Citrix Endpoint Management™

cloud SOFTWARE GROUP

Copyright © 1997–2025. Citrix Systems, Inc. All Rights Reserved.

Contents

Citrix Endpoint Management 9

What's new 14

Third-party notices 27

Deprecation 27

System requirements 42

Citrix Endpoint Management compatibility 54

Supported device operating systems 56

Language support 57

FIPS 140-2 compliance 59

About Citrix Endpoint Management 60

Citrix Endpoint Management integration with Microsoft Endpoint Manager 75

Onboarding and resource setup 112

Scale and size considerations for Cloud Connectors 123

Prepare to enroll devices and deliver resources 124

Certificates and authentication 140

Upload, update, and renew certificates 144

NetScaler Gateway and Citrix Endpoint Management 157

Domain or domain plus security token authentication 168

Client certificate or certificate plus domain authentication 174

PKI entities 196

Credential providers 214

APNs certificates 222

SAML for single sign-on with Citrix Files 231

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Authentication with Azure Active Directory through Citrix Cloud **241**

Authentication with Azure Active Directory Group-Based Administration **244**

Authentication with Azure Active Directory through NetScaler Gateway for MAM enrollment **246**

Authentication with Okta through Citrix Cloud **250**

Authentication with Okta through NetScaler Gateway for MAM enrollment **252**

Authentication with an on-premises NetScaler Gateway through Citrix Cloud **261**

nFactor authentication **263**

User accounts, roles, and enrollment **266**

Enrollment profiles **283**

Notifications **288**

Configure roles with RBAC **294**

Licenses **315**

Device management **315**

Alexa for Business **343**

Migrate from device administration to Android Enterprise **356**

Android Enterprise **361**

Distribute Android Enterprise apps **411**

Legacy Android Enterprise for Google Workspace (formerly G Suite) customers **437**

Android OS **474**

Firebase Cloud Messaging **480**

Support managed configurations feedback (Technical Preview) **487**

Android SafetyNet **492**

Play Integrity API **497**

Samsung **499**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Network Access Control **501**

iOS **507**

macOS **524**

Deploy devices through the Apple Deployment Programs **531**

Enroll Apple devices in bulk **548**

Integrate with Apple Education features **554**

Shared iPads **569**

Distribute Apple apps **581**

Network Access Control **608**

Windows Desktop and Tablet **614**

Enroll Windows devices in bulk **623**

Device policies **628**

AirPlay mirroring device policy **654**

AirPrint device policy **656**

App permissions device policy **657**

APN device policy **659**

App access device policy **661**

App attributes device policy **663**

App configuration device policy **665**

App inventory device policy **668**

Application Guard device policy **670**

App lock device policy **672**

Apps notifications device policy **677**

App uninstall device policy **678**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App uninstall restrictions device policy **680**

Automatically update managed apps device policy **680**

BitLocker device policy **682**

Bluetooth device policy **688**

Calendar (CalDav) device policy **688**

Cellular device policy **690**

Connection scheduling device policy **691**

Contacts (CardDAV) device policy **693**

Custom XML device policy **695**

Declarative Device Management policies (Technical Preview) **698**

Google Account device policy (Technical Preview) **699**

Passcode device policy (Technical Preview) **700**

Software Update Enforcement device policy (Technical Preview) **703**

Software Update Settings device policy (Technical Preview) **705**

Status Subscriptions device policy (Technical Preview) **707**

User Identity device policy (Technical Preview) **709**

Defender device policy **710**

Device Guard device policy **712**

Device Health Attestation device policy **713**

Device name device policy **714**

Education Configuration device policy **715**

Endpoint Management options device policy **718**

Citrix Endpoint Management uninstall device policy **720**

Exchange device policy **721**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Files device policy **727**

FileVault device policy **728**

Firewall device policy **731**

Font device policy **733**

Home screen layout device policy **734**

Import iOS & macOS Profile device policy **736**

Compliance Enforcement for Android device (Technical Preview) **739**

Keyguard Management device policy **745**

Kiosk device policy **749**

Knox Platform for Enterprise Key device policy **752**

Launcher configuration device policy **753**

LDAP device policy **754**

Location device policy **756**

Lock screen message device policy **762**

Mail device policy **763**

Managed configurations policy **766**

Managed domains device policy **778**

Maximum resident users device policy **780**

MDM options device policy **781**

Network device policy **782**

Network usage device policy **796**

Office device policy **797**

Organization information device policy **799**

OS Update device policy **799**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Passcode device policy **811**

Passcode lock grace period device policy **821**

Personal hotspot device policy **822**

Profile Removal device policy **823**

Provisioning profile device policy **823**

Provisioning profile removal device policy **824**

Proxy device policy **825**

Restrictions device policy **826**

Roaming device policy **872**

SCEP device policy **872**

Siri and dictation policies **876**

SSO account device policy **878**

Store device policy **879**

Subscribed calendars device policy **879**

Terms and conditions device policy **880**

Tunnel device policy **881**

VPN device policy **883**

Wallpaper device policy **919**

Web Content Filter device policy **921**

Web clip device policy **923**

Windows Agent device policy **925**

Windows GPO Configuration device policy **928**

Windows Hello for Business device policy **930**

Add apps **932**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App connector types **981**

Citrix Launcher **982**

Add apps using Apple Volume Purchase **985**

Use ShareFile with Citrix Endpoint Management **993**

SmartAccess for HDX™ apps **1009**

Upgrade MDX or enterprise apps **1026**

Add media **1028**

Deploy resources **1032**

Macros **1046**

Automated actions **1083**

Monitor and support **1093**

Connectivity checks **1101**

Mobile Service Provider **1107**

Reports **1109**

REST APIs **1116**

ActiveSync Gateway **1118**

Citrix Endpoint Management connector for Exchange ActiveSync **1120**

NetScaler Gateway connector for Exchange ActiveSync **1169**

Advanced concepts **1184**

Citrix Endpoint Management deployment **1185**

Management modes **1186**

Device requirements **1189**

Security and user experience **1190**

Apps **1207**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

User communities **1214**

Email strategy **1221**

Citrix Endpoint Management integration **1228**

Integrating with NetScaler Gateway and Citrix ADC **1235**

SSO and proxy considerations for MDX apps **1242**

Authentication **1247**

Server properties **1260**

Device and app policies **1276**

Client properties **1286**

User enrollment options **1297**

App provisioning and deprovisioning **1300**

Dashboard-based operations **1303**

Role-based access control and Citrix Endpoint Management support **1305**

Citrix Support process **1307**

Sending group enrollment invitations in Citrix Endpoint Management **1308**

Configuring certificate-based authentication with EWS for Citrix Secure Mail push notifications **1310**

Configuring an on-premises Device Health Attestation server **1313**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management

September 6, 2025

Citrix Endpoint Management is a solution for managing endpoints, offering Mobile Device Management (MDM), and mobile application management (MAM) capabilities. With Citrix Endpoint Management, you manage device and app policies and deliver apps to users. Your business information stays protected with strict security for identity, devices, apps, data, and networks.

Citrix® and customer responsibilities

Citrix Cloud Operations handles various infrastructure and monitoring tasks. As a result, you can focus on the user experience and on managing devices, apps, and policies.

Citrix responsibilities:

- Citrix Endpoint Management server nodes
- NetScaler Gateway (service or on-premises) initial integration and configuration
- NetScaler Gateway Load Balancer
- Database
- Cloud Connector software configuration
- SAML authentication integration with ShareFile
- Citrix Endpoint Management site monitoring: Instance, database, enterprise connectivity (LDAP), VPN tunnel (if applicable), public SSL certificate, Citrix Endpoint Management licensing

Customer responsibilities:

- NetScaler Gateway (on-premises) management and updates
- Machines where Cloud Connectors and Gateway Connector (for Citrix Gateway service) are installed
- LDAP/Active Directory
- DNS
- ShareFile: Initial ShareFile configuration, on-premises storage zones controller installation, Citrix Files updates
- Citrix Endpoint Management configuration: Devices, policies, apps, delivery groups, actions, and client certificates

Integration with Microsoft Endpoint Manager

Citrix Endpoint Management integrates with Microsoft Endpoint Manager (MEM). That integration adds the value of Citrix Endpoint Management micro VPN to Microsoft Intune aware apps, such as

© 1997–2025 Citrix Systems, Inc. All rights reserved.

the Microsoft Edge browser. With the integration, you can:

- Secure Office 365 applications with conditional access with Azure AD. For more information, see Integrate with Azure AD Conditional Access.
- Wrap your own line of business apps with Intune and Citrix to provide micro VPN capabilities inside an Intune mobile app management (MAM) container.
- Manage and deliver Office 365 apps, line of business apps, and Citrix Secure Mail in one container. This management method provides ultimate security and productivity. For example, you can:
  - Block individual devices or operating systems
  - Customize ActiveSync policies based on devices, users, or user groups
  - Quarantine at the device level
  - Monitor individual connections or devices
  - Avoid the security risks of credential and data caching

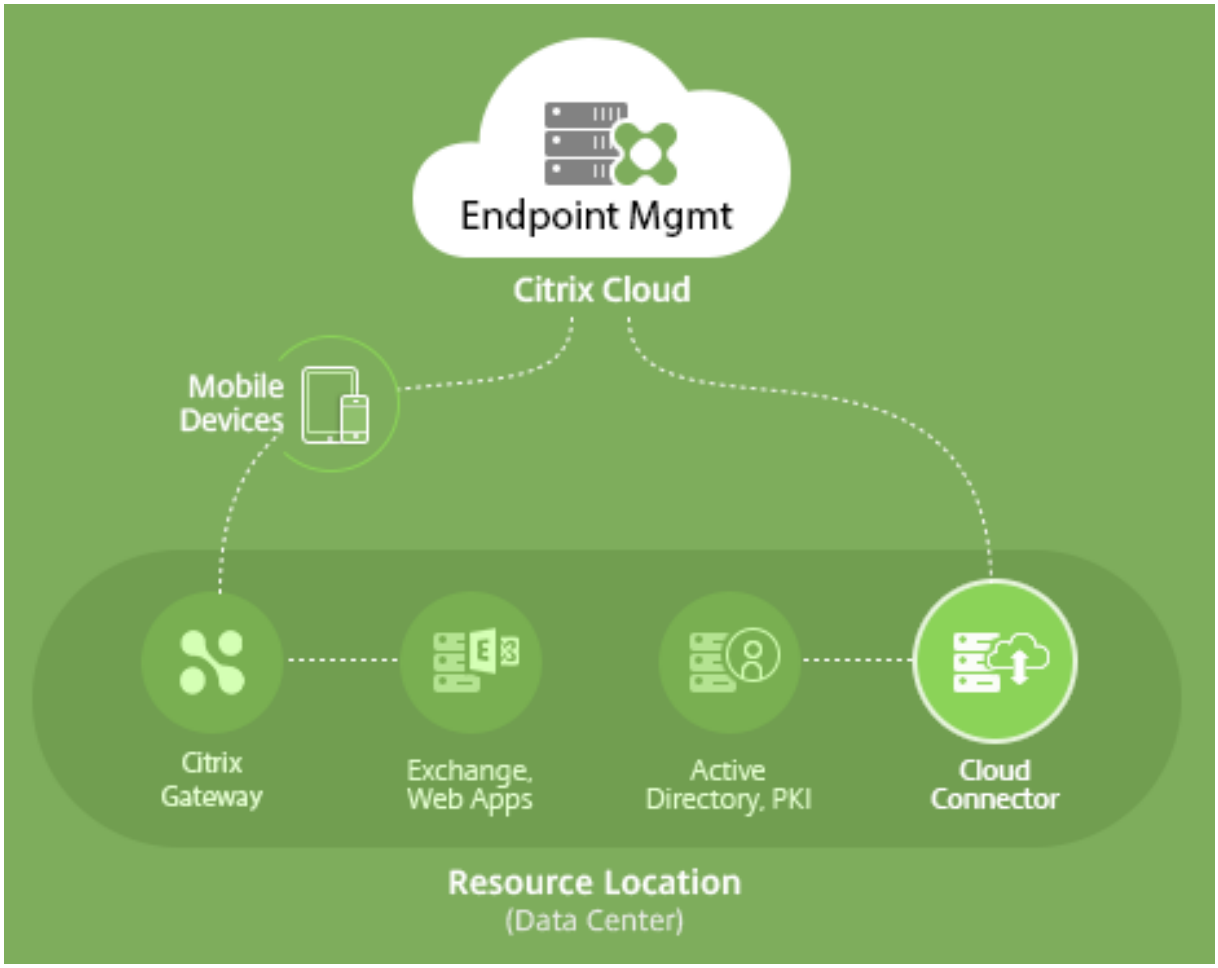
Use Citrix Endpoint Management MDM+MAM or Intune MDM to manage devices. For more information, see Citrix Endpoint Management integration with Microsoft Endpoint Manager.

Cloud Connector and resource locations

You connect to Citrix Endpoint Management through Cloud Connector. Cloud Connector serves as a channel for communication between Citrix Cloud and your resource locations. Cloud Connector enables cloud management without requiring any complex networking or infrastructure configuration such as VPNs or IPsec tunnels.

Resource locations have the resources required to deliver services to your subscribers. For Citrix Endpoint Management, resource locations are your NetScaler Gateway, LDAP, DNS, and PKI servers.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



For more information about Cloud Connector and resource locations, see About Citrix Endpoint Management.

Get started with Citrix Endpoint Management

> **Tip:**
>
> XenMobile® Migration Service
>
> If you're using XenMobile Server on-premises, our XenMobile Migration Service can get you started with Citrix Endpoint Management. Migration from XenMobile Server to Citrix Endpoint Management doesn't require you to re-enroll devices.
>
> For more information, contact your local Citrix salesperson, Systems Engineer, or Citrix Partner.
>
> To learn more about our migration service, see 3 reasons to move to Citrix Endpoint Management service.
>
> To see why to migrate, how to migrate, and the benefits of migrating to Citrix Endpoint Manage-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> ment, visit the CEM Migration Service Course Catalog, or refer to the Citrix Endpoint Management (CEM) Migration Service guide.

When you're evaluating or buying Citrix Endpoint Management, the Citrix Endpoint Management Operations team provides ongoing onboarding help. The Operations team also communicates with you to make sure the core Citrix Endpoint Management services are running and configured correctly. This figure shows the onboarding steps.

To sign up for a Citrix account and request an Citrix Endpoint Management trial, contact your Citrix Sales Representative. When you're ready to continue, go to https://onboarding.cloud.com.

For a quick overview of Citrix Endpoint Management onboarding and configuration, watch this video.

This is an embedded video. Click the link to watch the video

Want to learn more before starting? Try these resources:

Citrix Endpoint Management documentation: Provides full Citrix Endpoint Management documentation, from onboarding to initial configuration to advanced configuration. A "What's new" article describes new features and fixes. Citrix notifies you when that article is available for a new version.

Citrix Endpoint Management Onboarding Handbook: Consolidates all the available information around Citrix Endpoint Management, so you can continue smoothly enabling and onboarding Citrix Endpoint Management. You can use the document to record changes for your internal processes and to document your high-level and functional designs.

Citrix Endpoint Management Deployment Handbook: Planning an Citrix Endpoint Management deployment involves many considerations. The handbook includes recommendations, common questions, and use cases for your Citrix Endpoint Management environment.

SalesIQ: More resources for our Citrix Partners.

Next steps

For information about the Citrix Endpoint Management onboarding process, see Onboarding and resource setup.

After you complete onboarding, see Prepare to enroll devices and deliver resources.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Deprecation announcements

For advanced notice of the Citrix Endpoint Management features that are being phased out, see Deprecation.

Citrix Endpoint Management support

For details on how to access supported related information and tools in the Citrix Endpoint Management console, see Monitor and support.

Rolling updates to the Citrix Endpoint Management release occur approximately every two weeks. To you, the customer, this process is transparent. Initial updates are applied to Citrix internal sites only, and are then applied to customer environments gradually. We deliver updates incrementally in waves to provide product quality and to maximize availability.

Citrix Endpoint Management customers receive updates and communications directly from the Citrix Endpoint Management Cloud Operations team. Those updates keep you current with new features, known issues, fixed issues, and so on.

The Citrix Cloud Operations team maintains the Citrix Endpoint Management environments with the latest Citrix Endpoint Management rolling patches. To get specific patches or fixes that are required before the rolling patch, contact Citrix Technical Support.

If you have any issues with your environment, contact Citrix Technical Support or your Citrix Account team. Such issues might include mobile device enrollment, Citrix Endpoint Management console access, or Citrix Secure Mail issues.

If you need any integration or changes made on NetScaler Gateway in the Cloud or Citrix Endpoint Management, submit a request through Citrix Technical Support.

Examples of changes that you might request are:

- Citrix Files integration with NetScaler Gateway in the Cloud
- Change NetScaler Gateway authentication type
- Validate connectivity to customer data center resources
- Change split tunnel configuration for micro VPN
- Restart Citrix Endpoint Management components because of some server configuration changes

Service level agreement

Citrix Endpoint Management uses industry best practices to achieve cloud scale and a high degree of service availability.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For complete details about Citrix's commitment for availability of Citrix Cloud services, see the Service Level Agreement.

What's new

September 6, 2025

Citrix aims to deliver new features and product updates to Citrix Endpoint Management customers when they're available. New releases provide more value, so there's no reason to delay updates.

- Rolling updates to Citrix Endpoint Management go out approximately every three months.
- These updates don't result in any downtime for your instance or device users.
- Not every release has new features and some updates include fixes and performance enhancements.

To you, the customer, this process is transparent. We apply initial updates to Citrix® internal sites only, and then to customer environments gradually. Delivering updates incrementally in waves helps to provide product quality and to maximize availability.

You also receive Citrix Endpoint Management updates and communications directly from the Citrix Endpoint Management Cloud Operations team. Those updates keep you current with new features, known issues, fixed issues, and so on.

For more details, including cloud scale, and service availability, see the Citrix Endpoint Management Service Level Agreement. To monitor service interruptions and scheduled maintenance, see the Service Health Dashboard.

Citrix Endpoint Management 25.9.0

- **Support new strong certificate mappings for Certificate-based authentication:** A new mapping method is introduced to allow greater flexibility in issuing certificates that meet strong mapping requirements. Citrix Endpoint Management (CEM) now appends `URL=tag:microsoft.com,2022-09-14:sid:<user's SID>` to Subject Alternative Name (SAN) of certificates.
- **Support new iOS Setup Assistant Options in Apple Deployment Programs page:** Apple adds a few new iOS Setup Assistant Option screens for Apple Business Management enrollment. The following new options are added in the **Settings > Apple Deployment Programs > iOS Setup Assistant Options** page. You can configure Citrix Endpoint Management (CEM) to skip those screens. For more information, see iOS Setup Assistant Options.
  - Action Button

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - Lockdown Mode
  - Intelligence
  - Camera Button

- **Support new iOS restrictions for iOS 18.x version:** In Restriction policy for iOS, the following new settings have been added to block access to Apple Intelligence (AI) or restrict some of the new features. These settings are applicable for iOS versions 18 and later. Default is **On**. For more information, see Restrictions Policy.

  - Allow external intelligence integrations
  - Allow signing in to external intelligence integrations
  - Allow Mail Smart Replies
  - Allow Notes Transcription
  - Allow Safari Summary
  - Allow visual intelligence summary
  - Allow Notes Transcritpion Summary
  - Allow Apple Intelligence Report
  - Allow Default Calling App Modification
  - Allow Default Messaging App Modification
  - Allow External Intelligence Workspace IDs
  - Default Browser Modification
  - Allow FaceTime Remote Control

- **Support new iOS restrictions for iOS 17.x version:** In Restriction policy for iOS, the following new setting has been added for iOS versions 17.2 and later. Default is **On**. For more information, see Restrictions Policy.

  - Allow Live Voicemail

- **Manage Config policy text box:** When the customer uses **Knox Service Plugin** along with the **Managed Configuration policy**, the maximum character length for all the text boxes on **Separated Apps Policies** increases to 8,192 characters.

- **Enhanced dual SIM and eSIM support for Android Enterprise devices:** Citrix Endpoint Management (CEM) now provides comprehensive dual SIM support for Android Enterprise devices to ensure feature parity with iOS. This enhancement enables administrators to view all installed SIM cards and eSIMs in device properties, including configurations with two physical SIM cards, one SIM card plus one eSIM, or two eSIMs. This update addresses the growing adoption of dual SIM Android Enterprise devices and provides customers with complete visibility into their mobile device connectivity options, matching the eSIM capabilities previously delivered for iOS devices. This feature is supported only on Secure Hub version 25.7.0 or later.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Fixed issues in CEM 25.9.0

- The Legacy MDX alert continues to display on the CEM console even when no Legacy MDX application has been uploaded. [CXM-118574]
- Device Enrollment Program (DEP) devices continue to perform **MDM+MAM** enrollment even when the Enrollment Profile is configured as **MDM-only**. [CXM-118847]
- When the **Show New View** feature is enabled, the device count displays incorrectly even when filters are applied to the device list. [CXM-119347]
- Android Enterprise devices fail to receive **enrollment app** notifications sent by administrators through Citrix Endpoint Management™ (CEM). [CXM-119626]
- iOS users are unable to launch Secure Mail/Secure Web applications and experience "Unable to open"error when redirecting from Secure Mail/Secure Web to Secure Hub. [CXM-119659]

Citrix Endpoint Management 25.7.0

- **Enhanced user authentication workflow:** Users who enrolled devices with On-premises Active Directory (AD) and later integrated with Citrix identity provider using Microsoft Azure Active Directory (AAD) do not need to re-enroll. You can synchronize accounts from your on-premises Active Directory to Microsoft Azure Active Directory. For more information, see User authentication workflow.

Citrix Endpoint Management 25.5.0

- **Sync with Apple Business Management to manage device assignments:** Citrix Endpoint Management (CEM) now ensures accurate device assignment by syncing with Apple Business Management (ABM). This update verifies that only correctly assigned devices appear in CEM, preventing records of devices that have been removed from CEM and assigned to another vendor management solution. For example, if devices are moved to another solution, they no longer appear in CEM after the sync. This feature is controlled by a customer-managed tenant server property, `remove.unassigned.abm.devices`. By default, this property is set to **False**. For more information, see Server properties.

> **Note:**
>
> Apple Business Management (ABM) devices already enrolled are not removed from CEM, even if an administrator tries to move them.

- **Support for Declarative Device Management (DDM) (Technical Preview)**: A new feature "Declarative Device Management Support"is introduced to enable compatibility with Apple's Declarative Device Management (DDM) in iOS 15 and later. This feature improves performance and scalability by using a declarative data model, reducing reliance on serialized commands

© 1997–2025 Citrix Systems, Inc. All rights reserved.

and device polling. For more information, see Leveraging the declarative management data model to scale devices. Contact your admin to enable this feature if needed.

The following declarative device policies are supported when you enable the DDM feature:

- Google Account
- Passcode
- Software Update Enforcement
- Software Update Settings
- Status Subscriptions
- User Identity

Fixed issues in CEM 25.5.0

- The Role-Based Access Control (RBAC) admin is logged out unexpectedly when toggling **Show New View** on the Device page if they do not have the **Server Properties** permission.[CXM-118099]
- When the Show New View feature is enabled, Role-Based Access Control (RBAC) admins unexpectedly see the search input box.[CXM-118205]
- Some policies are not deployed to AE devices during re-enrollment when the **Deployment condition** is set to "Only when previous deployment has failed"in the **Deployment Schedule**.[CXM-118400]

Citrix Endpoint Management 25.3.0

- **Support for persistent filters on Device page:** In the new device page, filters are now supported for all **filterable** options. These filters are saved across sessions for the logged-in user, removing the need for the administrator to reapply the same filters each time they visit the device page. Filters are automatically removed if the corresponding column is de-selected.
- **Support preserve eSIM when the system erases the device:** A new setting, **Preserve eSIM on Erase**, is added to the Restriction Policy. This setting ensures that the eSIM is preserved when the system erases the device due to multiple failed password attempts or when the **Erase All Content and Settings** option is selected in **Settings > General > Reset**. This feature is available for iOS versions 17.2 and later, with the default setting set to **Off**. For more information, see the Restrictions Policy.

Fixed issues in CEM 25.3.0

- When the MDM certificate renewal fails, the old certificate is marked as revoked by Citrix Endpoint Management (CEM), preventing Secure Hub (SH) from reconnecting to the server. As a

© 1997–2025 Citrix Systems, Inc. All rights reserved.

result, SH is unable to communicate with the server using the old certificate, even though it has not yet expired. [CXM-117869]

- The Volume Purchase Program (VPP) app icon does not update when the application is upgraded to a new version. [CXM-117871]

Citrix Endpoint Management 25.1.0

- **Secure Hub APNs certificate renewal:** The Secure Hub Apple Push Notification service (APNs) certificate for Citrix Endpoint Management 24.10 expires on February 9, 2025. This update automatically renews the Secure Hub APNs certificate to a new certificate, valid until January 4, 2026.
- **Support blocking or restricting Apple Intelligence for iOS:** In the Restriction policy for iOS, new settings have been added to block access to Apple Intelligence (AI) or restrict some of the new features. These settings apply to iOS versions 18 and later, with the default set to **On**. For more information, see the Restrictions Policy. The new settings include:
  - Genmoji
  - Image Playground
  - Image Wand
  - iPhone Mirroring
  - Personalized Handwriting Results
  - Writing Tools
  - Call Recording
  - Apps To Be Hidden
  - Apps To Be Locked
  - Mail Summary
  - RCS Messaging
- **Support blocking or restricting Apple Intelligence for macOS:** In the Restriction policy for macOS, new settings have been added to block access to Apple Intelligence (AI) or restrict some of the new features. These settings apply to macOS versions 15 and later, with the default set to **On**. For more information, see the Restrictions Policy. The new settings include:
  - Image Playground
  - iPhone Mirroring
  - Writing Tools
  - Allow Media Sharing Modification

Fixed issues in CEM 25.1.0

- Numerous payload certificates were being generated for AE devices. [CXM-116956]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Some policies are not deployed to AE devices during re-enrollment when the **Deployment condition** is set to "Only when previous deployment has failed" in the **Deployment Schedule**. [CXM-117350]
- When you try to synchronize GEO specific Volume Purchase Program (VPP) applications to the Citrix Endpoint Management (CEM) server, the synchronization fails without any error message. The VPP applications do not reflect under the Citrix Endpoint Management App list even during manual Volume Purchase Synchronization. [CXM-117897]

Citrix Endpoint Management 24.10.0

- **Authentication with Azure Active Directory Group-Based Administration:** Citrix Endpoint Management supports group-based identity authentication through Azure Active Directory (AAD) and SAML identity providers, allowing administrators to manage access at the group level using AAD group membership. This update offers greater flexibility and enhanced security through centralized group controls. While this new functionality streamlines access management, the legacy Citrix Identity login mechanism also remains available to ensure backward compatibility. For more information, see Authentication with Azure Active Directory Group-Based Administration.
- **Support blocking of web distributed third party apps:** In Restriction policy, a new setting **Web Distribution apps** has been added to block the web distributed third party apps on iOS devices. This setting is applicable for iOS versions 17.5 and later. For more information see Restrictions Policy. Contact your admin to enable this feature if needed.
- **Unified Platform Experience:** Citrix Endpoint Management enables a unified platform experience by providing unified navigation across Citrix products. This feature changes the location of the navigation bar in the overall user interface and adds a new left navigation bar.
- **Citrix Endpoint Management enhancement to support Windows 2022 CA server:** Citrix Endpoint Management supports the following CA servers:
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server 2022
- **Monitor tab is deprecated:** Monitor Tab in Citrix Endpoint Management is deprecated from October 2024. For more information, see Deprecations and removals.
- **Update Public Rest API document to include device Lost Mode API:** Added the Lost Mode API in Public Rest API document.
- **Modify API call to be post body instead of URL:** Updated the API call to include the data in the request body rather than in the URL in Public Rest API document.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Support for Android 15:** Citrix Endpoint Management and Citrix Mobile productivity apps now supports Android Enterprise device updates to Android 15. For more information about security and privacy benefits, see the Android developer documentation.
- **Support for iOS 18:** Citrix Endpoint Management and Citrix Mobile productivity apps are now compatible with iOS 18, but don't currently support all the new iOS 18 features.
- **Support for macOS 15:** Citrix Endpoint Management and Citrix Mobile productivity apps are now compatible with macOS 15, but don't currently support all the new macOS 15 features.

Fixed issues in CEM 24.10.0

- VPP test connectivity and VPP synchronization failed for some apps. [CXM-117353]

Citrix Endpoint Management 24.8.0

- **Support managed configurations feedback (Technical Preview):** The Manage Configuration Feedback feature allows administrators to obtain feedback on app states from Android devices that are configured with managed configuration policies. For more information, see Support managed configurations feedback (Technical Preview).
- **Compliance Enforcement for Android device (Technical Preview):** For Android devices enrolled in Device Owner mode, the customer admin can manage the device compliance. For more information, see Compliance Enforcement for Android device (Technical Preview).

Fixed issues in CEM 24.8.0

- The secure action 'Delete All Users' failed on the shared iPad. [CXM-114866]
- Some iOS public apps on Citrix Endpoint Management cannot be located in the Apple Store. [CXM-114970]
- In Citrix Endpoint Management 24.4.0, SAML SSO fails after renewing the SAML certificate when using CEM as the SAML SSO Identity Provider (IDP). [CXM-115836]
- In a Certificate Based Authentication scenario, Secure Hub is experiencing functionality issues due to a failure in certificate renewal. The system admin might notice the generation of PKI certificates never stops, particularly on the Android platform. [CXM-116012]
- The Update option is not available in the Secure Hub store for MAM SDK enabled apps with new version. [CXM-116194]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management 24.6.0

- **Support block third party apps for iOS 17.4 and later:** In Restriction policy, a new setting **Alternative App Marketplace** has been added to prevent installation of alternative marketplace apps from the web and prevent any installed alternative marketplace apps from installing apps. For more information, see Restrictions device policy.
- **Support Firebase Cloud Messaging to use new HTTP v1 API:** The FCM legacy APIs for HTTP is going to be deprecated from Google on June 21, 2024. To make FCM work well with the new API, a new field **Service Account Key File** has been added to page Firebase Cloud Messaging for you to upload the service account key JSON file. For more information, see Firebase Cloud Messaging.

Fixed issues in CEM 24.6.0

- After an admin updates the AD group, the mobile apps assigned to the delivery group become inaccessible to the end users and the users may become anonymous. [CXM-115649]
- Secure Hub logs cannot be sent to the IT help desk when the customer selects **Send device logs to IT help desk** as directly in the **Client Support** settings. [CXM-115794]

Citrix Endpoint Management 24.4.0

- **Added new Knox Platform for Enterprise Key device policy:** A new device policy **Knox Platform for Enterprise Key** is added. 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. For more information, see Knox Platform for Enterprise Key device policy.
- **Enforce a minimum OS version in order to complete setup on Automated Enrollment:** With iOS 17, MDMs can now enforce a minimum operating system version on enrolling devices when using Automated Device Enrollment. For more information see, step 3 in Add your account to Citrix Endpoint Management.
- **Supports iOS 17 Return to Service:** 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.
- **Support Samsung Enhanced Attestation v3:** Samsung Enhanced Attestation v3 improves CEM security functionality on Samsung Knox devices. For more information see Samsung Knox Enhanced Attestation.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Modernize sorting and filtering in Device enrollment:** The list views in CEM are currently difficult to navigate and less user-friendly. By moving filtering and sorting options to the column headers, customers can easily combine these functions, making it much simpler and intuitive to find the data they need.
- **Support to install OS updates immediately for iOS devices:** In the OS Update device policy, a new radio button named **Install ASAP** is added in the OS update options for iOS. This feature allows you to install the previously downloaded OS updates immediately for iOS devices. For more information, see OS Update device policy for iOS.
- **Enhance automatic Always-On VPN connection restart:** A new managed configuration setting **Always On VPN (optional)** has been added to Citrix Secure Access app, which must be set to "true"for this enhancement to work reliably for Always On VPN profiles. For more information, see Configure the Citrix SSO protocol for Android and Create an Android Enterprise managed configuration for Citrix SSO.

Fixed issues in CEM 24.4.0

- Enterprise apps might report incorrect version number after upgrade in iOS devices. [CXM-112711]
- Enrolled iOS devices are prompted to enter UPN on Secure Hub. [CXM-114316]

Citrix Endpoint Management 24.1.0

This version addresses several issues that help to improve overall performance and stability. No new features were added.

Citrix Endpoint Management 23.12.0

Added a new mandatory field "Domain"in the 802.1x settings for Android: A new field **Domain** is added in the **Android Enterprise platform network policy** settings page for **802.1x EAP** authentication type. For more information, see 802.1x settings for Android.

Current known issues

Known issues in Citrix Endpoint Management 22.6.0

Intermittently, selecting all three log types (**Debug**, **Admin Audit**, **User Audit**) to download under **Troubleshooting and Support > Logs** isn't working. Only Debug logs are being downloaded. As

© 1997–2025 Citrix Systems, Inc. All rights reserved.

a workaround, you can download each log separately, or open your browser in incognito mode to download all logs by marking all three checkboxes. [CXM-105334]

When creating a web link in Android Enterprise, an error occurs when trying to save the app with an icon. This error is a Google services issue. As a workaround, save the app without uploading an icon. [CXM-105395]

Samsung Knox/SAFE policies are still active on enrolled devices even after deprecation, and cannot be disabled or configured. As a workaround, unenroll and reenroll the device. [CXM-104303]

Known issues in Citrix Endpoint Management 22.4.0

When searching for an enrolled active directory user on the **Monitor** tab, no enrolled devices are shown for the user. You can still see policies and apps assigned to the user, and use all security actions from **Manage > Devices**. Both iOS and Android enrolled devices are affected. [CXM-104283]

Private apps fail to publish using Android Enterprise because of an issue in Google services. We will update our documentation when the issue is resolved. [CXM-103690]

Known issues in Citrix Endpoint Management 21.12.0

After migrating to Citrix Cloud based RBAC, admin users with full access permission in Citrix Cloud also get full access permission in CEM, even if they had custom permission before the migration. As a workaround, you can update admin permissions on the Citrix Cloud Identity and Access Management page with the required access. [CXM-102765]

Customers who onboarded before 2018 have local admin access to the console. CEM admin users with permissions to add or edit local users can also add or edit local users in Citrix Cloud. These permissions include changing local users' passwords. To remediate this issue, you can call Support to have direct local admin access to the console blocked, allowing only Citrix Cloud admin access. [CXM-102780]

Known issues in Citrix Endpoint Management 21.11.0

On iOS devices enrolled only in MAM, enterprise apps fail to install. [CXM-101852]

Using the **Automatically Update Managed Apps** policy for Android Enterprise fails to apply on devices when the CEM server is upgraded to 21.11.0. The policy failure impacts app updates on the device. As a workaround, an administrator can edit and save the policy to refresh the default values. [CXM-102446]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Known issues in Citrix Endpoint Management 21.10.0

The VPN device policy does not work properly on managed Windows 11 devices. We reported this issue to Microsoft and are working with them to resolve it. We'll provide updates on any progress.

Known issues in Citrix Endpoint Management 21.9.1

On Android devices enrolled in work profile on corporate-owned devices mode: Users might see errors saying they can't install or search apps on their personal profile. If they see those errors, update the Google Play Store app and try again. [CXM-100678]

Known issues in Citrix Endpoint Management 21.5.0

Users can't authenticate to Azure Active Directory (AAD) if they:

1. Enroll their device in Citrix Endpoint Management using AAD credentials.
2. Launch an Office 365 app and complete the AAD registration.
3. Remove their account from the Microsoft Authenticator app.
4. Launch an Office 365 app and sign out.

As a workaround, unenroll the device from Citrix Endpoint Management and re-enroll. [CXM-90235]

Known issues in Citrix Endpoint Management 21.4.0

Re-enrollment fails on iOS devices if the user trying to re-enroll is a different Azure Active Directory user than the user originally enrolled on the device. As a workaround, unregister the original user from the Microsoft Authenticator app on the device before re-enrolling. [CXM-90218]

Known issues in Citrix Endpoint Management 21.2.0

When adding Citrix Secure Web as an MDX app for Android Enterprise, Managed Google Play can't find the app using the app identifier. If you search for "Citrix Secure Web"instead of the app identifier, Managed Google Play can find the app. This issue is a Google bug. [CXM-91991]

Importing the SSL Listener certificate might fail. Repackage the certificate keystore by following the steps in CTX-297153. [XMHELP-3346]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Known issues in Citrix Endpoint Management 20.10.1

If you upgrade on-premises Citrix ADC to 13.0-64.35 or later, and Citrix Endpoint Management isn't Workspace-enabled: Single sign-on to Citrix Files or the ShareFile domain URL results in an error. The user is unable to sign in. This error only occurs in a browser with the **Company Employee Sign in** option.

To work around this issue: If you haven't already run the following commands from the ADC CLI on NetScaler Gateway, run them to enable global SSO:

```
set vpn parameter SSO ON
```

```
bind vpn vs <vsName> -portalTheme X1
```

For more information, see:

- Citrix ADC Release
- Impacted SSO configurations

After you complete the workaround, users can authenticate to Citrix Files or the ShareFile domain URL using SSO in a browser with the **Company Employee Sign in** option. [CXM-88400]

Known issues in Citrix Endpoint Management 20.2.1

After configuring ShareFile with a ShareFile URL in the Citrix Endpoint Management console, clicking the **Test Connection** button results in an error. To resolve this issue, disable multifactor authentication for ShareFile. Learn more about this issue and the workaround on this Reset user phone number for Two Step Verification. [CXM-79240]

Known issues in Citrix Endpoint Management 20.1.0

When adding users to a library in Citrix Cloud, Citrix Endpoint Management reports success, but the users aren't added. [CXM-73726]

Known issues in Citrix Endpoint Management 19.11.0

MDX and Public apps can't be deleted from the console. As a workaround, select the app you want to delete and then click **Edit**. Deselect **Android Enterprise** and select any other platforms from the platform list. Save the app. You can then delete the app. [CXM-74468]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Known issues in Citrix Endpoint Management 19.5.0

When enrolling a Citrix Ready® workspace hub device, define the Ethernet (eth0) MAC address in the allow list to avoid failed enrollment. [CXM-43141]

Known issues in Citrix Endpoint Management 19.4.1

When tabbing through options in the Windows GPO device policy, radio buttons and checkboxes get skipped. [CXM-58277]

Known issues in Citrix Endpoint Management 19.2.1

If you unenroll an Android Enterprise enterprise by deleting it through the Google admin console: Trying to re-enroll the enterprise might fail. Always use the Citrix Endpoint Management console to unenroll an Android Enterprise enterprise, as described in Unenroll an Android Enterprise enterprise. Google Workspace customers, follow the instructions in Unenrolling an Android Enterprise enterprise. [CXM-62709] [CXM-62950]

Known issues in Citrix Endpoint Management 19.2.0

When creating a public store app in Citrix Endpoint Management 10.18.3: On the iPad App Settings page, if you click **Back** without searching for apps, and then you click **Next**, the following issue occurs. The navigation buttons appear unresponsive and don't allow you to search for apps. The issue occurs when creating public store apps for both iOS or Android. [CXM-46820]

Known issues in Citrix Endpoint Management 10.19.1

After you complete the registration process on the **Settings > Android Enterprise** page, the following error message appears: `A configuration error occurred. Please try again`. When you close the error message, your Android Enterprise configuration is saved, however **Enable Android Enterprise** is **Off**. To work around this issue, reduce the number of app categories to 30 or fewer. [CXM-60899]

Known issues in Citrix Endpoint Management 10.18.5

When a Chrome app is configured as a required app for Chrome OS devices: Users might need to log off and log back on to install the app. This third-party issue is Google bug ID #76022819. [CXM-48060]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Known issues in Citrix Endpoint Management 10.18.3

After you delete a Citrix Cloud administrator who has a device enrolled: Citrix Endpoint Management doesn't update the User Role in the Citrix Endpoint Management console until after the administrator logs in again from the Citrix Secure Hub app or the Self-Help Portal. [CXM-45730]

Known issues in Citrix Endpoint Management 10.7.4

If you configure Citrix Endpoint Management for single sign-on (SSO) using the Citrix identity provider with Azure Active Directory: When an Citrix Endpoint Management administrator or user gets redirected to the **Azure Active Directory sign-in** screen, the screen includes the message "Sign-in page for Citrix Secure Hub."The correct message is "Sign-in page for Citrix Endpoint Management console." [CXM-42309]

Third-party notices

September 6, 2025

Citrix Endpoint Management might include third-party software licensed under the terms defined in the following document:

Citrix Endpoint Management Third-Party Notices

Deprecation

September 6, 2025

The announcements in this article are advanced notice of the Citrix Endpoint Management features that are being phased out, so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality. For details about product lifecycle support, see the Product Lifecycle Support Policy article.

> **Important:**
>
> Thank you for using the Citrix Endpoint Management Analyzer Tool, we appreciate it. Owing to our frequent and stable release cadence, this tool is no longer required. Citrix has decided to stop this service from March 31, 2023. We recommend that you use the connectivity checks available within the Citrix Endpoint Management console or Citrix NetScaler Gateway. For more

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> information, see Connectivity checks.

Deprecations and removals

The following list shows the Citrix Endpoint Management features that are deprecated or removed.

Deprecated items aren't removed immediately. Citrix® continues to support a deprecated item until removing it in a future release.

Removed items are either removed, or are no longer supported, in Citrix Endpoint Management.

For information about the mobile productivity apps that reached End of Life, see EOL and deprecated apps.

Item	Description	Deprecation announced	Removed	Alternative
Manage Microsoft Intune apps through the Citrix Cloud™ (CC) Library.	Deprecated support for Microsoft Intune apps management through the CC Library. You will not be impacted if you already have Intune apps in use.	March 2025	April 2025	Contact Citrix Support to enable this feature if needed.
Two Samsung Fully managed device only restrictions for Android Enterprise.	Deprecated these settings from the Restrictions policy: Enable ODE Trusted Boot verification and Enable revocation check.	February 2025	March 2025	No alternative

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
Samsung Knox container only restrictions for Android Enterprise.	Deprecated these settings from the Restrictions policy: Move apps to container, Enforce multi-factor authentication, Enforce authentication for container, and Enable secure keypad	February 2025	Target: June, 2025	No alternative
Integration with ShareFile	Integration with ShareFile will be deprecated if ShareFile (now Progress) discontinues support.	January 2025		No alternative
Monitor tab	Deprecated Monitor Tab in Citrix Endpoint Management.	September 2024	October 2024	No alternative
Citrix Endpoint Management Government offering	Deprecated support for Citrix Endpoint Management Government offering.	January 2022	July 2022	Citrix Endpoint Management Standard edition

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
SafetyNet Attestation API	Deprecated support for Android SafetyNet Attestation per the announcement from Google here.	July 2023	November 2023	Play Integrity API
Chrome OS	Deprecated support for Chrome OS.	July 2022	May 2023	No alternative
tvOS	Deprecated support for tvOS.	July 2022	May 2023	No alternative
Windows Information Protection (WIP)	Deprecated support for Windows Information Protection per the announcement from Microsoft here.	August 2022	October 2022	No alternative
Citrix Endpoint Management Analyzer	Deprecated support for the Citrix Endpoint Management Analyzer tool.	July 2022	Target: March 31, 2023	No alternative
Workspace hub device management	Deprecated support for Citrix Ready® workspace hub devices.	January 2022	June 2022	No alternative

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
Microsoft Store for Business	Deprecated support for Microsoft Store for Business. Microsoft no longer supports this platform. For more information, see the Microsoft documentation.	July 2021	Target: March 2023	No alternative
Samsung SAFE	Deprecated support for Samsung SAFE.	January 2022	June 2022	Use Android Enterprise.
Custom XML for Zebra	Deprecated support for custom XML on Zebra devices.	January 2022	June 2022	Use Android Enterprise managed configuration.
PKI identities: Generic, Symantec PKI, DigiCert, and Entrust	Deprecated support for Generic, DigiCert Managed, and Entrust adapter PKI entities.	June 2021	January 2022	No alternative
Android for Workspace	Deprecated support for Android for Workspace	January 2022	April 2022	No alternative
Carrier SMS Gateway	Deprecated support for Nexmo SMS gateway notifications	January 2022	April 2022	Use SMTP server notifications

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
Mobile Service Provider (MSP)	Deprecated support for MSP interface to query Blackberry and other Exchange ActiveSync devices and issue operations	January 2022	April 2022	No alternative
MDX Toolkit	Deprecate support for the MDX Toolkit in favor of the Mobile App Management (MAM) SDK. During the transition period, you can use both MDX wrapped apps and MAM SDK developed apps.	March 2020	July 2023	To continue managing your enterprise applications, use the MAM SDK.
RBAC Role - Shared devices enroller and COSU devices enroller	Deprecate support for predefined Role Based Access Control settings for both Shared devices enroller and COSU devices enroller	July 2021	December 2021	Configure iOS devices through Apple School Manager or Apple Business Manager. Configure Android COSU (dedicated) devices through enrollment profiles.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
Allow auto-connect to Wi-Fi sense hotspots restriction for Windows devices.	Remove support for the Allow auto-connect to Wi-Fi sense hotspots restriction for Windows 10 devices. Windows 10 no longer supports this feature. For information, see the Microsoft documentation.	October 2021	February 2022	No alternative
MDX: Alternative Gateway Server	Deprecate step-up authentication for iOS and Android devices.	March 2020	September 2021	No alternative
MDX: Micro VPN (full tunnel mode)	Deprecated a full virtual private network (VPN) tunnel for iOS and Android devices.	March 2020	September 2021	Use the MAM SDK Web SSO mode or create a per-app VPN policy with the Citrix SSO connection type.
MDX: PAC file support	Deprecated support for a Proxy Automatic Configuration (PAC) file with a full VPN tunnel deployment for iOS and Android devices.	March 2020	September 2021	Use NetScaler Gateway to connect through a proxy server for access to internal networks.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
MDX shared device support	Deprecated shared device support for MDX apps.	March 2020	September 2021	For Android Enterprise, use shared devices enrolled as dedicated devices. For iOS, use Apple School Manager or GroundControl.
Android - Sony	Deprecated support for Android Sony devices and Sony-specific policies.	January 2021	February 2022	Use Android Enterprise
Android - HTC	Deprecated support for Android HTC devices and HTC-specific policies.	January 2021	February 2022	Use Android Enterprise
Android - Amazon	Deprecated support for Android Amazon devices and Amazon-specific policies.	January 2021	February 2022	Use Android Enterprise
Knox Mobile Enrollment (legacy DA)	Deprecated support for Knox Mobile Enrollment (KME) in the legacy Device Administrator mode on all Android versions.	May 4, 2021	September 2021	Use KME to enroll in Android Enterprise mode. Android 8, 9, 10, 11 support Android Enterprise.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
High Security enrollment mode	Deprecated support for generating enrollment invitations with the **High Security** enrollment security mode.	July 2021	February 2022	See Enrollment invitations for a list of supported enrollment security modes.
Derived credentials	Deprecated support for derived credentials and the Citrix Derived Credential Manager app.	March 2021	December 2021	See iOS for a list of authentication types supported for iOS.
APNs outgoing ports	Apple support for the APNs legacy binary protocol ends from March 31, 2021. Apple recommends that you use the HTTP/2-based APNs provider API instead. As part of this change, we're deprecating support for ports 2195 and 2196, used to send APNs notifications to `*.push.apple.com`.	October 2020	March 2021	Use port 443 instead. See Network and firewall requirements.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
MDX Service	Deprecated support for the MDX Service in favor of the Mobile App Management (MAM) SDK. During the transition period, you can use both MDX wrapped apps using the MDX Toolkit and MAM SDK developed apps.	March 2020	September 2021	To continue wrapping your enterprise applications, use the MDX Toolkit.
Enrollment invitation setup in the Self-Help Portal	Deprecated support for users to generate enrollment invitations from the Self-Help Portal.	July 2021	July 2021	Contact your administrator to generate enrollment invitations in the Citrix Endpoint Management console.
Enrollment invitation setup	Deprecated support for using a device IMEI, serial number, and UDID to create an enrollment invitation.	April 2021	July 2021	When you create an enrollment invitation, configure the available settings under **Manage > Enrollment Invitations** in the Citrix Endpoint Management console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
Certificate-based authentication signature algorithms (non-FIPS and weak ciphers)	Deprecated support for the following signature algorithms: SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA, SHA1withDSA, RIPEMD160withRSA, RIPEMD128withRSA, RIPEMD256withRSA.	May 2020	June 2021	When you create a CSR for a credential provider in the Citrix Endpoint Management console (**Settings > Credential Providers > Certificate Signing Request**), choose a stronger cipher.
Citrix mobility apps and Workspace apps for Android 7.x and iOS 12.x	Deprecated support for the Android 7.x and iOS 12.x versions of Citrix Secure Hub, Citrix Secure Mail, Citrix Secure Web, and Citrix Workspace app.	April 2021	June 2021	Use, at a minimum, the current and prior version of each major operating system platform. Older devices remain enrolled. However, Citrix doesn't test or support the legacy devices.
RSA soft token support for Android	Deprecated support for the direct import of RSA soft tokens into Citrix Secure Hub for Android.	January 2021	February 2021	You can import the RSA soft token inside the RSA secure ID app available in Google Play. You can then use the token for NetScaler Gateway authentication.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
Internet Explorer 11	Deprecated support of Internet Explorer use with the Citrix Endpoint Management console.	January 2021	January 2021	Use the latest version of these web browsers: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari
Gateway configuration checks in Citrix Endpoint Management Analyzer	Deprecated support for the Gateway configuration check option.	November 2020	November 2020	Use the Citrix Insight Services check in Analyzer to check your Citrix ADC configurations for Citrix Endpoint Management deployment readiness.
Apps published for the legacy Device Administrator mode on Android Enterprise devices	We no longer deliver apps published for the legacy DA platform to devices enrolled in Android Enterprise.	October 2020	November 2020	For Android Enterprise devices, publish apps for the Android Enterprise platform. To continue to publish legacy DA apps to devices in DA mode, create a separate delivery group for those apps.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
Legacy Device Administrator mode for Android 10 devices	Google deprecated some Device Administrator APIs. Citrix doesn't support Android 10 devices enrolled into Device Administrator mode as of the upgrade to Citrix Secure Hub that targets Android API level 29.	February 2020	November 2020	Migrate Android 10 devices to Android Enterprise.
Android TouchDown	DigiCert stopped supporting Android TouchDown. Citrix removed the Android TouchDown platform page from the Exchange device policy.	July 2018	November 2020	Recommendation: Use Citrix Secure Mail.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
New Device Administrator enrollments for Android 10	Deprecated support for new enrollments or re-enrollments into the legacy Device Administrator mode on Android 10 devices. Already enrolled devices continue to work.	February 2020	September 2020	Enroll new Android 10+ devices into Android Enterprise.
MDX encryption	Deprecated MDX encryption and the MDX encryption feature in the Citrix Endpoint Management console.	October 2019	September 2020	Enable iOS or Android platform encryption using our Encryption Management feature with added compliance checking. Ensure you have tested and planned for migration off MDX encryption by July 2020.
Windows Mobile/CE	Deprecated support for Windows Mobile/CE devices.	April 2018	September 2020	Use Windows 10 Desktop and Laptop.
Samsung SEAMS container	Deprecated support for the Samsung SEAMS container.	June 2020	August 2020	Use Android Enterprise.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
Remote Support	Deprecated the Remote Support client.	January 2019	August 2020	No alternative
Citrix mobility apps and Workspace apps for Android 6.x and iOS 11.x	Deprecated support for the Android 6.x and iOS 11.x versions of Citrix Secure Hub, Citrix Secure Mail, Citrix Secure Web, and Citrix Workspace app.	April 2020	June 2020	Use, at a minimum, the current and prior version of each major operating system platform. Older devices remain enrolled. However, Citrix doesn't test or support the legacy devices.
Citrix Secure Hub Network Extensions for iOS	Deprecated the Network Extension framework that allowed you to customize networking features for iOS devices. Citrix Secure Hub release 20.3.0.	October 2018	March 2020	No alternative
API sign in using local accounts	Administrators can no longer sign in to the REST API using a local account.	October 2020		Administrators can log in using a Citrix Cloud account. See REST API.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Item	Description	Deprecation announced	Removed	Alternative
Self-signed Secure Sockets Layer (SSL) certificates	Deprecated support for self-signed SSL certificates for all device platforms.	May 2020		Replace your existing self-signed certificate with a trusted SSL certificate from a well-known certificate authority (CA).
Full VPN tunnel - Android	Deprecated support for Android Full VPN tunnel.	March 2020	September 2021	MAM SDK Web SSO mode.
Permit VPN mode switching - Android	Deprecated support for Android Permit VPN mode switching.	March 2020	September 2021	No alternative
Inbound Document Exchange - Android	Deprecated support for Android Inbound Document Exchange.	March 2020	September 2021	No alternative

System requirements

February 22, 2024

While waiting for Citrix to provision Citrix Endpoint Management, be sure to prepare for your Citrix Endpoint Management deployment by installing Cloud Connector. Although Citrix hosts and delivers your Citrix Endpoint Management solution, some communication and port setup is required. That setup connects the Citrix Endpoint Management infrastructure to corporate services, such as Active Directory.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Cloud Connector requirements

Citrix uses Cloud Connector to integrate the Citrix Endpoint Management architecture into your existing infrastructure. Cloud Connector integrates the following resource locations to Citrix Endpoint Management securely over port 443: LDAP, PKI Server, internal DNS queries, and Citrix Workspace enumeration.

- At least two dedicated Windows Server machines that are joined to your Active Directory domain. The machines can be virtual or physical. The machine where you're installing the Connector must be in sync with UTC time for proper installation and operation. For a full list of the latest requirements, see the deployment materials provided by your Citrix Account team.

  The onboarding wizard guides you through installing Cloud Connector on those machines.
- For more platform system requirements, see Citrix Cloud Connector.

Supported Active Directory functional levels

For use with Citrix Endpoint Management, the Citrix Cloud Connector supports the following forest and domain functional levels in the Active Directory.

Forest Functional Level	Domain Functional Level	Supported Domain Controllers
Windows Server 2016	Windows Server 2016	Windows Server 2016, Windows Server 2019
Windows Server 2016	Windows Server 2019	Windows Server 2019
Windows Server 2019	Windows Server 2019	Windows Server 2019

> **Note:**
>
> Windows Servers 2012 R2, 2012, and 2008 R2 are no longer supported as they have reached end of life. For more information, see Microsoft products life cycle documentation.

NetScaler Gateway requirements

Citrix Endpoint Management requires a NetScaler Gateway installed in your resource location for the following scenarios:

- You require a micro VPN for access to internal network resources for line-of-business apps. Those apps are wrapped with Citrix MDX technology. The micro VPN needs NetScaler Gateway to connect to internal back-end infrastructures.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- You plan to use Citrix mobile productivity apps, such as Citrix Secure Mail.
- You plan to integrate Citrix Endpoint Management with Microsoft Endpoint Manager.

The requirements:

- Domain (LDAP) authentication
- NetScaler Gateway 12.1 or above, with a Platform/Universal license

For details, see Licensing.

- Public SSL Certificate.

For details, see Create and Use SSL Certificates on a Citrix ADC Appliance.

- Unused public IP address for NetScaler Gateway Virtual Server
- Publicly resolvable Fully Qualified Domain Name (FQDN) for NetScaler Gateway Virtual Server
- Cloud-hosted Citrix Endpoint Management Intermediate and Root certificates (provided in the script bundle)
- Unused internal private IP address for the proxy load balancer IP
- For port requirements, see NetScaler Gateway port requirements later in this article.
- Citrix Endpoint Management integration with Microsoft Endpoint Manager
- Deploy Citrix ADC VPX instance on Microsoft Azure

For information about NetScaler Gateway requirements, see the deployment materials provided by your Citrix Account team.

For information about Android Enterprise requirements, see the Android Enterprise section.

Citrix Files requirements

Citrix Files file sync and sharing services are available in the Citrix Endpoint Management Premium Service offering. Storage zones controller extends the Citrix Files software as a service (SaaS) cloud storage by giving private data storage to your Citrix Files account.

Storage zones controller requirements:

- A dedicated physical or virtual machine
- Windows Server 2012 R2 (Datacenter, Standard, or Essentials), Windows Server 2016, Windows Server 2019, or Windows Server 2022
- 2 vCPUs
- 4 GB RAM
- 50 GB hard disk space
- Server roles for Web Server (IIS):

© 1997–2025 Citrix Systems, Inc. All rights reserved.

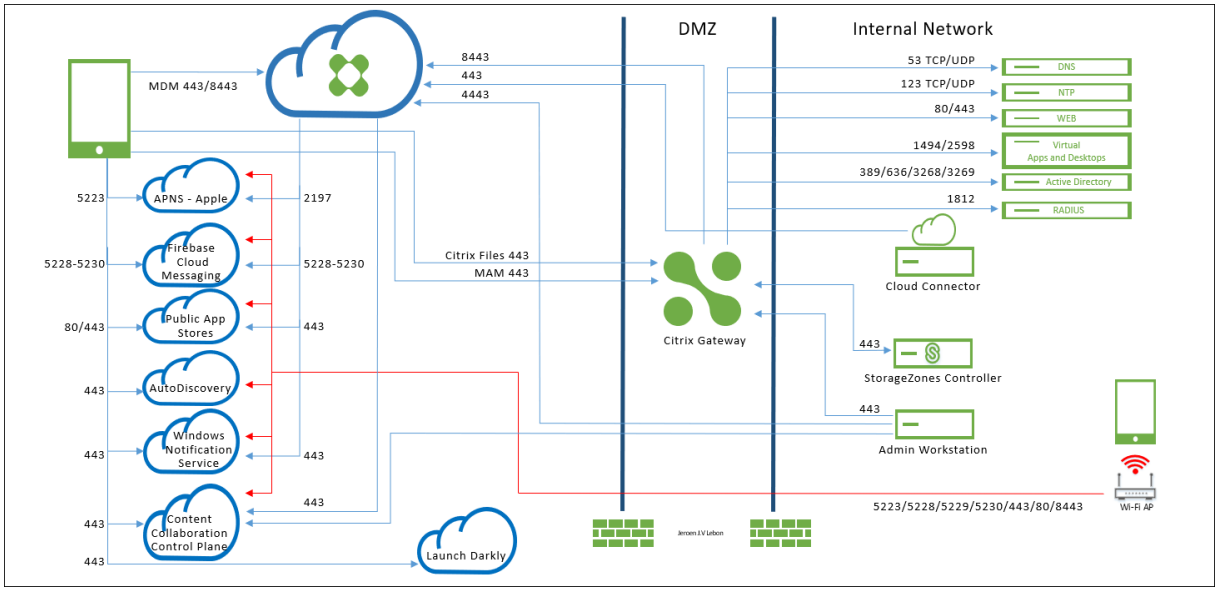
- Application Development: ASP. NET 4.5.2
- Security: Basic Authentication
- Security: Windows Authentication

Citrix Files platform requirements:

- The Citrix Files installer requires administrative privileges on the Windows Server
- Citrix Files Admin user name

Port requirements

To enable devices and apps to communicate with Citrix Endpoint Management, you open specific ports in your firewalls. The following diagram shows the traffic flow for Citrix Endpoint Management.



The following sections list the ports that you must open. For information about the URLs that mobile productivity apps use, see Feature flag management.

