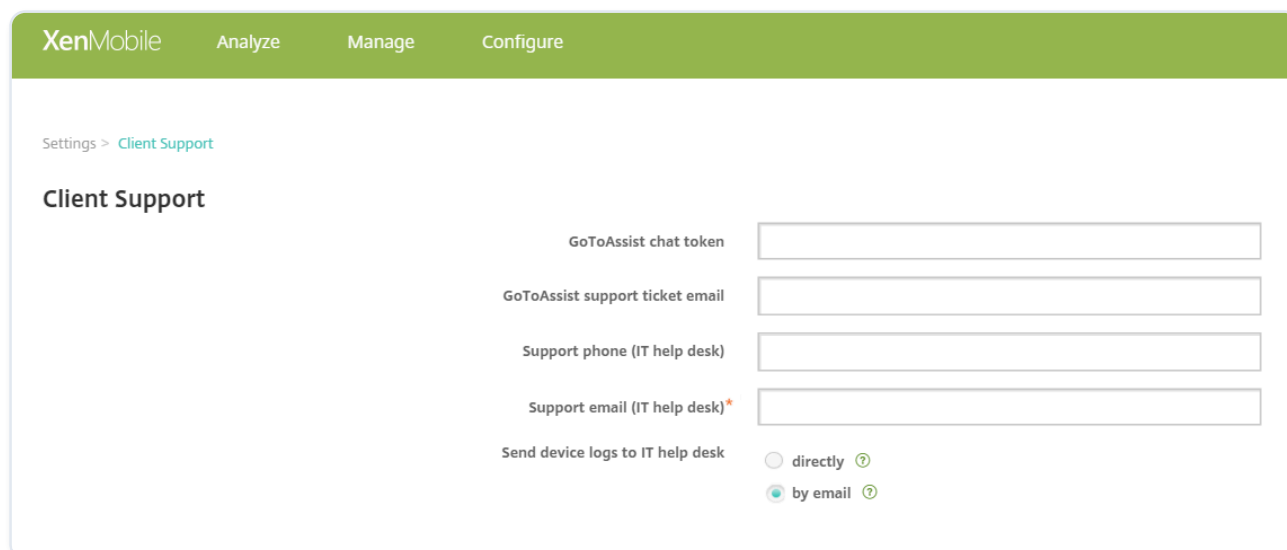
Secure Hub also offers users a variety of ways to get help. On tablets, tapping the question mark in the upper-right corner opens help options. On phones, users tap the hamburger menu icon in the upper-left corner and then tap **Help**.

The screenshot shows the 'Help Desk' screen. At the top, there is a 'Close' button and the title 'Help Desk'. Below the title bar, there are three main options, each with a right-pointing chevron:

- Your IT Department
- Report Issue
- Send Feedback to Citrix

At the bottom of the screen, there is a 'Citrix Support' button.

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.



XenMobile Analyze Manage Configure

Settings > [Client Support](#)

Client Support

GoToAssist chat token

GoToAssist support ticket email

Support phone (IT help desk)

Support email (IT help desk)*

Send device logs to IT help desk

☐ directly ?

☒ by email ?

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

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

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

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

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](#). Additionally, Secure Hub automatically collects and analyzes failure information so you can see what led to a particular failure. This function is supported by the software Crashlytics.

Citrix Secure Hub™

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 9.x and iOS 11.x versions of Secure Hub in Apr 2025.

What's new in the current version

Secure Hub for iOS 26.8.1

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

For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for Android 26.8.0

Set an auto-launch app in the Launcher Configuration policy in COSU mode

On Android Enterprise kiosk (COSU) devices running Citrix Launcher, administrators can now set an auto-launch app in the Launcher Configuration policy to start one managed app automatically at device boot. Secure Hub forwards the setting to Citrix Launcher, which performs the launch.

Automatic detection and renewal of the MDM device certificate

Secure Hub for Android now automatically detects an invalid, missing, or expired MDM device certificate and renews it in the background. This restores device connectivity without the user having to run manual certificate troubleshooting or re-enroll the device.

For more information on bug fixes, see [Known and fixed issues](#).

What's new in earlier versions

Secure Hub for iOS 26.8.0

Support for iOS/iPadOS 27

Starting with the release of Secure Hub 26.8.0 for iOS, the app is compatible with iOS/iPadOS 27. You can upgrade your device to iOS/iPadOS 27 and continue using the latest version of Secure Hub.

For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for Android 26.5.0

Support for Android 17

Starting with the release of Secure Hub 26.5.0 for Android, the app is compatible with Android 17. You can upgrade your device to Android 17 and continue using the latest version of Secure Hub.

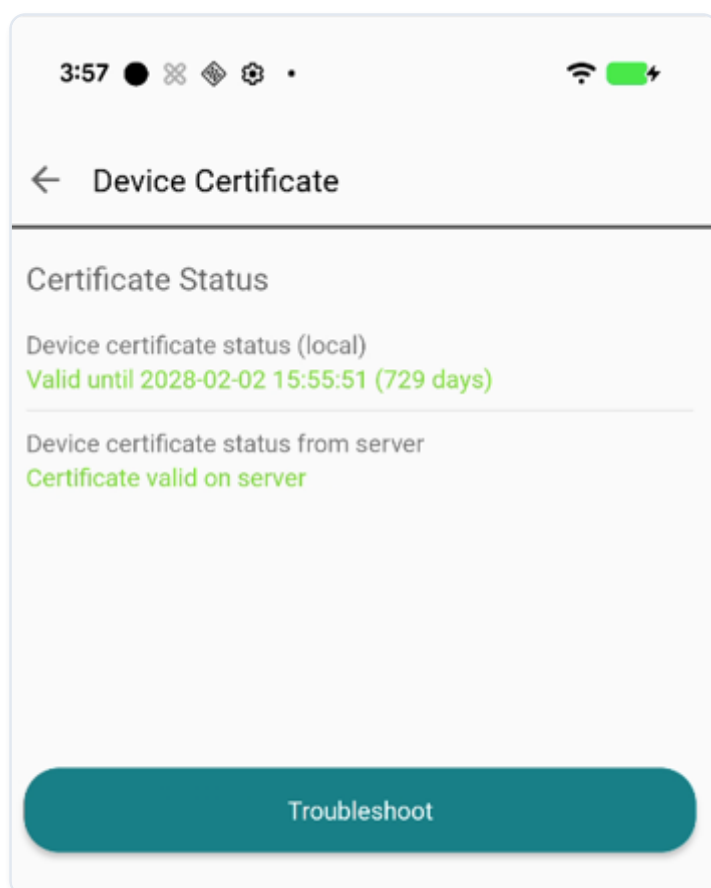
For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for Android 26.2.0

Device Certificate troubleshooting enhancement

Starting with the release of Secure Hub 26.2.0 for Android, Secure Hub includes a self-service device certificate troubleshooting tool that helps diagnose and resolve device connectivity issues caused by revoked or invalid client certificates.

When a certificate problem is detected, the tool automatically attempts to renew the certificate to restore connectivity. To access this tool, go to **Help > Troubleshoot > Device Certificate** and tap **Troubleshoot**.



For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for iOS 25.8.0

Support for iOS 26

Starting with the release of Secure Hub 25.8.0 for iOS, the app supports the devices running on iOS 26. Upgrading to Secure Hub version 25.8.0 ensures continuous support and compatibility for those devices that are updated to iOS 26.

For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for Android 25.10.0

Support for 16KB memory page size

Starting with the release of Secure Hub 25.10.0 for Android, the app supports 16KB memory page size to optimize performance and comply with Google Play requirements.

For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for Android 25.7.0

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

For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for iOS 25.6.0

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

For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for Android 25.4.0

Support for Android 16

Starting with the release of Secure Hub 25.4.0 for Android, the app is compatible with Android 16. You can upgrade your device to Android 16 and continue using the latest version of Secure Hub.

Support for TLS 1.3 protocol

Starting with the release of Secure Hub 25.4.0 for android, the app supports the TLS 1.3 protocol on android devices. TLS 1.3 is the latest version of the TLS protocol and it offers faster performance, enhanced security, and greater resilience against cyberattacks compared to TLS 1.2. TLS 1.3 also reduces network latency, resulting in faster HTTPS connections and a better user experience.

To learn more about TLS 1.3, see [The Transport Layer Security \(TLS\) Protocol Version 1.3](#).

For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for Android 25.1.0

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

For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for iOS 25.1.0

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

For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for iOS 24.11.0

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

For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for Android 24.10.0

Support for Android 15

Upgrading the Secure Hub version to 24.10.0 ensures continuous support for devices that are updated to Android 15.

For more information on bug fixes, see [Known and fixed issues](#).

Secure Hub for iOS 24.9.0

Displays Terms and Conditions on Device Enrolment Program

Starting with Secure Hub 24.9.0 for iOS, administrators can configure the Terms and Conditions device policy through Citrix Endpoint Management (CEM). Once configured, the **Terms and Conditions** page will be displayed during the enrollment process for devices enrolled via Apple's Device Enrollment Program (DEP). This ensures that users review and acknowledge the terms and conditions before completing their enrollment, enhancing compliance and security measures during device onboarding.

Secure Hub for Android 24.8.0

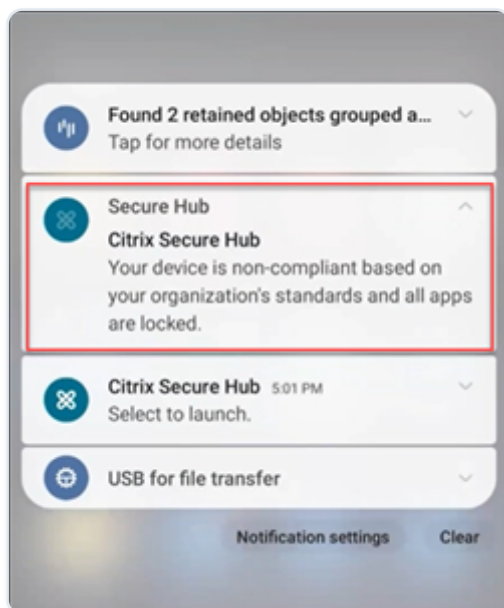
Compliance check on Android devices (Technical Preview)

NOTE:

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

Starting with this release, Secure Hub verifies the compliance of Android devices against the policies configured by admin through Citrix Endpoint Management. These compliance check includes ensuring device password strength, verifying installation of mandatory apps, and confirming removal of prohibited apps.

If a device is found not compliant with the policies set by administrator, Secure Hub locks all its apps and prompts users to resolve the compliance issues to unlock them. The following notification appears on user devices when the device is non-compliant.

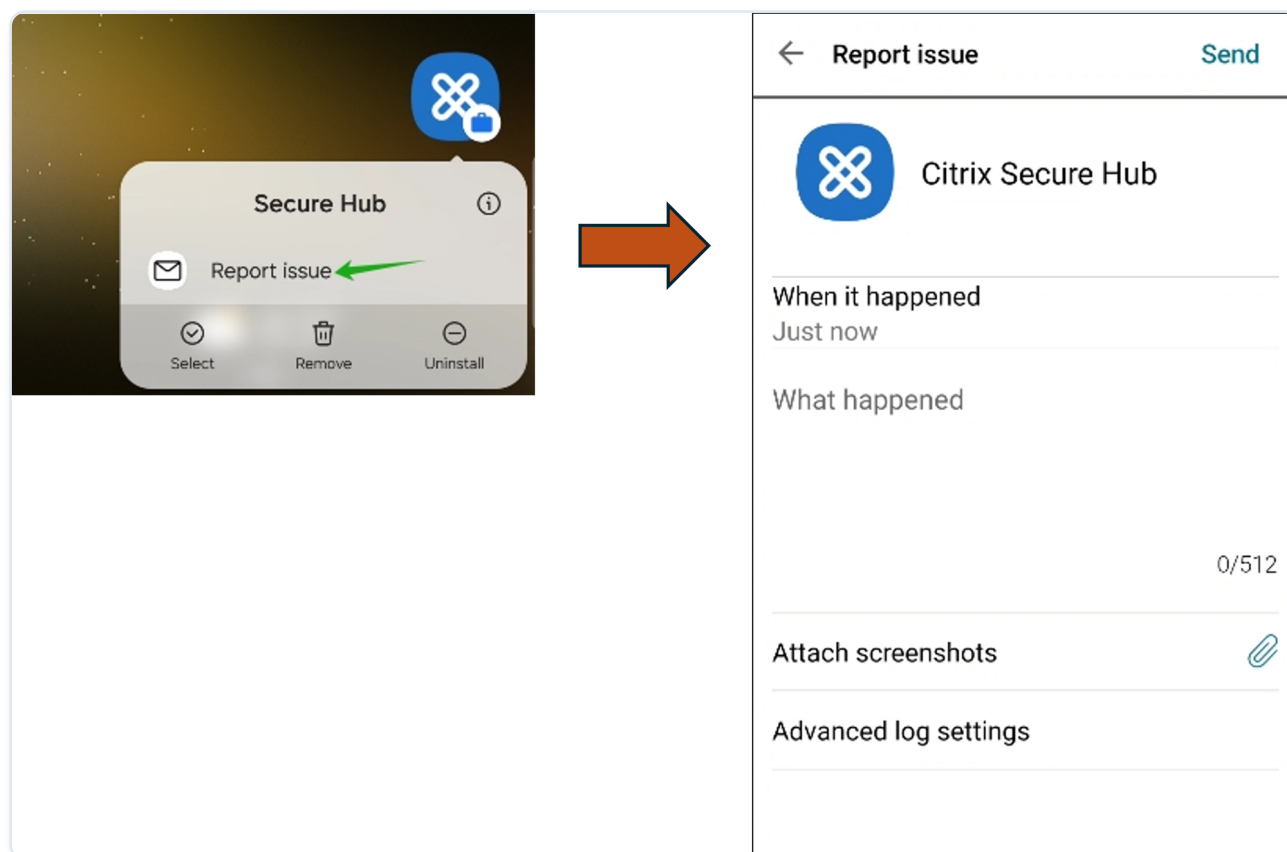


For more information, see [Compliance check on Android devices](#).

Secure Hub for Android 24.6.0

Improved log collection and reporting

Secure Hub introduces an enhanced ability to report issues and send logs seamlessly without opening Secure Hub. With this release, users can access the **Report Issue** option by long-pressing the Secure Hub app icon. Upon clicking the **Report Issue** option, Secure Hub opens the **Report Issue** page directly.



Secure Hub for iOS 24.5.0

Supports iOS 17 Return to Service

Secure Hub supports the Return to Service feature in iOS 17, which provides a more efficient and secure Mobile Device Management (MDM) experience. Previously, manual configuration was required to set it up for a new user after wiping the device. Now, the Return to Service feature automates this process, whether repurposing a company device or integrating a personal device (BYOD) with correct security policies.

With the Return to Service feature, MDM server can send an erase command that includes Wi-Fi details and a default MDM enrollment profile to the user device. The device then automatically wipes all user data, connects to the specified Wi-Fi network, and re-enrolls itself back into the MDM server using the provided enrollment profile.

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

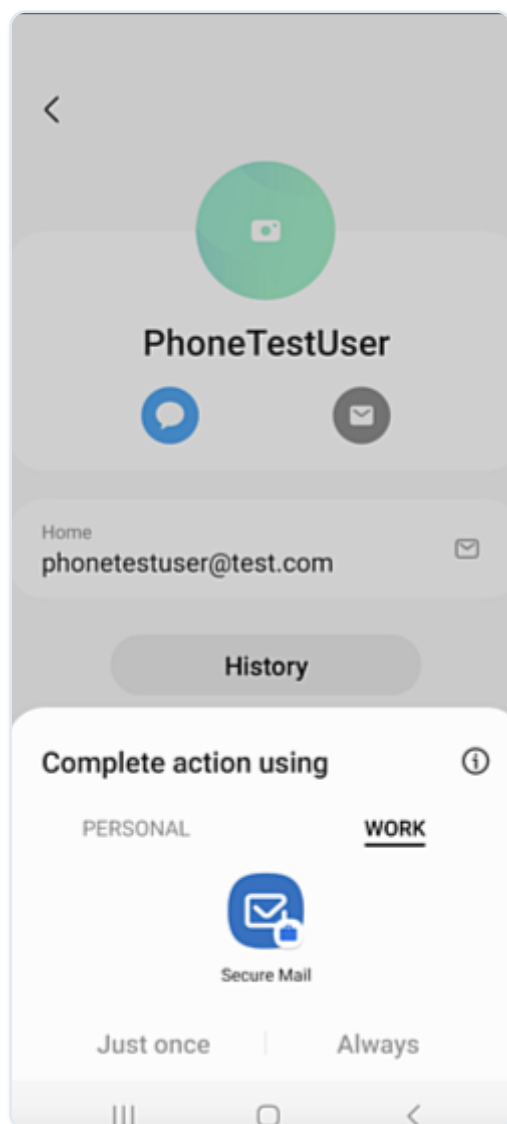
Enhanced Security with Samsung Knox

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](#).

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.



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.

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.

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.

- 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).

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.
- **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.

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.

NOTE:

If Secure Hub is not updated to version 21.7.1 before you upgrade to Android 12, your device might require a re-enrollment or a factory reset to recover prior functionality.

Citrix is committed to providing Day 1 support for Android 12 and will add further updates to subsequent versions of Secure Hub to fully support Android 12.

Secure Hub 21.7.0

Secure Hub for iOS

This release includes bug fixes.

Secure Hub for Android

This release includes bug fixes.

Secure Hub 21.6.0

Secure Hub for iOS

This release includes bug fixes.

Secure Hub for Android

This release includes bug fixes.

Secure Hub 21.5.1

Secure Hub for iOS

This release includes bug fixes.

Secure Hub for Android

This release includes bug fixes.

Secure Hub 21.5.0

Secure Hub for iOS

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

Secure Hub 21.4.0

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

Secure Hub 21.3.2

Secure Hub for iOS

This release includes bug fixes.

Secure Hub 21.3.0

This release includes bug fixes.

Secure Hub 21.2.0

Secure Hub for Android

This release includes bug fixes.

Secure Hub 21.1.0

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.

Secure Hub for Android

This release includes bug fixes.

Secure Hub 20.7.5

Secure Hub for Android

- Secure Hub for Android supports Android 11.
- **Transition from Secure Hub 32-bit to 64-bit for apps.** In Secure Hub version 20.7.5, support ends for 32-bit architecture for apps, and Secure Hub has been updated to 64-bit. Citrix recommends customers to upgrade to version 20.7.5 from 20.6.5. If users skip the upgrade to Secure Hub version 20.6.5, and instead update from 20.1.5 to 20.7.5 directly, they must

reauthenticate. Reauthentication involves entering credentials and resetting the Secure Hub PIN. Secure Hub version 20.6.5 is available in the Google Play Store.

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

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

Secure Hub 20.6.5

Secure Hub for Android

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

NOTE:

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

Secure Hub for iOS

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

Secure Hub 20.3.0

NOTE:

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

Secure Hub for iOS

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

NOTE:

New users are not prompted to install VPN.

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

Secure Hub 20.2.0

Secure Hub for iOS

This release includes bug fixes.

Secure Hub 20.1.5

This release includes:

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

Secure Hub 19.12.5

This release includes bug fixes.

Secure Hub 19.11.5

This release includes bug fixes.

Secure Hub 19.10.5

Secure Hub for Android

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

Secure Hub 19.10.0

This release includes bug fixes.

Secure Hub 19.9.5

Secure Hub for iOS

This release includes bug fixes.

Secure Hub for Android

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

For more information about the feature settings and how to configure the device policy, see [Keyguard Management device policy](#).

Secure Hub 19.9.0

Secure Hub for iOS

Secure Hub for iOS supports iOS 13.

Secure Hub for Android

This release includes bug fixes.

Secure Hub for Android 19.8.5

This release includes bug fixes.

Secure Hub 19.8.0

Secure Hub for iOS

This release includes performance enhancements and bug fixes.

Secure Hub for Android

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

Secure Hub 19.7.5

Secure Hub for iOS

This release includes performance enhancements and bug fixes.

Secure Hub for Android

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

NOTE:

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

Secure Hub 19.3.5 to 19.6.6

These releases include performance enhancements and bug fixes.

Secure Hub 19.3.0

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

Secure Hub 19.2.0

This release includes performance enhancements and bug fixes.

Secure Hub 19.1.5

Secure Hub for Android Enterprise now supports the following policies:

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

Secure Hub 19.1.0

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

Secure Hub 18.12.0

This release includes performance enhancements and bug fixes.

Secure Hub 18.11.5

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

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

Secure Hub 18.10.0

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

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

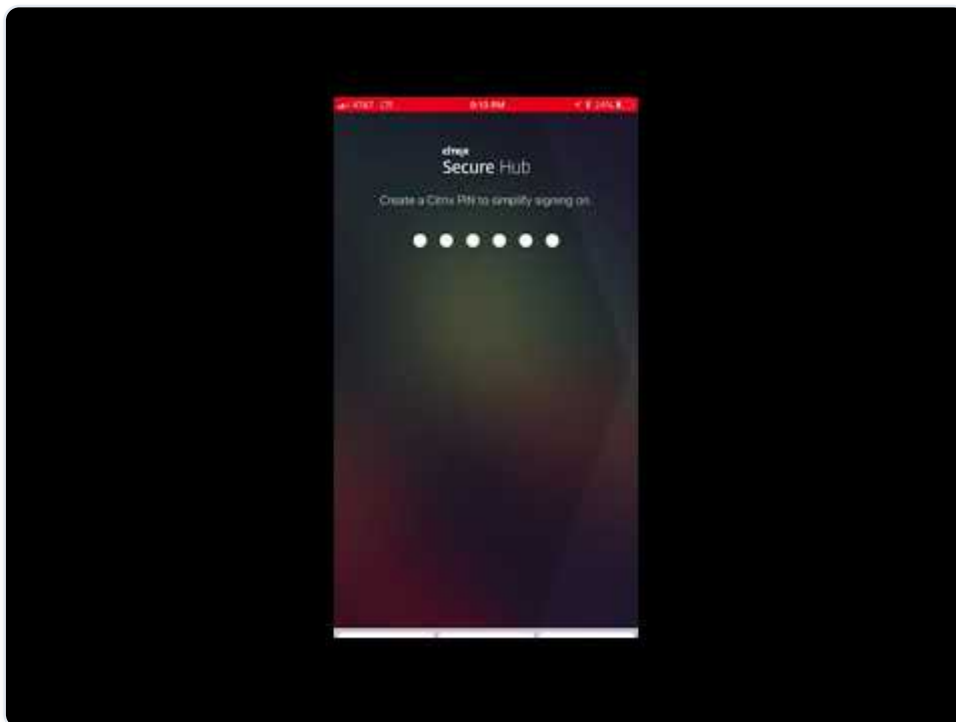
- **Support for Android SafetyNet:** You can configure Endpoint Management to use the **Android SafetyNet** feature to assess the compatibility and security of Android devices that have Secure Hub installed. The results can be used to trigger automated actions on the devices. For information, see [Android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

Secure Hub 10.8.60 to 18.9.0

These releases include performance enhancements and bug fixes.

Secure Hub 10.8.60

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



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.

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

Administering Secure Hub

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

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

IMPORTANT:

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

Citrix PIN

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

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

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

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

Certificate pinning

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

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

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

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

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

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

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

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

Certificate + one-time-password authentication

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

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

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

NOTE:

If different logon types are set for Endpoint Management and Citrix ADC, the Citrix ADC configuration overrides. For details, see [Citrix Gateway and Endpoint Management](#).

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

The **Create Rewrite Action** screen appears.

3. Fill in each field as shown in the following figure and then click **Create**.

Create Rewrite Action

Name*
InsertGatewayAuthTypeHeader ?

Type*
INSERT_HTTP_HEADER

Use this action type to insert a header.

Header Name*
X-Citrix-AM-GatewayAuthType

Expression Expression Editor

Operators Saved Policy Expressions Frequently Used Expressions Clear

"CertAndRSA"

Evaluate

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

Comments

Create Close

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

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

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

The screenshot shows the NetScaler Configuration page. The left sidebar contains a navigation menu with categories like System, AppExpert, Traffic Management, Optimization, Security, and NetScaler Gateway. The 'Virtual Servers' option under NetScaler Gateway is selected. The main content area displays a table of Virtual Servers. The 'Edit' button is highlighted with a mouse cursor.

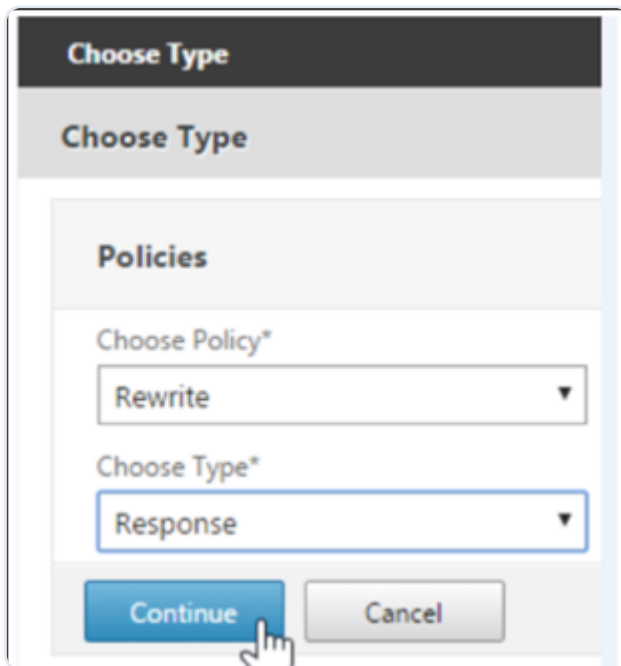
Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
_XM_gwcamamappc8	Up	10.71.12.30	443	SSL	0	3	3
SessionTransfer	Up	10.71.12.30	500	SSL	0	0	0

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

The screenshot shows the NetScaler configuration page for a specific virtual server. The 'Policies' section is expanded, and a mouse cursor is clicking the '+' button to add a new policy. The 'Policies' section lists various policy types and their counts.