NetScaler Gateway port requirements

Open ports to allow user connections from Citrix Secure Hub and Citrix Workspace through NetScaler Gateway to:

- Citrix Endpoint Management
- StoreFront
- Other internal network resources, such as intranet websites

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For more information about NetScaler Gateway, see Configuring Settings for your Citrix Endpoint Management Environment in the NetScaler Gateway documentation. For information about IP addresses, see How NetScaler Gateway uses IP addresses in the NetScaler Gateway documentation.

TCP Port	Description	Source	Destination
53 (TCP and UDP)	Used for DNS connections.	NetScaler Gateway SNIP	DNS server
80/443	NetScaler Gateway passes the micro VPN connection to the internal network resource through the second firewall.	NetScaler Gateway SNIP	Intranet websites
123 (TCP and UDP)	Used for Network Time Protocol (NTP) services.	NetScaler Gateway SNIP	NTP server
389	Used for insecure LDAP connections.	NetScaler Gateway NSIP (or, if using a load balancer, SNIP)	LDAP authentication server or Microsoft Active Directory
443	Used for connections to StoreFront from Citrix Workspace to Citrix Virtual Apps and Desktops.	Internet	NetScaler Gateway
443	Used for connections to Citrix Endpoint Management for web, mobile, and SaaS app delivery.	Internet	NetScaler Gateway
443	Used for Cloud Connector communication –LDAP, DNS, PKI & Citrix Workspace enumeration	Cloud Connector Servers	`https://*.citrixworkspacesapi.net`, `https://*.cloud.com (commercial)`, `https://*.blob.core.windows.net/`, `https://*.servicebus.windows.net`

© 1997–2025 Citrix Systems, Inc. All rights reserved.

TCP Port	Description	Source	Destination
443	Used for accessing the Citrix Endpoint Management Self-Help Portal, if enabled, through the browser.	Access point (browser)	Citrix Endpoint Management (`https://<sitename>/zdm/shp`)
636	Used for secure LDAP connections.	NetScaler Gateway NSIP (or, if using a load balancer, SNIP)	LDAP authentication server or Active Directory
1494	Used for ICA connections to Windows-based applications in the internal network. Citrix recommends keeping this port open.	NetScaler Gateway SNIP	Citrix Virtual Apps and Desktops
1812	Used for RADIUS connections.	NetScaler Gateway NSIP	RADIUS authentication server
2598	Used for connections to Windows-based applications in the internal network using session reliability. Citrix recommends keeping this port open.	NetScaler Gateway SNIP	Citrix Virtual Apps and Desktops
3269	Used for Microsoft Global Catalog secure LDAP connections.	NetScaler Gateway NSIP (or, if using a load balancer, SNIP)	LDAP authentication server or Active Directory
4443	Used for accessing the Citrix Endpoint Management console by an administrator through the browser.	Access point (browser)	Citrix Endpoint Management

© 1997–2025 Citrix Systems, Inc. All rights reserved.

TCP Port	Description	Source	Destination
8443	Used for enrollment, app store, and mobile app management (MAM).	NetScaler Gateway SNIP	Citrix Endpoint Management
8443	Secure Ticket Authority (STA) port used for Citrix Secure Mail authentication token	NetScaler Gateway SNIP	Citrix Endpoint Management

Network and firewall requirements

To enable devices and apps to communicate with Citrix Endpoint Management, you open specific ports in your firewalls. The following tables list those ports.

Open ports from the internal network to Citrix Cloud:

TCP port	Source IP	Description	Destination	Destination IP
443		Cloud Connector	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.sharefile.com, https://cwsproduction.blob.core.windows.net/downloads, https://*.servicebus.windows.net	

© 1997–2025 Citrix Systems, Inc. All rights reserved.

TCP port	Source IP	Description	Destination	Destination IP
443		Administrative Console	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.citrix.com, https://cwsproduction.blob.core.windows.net/downloads	
443		Citrix Endpoint Management Self-Help Portal access through a browser (if the portal is enabled)	Citrix Endpoint Management	
4443		Citrix Endpoint Management console access through a browser	Citrix Endpoint Management	

Open ports from the Internet to the DMZ:

TCP port	Description	Source IP	Destination	Destination IP
443	Citrix Endpoint Management Client Device		NetScaler Gateway IP	
443	Citrix Endpoint Management Client Device		NetScaler Gateway VIP	
443	Citrix Files Public IP	CTX208318	NetScaler Gateway VIP	

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Open ports from the DMZ to the internal network:

TCP port	Description	Source IP	Destination	Destination IP
389 or 636	NetScaler Gateway NSIP		Active Directory IP	
53 (UDP)	NetScaler Gateway NSIP		DNS Server IP	
443	NetScaler Gateway SNIP		Exchange (EAS) Server IP	
443	NetScaler Gateway SNIP		Internal Web Apps/Services	
443	NetScaler Gateway SNIP		Storage zones controller IP	

Open ports from the internal network to the DMZ:

TCP port	Description	Source IP	Destination	Destination IP
443	Admin Client		NetScaler Gateway NSIP	

Open ports from the internal network to the Internet:

TCP port	Description	Source IP	Destination	Destination IP
443	Exchange (EAS) Server IP		Citrix Endpoint Management Push Notification Listeners (1)	
443	Storage zones controller IP		Citrix Files Control Plane	CTX208318

(1)us-east-1.mailboxlistener.xm.citrix.com, eu-west-1.mailboxlistener.xm.citrix.com, ap-southeast-1.mailboxlistener.xm.citrix.com

Open ports from the corporate Wi-Fi to the Internet:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

TCP port	Description	Source IP	Destination	Destination IP
8443 / 443	Citrix Endpoint Management Client Device		Citrix Endpoint Management	
5223	Citrix Endpoint Management Client Device		Apple APNS Servers	17.0.0.0/8
5228	Citrix Endpoint Management Client Device		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
5229	Citrix Endpoint Management Client Device		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
5230	Citrix Endpoint Management Client Device		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
443	Citrix Endpoint Management Client Device		Firebase Cloud Messaging	fcm.googleapis.com
443	Citrix Endpoint Management Client Device		Windows Push Notification Service	*.notify.windows.com
443 / 80	Citrix Endpoint Management Client Device		Apple iTunes App Store	ax.apps.apple.com, *.mzstatic.com, vpp.itunes.apple.com

© 1997–2025 Citrix Systems, Inc. All rights reserved.

TCP port	Description	Source IP	Destination	Destination IP
443 / 80	Citrix Endpoint Management Client Device		Google Play	play.google.com, android.clients.google.com, android.l.google.com, android.com, google-analytics.com
443 / 80	Citrix Endpoint Management Client Device		Microsoft App Store	login.live.com, *.notify.windows.com
443	Citrix Endpoint Management Client Device		Citrix Endpoint Management AutoDiscovery service for iOS and Android	discovery.cem.cloud.us
443	Citrix Endpoint Management Client Device		Citrix Endpoint Management AutoDiscovery service for Windows	enterpriseenrollment.mycompany.com, discovery.cem.cloud.us
443	Storage zones controller IP		Citrix Files Control Plane	CTX208318
443	Citrix Endpoint Management Client Device		Google Mobile Management, Google APIs, Google Play Store APIs	*.googleapis.com

© 1997–2025 Citrix Systems, Inc. All rights reserved.

TCP port	Description	Source IP	Destination	Destination IP
443	Citrix Endpoint Management Client Device		Connectivity checks for CloudDPC versions earlier than v470. Android connectivity checks starting with N MR1 requires `https://www.google.com/generate_204` to be reachable, or for the given Wi-Fi network to point to a reachable PAC file)	`connectivitycheck.android.com`, `www.google.com`

Port requirement for AutoDiscovery service connectivity

This port configuration makes sure that Android devices connecting from Citrix Secure Hub for Android can access the Citrix Endpoint Management AutoDiscovery service (ADS) from within the internal network. The ability to access the ADS is important when downloading any security updates made available through the ADS.

> **Note:**
>
> ADS connections might not support your proxy server. In this scenario, allow the ADS connection to bypass the proxy server.

If you want to enable certificate pinning, complete the following prerequisites:

- **Collect Citrix Endpoint Management server and NetScaler Gateway 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're asked for your certificates.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Certificate pinning requires that devices connect to ADS before the device enrolls. This requirement makes sure that the latest security information is available to Citrix Secure Hub. For Citrix Secure Hub to enroll a device, the device must reach the ADS. So opening ADS access within the internal network is critical to enabling devices to enroll.

To allow access to the ADS for Citrix Secure Hub for Android/iOS, open port 443 for the following FQDN :

FQDN	Port	IP and port usage
`discovery.cem.cloud.us`	443	Citrix Secure Hub - ADS Communication via CloudFront

For information on supported IP addresses, see Cloud-based storage centers from AWS.

Android Enterprise network requirements

For information about the outbound connections to consider when setting up network environments for Android Enterprise, see the Google support article, Android Enterprise Network Requirements.

App requirements

Citrix Endpoint Management supports adding and maintaining up to 300 apps. Going over this limit causes your system to become unstable.

Citrix Endpoint Management compatibility

September 6, 2025

To use the new features, fixes, and policy updates, Citrix® recommends that you install the most recent version of the following:

- Citrix recommends that you integrate the Mobile Application Management (MAM) SDK with enterprise iOS and Android apps to apply MDX capabilities to the apps.

  The MDX Toolkit is scheduled to reach EOL in July 2023. To continue managing your enterprise apps, you must incorporate the MAM SDK.

- Mobile productivity apps

© 1997–2025 Citrix Systems, Inc. All rights reserved.

This article summarizes the versions of the supported Citrix Endpoint Management components that you can integrate.

The latest versions of Citrix Secure Hub, MDX Toolkit, and mobile productivity apps are compatible with the latest version and the two prior versions of Citrix Endpoint Management.

Mobile productivity apps

Users access the mobile productivity apps from the public app stores. The latest version of the mobile productivity apps requires the latest version of Citrix Secure Hub. The two previous versions of the apps are compatible with the latest Citrix Secure Hub.

For more information about the mobile productivity apps two-week phased release cadence, see Release timeline. For support details, see Support for mobile productivity apps.

MAM SDK

The MAM SDK provides MDX functionality that isn't covered by the iOS and Android platforms. You make those apps available in either an internal store or public app stores. See MDX App SDK.

MDX Toolkit

The MDX Toolkit is scheduled to reach EOL in July 2023. To continue managing your enterprise applications, you must incorporate the MAM SDK.

Citrix supports the latest three releases (n.n.n) of the MDX Toolkit. See What's new in the MDX Toolkit.

Browser support

The Citrix Endpoint Management console requires one of the following supported web browsers:

- Latest version of Google Chrome
- Latest version of Mozilla Firefox
- Latest version of Microsoft Edge
- Latest version of Apple Safari

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Supported device operating systems

September 6, 2025

This article covers supported devices for enterprise mobility management with Citrix Endpoint Management. Because of platform restrictions and security features, Citrix Endpoint Management doesn't support all functionality on all platforms.

For the latest versions of the mobile productivity apps, see Support for mobile productivity apps.

> **Note:**
>
> - Citrix supports the current and prior versions of each major operating system platform. Some Citrix Endpoint Management features don't work on older platform versions. For deprecation announcements, see Deprecation.
> - Citrix Endpoint Management™ supports device management for Windows x86 and ARM type devices.

Operating system support list

Citrix Endpoint Management supports the following operating systems:

- **Android:** 10.x, 11.x, 12.x, 13.x, 14.x, 15.x

  Citrix® recommends upgrading to Android 10+ before using Android Enterprise. For more information, see Android considerations.

- **iOS:** 13.x, 14.x, 15.x, 16.x, 17.x, 18.x

  Citrix Endpoint Management and Citrix mobile productivity apps don't currently support all the new features available for iOS 14.x, iOS 15.x, iOS 16.x, iOS 17.x and iOS 18.x.

- **iPadOS:** 13.x, 14.x, 15.x, 16.x, 17.x, 18.x

  Citrix Endpoint Management and Citrix mobile productivity apps don't currently support all the new features available for iPadOS 14.x, iPadOS 15.x, iPadOS 16.x, iPadOS 17.x, and iPadOS 18.x.

- **macOS:** 11.x, 12.x, 13.x, 14.x, 15x

  Citrix Endpoint Management and Citrix mobile productivity apps don't currently support all the new features available for macOS 11, macOS 12, macOS 13, macOS 14, and macOS 15.

- **Windows 10 and Windows 11 Desktops and Tablets:** (MDM only)

  - Windows 10 Professional and Windows 11 Professional
  - Windows 10 Enterprise and Windows 11 Enterprise
  - Windows 10 Education and Windows 11 Education

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Windows IoT Enterprise

Refer to Microsoft documentation for the level of support for a specific operating system.

Android considerations

Before upgrading to Android 10 or later: For information about how the deprecation of Google Device Administration APIs impacts devices running Android 10+, see Migrate from device administration to Android Enterprise. Also see this Citrix blog.

- Google deprecated Device Administration APIs, which impact devices running Android 10+. Enrollment of Android 10+ devices in legacy device administration mode fails. Citrix doesn't support enrolling Android devices in device administration mode.
- Citrix recommends using Android Enterprise for Android devices. For more information, see Migrate from device administration to Android Enterprise.
- The Google API change doesn't impact devices enrolled in MAM-only mode.
- Also see this Citrix blog.

Before upgrading:

- Make sure 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. Citrix only trusts certificates that have a SAN that matches the host name.

Language support

September 6, 2025

Citrix mobile productivity apps and the Citrix Endpoint Management console are adapted for use in languages other than English. The support includes non-English characters and keyboard input even when the app isn't localized in the preferred language of a user. For more information about globalization support for all Citrix products, see https://support.citrix.com/article/CTX119253.

This article lists the supported languages in the latest version of Citrix Endpoint Management.

Citrix Endpoint Management console and the Self-Help Portal

- French
- German

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Spanish
- Japanese
- Korean
- Portuguese
- Simplified Chinese

Citrix mobile productivity apps

An X indicates that the app is available in that particular language.

iOS and Android

Language	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
Japanese	X	X	X	X	X	X
Simplified Chinese	X	X	X	X	X	X
Traditional Chinese	X	X	X	X	X	X
French	X	X	X	X	X	X
German	X	X	X	X	X	X
Spanish	X	X	X	X	X	X
Korean	X	X	X	X	X	X
Portuguese	X	X	X	X	X	X
Dutch	X	X	X	X	X	X
Italian	X	X	X	X	X	X
Danish	X	X	X	X	X	X
Swedish	X	X	X	X	X	X
Hebrew	X	X	X	X	X	iOS only
Arabic	X	X	X	X	X	X
Russian	X	X	X	X	X	X
Turkish	X	X	Android only	-	-	-
Polish	X	X	X	-	-	-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Right-to-left language support

The following table summarizes support for text in Middle Eastern languages for each app. An X indicates that the feature is available for that platform. Right-to-left language support isn't available for Windows devices.

App	iOS	Android
Citrix Secure Hub	X	X
Citrix Secure Mail	X	X
Citrix Secure Web	X	X
QuickEdit	X	X

FIPS 140-2 compliance

September 6, 2025

The US National Institute of Standards and Technologies (NIST) issues the Federal Information Processing Standard (FIPS). FIPS specifies the security requirements for cryptographic modules used in security systems. FIPS 140-2 is the second version of this standard. For more information about NIST-validated FIPS 140 modules, see the NIST Computer Security Resource Center.

All data-at-rest and data-in-transit cryptographic operations on iOS use FIPS-validated cryptographic modules. On Android, all data-at-rest cryptographic operations use FIPS-validated cryptographic modules provided by Citrix® or the platform's crypto modules provided by the device manufacturer. Contact your Citrix representative for more information on the device manufacturer's modules.

All data-at-rest and data-in-transit cryptographic operations for Mobile Device Management (MDM) on supported Windows devices use FIPS-validated cryptographic modules.

All data-at-rest and data-in-transit cryptographic operations for Citrix Endpoint Management MDM use FIPS-validated cryptographic modules. All data-at-rest and data-in-transit for MDM flows use FIPS-compliant cryptographic modules end-to-end. That security includes the cryptographic operations described earlier for mobile devices, plus the cryptographic operations between mobile devices and NetScaler Gateway.

The MDX Vault encrypts MDX-wrapped apps and associated data-at-rest on both iOS and Android devices using FIPS-validated cryptographic modules.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

About Citrix Endpoint Management

September 6, 2025

Citrix Endpoint Management is a Unified Endpoint Management (UEM) solution that brings every app and endpoint into one unified view to increase security and improve productivity. For an overview of UEM, see the Citrix Tech Zone technical brief, Citrix Endpoint Management.

Citrix Endpoint Management provides Mobile Device Management (MDM) and Mobile App Management (MAM).

MDM features of Citrix Endpoint Management let you:

- Deploy device policies and apps.
- Retrieve asset inventories.
- Carry out actions on devices, such as a device wipe.

MAM features of Citrix Endpoint Management let you:

- Secure apps and data on BYO mobile devices.
- Deliver enterprise mobile apps.
- Lock the apps and wipe their data.

With a combination of MDM and MAM features, you can:

- Manage a corporate-issued device by using MDM
- Deploy device policies and apps
- Retrieve an asset inventory
- Wipe devices
- Deliver enterprise mobile apps
- Lock apps and wipe the data on devices

The following table summarizes the Citrix Endpoint Management features supported for MDM, MAM, or MDM+MAM.

Feature (by platform)	MDM (1)	MAM (2)	MDM+MAM
Android Enterprise:			
Device enrollment support	Yes	Yes	Yes
Domain authentication support	Yes	No	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Feature (by platform)	MDM (1)	MAM (2)	MDM+MAM
Domain plus security token authentication support	No	No	Yes
Client certificate authentication support	No	Yes	Yes
Client certificate plus domain authentication support	No	No	Yes
Client certificate plus security token support	No	No	Yes
Azure AD identity provider support	Yes	No	Yes
Okta identity provider support	Yes	No	Yes
Single sign on to native SaaS apps	Yes	No	Yes
Citrix Content Delivery Network support for enterprise apps	Yes	Yes	Yes
Citrix Content Delivery Network support for MDX apps	Yes	Yes	Yes
Shared device support by provisioning dedicated Android Enterprise (COSU) devices	Yes	No	Yes
Android (legacy):			
Device enrollment support	Yes	Yes	Yes
Domain or domain plus security token authentication support	No	No	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Feature (by platform)	MDM (1)	MAM (2)	MDM+MAM
Client certificate authentication support	No	Yes	Yes
Client certificate plus domain authentication support	No	No	Yes
Client certificate plus security token support	No	No	Yes
Azure AD and Citrix identity provider support	Yes	No	Yes
Okta identity provider support	Yes	No	Yes
Single sign on to native SaaS apps	Yes	No	Yes
Citrix Content Delivery Network support for enterprise apps	Yes	Yes	Yes
Citrix Content Delivery Network support for MDX apps	Yes	Yes	Yes
Chrome:			
Device enrollment support	Yes	No	Yes
User name and password authentication support	Yes	No	Yes
iOS:			
Device enrollment support	Yes	Yes	Yes
Domain or domain plus security token authentication support	No	No	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Feature (by platform)	MDM (1)	MAM (2)	MDM+MAM
Client certificate authentication support	No	Yes	Yes
Client certificate plus domain authentication support	No	No	Yes
Azure AD and Citrix identity provider support	Yes	No	Yes
Okta identity provider support	Yes	No	Yes
Single sign on to native SaaS apps	Yes	No	Yes
Citrix Content Delivery Network support for enterprise apps	Yes	Yes	Yes
Citrix Content Delivery Network support for MDX apps	Yes	Yes	Yes
Apple Education integration	Yes	No	Yes
macOS:			
Device enrollment support	Yes	No	No
Domain or domain plus one-time password support	Yes	No	No
Invitation URL plus one-time password support	Yes	No	No
Windows:			
Device enrollment support	Yes	No	No

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Feature (by platform)	MDM (1)	MAM (2)	MDM+MAM
Automatic enrollment of Windows 10 and Windows 11 devices through Citrix Workspace app	Yes	No	No
Domain or domain plus security token authentication support	Yes	No	No
Client certificate authentication support	Yes	No	No
Client certificate plus domain authentication support	Yes	No	No
Federated authentication through Azure AD or Citrix identity provider	Yes	No	No
Citrix Content Delivery Network support for enterprise apps	Yes	No	No
Workspace Environment Management™ integration (3)	Yes	No	No

> **Notes:**
>
> (1) Deployment ordering applies only to devices in a delivery group that has an enrollment profile configured for MDM.
>
> (2) MAM enrollment requires NetScaler Gateway.
>
> (3) Workspace Environment Management (WEM) integration provides access to MDM features on a wide spectrum of Windows operating systems.

For more information, see Management modes.

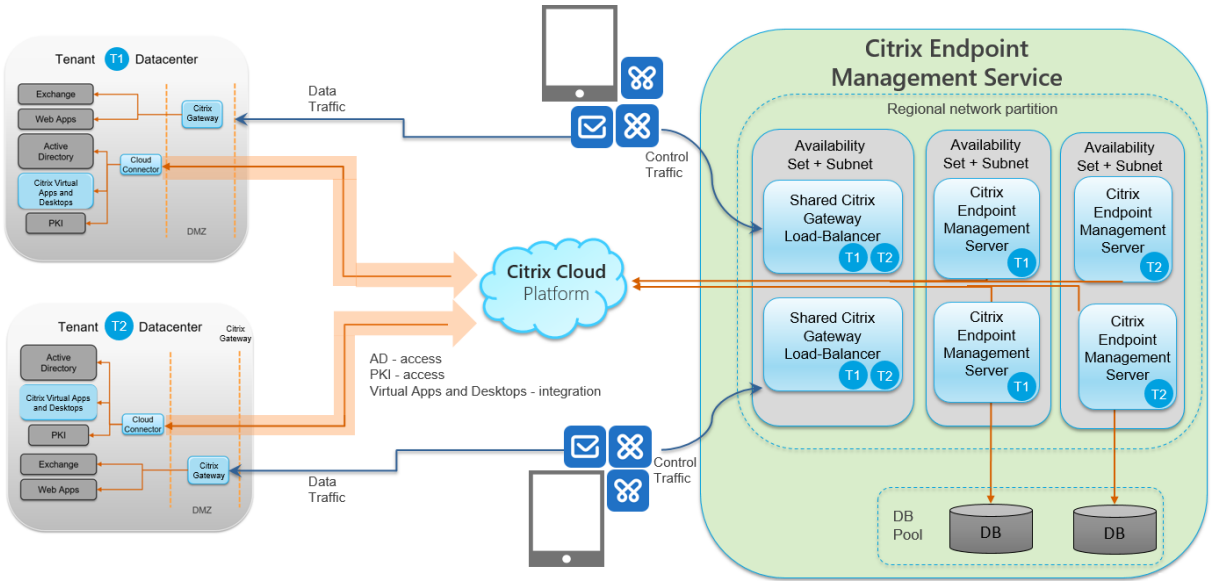
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Architecture

The device and app management requirements of your organization determine the Citrix Endpoint Management components in your Citrix Endpoint Management architecture. The components of Citrix Endpoint Management are modular and build on each other. For example, your deployment includes NetScaler Gateway:

- NetScaler Gateway gives users remote access to mobile apps and tracks user device types.
- Citrix Endpoint Management is where you manage those apps and devices.

The following diagram shows a general architectural overview of an Citrix Endpoint Management cloud deployment and its integration with your data center.



The following subsections have reference architecture diagrams for:

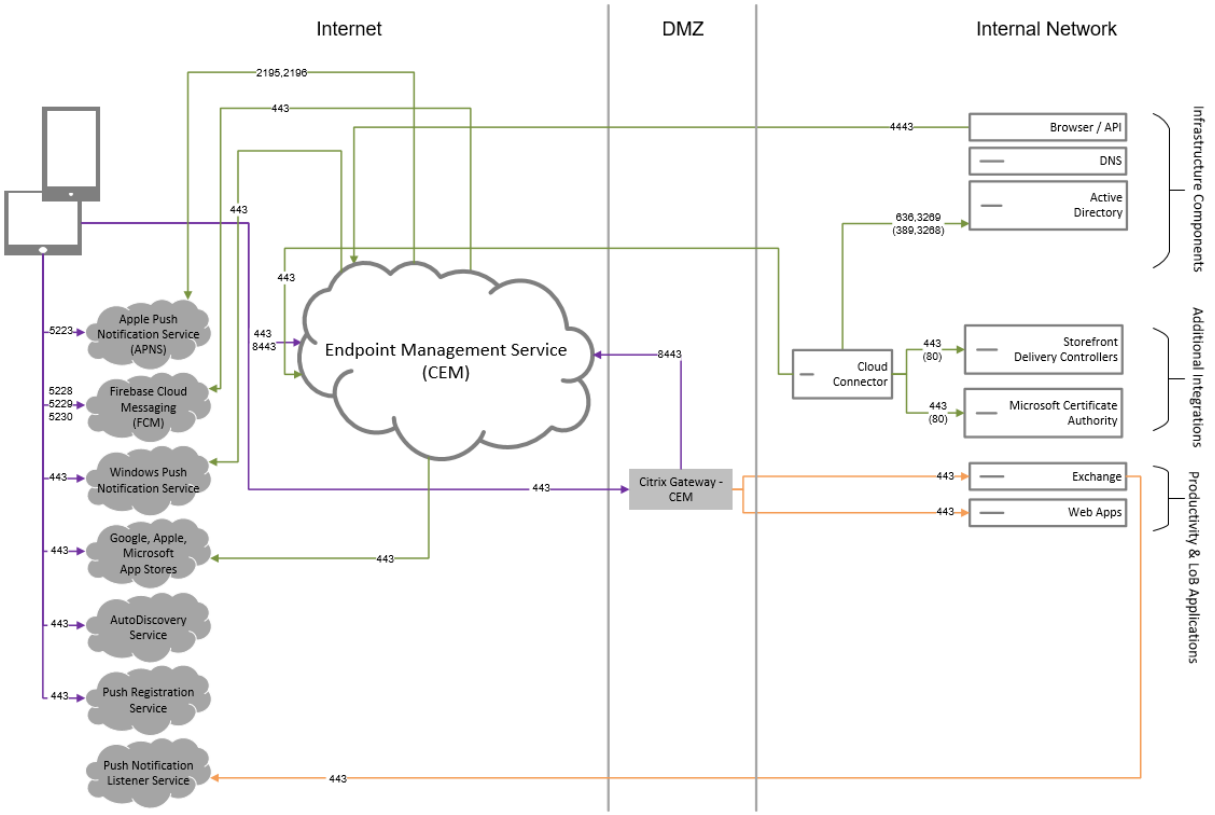
- Citrix Endpoint Management
- Optional components such as an external Certificate Authority, Citrix Endpoint Management connector for Exchange ActiveSync, and Citrix Endpoint Management MDM+MAM and Intune MAM traffic flow.

For more information about Citrix ADC and NetScaler Gateway requirements, see the Citrix product documentation at https://docs.citrix.com/.

Core reference architecture

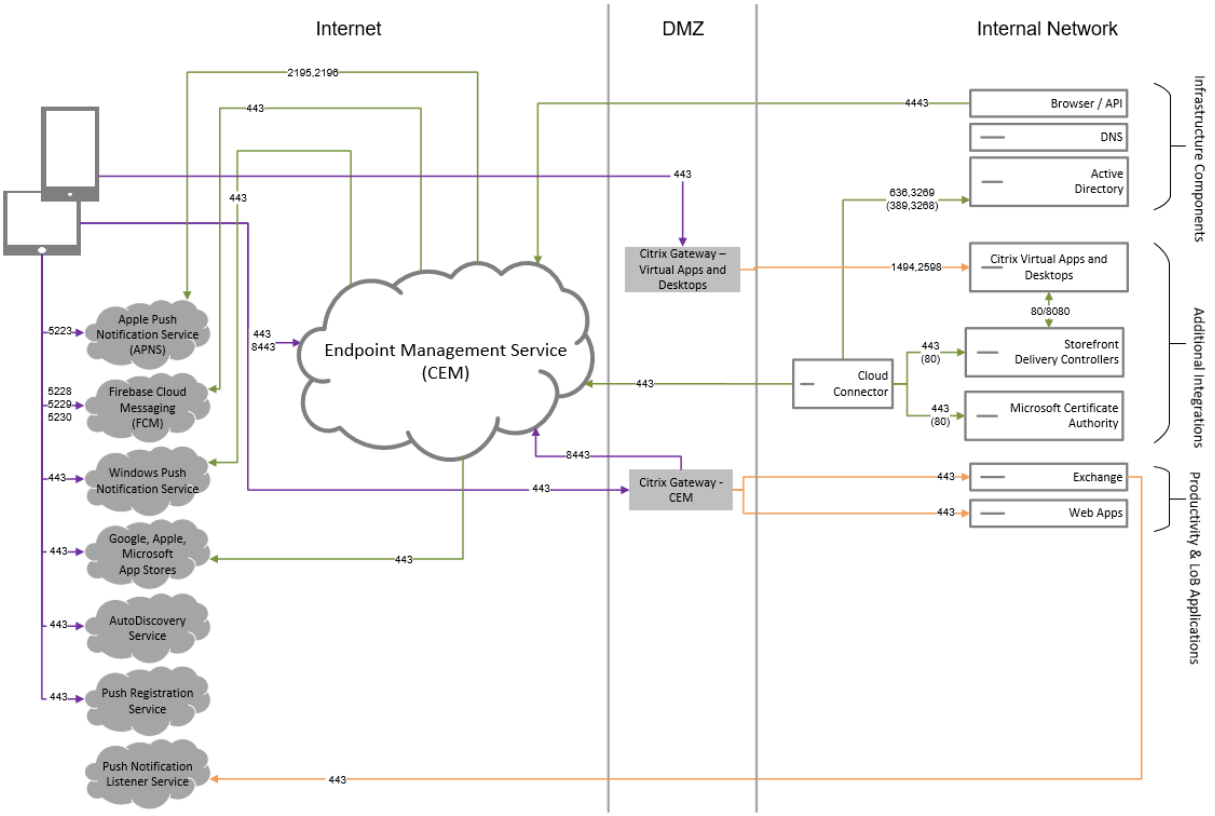
For details about port requirements, see System requirements.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



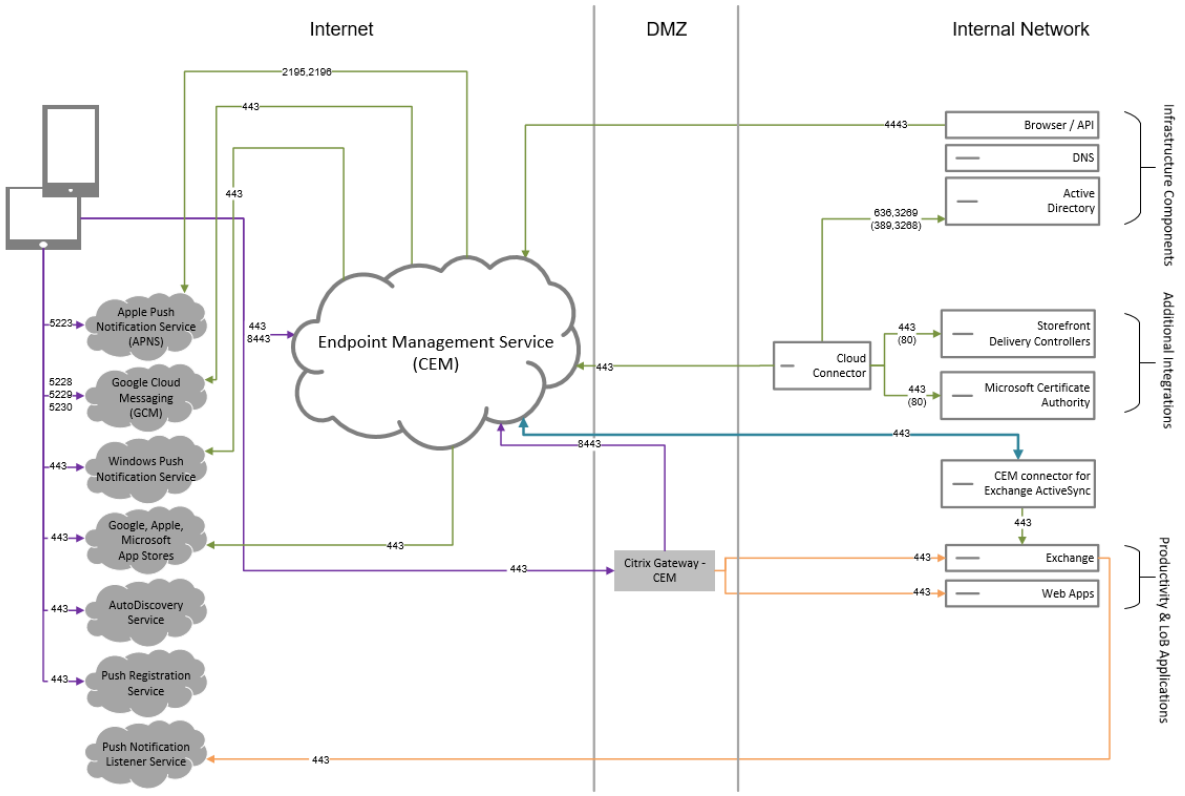
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Reference architecture with Citrix Virtual Apps and Desktops™



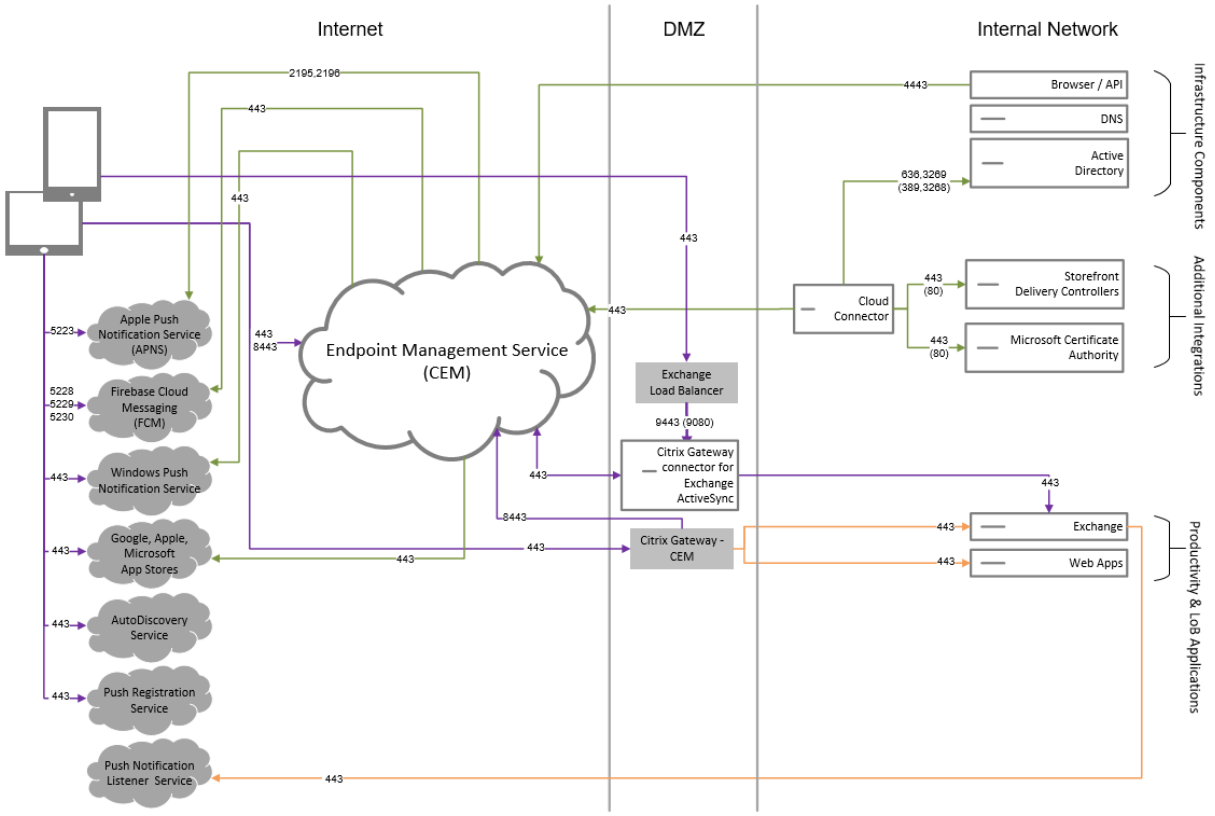
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Reference architecture with Citrix Endpoint Management connector for Exchange ActiveSync

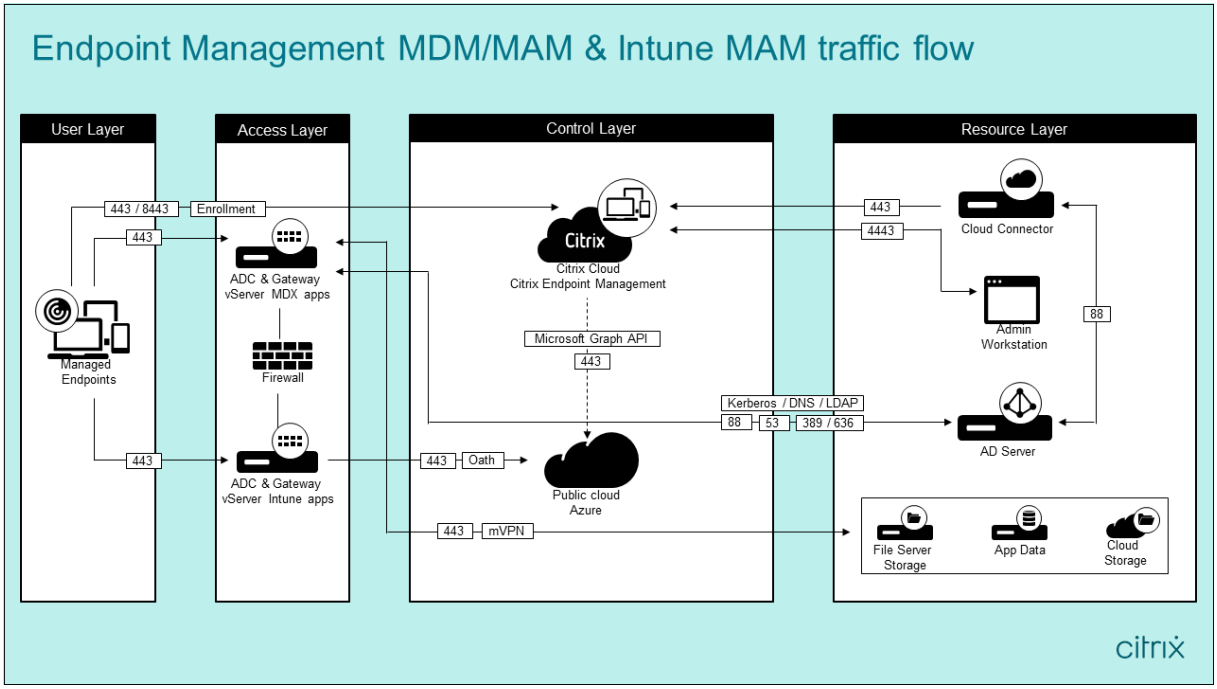


© 1997–2025 Citrix Systems, Inc. All rights reserved.

Reference architecture with NetScaler Gateway connector for Exchange ActiveSync



Reference architecture with Citrix Endpoint Management MDM+MAM and Intune MAM



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Resource locations

Place resource locations where they best meet your business needs. For example, in a public cloud, in a branch office, a private cloud, or a data center. Factors that determine the choice of location include:

- Proximity to subscribers
- Proximity to data
- Scale requirements
- Security attributes

You can build any number of resource locations. For example, you might:

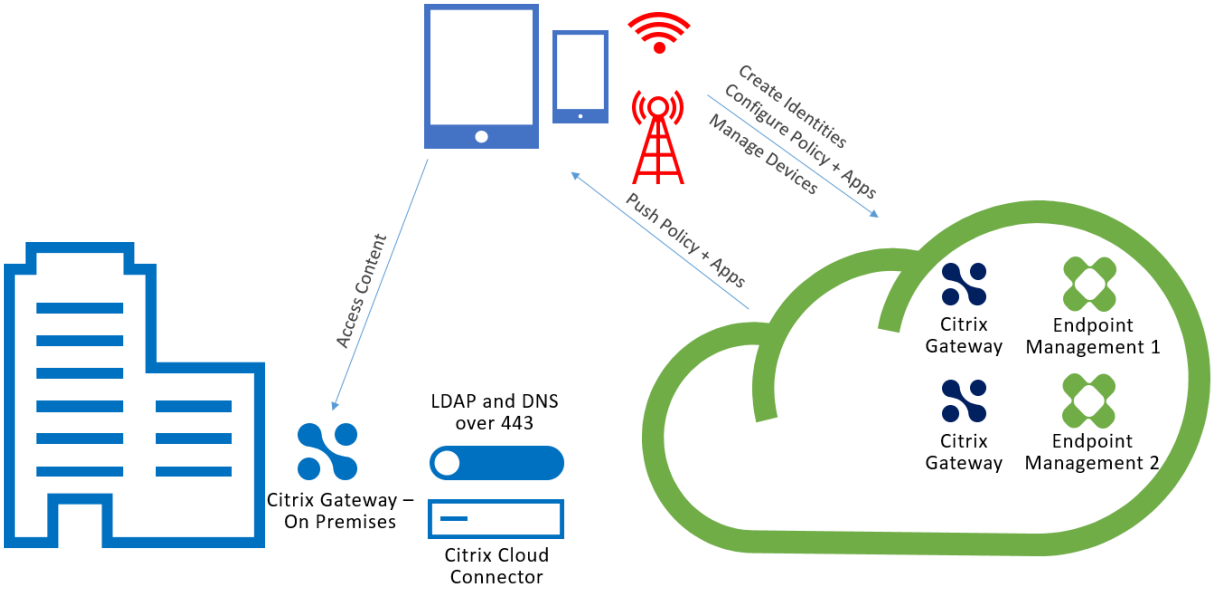
- Build a resource location in your data center for the head office, based on subscribers and applications that require proximity to the data.
- Add a separate resource location for your global users in a public cloud. Or, build separate resource locations in branch offices to provide the applications best served close to the branch workers.
- Add a further resource location on a separate network that provides restricted applications. This setup provides restricted visibility to other resources and subscribers without the need to adjust the other resource locations.

Cloud Connector

Cloud Connector authenticates and encrypts all communication between Citrix Cloud and your resource locations. Cloud Connector is required to access the following services: LDAP, IdPs, PKI Server, internal DNS queries, Citrix Virtual Apps, NetScaler Gateway, Citrix Workspace, and Microsoft Endpoint Manager.

The following diagram shows the traffic flow for Cloud Connector.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Cloud Connector establishes connections to Citrix Cloud. Cloud Connector doesn't accept incoming connections.

Cloud Connector is under load only during device enrollment. For more information, see Scale and size considerations for Cloud Connectors.

A solution that includes Mobile App Management (MAM) requires a micro VPN that is provided by an on-premises NetScaler Gateway. In this scenario:

- The following components are in your data center:
  - Cloud Connector
  - NetScaler Gateway
  - Your servers for Exchange, web apps, Active Directory, and PKI
- Mobile devices communicate with Citrix Endpoint Management and your on-premises NetScaler Gateway.

Citrix Endpoint Management components

Citrix Endpoint Management console. You use the Citrix Endpoint Management administrator console to configure Citrix Endpoint Management. For details about using the Citrix Endpoint Management console, see the articles under Citrix Endpoint Management. Citrix notifies you when the What's new articles for Citrix Endpoint Management are updated for a new release.

Note these differences between the Citrix Endpoint Management service and the on-premises releases:

- The Remote Support client is not available for Citrix Endpoint Management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Citrix does not support syslog integration in Citrix Endpoint Management with an on-premises syslog server. Instead, you can download the logs from the **Troubleshooting and Support** page in the Citrix Endpoint Management console. When doing so, you must click **Download All**.

MAM SDK. The MDX Toolkit is scheduled to reach EOL in July 2023. To continue managing your enterprise applications, you must incorporate the MAM SDK.

- The Mobile Application Management (MAM) SDK provides MDX functionality that isn't covered by the iOS and Android platforms. You can MDX-enable and secure iOS or Android apps. You make those apps available in either an internal store or public app stores. See MDX App SDK.

Mobile productivity apps. Citrix-developed mobile productivity apps provide a suite of productivity and communication tools within the Citrix Endpoint Management environment. Your company policies secure those apps. For more information, see Mobile productivity apps.

Citrix Endpoint Management connector for Exchange ActiveSync. Citrix Endpoint Management connector for Exchange ActiveSync provides secure email access to users who use native mobile email apps. The connector for Exchange ActiveSync provides ActiveSync filtering at the Exchange service level. As a result, filtering only occurs once the mail reaches the Exchange service, rather than when it enters the Citrix Endpoint Management environment. The connector doesn't require the use of NetScaler Gateway. You can deploy the connector without changing the routing for the existing ActiveSync traffic. For more information, see Citrix Endpoint Management connector for Exchange ActiveSync.

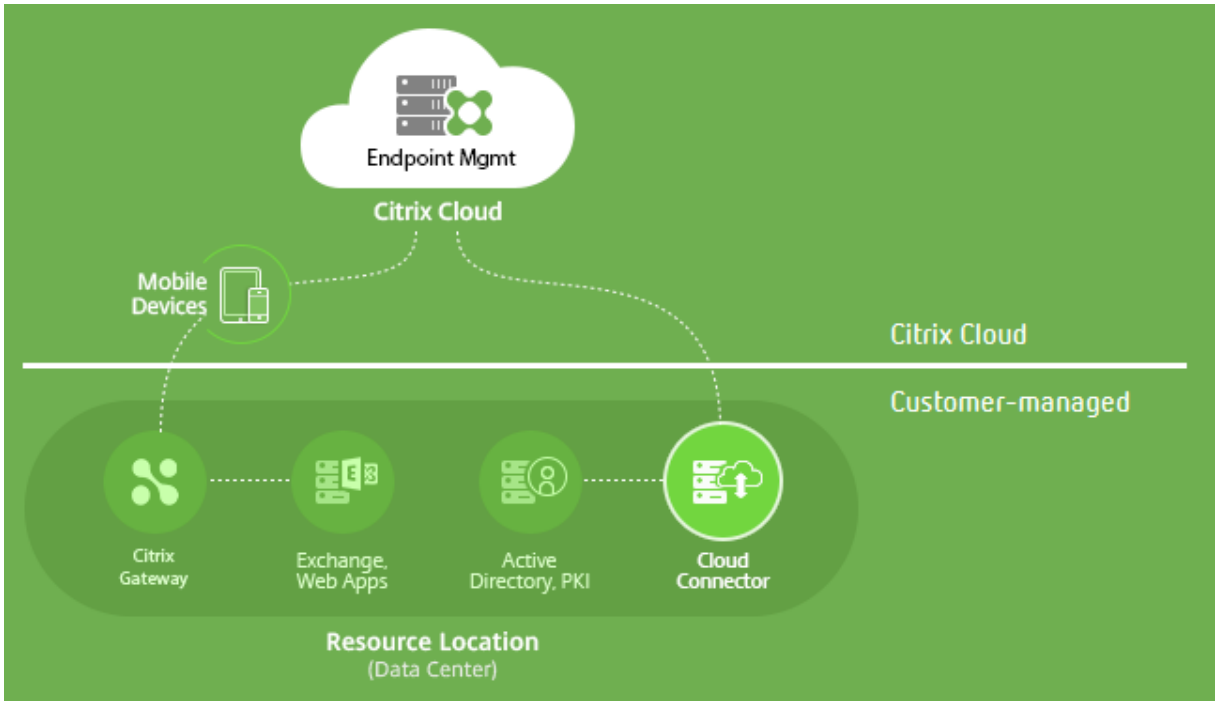
NetScaler Gateway connector for Exchange ActiveSync. NetScaler Gateway connector for Exchange ActiveSync provides secure email access to users who use native mobile email apps. The connector for Exchange ActiveSync provides ActiveSync filtering at the perimeter. The filtering uses NetScaler Gateway as a proxy for ActiveSync traffic. As a result, the filtering component sits in the path of mail traffic flow, intercepting mail as it enters or leaves the environment. The connector for Exchange ActiveSync acts an intermediary between NetScaler Gateway and Citrix Endpoint Management. For more information, see NetScaler Gateway connector for Exchange ActiveSync.

Citrix Endpoint Management technical security overview

Citrix Cloud manages the control plane for Citrix Endpoint Management environments. The control plane includes the Citrix Endpoint Management server, Citrix ADC load balancer, and a single-tenant database. The cloud service integrates with a customer data center using the Citrix Cloud Connector. Citrix Endpoint Management customers who use Cloud Connector typically manage NetScaler Gateway in their data centers.

The following figure illustrates the service and its security boundaries.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The information in this section:

- Provides an introduction to the security functionality of Citrix Cloud.
- Defines the division of responsibility between Citrix and customers for securing the Citrix Cloud deployment.
- Isn't the configuration or administration guidance for Citrix Cloud or any of its components or services.

For information about the technology used by Citrix Endpoint Management to deliver comprehensive, end-to-end security, see Security and Productivity for the Mobile Enterprise.

Data flow

The control plane has limited read access to user and group objects. Those objects are in your directory, DNS, and similar services. The control plane accesses those services over Citrix Cloud Connector through secure HTTPS connections.

Company data, such as email, intranet, and web-app traffic, flows directly between a device and the application servers over NetScaler Gateway. NetScaler Gateway is deployed in the customer data center.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Data isolation

The control plane stores metadata needed for managing user devices and their mobile applications. The service itself consists of a mix of multi- and single-tenant components. However, per the service architecture, customer metadata is always stored separately for each tenant and secured by using unique credentials.

Credential handling

The service handles the following types of credentials:

- **User credentials:** User credentials are transmitted from the device to the control plane over an HTTPS connection. The control plane validates these credentials with a directory in the customer directory over a secure connection.
- **Administrator credentials:** Administrators authenticate against Citrix Cloud, which uses the sign-on system from Citrix Online. This process generates a one-time signed JSON Web Token (JWT), which gives the administrator access to the service.
- **Active Directory credentials:** The control plane requires bind-credentials to read user metadata from the Active Directory. These credentials are encrypted using AES-256 encryption and saved in a per-tenant database.

Deployment considerations

Citrix recommends that you consult the published best practices documentation for deploying NetScaler Gateway within your environments.

More resources

Customers are advised to review security bulletins that relate to their Citrix products. For information on new and updated security bulletins, see Citrix Security Bulletins. Also consider signing up to receive alerts under your Alert Settings.

See the following resources for more security information:

- Citrix Security Site: https://www.citrix.com/security
- Citrix Cloud Documentation: Secure Deployment Guide for the Citrix Cloud Platform
- Secure Deployment Guide for Citrix ADC

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Integration with Mobile Threat Defense software

Mobile Threat Defense (MTD) software detects, analyzes, and helps prevent advanced cyberattacks against enterprise mobile devices. The combination of MTD and Unified Citrix Endpoint Management (UEM) increases security and visibility for your organization.

MTD software provides threat data that Citrix Endpoint Management uses to:

- Protect against malware, phishing, network attacks, and man-in-the-middle attacks
- Determine device compliance status
- Determine risk levels
- Take policy-based actions to protect your apps, data, devices, and mobile network

Citrix Endpoint Management integrates with the following MTD vendors:

- Check Point
- Lookout
- Wandera
- Zimperium

For more information or to request a demo, contact our MTD partners or your Citrix Sales Representative.

Citrix Endpoint Management integration with Microsoft Endpoint Manager

September 6, 2025

Citrix Endpoint Management integration with Microsoft Endpoint Manager (MEM) adds the value of Citrix Endpoint Management micro VPN to Microsoft Intune aware apps, such as the Microsoft Edge browser.

To activate the integration, contact the Citrix Cloud Operations team.

This release supports the following use cases:

- Intune MAM with Citrix Endpoint Management MDM+MAM.

  This article focuses on the Intune MAM + Citrix Endpoint Management MDM+MAM use case. After you add Citrix as your MDM provider, configure Intune managed apps for delivery to devices.

  > **Important:**
  >
  > - For this use case, Citrix Secure Mail doesn't support integration with Intune.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

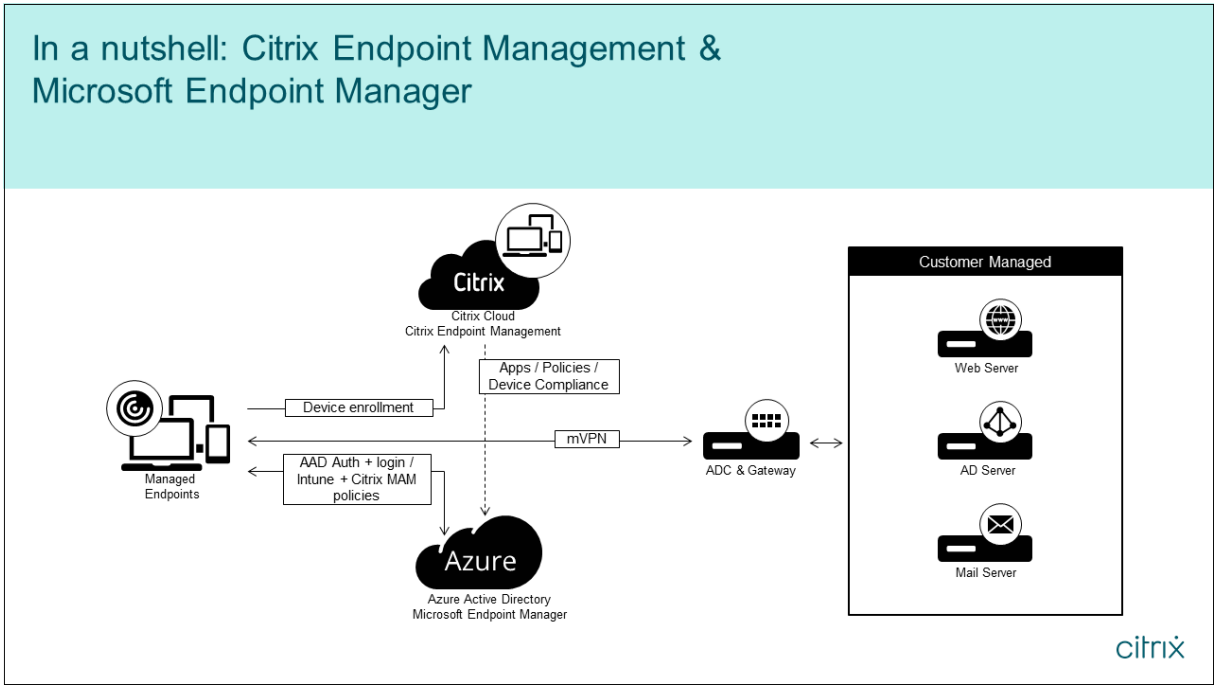
> – The Citrix Secure Mail integration with Intune is deprecated and will be removed in a future release. Refer to What's new in Secure Mail for more details.

- Intune MAM and Citrix Endpoint Management MDM.
- Intune MAM.
- Intune MAM and Intune MDM. Citrix Secure Mail for iOS supports single sign-on for this use case.

For an easy-to-follow, graphical guide to setting up Citrix Endpoint Management integration with MEM, see Getting Started Guide.

For information on integrating with Azure AD Conditional Access, see Integrate with Azure AD Conditional Access.

The following diagram provides an overview of Citrix Endpoint Management integration with Microsoft Endpoint Manager.



System requirements

MDX-enable

- MAM SDK

  or

- MDX Toolkit

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Microsoft

- Azure Active Directory (AD) access (with Tenant Admin privileges)
- Intune-enabled tenant

Firewall rule

- Enable a firewall rule to allow DNS and SSL traffic from a NetScaler Gateway subnet IP to `*.manage.microsoft.com`, `https://login.microsoftonline.com`, and `https://graph.windows.net` (port 53 and 443)

Prerequisites

- **Microsoft Edge browser:** The Mobile Apps SDK is integrated within the Microsoft Edge browser app for iOS and Android. For more information about Microsoft Edge, see the Microsoft Edge documentation.
- **Citrix Cloud account:** To sign-up for a Citrix account and request a Citrix Endpoint Management trial, contact your Citrix Sales Representative. When you're ready to continue, go to https://onboarding.cloud.com. For more information on requesting a Citrix Cloud account, see Sign-up for Citrix Cloud.

  > **Note:**
  >
  > The email you supply must be an address that is not associated with Azure AD. You can use any free email service.

- **APNs certificates for iOS:** Ensure that you configure APNs certificate for iOS. To learn more about setting up these certificates, see this Citrix blog post: Creating and Importing APNs Certificates.
- **Azure AD sync:** Set up synchronization between Azure AD and on-premises Active Directory. Do not install the AD sync tool on the domain controller machine. For more information on setting up this sync, see the Microsoft documentation on Azure Active Directory.

Configuring NetScaler Gateway

If you're setting up a new Citrix Endpoint Management deployment, install one of these NetScaler Gateway appliances:

- NetScaler® Gateway VPX 3000 series or greater
- NetScaler Gateway MPX or dedicated SDX instance

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To use NetScaler Gateway with Citrix Endpoint Management integration with MEM:

- Configure NetScaler Gateway with a management interface and a subnet IP.
- Use TLS 1.2 for all client to server communication. For information about configuring TLS 1.2 for NetScaler Gateway, see CTX247095.

If you're using Citrix Endpoint Management integration with MEM with an Citrix Endpoint Management MDM+MAM deployment, configure two Citrix Gateways. MDX app traffic is routed through one NetScaler Gateway. Intune app traffic is routed through the other NetScaler Gateway. Configure:

- Two public IPs.
- Optionally, one network address translated IP.
- Two DNS names. Example: `https://mam.company.com`.
- Two public SSL certificates. Configure certificates that match the reserved public DNS name or use wildcard certificates.
- A MAM load balancer with an internal non-routable RFC 1918 IP address.
- An LDAP Active Directory service account.

Consenting to delegated permission prompts

For managed apps that require users to authenticate, the apps request application permissions exposed by Microsoft Graph. By consenting to these permission prompts, the app can access the required resources and APIs. Some apps require consent by the global administrator for Microsoft Azure AD. For these delegated permissions, the global administrator must grant Citrix Cloud permission to request tokens. The tokens then enable the following permissions. For more information, see Microsoft Graph permissions reference.

- **Sign in and read user profile:** This permission allows users to sign in and connect to Azure AD. Citrix® can't view user credentials.
- **Read all users'basic profiles:** The app reads profile properties for users in the organization. The properties include the display name, first and last name, and email address and photo of users in the organization.
- **Read all groups:** This permission enables Azure AD groups to be specified for app and policy assignment.
- **Access directory as the signed-in user:** This permission verifies the Intune subscription and enables NetScaler Gateway and VPN configurations.
- **Read and write Microsoft Intune apps:** The app can read and write the following:
  - Microsoft-managed properties
  - Group assignments and the status of apps

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- App configurations
- App protection policies

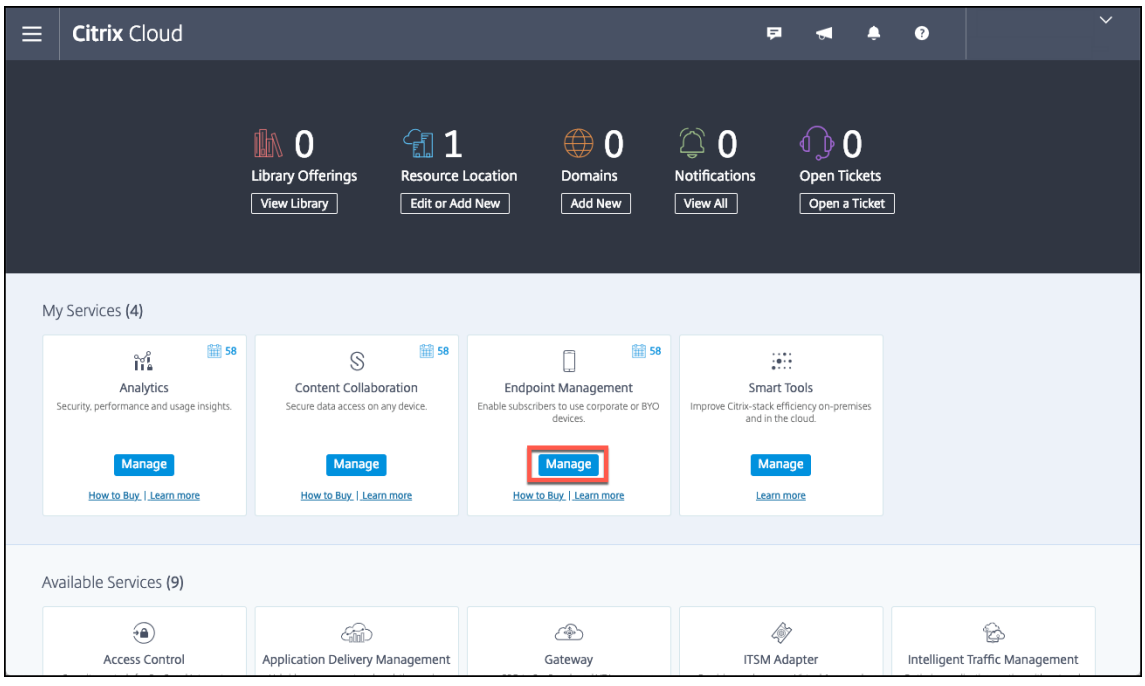
Also, during the NetScaler Gateway configuration, the Azure AD global administrator must:

- Approve the Active Directory chosen for micro VPN. The global administrator must also generate a client secret that NetScaler Gateway uses to communicate with Azure AD and Intune.
- Not have the role of Citrix administrator. Instead, the Citrix administrator assigns Azure AD accounts to users with appropriate Intune application admin privileges. The Intune administrator then serves the role of a Citrix Cloud admin to manage Intune from within Citrix Cloud.

> **Note:**
>
> Citrix only uses the Intune Global Administrator password during setup and redirects the authentication to Microsoft. Citrix can't access the password.

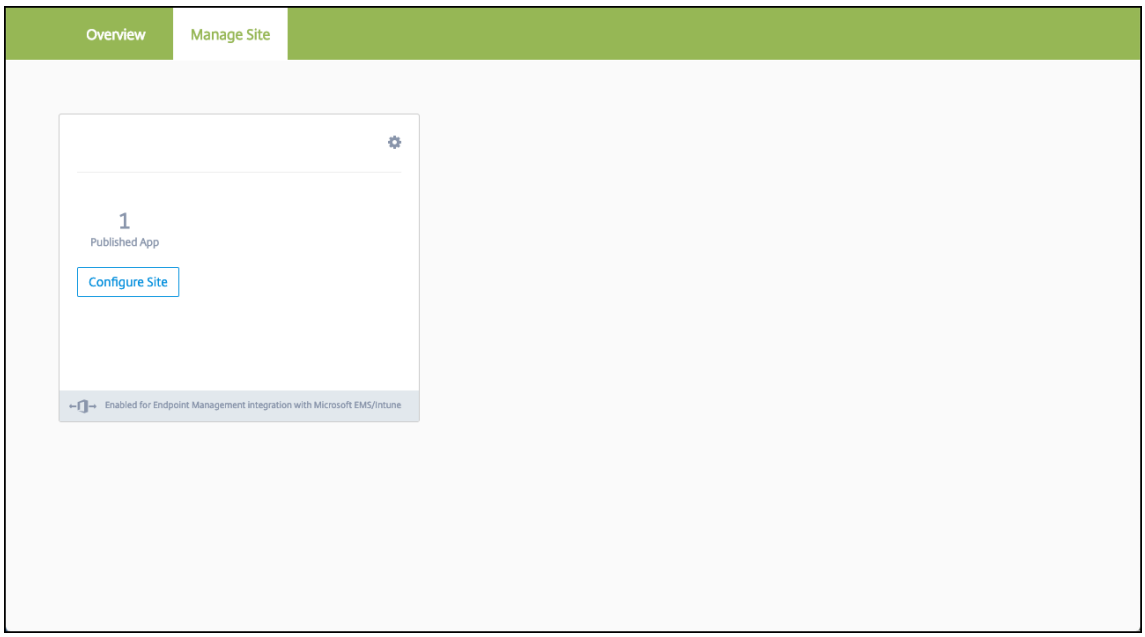
To configure Citrix Endpoint Management integration with MEM

1. Log on to the Citrix Cloud site and request a trial for Citrix Endpoint Management.
2. A sales engineer schedules an onboarding meeting with you. Let them know that you want Citrix Endpoint Management integration with MEM. When your request is approved, click **Manage**.

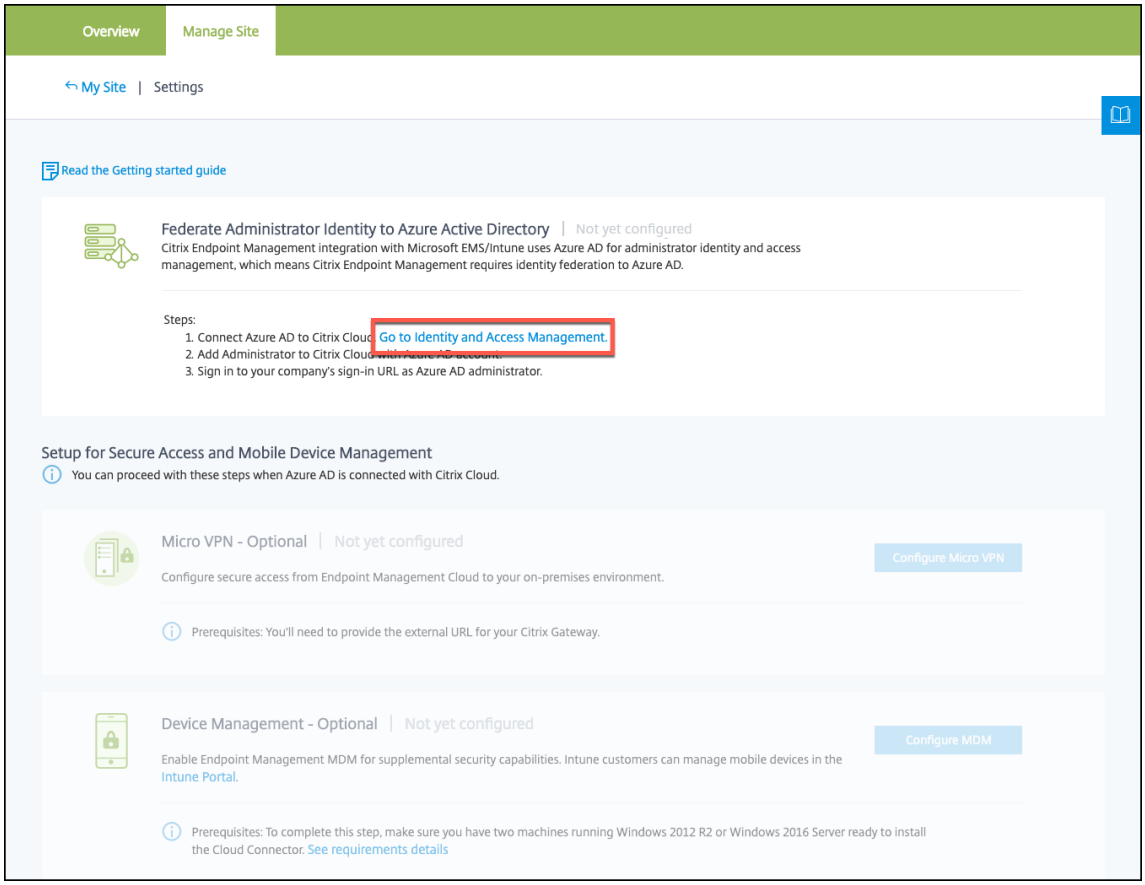


3. From here you can click the cog in the upper right of your site or you can click **Configure Site**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

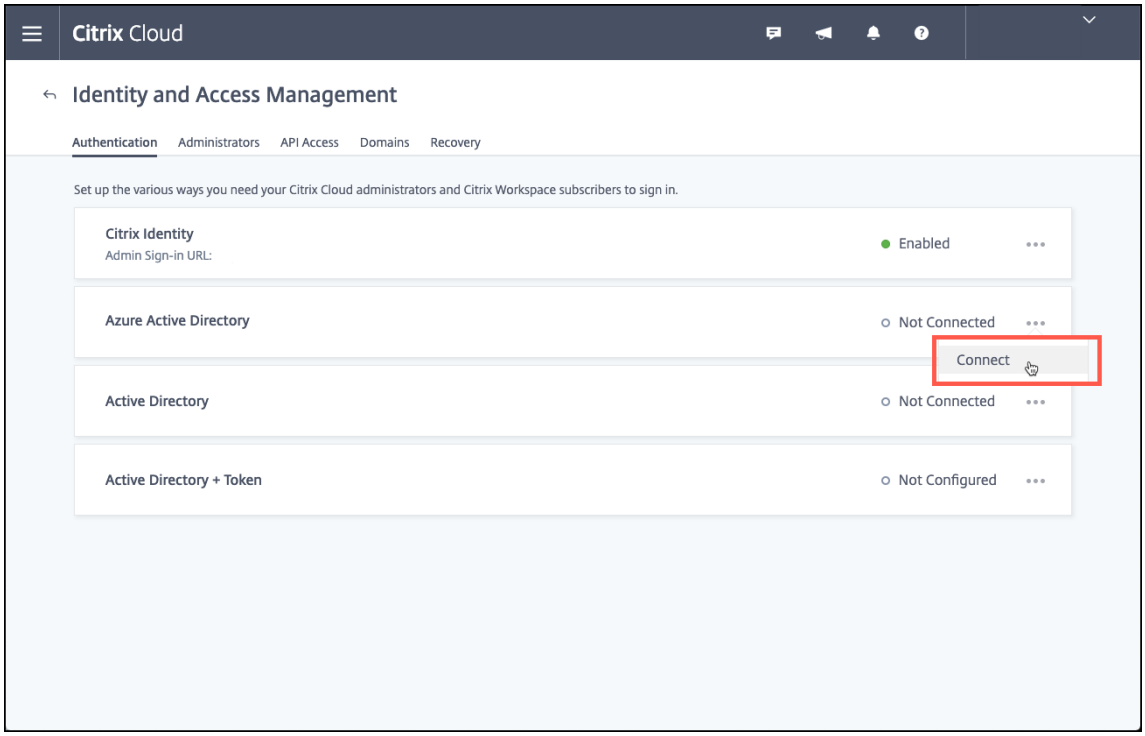


4. Follow the link in the first step to the **Identity and Access Management** page.

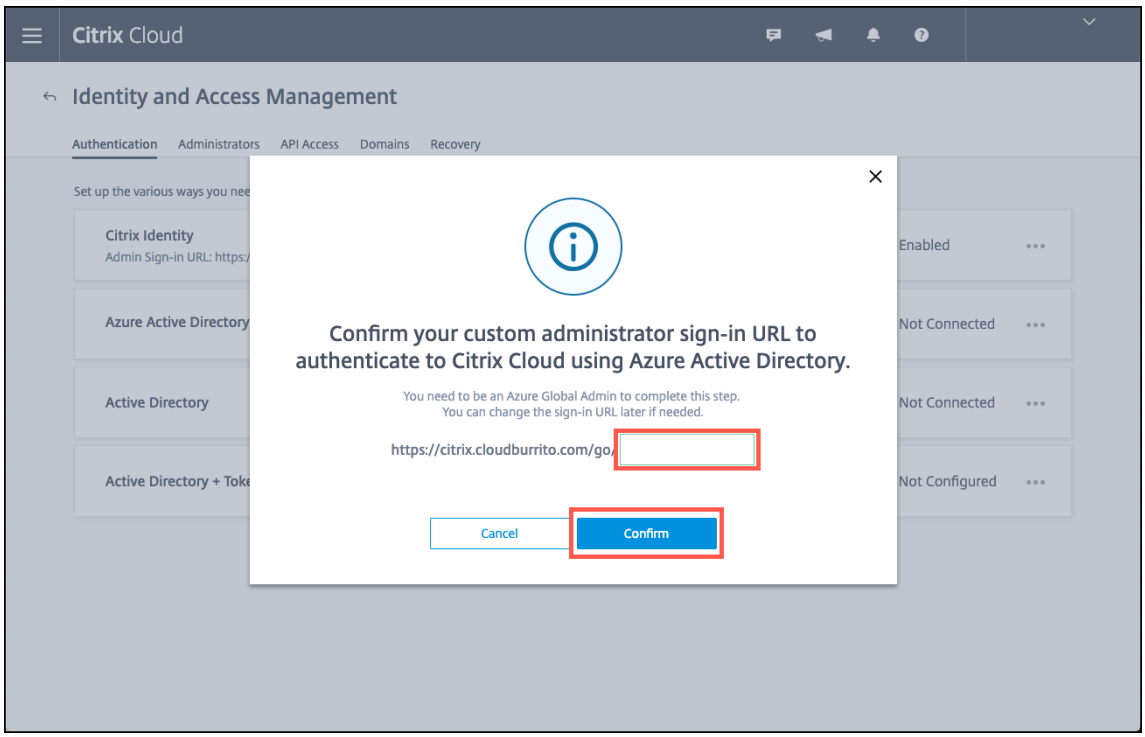


5. Click **Connect** to connect your Azure AD installation.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

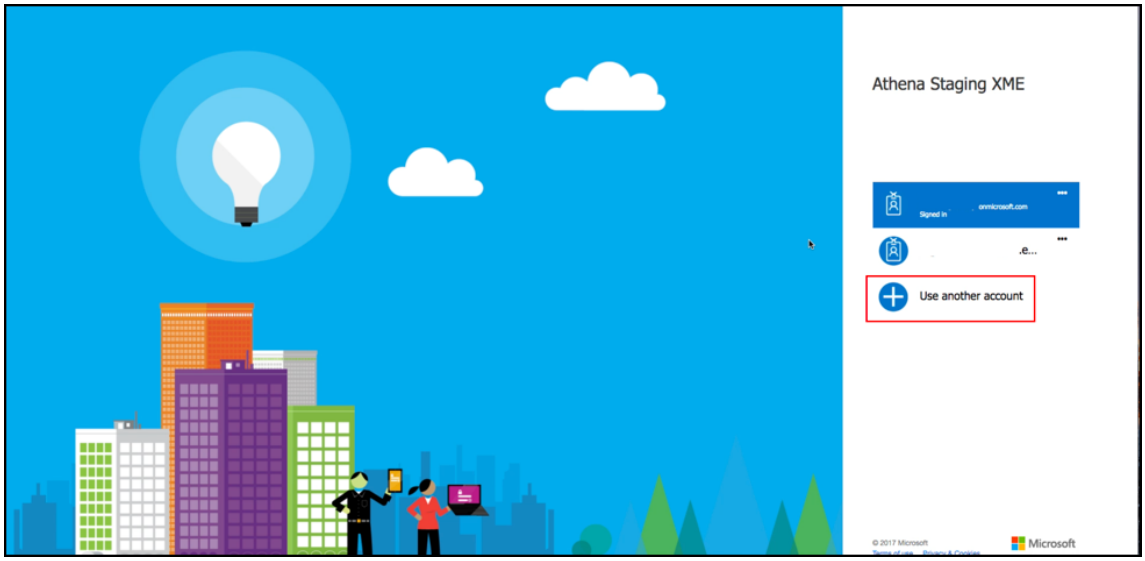


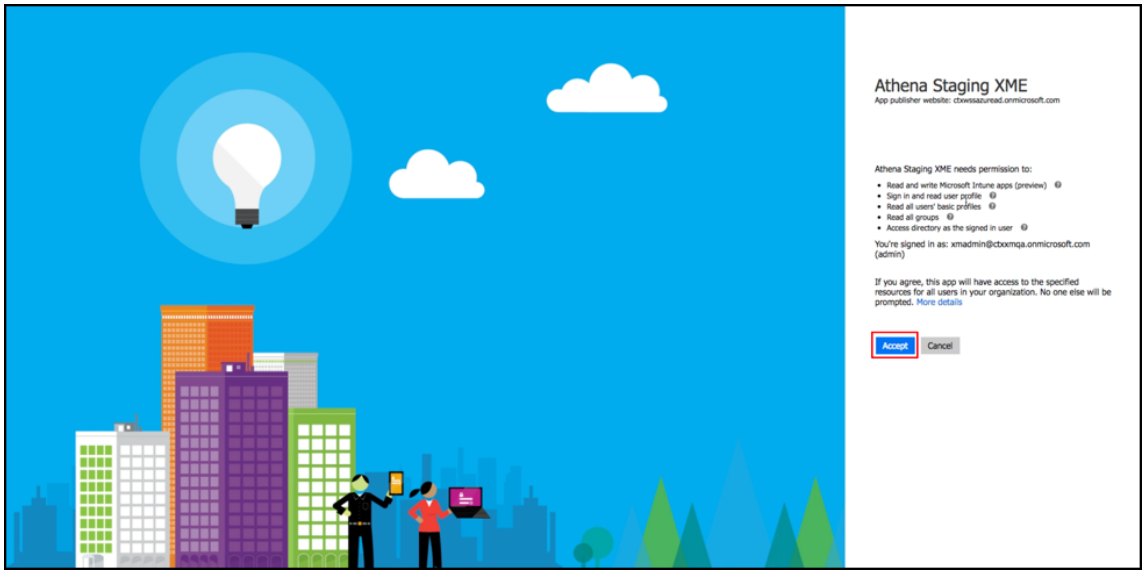
6. Enter a unique logon URL that the Azure AD administrator uses to log on and then click **Confirm**.



7. Add an Azure AD global administrator account and then accept the permission request.

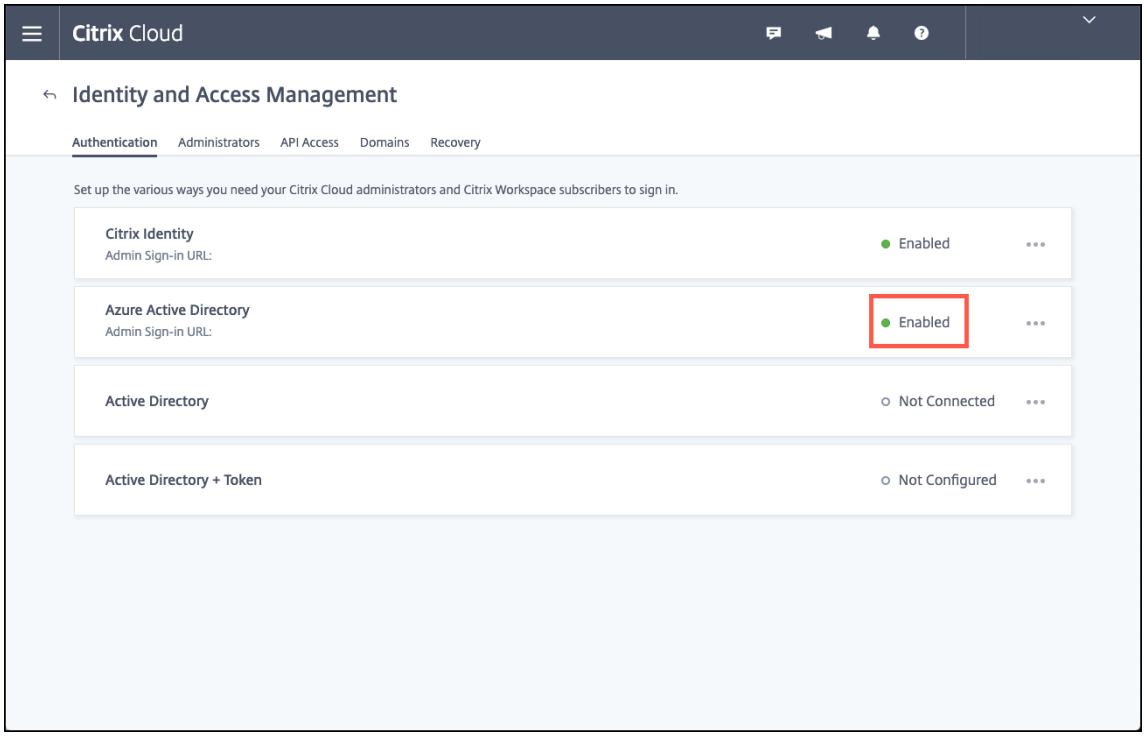
© 1997–2025 Citrix Systems, Inc. All rights reserved.





8. Confirm that your Azure AD instance connects successfully. To indicate a successful connection, the **Not Connected** text changes to say **Enabled**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



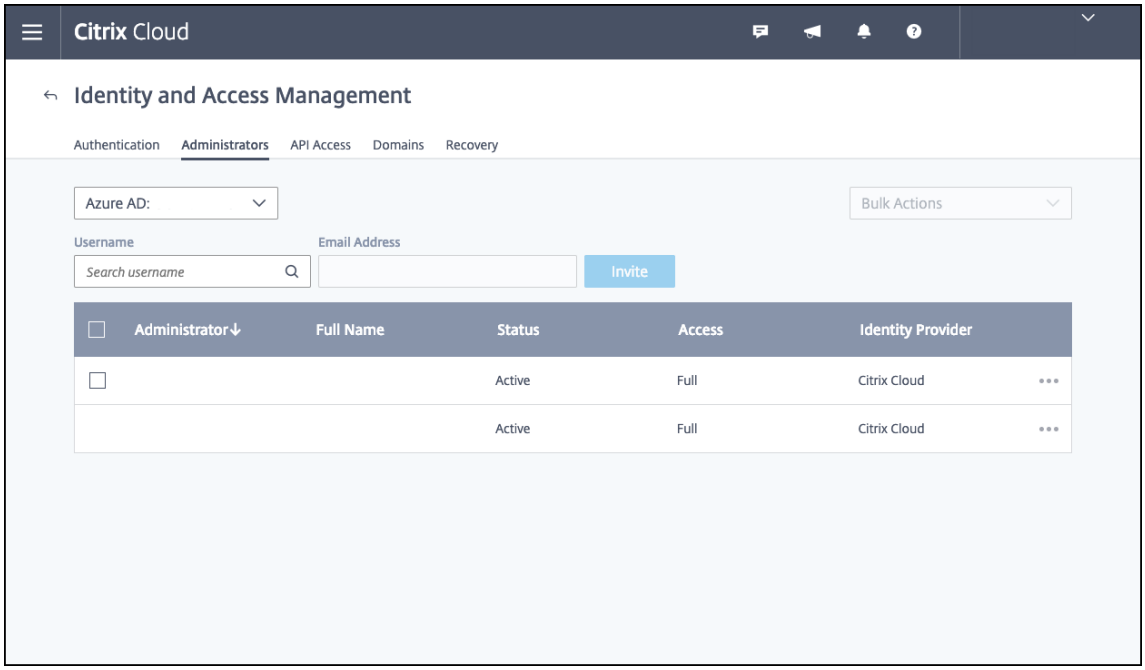
9. Click the **Administrators** tab and then add your Azure AD Intune administrator as a Citrix Cloud administrator. Select Azure AD or Citrix Identity from the drop-down menu, and then search for the user name you want to add. Click **Invite** and then grant the user **Full Access** or **Custom Access** before clicking **Send Invite**.

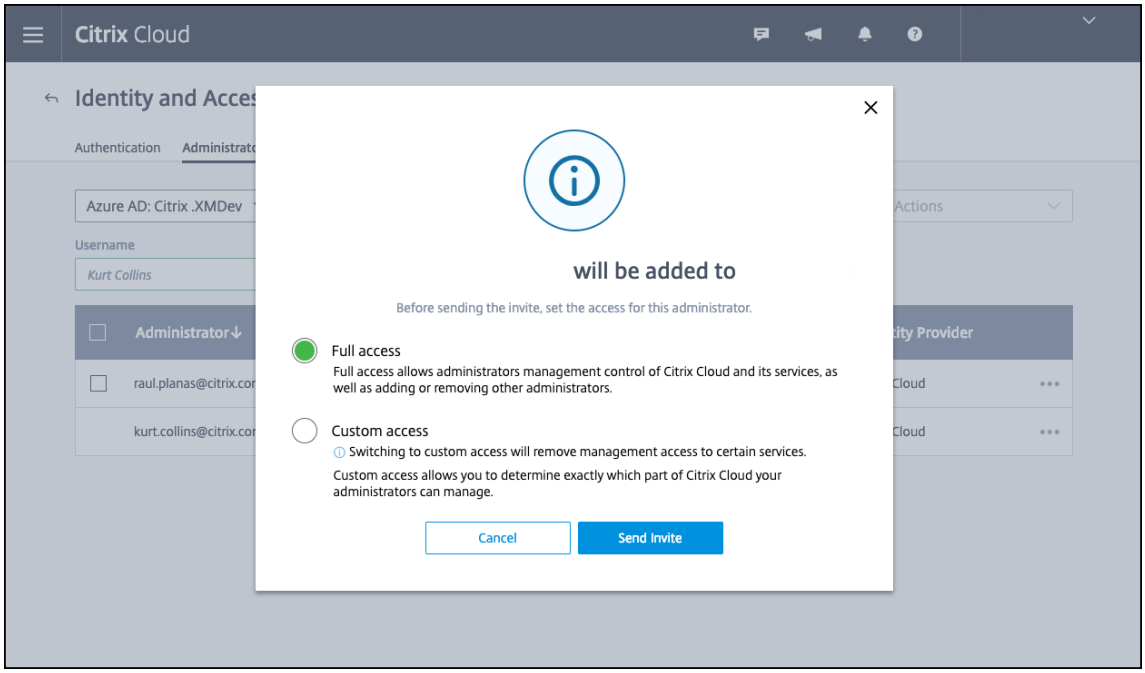
   > **Note:**
   >
   > Citrix Endpoint Management requires the following rules for **Custom Access:** Library and Citrix Endpoint Management.

   As a result, the Azure AD Intune administrator receives an email invitation to create a password and sign in to Citrix Cloud. Before the administrator signs in, make sure that you sign out of all other accounts.

   The Azure AD Intune administrator must follow the remaining steps in this procedure.

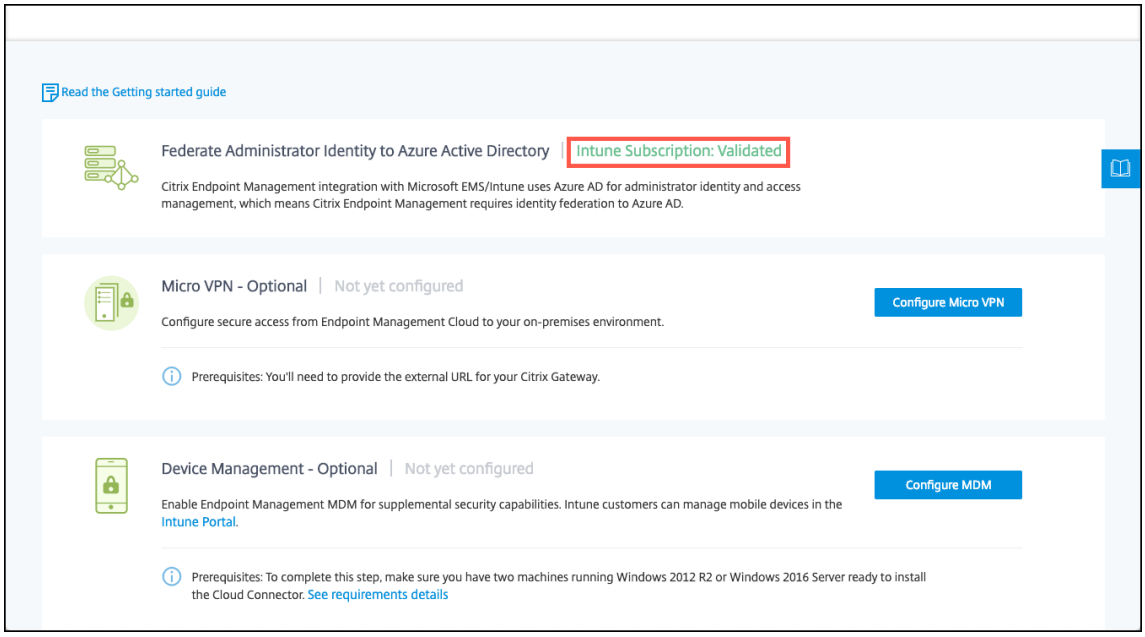
© 1997–2025 Citrix Systems, Inc. All rights reserved.





10. After signing in with the new account, under **Citrix Endpoint Management**, click **Manage**. If you configure everything correctly, the page shows that the Azure AD administrator is signed in and that your Intune subscription is valid.

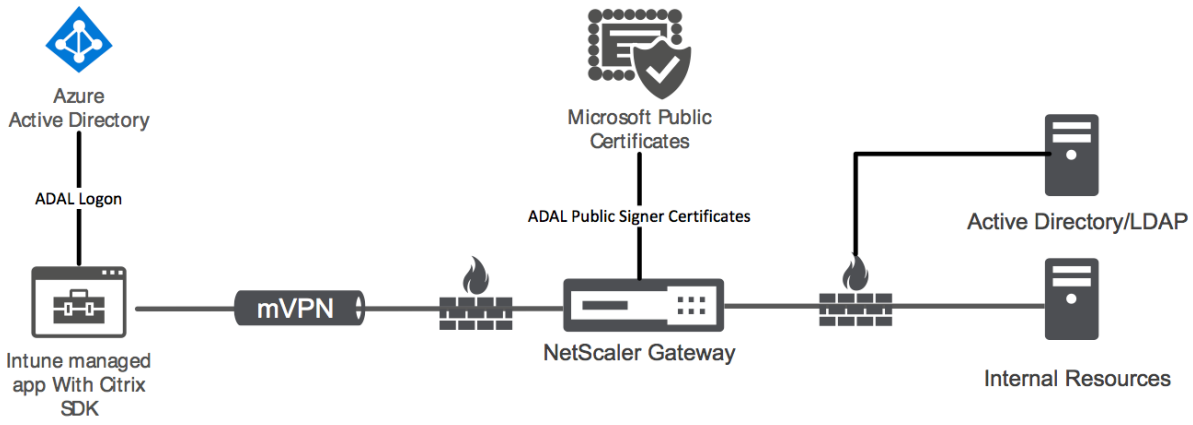
© 1997–2025 Citrix Systems, Inc. All rights reserved.



To configure NetScaler Gateway for micro VPN

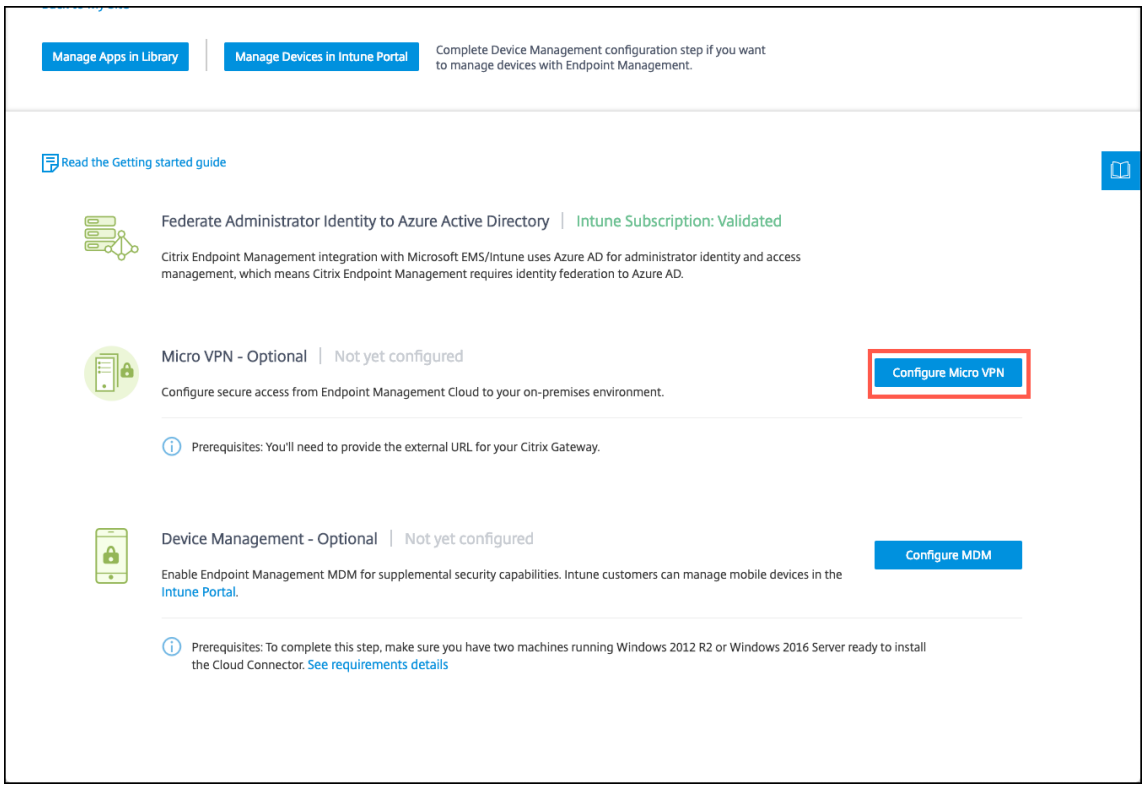
To use micro VPN with Intune, you must configure NetScaler Gateway to authenticate to Azure AD. An existing NetScaler Gateway virtual server does not work for this use case.

First, configure Azure AD to sync with the on-premises Active Directory. This step is necessary to make sure that authentication between Intune and NetScaler Gateway occurs properly.



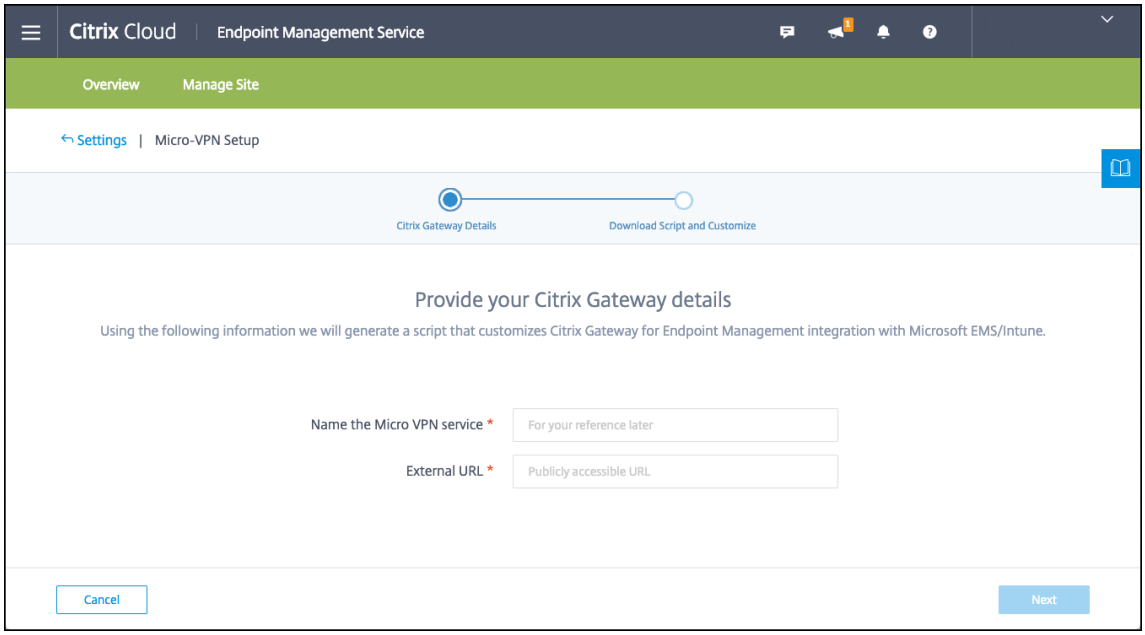
1. From the Citrix Cloud console, under **Citrix Endpoint Management**, click **Manage**.
2. Next to **Micro VPN**, click **Configure Micro VPN**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Enter a name for the micro VPN service and the external URL for your NetScaler Gateway and then click **Next**.

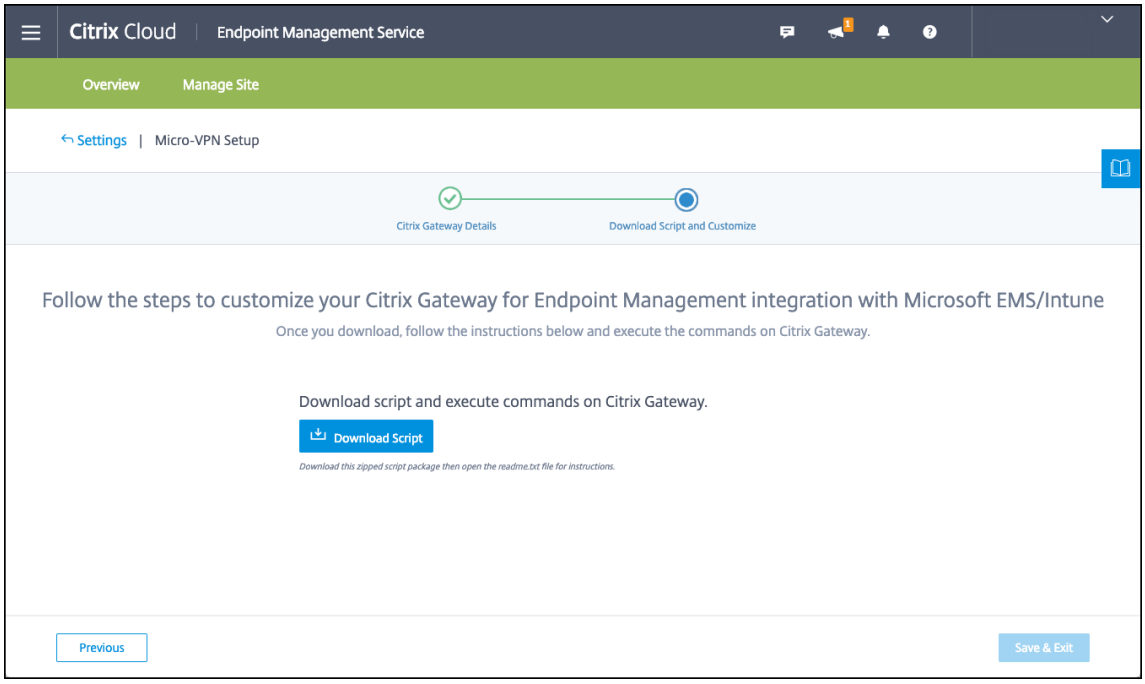
   This script configures NetScaler Gateway to support Azure AD and the Intune apps.



4. Click **Download Script**. The .zip file includes a readme with instructions for implementing the script. Even though you can Save and Exit from here, the Micro VPN isn't set up until you run

© 1997–2025 Citrix Systems, Inc. All rights reserved.

the script on your NetScaler Gateway installation.



> **Note:**
>
> When you finish the NetScaler Gateway configuration process, if you see an OAuth Status other than COMPLETE, see the Troubleshooting section.

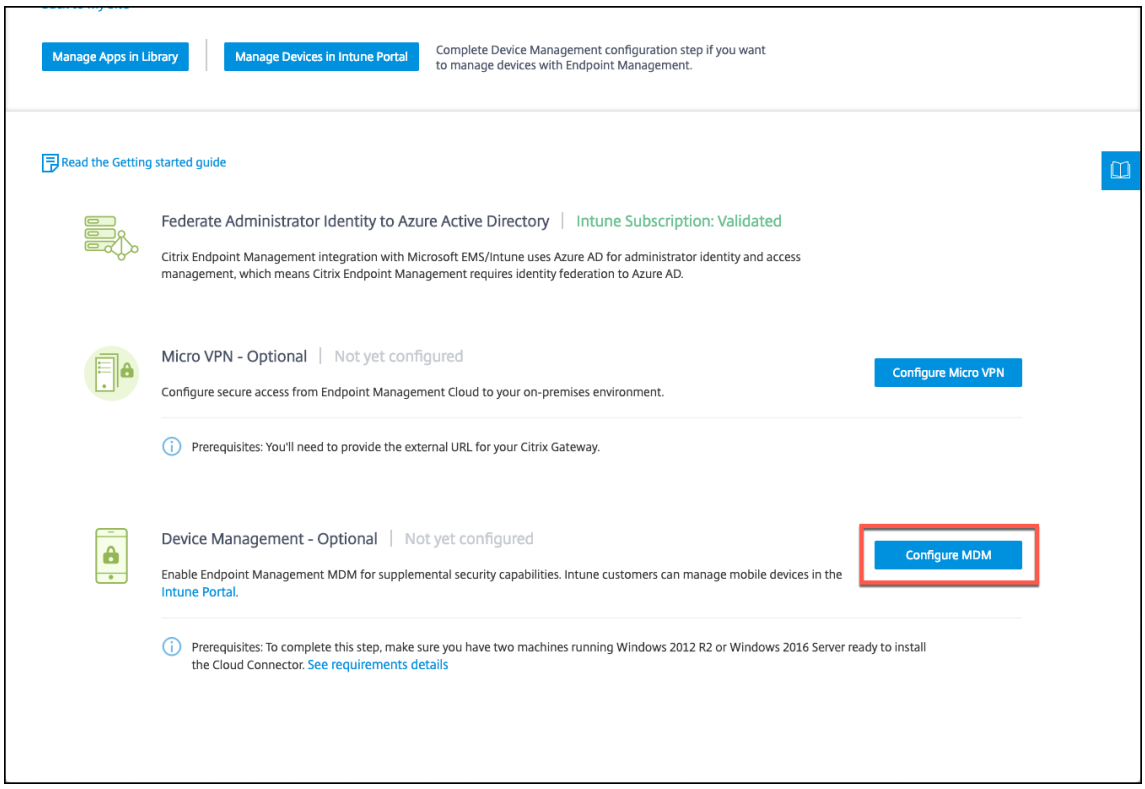
To configure device management

If you want to manage devices in addition to apps, choose a method of device management. You can use Citrix Endpoint Management MDM+MAM or Intune MDM.

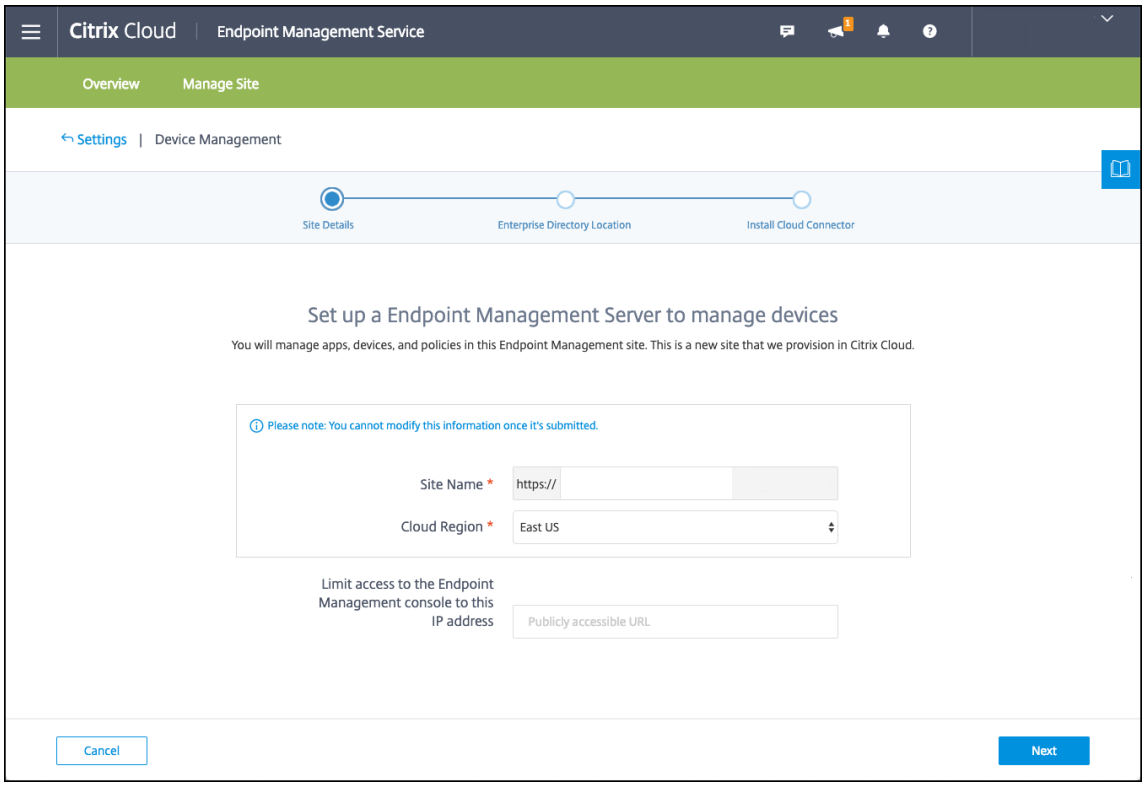
> **Note:**
>
> The console defaults to Intune MDM. To use Intune as your MDM provider, see the Microsoft Intune documentation.

1. From the Citrix Cloud console, under Citrix Endpoint Management integration with MEM, click **Manage**. Next to **Device Management - Optional**, click **Configure MDM**.

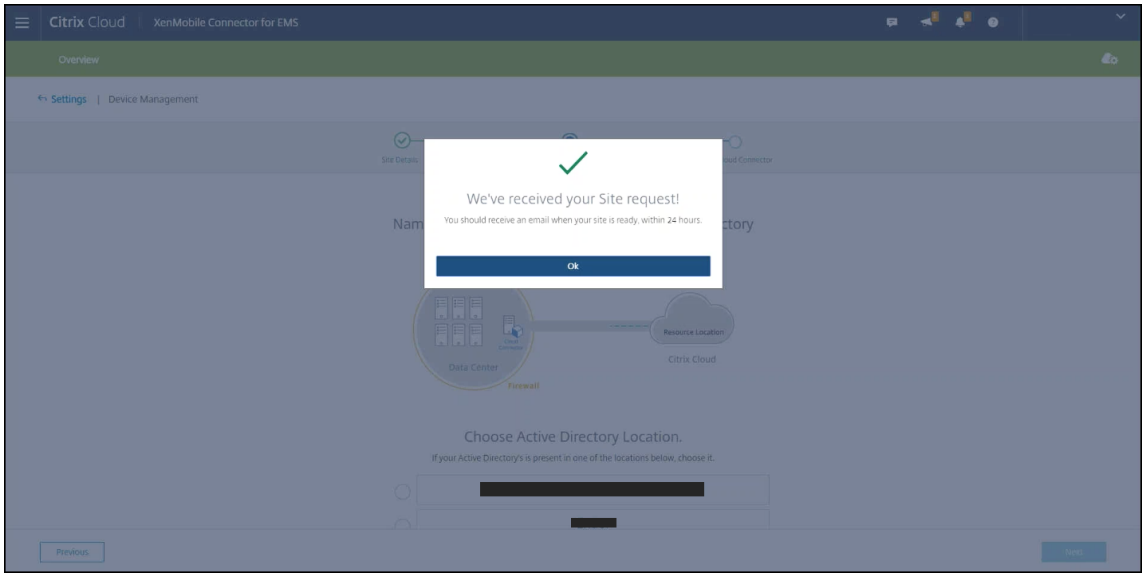
© 1997–2025 Citrix Systems, Inc. All rights reserved.



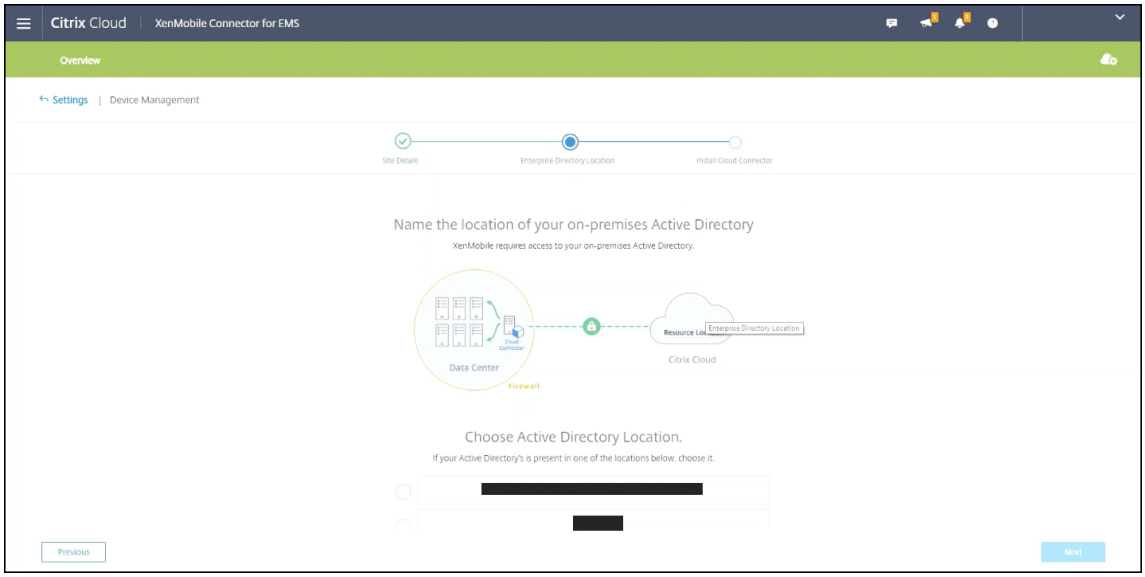
2. Enter a unique site name, select the Cloud region closest to you, and then click **Request a Site**. You receive an email when your site is ready.

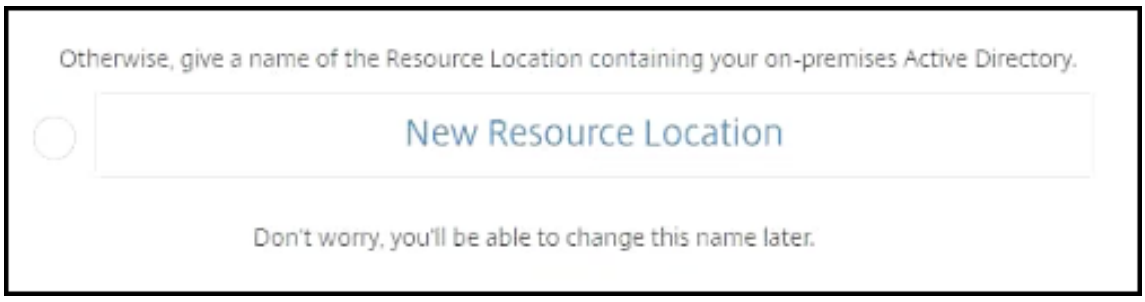


© 1997–2025 Citrix Systems, Inc. All rights reserved.



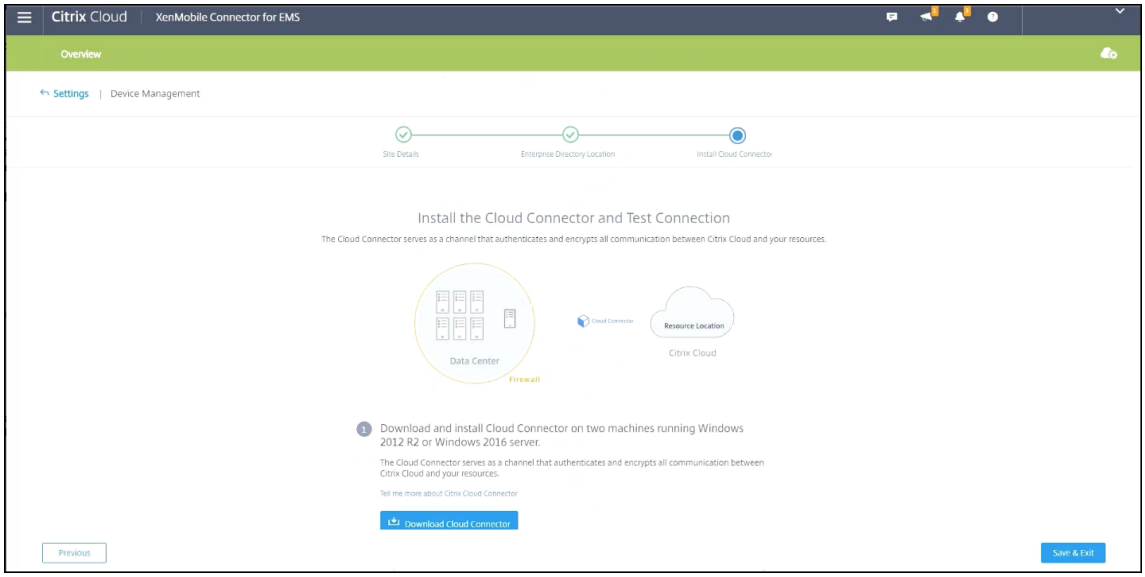
3. Click **OK** to close the prompt. Select an Active Directory Location to associate with your site or create a resource location and then click **Next**.

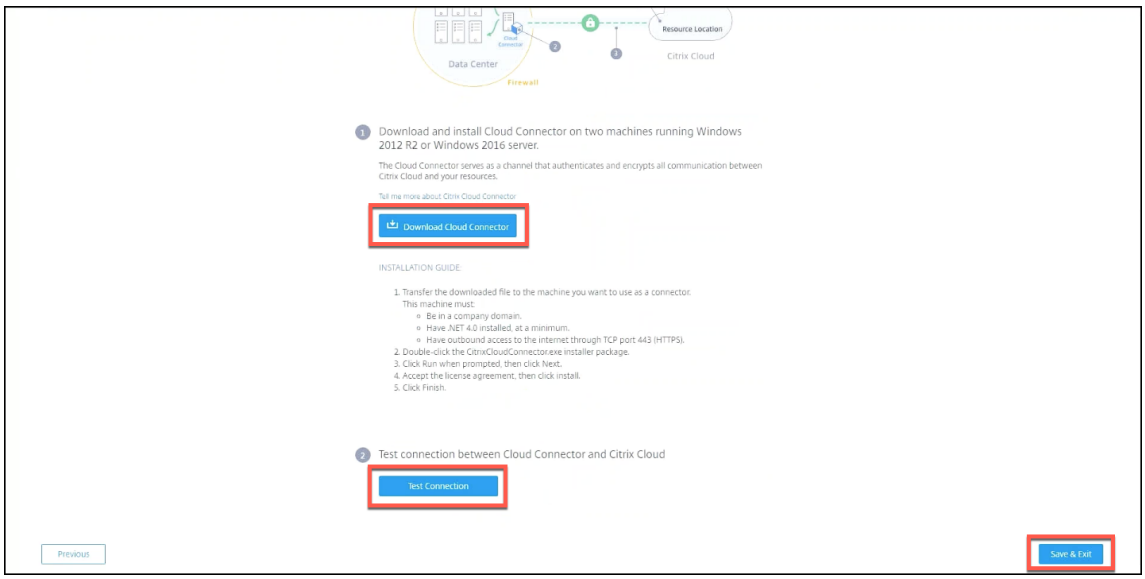




4. Click **Download Cloud Connector** and follow the on-screen instructions to install the cloud connector. After installation, click **Test Connection** to verify the connection between Citrix Cloud and the Cloud Connector.

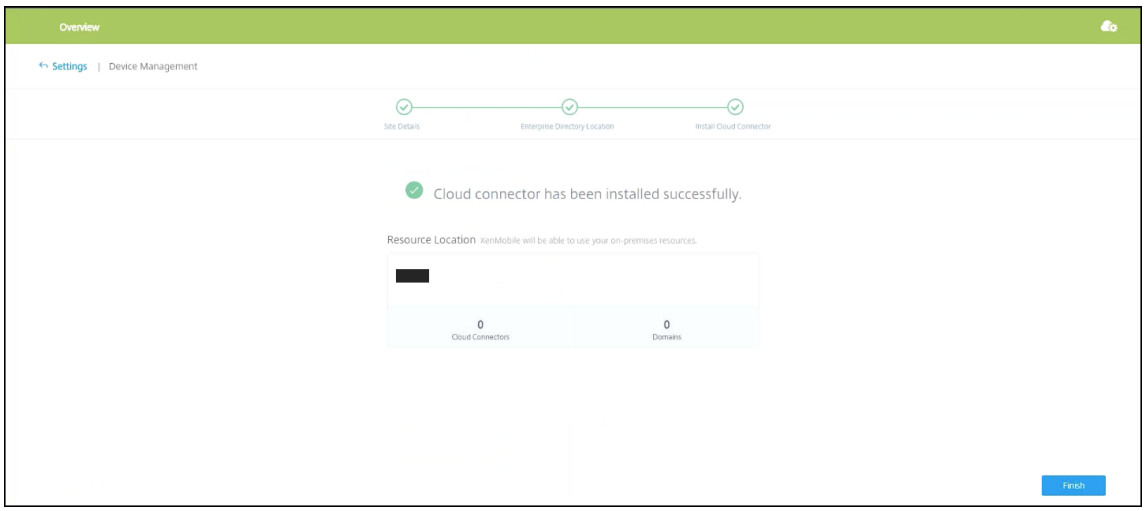
© 1997–2025 Citrix Systems, Inc. All rights reserved.



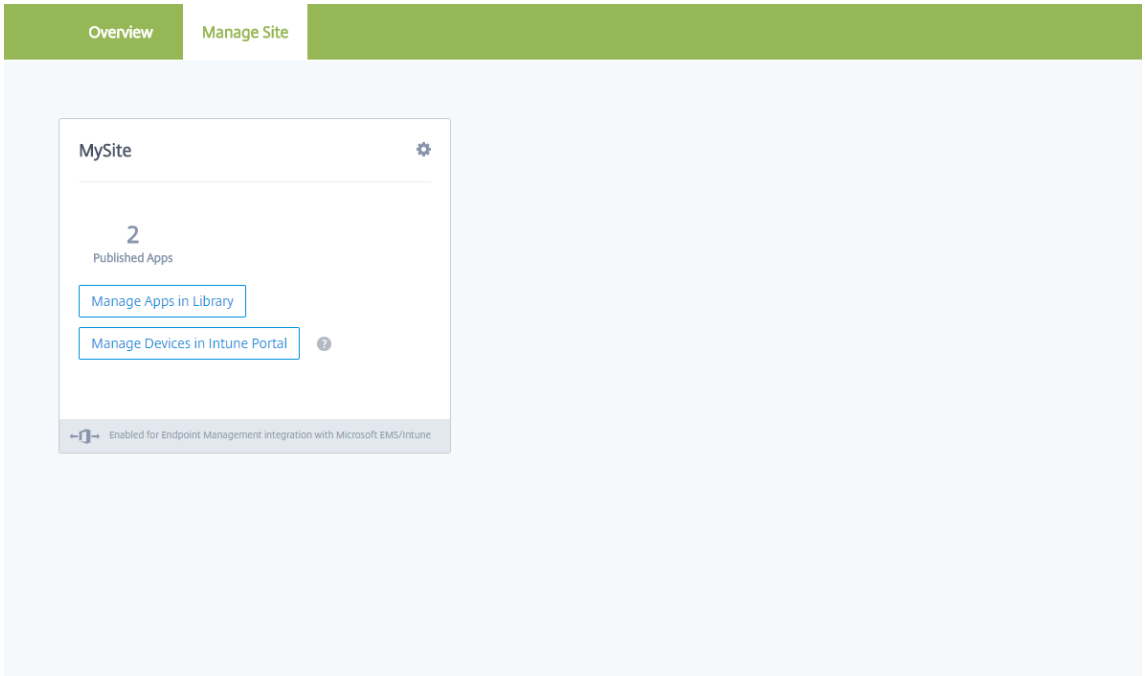


5. Click **Save & Exit** to finish. Your resource location appears. Clicking **Finish** takes you back to the settings screen.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. You can now access the Citrix Endpoint Management console from your site tile. From here, you can do MDM management tasks and assign device policies. For more information on device policies, see Device Policies.