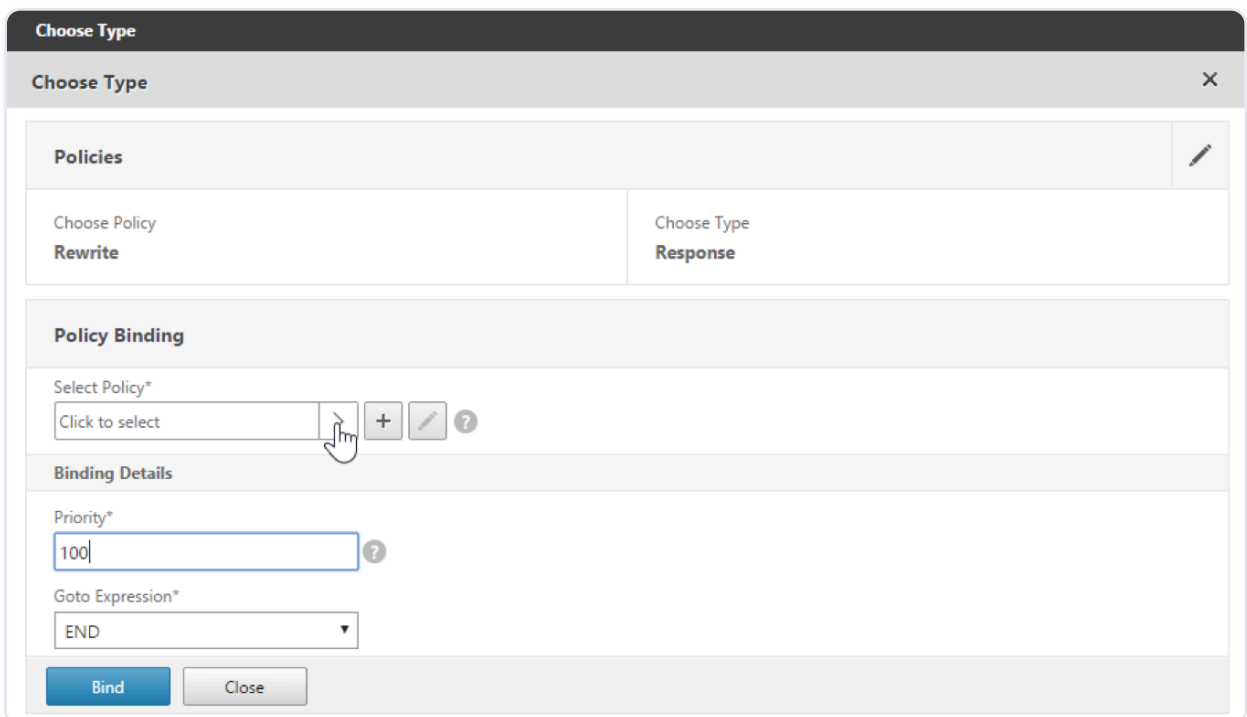
Policy Type	Count
Request Policies	3
Session Policies	2
ClientlessAccess Policies	2
Cache Policies	5

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



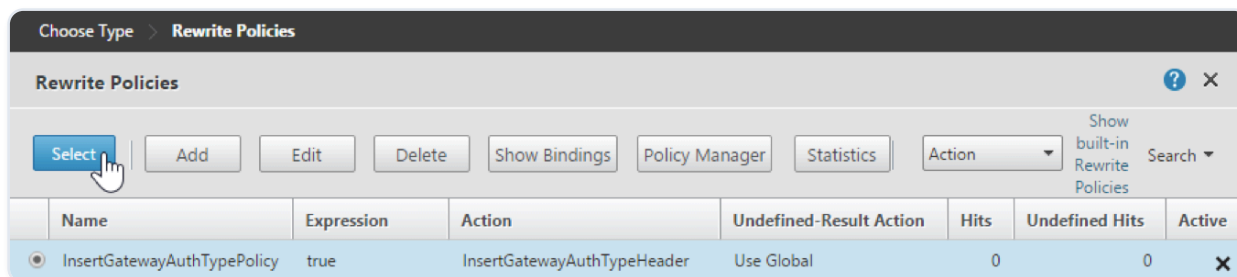
10. Click **Continue**.

The **Policy Binding** section expands.

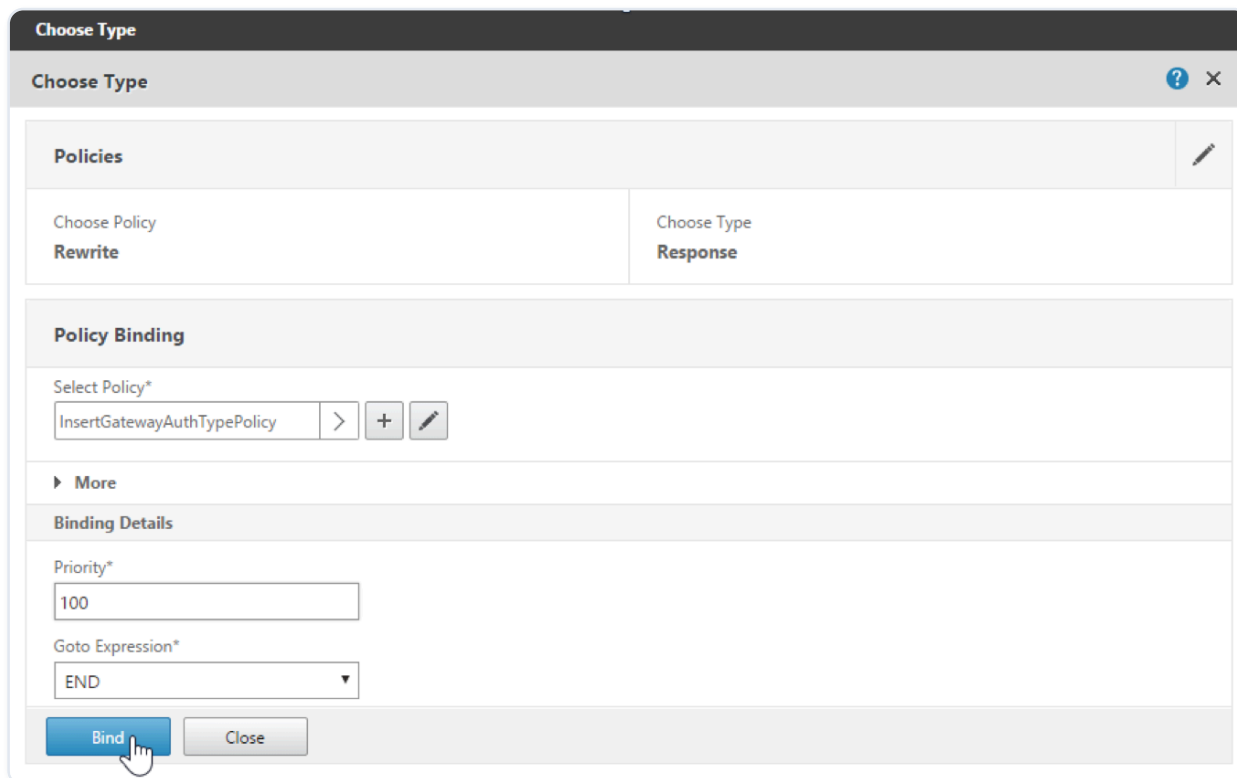


11. Click **Select Policy**.

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.

Enable DH Param DISABLED	Clear Text Port 0	SSLv2 Redirect DISABLED
Enable Ephemeral RSA ENABLED	Enable Cipher Redirect DISABLED	SSLv2 DISABLED
Refresh Count 0	Client Authentication ENABLED	SSLv3 ENABLED
Enable Session Reuse ENABLED	Client Certificate Mandatory	TLSv1 ENABLED
Time-out 120	Send Close-Notify YES	TLSv1.1 ENABLED
SSL Redirect DISABLED	PUSH Encryption Trigger Always	TLSv1.2 ENABLED
	SNI Enable DISABLED	

Published Applications	
No Next HOP Server	>
1 STA Server	>
No Uri	>

Other Settings	
ICMP Virtual Server Response Passive	Listen Priority
RHI State Passive	Listen Policy Expression None
Redirect to Home page true	ShareFile
	AppController https://xms3.dm.com:8443
	L2 Connection false

Policies	
Request Policies	>
3 Session Policies	>
2 ClientlessAccess Policies	>
4 Cache Policies	>
Response Policies	>
1 Rewrite Policy	>

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

VPN Virtual Server Rewrite Policy Binding					
VPN Virtual Server Rewrite Policy Binding					
Add Binding	Unbind	Edit			
Priority	Policy Name	Expression	Action	Goto Expression	
100	InsertGatewayAuthTypeHeaderPolicy	true	InsertGatewayAuthTypeHeader	END	
Close					

Port requirement for ADS connectivity for Android devices

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

IMPORTANT:

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

Prerequisites:

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

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

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

FQDN	IP ADDRESS	PORT	IP AND PORT USAGE
<code>discovery.mdm.ze nprise.com</code>	52.5.138.94	443	Secure Hub - ADS Communication
<code>discovery.mdm.ze nprise.com</code>	52.1.30.122	443	Secure Hub - ADS Communication
<code>ads.xm.cloud.com</code> : note that Secure Hub version 10.6.15 and later uses <code>ads.xm.cloud.com</code> .	34.194.83.188	443	Secure Hub - ADS Communication

FQDN	IP ADDRESS	PORT	IP AND PORT USAGE
<code>ads.xml.cloud.com</code> : note that Secure Hub version 10.6.15 and later uses <code>ads.xml.cloud.com</code> .	34.193.202.23	443	Secure Hub - ADS Communication

If certificate pinning is enabled:

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

NOTE:

If you enable certificate pinning after an upgrade, users must enroll again.

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

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

Disabling the Delete Account option

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

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

1. Configure ADS for your domain.
2. Open the **AutoDiscovery Service Information** in Citrix Endpoint Management and set the value for `displayReenrollLink` to **False**. By default this value is **True**.
3. If your device is enrolled in the MDM+MAM (ENT) mode, log off and log in again for the changes to take effect. If your device is enrolled in other modes, you must re-enroll the device.

Using Secure Hub

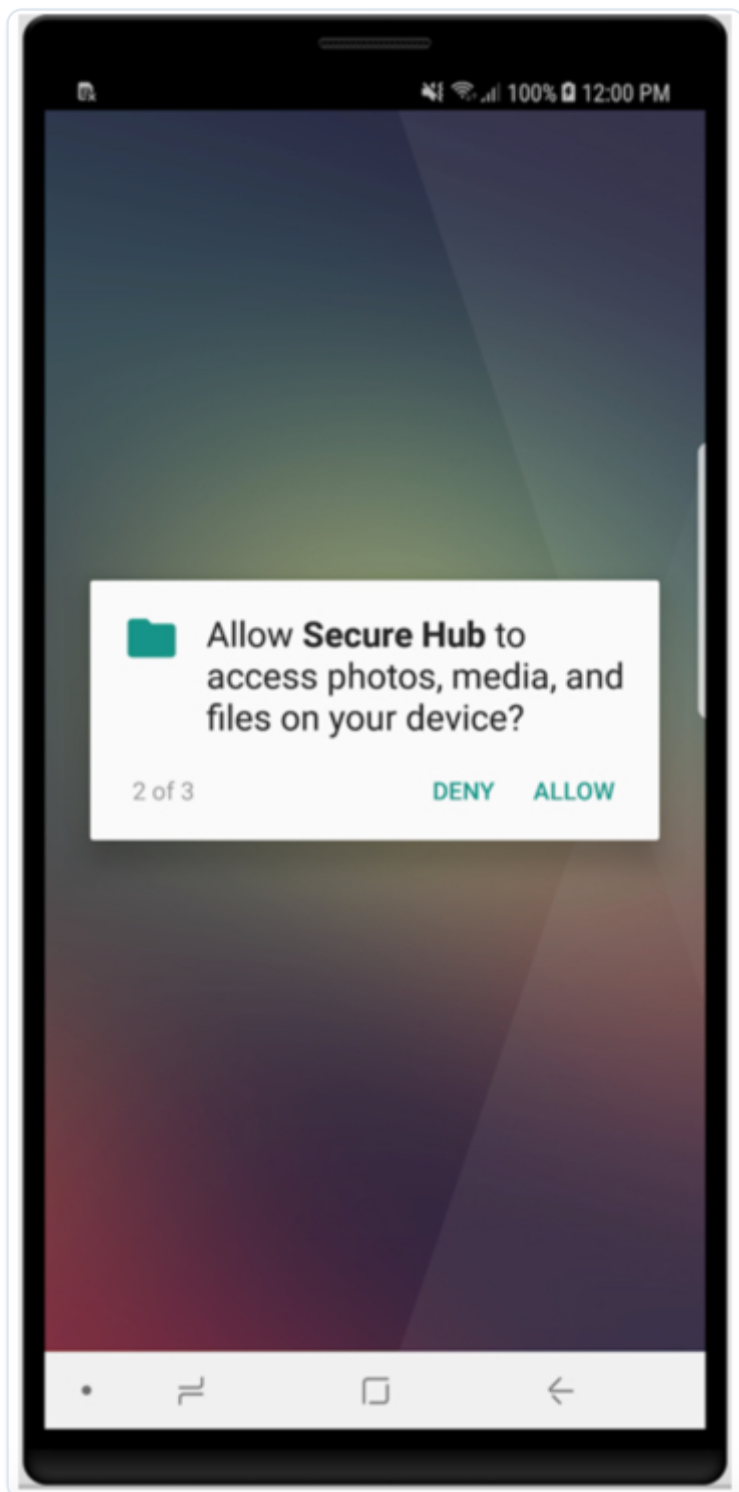
Users begin by downloading Secure Hub on to their devices from the Apple or Android store.

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

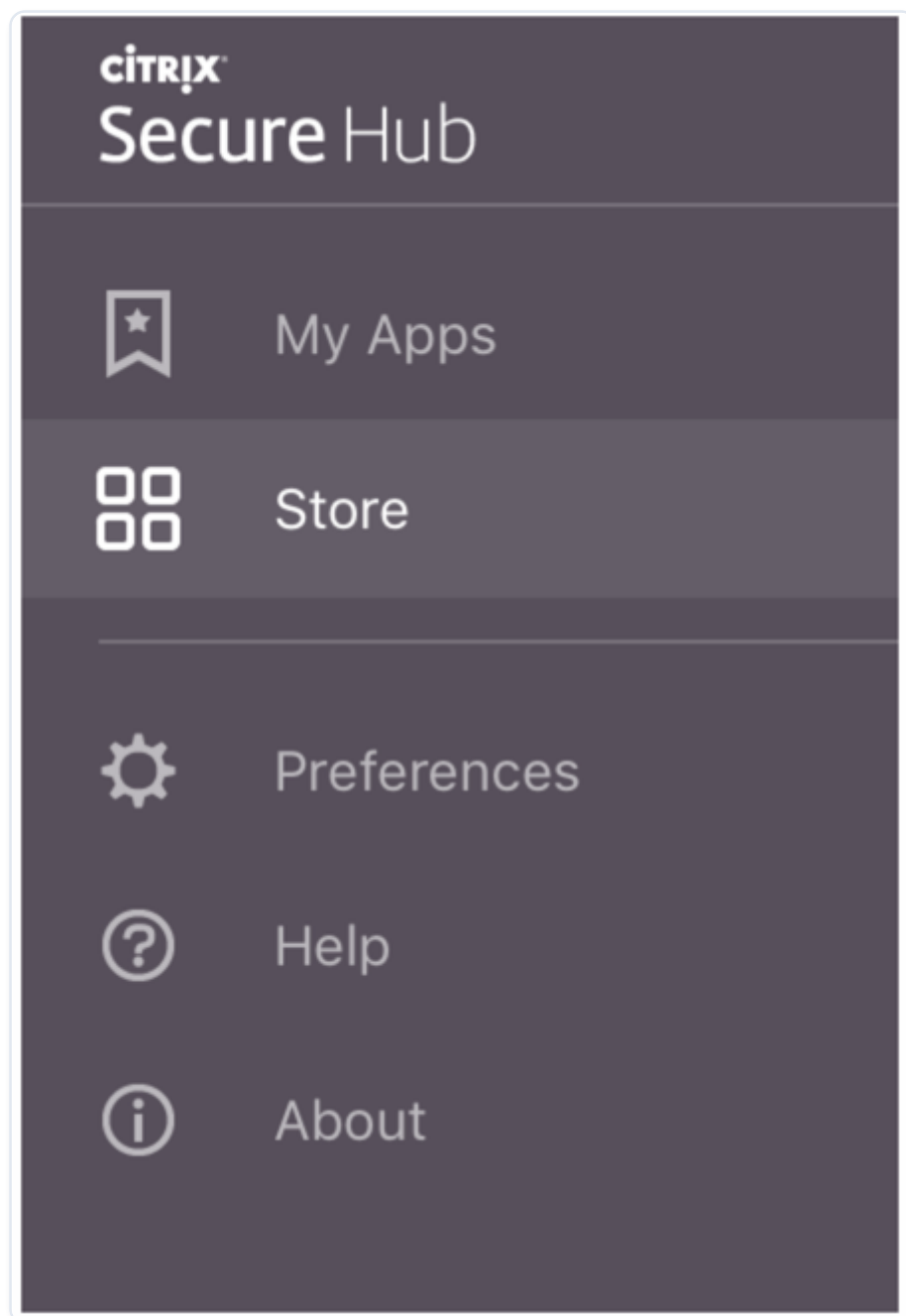
On Secure Hub for Android, during initial installation and enrollment, the following message appears: Allow Secure Hub to access photos, media, and files on your device?

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

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



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 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.

The screenshot shows the XenMobile console interface. The top navigation bar is green with the XenMobile logo and tabs for Analyze, Manage, and Configure. The user is logged in as 'administrator'. The breadcrumb trail is 'Settings > Client Branding'. The main heading is 'Client Branding' with a subtext: 'You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.' The form includes: 'Store name*' with a text box containing 'Store'; 'Default store view' with radio buttons for 'Category' and 'A-Z' (selected); 'Device' with radio buttons for 'Phone' (selected) and 'Tablet'; 'Branding file' with a text box and a 'Browse' button. A 'Note' section lists requirements for the branding file: it must be a .png, have specific dimensions, be named 'Header.png' or 'Header@2x.png', and be a zip file containing these files. At the bottom right are 'Cancel' and 'Save' buttons.

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.

The screenshot shows the XenMobile 'Configure' page. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Apps' tab is selected, and the 'App Information' section is active. On the left, a sidebar lists steps: '1 App Information' (selected), '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. The main area contains form fields for 'Name' (set to 'Workmail'), 'Description' (empty), and 'App category' (set to 'Workapps').

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**.

The screenshot shows the 'Help Desk' screen. At the top, there is a 'Close' button and the title 'Help Desk'. Below the title, there are three main options: 'Your IT Department', 'Report Issue', and 'Send Feedback to Citrix'. Each option has a right-pointing chevron icon. At the bottom of the screen, there is a 'Citrix Support' link.

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.

XenMobile Analyze Manage Configure

Settings > Client Support

Client Support

GoToAssist chat token

GoToAssist support ticket email

Support phone (IT help desk)

Support email (IT help desk)*

Send device logs to IT help desk ☐ directly ☒ by email

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

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

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

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

Location policies

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

Crash collection and analysis

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

For more features available for iOS and Android, see the Features by platform matrix for [Citrix Secure Hub](#).

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.
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

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

Secure Hub for iOS 26.8.1

Fixed issues

- When launching HDX apps from Secure Hub for iOS through the Citrix Workspace app, the apps might fail to launch.

Known issues

There are no known issues in this release.

Secure Hub for Android 26.8.0

Fixed issues

- In the Android Enterprise Restrictions policy, configuring a specific system app whitelist might override the **All#** setting and re-hide already-whitelisted system apps.
- On Android Enterprise kiosk (COSU) devices, the device lock PIN that Secure Hub applied when a device left a geofence perimeter might not be removed after the device returned to the permitted area. As a result, the device keeps prompting for the PIN, and an administrator has to retrieve it from the console and unlock the device manually.
- On devices running Android 16 and Android 17, including Samsung devices running One UI 8.5, the device might remain in lock task (kiosk) mode after fully managed device or dedicated device enrollment completes. As a result, users cannot leave the Secure Hub screen, enrollment appears to be incomplete, and the device has to be restarted.

Known issues

There are no known issues in this release.

Secure Hub for iOS 26.8.0

Fixed issues

- When calling Microsoft Authentication Library (MSAL) signout, Secure Hub might crash due to a race condition or deadlock.
- Secure Mail and Secure Web might fail on first-time use when the `mam-app-data-sharing` feature flag is enabled.
- On DEP devices, the MDM profile might not be deleted during a selective wipe triggered by secure apps.
- When users submit feedback from Secure Hub, the feedback might be sent to an outdated support email address.
- The PIN popup might persist even after the account is deleted.
- The **Send Log** button might not respond when tapped.
- Secure Hub might include the unnecessary `NSAppleMusicUsageDescription` permission.
- For tenants with more than 2100 licenses, installing a Volume Purchase Program (VPP) app might redirect users to the App Store instead of installing the app.
- Secure Hub might crash with a SIGABRT error while loading the shared keychain vault.

Known issues

There are no known issues in this release.

Secure Hub for Android 26.5.0

Fixed issues

Secure Hub auto-discovery might fail when ADS server URLs include an invalid port value.

Known issues

There are no known issues in this release.

Secure Hub for Android 26.2.0

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 25.10.0

Fixed issues

Secure Hub reports deployment failure to the CEM server when the required app is not installed to unblock policy deployment.

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.
- 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.

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).

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.

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.
- 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.
- 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.

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"

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.
- 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.

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.

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."

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.

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](#).

History of Secure Hub known and fixed issues

This article lists fixed and known issues for Secure Hub for versions earlier than the recent supported versions. For the most recent documentation, see [Citrix Secure Hub](#).

Secure Hub for Android 23.7.0

Fixed issues

- On the Android Enterprise platform, the Managed Configurations policy might not apply to the device after enrollment.
- On the Android Enterprise platform, the required Public App Store app might not install automatically on the device after enrollment.
- When you reboot your device and don't unlock it, you might not be able to reset the device passcode through the lock command that is issued by the IT administrator.

This method is helpful in case the end user loses their device passcode or loses the device, they can ask the administrator to reset the device passcode or lock the device through the lock command.

- When end users open Secure Hub on certain Android devices for enrollment, the Secure Hub app becomes unresponsive

The issue occurs when MDM enrollment fails due to an expired license. Consequently, the Secure Mail app is unavailable.

- When you configure Citrix Gateway as the identity provider (IdP) for authentication purposes, and the network connection to the gateway is unstable, authentication fails, and end users can't sign in to Secure Hub.

Known issues

There are no known issues in this release.

Secure Hub for iOS 23.4.0

Fixed issues

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

Known issues

There are no known issues in this release.

Secure Hub for Android 23.4.1

Fixed issues

- A loading spinner UI appears when you start the Secure Hub app. This issue occurs due to a deadlock condition.

Known issues

There are no known issues in this release.

Secure Hub for Android 23.4.0

Fixed issues

- After you upgrade a device from Android 11 to Android 12 and then to Android 13, the Secure Hub app fails to start.
- After you enroll in a corporate owned single use (COSU) device, the Secure Hub app requests an active directory (AD) password instead of Citrix PIN. The issue might occur due to loss of cached credentials in Secure Hub version 23.2.0 and earlier.
- Secure Hub app becomes unresponsive as the PIN is not accepted due to an exception in the code.

Known issues

There are no known issues in this release.

Secure Hub for Android 23.2.0

Fixed issues

- After you enroll in a corporate owned single use (COSU) device, and the restrictions policy allows the use of SD cards, you still might not be able to access the external SD card on these devices. The issue is that it is a dedicated device.
- The passcode policy settings for password expiration on Android Enterprise devices do not work as expected. The passcode change prompt doesn't appear. Instead, you have to change the passcode manually.
- Occasionally, after you upgrade a device from Android 11 to Android 13, the Secure Hub app becomes unresponsive.
- Each time you sign in to Secure Hub, the app requests active directory (AD) password instead of Citrix PIN. The issue occurs after you have changed the AD password.
- After you change the active directory (AD) password, attempts to sign in to Secure Hub fail with the following error message:

Incorrect credentials.

Secure Hub 22.11.0

- When a push message is sent from the CEM console to the **Enrollment App** channel, the message arrives on the device but does not trigger the sound alert.
- When you configure the **Credentials Policy** and define the certificate alias, the Citrix SSO app fails to connect to the VPN with an authentication error when using the custom certificate alias. The following error message appears:

Connection Error: Cannot connect to the *certificate ID*. Check your internet connection and verify the settings for *certificate ID*.

The issue occurs when you allow apps to use the certificates for the Citrix SSO app.

Secure Hub 22.9.0

There are no known or fixed issues in this release.