Configure Intune managed apps for delivery to devices

> **Note:**
>
> Starting from April 1, 2025, managing Microsoft Intune apps through the Library is no longer available. If you need assistance with relevant services, contact Citrix Support to enable this feature.

To configure Intune managed apps for delivery:

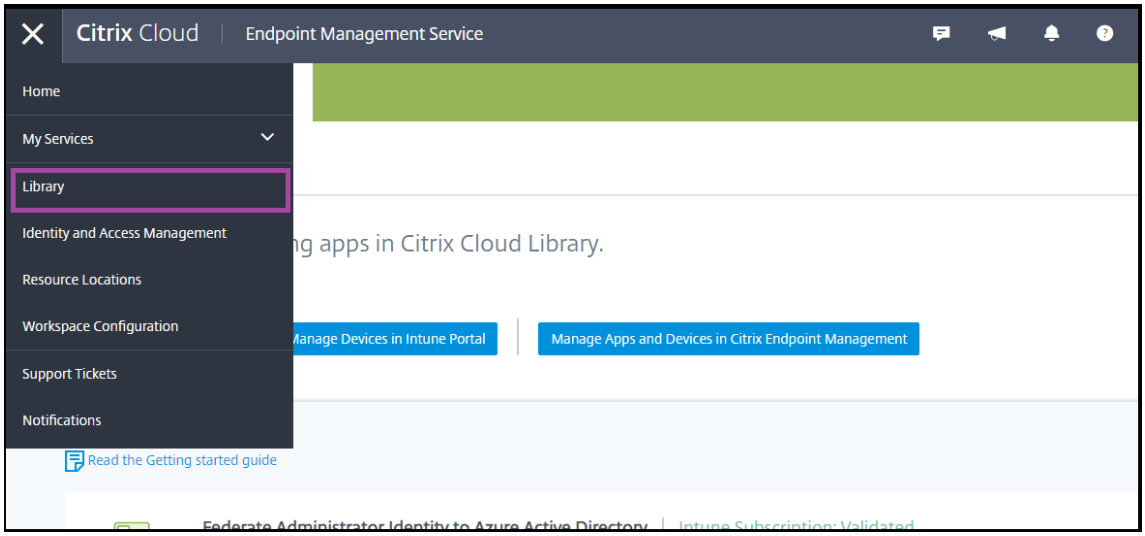
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Add the apps to the Citrix Cloud library
- Create Citrix Endpoint Management device policies to control the flow of data
- Create a delivery group for the apps and policies

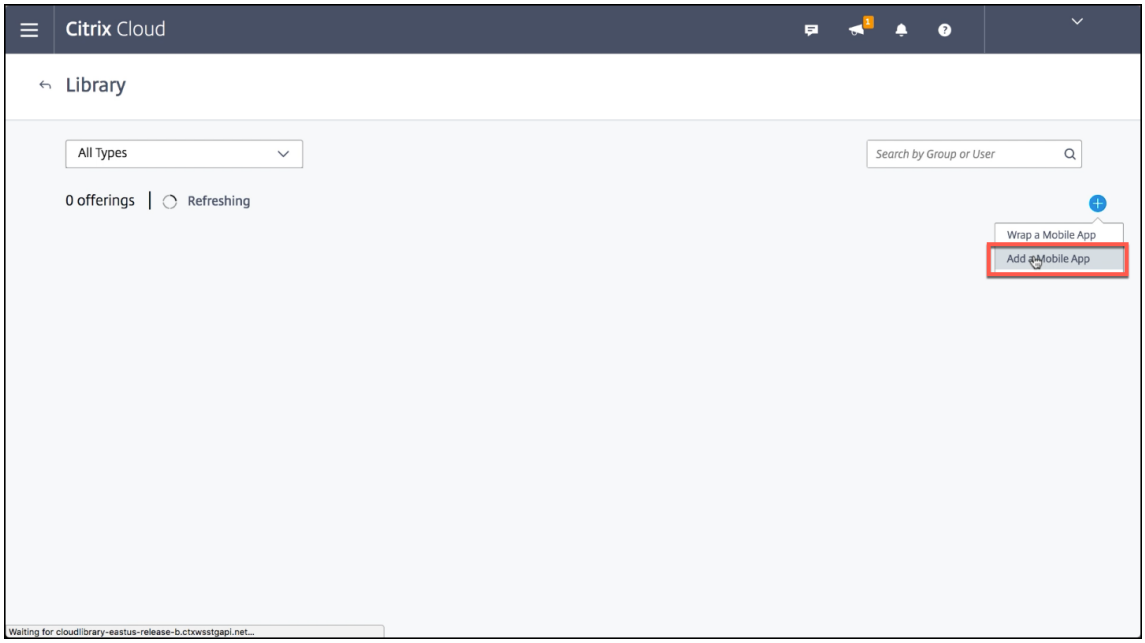
Add Microsoft Intune apps to the Citrix Cloud library

For each app you want to add:

1. From the Citrix Cloud console, click the menu icon and then click **Library**.



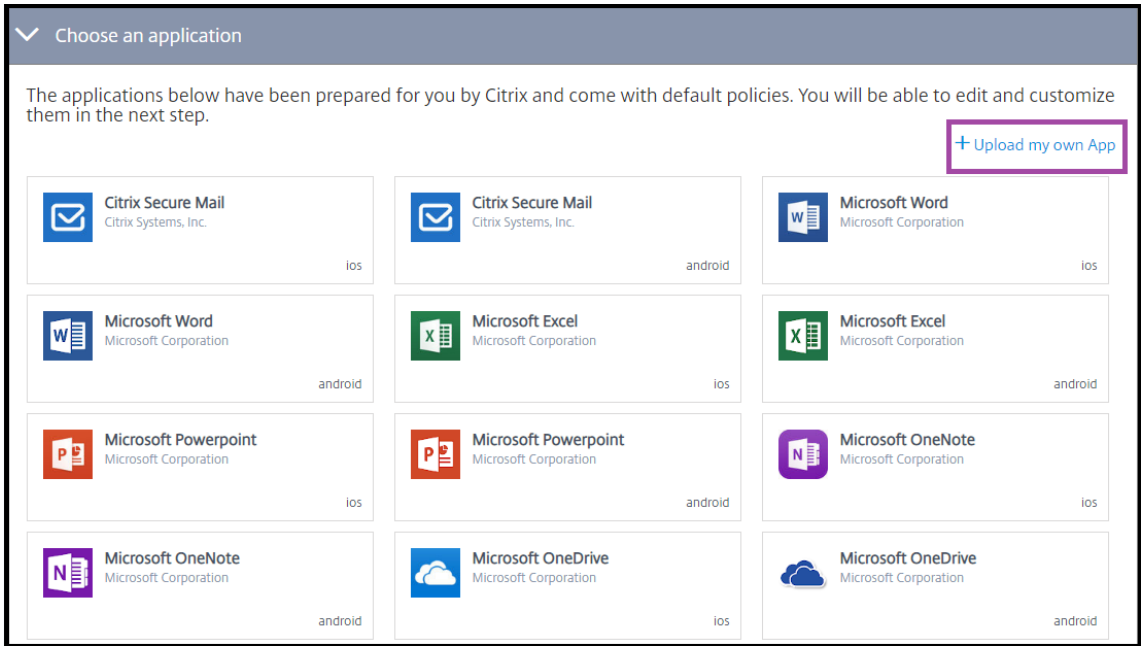
2. Click the plus sign icon on the upper-right, and then click **Add a Mobile app**.



3. If you have Android Enterprise configured in the Citrix Endpoint Management console, select

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Microsoft Intune Apps under **Choose an application**. Select an app template to customize or click **Upload my own App**.



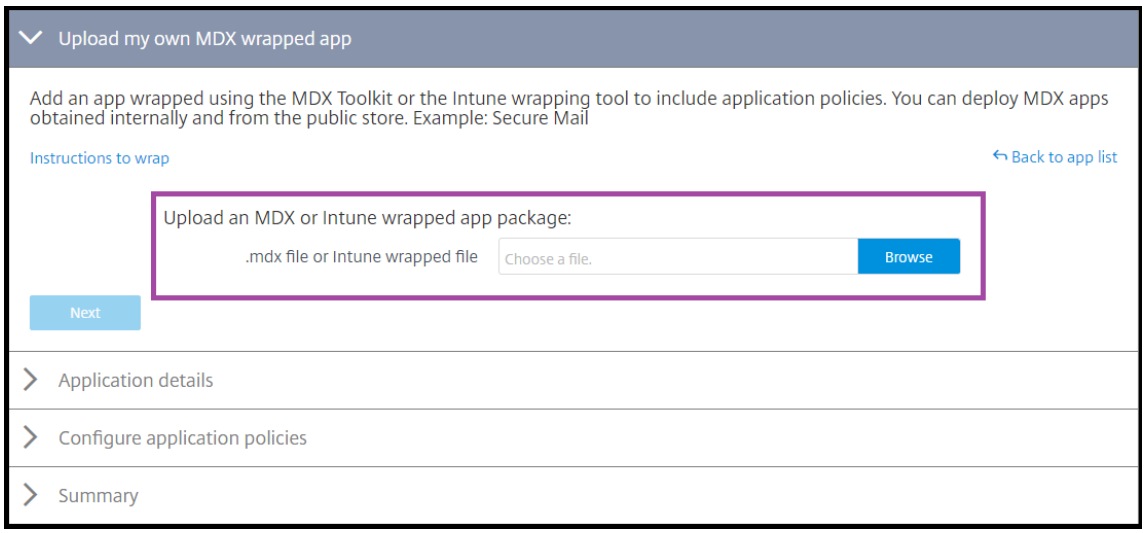
Citrix supplies the existing app templates, each of which comes with a set of preconfigured default policies. For apps that customers upload, the following policies apply:

- **MDX Files:** Includes MAM SDK enabled apps or MDX-wrapped apps, such as:
  - Intune app protection policies and the default MDX policies in the package
  - Public store apps, such as Intune app protection policies and default MDX policies that match the bundle ID or package ID
- **IPA Files:** Intune app protection policies.
- **APK Files:** Intune app protection policies.

> **Note:**
>
> If the app isn't wrapped with Intune, Intune app protection policies do not apply.

4. Click **Upload my own App** and upload your .mdx or Intune wrapped file.

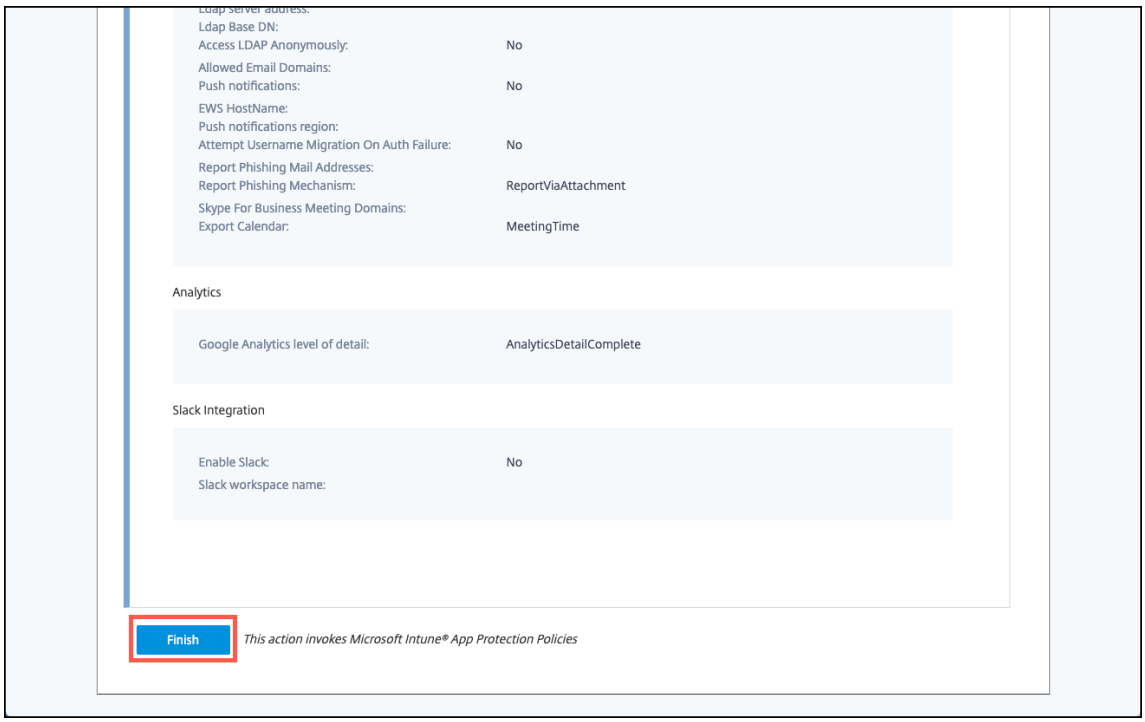
© 1997–2025 Citrix Systems, Inc. All rights reserved.



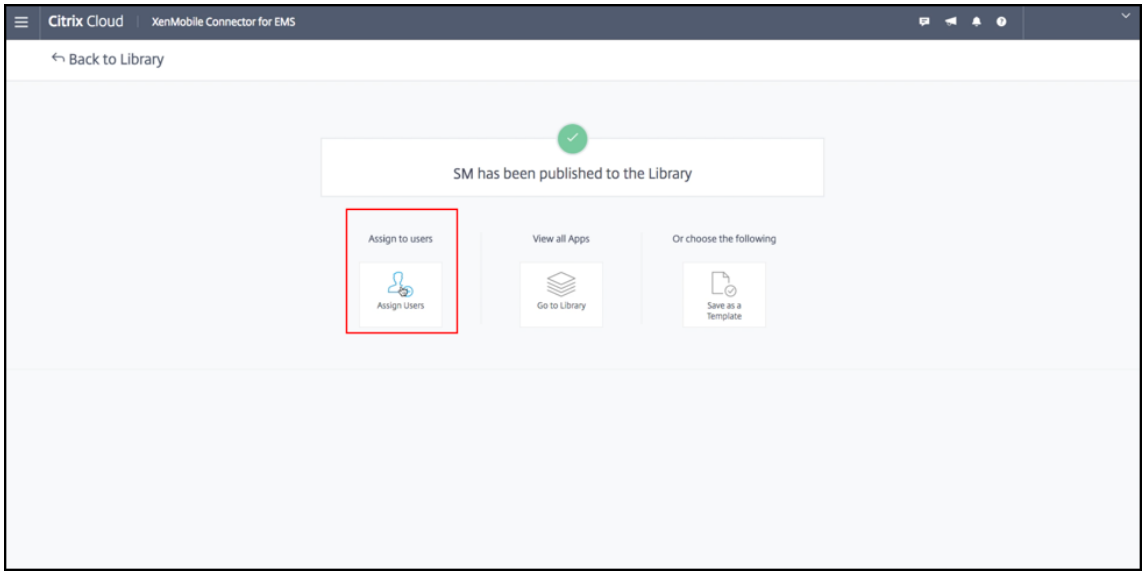
5. Enter a name and description for the app, choose whether the app is optional or required, and then click **Next**.
6. Configure the application settings. The following configurations enable Citrix Endpoint Management and Intune containers to transfer data to each other.
   - **Allow apps to receive data from other apps:** Select **Policy managed apps**.
   - **Allow app to transfer data to other apps:** Select **All apps**.
   - **Restrict cut, copy, paste with other apps:** Select **Policy managed apps**.
7. Configure the storage repositories for saved data. For **Select which storage services corporate data can be saved to**, select **LocalStorage**.
8. Optional: Set Data Relocation, Access, and PIN policies for the app. Click **Next**.
9. Review the summary of the app, and then click **Finish**.

   The app configuration process might take a few minutes. When the process completes, a message indicates that the app has been published to the library.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

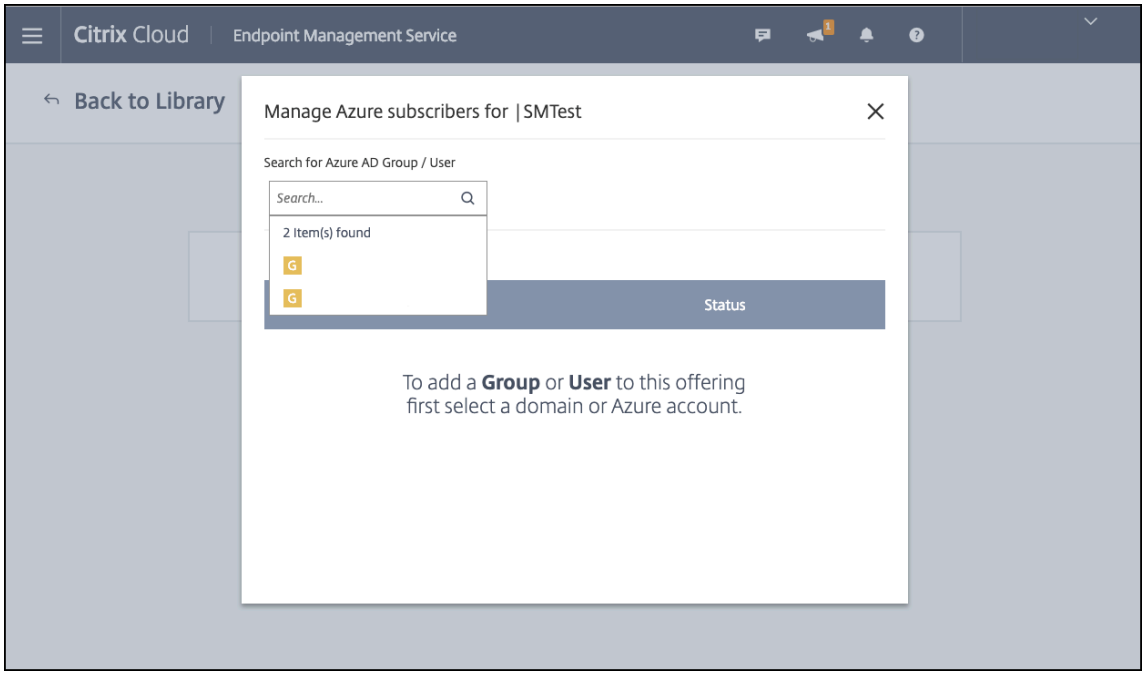


10. To assign user groups to the app, click **Assign Users**.

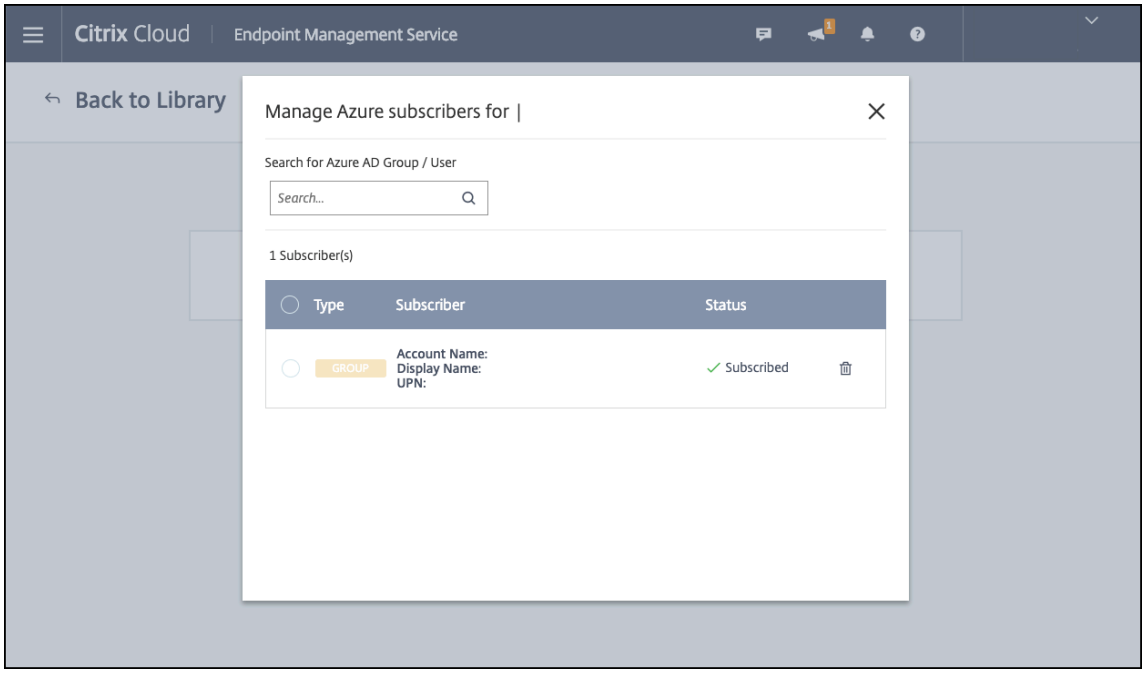


11. In the search box, search for user groups and click to add them. You can't add individual users.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



12. When you've added all the groups you want, close the window by clicking the X.



You might see an error when adding user groups. This error occurs when the user group hasn't been synchronized to the Local Active Directory.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

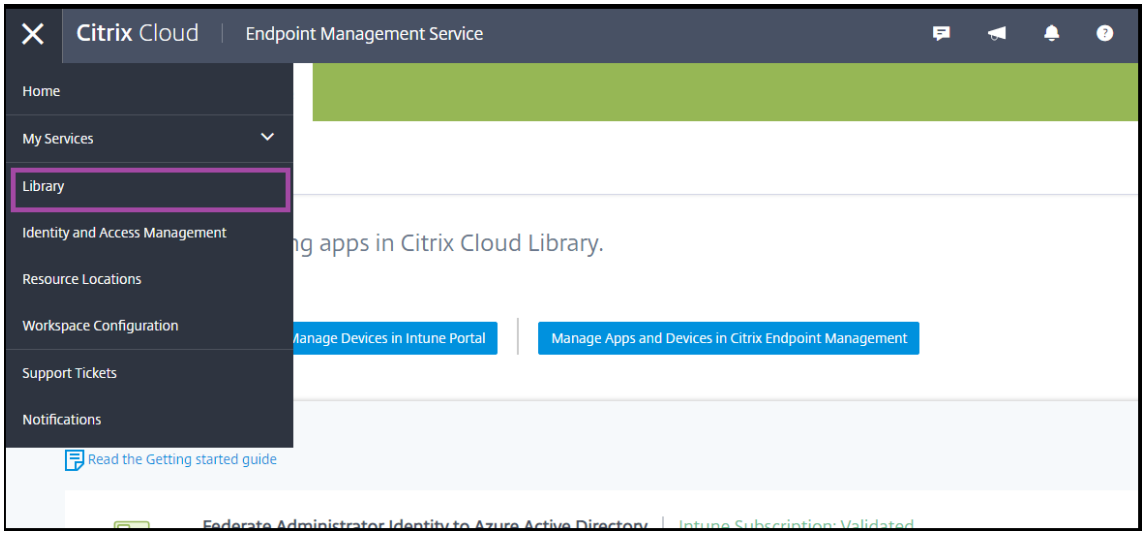
Add Android Enterprise apps to the Citrix Cloud Library

To add Android Enterprise apps to the Citrix Cloud Library and set Intune app protection policies, configure your cloud environment with the following:

- Federate Citrix Cloud with your Azure Active Directory (AAD) account. See Connect Azure Active Directory to Citrix Cloud.
- Configure LDAP and Cloud Connector in Citrix Endpoint Management.
- Set up Android Enterprise in Citrix Endpoint Management. Make sure that Android Enterprise devices enroll in MDM+MAM. To set up Android Enterprise, see Android Enterprise.

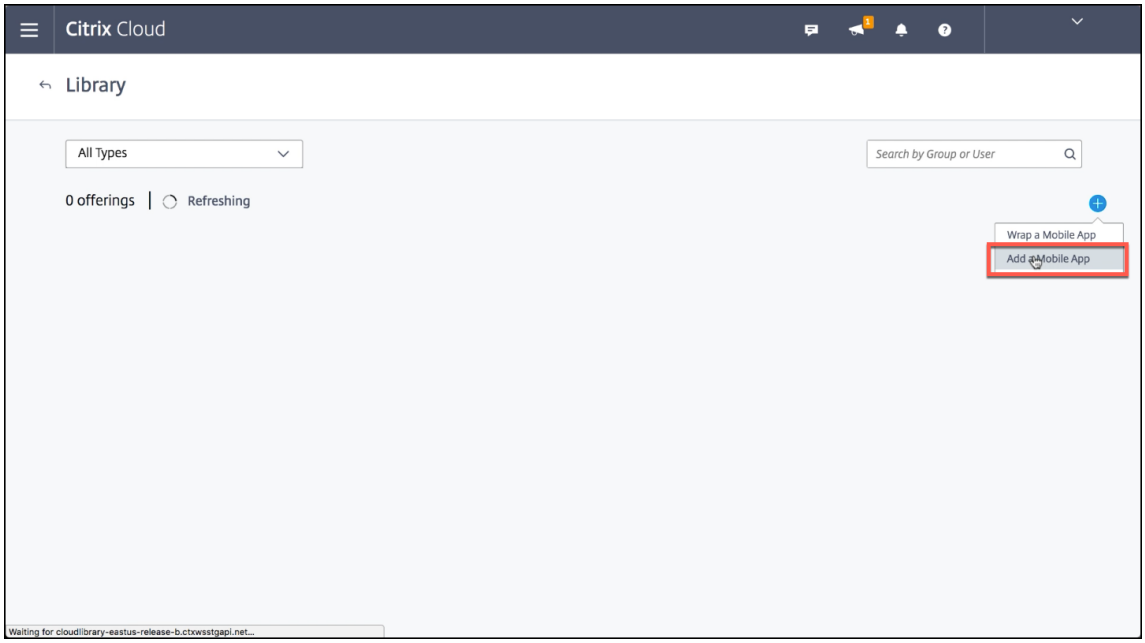
Following this procedure adds Android Enterprise apps to the Citrix Endpoint Management console and the Intune console simultaneously. For each Android Enterprise app you want to add:

1. From the Citrix Cloud console, click the menu icon and then click **Library**.

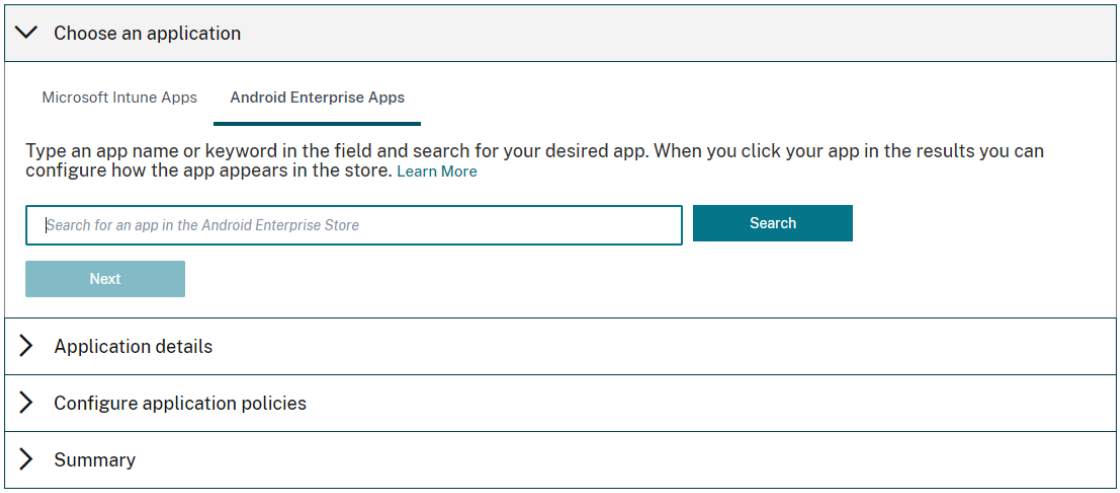


2. Click the plus sign icon on the upper-right, and then click **Add a Mobile app**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

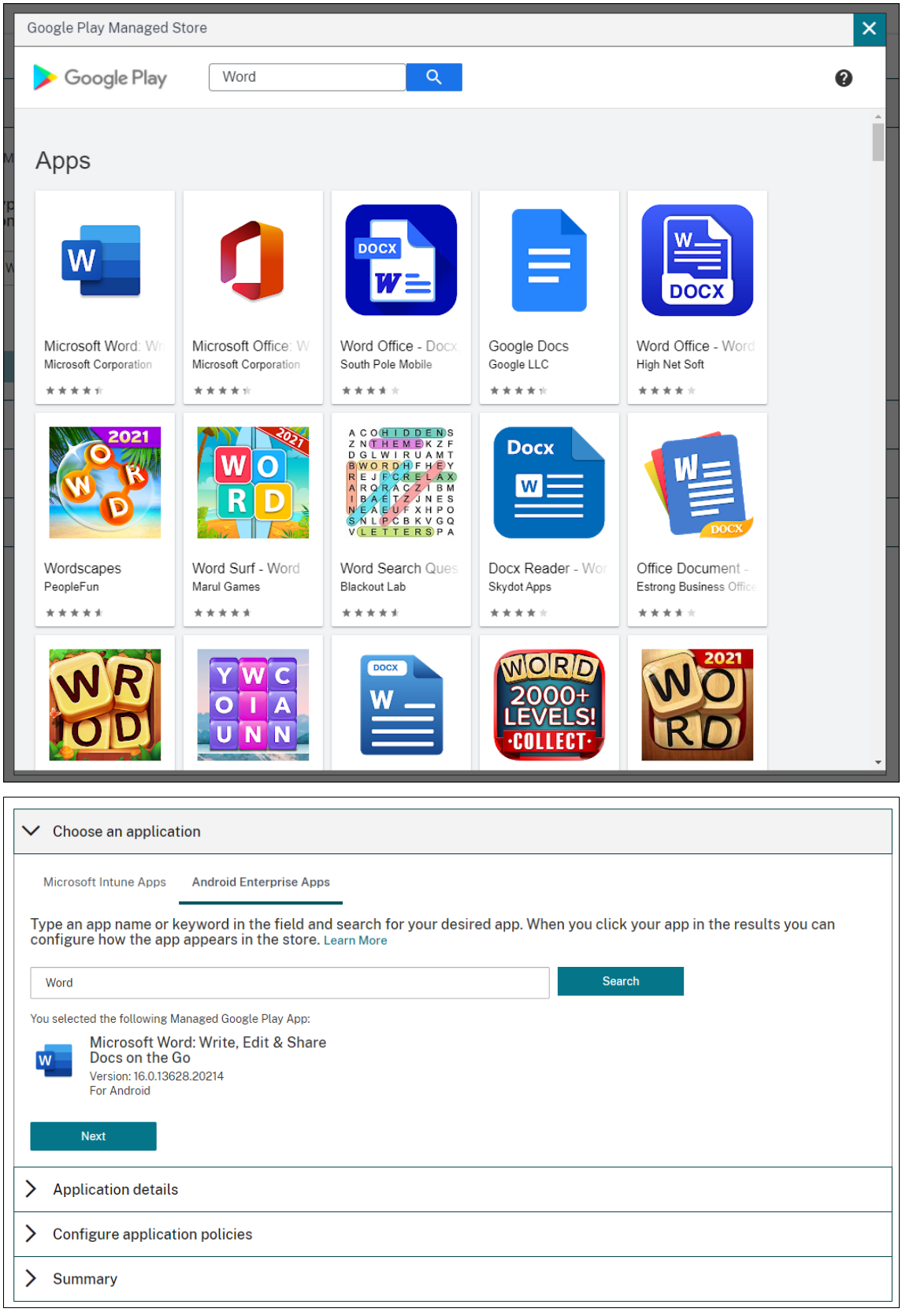


3. Under **Choose an application**, select **Android Enterprise Apps**.



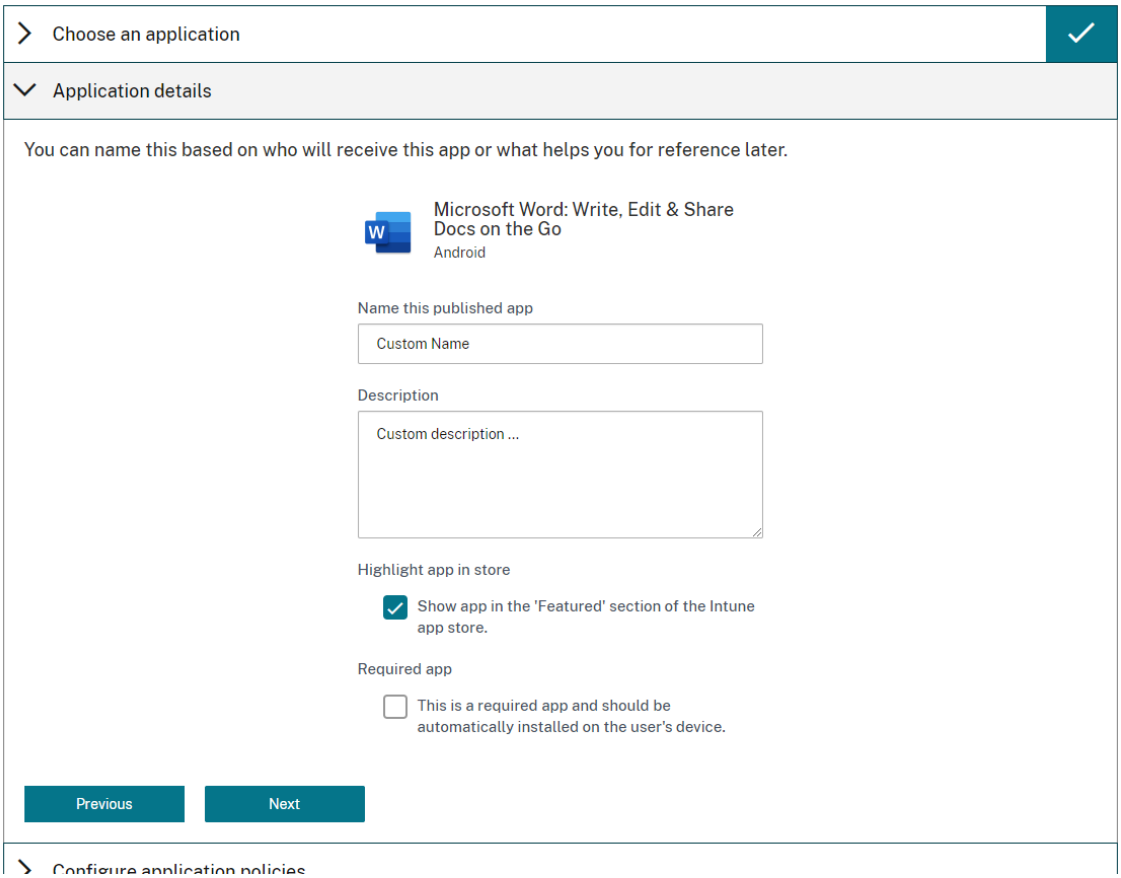
4. Search for an app and approve it in the Managed Google Play store window. After the Google window closes, click **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



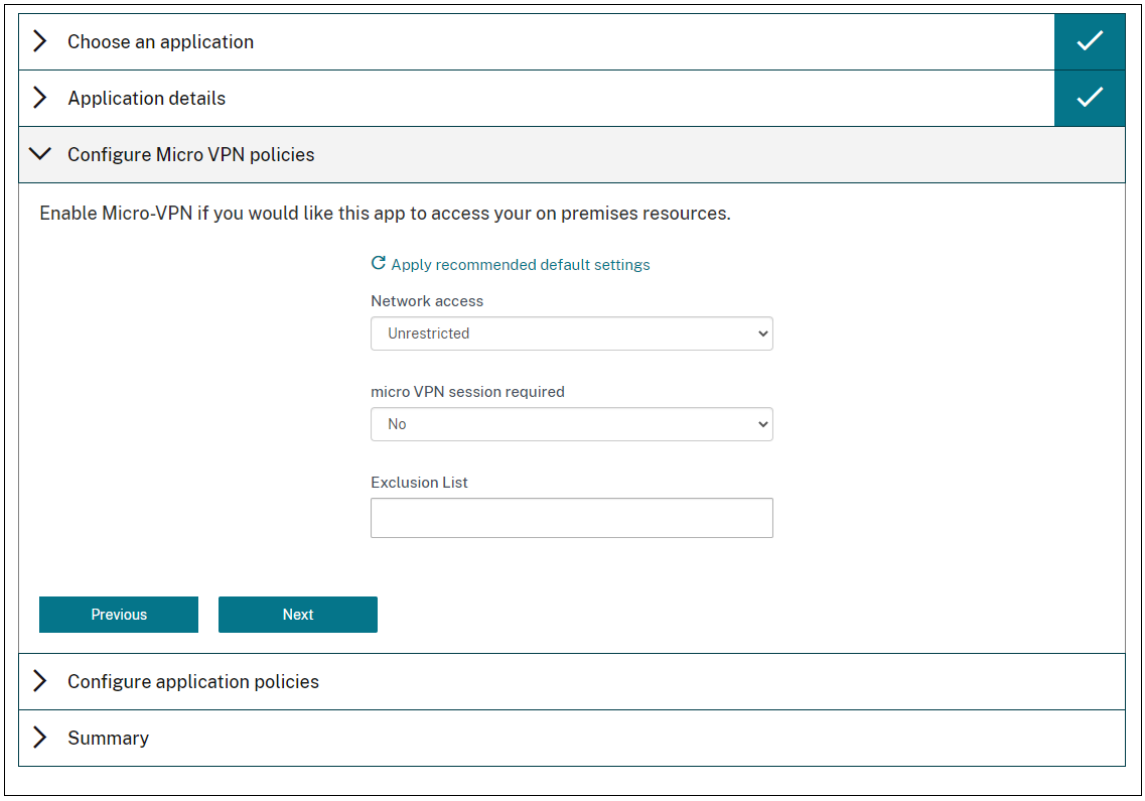
5. Add application details, and then click **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

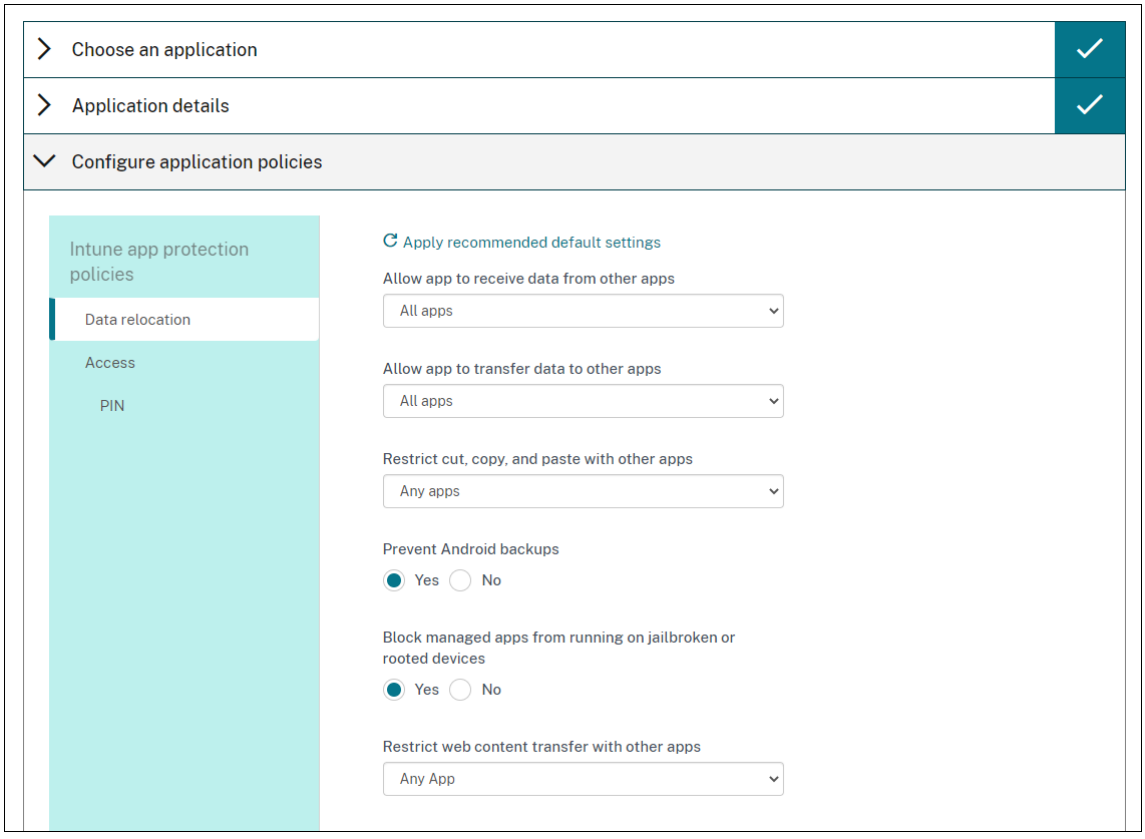


6. If you searched for and selected a Citrix mobile productivity app, you can configure Micro VPN policies. After you configure those policies, click **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



7. Configure Intune app protection policies. Click **Next**.



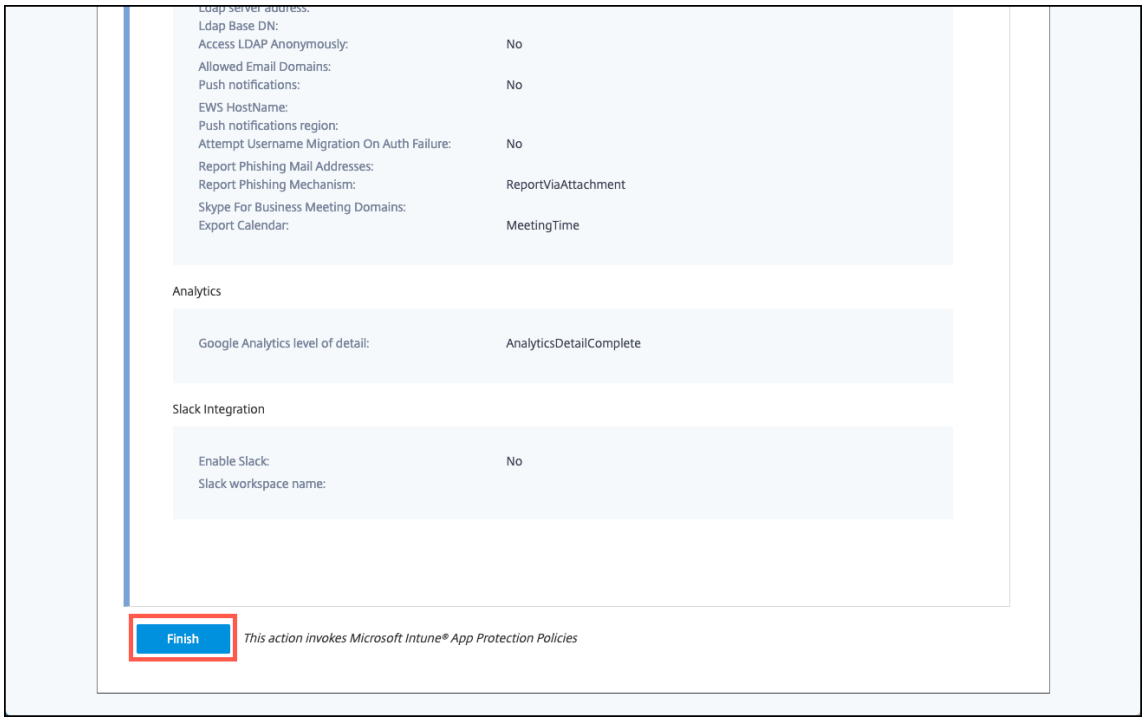
© 1997–2025 Citrix Systems, Inc. All rights reserved.

8. Configure the application settings. The following configurations enable Citrix Endpoint Management and Intune containers to transfer data to each other.

    - **Allow apps to receive data from other apps:** Select **Policy managed apps**.
    - **Allow app to transfer data to other apps:** Select **All apps**.
    - **Restrict cut, copy, paste with other apps:** Select **Policy managed apps**.

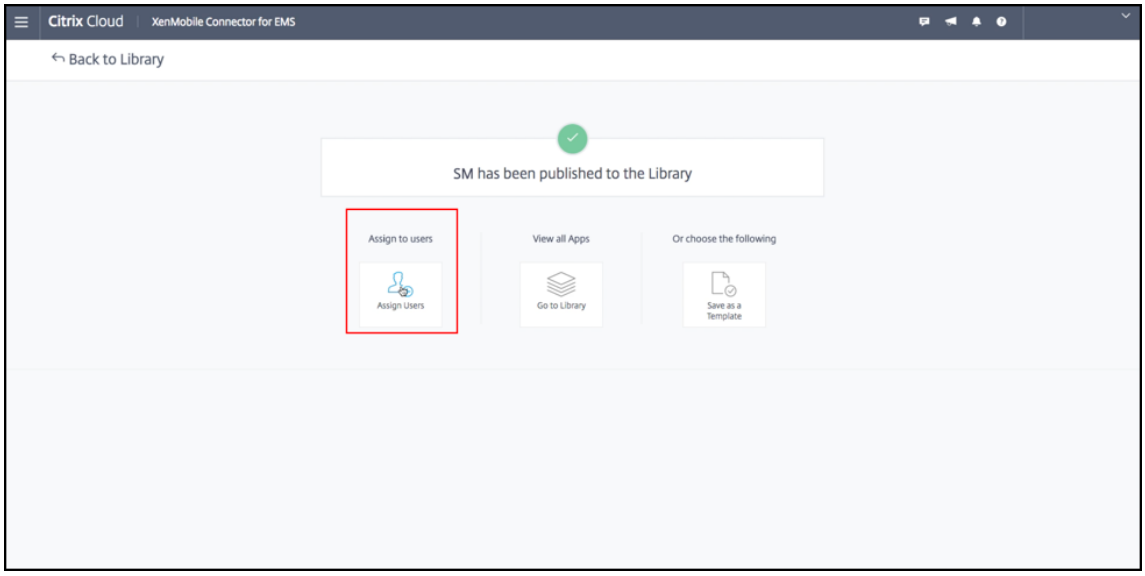
9. Configure the storage repositories for saved data. For **Select which storage services corporate data can be saved to**, select **LocalStorage**.
10. Optional: Set Data Relocation, Access, and PIN policies for the app. Click **Next**.
11. Review the summary of the app, and then click **Finish**.

    The app configuration process might take a few minutes. When the process completes, a message indicates that the app has been published to the library. The app is available in the Citrix Endpoint Management and Intune consoles. In the Citrix Endpoint Management console, the app is part of a new delivery group and is identified as a public app store app.

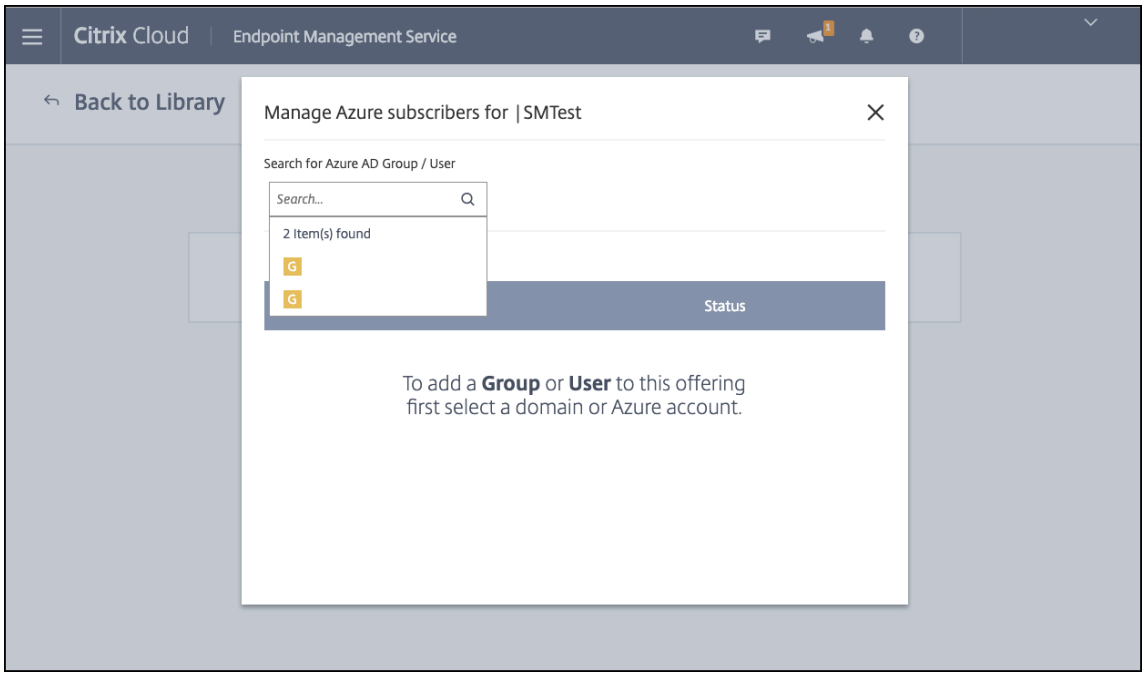


12. To assign user groups to the app, click **Assign Users**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

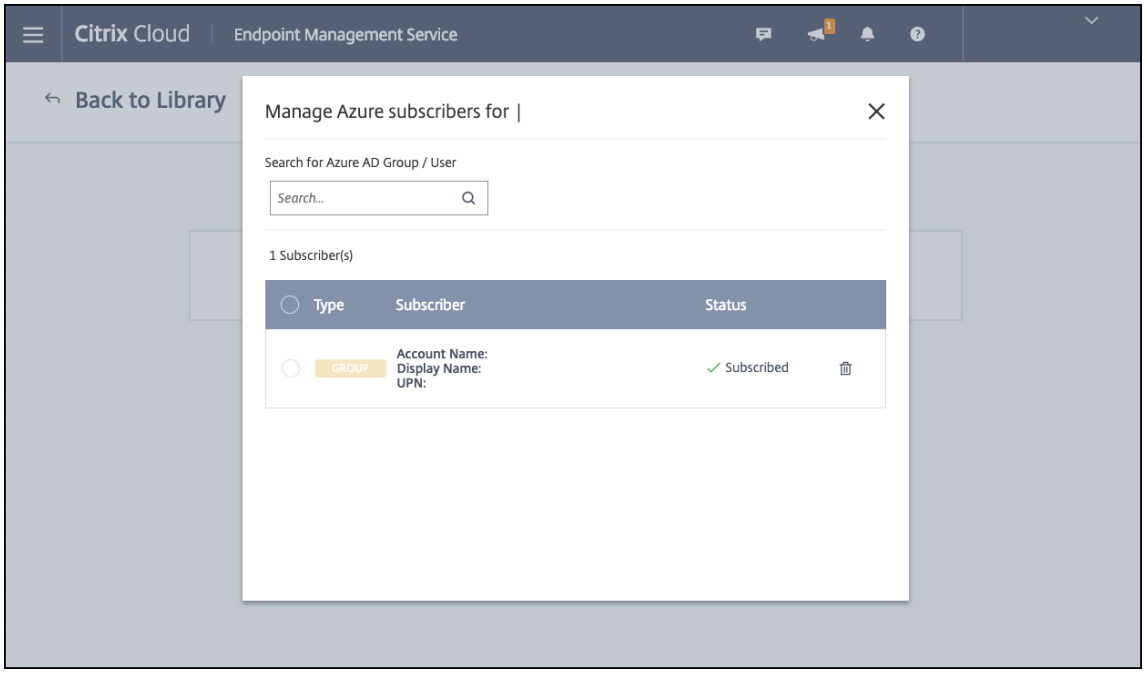


13. In the search box, search for user groups and click to add them. You can't add individual users.



14. When you've added all the groups you want, close the window by clicking the X.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



You might see an error when adding user groups. This error occurs when the user group hasn't been synchronized to the Local Active Directory.

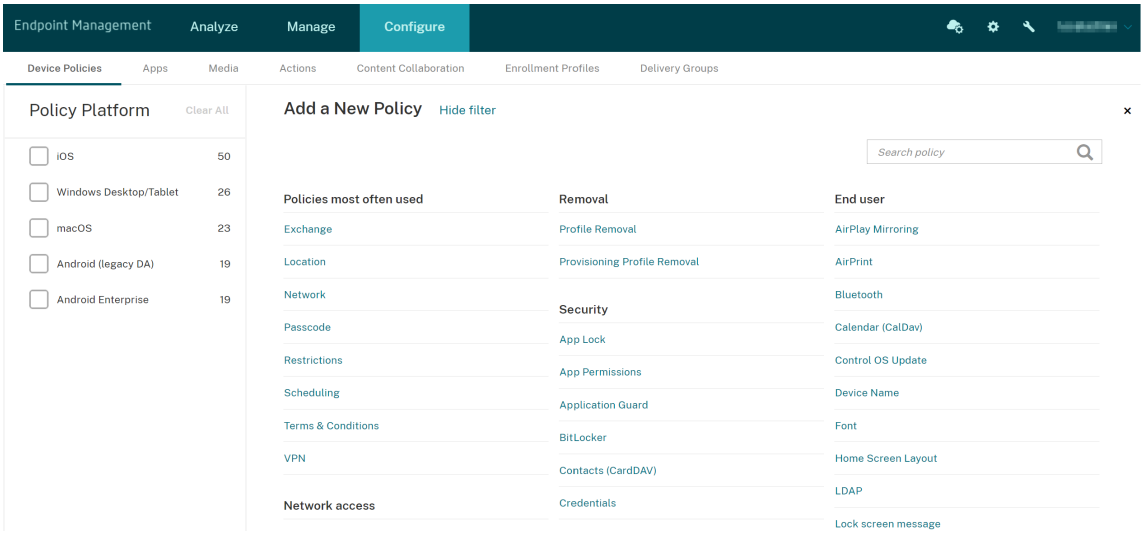
Control the type of data transferred between managed apps

Control the type of data can transfer between managed apps within the Citrix Endpoint Management or Intune containers using Citrix Endpoint Management device policies. You can configure a Restrictions policy to allow only data tagged as "corporate". Configure an App Configuration policy to tag the data.

To configure the Restrictions device policy:

1. In the Citrix Endpoint Management console, click **Configure > Device Policies**.
2. On the **Device Policies** page, click **Add**. The **Add a New Policy** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Click **Restrictions** from the list of policies.
4. On the **Policy Information** page, type a name and (optionally) a description for the policy. Click **Next**.
5. To create a device policy for iOS apps, select **iOS** in the **Platforms** pane.
6. Under **Security - Allow**, set **Documents from managed apps in unmanaged apps** to **Off**. Turning this setting **Off** also sets **Unmanaged apps read managed contacts** and **Managed apps write unmanaged contacts** to **Off**. Click **Next**.
7. Click **Next** until the **Save** button appears. Click **Save**.