Secure hub 22.7.0

Fixed issues

- After you switch from Mobile Device Experience (MDX) to Citrix Mobile Application Management (MAM) SDK, and upgrade XenMobile Server to 10.13 RP4, you might not be able to access intranet sites through Secure Hub/ Secure Web.

The following error message appears: "Err_Name_not_resolved".

- The managed configuration policy settings are not applied on work profiles that have the enrollment configuration as Work Profile for Company Owned Devices (WPCOD). The issue occurs when the authentication is through the Identity Provider (IdP), and the Work Profile isn't marked as provisioned.

Secure Hub 22.6.0

There are no known or fixed issues in this release.

Secure Hub 22.5.0

There are no known or fixed issues in this release.

Secure Hub 22.4.0

There are no known or fixed issues in this release.

Secure Hub 22.2.0

Known issues in Secure Hub 22.2.0

There are no known issues in this release.

Fixed issues in Secure Hub 22.2.0

Secure Hub for iOS

- In Secure Hub for iOS, you are prompted to enroll using a PIN on devices enrolled through the Apple Deployment Program.
- When you sign in to Secure Mail after your device has been idle, Secure Hub for iOS opens with the following error message:

"Secure Hub needs to authorize this app."

Once you click authorize and provide your credentials, authentication goes into a loop. You can't reauthenticate or sign in even after a reboot.

- Secure Hub for iOS becomes unresponsive on devices running iOS 15.1 when you are reporting an error.
- In Secure Hub for iOS, the badge count appears as 1 or 2 despite there being no new notifications.
- In Secure Hub for iOS, enrollment might fail on some devices.
- If you configure the Citrix Gateway Session time-out policy value to 30 days, Secure Hub for iOS prompts users to reauthenticate every 24–72 hours.

Secure Hub for Android

- In the Samsung DeX mode, Secure Hub becomes unresponsive when you enter the PIN.
- When you enroll Samsung S20 devices, in the fully managed mode, to Android Enterprise, the following error appears: "Invalid server certificate"
- Enrollment of devices running Android 10 or 11 fails and the following error message appears: "Security policy does not allow you to connect".
- When you enroll to Secure Hub for Android, your credentials are replaced with random numbers if you switch from portrait to landscape mode.

Secure Hub 21.11.0

Known issues in Secure Hub 21.11.0

There are no known issues in this release.

Fixed issues in Secure Hub 21.11.0

Secure Hub for Android

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

Secure Hub 21.10.0

Known issues in Secure Hub 21.10.0

There are no known issues in this release.

Fixed issues in Secure Hub 21.10.0

Secure Hub for iOS

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

Secure Hub for Android

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

Secure Hub 21.8.0

Secure Hub for iOS

Known issues in Secure Hub 21.8.0

There are no known issues in this release.

Fixed issues in Secure Hub 21.8.0

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

Secure Hub 21.7.1

Secure Hub for Android

There are no known or fixed issues in this release.

Known and fixed issues in earlier versions

For known and fixed issues in earlier versions of Secure Hub, see [History of Secure Hub known and fixed issues](#).

Secure Hub 21.7.1

Secure Hub for Android

There are no known or fixed issues in this release.

Secure Hub 21.7.0

Secure Hub for iOS

There are no known or fixed issues in this release.

Secure Hub for Android

Known issues in Secure Hub 21.7.0

There are no known issues in this release.

Fixed issues in Secure Hub 21.7.0

- In Secure Hub for Android, Secure Mail and Secure Web logs are missing when you navigate to **Help > Report Issue** after you reboot your device.

Secure Hub 21.6.0

Secure Hub for iOS

Known issues in Secure Hub 21.6.0

There are no known issues in this release.

Fixed issues in Secure Hub 21.6.0

In Secure Hub for iOS, when you enroll a device using User Principal Name (UPN), the user name does not auto-populate. This issue occurs when Auto Discovery Service is enabled.

Secure Hub for Android

Known issues in Secure Hub 21.6.0

In Secure Hub for Android, you cannot enroll a device in the MDM+MAM mode if the FQDN provided contains capital letters. Instead, the device is enrolled in MAM mode.

Fixed issues in Secure Hub 21.6.0

In Secure Hub for Android, you are unable to enroll factory reset devices running Samsung Knox in the Device Administrator mode.

Secure Hub 21.5.1

Secure Hub for iOS

There are no known or fixed issues in this release.

Secure Hub for Android

There are no known or fixed issues in this release.

Secure Hub 21.5.0

Known issues in Secure Hub 21.5.0

There are no known issues in this release.

Fixed issue in Secure Hub 21.5.0

In Secure Hub for Android, you are unable to deploy the Wi-Fi device policy on Android Enterprise devices. The policy remains in the Pending state.

Secure Hub 21.4.0

There are no known or fixed issues in this release.

Secure Hub 21.3.2

Secure Hub for iOS

Known issues in Secure Hub 21.3.2

There are no known issues in this release.

Fixed issue in Secure Hub 21.3.2

You are unable to enroll a device on Citrix Endpoint Management™, after entering the Citrix PIN. Secure Hub does not display the correct message for the PIN requirement.

Secure Hub 21.3.0

Known issue in Secure Hub 21.3.0

In Secure Hub for Android version 20.9.0 and later, you can't connect in VPN mode on Google Pixel 2 devices.

Fixed issues in Secure Hub 21.3.0

- In Secure Hub for Android, the Integrated Circuit Card ID (ICCID) is displayed for devices that have no SIM card inserted.
- In Secure Hub for Android, the installed mobile productivity apps are not displayed on the **My Apps** screen upon restarting the device.
- In Secure Hub for Android, you are unable to unlock Android Enterprise devices if you've entered the wrong password multiple times and try restarting the device. The following error message appears: **Phone turned off, Contact your IT administrator.**

Secure Hub 21.2.0

Secure Hub for Android

Known issues in Secure Hub 21.2.0

In Secure Hub for Android, the installed mobile productivity apps do not appear on the **My Apps** screen upon restarting the device.

Fixed issues in Secure Hub 21.2.0

- Secure Hub for Android hangs during enrollment of devices.
- On certain versions of Secure Hub for Android, the **Home** and **Back** buttons are not visible once enrollment is complete on Samsung Knox devices.

Secure Hub 21.1.0

Known issues in Secure Hub 21.1.0

There are no known issues in this release.

Fixed issues in Secure Hub 21.1.0

- On devices running Android, Secure Hub fails to connect to Citrix Endpoint Management when the Connection scheduling device policy is enabled.
- On certain registered Samsung devices, the wrong serial number is reported on the Citrix Endpoint Management console.

Secure Hub 20.12.0

Known issues in Secure Hub 20.12.0

There are no known issues in this release.

Fixed issues in Secure Hub 20.12.0

- In Secure Hub for iOS, you are unable to enroll your devices. You get the following error: **Your device isn't enrolled.**
- In Secure Hub for iOS, the user agent string doesn't include the OS version for devices enrolled in the MAM+MDM.
- On Android Enterprise devices, Secure Hub crashes during enrollment.
- Secure Hub for Android version 20.11.0 crashes on certain Samsung devices.

Secure Hub 20.11.0

Secure Hub for Android

Known issues in Secure Hub 20.11.0

There are no known issues in this release.

Fixed issues in Secure Hub 20.11.0

On some Samsung devices, Secure Hub for Android crashes, and you get the following error:
Secure Hub keeps stopping.

Secure Hub 20.10.5

Known issues in Secure Hub 20.10.5

There are no known issues in this release.

Fixed issues in Secure Hub 20.10.5

- On corporate-owned single-use (COSU) devices running Android 11, you can't set Secure Hub as the default launcher.
- On devices running Android, the creation of a work profile fails on certain Samsung devices. You get the following error: **Unable to configure work profile.**
- The mobile app management (MAM) enrollment of Android devices fails through the Citrix Endpoint Management AutoDiscovery Service.
- On devices running iOS, you can't launch certain apps. You get the error **Please update Secure hub to use this app** even when there's no update available for Secure Hub.
- On devices running iOS, Secure Mail prompts for authorization after the maximum offline period expires. Secure Mail then switches to Secure Hub, preventing you from using it.

Secure Hub 20.9.0

Known issues in Secure Hub 20.9.0

There are no known issues in this release.

Fixed issues in Secure Hub 20.9.0

- In Secure Hub for iOS, when certificate pinning is enabled, connections are established across servers even if the certificate pinned from one of the servers is incorrect.
- In Secure Hub for iOS, you can't receive notifications. You get the following error: **There are no devices with a valid Secure Hub token.**

Secure Hub 20.7.5

Known issues in Secure Hub 20.7.5

On corporate-owned single-use (COSU) devices running Android 11, you can't set Secure Hub as the default launcher.

Fixed issues in Secure Hub 20.7.5

- In Secure Hub for Android, enrolling Android devices fails when certificate pinning is enabled.
- In Secure Hub for Android, the **Date Time Change** feature in the Restrictions policy does not work on Samsung devices.
- In Secure Hub for Android, the firewall policy doesn't work on Samsung devices running versions 19.12.5 and later.
- In Secure Hub for Android, you are unable to uninstall apps from **My apps**.

Secure Hub 20.6.5

There are no known or fixed issues in this release

Secure Hub 20.3.0

Secure Hub for iOS

There are no known or fixed issues in this release.

Secure Hub 20.2.0

Secure Hub for iOS

Known issues in Secure Hub 20.2.0

There are no known issues in this release.

Fixed issues in Secure Hub 20.2.0

- In Secure Hub for iOS, Mobile Application Management (MAM) enrollment fails on a few iOS devices.
- In Secure Hub for iOS, apps are being removed randomly from devices.

Secure Hub 20.1.5

There are no known or fixed issues in this release.

Secure Hub 19.12.5

Known issues in Secure Hub 19.12.5

There are no known issues in this release.

Fixed issues in Secure Hub 19.12.5

On devices running iOS 13, the user certificates for XenMobile® Server are checked and renewed on the actual expiration date rather than relying on the SSL error code to check user certificate expiration.

Secure Hub 19.11.5

Known issues in Secure Hub 19.11.5

There are no known issues in this release.

Fixed issues in Secure Hub 19.11.5

In Secure Hub for iOS, enrollment fails for MDX wrapped apps after disabling user entropy.

Secure Hub 19.10.5

Secure Hub for Android

Known issues in Secure Hub 19.10.5

There are no known issues in this release.

Fixed issues in Secure Hub 19.10.5

In Secure Hub for Android, you are unable to install business apps on devices running Secure Hub version 19.10.5 when the Credentials policy is configured.

Secure Hub 19.10.0

Known issues in Secure Hub 19.10.0

- In Secure Hub for Android, enrollment of Google Pixel 2 devices running on Android version 10 in Device Owner mode fails due to permission failure.
- In Secure Hub for Android, on Google Pixel devices running Android version 10, enrollment of devices in Device Owner mode fails due to failure in validating the location permission.

Fixed issues in Secure Hub 19.10.0

There are no fixed issues in this release.

Secure Hub 19.9.5

There are no known or fixed issues in this release.

Secure Hub 19.9.0

Known issues in Secure Hub 19.9.0

In Secure Hub for Android 19.9.0 with Android Enterprise enabled, the following issue occurs on Pixel 2 devices: The Credentials policy does not deploy successfully. As a result, users are not prompted for a certificate along with a password and a certificate is not installed. As a workaround, users can manually refresh their policies in the app from **Preferences > Device Information**. From there, they press **Refresh policy**, enter their credentials, and confirm the success message.

Fixed issues in Secure Hub 19.9.0

There are no fixed issues in this release.

Secure Hub 19.8.5

There are no known issues or fixed issues in this release.

Secure Hub 19.8.0

Known issues in Secure Hub 19.8.0

In Secure Hub for iOS, when you enter an incorrect password on a shared device, and tap **Switch user** to log in again, the **Please wait** message appears indefinitely.

Fixed issues in Secure Hub 19.8.0

The Mobile Device Management network is incorrectly routed when connected through the full VPN.

Secure Hub 19.7.5

Known issues in Secure Hub 19.7.5

There are no known issues in this release.

Fixed issues in Secure Hub 19.7.5

- In Secure Hub for Android, prompts to install web clips appear rapidly, interfering with the configuration of the Secure Hub PIN.
- On Samsung Knox devices version 3 and higher, when you enroll Secure Hub in Profile Owner mode and push **Samsung MDM license key** policy for the Android Enterprise platform, the **Device Container Password Reset** command fails.
- The following error appears in Secure Hub for iOS when you attempt to configure a Public App in the MAM mode by using the new app URL from the Apple Store: **Couldn't Load Store. Please try again.** Refer to the workaround in <https://support.citrix.com/article/CTX256704>.
- In Secure Hub for Android, you are unable to install MDX apps when a full VPN tunnel is established.
- When a session time-out occurs on Point Mobile PM80 devices running Secure Hub for Android in the Shared Devices mode, you are unable to log in again.