Configure the App Configuration device policy for each app:

1. In the Citrix Endpoint Management console, click **Configure > Device Policies**.
2. Click **Add**. The **Add a New Policy** page appears.
3. Click **App Configuration** from the list of policies.
4. On the **Policy Information** page, type a name and (optionally) a description for the policy. Click **Next**.
5. To create a device policy for an iOS app, select **iOS** in the **Platforms** pane.
6. Select the identifier for the app to be configured.
7. For iOS apps, add the following text to **Dictionary content**:

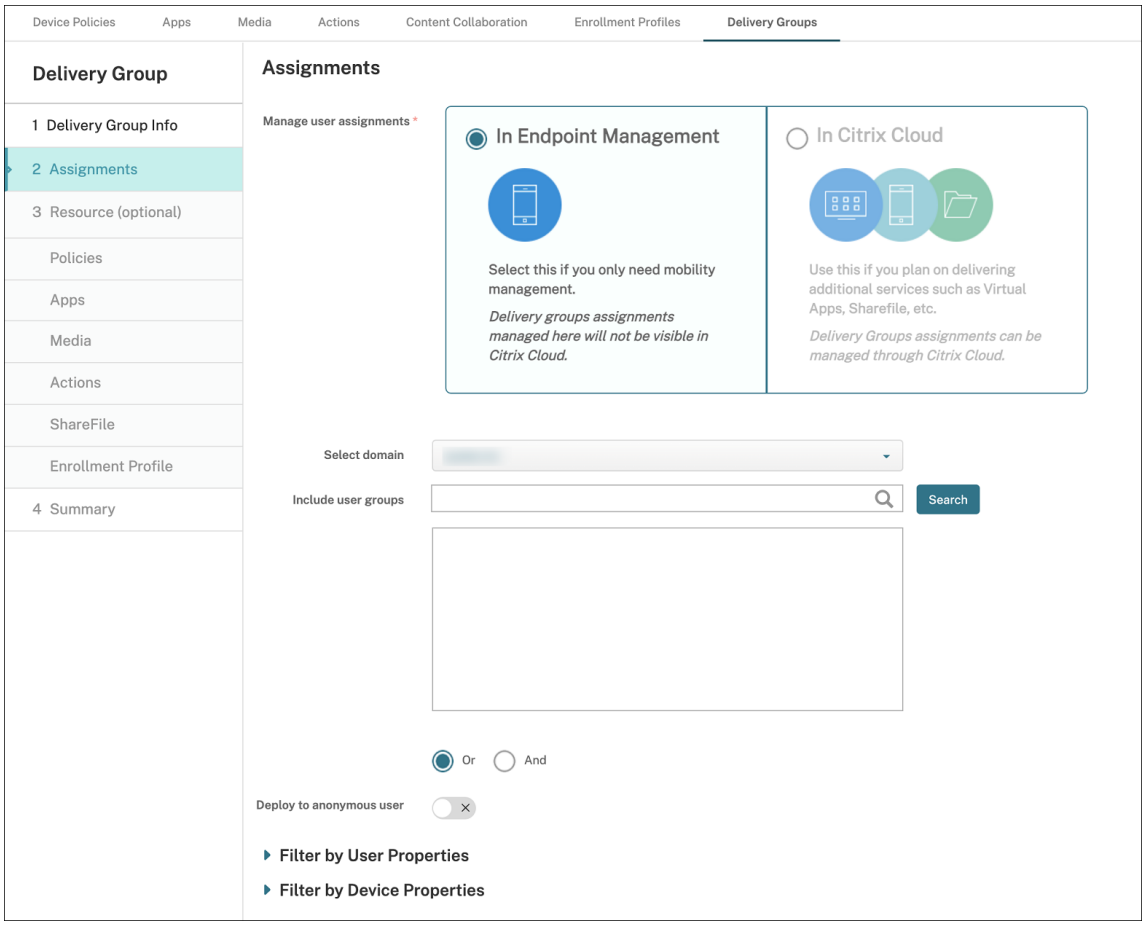
```
<dict>
    <key>IntuneMAMUPN</key>
    <string>${
 user.userprincipalname }
 </string>
</dict>
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

8. Click **Check Dictionary**.
9. Click **Next**.
10. Click **Save**.

Configure delivery groups for the apps and device policies

1. In the Citrix Endpoint Management console, click **Configure > Delivery Groups**.
2. On the **Delivery Groups** page, click **Add**. The **Delivery Group Information** page appears.
3. On the **Delivery Group Information** page, type a name and (optionally) a description for the delivery group. Click **Next**.
4. On the **Assignments** page, specify how you want to deploy the delivery group: Choose **In Citrix Endpoint Management** or **In Citrix Cloud**.



5. If you chose **In Citrix Endpoint Management**:
   - **Select domain:** From the list, select the domain from which to choose users.
   - **Include user groups:** Do one of the following:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- In the list of user groups, click the groups you want to add. The selected groups appear in the **Selected user groups** list.
- Click **Search** to see a list of all user groups in the selected domain.
- Type a full or partial group name in the search box, and then click **Search** to limit the list of user groups.

To remove a user group from the **Selected user groups** list, do one of the following:

- In the **Selected user groups** list, click the **X** next to each of the groups you want to remove.
- Click **Search** to see a list of all user groups in the selected domain. Scroll through the list and clear the checkbox of each of the groups you want to remove.
- Type a full or partial group name in the search box, and then click **Search** to limit the list of user groups. Scroll through the list and clear the checkbox of each of the groups you want to remove.

6. Click **Next**.
7. In the **Policies** page, drag the Restrictions policy and the App Configuration policy you create from the left to right. Click **Next**.
8. In the **Apps** page, drag the apps you want to deliver from the left side of the page to **Required Apps** or **Optional Apps**. Click **Next**.
9. Optional, configure the settings on the **Media** page, **Actions** page, and **Enrollments** page. Or accept the defaults on each page and click **Next**.
10. On the **Summary** page, review the delivery group settings and click **Save** to create the delivery group.

When publishing the app in the Intune console, select **Force apps to be managed**. Users on unsupervised devices are prompted to allow management of the app. If users accept the prompt, the app is managed on the device. If users decline the prompt, the app isn't available on the device.

Configure Citrix Secure Mail

> **Note:**
>
> The Citrix Secure Mail integration with Intune is deprecated and will be removed in a future release. Refer to What's new in Secure Mail for more details.

Citrix Secure Mail now supports various configurations. You can wrap Citrix Secure Mail in an Intune MAM container connecting to an on-premises Exchange Server. You can connect Citrix Secure Mail to hosted Exchange or Office 365 accounts. This release does not support certificate-based authentication, however, so use LDAP instead.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> To use Citrix Secure Mail in MDX mode, you must use Citrix Endpoint Management MDM+MAM.

Citrix Secure Mail also automatically populates user names. To enable this feature, you must configure the following custom policies first.

1. From your Citrix Endpoint Management console, go to **Settings > Server Properties** and then click **Add**.
2. In the list, click **Custom Key** and then in the **Key** field, type `xms.store.idpuser_attrs`.
3. Set the value to **true** and then in **Display name**, type `xms.store.idpuser_attrs`. Click **Save**.
4. Click **Client Properties** and then click **Add**.
5. Select **Custom Key** and then type **SEND_LDAP_ATTRIBUTES** in the **Key** field.
6. Type `userPrincipalName=${ user.userprincipalname } ,email=${ user.mail } ,displayname=${ user.displayname } ,sAMAccountName=${ user.samaccountname } ,aadupn=${ user.id_token.upn } ,aadtid=${ user.id_token.tid }` in the **Value** field. Enter a description and then click **Save**.

   The following steps only apply for iOS devices.
7. Go to **Configure > Device Policies**, click Add, and then select the **App Configuration** policy.
8. Enter a policy name and then click **Next**.

   In the Identifier list, click **Add new**. In the text box that appears, enter the bundle ID for your Citrix Secure Mail app.
9. In the **Dictionary** content box, type the following text.

```
<dict>

<key>XenMobileUserAttributes</key>

<dict>

<key>userPrincipalName</key>

<string>${
 user.userprincipalname }
 </string>

<key>email</key>

<string>${
 user.mail }
 </string>
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
18
19 <key>displayname</key>
20
21 <string>${
22  user.displayname }
23  </string>
24
25 <key>sAMAccountName</key>
26
27 <string>${
28  user.samaccountname }
29  </string>
30
31 <key>aadupn</key>
32
33 <string>${
34  user.id_token.upn }
35  </string>
36
37 <key>aadtid</key>
38
39 <string>${
40  user.id_token.tid }
41  </string>
42
43 </dict>
44
45 <key>IntuneMAMUPN</key>
46
47 <string>${
48  user.id_token.upn }
49  </string>
50
51 </dict>
```

10. Clear the **Windows Desktop/Tablet** checkbox and then click **Next**.
11. Select the user groups to which you want the policy deployed and then click **Save**.

Troubleshooting

General issues

Issue: When opening an app, the following error message appears: App Policy Required.

Resolution: Add policies in the Microsoft Graph API.

Issue: You have policy conflicts.

Resolution: Only a single policy per app is allowed.

Issue: Your app can't connect to internal resources.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Resolution: Ensure that the correct firewall ports are open, you use the correct tenant ID, and so on.

NetScaler Gateway issues

The following table lists common issues with NetScaler Gateway configurations and their solutions. For troubleshooting, enable more logs and check them by doing the following:

1. In the command-line interface, run the following command: `set audit syslogParams -logLevel ALL`
2. Check the logs from the shell using `tail -f /var/log/ns.log`

Issue	Solution
The permissions required to be configured for the Gateway App on Azure are unavailable.	Check if a proper Intune license is available. Try using the manage.windowsazure.com portal to see if the permission can be added. Contact Microsoft support if the issue persists.
NetScaler Gateway can't reach `login.microsoftonline.com` and `graph.windows.net`.	From NS Shell, check if you can reach the following Microsoft website: `curl -v -k https://login.microsoftonline.com`. Then, check whether DNS is configured on NetScaler Gateway and that the firewall settings are correct (in case DNS requests are firewalled).
An error appears in ns.log after you configure OAuthAction.	Check if Intune licensing is enabled and the Azure Gateway app has the proper permissions set.
Sh OAuthAction command does not show OAuth status as complete.	Check the DNS settings and configured permissions on the Azure Gateway App.
The Android or iOS device does not show the dual authentication prompt.	Check if the Dual Factor Device ID logonSchema is bound to the authentication virtual server.

OAuth error condition and status

Status	Error Condition
COMPLETE	Success
AADFORGRAPH	Invalid secret, URL not resolved, connection timeout

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Status	Error Condition
MDMINFO	*manage.microsoft.com is down or unreachable
GRAPH	Graph endpoint is down unreachable
CERTFETCH	Cannot talk to "Token Endpoint: `https://login.microsoftonline.com` because of a DNS error. To validate this configuration, go to shell and type `curl https://login.microsoftonline.com`. This command must validate.

Limitations

The following items describe some limitations of using MEM with Citrix Endpoint Management.

- When you deploy apps with Citrix and Intune to support micro VPN: When users provide their user name and password to access digest sites, even though their credentials are valid, an error appears. [CXM-25227]
- After changing **Split tunnel** from **On** to **Off** and waiting for the current gateway session to expire: External traffic passes directly on without going through NetScaler Gateway until the user launches an internal site in Full VPN mode. [CXM-34922]
- After changing the Open-in policy from **Managed apps** only to **All apps**, users can't open documents in unmanaged apps until they close and relaunch Citrix Secure Mail. [CXM-34990]
- When split tunneling is **On** in Full VPN mode, and the split DNS changes from local to remote, internal sites fail to load. [CXM-35168]

Known issues

When the mVPN policy **Enable http/https redirection (with SSO)** is disabled, Citrix Secure Mail does not function. [CXM-58886]

Third-party known issues

On Citrix Secure Mail for Android, when a user taps **Create New Event**, the new event creation page does not display. [CXM-23917]

When you deploy Citrix Secure Mail for iOS with Citrix and Intune to support micro VPN: The app policy that obscures the Citrix Secure Mail screen when users move the app to the background isn't enforced. [CXM-25032]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Onboarding and resource setup

September 6, 2025

If you are new to Citrix, Citrix Cloud, or to Citrix Endpoint Management, this article guides you through onboarding. Learn about workflow and the details that you need to get started.

- **Where do I start?**
  - If you haven't bought an Citrix Endpoint Management subscription, see For new Citrix customers.
  - If you have an Citrix Endpoint Management subscription, skip to When the Manage button is available.
  - If your Citrix Endpoint Management site is provisioned, skip to Configure authentication.
- **Does the configuration order matter?** This article follows a recommended configuration sequence. You can work in a different order. The Citrix Endpoint Management console lets you know if prerequisites are missing, through messages such as "Set up after provisioning".
- **What do I do after onboarding?** After you complete the onboarding and resource configuration described in this article, continue your configuration in the Citrix Endpoint Management console. For information about the next steps, see Prepare to enroll devices and deliver resources.

For new Citrix® customers

For Citrix Cloud customers new to Citrix Endpoint Management:

If you already bought an Citrix Endpoint Management subscription, skip to When the Manage button is available.

If you haven't set up a Citrix Cloud account, see Sign-up for Citrix Cloud.

If you already set up a Citrix Cloud account, but haven't bought Citrix Endpoint Management, request a service demo.

1. Use your Citrix Cloud administrator credentials to sign in to your Citrix Cloud account. The Citrix Cloud home page appears.

   All Citrix Cloud administrator accounts are created as follows:

   - Citrix Cloud administrators are Citrix Endpoint Management administrators by default.
   - Citrix Cloud administrators created with customer access must have Citrix Endpoint Management selected for them to administrate Citrix Endpoint Management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. On the Citrix Cloud home page, locate the Citrix Endpoint Management service tile and click **Request Demo**.
3. Complete and submit the demo request form. The button on the Citrix Endpoint Management services tile changes to **Demo Requested**.

If you click the Citrix Endpoint Management services tile before your request is handled, a screen appears advising you to contact your representative or partner. A Citrix sales representative can provide more information and details about the service.

While waiting for the trial, be sure to prepare for your Citrix Endpoint Management deployment by reviewing System requirements. Although Citrix hosts and delivers your Citrix Endpoint Management solution, you must handle some communication and port requirements.

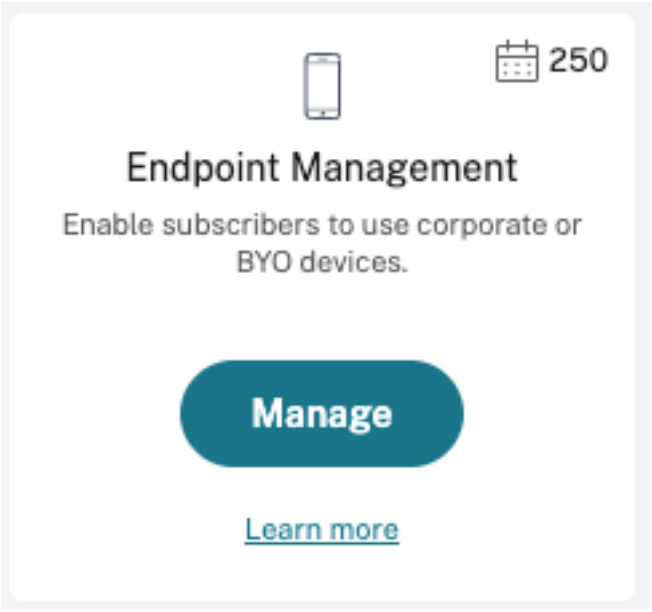
Continue with the next section.

When the Manage button is available

This video guides you through onboarding:

This is an embedded video. Click the link to watch the video

When your Citrix Endpoint Management service is available, the button on the Citrix Endpoint Management services tile changes to **Manage**.

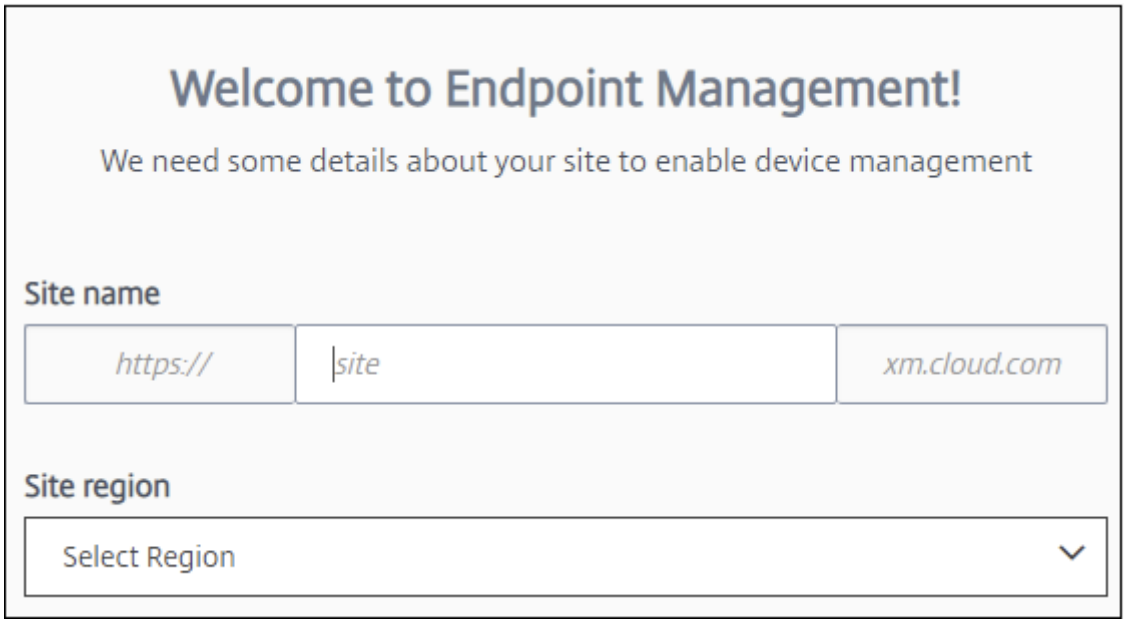


To start setup:

1. Sign in to your Citrix Cloud account using your Citrix Cloud administrator credentials.
2. Click **Manage** in the Citrix Endpoint Management tile to access the Citrix Endpoint Management console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

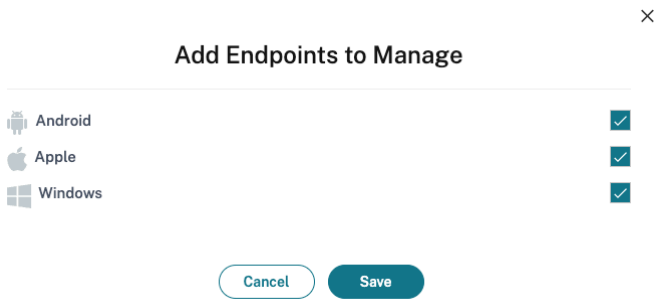
3. Type your site name and select a region. Then select **Save & Continue**.



> **Note:**
>
> To request the IPs to allow, contact the Citrix Support representative.

The Citrix Endpoint Management console then opens with a message saying that we are provisioning your suite and that some Citrix Endpoint Management functions are locked during provisioning.

1. In the **Welcome** screen, click **Start setup**.
2. Select the endpoints that you want to manage and click **Save**. You can add or clear endpoints at any time to show or hide them in the console. Showing and hiding endpoints doesn't affect your configuration.



We send you an email when provisioning completes.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Resource Center

Click the **Resource Center** icon to watch how-to videos without leaving the console.

During provisioning

While we provision Citrix Endpoint Management, you can get started with configuration.

Configure resource locations

You need resource locations before you can configure Lightweight Directory Access Protocol (LDAP) connections for Citrix Endpoint Management. Resource locations have the resources required to deliver cloud services to your subscribers. You need one resource location per domain. For help, see the Citrix Cloud article, Resource Locations.

While waiting for the trial, be sure to prepare for your Citrix Endpoint Management deployment by reviewing System requirements. Although Citrix hosts and delivers your Citrix Endpoint Management solution, some communication and port requirements are required. That setup connects the Citrix Endpoint Management infrastructure to corporate services, such as Active Directory. The information that you must provide is included in the Onboarding Handbook under "Citrix Endpoint Management Trial Sales Engineer engagement."

After you are authorized to access the trial, the button for **Citrix Endpoint Management** changes to **Manage**. Click **Manage** to open the Citrix Endpoint Management console.

Configure authentication

After your site is provisioned, you can continue with the configuration. We recommend that you set up a cloud-hosted identity provider (IdP) or Lightweight Directory Access Protocol (LDAP) to import groups, user accounts, and related properties.

To configure IdP

Citrix Endpoint Management supports authentication with identity providers, such as Azure Active Directory, Okta, and on-premises NetScaler Gateway.

To configure an IdP in Citrix Cloud and set it up for Citrix Endpoint Management:

- Authentication with Azure Active Directory through Citrix Cloud
- Authentication with Okta through Citrix Cloud

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Authentication with an on-premises NetScaler Gateway through Citrix Cloud

To configure LDAP

You can configure a connection in Citrix Endpoint Management to one or more LDAP-compliant directories for domain-based authentication. Citrix Endpoint Management supports groups that are nested in LDAP. Nested groups synchronize daily at 12 AM local time.

As a part of configuring LDAP, you must install at least one Cloud Connector.

For a quick overview, watch this video.

This is an embedded video. Click the link to watch the video

To set up LDAP:

1. On the **Settings** page, scroll to the **LDAP** tile and then click **Set Up**.
2. Follow the on-screen guidance to download and install a Cloud Connector. Cloud Connectors are required for enabling communication between Citrix Cloud and your resources. For help, see Citrix Cloud Connector.

If you have the LDAP configuration and you add Azure AD or Okta as an identity provider, Citrix Endpoint Management synchronizes IdP-specific information for your Active Directory groups in the Citrix Endpoint Management database. This configuration doesn't affect your existing delivery groups and user enrollments. But, you can't add LDAP settings in Citrix Endpoint Management afterwards. For more information, see Identity provider authentication.

If you change the **Domain alias** or **User search by** settings after enrollment, users must re-enroll. For more information about LDAP configuration, see Domain or domain plus security token authentication.

After setting up LDAP, you can continue with the authentication configuration or set up a specific platform.

Configure NetScaler Gateway

When integrated with Citrix Endpoint Management, NetScaler Gateway provides remote device access to your internal network and resources.

Citrix Endpoint Management requires NetScaler Gateway for the following scenarios:

- You require a micro VPN for access to internal network resources for line-of-business apps. Those apps are wrapped with Citrix MDX technology. The micro VPN needs NetScaler Gateway to connect to internal back-end infrastructures.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- You plan to use Citrix Endpoint Management to manage apps (MAM or MDM+MAM). NetScaler Gateway isn't required to manage devices only (MDM).
- You plan to integrate Citrix Endpoint Management with Microsoft Endpoint Manager. (Requires an on-premises NetScaler Gateway.)

For a quick overview, watch this video.

This is an embedded video. Click the link to watch the video

The following table summarizes the features supported by the on-premises NetScaler Gateway solutions.

Supported features	NetScaler Gateway on-premises
Citrix Secure Mail (STA)*	yes
Tunneled - Web SSO (web single sign-on)	yes
Full VPN (not available for Citrix mobile productivity apps for iOS)	yes
Per-app VPN	yes
Mobile single sign-on (access control)	no
High Availability	yes**
Multi-POP deployment	yes***
Proxy support	yes
Split-tunneling	yes
Split DNS	yes

* Citrix Cloud Secure Ticket Authority (STA) service configuration

** On-premises configuration

*** Global Server Load Balancing configuration

On-premises NetScaler Gateway use cases

Use one or more on-premises NetScaler Gateway appliances with Citrix Endpoint Management when:

- You require per-app VPN capabilities.
- You require full tunneling, split tunneling, reverse split tunneling, or split DNS. We recommend full VPN tunnel for connections that use client certificates or end-to-end SSL to a resource in the internal network.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- You use the Citrix Endpoint Management integration with Microsoft Endpoint Manager.

The usage of on-premises NetScaler Gateway involves significant configuration and maintenance. After you configure LDAP and NetScaler Gateway in the Citrix Endpoint Management console, you export a script from that console. You then run the script on the NetScaler Gateway.

1. On the **Settings** page, scroll to the **NetScaler Gateway** tile and then click **Start setup**.
2. Select **NetScaler Gateway (on-premises)** as the type.
3. Follow the on-screen guidance. For information, see Configure on-premises NetScaler Gateway for use with Citrix Endpoint Management.

Configure notification server

To send notifications, you must configure a gateway and a notification server. A notification server makes sure of the connectivity and the possibility of communication between end users and the administrator. To set up a notification server in Citrix Endpoint Management, see Notifications.

Configure an Apple Push Notification service (APNs) certificate for Apple devices

Citrix Endpoint Management requires an Apple Push Notification service (APNs) certificate from Apple to enroll and manage Apple devices. Citrix Endpoint Management also requires an APNs certificate if you plan to use push notifications for Citrix Secure Mail for Apple. For information about Citrix Endpoint Management and APNs, see Push Notifications for Citrix Secure Mail for iOS.

To get a certificate from Apple requires an Apple ID and developer account. For details, see the Apple Developer Program website.

For a quick overview, watch this video.

This is an embedded video. Click the link to watch the video

To configure APNs with a Citrix Certificate Signing Request:

1. On the **Settings** page, expand the **Apple** tile.
2. On the **APNs Certificate** tile, click **Set Up** and then follow the on-screen guidance.

For more information, see Certificates and authentication.

Configure Android Enterprise

Citrix Endpoint Management is fully configured after you create delivery groups and assign users to the delivery groups through the Cloud Library. From this point on, Citrix Endpoint Management administration takes place within Citrix Cloud. The combined interface simplifies switching between Citrix Cloud and Citrix Endpoint Management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

You can set up Android Enterprise for Citrix Endpoint Management with either Google Play or Google Workspace.

1. **If your organization does not use Google Workspace:** You can use managed Google Play to register Citrix as your EMM provider. If you use managed Google Play, you provision managed Google Play Accounts for devices and end users. Managed Google Play Accounts provide access to managed Google Play, allowing users to install and use the work apps you make available. If your organization uses a third-party identity service, you can link managed Google Play Accounts with your existing identity accounts.

   Because this type of enterprise isn't tied to a domain, you can create more than one enterprise for a single organization. For example, each department or region within an organization can enroll as a different enterprise. That setup enables you to use different enterprises to manage separate sets of devices and apps.

2. **If your organization already uses Google Workspace to provide users access to Google apps:** You can use Google Workspace to register Citrix as your EMM. If your organization uses Google Workspace, it has an existing enterprise ID and existing Google Accounts for users. To use Citrix Endpoint Management with Google Workspace, you sync with your LDAP directory and retrieve Google Account information from Google using the Google Directory API.

   This type of enterprise is tied to an existing domain. So, each domain can only create one enterprise. To enroll a device in Citrix Endpoint Management, each user must manually sign in with their existing Google Account. The account gives users access to managed Google Play and to other Google services through your Google Workspace plan.

For a quick overview, watch this video.

This is an embedded video. Click the link to watch the video

To get started:

1. On the **Settings** page, expand the **Android** tile.
2. On the **Android Enterprise** tile, click **Set Up**.
3. Choose **Google Play** or **G Suite**, according to how you provide users access to Google applications.
   If you previously configured the Android Enterprise platform with Google Play, the UI takes you to the Google Play store to reenroll. Click **Re-enroll**, return to the CEM console, and refresh the page.
4. Follow the on-screen guidance.

See:

- Create an Android Enterprise Account

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure Firebase Cloud Messaging

Citrix recommends that you use Firebase Cloud Messaging (FCM) to control how and when Android devices connect to Citrix Endpoint Management. Citrix Endpoint Management sends connection notifications to Android devices that are enabled for FCM. Any security action or deploy command triggers a push notification to prompt the user to reconnect to the Citrix Endpoint Management server. See Firebase Cloud Messaging.

Integrate with Microsoft Endpoint Manager

Citrix Endpoint Management integration with Microsoft Endpoint Manager adds the value of the Citrix Endpoint Management micro VPN to Microsoft Intune aware apps, such as the Microsoft Edge browser.

Citrix Endpoint Management integration with MEM also allows enterprises to wrap their own line of business apps with Intune and Citrix. The app wrapping provides micro VPN capabilities inside an Intune mobile app management (MAM) container. Citrix Endpoint Management micro VPN enables your apps to access on-premises resources. You can manage and deliver Office 365 apps, line of business apps, and Citrix Secure Mail in one container. A single container provides ultimate security and productivity.

- Citrix Cloud administrators are Citrix Endpoint Management administrators by default.
- Citrix Cloud administrators created with customer access must have Citrix Endpoint Management selected for them to administrate Citrix Endpoint Management.

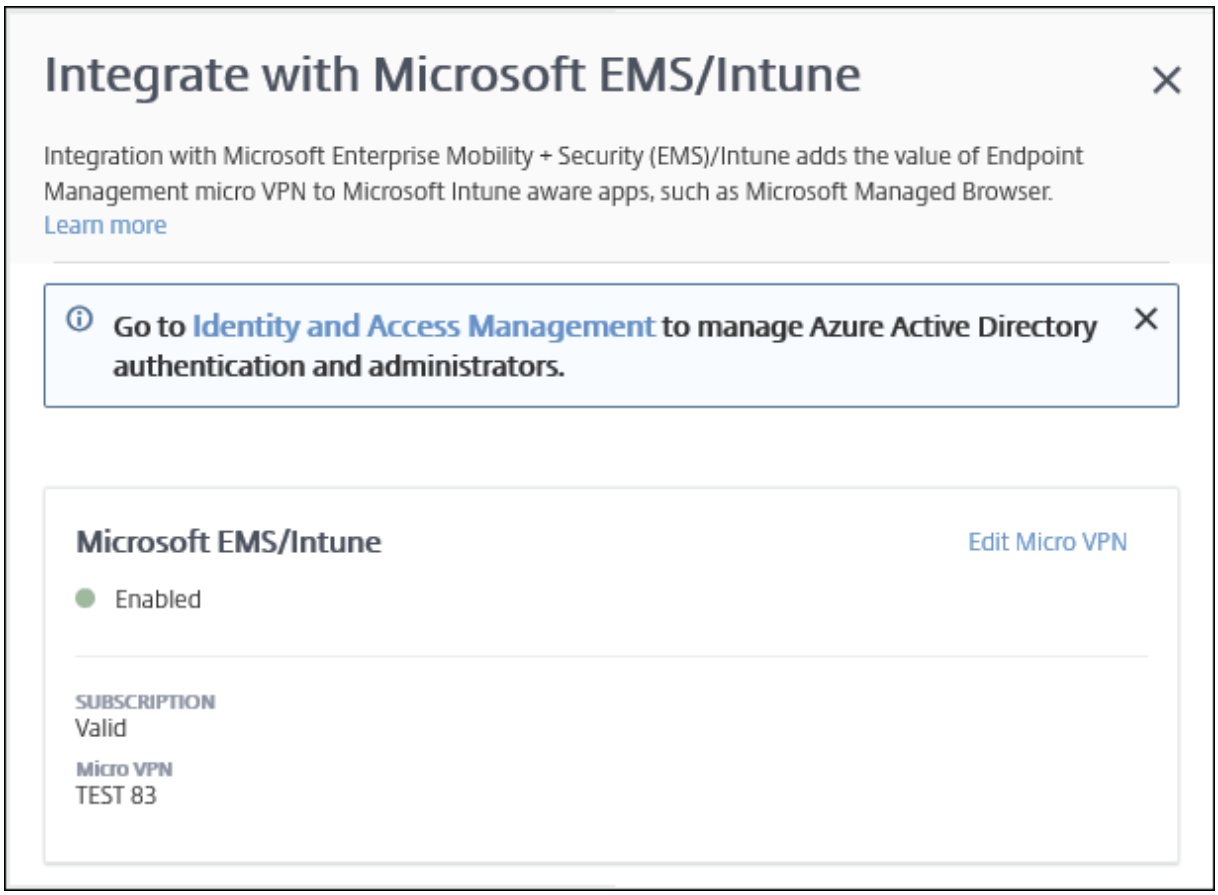
In the Citrix Endpoint Management console, you can change only the role and membership of a user. To change a role at any time, access the Citrix Endpoint Management console from the Citrix Cloud dashboard. Go to the **Manage** tab and click **Users**. Select a specific user and click **Edit** to change the role. For more information, see Configure roles with RBAC.

To integrate with MEM, see Citrix Endpoint Management integration with Microsoft Endpoint Manager.

After you complete the configuration in Citrix Cloud, return to the Citrix Endpoint Management console as follows: Go to the Citrix Cloud **Home** page and then click **Manage** on the **Citrix Endpoint Management** tile. Then you can verify if you signed in to Citrix Endpoint Management with your Azure Active Directory account.

1. On the **Settings** page, scroll to the **Integrate with Microsoft EMS/Intune** tile.
2. Click **See more**. The UI indicates if you successfully enabled the connection.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



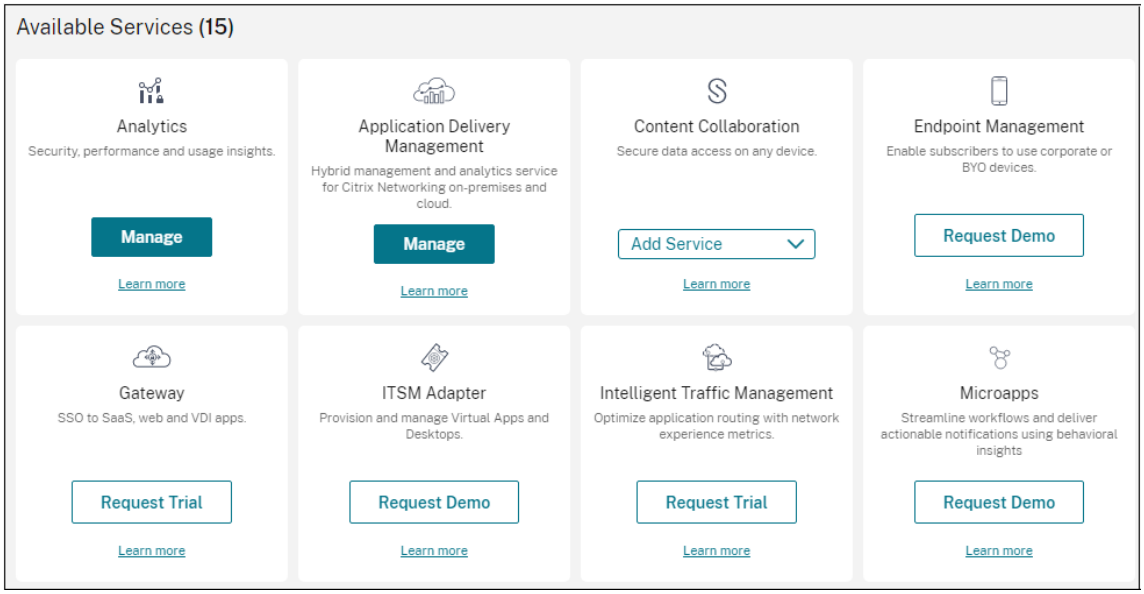
In the Citrix Cloud console, you can also change user names or passwords, and delete or edit local users. See Identity and access management.

Link an existing ShareFile account to Citrix Cloud

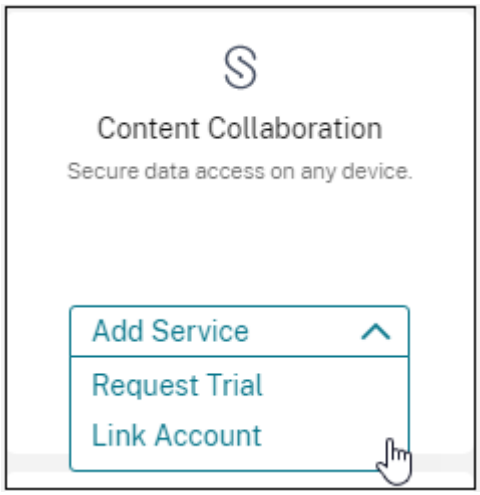
If you had a ShareFile account before you signed up with Citrix Cloud, you must link that account to Citrix Cloud. To link your account, your email address must be an administrator of the ShareFile account. When you're ready to continue, go to https://onboarding.cloud.com.

1. After you log in, a screen similar to the following appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

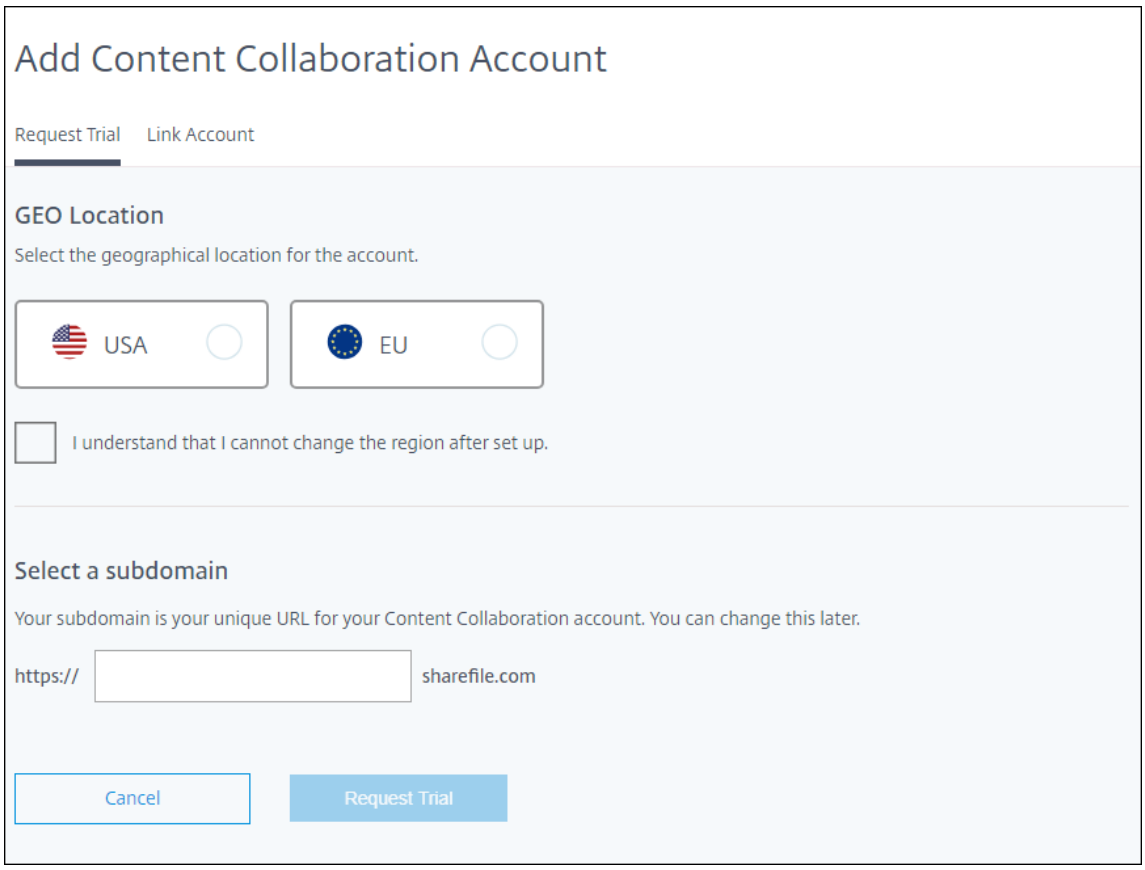


2. In the **ShareFile** tile, choose **Link Account**.



3. After we confirm your ShareFile account, the following page appears:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Click the **Link Account** tab to complete the process. You can immediately manage your ShareFile account from Citrix Cloud.

Scale and size considerations for Cloud Connectors

September 6, 2025

When evaluating the Citrix Endpoint Management service for sizing and scalability, research and test the configuration of the Cloud Connectors for your specific requirements. Cloud Connector is under load only during device enrollment. Undersizing the machines can impact system performance negatively.

Citrix® requires two Cloud Connectors per resource location. Install Cloud Connector on a dedicated server that doesn't share responsibilities with any other components or products. In our testing, Cloud Connectors were deployed in HA sets (**they are not load-balanced**).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Test configuration

- Two dedicated Windows Server 2019, 2 vCPU, 4 GB memory
- Android and iOS device enrollments into MDM+MAM, split evenly over an 8-hour period
- Citrix Endpoint Management configured to enroll 125 devices per hour per 1,000 devices
  - 1,000 devices (125 device enrollments per hour)
  - 5,000 devices (625 device enrollments per hour)
  - 10,000 devices (1250 device enrollments per hour)
  - 20,000 devices (2500 device enrollments per hour)

Test results

Cloud Connector	1,000 devices	5,000 devices	10,000 devices	20,000 devices
CPU average	2%	2%	4%	4%
CPU maximum	8%	8%	10%	11%
Memory average	73%	73%	75%	75%
Memory maximum	76%	76%	76%	79%

Prepare to enroll devices and deliver resources

September 6, 2025

> **Important:**
>
> Before proceeding, be sure to complete all the tasks described in Onboarding and resource setup.
>
> Keep your users informed about upcoming changes. See Welcome to your Citrix User Adoption Kit.

Citrix Endpoint Management supports various enrollment options. This article covers the basic setup required to enable all supported devices to enroll. The following diagram summarizes the basic setup.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For a list of supported devices, see Supported device operating systems.

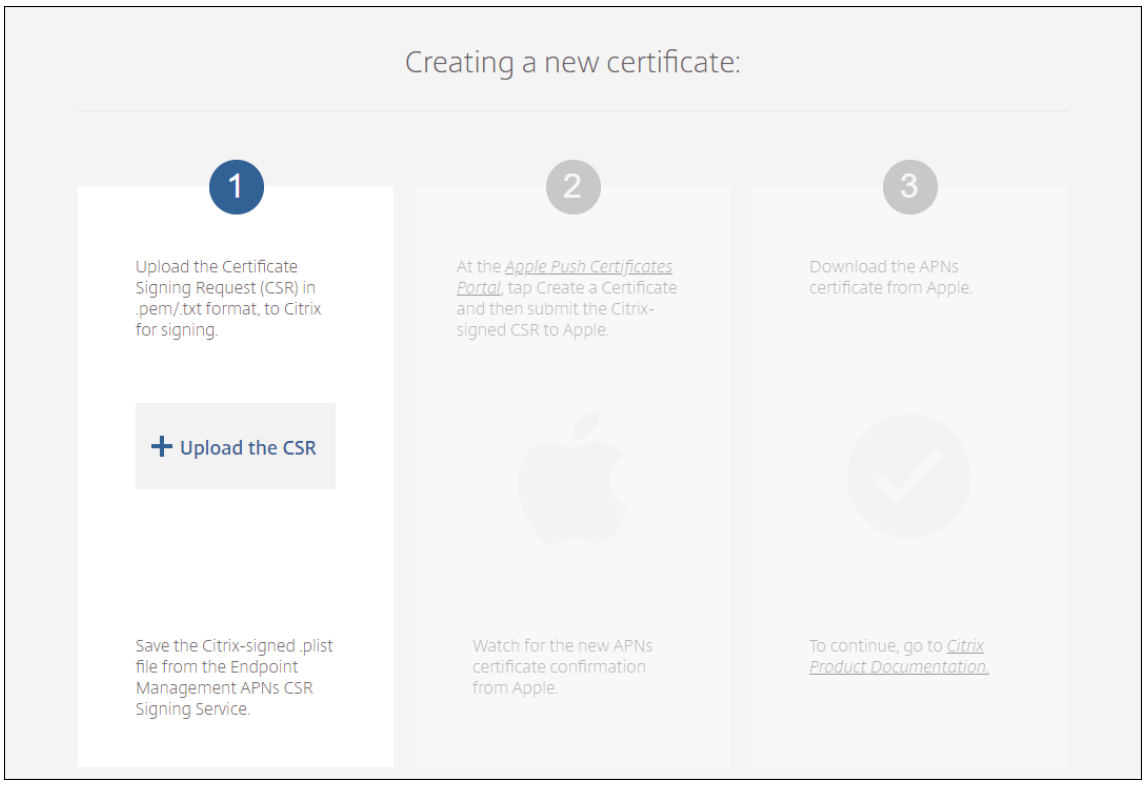
Set up an Apple Push Notification service (APNs) certificate for iOS devices

> **Important:**
>
> Apple support for the APNs legacy binary protocol ends on March 31, 2021. Apple recommends that you use the HTTP/2-based APNs provider API instead. From version 20.1.0, Citrix Endpoint Management supports the HTTP/2-based API. For more information, see the news update, "Apple Push Notification Service Update"in https://developer.apple.com/. For help with checking connectivity to APNs, see Connectivity checks.

Citrix Endpoint Management requires an Apple Push Notification service (APNs) certificate from Apple to enroll and manage iOS devices. Citrix Endpoint Management also requires an APNs certificate for Citrix Secure Mail for iOS push notifications.

- To get a certificate from Apple requires an Apple ID and developer account. For details, see the Apple Developer Program website.
- To get an APNs certificate and import it into Citrix Endpoint Management, see APNs certificates.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- For more information about Citrix Endpoint Management and APNs, see Push Notifications for Citrix Secure Mail for iOS.

Set up Firebase Cloud Messaging (FCM) for Android devices

Firebase Cloud Messaging (FCM) controls how and when Android devices connect to the Citrix Endpoint Management service. Any security action or deployment command triggers a push notification. The notification prompts users to reconnect to Citrix Endpoint Management.

- FCM setup requires that you configure your Google account. To create Google Play credentials, see Manage your developer account information. You also use Google Play to add, buy, and approve apps for deployment to the Android Enterprise workspace on a device. You can use Google Play to deploy your private Android apps, public apps, and third-party apps.
- To set up FCM, see Firebase Cloud Messaging.

Set up Citrix Endpoint Management AutoDiscovery service

The AutoDiscovery service simplifies the enrollment process for users through email-based URL discovery. The AutoDiscovery service also provides features such as enrollment verification, certificate pinning, and other benefits for Citrix Workspace customers. The service, hosted in Citrix Cloud, is an important part of many Citrix Endpoint Management deployments.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

With the AutoDiscovery service, users:

- Can use their corporate network credentials to enroll their devices.
- Don't need to enter details about the Citrix Endpoint Management server address.
- Enter their user name in user principal name (UPN) format. For example, `user@mycompany.com`.

We recommend that you use the AutoDiscovery service for high-security environments. The AutoDiscovery service supports public key certificate pinning, which prevents man-in-the-middle attacks. Certificate pinning makes sure that the certificate signed by your enterprise is used when Citrix clients communicate with Citrix Endpoint Management. To configure certificate pinnings for your Citrix Endpoint Management sites, contact Citrix Support. For information about certificate pinning, see Certificate pinning.

To access the AutoDiscovery service, navigate to https://adsui.cloud.com (commercial).

Prerequisites

- The new AutoDiscovery service in Citrix Cloud requires the latest version of Citrix Secure Hub:
  - For iOS, Citrix Secure Hub version 21.6.0 or later
  - For Android, Citrix Secure Hub version 21.8.5 or later

    Devices running on earlier versions of Citrix Secure Hub might experience interruptions in service.
- To access the new AutoDiscovery service, you must have a Citrix Cloud administrator account with full access. The AutoDiscovery service doesn't support administrator accounts with custom access. If you don't have an account, see Sign-up for Citrix Cloud.

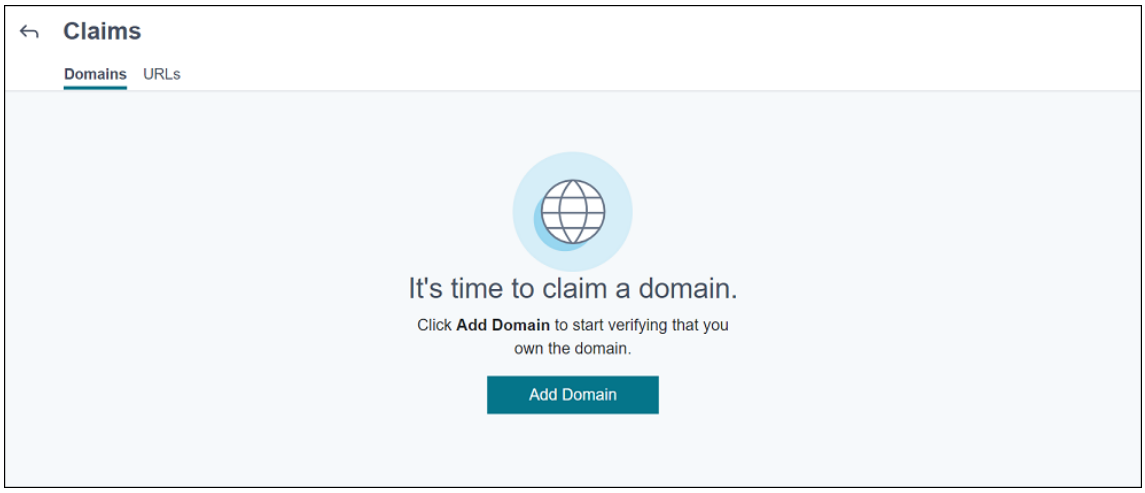
  Citrix migrated all existing AutoDiscovery records to Citrix Cloud without a disruption in service. The migrated records don't automatically appear in the new console. You must reclaim domains in the new AutoDiscovery service to prove ownership. For more information, see CTX312339.
- Before starting using the AutoDiscovery service for your Citrix Endpoint Management deployments, verify and claim your domain. You can claim up to 10 domains. The claim associates the verified domain with the AutoDiscovery service. To claim more than 10 domains, open an SRE ticket or contact Citrix Technical Support.
- Use the MAM Port setting instead of NetScaler Gateway FQDN to direct MAM traffic to your data center. If you enter a fully qualified domain name along with the port of your NetScaler Gateway, the client device uses the configuration from the **MAM Port** setting.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

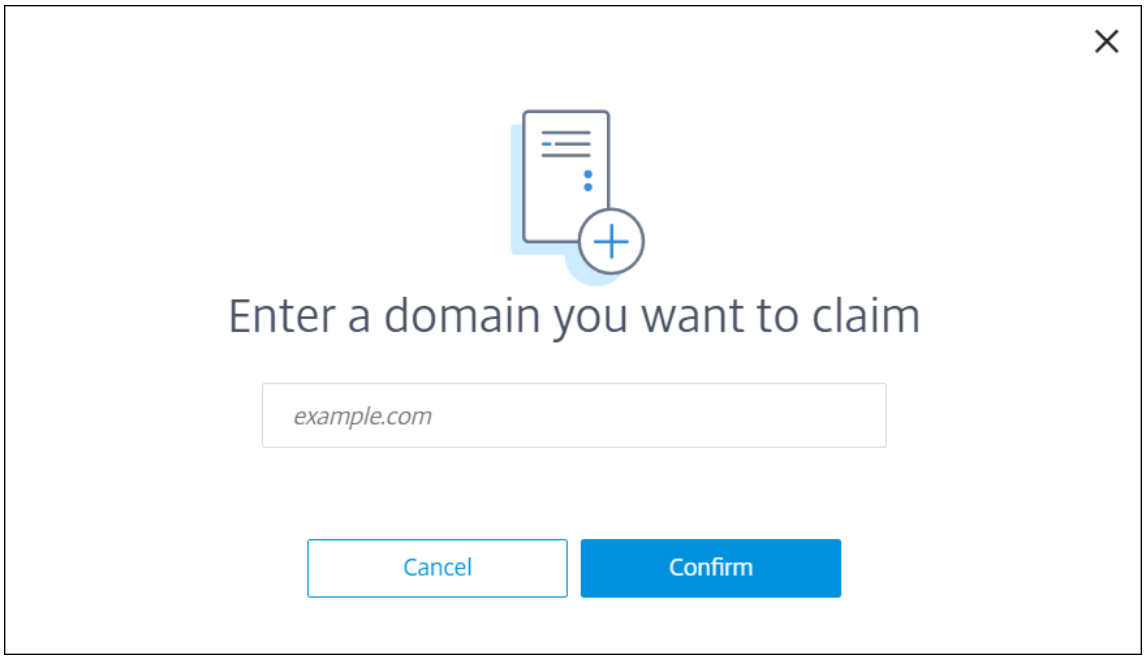
- If an ad blocker prevents the site from opening, make sure that you disable the ad blocker for the entire website.

Claim a domain

1. On the **Claims > Domains** tab, click **Add Domain**.

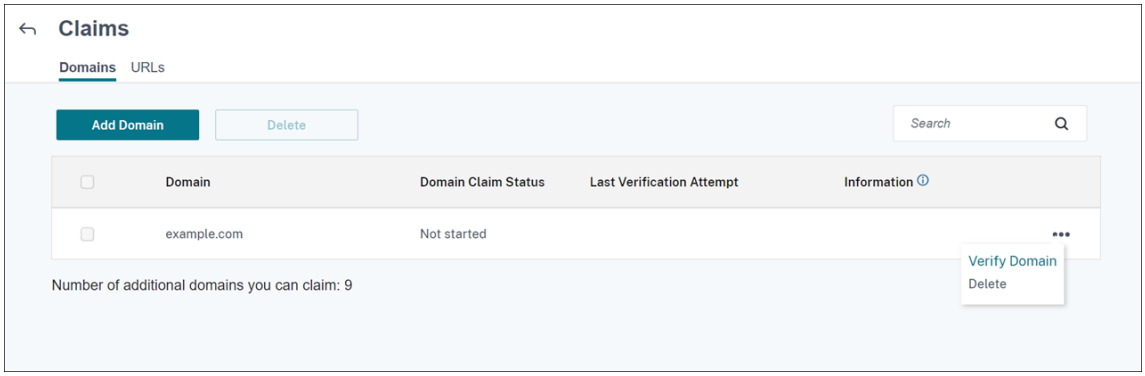


2. In the dialog box that appears, enter the domain name of your Citrix Endpoint Management environment and then click **Confirm**. Your domain appears in **Claims > Domains**.

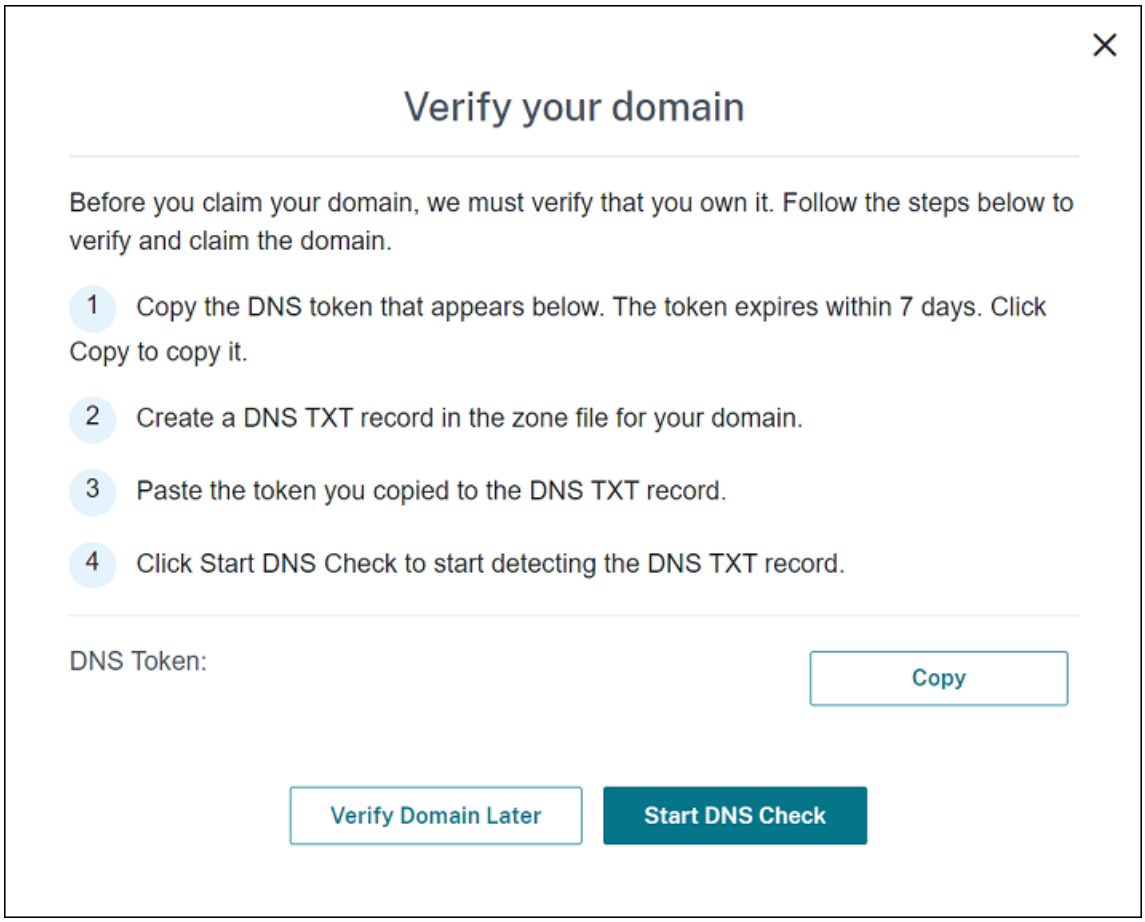


3. On the domain you added, click the ellipsis menu and select **Verify Domain** to start the verification process. The **Verify your domain** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. On the **Verify your domain** page, follow the instructions to verify that you own the domain.

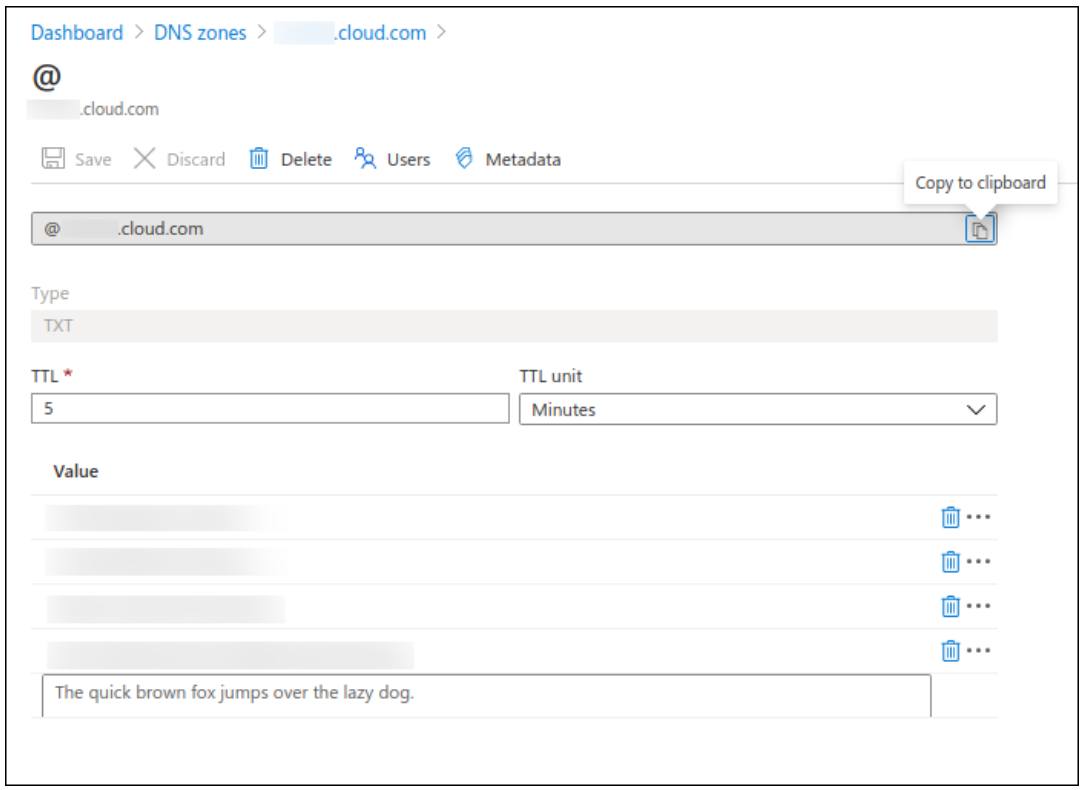


   a) Click **Copy** to copy the DNS token to the clipboard.

   b) Create a DNS TXT record in the zone file for your domain. To do so, go to your domain hosting provider portal and add the DNS token you copied.

      The following screenshot shows a domain hosting provider portal. Your portal might look different.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



c) In Citrix Cloud, on the **Verify your domain** page, click **Start DNS Check** to start detecting your DNS TXT record. If you want to verify the domain later, click **Verify Domain Later**.

The verification process generally takes about an hour. However, it can take up to two days to return a response. It is OK for you to log out and log in again during the status check.

After the configuration completes, the status of your domain changes from **Pending** to **Verified**.

5. After you claim your domain, provide information about the AutoDiscovery service. Click the ellipsis menu on the domain that you added and then click **Add Citrix Endpoint Management Info**. The **AutoDiscovery Service Information** page appears.
6. Enter the following information and then click **Save**.

   - **Citrix Endpoint Management Server FQDN:** Enter the fully qualified domain name of the Citrix Endpoint Management server. For example: `example.xm.cloud.com`. This setting is used for MDM and MAM traffic control.
   - **NetScaler Gateway FQDN:** Enter the fully qualified domain name of NetScaler Gateway, in the form FQDN or FQDN:port. For example: `example.com`. This setting is used to direct MAM traffic to your data center. For MDM-only deployments, leave this field blank.

     > **Note:**
     >
     > Citrix recommends that you use the **MAM Port** setting instead of **NetScaler Gateway**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **FQDN** to control MAM traffic. If you enter a fully qualified domain name along with the port of your NetScaler Gateway, the client device uses the configuration from the **MAM Port** setting.

- **Instance Name:** Enter the instance name of the Citrix Endpoint Management server you configured earlier. If you are unsure about your instance name, leave the default value **zdm**.
- **MDM Port:** Enter the port used for MDM control traffic and MDM enrollment. For cloud-based services, the default is 443.
- **MAM Port:** Enter the port used for MAM control traffic, MAM enrollment, iOS enrollment, and app enumeration. For cloud-based services, the default is 8443.

Request AutoDiscovery for Windows devices

If you plan to enroll Windows devices, do the following:

1. Contact Citrix Support and create a support request to enable Windows AutoDiscovery.
2. Get a publicly signed, non-wildcard SSL certificate for `enterpriseenrollment.mycompany.com`. The `mycompany.com` portion is the domain that has the accounts that users use to enroll. Attach the SSL certificate in .pfx format and its password to the support request created in the previous step.

   To use more than one domain to enroll Windows devices, you can also use a multi-domain certificate with the following structure:

   - A SubjectDN with a CN that specifies the primary domain it serves (for example, enterpriseenrollment.mycompany1.com).
   - The appropriate SANs for the remaining domains (for example, enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com, and so on).
3. Create a canonical name (CNAME) record in your DNS and map the address of your SSL certificate (enterpriseenrollment.mycompany.com) to autodisc.xm.cloud.com.

   When a Windows device user enrolls using a UPN, the Citrix enrollment server:

   - Provides the details of your Citrix Endpoint Management server.
   - Instructs the device to request a valid certificate from Citrix Endpoint Management.

At this point, you can enroll all supported devices. Go to the next section to prepare to deliver resources to devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Integrate with Azure AD Conditional Access

You can configure Citrix Endpoint Management to apply Azure AD Conditional Access support to Office 365 applications. This feature lets you deploy the Zero Trust methodology to device users when deploying Office 365 applications. You can use device state, risk score, location, and device protections to apply automated actions and define access to the Office 365 applications on managed Android Enterprise and iOS devices.

To enforce Azure AD device compliance, you must configure Conditional Access policies for individual Office 365 applications. You can restrict user access to specific Office 365 applications on non-managed and non-compliant devices and allow access to individual applications only on managed and compliant devices.

Prerequisites

- For this integration, you must have a valid Azure AD premium subscription, including Intune and Microsoft Office 365 licenses.
- Citrix Secure Hub version 21.4.0 and later
- Configure Azure AD as an identity provider (IdP) in Citrix Cloud, and then set Citrix identity as the IdP type for Citrix Endpoint Management. For information, see Authentication with Azure Active Directory through Citrix Cloud.
- Consent to the Citrix multitenant AAD application to allow mobile applications to authenticate with the AAD client app. Only required if the Azure Global Administrator set the value for **Users can register applications** to **No**. Configure this setting in the Azure portal under **Azure Active Directory > Users > User Settings**. To provide consent, see Configure Citrix Endpoint Management for Azure AD Compliance Management.
- Install the Microsoft Authenticator application on the device before starting the Azure AD device registration process.
- For the Android Enterprise platform, configure a web browser app as the required public store app.
- Disable the **Security defaults** setting in the Azure AD console. When you start Azure AD configuration, you replace security defaults with more granular Azure AD Conditional Access policies. For more information about security defaults, see the Microsoft documentation.

Configure device compliance through Azure AD Conditional Access policies

The general steps to configure device compliance through Azure AD Conditional Access policies are as follows:

1. **Citrix Endpoint Management configuration:**

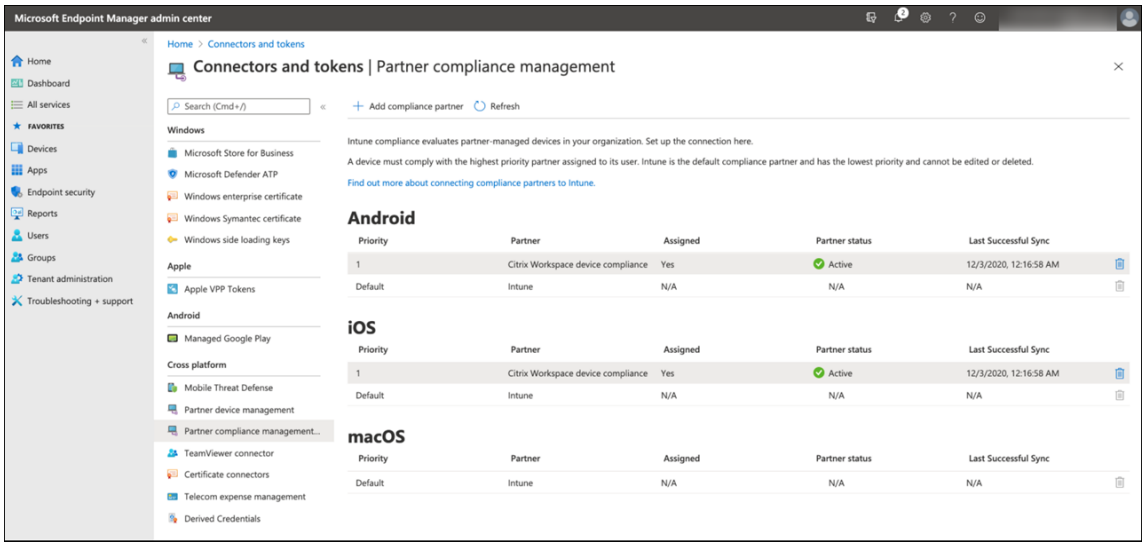
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- In the Microsoft Endpoint Manager admin center, add **Citrix Workspace device compliance** as the compliance partner for each device platform and assign user groups.
- In Citrix Endpoint Management, synchronize information from the Microsoft Endpoint Manager admin center.

2. **Azure AD configuration:** In the Azure AD portal, set Conditional Access policies for individual Office 365 apps.
3. **Citrix Endpoint Management configuration:** After configuring Conditional Access policies for Office 365 apps, add the Microsoft Authenticator app and Office 365 apps as public app store apps in Citrix Endpoint Management. Assign these public apps to the delivery group and set them as required apps.

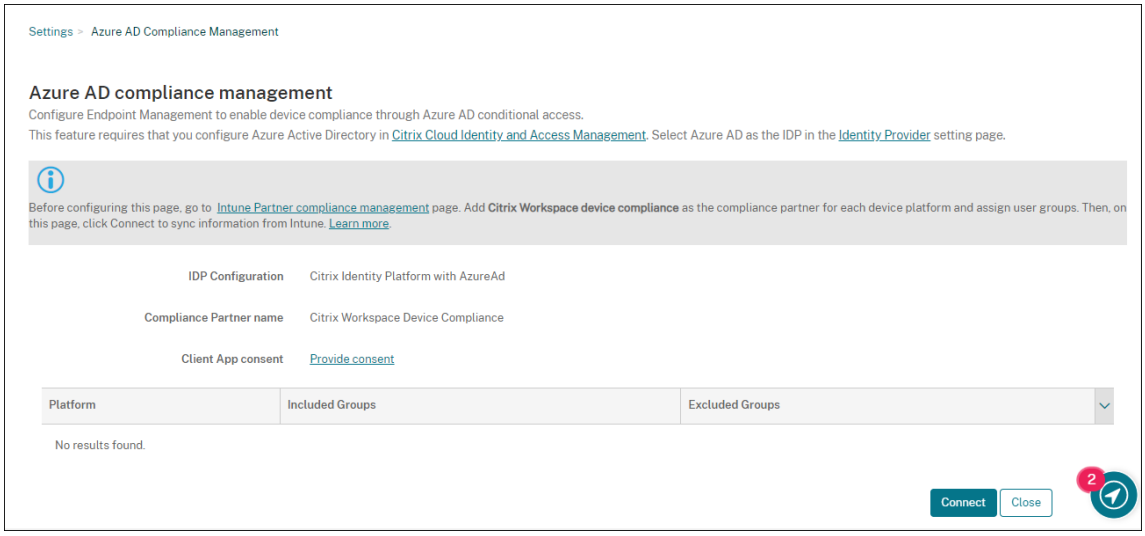
Configure Citrix Endpoint Management for Azure AD compliance management

1. Sign in to the Microsoft Endpoint Manager admin center and navigate to **Tenant administration > Connectors and tokens > Device compliance management**. Click **Add compliance partner** and choose **Citrix Workspace device compliance** as the compliance partner for each device platform. Then assign user groups.



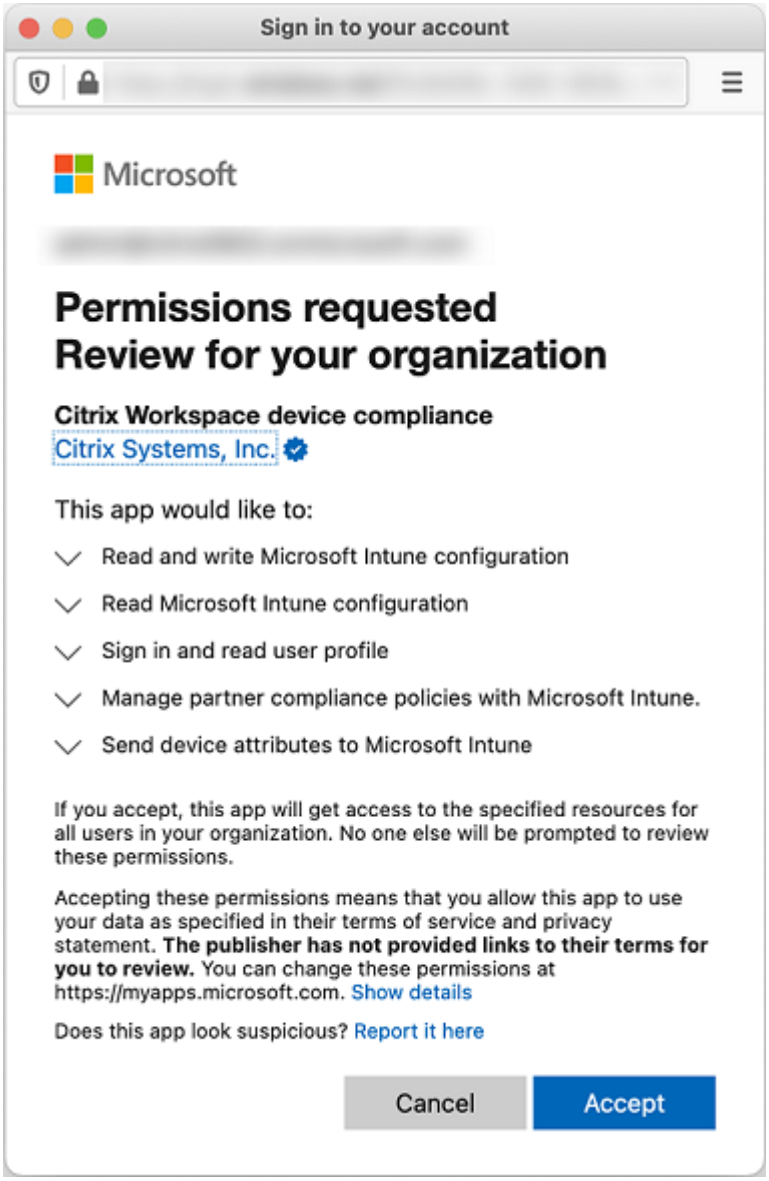
2. In Citrix Endpoint Management, go to **Settings > Azure AD compliance management**.
3. Optionally, set global consent so that users don't need to provide consent on each device. Next to **Client App consent**, click **Provide consent**. Enter your global admin Azure AD credentials and follow the prompts to provide global consent for the client apps.
4. Click **Connect** to sync information from the Microsoft Endpoint Manager admin center.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



A dialog box prompts you to accept the permissions for this configuration. Click **Accept**. After the configuration completes, synchronized device platforms appear in the list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure Conditional Access policies in Azure AD

In the Azure AD portal, configure Conditional Access policies for Office 365 apps to enforce device compliance. Go to **Devices > Conditional Access > Policies > New policy**. For more information, see the Microsoft documentation.

To configure device compliance for Intune managed apps:

- Configure Intune managed apps for delivery to devices
- Require approved client apps
- Require app protection policy and an approved client app for cloud app access

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure apps in Citrix Endpoint Management

After configuring Conditional Access policies for Office 365 apps, add the Microsoft Authenticator app and Office 365 apps as public app store apps in Citrix Endpoint Management. Assign these public apps to the delivery group and set them as required apps. For information, see Add a public app store app.

User authentication workflow

1. Users who enrolled devices with On-premises Active Directory (AD) and later integrated with Citrix identity provider using Microsoft Azure Active Directory (AAD) do not need to re-enroll. You can synchronize accounts from your on-premises Active Directory to Microsoft Azure Active Directory. For more information, see Prepare your Active Directory and Azure AD.
2. Citrix Endpoint Management pushes Microsoft Authenticator and configured Office 365 apps to a device as required apps. If you configured a web browser app as the required public store app for the Android platform, Citrix Endpoint Management pushes it to the user device as well.
3. Citrix Secure Hub automatically installs and displays all apps managed through Citrix Endpoint Management.
4. When a user tries to sign in to any available Office 365 app, the device prompts the user to tap the **Azure AD registration** link to start the registration process.
5. After the user taps the registration link, the Microsoft authenticator app opens. The user enters Azure AD credentials and agrees to the device enrollment terms. Then the Microsoft authenticator app closes and Citrix Secure Hub reopen.
6. Citrix Secure Hub displays a message that Azure AD device registration is complete. The user can now use Microsoft apps to access their cloud resources.

   After the registration completes, Azure AD marks the device as managed and compliant in the console.

Default device policies and mobile productivity apps

If you onboard starting with Citrix Endpoint Management 19.5.0 or later, we preconfigure a few device policies and mobile productivity apps. That configuration enables you to:

- Immediately deploy basic functionality to devices
- Start with the recommended baseline configurations for a secure workspace

For the Android, Android Enterprise, iOS, macOS, and Windows Desktop/Tablet platforms, your site has these preconfigured device policies:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Passcode device policy:** The Passcode device policy is **On**, with all default passcode settings enabled.
- **App inventory device policy:** The App inventory device policy is **On**.
- **Restrictions device policy:** The Restrictions device policy is **On**, with all default restrictions settings enabled.

Those policies are in the **AllUsers** delivery group, which has all Active Directory and local users. We recommend that you use the AllUsers delivery group only for initial testing. Then, create your delivery groups and disable the AllUsers delivery group. You can reuse the preconfigured device policies and apps in your delivery groups.

All Citrix Endpoint Management device policies are documented under Device policies. That article includes information about how to use the console to edit device policies. For information about some commonly used device policies, see Device policies and Use Case Behavior.

For the iOS and Android platforms, your site has these preconfigured mobile productivity apps:

- **Citrix Secure Mail**
- **Citrix Secure Web**
- **Citrix Files**

Those apps are in the **AllUsers** delivery group.

For more information, see About mobile productivity apps.

Continue your Citrix Endpoint Management configuration

After you complete the basic setup for device enrollment, how you configure Citrix Endpoint Management varies widely based on your use cases. For example:

- What are your security requirements and how do you want to balance those requirements with user experience?
- Which device platforms do you support?
- Do users own their devices or use corporate-owned devices?
- What device policies do you want to push to devices?
- What types of apps do you provide users?

This section helps you navigate through the many configuration choices by directing you to the articles in this documentation set.

As you complete configuration in third-party sites, make note of the information and its location, for reference when you configure Citrix Endpoint Management console settings.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Security and authentication. Citrix Endpoint Management uses certificates to create secure connections and authenticate users. Citrix provides wildcard certificates for your Citrix Endpoint Management instance.
  - For a discussion of authentication components and recommended configurations by security level, see the "Advanced concepts"article, Authentication. See also, Security and user experience.
  - For an overview of the authentication components used during Citrix Endpoint Management operations, see Certificates and authentication.
  - You can choose from the following types of authentication. Configuring authentication includes tasks in the Citrix Endpoint Management and NetScaler Gateway consoles.
    - Domain or domain plus security token authentication
    - Client certificate or certificate plus domain authentication
  - To deliver certificates to users, configure:
    - PKI entities
    - Credential providers
  - Device enrollment security modes. Device enrollment security modes specify the credential types and use enrollment steps required for users to enroll their devices in Citrix Endpoint Management. For information, see Configure enrollment security modes.
  - To allow users to authenticate with Azure Active Directory credentials, see Authenticate with Azure Active Directory through Citrix Cloud.
- Device enrollment
  - Programs are available to enroll large numbers of devices:
    - Deploy devices through Apple Deployment Program
    - Bulk enrollment of Apple devices
    - Enroll Windows devices in bulk
  - To enroll Android devices, create an Android Enterprise administrator account. See Android Enterprise. Or, see Legacy Android Enterprise for Google Workspace Customers.
  - You can use enrollment invitations or send notifications for enrollment.
    - Enrollment invitations.
    - Notifications.
  - For more information about enrollment, see Device management and articles under that node.
- Device policies and management

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - Device (MDM) policies. All Citrix Endpoint Management device policies are documented under Device policies. For information about some commonly used device policies, see Device Policies and Use Case Behavior.
  - Client properties. Client properties have information that is provided directly to Citrix Secure Hub on user devices. See Client properties and Citrix Endpoint Management client properties.
  - Delivery groups. For a sample use case related to delivery groups, see User Communities and Add a delivery group.

- Prepare apps for deployment
  - For information about the apps supported by Citrix Endpoint Management, see Add apps.
  - You can manage iOS app licensing by using Apple Volume Purchase. For more information, see Apple Volume Purchase.
  - You can use Citrix Endpoint Management to deploy iBooks that you obtain through Apple Volume Purchase. See Add media.
  - Citrix provides mobile productivity apps, including Citrix Secure Mail and Citrix Secure Web. See About mobile productivity apps.
  - As an alternative to Citrix Secure Mail, you can deliver native mail to devices. See:
    * Email strategy
    * Citrix Endpoint Management connector for Exchange ActiveSync
    * NetScaler Gateway connector for Exchange ActiveSync
  - To allow users to securely transfer docs and data to Microsoft Office 365 apps, see Allowing Secure Interaction with Office 365 Apps and Office device policy.
  - For general information about app policies, see App Policies and Use Case Scenario.
  - The MDX Toolkit is an app wrapping technology that prepares enterprise apps for secure deployment with Citrix Endpoint Management. The MAM SDK replaces the MDX Toolkit. The MDX Toolkit is scheduled to reach EOL in July 2023.

    For information about the MAM SDK, see MAM SDK overview.
  - For more information about apps, see other articles under Add apps.

- The Role-Based Access Control (RBAC) feature in Citrix Endpoint Management lets you assign predefined roles, or sets of permissions, to users and groups. These permissions control the level of access users have to system functions. For information, see Configure roles with RBAC.
- You create automated actions in Citrix Endpoint Management to specify the action to take in reaction to events, certain settings, or the presence of apps on user devices. For information, see Automated actions.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Certificates and authentication

February 23, 2024

Several components play a role in authentication during Citrix Endpoint Management operations:

- **Citrix Endpoint Management:** The Citrix Endpoint Management server is where you define enrollment security and the enrollment experience. Options for onboarding users include:
  - Whether to make the enrollment open for all or by invitation only.
  - Whether to require two-factor authentication or three-factor authentication. Citrix Endpoint Management client properties allow you to enable Citrix PIN authentication and configure the PIN complexity and expiration.
- **NetScaler Gateway:** NetScaler Gateway provides termination for micro VPN SSL sessions. NetScaler Gateway also provides network in-transit security, and lets you define the authentication experience used each time a user accesses an app.
- **Citrix Secure Hub:** Citrix Secure Hub and Citrix Endpoint Management work together in enrollment operations. Citrix Secure Hub is the entity on a device that talks to NetScaler Gateway: When a session expires, Citrix Secure Hub gets an authentication ticket from NetScaler Gateway and passes the ticket to the MDX apps. Citrix recommends certificate pinning, which prevents man-in-the-middle attacks. For more information, see this section in the Citrix Secure Hub article: Certificate pinning.

  Citrix Secure Hub also facilitates the MDX security container: Citrix Secure Hub pushes policies, creates a session with NetScaler Gateway when an app times out, and defines the MDX timeout and authentication experience. Citrix Secure Hub is also responsible for jailbreak detection, geolocation checks, and any policies you apply.
- **MDX policies:** MDX policies create the data vault on the device. MDX policies direct micro VPN connections back to NetScaler Gateway, enforce offline mode restrictions, and enforce client policies, such as time-outs.

Citrix Endpoint Management authenticates users to their resources using the following authentication methods:

- Mobile Device Management (MDM)
  - Cloud-hosted identity providers (IdPs)
  - Lightweight Directory Access Protocol (LDAP)
    - Invitation URL + Pin
    - Two-factor authentication
- Mobile application management (MAM)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - LDAP
  - Certificate
  - Security token

    MAM authentication requires NetScaler Gateway.

For other configuration details, see the following articles:

- Upload, update, and renew certificates
- NetScaler Gateway and Citrix Endpoint Management
- Domain or domain plus security token authentication
- Client certificate or certificate plus domain authentication
- PKI entities
- Credential providers
- APNs certificates
- SAML for single sign-on with Citrix Files
- Authentication with Azure Active Directory through Citrix Cloud
- Authentication with Okta through Citrix Cloud
- Authentication with an on-premises NetScaler Gateway through Citrix Cloud
- To authenticate to a Wi-Fi server, send a certificate to the devices: Network device policy
- To push a unique certificate not used for authentication, such as an internal root certificate authority (CA) certificate, or a specific policy: Credentials device policy

Certificates

Citrix Endpoint Management generates a self-signed Secure Sockets Layer (SSL) certificate during installation to secure the communication flows to the server. Replace the SSL certificate with a trusted SSL certificate from a well-known certificate authority.

Citrix Endpoint Management also uses its own Public Key Infrastructure (PKI) service or gets certificates from the CA for client certificates. All Citrix products support wildcard and Subject Alternative Name (SAN) certificates. For most deployments, you only need two wildcard or SAN certificates.

Client certificate authentication provides an extra layer of security for mobile apps and lets users seamlessly access HDX Apps. When client certificate authentication is configured, users type their Citrix PIN for single sign-on (SSO) access to Citrix Endpoint Management-enabled apps. Citrix PIN also simplifies the user authentication experience. Citrix PIN is used to secure a client certificate or save Active Directory credentials locally on the device.

To enroll and manage iOS devices with Citrix Endpoint Management, set up and create an Apple Push Notification Service (APNs) certificate from Apple. For steps, see APNs certificates.

The following table shows the certificate format and type for each Citrix Endpoint Management component:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management component	Certificate format	Required certificate type
NetScaler Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Root (NetScaler Gateway converts PFX to PEM automatically.
Citrix Endpoint Management	.p12 (.pfx on Windows-based computers)	SSL, SAML, APNs (Citrix Endpoint Management also generates a full PKI during the installation process.) **Important:** Citrix Endpoint Management doesn't support certificates with a .pem extension. To use a .pem certificate, split the .pem file into a certificate and key and import each into Citrix Endpoint Management.
StoreFront	PFX (PKCS #12)	SSL, Root

Citrix Endpoint Management supports client certificates with bit lengths of 4096 and 2048.

For NetScaler Gateway and Citrix Endpoint Management, it is recommended to get server certificates from a public CA, such as Verisign, DigiCert, or Thawte. You can create a Certificate Signing Request (CSR) from the NetScaler Gateway or the Citrix Endpoint Management configuration utility. After you create the CSR, you submit it to the CA for signing. When the CA returns the signed certificate, you can install the certificate on NetScaler Gateway or Citrix Endpoint Management.

> **Important:**
>
> Requirements for trusted certificates in iOS, iPadOS, and macOS
>
> Apple has new requirements for TLS server certificates. Verify that all certificates follow the Apple requirements. See the Apple publication, https://support.apple.com/en-us/HT210176.
>
> Apple is reducing the maximum allowed lifetime of TLS server certificates. This change affects only server certificates issued after September 2020. See the Apple publication, https://support.apple.com/en-us/HT211025.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

LDAP authentication

Citrix Endpoint Management supports domain-based authentication for one or more directories that are compliant with the Lightweight Directory Access Protocol (LDAP). LDAP is a software protocol that provides access to information about groups, user accounts, and related properties. For more information, see Domain or domain plus security token authentication.

Identity provider authentication

You can configure an identity provider (IdP) through Citrix Cloud to enroll and manage user devices.

Supported use cases for IdPs:

- Azure Active Directory through Citrix Cloud
  - Workspace integration is optional
  - NetScaler Gateway configured for certificate-based authentication
  - Android Enterprise (Preview. Supports BYOD, fully managed devices, and enhanced enrollment profiles)
  - iOS for MDM+MAM and MDM enrollments
  - iOS and macOS for Apple Business Manager enrollments
  - Legacy Android (DA)

  Auto enrollment features such as the Apple School Manager are currently not supported.
- Okta through Citrix Cloud
  - Workspace integration is optional
  - NetScaler Gateway configured for certificate-based authentication
  - Android Enterprise (Preview. Supports BYOD, fully managed devices, and enhanced enrollment profiles)
  - iOS for MDM+MAM and MDM enrollments
  - iOS and macOS for Apple Business Manager enrollments
  - Legacy Android (DA)

  Auto enrollment features such as the Apple School Manager are currently not supported.
- On-premises NetScaler Gateway through Citrix Cloud
  - NetScaler Gateway configured for certificate-based authentication
  - Android Enterprise (Preview. Supports BYOD, fully managed devices, and enhanced enrollment profiles)
  - iOS for MDM+MAM and MDM enrollments

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - Legacy Android (DA)
    Auto enrollment features such as the Apple Deployment Program are currently not supported.

Upload, update, and renew certificates

September 6, 2025

We recommend that you list the certificates needed for your Citrix Endpoint Management deployment. Use the list to track the certificate expiration dates and passwords. This article helps you administer certificates throughout their lifespan.

Your environment might include the following certificates:

- Citrix Endpoint Management server
  - SSL Certificate for MDM FQDN (Needed if you migrated from XenMobile Server to Citrix Endpoint Management. Otherwise, Citrix manages this certificate.)
  - SAML Certificate (for Citrix Files)
  - Root and Intermediate CA Certificates for the preceding certificates and any other internal resources (StoreFront/Proxy, and so on)
  - APNs Certificate for iOS Device Management
  - PKI User Certificate for connectivity to PKI (required if your environment requires certificate-based authentication)
- MDX Toolkit
  - Apple Developer Certificate
  - Apple Provisioning Profile (per application)
  - Apple APNs Certificate (for use with Citrix Secure Mail)
  - Android Keystore File

  The MAM SDK doesn't wrap apps, so it doesn't require a certificate.
- NetScaler Gateway
  - SSL Certificate for MDM FQDN
  - SSL Certificate for Gateway FQDN
  - SSL Certificate for ShareFile SZC FQDN
  - SSL Certificate for Exchange Load Balancing (offload configuration)
  - SSL Certificate for StoreFront Load Balancing
  - Root and Intermediate CA Certificates for the preceding certificates

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The client device must have the required root/intermediate certificate to establish trust with the certificate authority who issued the server certificate. Otherwise, you might receive SSL Error 61. To resolve the issue:
>
> 1. Download or get the SSL root/intermediate certificate file (.crt or .cer) issued by your SSL certificate provider. Usually the root/intermediate/server certificate is present in the certificate bundle provided by your SSL service provider.
> 2. Install the root/intermediate certificate on the client device.
> 3. If an antivirus is installed on the client device, make sure the antivirus trusts the certificate.

Upload certificates

Each certificate you upload has an entry in the Certificates table, including a summary of its contents. When you configure PKI integration components that require a certificate, choose a server certificate to satisfy the criteria. For example, you might want to configure Citrix Endpoint Management to integrate with your Microsoft certificate authority (CA). The connection to the Microsoft CA must be authenticated by using a client certificate.

Citrix Endpoint Management might not have the private key for a given certificate. Likewise, Citrix Endpoint Management might not require a private key for uploaded certificates.

This section provides general procedures for uploading certificates. For details about creating, uploading, and configuring client certificates, see Client certificate or certificate plus domain authentication.

You have two options for uploading certificates:

- Upload the certificates to the console individually.
- Do a bulk upload of certificates using the REST API. This option is available for iOS devices only.

When uploading certificates to the console, you can:

- Import a keystore. Then, you identify the entry in the keystore repository you want to install, unless you are uploading a PKCS #12 format.
- Import a certificate.

You can upload the CA certificate (without the private key) that the CA uses to sign requests. You can also upload an SSL client certificate (with the private key) for client authentication.

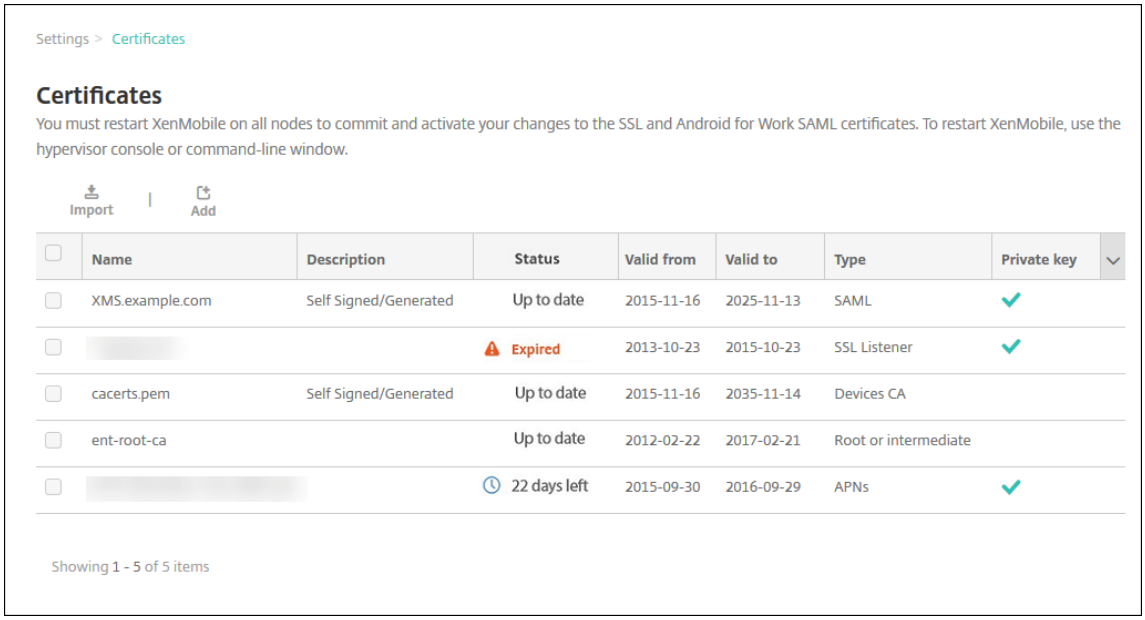
When configuring the Microsoft CA entity, you specify the CA certificate. You select the CA certificate from a list of all server certificates that are CA certificates. Likewise, when configuring client authentication, you can select from a list of all the server certificates for which Citrix Endpoint Management has the private key.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To import a keystore

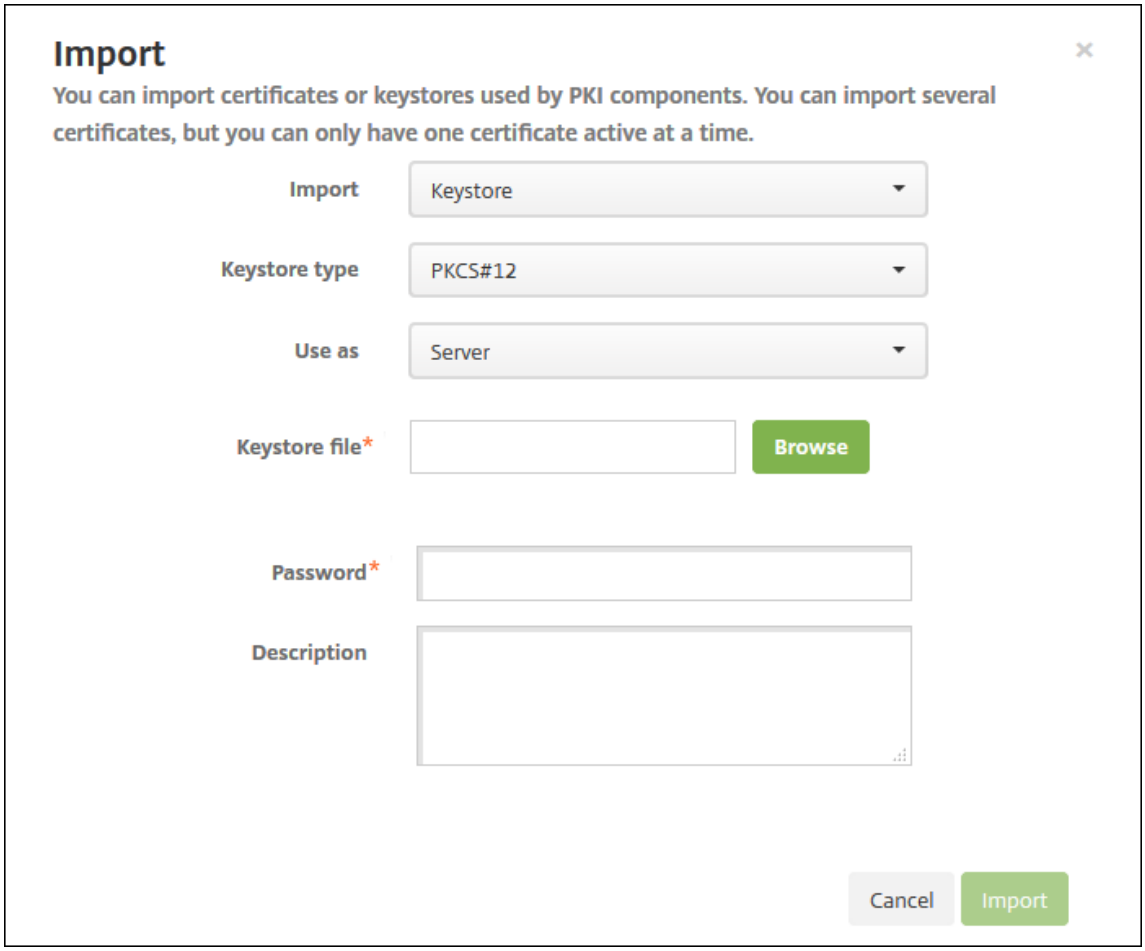
A keystore is a repository of security certificates. By design, keystores can have many entries. When loading from a keystore, you must specify the entry alias that identifies the entry you want to load. If you don't specify an alias, the first entry from the store loads. Because PKCS #12 files usually have only one entry, the alias field doesn't appear when you select PKCS #12 as the keystore type.

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console. Use the search bar to find and open the **Certificates** setting.



2. Click **Import**. The **Import** dialog box appears.
3. Configure these settings:
    - **Import:** Select **Keystore**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Keystore type:** Click **PKCS #12** in the drop-down list.
- **Use as:** In the list, click how you plan to use the certificate. The available options are:
  - **Server:** Server certificates are certificates used functionally by Citrix Endpoint Management. You upload server certificates to the Citrix Endpoint Management web console. Those certificates include CA certificates, RA certificates, and certificates for client authentication with other components of your infrastructure. Also, you can use server certificates as storage for certificates you want to deploy to devices. This use especially applies to CAs used to establish trust on the device.
  - **SAML:** Security Assertion Markup Language (SAML) certification allows you to provide SSO access to servers, websites, and apps.
  - **APNs:** APNs certificates from Apple enable Mobile Device Management via the Apple Push Network.
  - **SSL Listener:** The Secure Sockets Layer (SSL) Listener notifies Citrix Endpoint Management of SSL cryptographic activity.
- **Keystore file:** Browse to find the keystore you want to import. The keystore is a .p12 or .pfx file. Select the file and click **Open**.
- **Password:** Type the password assigned to the certificate.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Description:** Optionally, type a description for the keystore to help you distinguish it from your other keystores.

4. Click **Import**. The keystore is added to the Certificates table.

To import a certificate

When importing a certificate, Citrix Endpoint Management tries to construct a certificate chain from the input. Citrix Endpoint Management imports all certificates in a chain to create a server certificate entry for each certificate. This operation only works if the certificates in the file or keystore entry do form a chain. Each subsequent certificate in the chain must be the issuer of the previous certificate.

You can add an optional description for the imported certificate. The description only attaches to the first certificate in the chain. You can update the description of the remaining certificates later.

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console. Use the search bar to find and open the **Certificates** setting.
2. On the **Certificates** page, click **Import**. The **Import** dialog box appears. Configure the following:
   - **Import:** click **Certificate**.
   - **Use as:** Select how you plan to use the certificate. The available options are:
     - **Server:** Server certificates are certificates used functionally by Citrix Endpoint Management. You upload server certificates to the Citrix Endpoint Management web console. Those certificates include CA certificates, RA certificates, and certificates for client authentication with other components of your infrastructure. Also, you can use server certificates as storage for certificates you want to deploy to devices. This option especially applies to CAs used to establish trust on the device.
     - **SAML:** Security Assertion Markup Language (SAML) certification allows you to provide single sign-on (SSO) access to servers, websites, and apps.
     - **SSL Listener:** The Secure Sockets Layer (SSL) Listener notifies Citrix Endpoint Management of SSL cryptographic activity.
   - **Certificate import:** Browse to find the certificate you want to import. Select the file and click **Open**.
   - **Private key file:** Browse to find an optional private key file for the certificate. The private key is used for encryption and decryption along with the certificate. Select the file and click **Open**.
   - **Description:** Type a description for the certificate, optionally, to help you identify it from your other certificates.
3. Click **Import**. The certificate is added to the Certificates table.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Upload certificates in bulk using the REST API Sometimes uploading certificates one at a time isn't reasonable. In those cases, do a bulk upload of certificates using the REST API. This method supports certificates in the .p12 format. For more information about the REST API, see REST APIs.

1. Rename each of the certificate files in the format `device_identity_value.p12`. The `device_identity_value` can be the IMEI, Serial Number, or MEID of each device.

   As an example, you choose to use serial numbers as your identification method. One device has a serial number `A12BC3D4EFGH`, so name the certificate file you expect to install on that device `A12BC3D4EFGH.p12`.

2. Create a text file to store the passwords for the .p12 certificates. In that file, type the device identifier and password for each device on a new line. Use the format `device_identity_value=password`. See the following:

   ```
   A12BC3D4EFGH.p12=password1!
   A12BC3D4EFIJ.p12=password2@
   A12BC3D4EFKL.p12=password3#
   ```

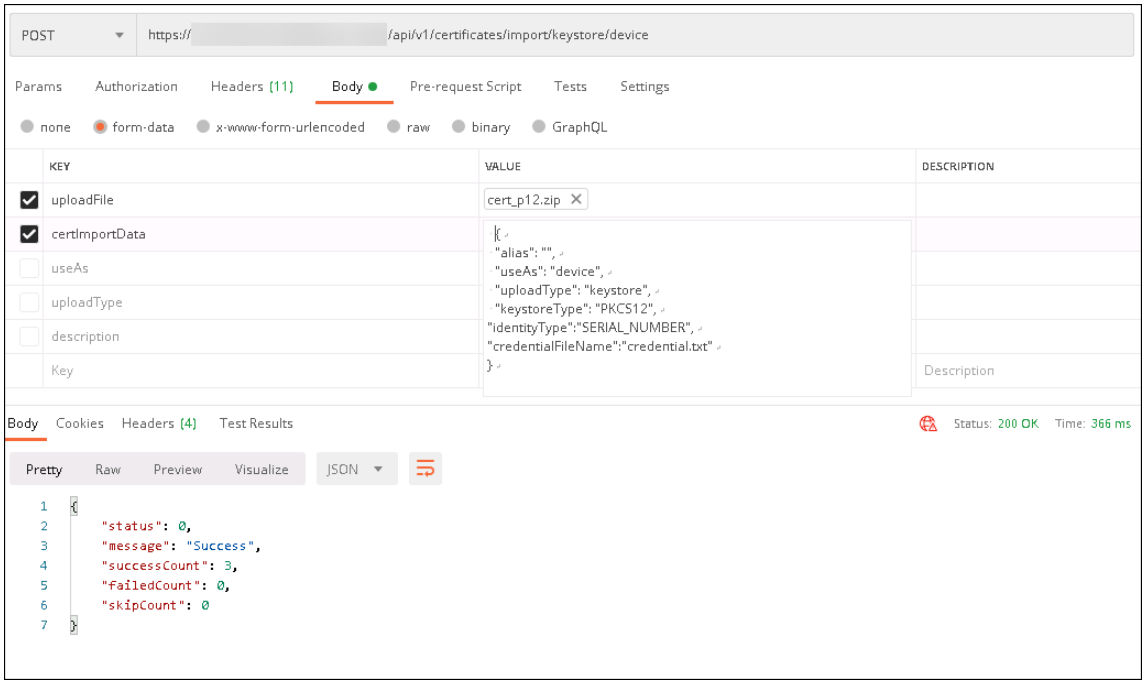
3. Pack all certificates and the text file that you created into a .zip file.

4. Launch your REST API client, log in to Citrix Endpoint Management, and get an authentication token.

5. Import your certificates and make sure that you put the following in the message body:

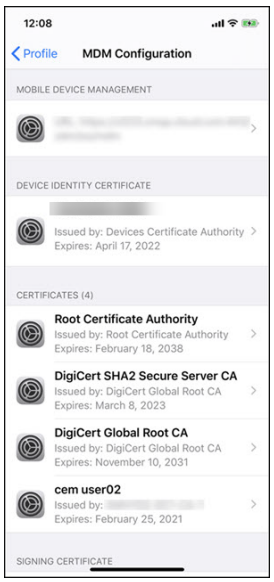
   ```
   {