- In Secure Hub for Android, you get the following error after installing and launching internally wrapped applications: **The way that your data is encrypted in this app has changed. Please delete this app and reinstall it.**

Secure Hub 19.6.5

Known issues in Secure Hub 19.6.5

There are no known issues in this release

Fixed issues in Secure Hub 19.6.5

- On devices running iOS, Secure Hub does not load the store when there is a Global Server Load Balancing failover.
- In Secure Hub for Android, the Refresh policy fails. As a result, you are unable to deploy any new device policies.
- In Secure Hub for Android, enrollment or Refresh policy actions on Samsung S10 devices take a long time.
- On devices running Android, non-managed apps lose connectivity when Secure Hub establishes a full VPN connection.

Secure Hub 19.5.5

Known issues in Secure Hub 19.5.5

- In Secure Hub for Android, devices in Corporate Owned Single Use (COSU) mode lose connectivity after few minutes of enrollment, and do not receive notifications even with GCM enabled.
- When you deploy the Location policy on devices, at a time, for both Profile Owner and Device Owner modes, the user account in Device Owner mode is deleted. This issue occurs during NFC bump enrollment and when Endpoint Management is configured in the MDM mode.

Fixed issues in Secure Hub 19.5.5

- From this release, Secure Hub only supports devices running Android 5.0 and later.
- In Secure Hub for Android, enroll a device in device owner mode and set a new password. The device is not locked in the first attempt.

Secure Hub 19.5.0

Known issues in Secure Hub 19.5.0

- After enrollment, devices OnePlus Android version 7.1.1 and OnePlus 5T Android version 9.0.3 require manual restart of Secure Hub to be prompted for Citrix PIN.
- In Secure Hub for Android, required apps are not deployed on Android devices unless you refresh the policy or refresh the store.

Fixed issues in Secure Hub 19.5.0

- From this release, Secure Hub only supports devices running Android 5.0 and later.
- In Secure Hub for Android, Android 6.0 devices fail to enroll if multiple subject alternative names are present in the server certificate.
- In Secure Hub for Android, managed apps are not uninstalled after disenrollment of devices.
- On Samsung S9 devices, after users update to Android P, the following issue occurs: When you change the device password via Endpoint Management, the password on the device is not changed. Instead the screen turns black and the Endpoint Management console shows a locked device status.

Secure Hub 19.4.5

Known issues in Secure Hub 19.4.5

There are no known issues in this release.

Fixed issues in Secure Hub 19.4.5

On iOS devices, when you click the device enrollment link, the Endpoint Management FQDN instance name is not auto-populated in Secure Hub. The device enrollment request fails.

Secure Hub 19.3.5

Known issues in Secure Hub 19.3.5

When notifications are sent from Secure Hub for iOS, the notification badge count is not updated for Secure Hub.

Fixed issues in Secure Hub 19.3.5

- In Secure Hub for Android, when you enroll shared devices, deploy the **Webclip** policy and add web and SaaS apps, the deployment is successful. However, this deployment appears as failed in the **App inventory** screen in the Citrix Endpoint Management console.
- In Secure Hub for Android, when users log in with secure PIN, a VPN tunnel is established, but Secure Web does not load any website. However, the website loads as expected when Secure Web is closed and reopened.
- Secure Mail for Android configured with Microsoft Intune policies returns a blank screen after authentication.
- In Secure Hub for Android, apps that have disabled encryption are attempting to obtain encryption keys from Secure Hub.
- Secure Mail for Android crashes at launch when Intune Company Portal version 5.0.4324.0 is installed.
- In Secure Hub for Android, you are unable to use the system apps on corporate owned single use (COSU) Android Enterprise devices running on Android 7.1.1.
- In Secure Hub for Android, when you configure multiple apps from Google Play as Required apps and try to enroll, you are prompted to install the first app. The initial prompt is immediately followed by another prompt to install the second app and so on.

Secure Hub 19.3.0

Known issues in Secure Hub 19.3.0

- In Secure Hub for Android, when you enroll shared devices, deploy the Webclip policy and add web and SaaS apps, the deployment is successful. However, this deployment appears as failed in the **App inventory** screen in the Citrix Endpoint Management console.
- On Android Enterprise devices, when a lock action is set for geofence breach in the Location policy, the device prompts you to set a new passcode instead of using the system generated passcode.

Fixed issues in Secure Hub 19.3.0

Locking fully managed Android Enterprise devices remotely using the Lock with passcode security action might fail without notifying you of the failure. To ensure a device is locked, set Lock with passcode twice. The device is locked with the second passcode you set.

Secure Hub 19.2.0

Known issues in Secure Hub 19.2.0

There are no known issues in this release.

Fixed issues in Secure Hub 19.2.0

- In Secure Hub for iOS, the following SSL handshake failure message appears repeatedly when users log off from Secure Hub store: Network request to fetch apps is timed out from Server.
- The Files device policy for Android Enterprise does not deploy to Android devices in work profile mode.
- In Secure Hub for Android, the login authorization for a new user takes a long time on shared devices. When you log off as an enrolled user and try to login as a new user, Secure Hub keeps loading until you reboot the device.
- In Secure Hub for Android, cloud customers are unable to enroll Android Enterprise devices with an external identity provider.
- In Secure Hub for Android, when you are in Corporate Owned Single Use (COSU) mode, the app icons are overlapped in Secure Hub.
- In Secure Hub for Android, when certificate pinning is enabled for your existing setup, the authentication fails and returns to the first-time user screen when the certificate has multiple Subject Alternative Names.

Secure Hub 19.1.5

Known issues in Secure Hub 19.1.5

- In Secure Hub for Android, when you update password due to password policy change, the badged apps do not appear on Samsung Galaxy S8 devices.
- In Secure Hub for Android, the Files device policy Android Enterprise does not deploy to devices in work profile mode.

Fixed issues in Secure Hub 19.1.5

- In Secure Hub for Android, when users log in with Secure PIN a VPN tunnel is established, but Secure Web does not load any website. However, the website loads as expected when Secure Web is closed and reopened.

- In Secure Hub for Android, when you log on with Secure PIN a VPN tunnel is established, but Secure Web does not load any website. However, the website loads as expected when Secure Web is closed and reopened.
- In Secure Hub for Android, when you try to capture logs of the in-house app called TechXpert, Secure Hub restarts and asks you to reauthenticate.

Secure Hub 19.1.0

Known issues in Secure Hub 19.1.0

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 have the format of old UI branding.

Fixed issues in Secure Hub 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.
- You are unable to enroll OnePlus 5T devices for Android Enterprise using the QR code enrollment method.

Secure Hub 18.11.0

Fixed issues in Secure Hub 18.11.0

- 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.**
- You cannot edit Android volume levels on corporate-owned, single-use (COSU) devices.

Secure Hub 18.10.5

Fixed issues in Secure Hub 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.

Secure Hub versions 10.8.25 to 18.10.6

Fixed issues in Secure Hub 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.

Secure Hub 18.10.0

Fixed issues in Secure Hub 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.

Secure Hub 10.8.60

Fixed issues in Secure Hub 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.
- Secure Hub for Android becomes unresponsive during enrollment of devices when the VPN policy is configured and the Citrix SSO application is not installed on the device. It becomes responsive if you tap the **Back** button or restart the app.
- Secure Hub for Android crashes during enrollment in the Device Owner mode in an Android Enterprise environment.
- After users enter a valid PIN for Secure Hub for iOS, Secure Hub prompts users for the PIN repeatedly.
- Secure Hub for Android crashes during enrollment in the Profile Owner mode in an Android Enterprise environment.
- Using Android Enterprise in Secure Hub for Android installs Google Chrome by default.
- Upgrading Secure Hub for iOS to version 10.8.55, doesn't allow existing or new iOS device enrollments.

Secure Hub 10.8.55

Fixed issues in Secure Hub 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.

MDX-related fixed issues in version 10.8.55

- Enterprise apps might experience connectivity issues to internal resources when Preferred VPN mode is set to SecureBrowse.
- Apps that specify `android.support.multidex.MultiDexApplication` or `android.app.Application` as their application class cannot connect to internal networks in the Tunneled – Web SSO mode.
- On Android devices, multiple certificates are being generated and certificates are being revoked before their expiration date.

Secure Hub 10.8.55

Known issue in Secure Hub 10.8.55

- After removing your Secure Hub account from your device, MDM re-enrollment fails.

Secure Hub 10.8.50

Known issue in Secure Hub 10.8.50

- On Secure Hub for Android, users cannot add a web link shortcut.

Secure Hub 10.8.35

Fixed issues in Secure Hub 10.8.35

- On Android O, shortcuts created by policies do not appear on the device home screen. This behavior is by design in Android O.
- On Android, Secure Hub does not open on Samsung tablets after a period of inactivity.
- In Secure Hub for Android, you are unable to deploy the push policy on Samsung Knox devices.
- 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.

Secure Hub 10.8.25

Fixed issues in Secure Hub 10.8.25

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

Secure Hub 10.8.20

Fixed issues in Secure Hub 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.

Secure Hub 10.8.15

Fixed issues in Secure Hub 10.8.15

- Secure Hub for Android crashes while fetching location details on devices running Android O.

Secure Hub 10.8.10

Fixed issues in Secure Hub 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.
- 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.

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.

Secure Hub for Android and iOS - Preview

Look forward to the new features and resolved issues in the upcoming release.

For more information on the current release, see [What's new in Secure Hub](#).

Feature flag management

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

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:

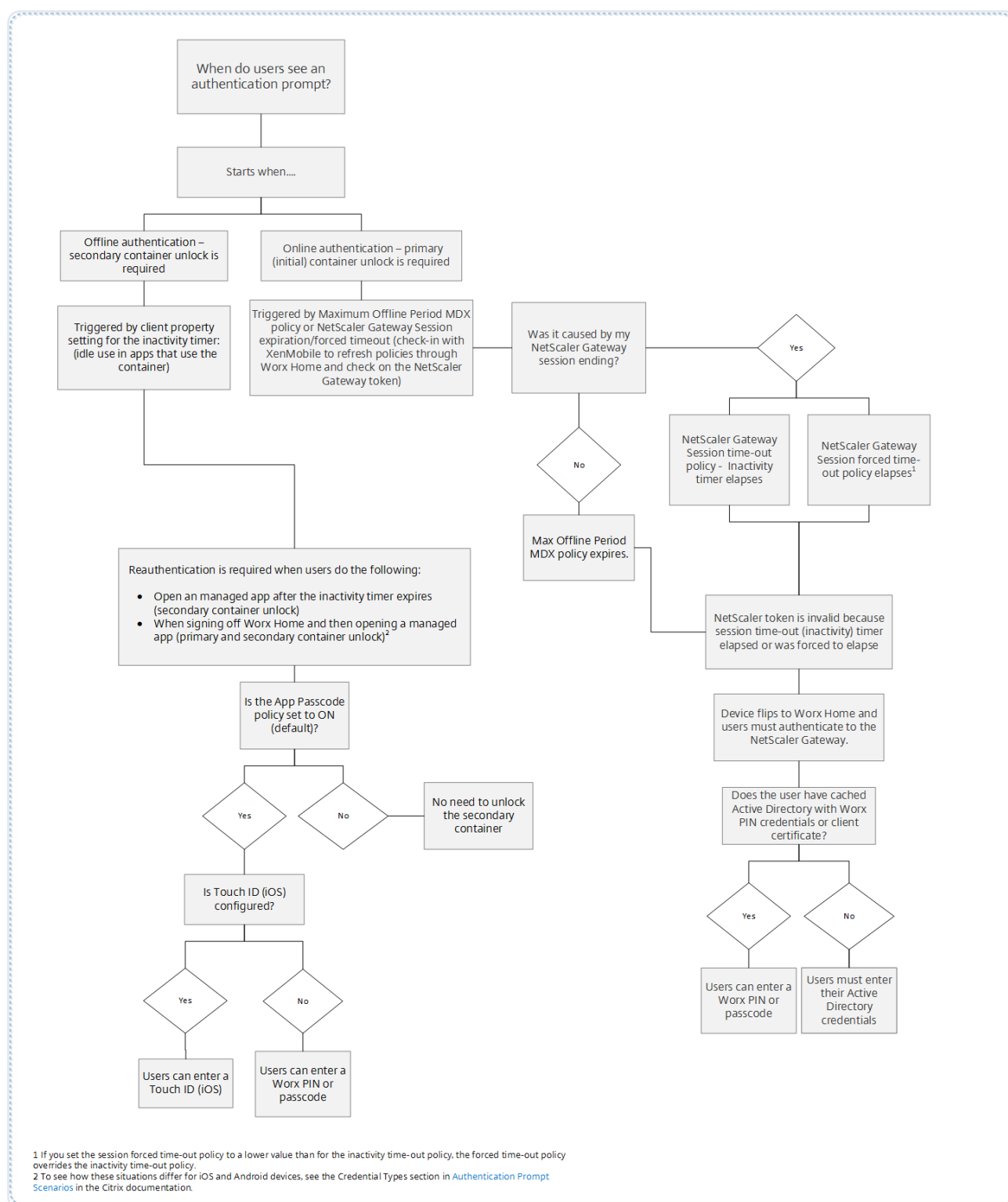
- **Primary container unlock:** An Active Directory password, Citrix PIN or passcode, one-time password, Touch ID or fingerprint ID are required to unlock the primary container.
 - On iOS, when users open Secure Hub or a managed app for the first time after the app is installed on the device.
 - On iOS, 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.



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

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).

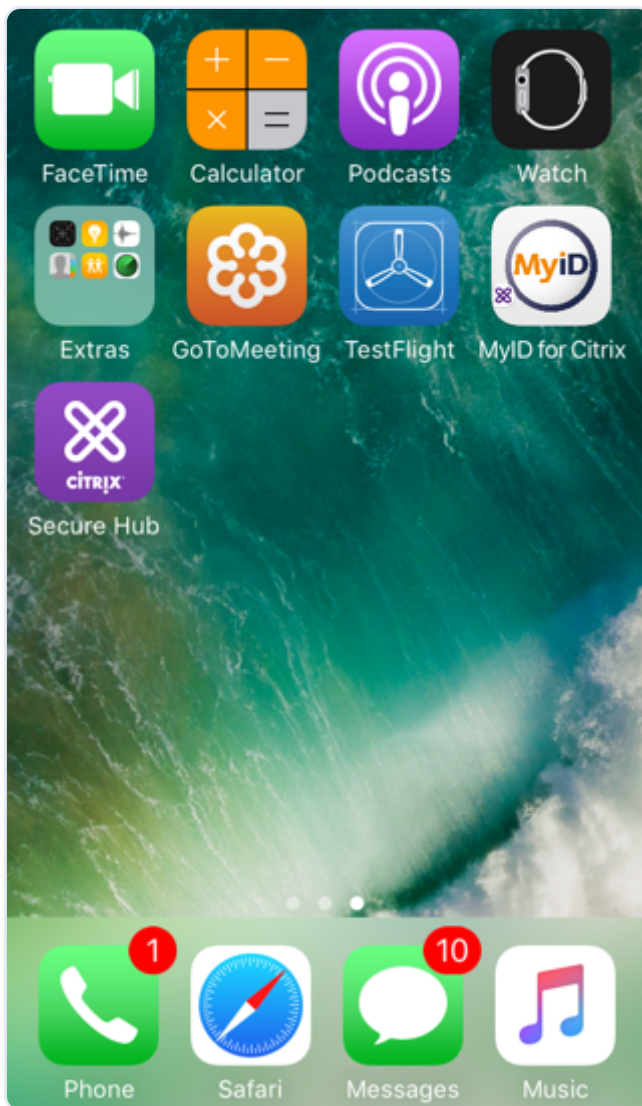
The derived credentials are an enrollment certificate that contains the user identifier, such as UPN. Endpoint Management stores the credentials obtained from the credential provider in a secure vault on the device.

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.

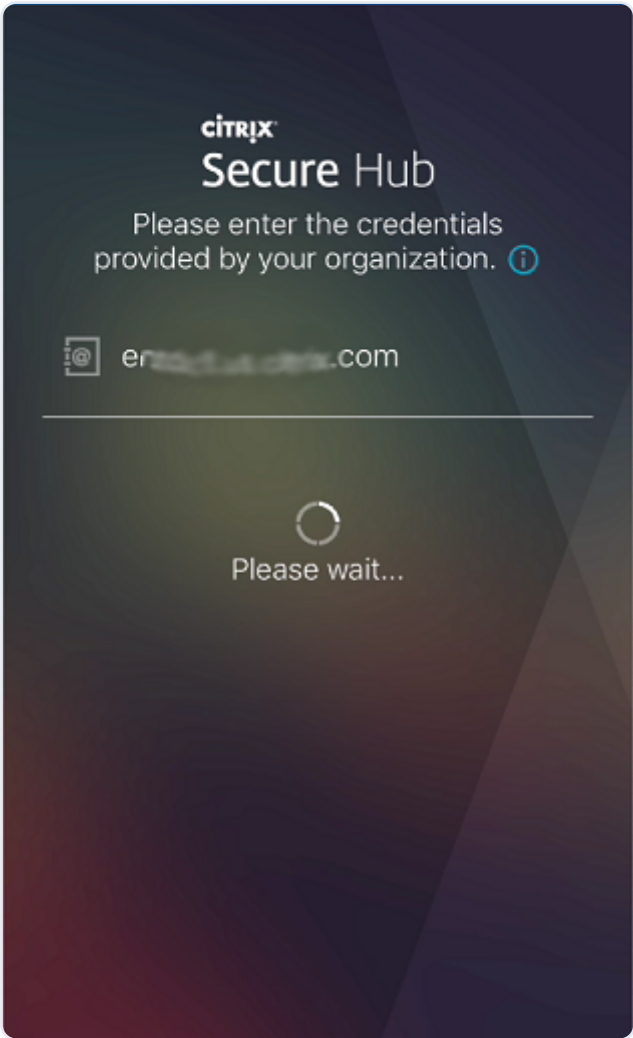
Device enrollment steps when using derived credentials

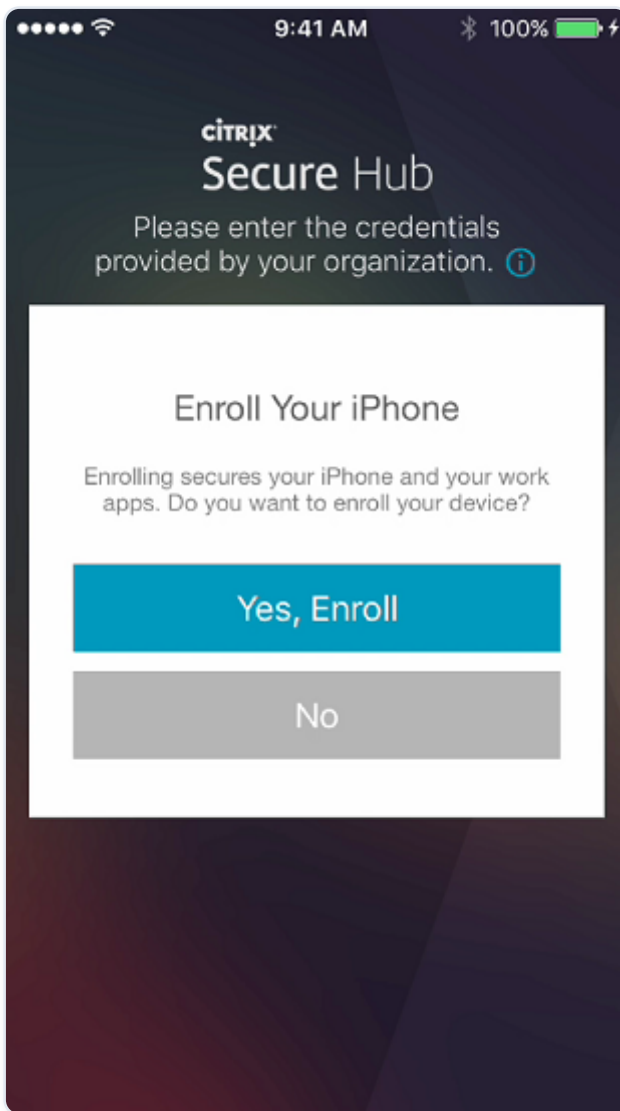
Enrollment requires that users insert their smart card to a reader attached to their desktop.

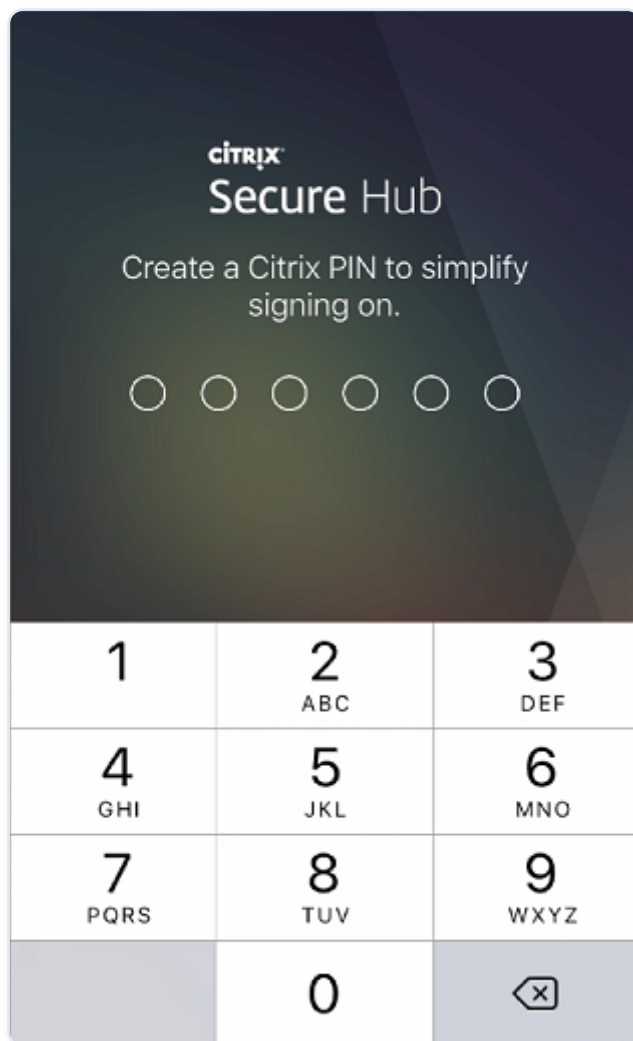
1. The user installs Secure Hub and the app from your derived credential provider. In this example, the identity provider app is the Intercede MyID Identity Agent.



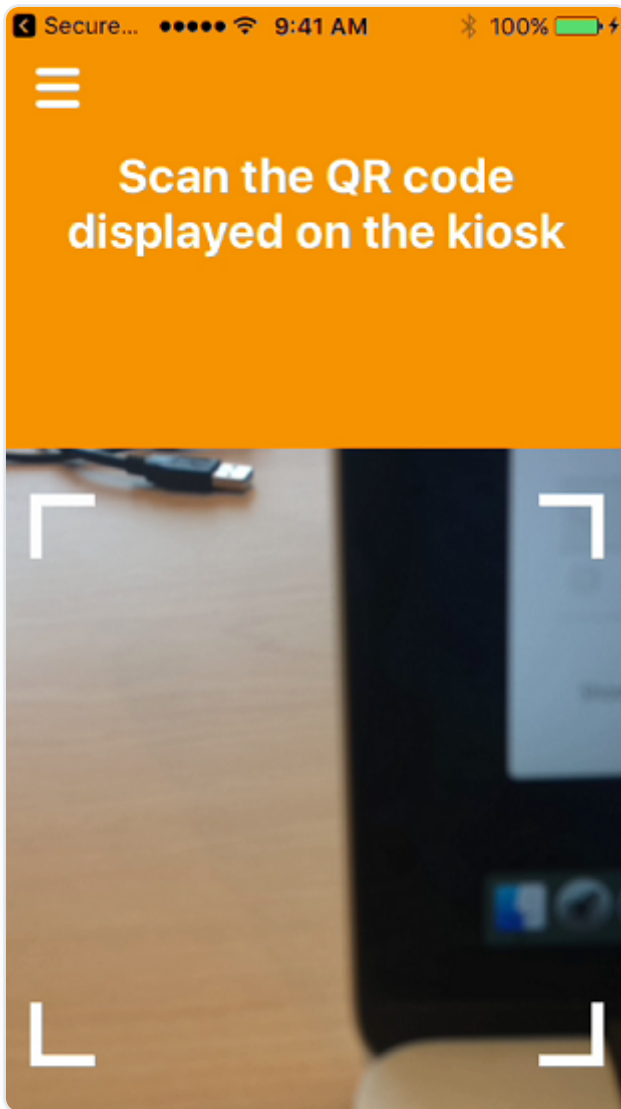
2. The user starts Secure Hub. When prompted, the user types the Endpoint Management fully qualified domain name (FQDN) and then clicks **Next**. Enrollment in Secure Hub starts. If Endpoint Management supports derived credentials, Secure Hub prompts the user to create a Citrix PIN.