       "alias": "",
       "useAs": "device",
       "uploadType": "keystore",
       "keystoreType": "PKCS12",
       "identityType":"SERIAL_NUMBER",         # identity type can be
          "SERIAL_NUMBER","IMEI","MEID"
       "credentialFileName":"credential.txt"    # The credential file
          name in .zip
    }
   ```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

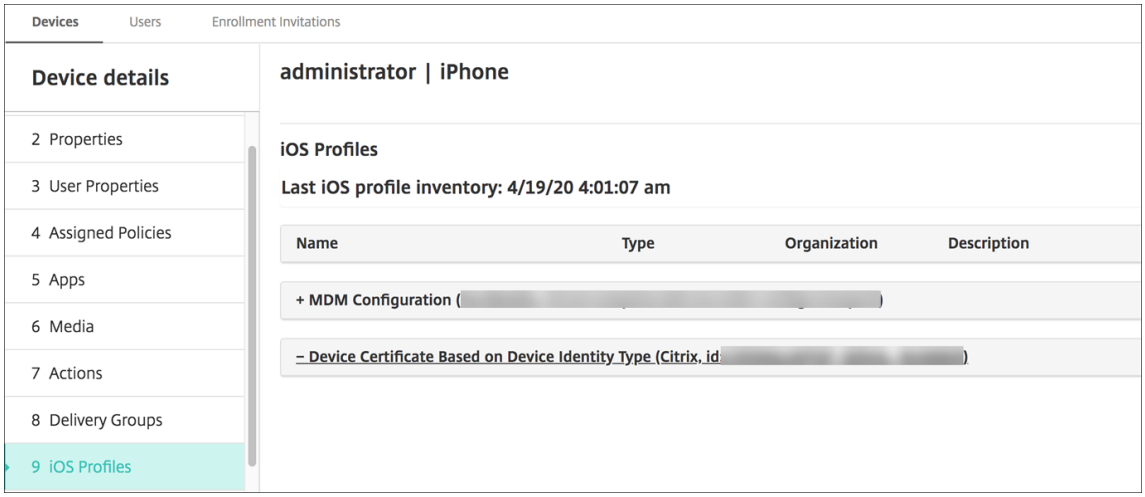


6. Create a VPN policy with the credential type **Always on IKEv2** and the device authentication method **Device Certificate Based on Device Identity**. Select the **Device identity type** you used in your certificate file names. See VPN device policy.

7. Enroll an iOS device and wait for the VPN policy to deploy. Confirm the certificate installation by checking the MDM configuration on the device. You can also check the device details in the Citrix Endpoint Management console.



© 1997–2025 Citrix Systems, Inc. All rights reserved.



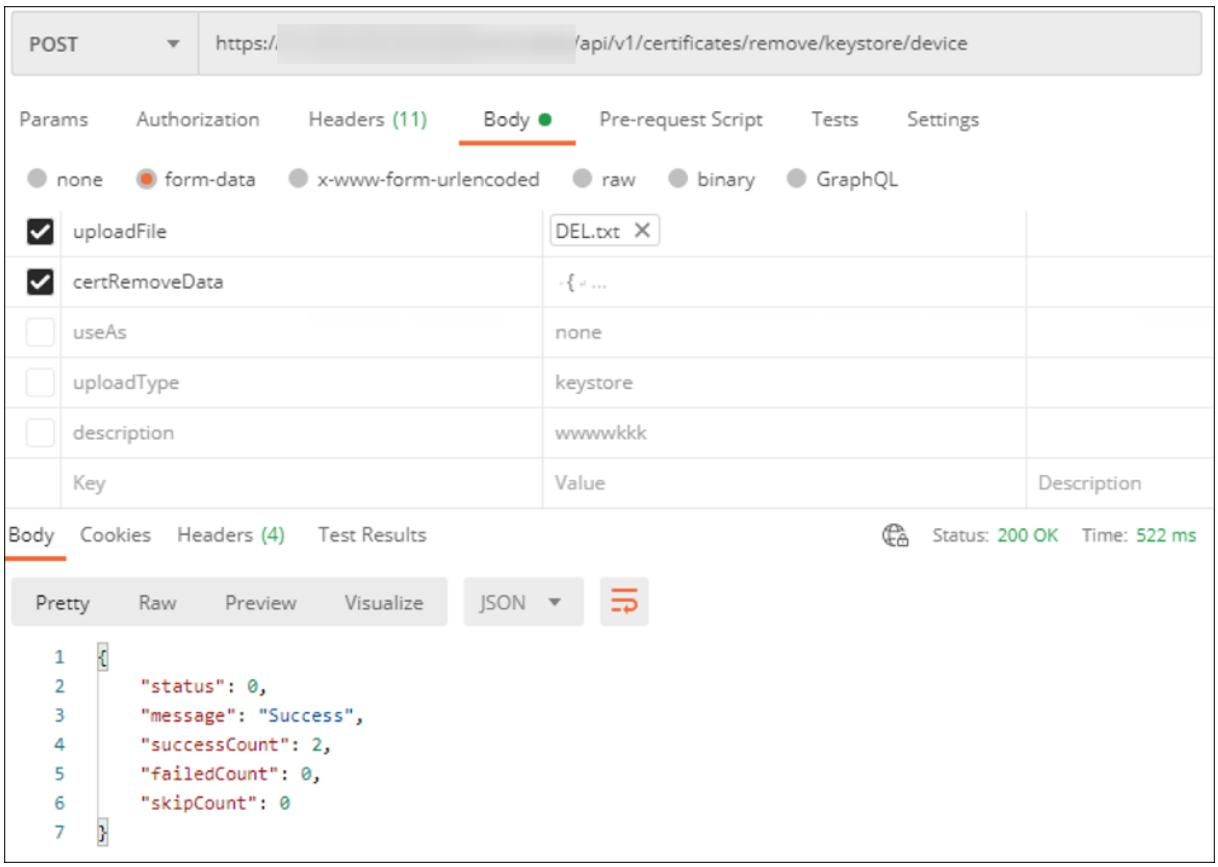
You can also delete certificates in bulk by creating a text file with the `device_identity_value` listed for each certificate to delete. In the REST API, call the delete API and use the following request, replacing `device_identity_value` with the appropriate identifier:

```
```
{

    "identityType"="device_identity_value"
 }

```
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Update a certificate

Citrix Endpoint Management only allows one certificate per public key to exist in the system at a time. If you try to import a certificate for the same key pair as an already imported certificate you can:

- Replace the existing entry.
- Delete the entry.

After you upload a new certificate to replace an old certificate, you can't delete the old certificate. When you configure the PKI Entities setting, both certificates exist in the **SSL client certificate** menu. The newer certificate is lower in the list than the old certificate.

To update your certificates

1. Create a replacement certificate by following the steps in Client certificate or certificate plus domain authentication.

   > **Important:**
   >
   > Do not use the option to create a certificate with the existing private key. When you create

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> a certificate to update an expiring certificate, the private key must be new as well.

2. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console. Use the search bar to find and open the **Certificates** setting.
3. In the **Import** dialog box, import the new certificate.

When you update a server certificate, components using the previous certificate automatically switch to using the new certificate. Likewise, if you have deployed the server certificate on devices, the certificate automatically updates on the next deployment.

To update an APNs certificate, do the steps to create a certificate, then go to the Apple Push Certificates Portal. For more information, see Renew an APNs certificate.

If your NetScaler Gateway is set up for SSL offload, make sure that you update your load balancer with the new cacert.pem.

> **Note:**
>
> If you have migrated from XenMobile on-prem to Citrix Endpoint Management, and you are updating your certificate, contact Citrix Support after completing the previous steps. You need to supply them with a copy of the new certificate (in PFX format), including the certificate password. Citrix Support updates the cloud NetScaler and reboot tenant nodes to finalize the certificate update process.

To update a PKI service certificate authority (CA)

You can request that Citrix Cloud Operations refresh or regenerate the internal PKI certificate authorities (CAs) in your Citrix Endpoint Management deployment. Open a Technical Support case for these requests.

```
When the new CAs are available, Cloud Operations lets you know that you
    can proceed with renewing the device certificates for your users.
```

Renew device certificates

If a certificate on a device expires, the certificate becomes invalid. You can no longer run secure transactions on your environment and you can't access Citrix Endpoint Management resources. The Certification Authority (CA) prompts you to renew your SSL certificate before the expiration date. Do the steps described previously to update the certificate, and then start a certificate renewal on enrolled devices.

For supported iOS, macOS, and Android devices, you can start certificate renewal through the security action, Certificate Renewal. You renew device certificates from the Citrix Endpoint Management

© 1997–2025 Citrix Systems, Inc. All rights reserved.

console or the Public REST API. For enrolled Windows devices, users must re-enroll their devices to receive a new device certificate authority (CA).

The next time that devices connect back to Citrix Endpoint Management, the Citrix Endpoint Management server issues new device certificates based on the new CA.

To renew device certificates by using the console

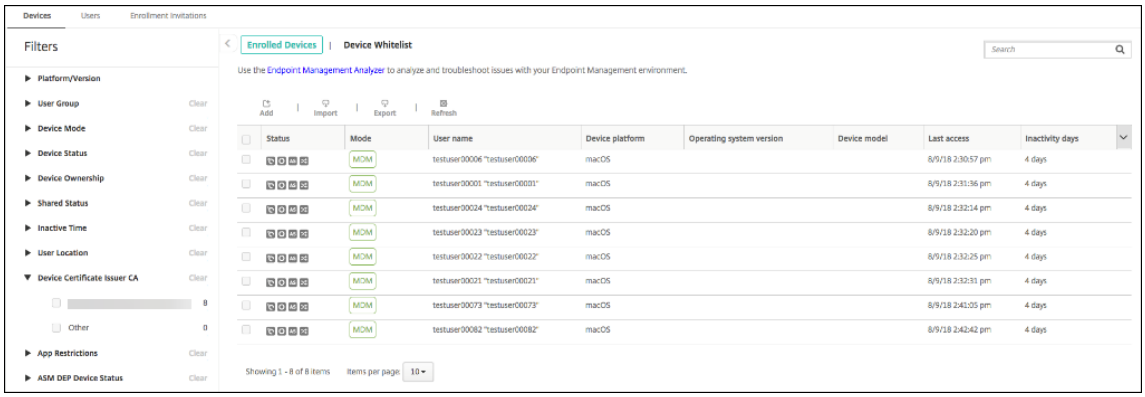
1. Go to **Manage > Devices** and select the devices for which you want to renew device certificates.
2. Click **Secure** and then click **Certificate Renewal**.

   Enrolled devices continue to work without disruption. Citrix Endpoint Management issues a device certificate when a device connects back to the server.

To query for the devices that are in a specific device certificate issuer CA group:

1. In **Manage > Devices**, expand the **Filters** pane.
2. In the **Filters** pane, expand **Device Certificate Issuer CA** and then select the issuer CAs that you want to renew.

   In the table of devices, the devices for the selected issuer CAs appear.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

To renew device certificates by using the REST API

Citrix Endpoint Management uses the following certificate authorities (CAs) internally for PKI: Root CA, device CA, and server CA. Those CAs are a logical group and have a group name. During Citrix Endpoint Management provisioning, the server generates three CAs and gives them the group name "default".

The CA issues the following APIs to manage and renew the device certificates. Already enrolled devices continue to work without disruption. Citrix Endpoint Management issues a device certificate when a device connects back to the server. For more information, download the Public API for REST Services PDF.

- Return a list of devices still using the old CA (see section 3.16.2 in the Public API for REST Services PDF)
- Renew Device Certificate (see section 3.16.58)
- Get all CA groups (see section 3.23.1)

APNs certificate for Citrix Secure Mail

Apple Push Notification Service (APNs) certificates expire every year. Be sure to create an APNs SSL certificate and update it in the Citrix portal before the certificate expires. If the certificate expires, users face inconsistency with Citrix Secure Mail push notifications. Also, you can no longer send push notifications for your apps.

APNs certificate for iOS device management

To enroll and manage iOS devices with Citrix Endpoint Management, set up and create an APNs certificate from Apple. If the certificate expires, users cannot enroll in Citrix Endpoint Management and you cannot manage their iOS devices. For details, see APNs certificates.

You can view the APNs certificate status and expiration date by logging on to the Apple Push Certificates Portal. Be sure to log on as the same user who created the certificate.

You also receive an email notification from Apple 30 and 10 days before the expiration date. The notification includes the following information:

```
1 The following Apple Push Notification Service certificate, created for
    Apple ID CustomerID will expire on Date. Revoking or allowing this
    certificate to expire will require existing devices to be re-
    enrolled with a new push certificate.
2
3 Please contact your vendor to generate a new request (a signed CSR),
    then visit https://identity.apple.com/pushcert to renew your Apple
    Push Notification Service certificate.
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
4
5  Thank You,
6
7  Apple Push Notification Service
```

MDX Toolkit (iOS distribution certificate)

An app that runs on a physical iOS device (other than apps in the Apple App Store) have these signing requirements:

- Sign the app with a provisioning profile.
- Sign the app with a corresponding distribution certificate.

To verify that you have a valid iOS distribution certificate, do the following:

1. From the Apple Enterprise Developer portal, create an explicit App ID for each app you plan to wrap with MDX. An example of an acceptable App ID is: `com.CompanyName.ProductName`.
2. From the Apple Enterprise Developer portal, go to **Provisioning Profiles > Distribution** and create an in-house provisioning profile. Repeat this step for each App ID created in the previous step.
3. Download all provisioning profiles. For details, see Wrapping iOS Mobile Apps.

To confirm that all Citrix Endpoint Management server certificates are valid, do the following:

1. In the Citrix Endpoint Management console, click **Settings > Certificates**.
2. Check that all certificates including APNs, SSL Listener, Root, and Intermediate certificates are valid.

Android keystore

The keystore is a file that has certificates used to sign your Android app. When your key validity period expires, users can no longer seamlessly upgrade to new versions of your app.

NetScaler Gateway

For details on how to handle certificate expiration for NetScaler Gateway, see How to handle certificate expiry on NetScaler in the Citrix Support Knowledge Center.

An expired NetScaler Gateway certificate prevents users from enrolling and accessing the Store. The expired certificate also prevents users from connecting to Exchange Server when using Citrix Secure Mail. Also, users cannot enumerate and open HDX apps (depending on which certificate expired).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The Expiry Monitor and Command Center can help you to track your NetScaler Gateway certificates. The Center notifies you when the certificate expires. These tools assist to monitor the following NetScaler Gateway certificates:

- SSL Certificate for MDM FQDN
- SSL Certificate for Gateway FQDN
- SSL Certificate for ShareFile SZC FQDN
- SSL Certificate for Exchange Load Balancing (offload configuration)
- SSL Certificate for StoreFront Load Balancing
- Root and Intermediate CA Certificates for the preceding certificates

NetScaler Gateway and Citrix Endpoint Management

September 6, 2025

When integrated with Citrix Endpoint Management, NetScaler Gateway provides remote device access to your internal network and resources. Citrix Endpoint Management creates a micro VPN from the apps on the device to NetScaler Gateway.

You can use the Citrix Gateway service (Preview) or on-premises NetScaler Gateway, also known as NetScaler Gateway. For an overview of the two NetScaler Gateway solutions, see Configure NetScaler Gateway use with Citrix Endpoint Management.

Configure authentication for remote device access to the internal network

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Under **Server**, click **NetScaler Gateway**. The **NetScaler Gateway** page appears. In the following example, a NetScaler Gateway instance exists.

3. Configure these settings:
    - **Authentication:** Select whether to enable authentication. The default is **On**.
    - **Deliver user certificate for authentication:** Select whether you want Citrix Endpoint Management to share the authentication certificate with Citrix Secure Hub. Sharing the certificate enables NetScaler Gateway to handle the client certificate authentication. The default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

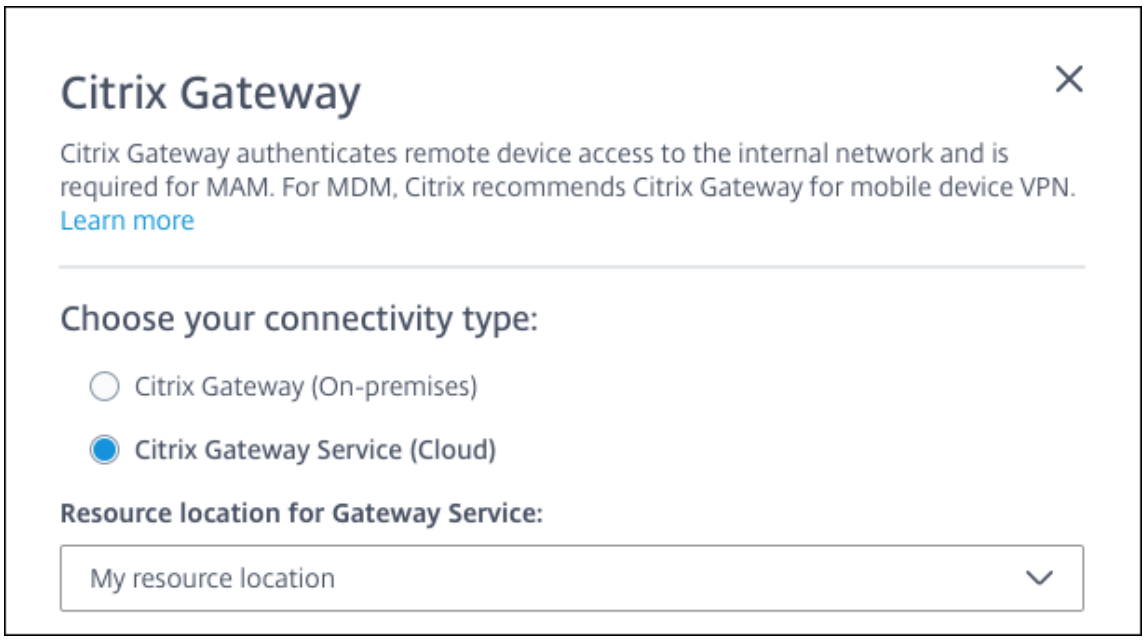
- **Credential Provider:** Click the credential provider to use fin the drop-down list. For more information, see Credential providers.

4. Click **Save**.

Add a Citrix Gateway service instance (Preview)

After you save the authentication settings, you add a NetScaler Gateway instance to Citrix Endpoint Management.

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page opens.
2. On the **Settings** page, scroll to the NetScaler Gateway tile and then click **Start setup**. The **NetScaler Gateway** page appears.
3. Select **Citrix Gateway service (cloud)** and specify the resource location for the Gateway service.



- **Resource location for Gateway service:** is required if you use Citrix Secure Mail. Specify the resource location for the STA service. The resource location must include a configured NetScaler Gateway. If you later want to remove a resource location that's configured for the Gateway service, update this setting.

After you complete those settings, click **Connect** to establish the connection. The new NetScaler Gateway is added. The **Citrix Gateway service (cloud)** tile appears on the **Settings** page. To

© 1997–2025 Citrix Systems, Inc. All rights reserved.

edit an instance, click **See More**. If Gateway Connectors are not available in the selected resource location, click **Add Gateway Connector**. Follow the on-screen guidance to install Gateway Connectors. You can also add Gateway Connectors later.

4. Click **Save and Export Script**.

   - **Save and Export Script**. Click the button to save your settings and export a configuration bundle. You can upload a script from the bundle to NetScaler Gateway to configure it with Citrix Endpoint Management settings. For information, see "Configure an on-premises NetScaler Gateway for use with Citrix Endpoint Management"after these steps.

   You've added the new NetScaler Gateway. The **NetScaler Gateway** tile appears on the **Settings** page. To edit an instance, click **See More**.

Configure on-premises NetScaler Gateway for use with Citrix Endpoint Management

To configure an on-premises NetScaler Gateway for use with Citrix Endpoint Management, do the following general steps as detailed in the following sections.

1. Verify that your environment meets the prerequisites.
2. Export the script bundle from the Citrix Endpoint Management console.
3. Extract the files from the bundle. If you're only using classic policies on NetScaler Gateway and you're running Citrix ADC 13.0 or earlier, use the script with "Classic"in the file name. If you're using any advanced policies or you're running Citrix ADC 13.1 or later, use the script with "Advanced"in the file name.
4. Run the appropriate script on the NetScaler Gateway. See the readme file provided with the scripts for the latest detailed instructions.
5. Test the configuration.

The scripts configure these NetScaler Gateway settings required by Citrix Endpoint Management:

- NetScaler Gateway virtual servers needed for MDM and MAM
- Session policies for the NetScaler Gateway virtual servers
- Citrix Endpoint Management server details
- Proxy load balancer for certificate validation
- Authentication Policies and Actions for the NetScaler Gateway virtual server. The scripts describe the LDAP configuration settings.
- Traffic actions and policies for the proxy server
- Clientless access profile
- Static local DNS record on NetScaler Gateway
- Other bindings: Service policy, CA certificate

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The scripts don't handle the following configuration:

- Exchange load balancing
- Citrix Files load balancing
- ICA® Proxy configuration
- SSL Offload

Prerequisites for using the NetScaler Gateway configuration scripts

Citrix Endpoint Management requirements:

- Complete the LDAP and NetScaler Gateway configuration in Citrix Endpoint Management before exporting the script bundle. If you change the settings, export the script bundle again.

NetScaler Gateway requirements:

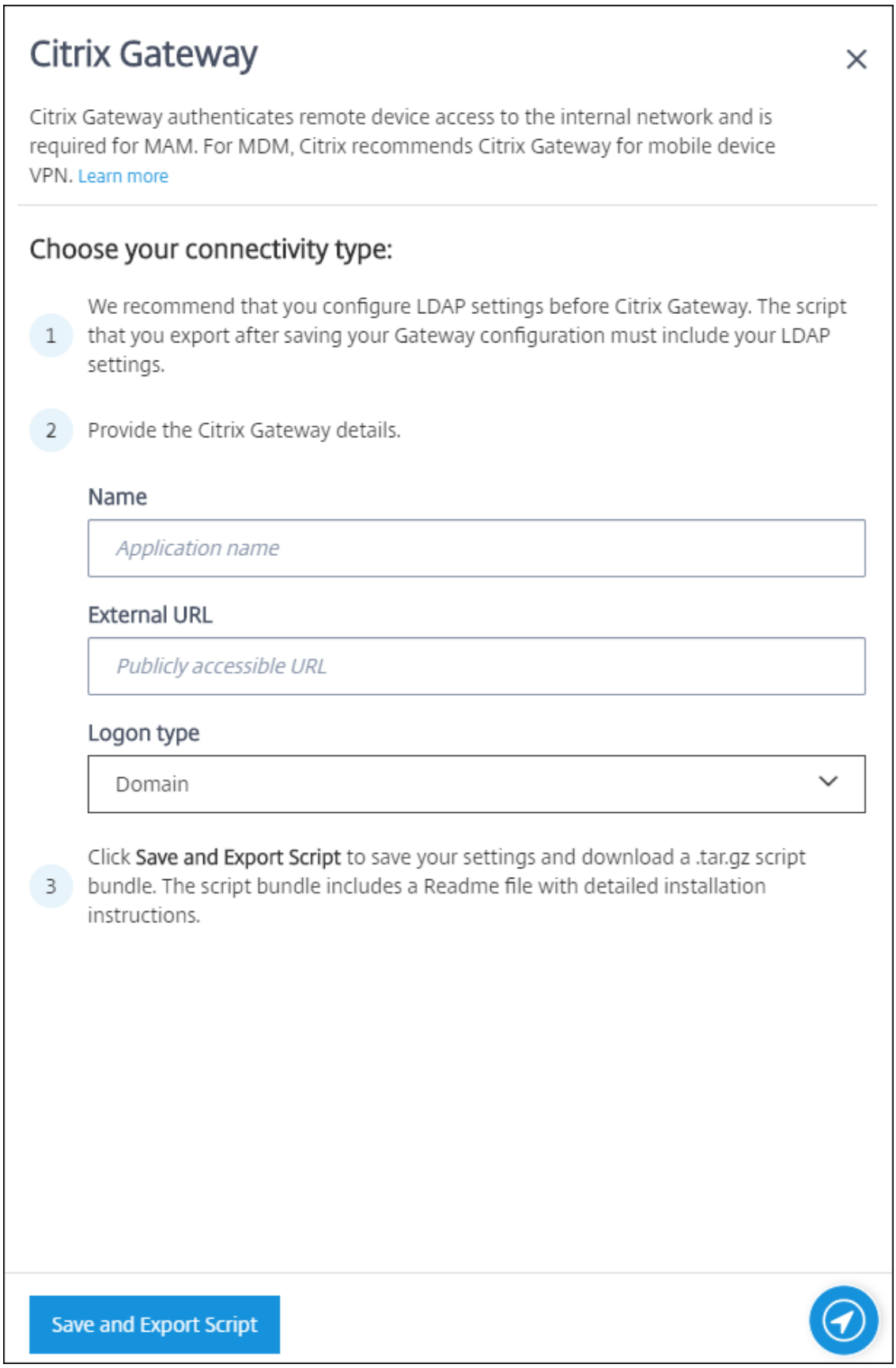
- When using certificate-based authentication at the NetScaler Gateway, you must create SSL certificates on a Citrix ADC Appliance. See Create and Use SSL Certificates on a Citrix ADC Appliance.
- NetScaler Gateway (minimum version 11.0, Build 70.12).
- The NetScaler Gateway IP address is configured and has connectivity to the LDAP server, unless LDAP is load balanced.
- NetScaler Gateway Subnet (SNIP) IP address is configured, has connectivity to the necessary back end servers, and has public network access over port 8443/TCP.
- DNS can resolve public domains.
- NetScaler Gateway is licensed with Platform/Universal or Trial licenses. For information, see https://support.citrix.com/article/CTX126049.

Export the script bundle from Citrix Endpoint Management

After you save the authentication settings, you add a NetScaler Gateway instance to Citrix Endpoint Management.

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page opens.
2. On the **Settings** page, scroll to the NetScaler Gateway tile and then click **Start setup**. The **NetScaler Gateway** page appears.
3. Select **NetScaler Gateway (On-premises)** and configure these settings:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Name:** Type a name for the NetScaler Gateway instance.
- **External URL:** Type the publicly accessible URL for NetScaler Gateway. For example, `https://receiver.com`.
- **Logon Type:** Choose a logon type. Types include: **Domain**, **Security token only**, **Domain and security token**, **Certificate**, **Certificate and domain**, and **Certificate and security token**. The default is **Domain**.

If you have multiple domains, use **Certificate and domain**. For more information, see Configure authentication for multiple domains.

Certificate-based authentication at the NetScaler Gateway requires extra configuration. For example, you must upload your root CA certificate to your Citrix ADC Appliance. See Create and Use SSL Certificates on a Citrix ADC Appliance.

For more information, see Authentication in the Deployment Handbook.

4. Click **Save and Export Script**.

   - **Save and Export Script**. Click the button to save your settings and export a configuration bundle. You can upload a script from the bundle to NetScaler Gateway to configure it with Citrix Endpoint Management settings. For information, see "Configure an on-premises NetScaler Gateway for use with Citrix Endpoint Management"after these steps.

   You've added the new NetScaler Gateway. The **NetScaler Gateway** tile appears on the **Settings** page. To edit an instance, click **See More**.

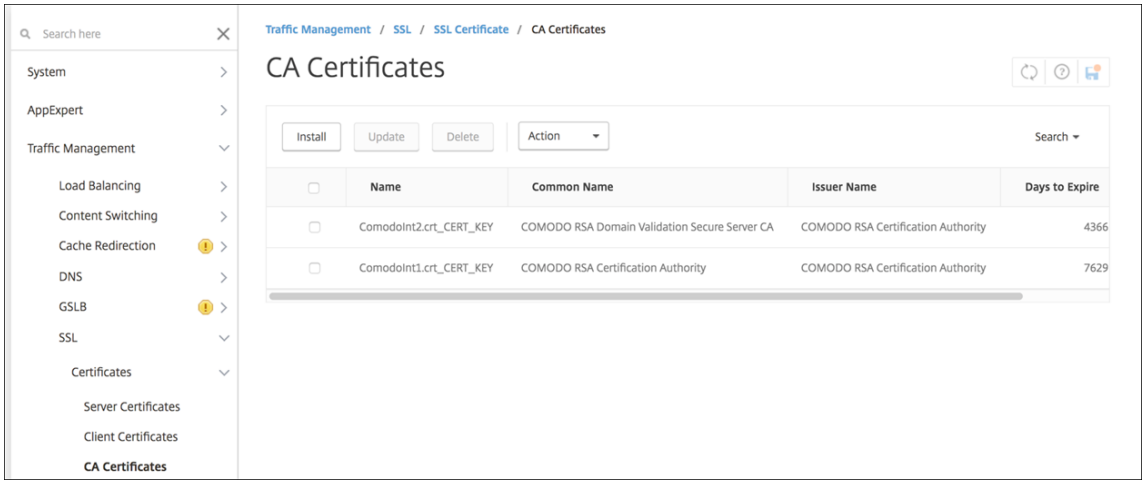
Install the script in your environment

The script bundle includes the following.

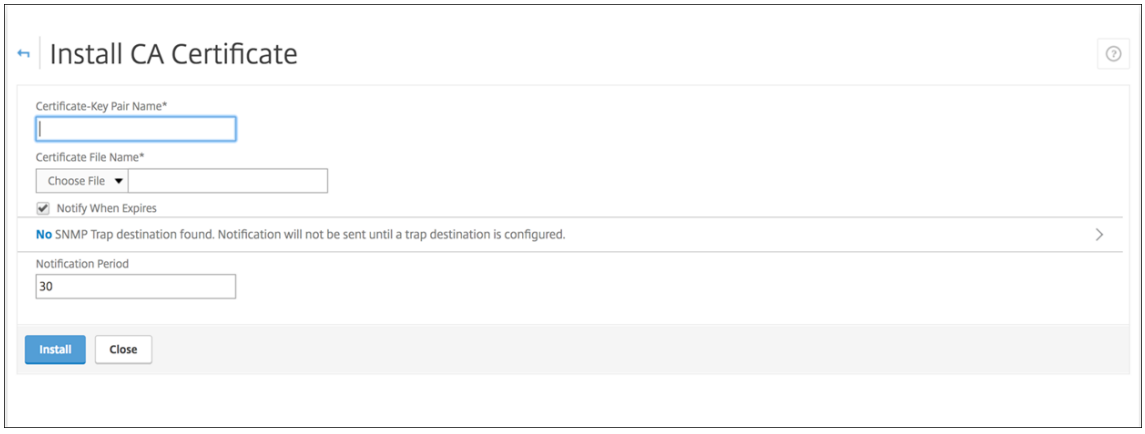
- Readme file with detailed instructions
- Scripts that have the NetScaler® CLI commands used to configure the required components in NetScaler
- Public Root CA certificate and the Intermediate CA certificate
- Scripts that have the NetScaler CLI commands used to remove the NetScaler configuration

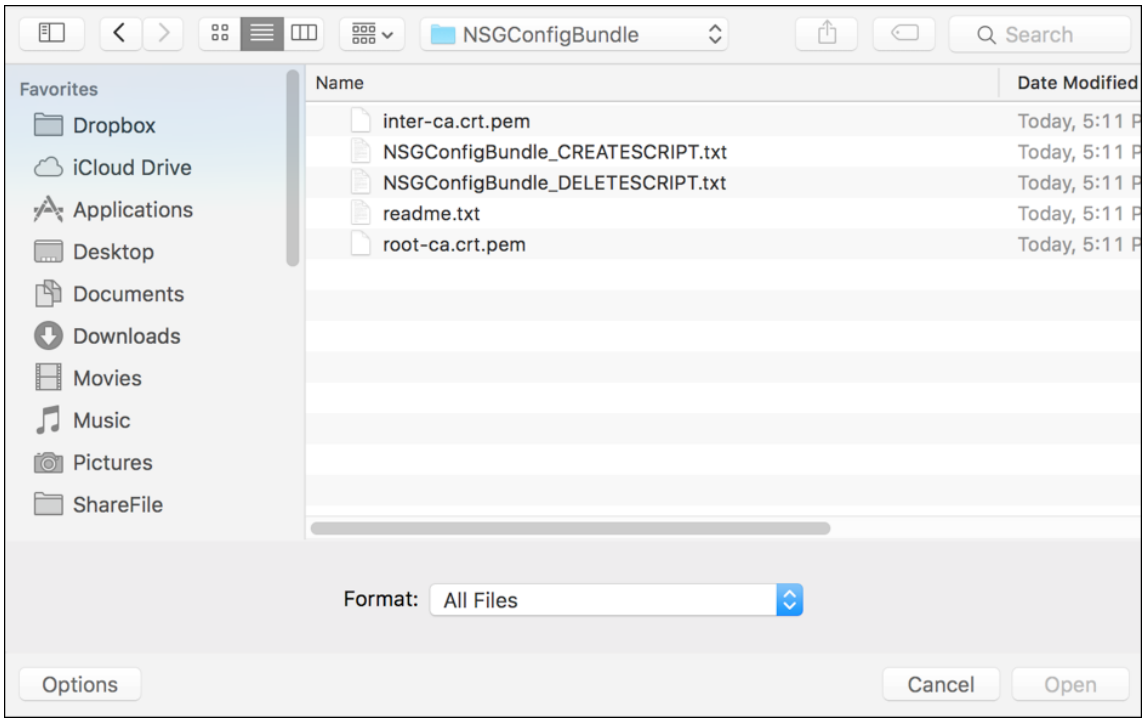
1. Upload and install the certificate files (provided in the script bundle) on the Citrix ADC appliance in the /nsconfig/ssl/ directory. See Create and Use SSL Certificates on a Citrix ADC Appliance.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

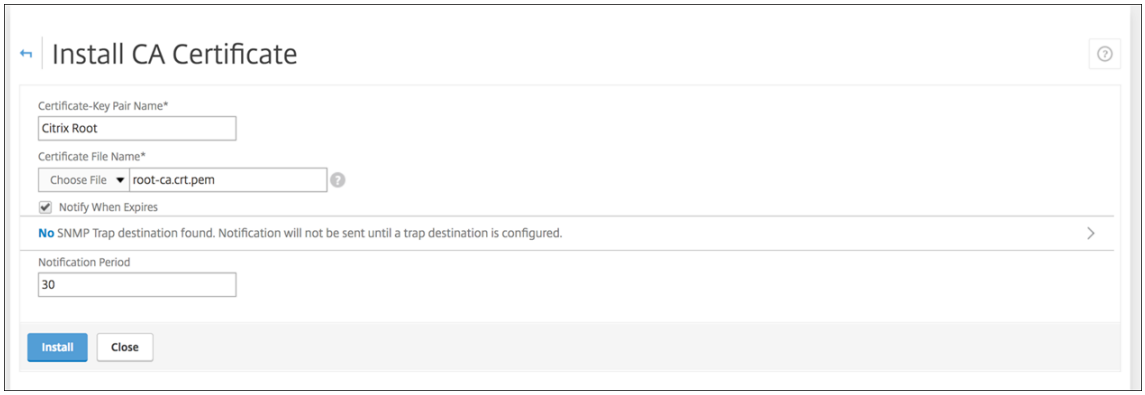


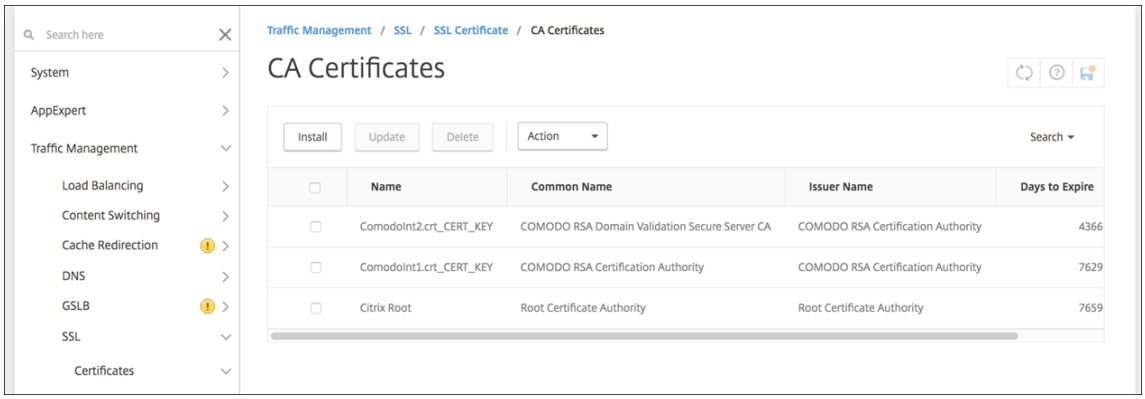
The following examples show how to install the root certificate.





© 1997–2025 Citrix Systems, Inc. All rights reserved.





Make sure that you install both the root and intermediate certificates.

2. Edit the script (ConfigureCitrixGatewayScript_Classic.txt or ConfigureCitrixGatewayScript_Advanced.txt) to replace all placeholders with details from your environment.

```
#Important Note: Please update the following placeholders with valid values:
# <NSG_IP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reachable from your devices either directly or via a
NAT.
# <PROXY_LB_VIP> -- Virtual IP Address to be assigned to the proxy load-balancer configured on the NetScaler. This IP address must be a private address.
# <LDAP_SVC_USERNAME> -- LDAP Service Account Username.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <SERVER_CERT_NAME> -- Name of the server certificate file on the NetScaler. This certificate is bound to the NetScaler Gateway virtual server.
```

3. Run your edited script in the NetScaler bash shell, as described in the readme file included in the script bundle. For example:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/OfflineNSGConfigtBundle_CREATESCRIPT.txt"
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
login as: nsroot
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you are not an authorized user!            #
#                                                                              #
################################################################################

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

When the script completes, the following lines appear.

```
exec: save ns config
 Done
 Done
root@ns#
```

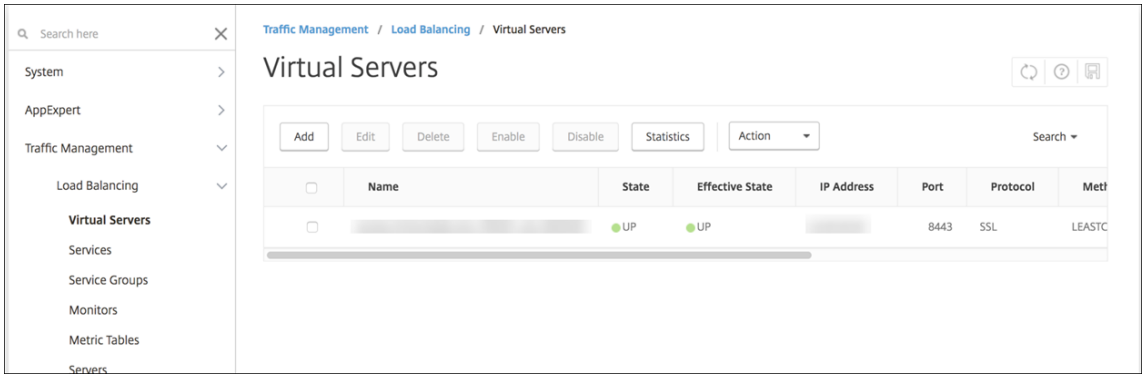
Test the configuration

To validate the configuration:

1. Validate that NetScaler Gateway Virtual Server shows a state of **UP**.

2. Validate that the Proxy Load Balancing Virtual Server shows a state of **UP**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Open a web browser, connect to the NetScaler Gateway URL, and try to authenticate. If the authentication succeeds, you are redirected to an "HTTP Status 404 - Not Found"message.
4. Enroll a device and make sure that it gets both MDM and MAM enrollment.

Configure authentication for multiple domains

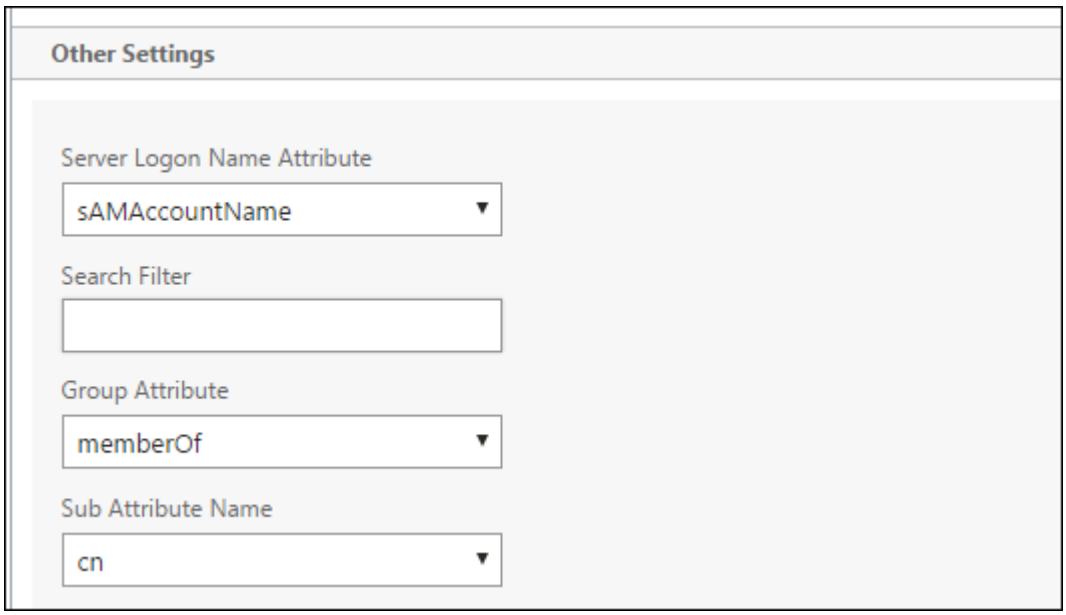
If you have multiple Citrix Endpoint Management instances, such as for test, development, and production environments, you configure NetScaler Gateway for the additional environments manually. (You can use the NetScaler for XenMobile wizard only one time.)

NetScaler Gateway configuration

To configure NetScaler Gateway authentication policies and a session policy for a multi-domain environment:

1. In the NetScaler Gateway configuration utility, on the **Configuration** tab, expand **NetScaler Gateway > Policies > Authentication**.
2. In the navigation pane, click **LDAP**.
3. Click to edit the LDAP profile. Change the **Server Logon Name Attribute** to **userPrincipalName** or the attribute that you want to use for searches. Make a note of the attributes that you specify. You provide it when configuring LDAP settings in the Citrix Endpoint Management console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

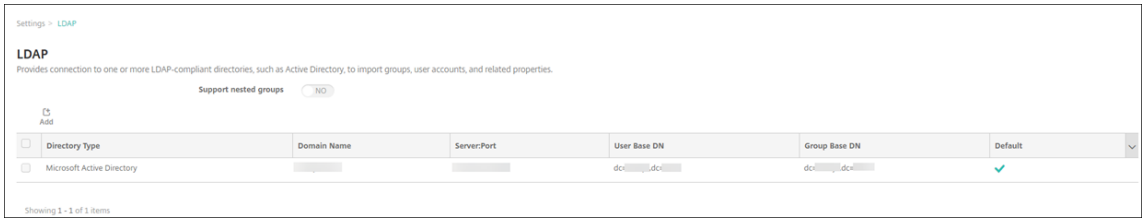


4. Repeat those steps for each LDAP policy. A separate LDAP policy is required for each domain.
5. In the session policy bound to the NetScaler Gateway virtual server, navigate to **Edit session profile > Published Applications**. Make sure that **Single Sign-On Domain** is blank.

Citrix Endpoint Management configuration

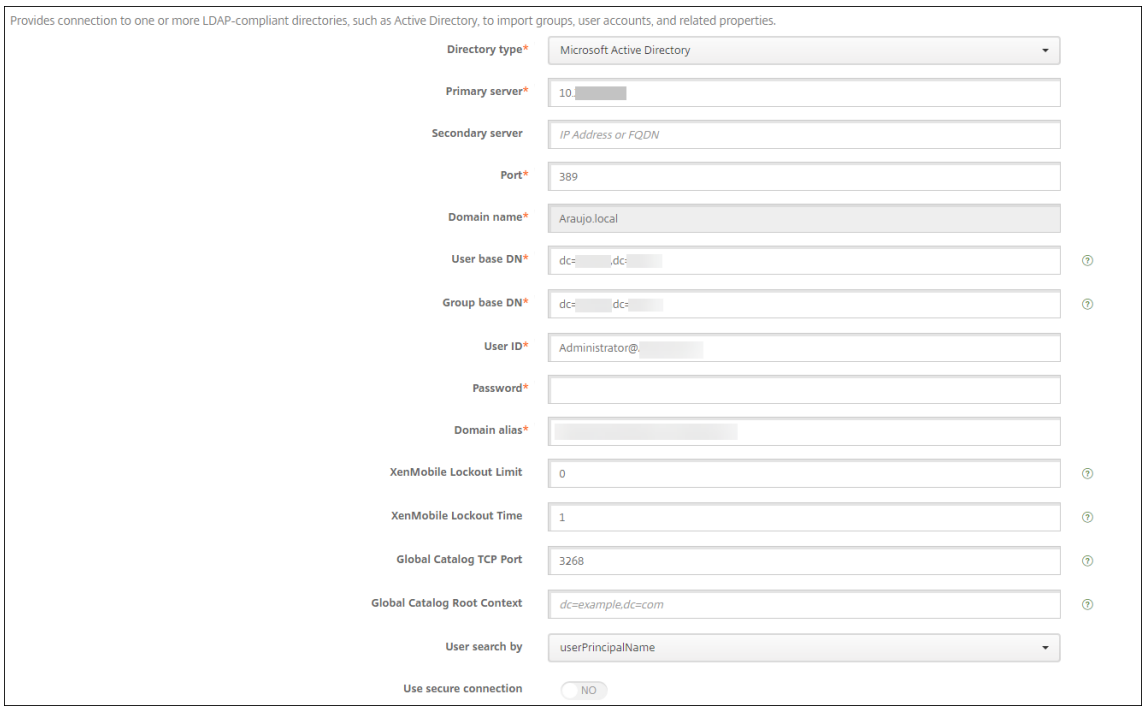
To configure Citrix Endpoint Management LDAP for a multi-domain environment:

1. In the Citrix Endpoint Management console, go to **Settings > LDAP** and add or edit a directory.



2. Provide the information.
   - In **Domain Alias**, specify each domain to use for user authentication. Separate the domains with a comma and don't use spaces between the domains. For example: domain1.com,domain2.com,domain3.com
   - Make sure that the **User search by** field matches the **Server Logon Name Attribute** specified in the NetScaler Gateway LDAP policy.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Drop inbound connection requests to specific URLs

If the NetScaler Gateway in your environment is configured for SSL offload, you might prefer that the gateway drop inbound connection requests for specific URLs. If you prefer that extra security, contact Citrix Cloud Operations and request that they allow your IP to your on-premises data centers.

Domain or domain plus security token authentication

September 6, 2025

Citrix Endpoint Management supports domain-based authentication against one or more directories that are compliant with the Lightweight Directory Access Protocol (LDAP). You configure a connection in Citrix Endpoint Management to one or more directories. Citrix Endpoint Management uses the LDAP configuration to import groups, user accounts, and related properties.

> **Important:**
>
> Citrix Endpoint Management doesn't support changing the authentication mode from one type of authentication mode to a different authentication mode after users enroll devices in Citrix Endpoint Management. For example, you can't change the authentication mode from **Domain authentication** to **Domain + Certificate** after users have enrolled.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

About LDAP

LDAP is an open-source, vendor-neutral application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory information services are used to share information about users, systems, networks, services, and applications available throughout the network.

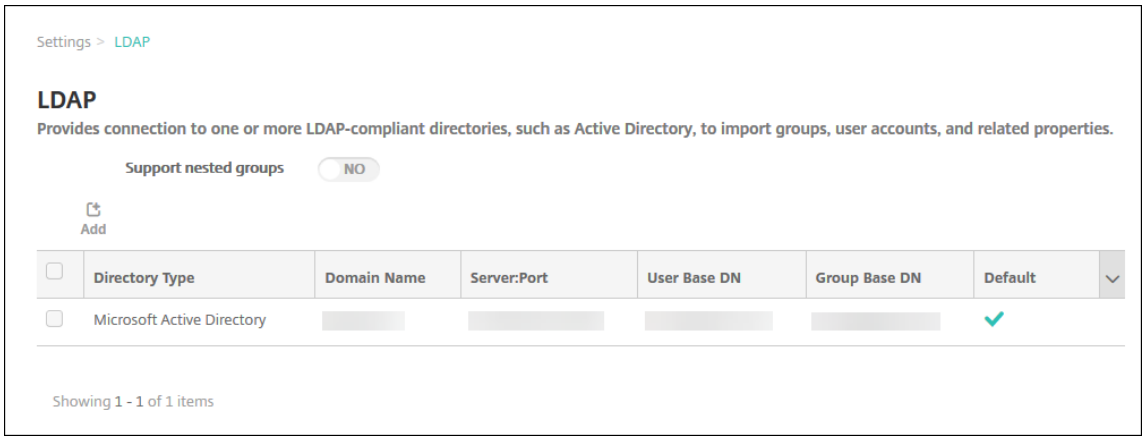
A common usage of LDAP is to provide single sign-on (SSO) for users, where a single password (per user) is shared among many services. Single sign-on enables a user to log on one time to a company website, for authenticated access to the corporate intranet.

A client starts an LDAP session by connecting to an LDAP server, known as a Directory System Agent (DSA). The client then sends an operation request to the server, and the server responds with the appropriate authentication.

To add or edit LDAP connections in Citrix Endpoint Management

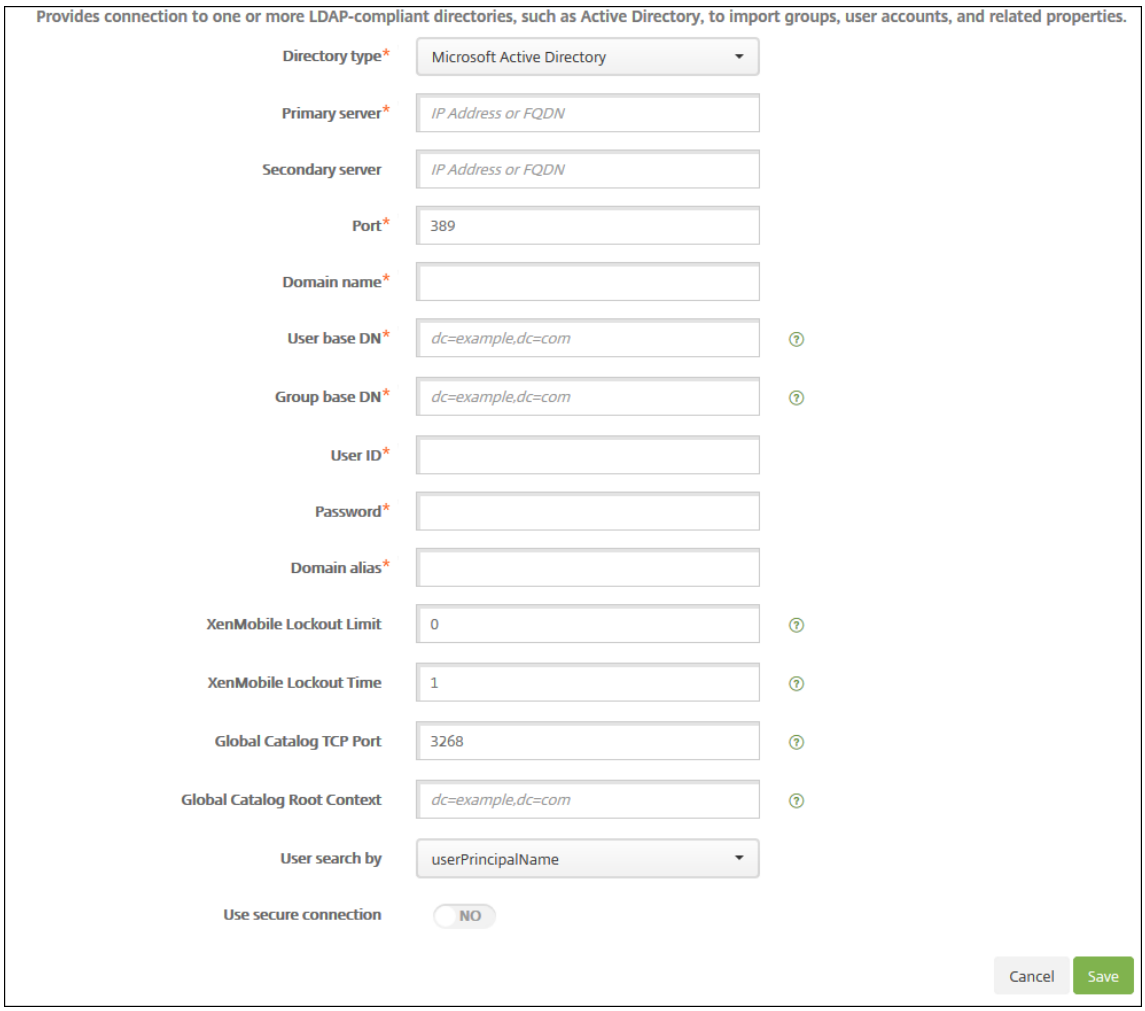
You typically configure LDAP connections when you onboard to Citrix Endpoint Management, as described in To configure LDAP. If you onboarded before the screens shown in that section are available, use the information in this section to add LDAP connections.

1. In the Citrix Endpoint Management console, go to **Settings > LDAP**.
2. Under **Server**, click **LDAP**. The **LDAP** page appears.



3. On the **LDAP** page, click **Add** or **Edit**. The **Add LDAP** or **Edit LDAP** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Configure these settings:

   - **Directory type:** Click the appropriate directory type in the drop-down list. The default is **Microsoft Active Directory**.
   - **Primary server:** Type the primary server used for LDAP; you can enter either the IP address or the fully qualified domain name (FQDN).
   - **Secondary server:** Optionally, if a secondary server has been configured, enter the IP address or FQDN for the secondary server. This server is a failover server used if the primary server cannot be reached.
   - **Port:** Type the port number used by the LDAP server. By default, the port number is set to **389** for unsecured LDAP connections. Use the port number **636** for secure LDAP connections, use **3268** for Microsoft unsecure LDAP connections, or **3269** for Microsoft secure LDAP connections.
   - **Domain name:** Type the domain name.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **User base DN:** Type the location of users in the Active Directory through a unique identifier. Syntax examples include: `ou=users`, `dc=example`, or `dc=com`.
- **Group base DN:** Type the location of groups in the Active Directory. For example, `cn=users, dc=domain, dc=net` where `cn=users` represents the container name of the groups and `dc` represents the domain component of the Active Directory.
- **User ID:** Type the user ID associated with the Active Directory account.
- **Password:** Type the password associated with the user.
- **Domain alias:** Type an alias for the domain name. If you change the **Domain alias** setting after enrollment, users must re-enroll.
- **Citrix Endpoint Management Lockout Limit:** Type a number between **0** and **999** for the number of failed logon attempts. A value of **0** means that Citrix Endpoint Management never locks out the user based on failed logon attempts. The default is **0**.

  Consider setting this lockout limit to a lower value than your LDAP lockout policy. Doing so helps prevent user lockouts if Citrix Endpoint Management is unable to authenticate to the LDAP server. For example, if the LDAP lockout policy is 5 attempts, configure this lockout limit to **4** or lower.
- **Citrix Endpoint Management Lockout Time:** Type a number between **0** and **99999** representing the number of minutes a user must wait after exceeding the lockout limit. A value of **0** means that the user isn't forced to wait after a lockout. The default is **1**.
- **Global Catalog TCP Port:** Type the TCP port number for the Global Catalog server. By default, the TCP port number is set to **3268**; for SSL connections, use port number **3269**.
- **Global Catalog Root Context:** Optionally, type the Global Root Context value used to enable a global catalog search in the Active Directory. This search is in addition to the standard LDAP search, in any domain without the need to specify the actual domain name.
- **User search by:** Select the format of user name or user ID that Citrix Endpoint Management uses to search for users in this directory. Users enter their user name or user ID in this format when enrolling. If you change the **User search by** setting after enrollment, users must re-enroll.

  If you choose **userPrincipalName**, users enter a user principal name (UPN) in this format:

  - `*username*@*domain*`

  If you choose **sAMAccountName**, users enter a secure account manager (SAM) name in one of these formats:

  - `*username*@*domain*`
  - `*domain\username*`

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Use secure connection:** Select whether to use secure connections. The default is **NO**.

5. Click **Save**.

To delete an LDAP-compliant directory

1. In the **LDAP** table, select the directory you want to delete.

   You can select more than one property to delete by selecting the checkbox next to each property.

2. Click **Delete**. A confirmation dialog box appears. Click **Delete** again.

Configure domain plus security token authentication

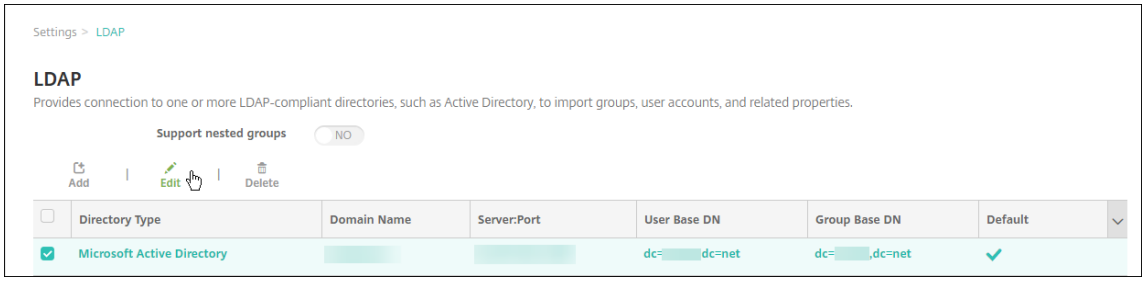
You can configure Citrix Endpoint Management to require users to authenticate with their LDAP credentials plus a one-time password, using the RADIUS protocol.

For optimal usability, you can combine this configuration with Citrix PIN and Active Directory password caching. With that configuration, users don't have to enter their LDAP user names and passwords repeatedly. Users enter user names and passwords for enrollment, password expiration, and account lockout.

Configure LDAP settings

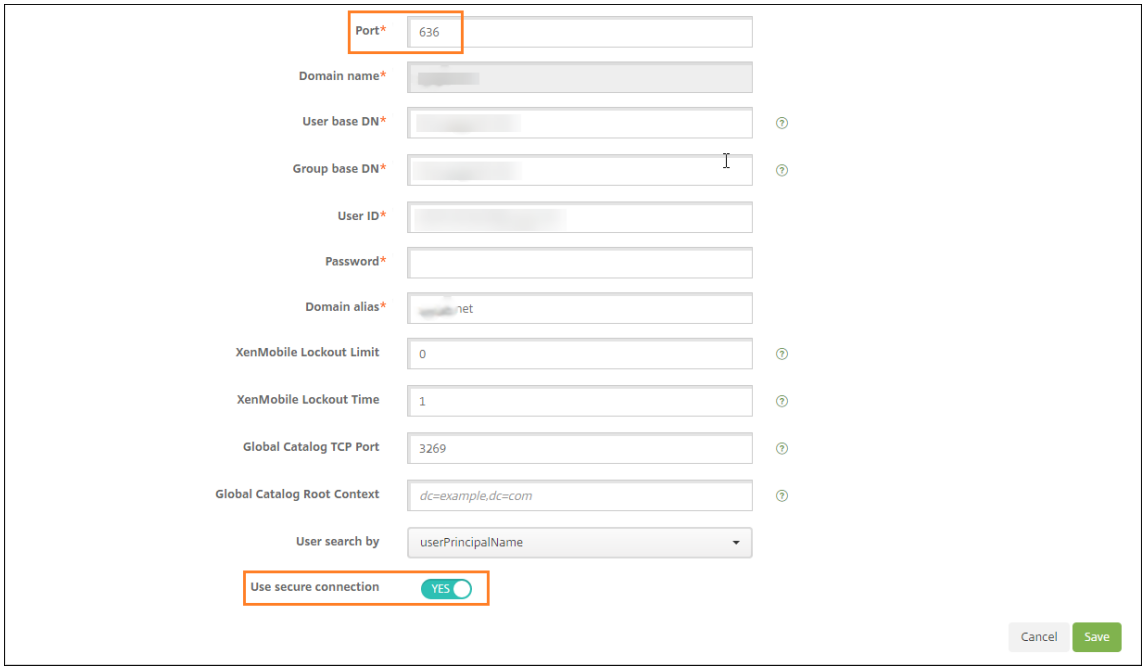
Use of LDAP for authentication requires that you install an SSL certificate from a Certificate Authority on Citrix Endpoint Management. For information, see Upload certificates.

1. In **Settings**, click **LDAP**.
2. Select **Microsoft Active Directory** and then click **Edit**.



3. Verify that the Port is **636**, which is for secure LDAP connections, or **3269** for Microsoft secure LDAP connections.
4. Change **Use secure connection** to **Yes**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure NetScaler Gateway settings

The following steps assume that you already have added a NetScaler Gateway instance to Citrix Endpoint Management. To add a NetScaler Gateway instance, see NetScaler Gateway and Citrix Endpoint Management.

1. In **Settings**, click **NetScaler Gateway**.
2. Select the NetScaler Gateway and then click **Edit**.
3. From **Logon Type**, select **Domain and security token**.

Enable Citrix PIN and user password caching

To enable Citrix PIN and user password caching, go to **Settings > Client Properties** and select these checkboxes: **Enable Citrix PIN Authentication** and **Enable User Password Caching**. For more information, see Client properties.

Configure NetScaler Gateway for domain and security token authentication

Configure NetScaler Gateway session profiles and policies for your virtual servers used with Citrix Endpoint Management. For information, see the NetScaler Gateway documentation.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Client certificate or certificate plus domain authentication

September 6, 2025

The default configuration for Citrix Endpoint Management is user name and password authentication. To add another layer of security for enrollment and access to Citrix Endpoint Management environment, consider using certificate-based authentication. In the Citrix Endpoint Management environment, this configuration is the best combination of security and user experience. Certificate plus domain authentication has the best SSO possibilities coupled with the security provided by two-factor authentication at NetScaler Gateway.

For optimal usability, you can combine certificate plus domain authentication with Citrix PIN and Active Directory password caching. As a result, users don't have to enter their LDAP user names and passwords repeatedly. Users enter user names and passwords for enrollment, password expiration, and account lockout.

> **Important:**
>
> Citrix Endpoint Management doesn't support changing the authentication mode from domain authentication to some other authentication mode after users enroll devices in Citrix Endpoint Management.

If you don't allow LDAP and use smart cards or similar methods, configuring certificates allows you to represent a smart card to Citrix Endpoint Management. Users then enroll using a unique PIN that Citrix Endpoint Management generates for them. After a user has access, Citrix Endpoint Management then creates and deploys the certificate used to authenticate to the Citrix Endpoint Management environment.

You can use the NetScaler for XenMobile wizard to do the configuration required for Citrix Endpoint Management when using NetScaler Gateway certificate-only authentication or certificate plus domain authentication. You can run the NetScaler for XenMobile wizard one time only.

In highly secure environments, usage of LDAP credentials outside of an organization in public or insecure networks is considered a prime security threat for the organization. For highly secure environments, two-factor authentication that uses a client certificate and a security token is an option. For more information, see Configuring Citrix Endpoint Management for Certificate and Security Token Authentication.

Client certificate authentication is available for devices enrolled in MAM and MDM+MAM. To use client certificate authentication for those devices, you must configure the Microsoft server, Citrix Endpoint Management, and then NetScaler Gateway. Follow these general steps, as described in this article.

On the Microsoft server:

1. Add a certificate snap-in to the Microsoft Management Console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Add the template to Certificate Authority (CA).
3. Create a PFX certificate from the CA server.

On Citrix Endpoint Management:

1. Upload the certificate to Citrix Endpoint Management.
2. Create the PKI entity for certificate-based authentication.
3. Configure credentials providers.
4. Configure NetScaler Gateway to deliver a user certificate for authentication.

For information about the NetScaler Gateway configuration, see these articles in the Citrix ADC documentation:

- Client authentication
- SSL profile infrastructure
- Configuring and Binding a Client Certificate Authentication Policy.

Prerequisites

- When you create a Microsoft Certificate Services Entity template, avoid possible authentication issues with enrolled devices by excluding special characters. For example, don't use these characters in the template name: `: ! $ ()# % + * ~ ? | { } []`
- To configure Certificate-based Authentication for Exchange ActiveSync, see the Microsoft documentation on Exchange Server. Configure the certificate authority (CA) server site for Exchange ActiceSync to require client certificates.
- If you use private server certificates to secure the ActiveSync traffic to the Exchange Server, make sure that the mobile devices have all of the Root/Intermediate certificates. Otherwise, certificate-based authentication fails during the mailbox setup in Citrix Secure Mail. In the Exchange IIS Console, you must:
  - Add a website for Citrix Endpoint Management use with Exchange and bind the web server certificate.
  - Use port 9443.
  - For that website, you must add two applications, one for "Microsoft-Server-ActiveSync" and one for "EWS". For both of those applications, under **SSL Settings**, select **Require SSL**.

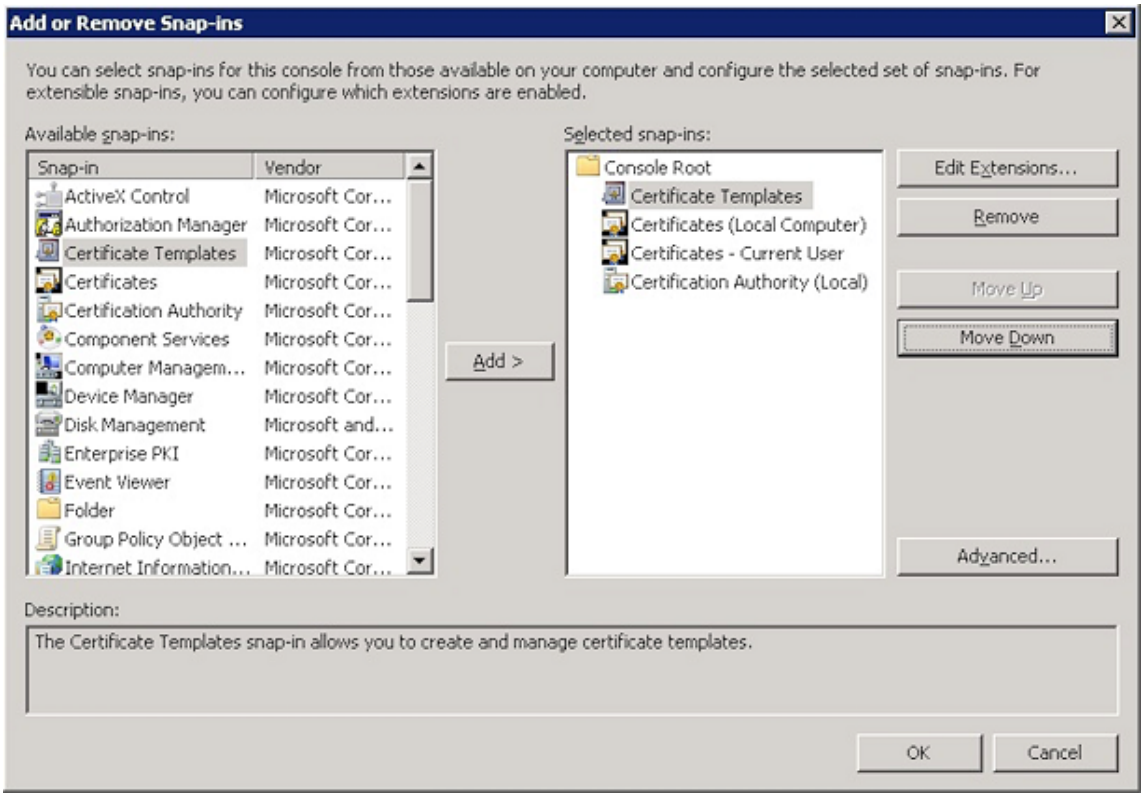
Add a certificate snap-in to the Microsoft Management Console

1. Open the console and then click **Add/Remove Snap-ins**.

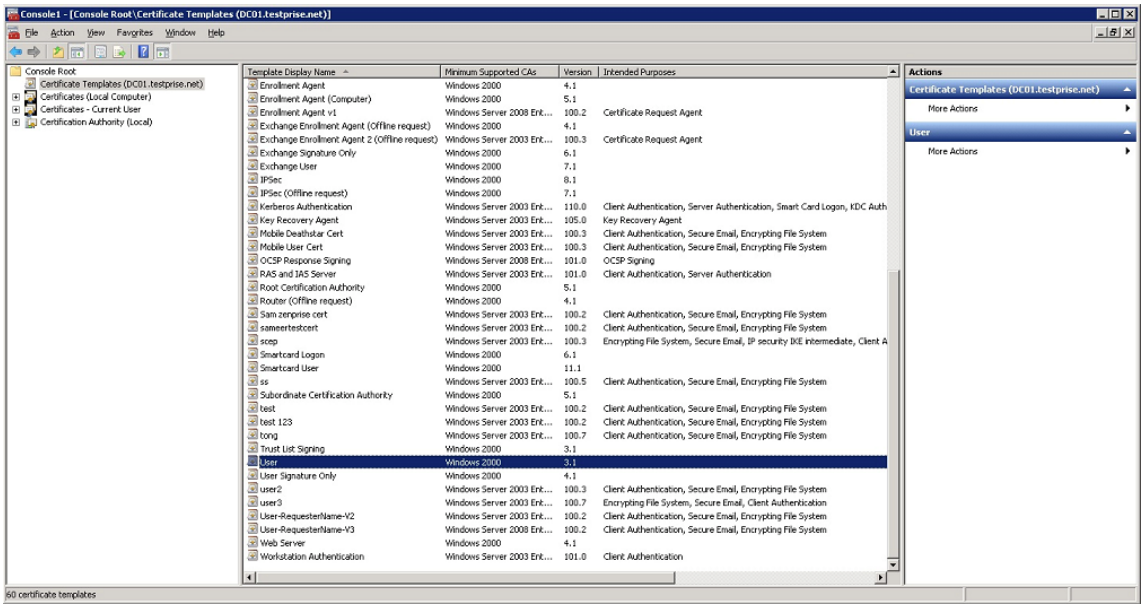
© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Add the following snap-ins:

    - Certificate Templates
    - Certificates (Local Computer)
    - Certificates - Current User
    - Certificate Authority (Local)

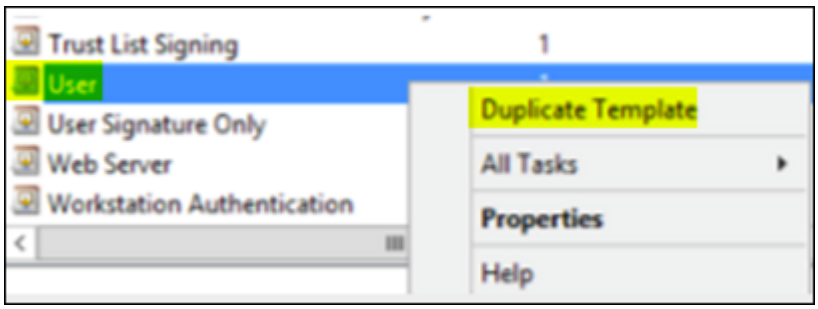


3. Expand **Certificate Templates**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. Select the **User** template and **Duplicate Template**.



5. Provide the Template display name.

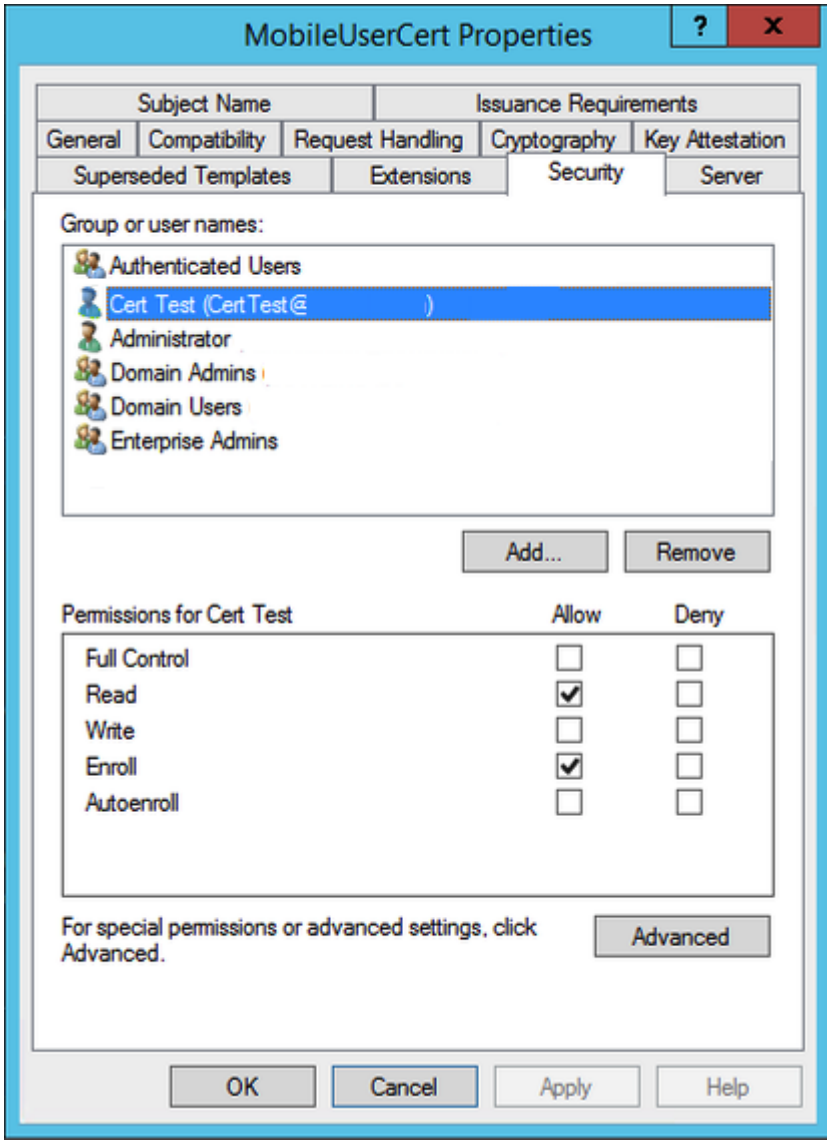
> **Important:**
>
> It is not recommended to select the **Publish certificate in Active Directory** option. If this option is selected, it creates client certificates for all users in Active Directory, which might clutter your Active Directory database.

6. Select **Windows 2003 Server** for the template type. In the Windows 2012 R2 server, under **Compatibility**, select **Certificate authority**, and set the recipient as **Windows 2003**.
7. Under **Security**, click **Add** and then select the AD user account that Citrix Endpoint Management uses to generate certificates.

> **Important:**
>
> Add only the service account user here. Add the **Enroll** permission only to this AD user account.