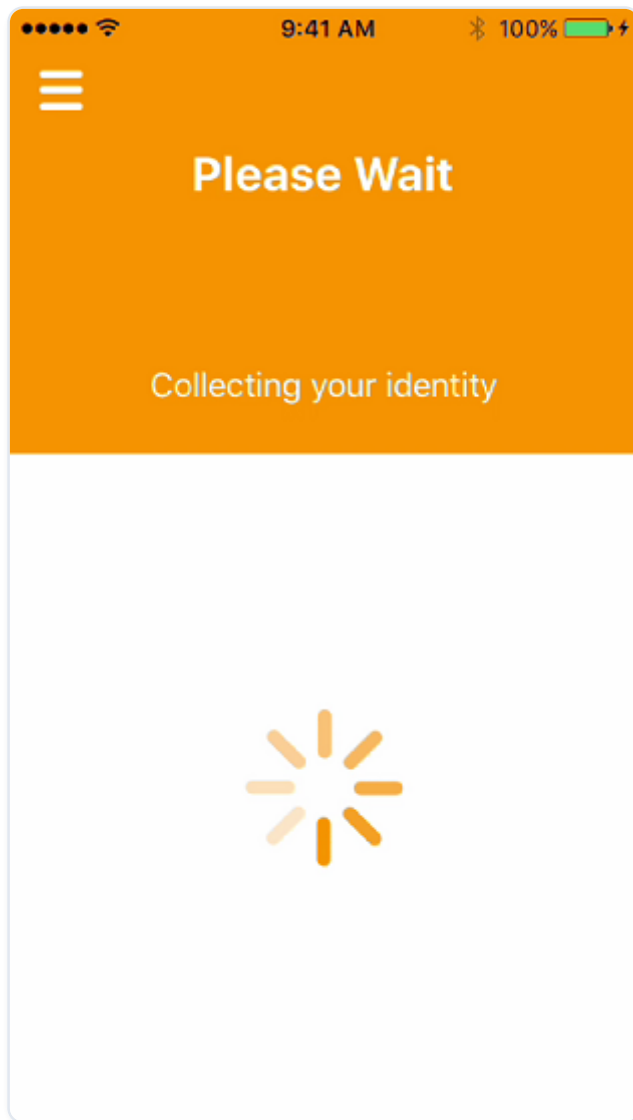




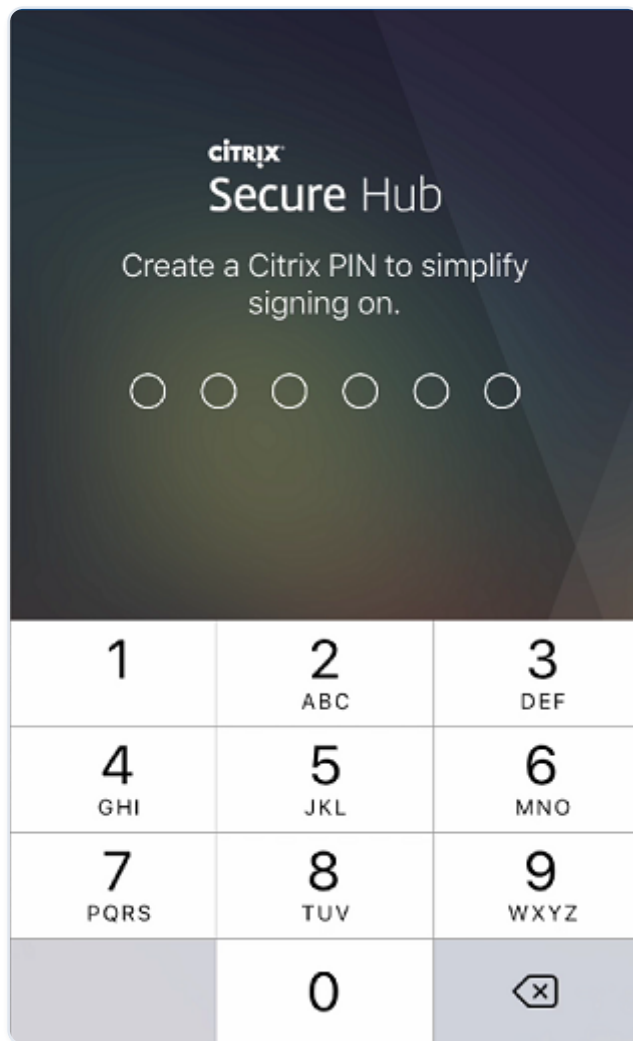
3. The user follows the instructions to activate their smart credential. A splash screen appears, followed by a prompt to scan a QR code.



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

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.

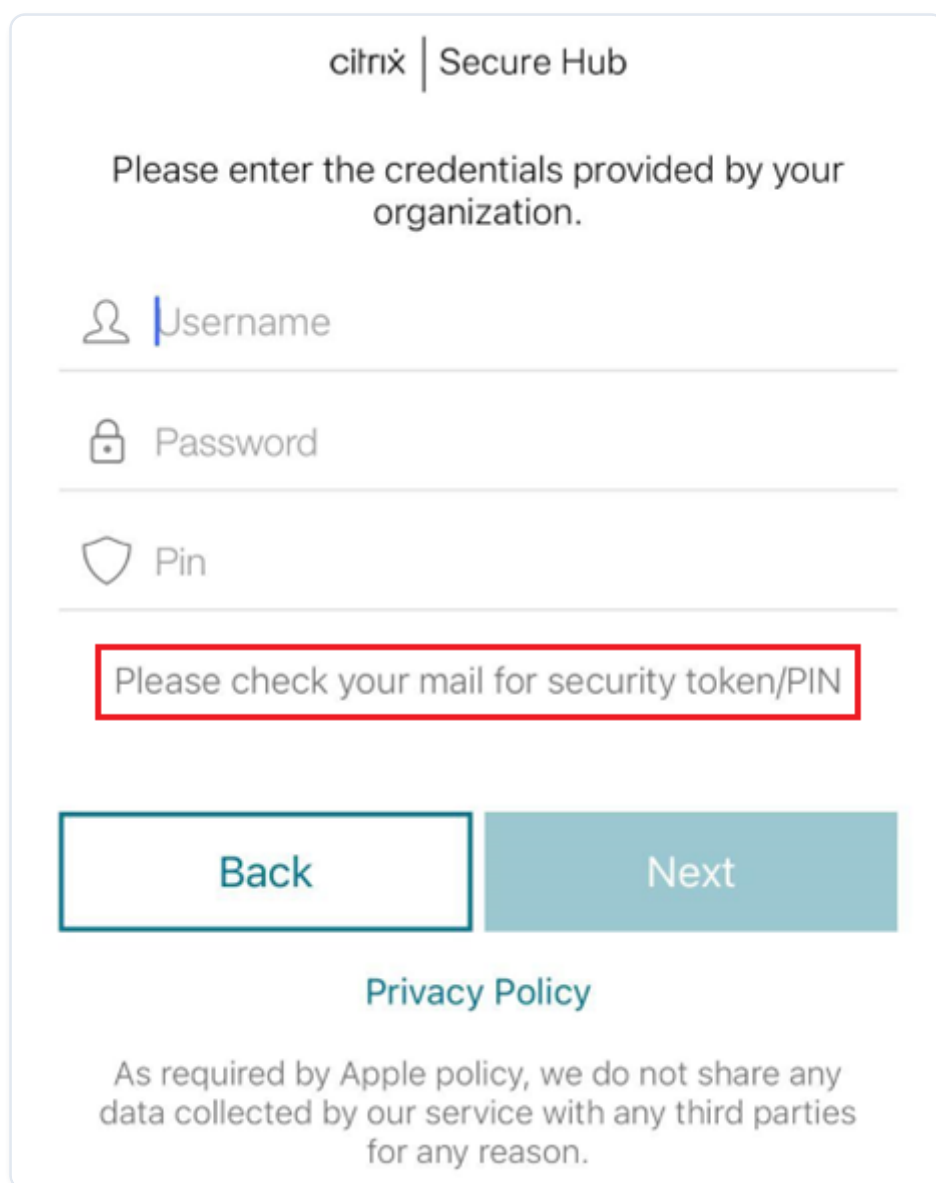
Settings > Client Properties > Add New Client Property

Add New Client Property

Key	Custom Key
Key *	enrollment.twofactor.token.hint
Value *	Please check your mail for security token/PIN
Name *	enrollment.twofactor.token.hint
Description *	Please check your mail for security token/PIN. This is where to get your security token/PIN.

8. Click **Save**.

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



The image shows the Citrix Secure Hub login interface. At the top, the Citrix logo and 'Secure Hub' text are displayed. Below this, a message asks the user to enter credentials provided by their organization. There are three input fields: 'Username' (with a person icon), 'Password' (with a lock icon), and 'Pin' (with a shield icon). A red rectangular box highlights the text 'Please check your mail for security token/PIN'. At the bottom, there are two buttons: 'Back' (white with a blue border) and 'Next' (solid blue). Below the buttons is a link for 'Privacy Policy' and a disclaimer stating that data is not shared with third parties as required by Apple policy.

citrix | Secure Hub

Please enter the credentials provided by your organization.

Username

Password

Pin

Please check your mail for security token/PIN

Back Next

[Privacy Policy](#)

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

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.

Settings > Client Properties > Add New Client Property

Add New Client Property

Key	Custom Key	?
Key *	enrollment.twofactor.token.hint.url	
Value *	https://www.citrix.com/contact/	
Name *	enrollment.twofactor.token.hint.url	
Description *	https://www.citrix.com/contact/	

8. Click **Save**.

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

citrix | Secure Hub

Please enter the credentials provided by your organization.

 Username Password Pin[Where to get your enrollment token?](#)[Back](#)[Next](#)[Privacy Policy](#)

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

Compliance check on Android devices (Technical Preview)

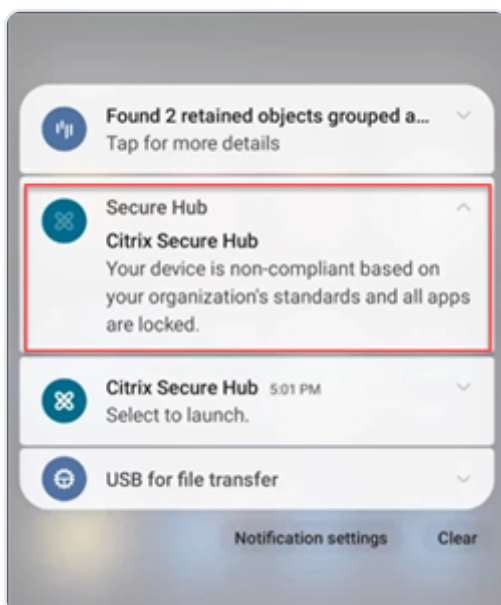
NOTE:

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

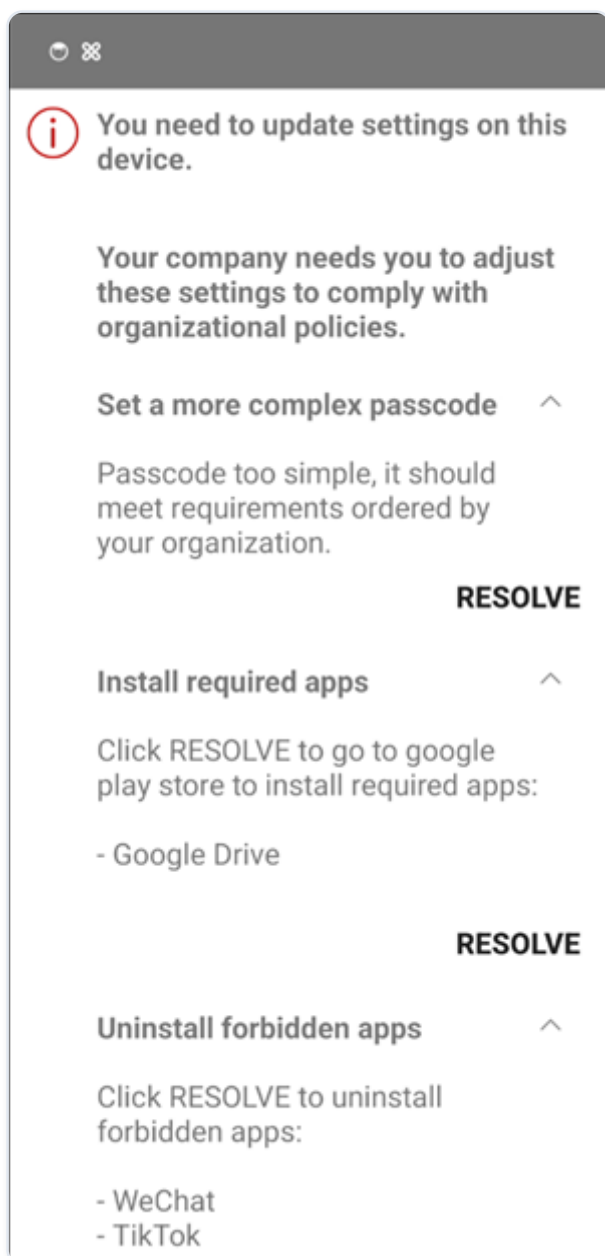
Starting from the release of Secure Hub for Android 24.8.0, Secure Hub verifies the compliance of Android devices against the policies configured by administrator through Citrix Endpoint Management. These compliance check includes:

- 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.