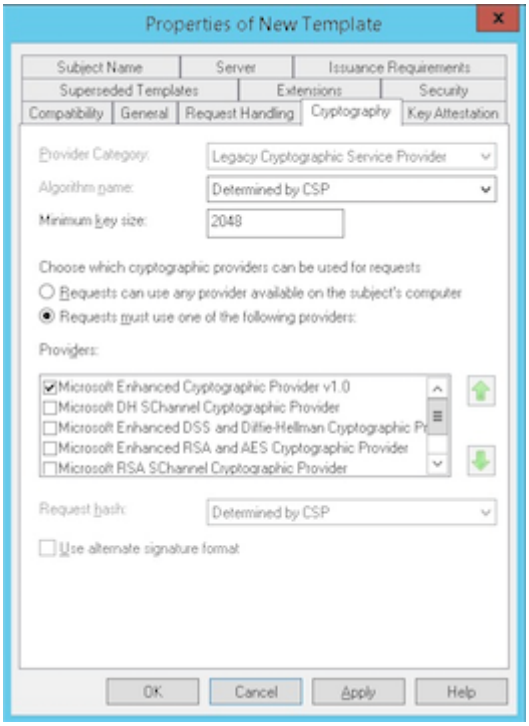
As described later in this article, you create a user .pfx certificate using the service account. For information, see Creating a PFX certificate from the CA server.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

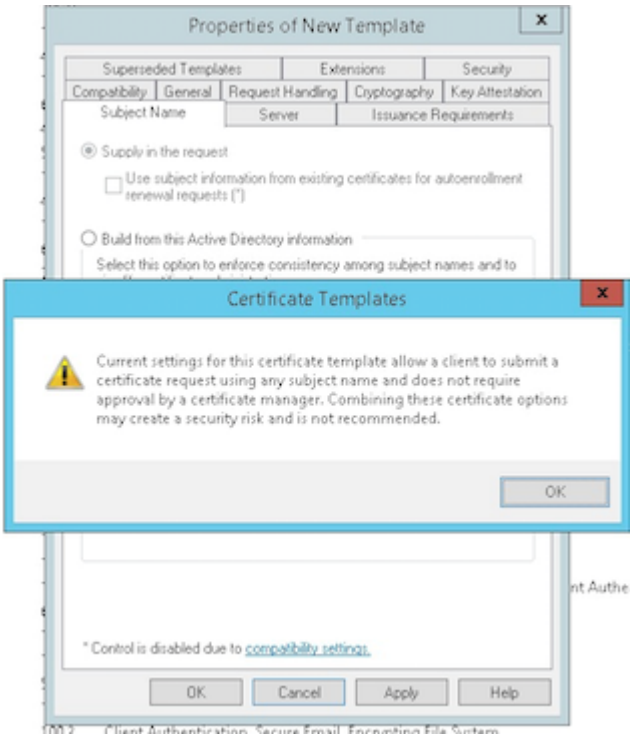


8. Under **Cryptography**, make sure that you provide the key size. You later enter the key size during Citrix Endpoint Management configuration.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



9. Under **Subject Name**, select **Supply in the request**. Apply the changes and then save.

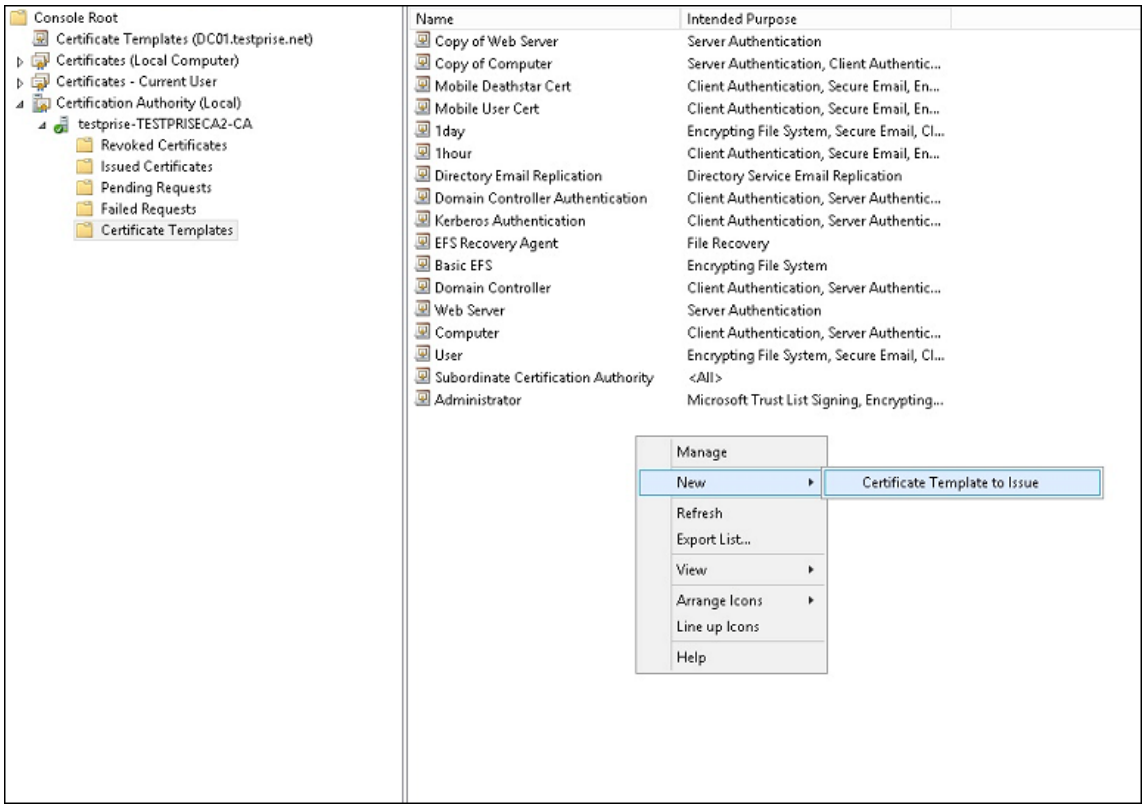


Adding the template to Certificate Authority

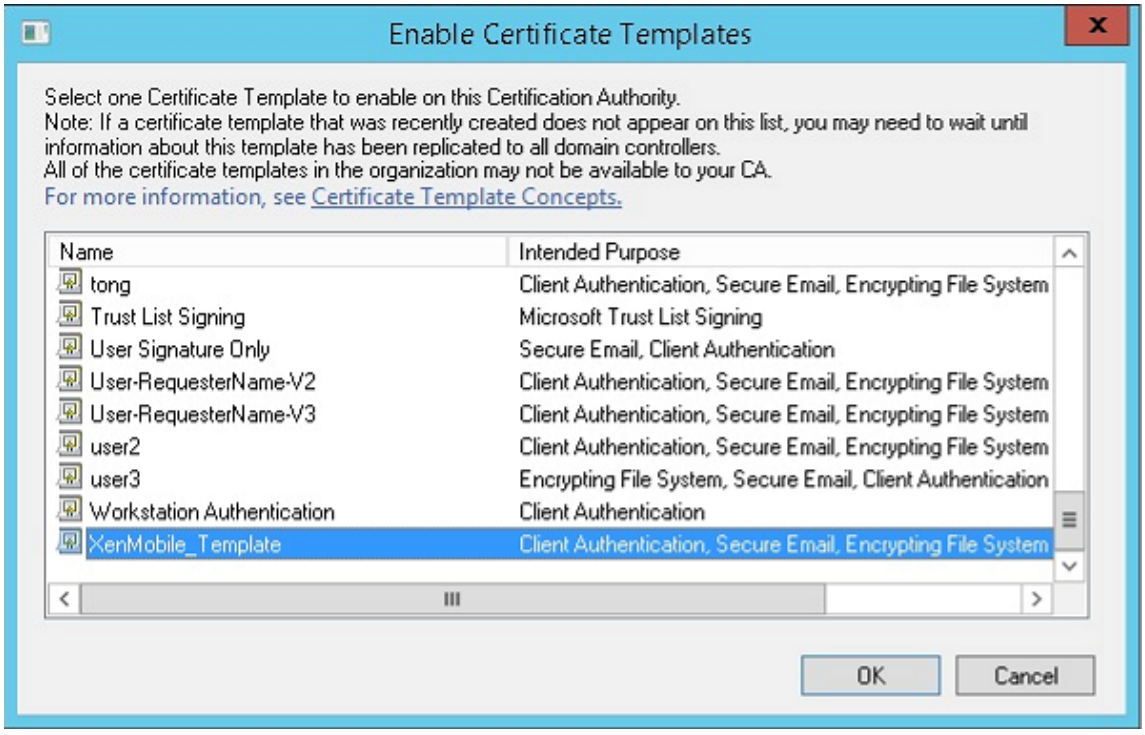
1. Go to **Certificate Authority** and select **Certificate Templates**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Right-click in the right pane and then select **New > Certificate Template to Issue**.



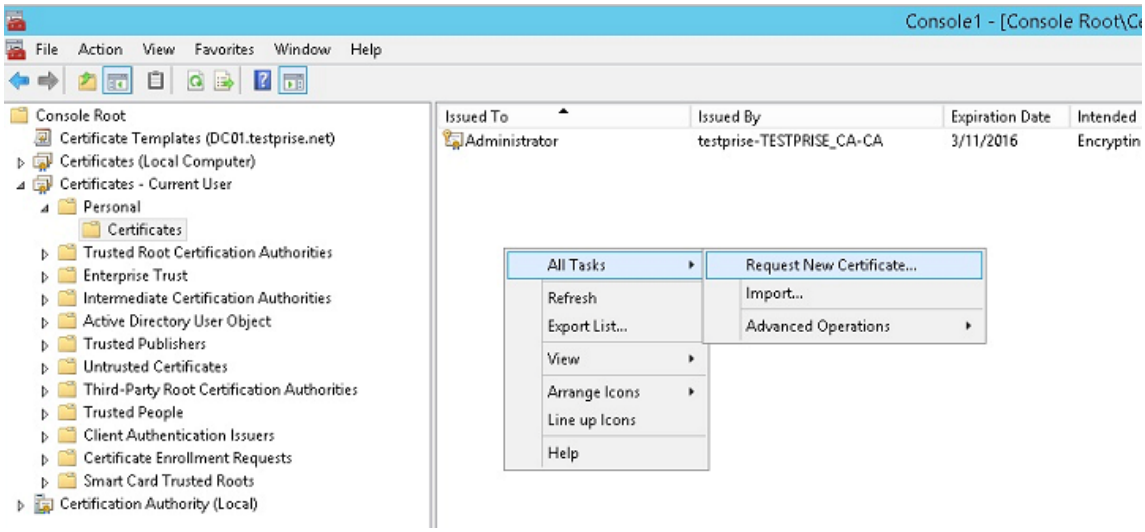
3. Select the template that you created in the previous step and then click **OK** to add it into the **Certificate Authority**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

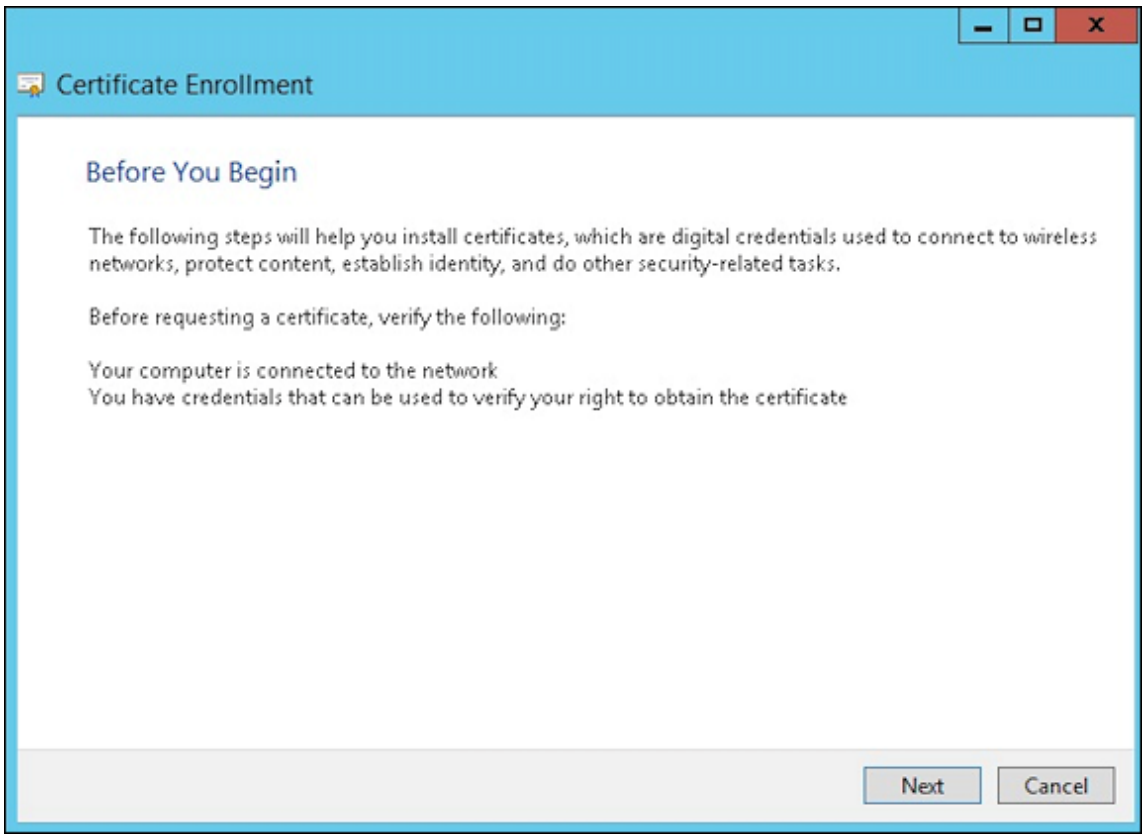
Creating a PFX certificate from the CA server

1. Create a user .pfx cert using the service account with which you logged in. The .pfx uploads to Citrix Endpoint Management, which then requests a user certificate for the users who enroll their devices.
2. Under **Current User**, expand **Certificates**.
3. Right-click in the right pane and then click **Request New Certificate**.



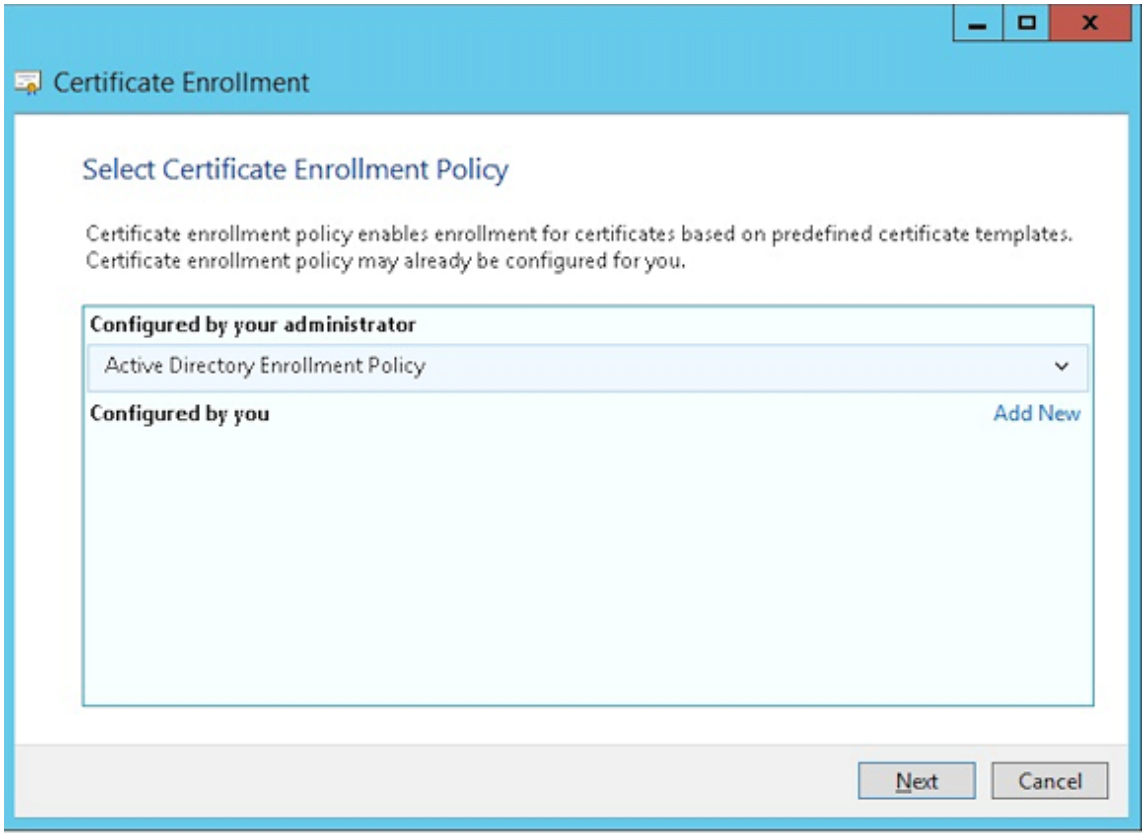
4. The **Certificate Enrollment** screen appears. Click **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



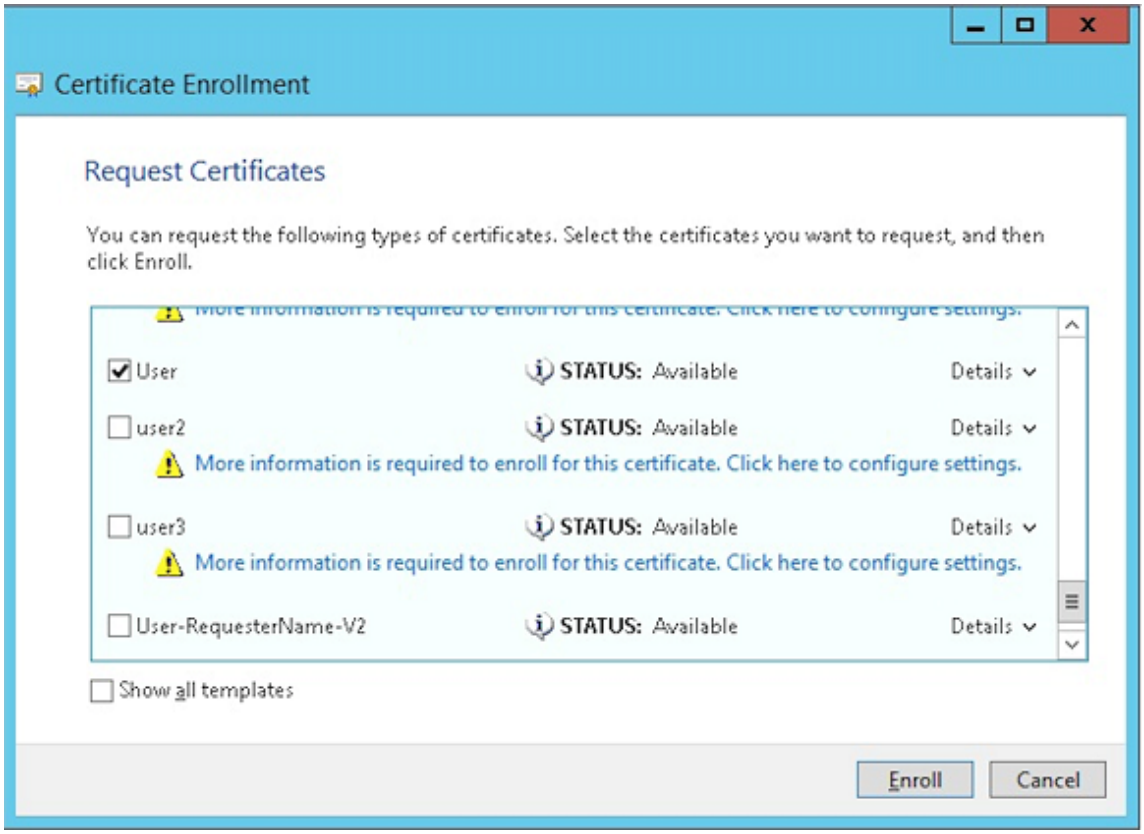
5. Select **Active Directory Enrollment Policy** and then click **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

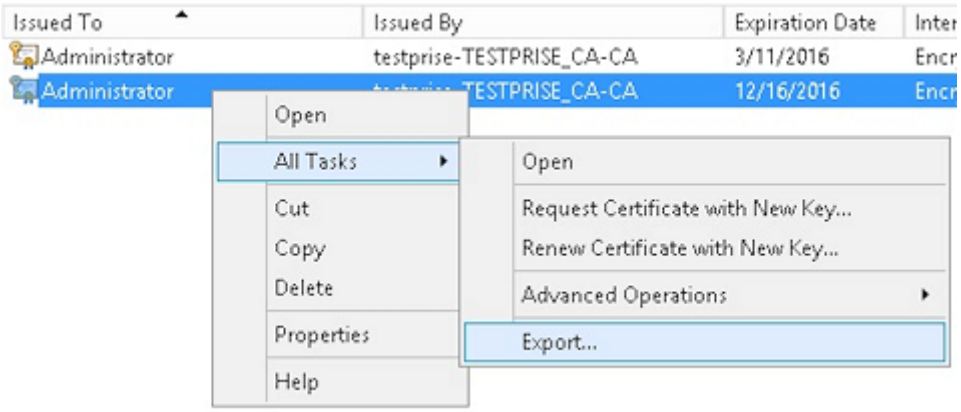


6. Select the **User** template and then click **Enroll**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

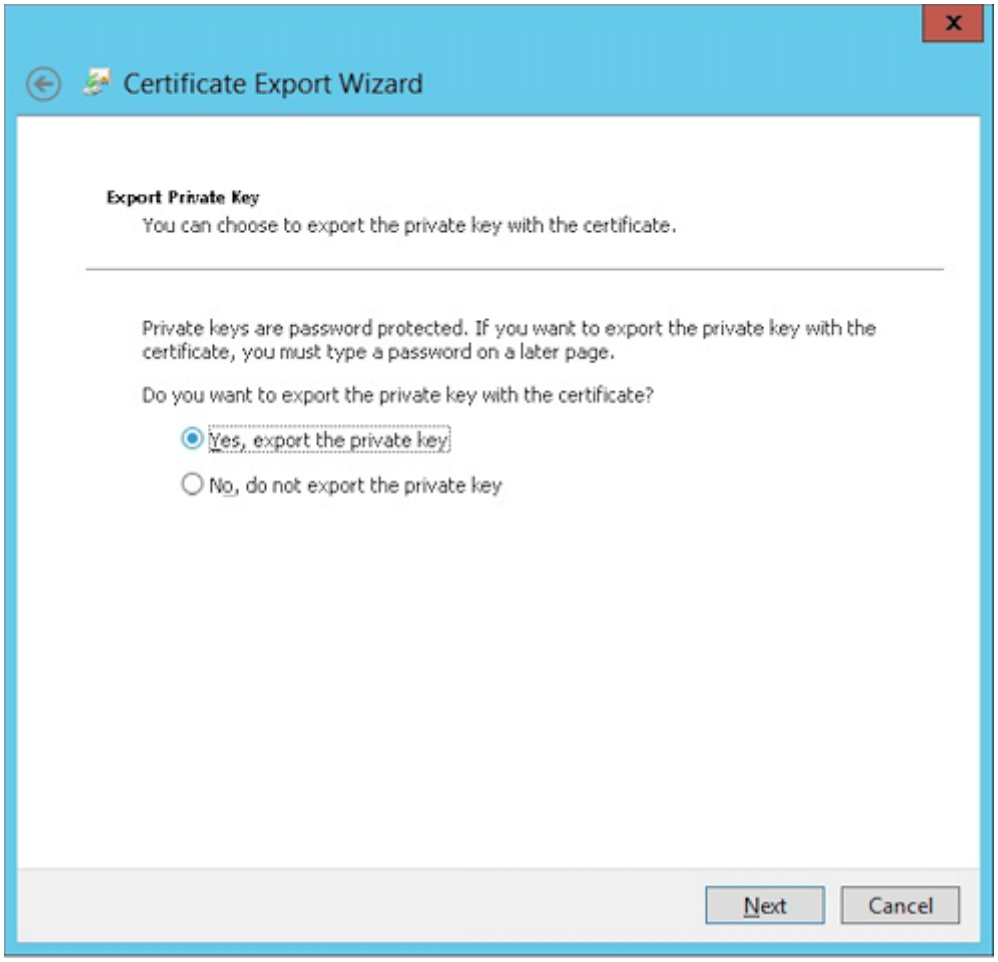


7. Export the .pfx file that you created in the previous step.



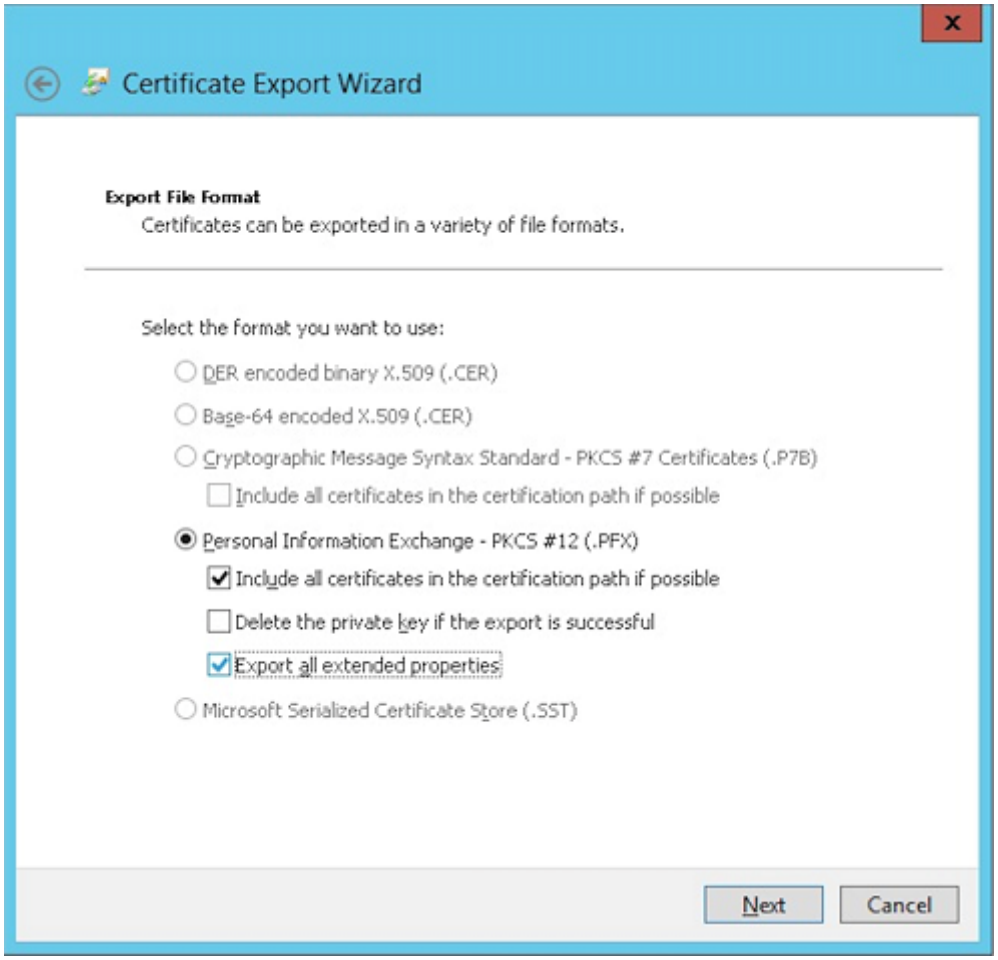
8. Click **Yes, export the private key**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



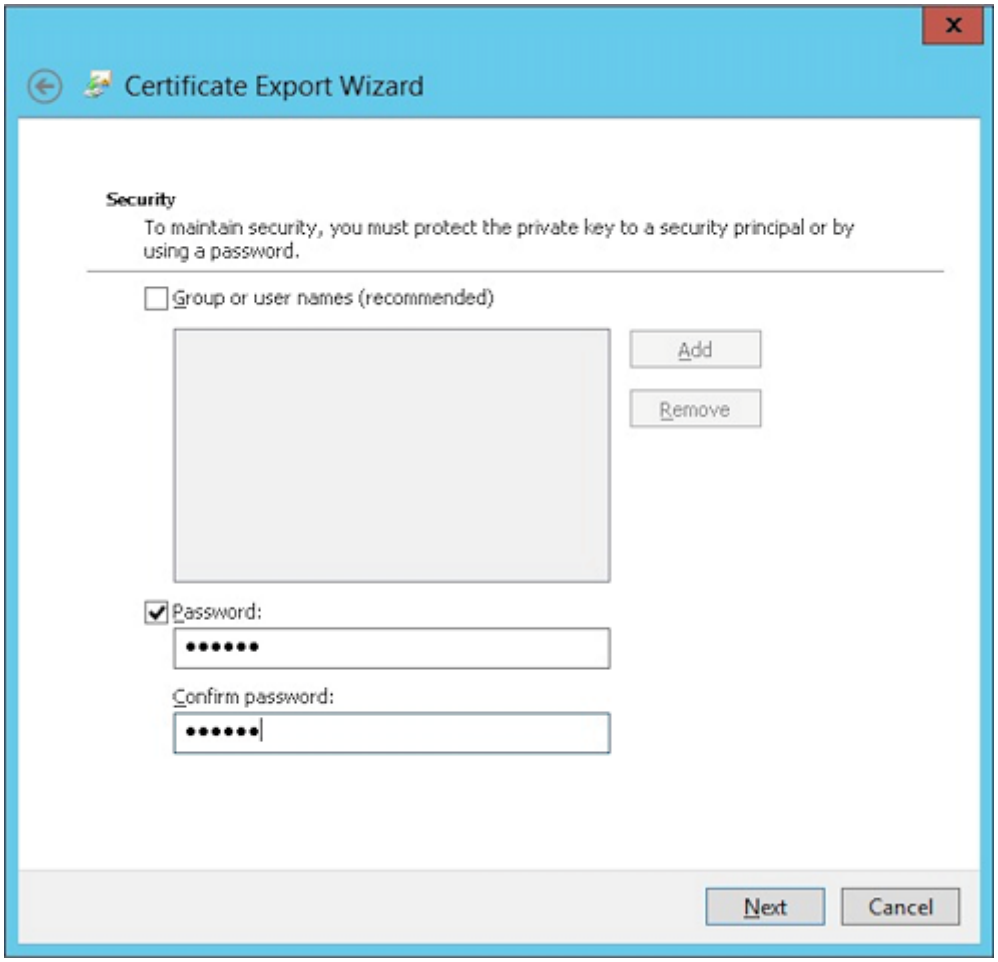
9. Select **Include all certificates in the certification path if possible** and select the **Export all extended properties** checkbox.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



10. Set a password to use when uploading this certificate into Citrix Endpoint Management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

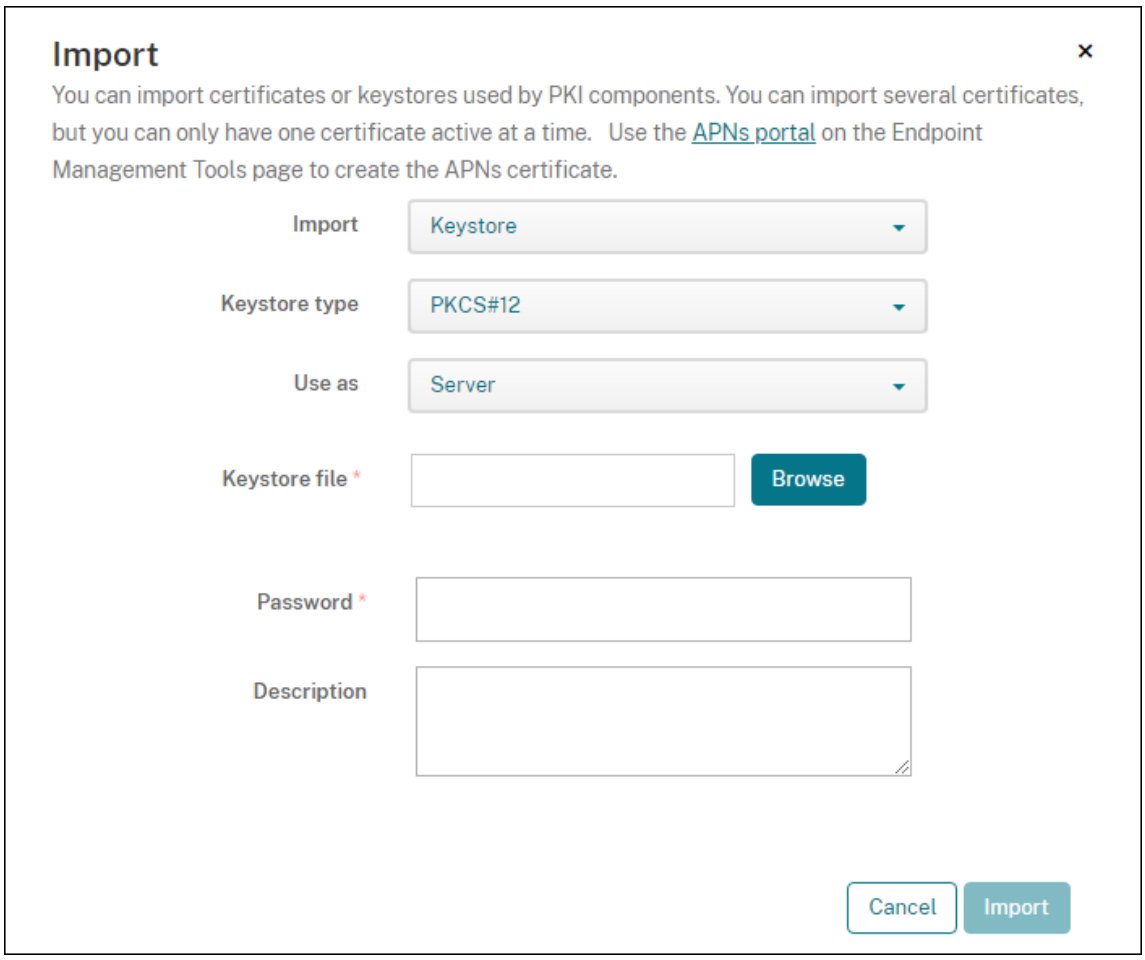


11. Save the certificate onto your hard drive.

Uploading the certificate to Citrix Endpoint Management

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** screen appears.
2. Click **Certificates** and then click **Import**.
3. Enter the following parameters:
    - **Import:** Keystore
    - **Keystore type:** PKCS #12
    - **Use as:** Server
    - **Keystore file:** Click Browse to select the .pfx certificate you created.
    - **Password:** Enter the password that you created for this certificate.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Click **Import**.
5. Verify that the certificate installed correctly. A correctly installed certificate displays as a User certificate.

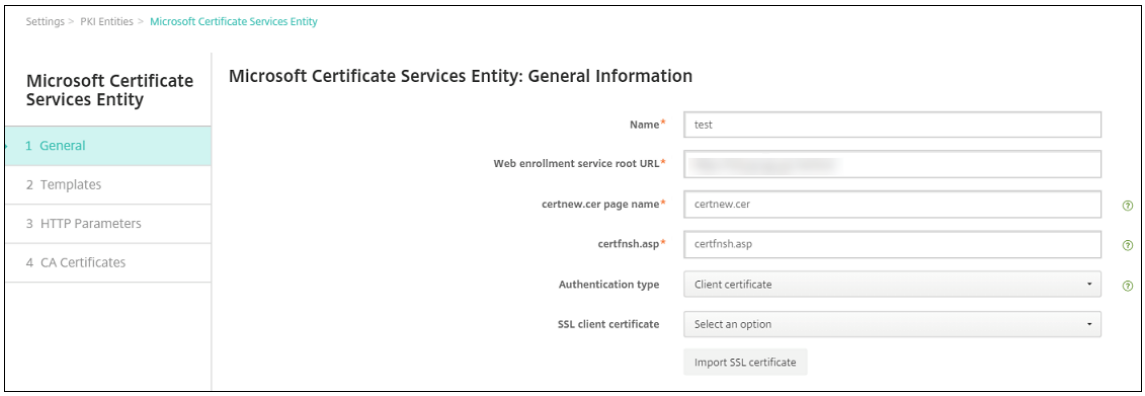
Creating the PKI entity for certificate-based authentication

1. In **Settings**, go to **More > Certificate Management > PKI Entities**.
2. Click **Add** and then click **Microsoft Certificate Services Entity**. The **Microsoft Certificate Services Entity: General Information** screen appears.
3. Enter the following parameters:

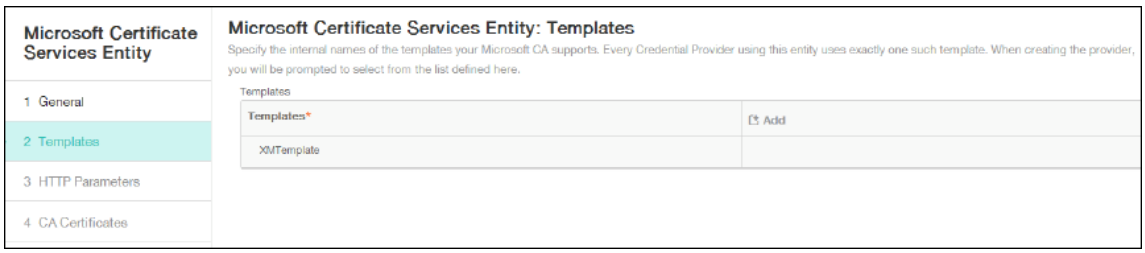
   - **Name:** Type any name.
   - **Web enrollment service root URL:** `https://RootCA-URL/certsrv/` (Be sure to add the last slash, /, in the URL path.)
   - **certnew.cer page name:** certnew.cer (default value)
   - **certfnsh.asp:** certfnsh.asp (default value)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

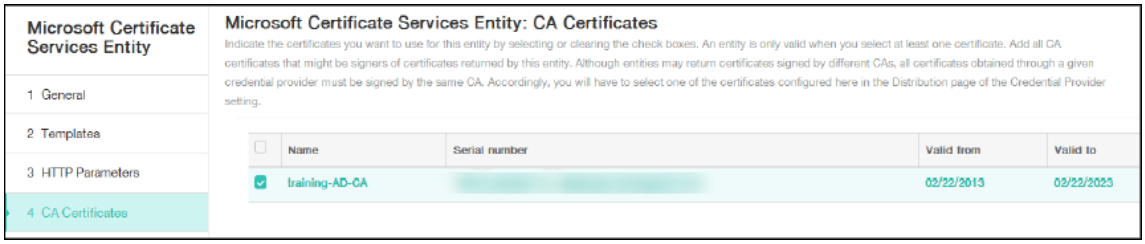
- **Authentication type:** Client certificate
- **SSL client certificate:** Select the user certificate to be used to issue the Citrix Endpoint Management client certificate. If no certificate exists, follow the procedure in the preceding section to upload certificates.



4. Under **Templates**, add the template that you created when configuring the Microsoft certificate. Don't add spaces.



5. Skip HTTP Parameters and then click **CA Certificates**.
6. Select the root CA name that corresponds to your environment. This root CA is part of the chain imported from the Citrix Endpoint Management client certificate.



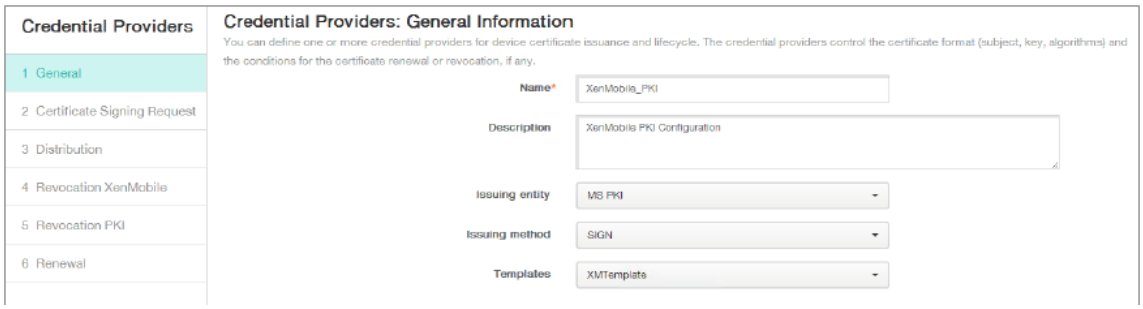
7. Click **Save**.

Configuring credentials providers

1. In **Settings**, go to **More > Certificate Management > Credential Providers**.
2. Click **Add**.
3. Under **General**, enter the following parameters:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Name:** Type any name.
- **Description:** Type any description.
- **Issuing entity:** Select the PKI entity created earlier.
- **Issuing method:** SIGN
- **Templates:** Select the template added under the PKI entity.



4. Click **Certificate Signing Request** and then enter the following parameters:

   - **Key algorithm:** RSA
   - **Key size:** 2048
   - **Signature algorithm:** SHA256withRSA
   - **Subject name:** `cn=$user.username`

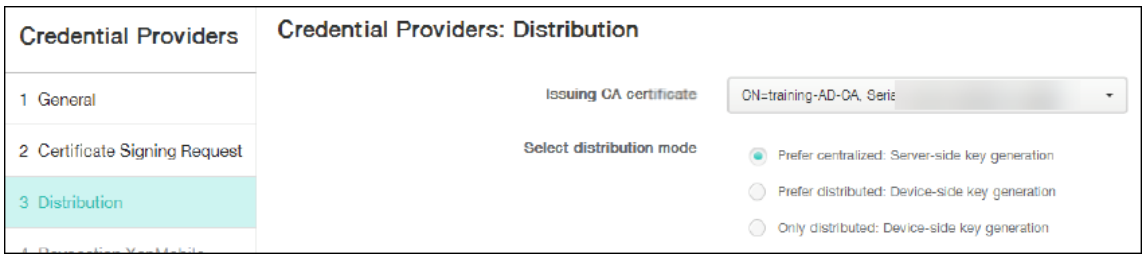
   For **Subject Alternative Names**, click **Add** and then enter the following parameters:

   - **Type:** User Principal name
   - **Value:** `$user.userprincipalname`

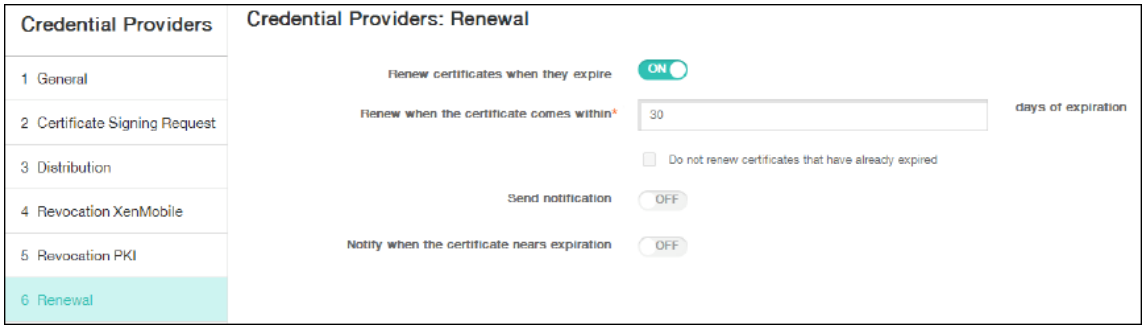
5. Click **Distribution** and enter the following parameters:

   - **Issuing CA certificate:** Select the Issuing CA that signed the Citrix Endpoint Management Client Certificate.
   - **Select distribution mode:** Select **Prefer centralized: Server-side key generation**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



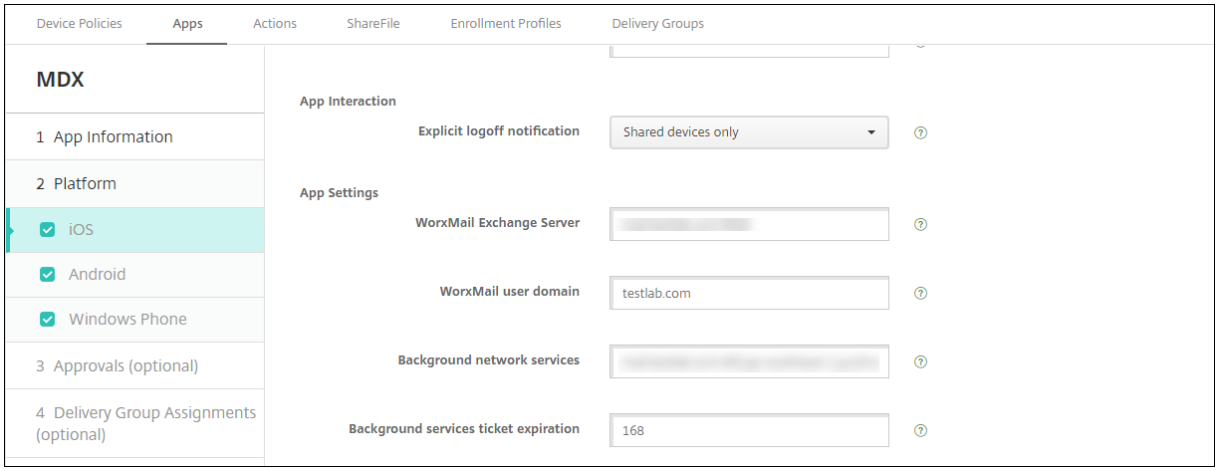
6. For the next two sections, **Revocation Citrix Endpoint Management** and **Revocation PKI**, set the parameters as required. In this example, both options are skipped.
7. Click **Renewal**.
8. Enable **Renew certificates when they expire**.
9. Leave all other settings as default or change them as required.



10. Click **Save**.

Configuring Citrix Secure Mail to use certificate-based authentication

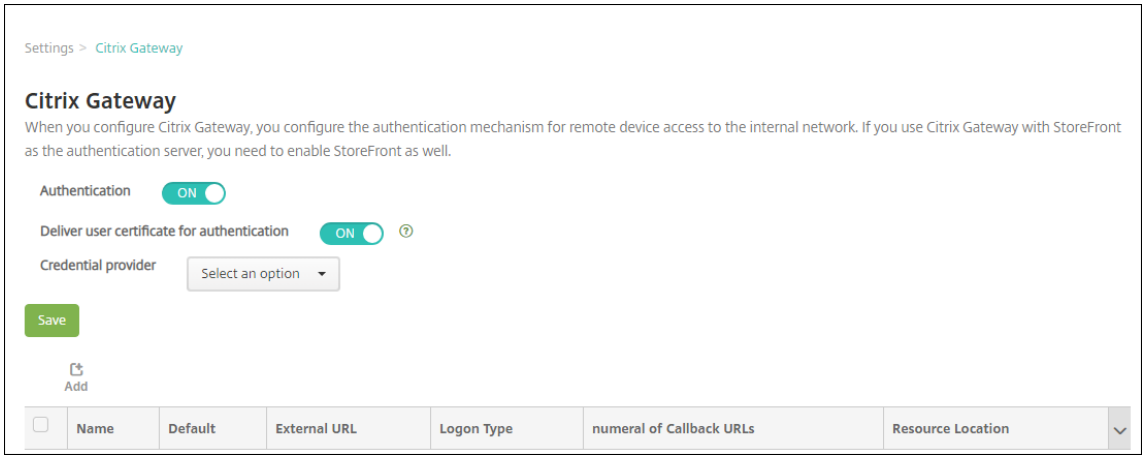
When you add Citrix Secure Mail to Citrix Endpoint Management, be sure to configure the Exchange settings under **App Settings**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

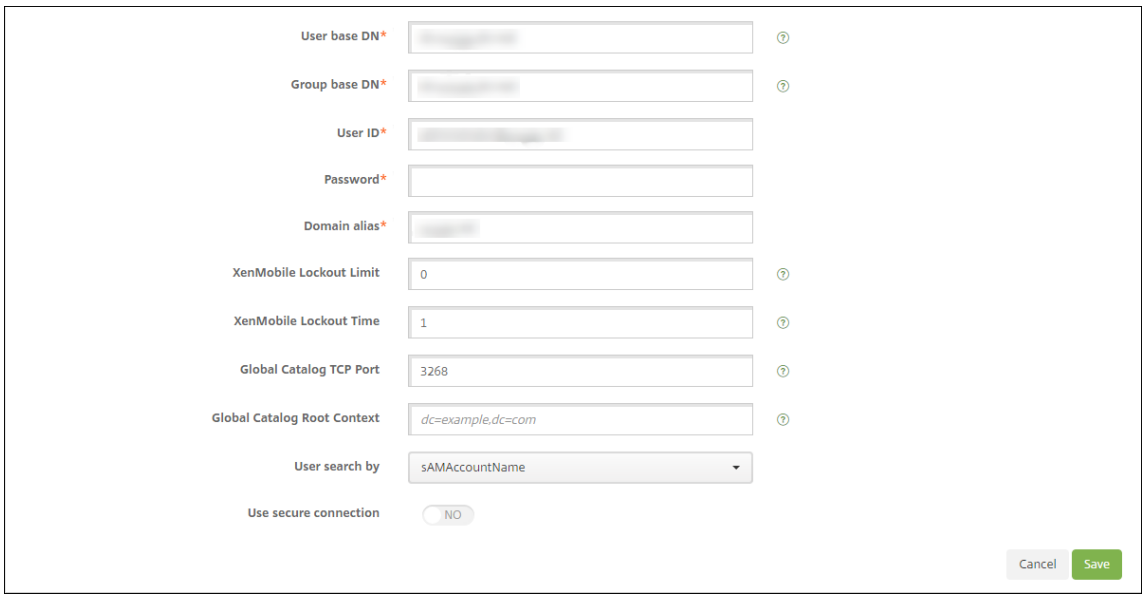
Configuring NetScaler Gateway certificate delivery in Citrix Endpoint Management

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** screen appears.
2. Under **Server**, click **NetScaler Gateway**.
3. If NetScaler Gateway isn't already added, click **Add** and specify the settings:
   - **Name:** A descriptive name for the appliance.
   - **Alias:** An optional alias for the appliance.
   - **External URL:** `https://YourCitrixGatewayURL`
   - **Logon Type:** Select **Certificate and domain**
   - **Password Required:** Off
   - **Set as Default:** On
4. For **Authentication** and **Deliver user certificate for authentication**, select **On**.



5. For **Credential Provider**, select a provider and then click **Save**.
6. To use the sAMAccount attributes in the user certificates as an alternative to User Principal Name (UPN), configure the LDAP connector in Citrix Endpoint Management as follows: Go to **Settings > LDAP**, select the directory and click **Edit**, and select **sAMAccountName** in **User search by**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Enable Citrix PIN and user password caching

To enable Citrix PIN and user password caching, go to **Settings > Client Properties** and select these checkboxes: **Enable Citrix PIN Authentication** and **Enable User Password Caching**. For more information, see Client properties.

Troubleshooting your client certificate configuration

After a successful configuration of the preceding configuration plus the NetScaler Gateway configuration, the user workflow is as follows:

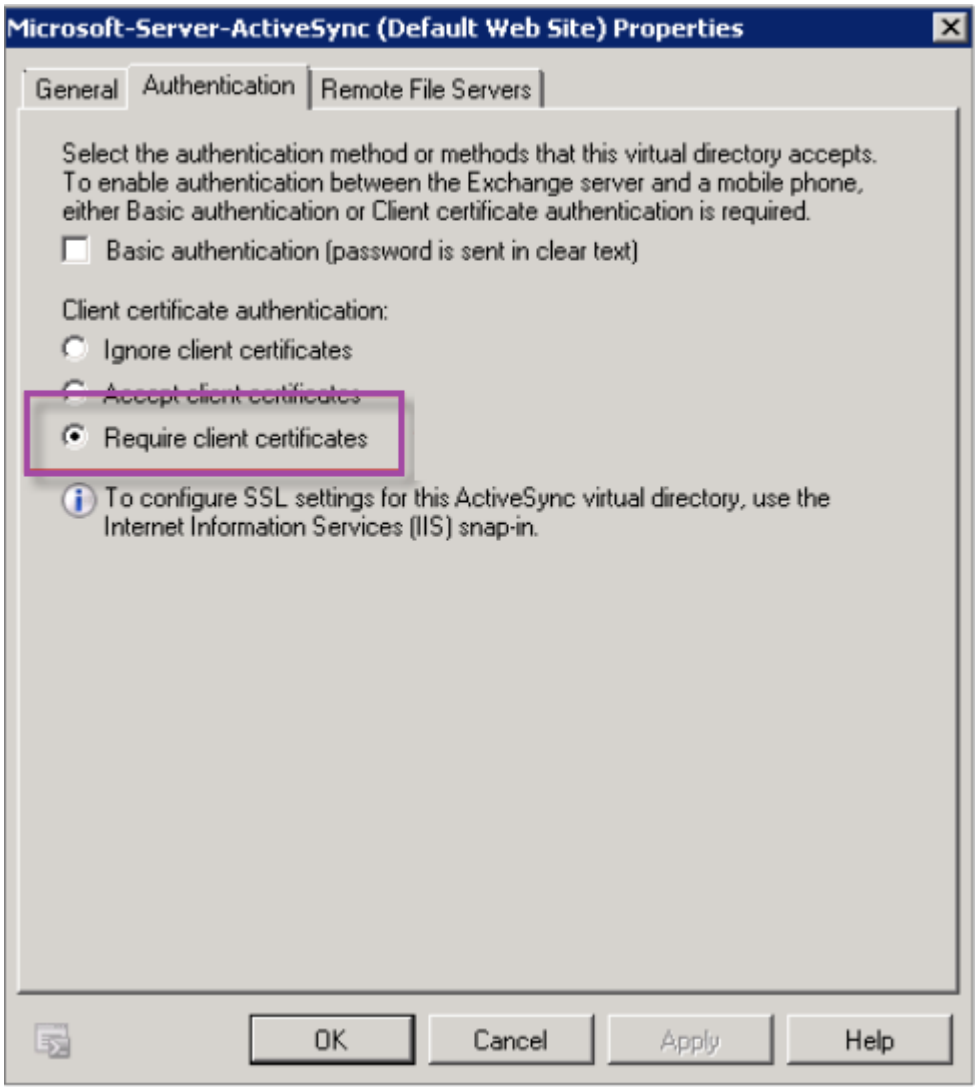
1. Users enroll their mobile device.
2. Citrix Endpoint Management prompts users to create a Citrix PIN.
3. Users are then redirected to the app store.
4. When users start Citrix Secure Mail, Citrix Endpoint Management doesn't prompt them for user credentials for mailbox configuration. Instead, Citrix Secure Mail requests the client certificate from Citrix Secure Hub and submits it to the Microsoft Exchange Server for authentication. If Citrix Endpoint Management prompts for credentials when users start Citrix Secure Mail, check your configuration.

If users can download and install Citrix Secure Mail, but during the mailbox configuration Citrix Secure Mail fails to finish the configuration:

1. If Microsoft Exchange Server ActiveSync uses private SSL server certificates to secure the traffic, verify that the Root/Intermediate certificates installed on the mobile device.

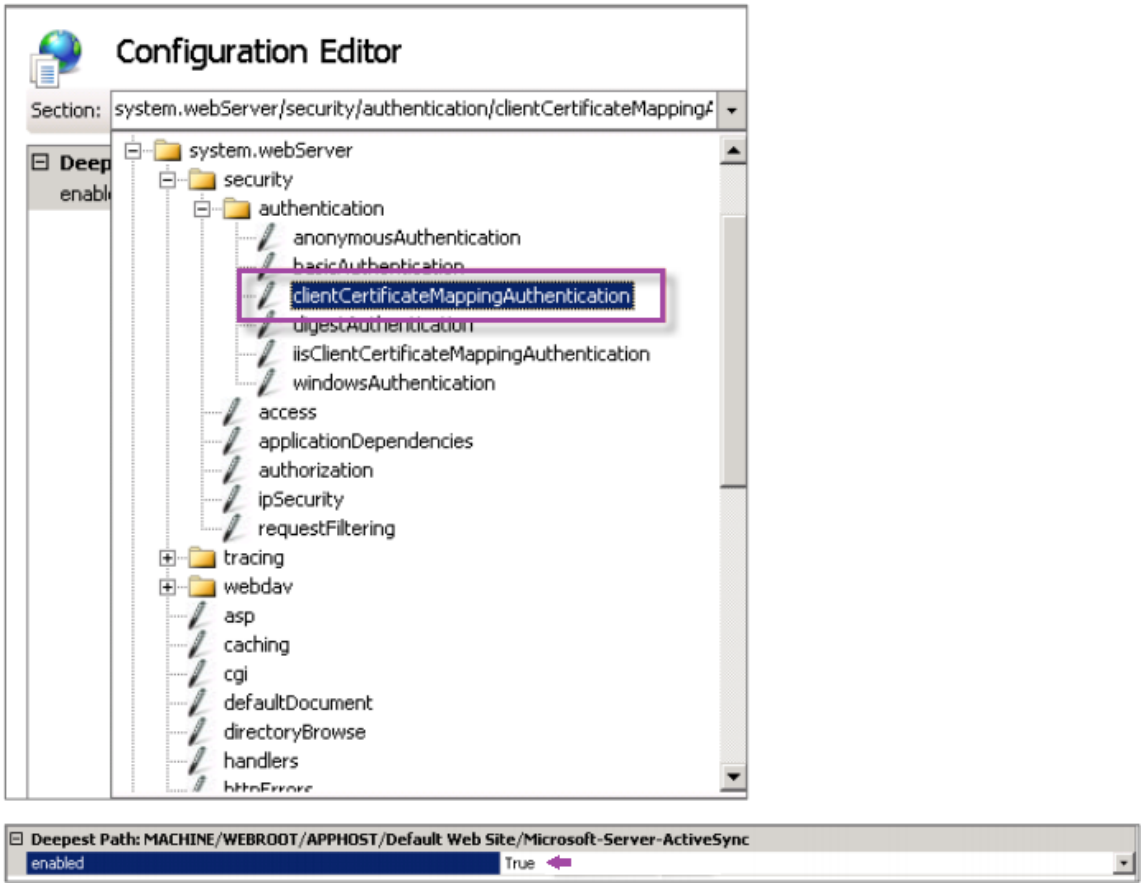
© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Verify that the authentication type selected for ActiveSync is set as **Require client certificates**.



3. On the Microsoft Exchange Server, check the **Microsoft-Server-ActiveSync** site to verify that client certificate mapping authentication is enabled. By default client certificate mapping authentication is disabled. The option is under **Configuration Editor > Security > Authentication**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



After selecting **True**, be sure to click **Apply** for the changes take effect.

4. Check the NetScaler Gateway settings in the Citrix Endpoint Management console: Make sure that **Deliver user certificate for authentication** is **On** and that **Credential provider** has the correct profile selected.

To determine if the client certificate was delivered to a mobile device

1. In the Citrix Endpoint Management console, go to **Manage > Devices** and select the device.
2. Click **Edit** or **Show More**.
3. Go to the **Delivery Groups** section, and search for this entry:

   NetScaler Gateway Credentials: Requested credential, CertId=

To validate whether client certificate negotiation is enabled

1. Run this `netsh` command to show the SSL Certificate configuration that is bound on the IIS website:

   ```
   netsh http show sslcert
   ```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. If the value for **Negotiate Client Certificate** is **Disabled**, run the following command to enable it:

   ```
   netsh http delete sslcert ipport=0.0.0.0:443
   ```

   ```
   netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash
   appid={ app_id } certstorename=store_name verifyclientcertrevocation
   =Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck
   =Enable clientcertnegotiation=Enable
   ```

   For example:

   ```
   netsh http add sslcert ipport=0.0.0.0:443 certhash=23498dfsdfhaf98rhkjqf98
    appid={ 123asd456jd-a12b-3c45-d678-123456lkjhgf } certstorename=
   ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWit
   =Disable UsageCheck=Enable clientcertnegotiation=Enable
   ```

If you cannot deliver Root/Intermediate certificates to a Windows Phone 8.1 device through Citrix Endpoint Management:

- Send Root/Intermediate certificates (.cer) files through email to the Windows Phone 8.1 device and install them directly.

If Citrix Secure Mail doesn't install successfully on Windows Phone 8.1, verify the following:

- The Application Enrollment Token (.AETX file) is delivered through Citrix Endpoint Management using the Enterprise Hub device policy.
- The Application Enrollment Token was created using the same Enterprise Certificate from the certificate provider used to wrap Citrix Secure Mail and sign Citrix Secure Hub apps.
- The same Publisher ID is used to sign and wrap Citrix Secure Hub, Citrix Secure Mail, and the Application Enrollment Token.

PKI entities

September 6, 2025

An Citrix Endpoint Management Public Key Infrastructure (PKI) entity configuration represents a component doing actual PKI operations (issuance, revocation, and status information). These components are either internal or external to Citrix Endpoint Management. Internal components are referred to as discretionary. External components are part of your corporate infrastructure.

Citrix Endpoint Management supports the following types of PKI entities:

- Microsoft Certificate Services

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Discretionary Certificate Authorities (CAs)

Citrix Endpoint Management supports the following CA servers:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

> **Note:**
>
> Windows Servers 2012 R2, 2012, and 2008 R2 are no longer supported as they have reached end of life. For more information, see Microsoft products life cycle documentation.

Common PKI concepts

Regardless of its type, every PKI entity has a subset of the following capabilities:

- **Sign:** Issuing a new certificate, based on a Certificate Signing Request (CSR).
- **Fetch:** Recovering an existing certificate and key pair.
- **Revoke:** Revoking a client certificate.

About CA certificates

When you configure a PKI entity, indicate to Citrix Endpoint Management which CA certificate is the signer of certificates issued by (or recovered from) that entity. That PKI entity can return (fetched or newly signed) certificates signed by any number of different CAs.

Provide the certificate of each of these authorities as part of the PKI entity configuration. To do so, upload the certificates to Citrix Endpoint Management and then reference them in the PKI entity. For discretionary CAs, the certificate is implicitly the signing CA certificate. For external entities, you must specify the certificate manually.

> **Important:**
>
> When you create a Microsoft Certificate Services Entity template, avoid possible authentication issues with enrolled devices: Don't use special characters in the template name. For example, don't use: `! : $ ( )# % + * ~ ? | { } [ ]`

Microsoft Certificate Services

Citrix Endpoint Management interfaces with Microsoft Certificate Services through its web enrollment interface. Citrix Endpoint Management only supports the issuing of new certificates through that interface. If the Microsoft CA generates a NetScaler Gateway user certificate, NetScaler Gateway supports renewal and revocation for those certificates.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To create a Microsoft CA PKI entity in Citrix Endpoint Management, you must specify the base URL of the Certificate Services web interface. If you choose, use SSL client authentication to secure the connection between Citrix Endpoint Management and the Certificate Services web interface.

Add a Microsoft Certificate Services entity

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console and then click **PKI Entities**.
2. On the **PKI Entities** page, click **Add**.

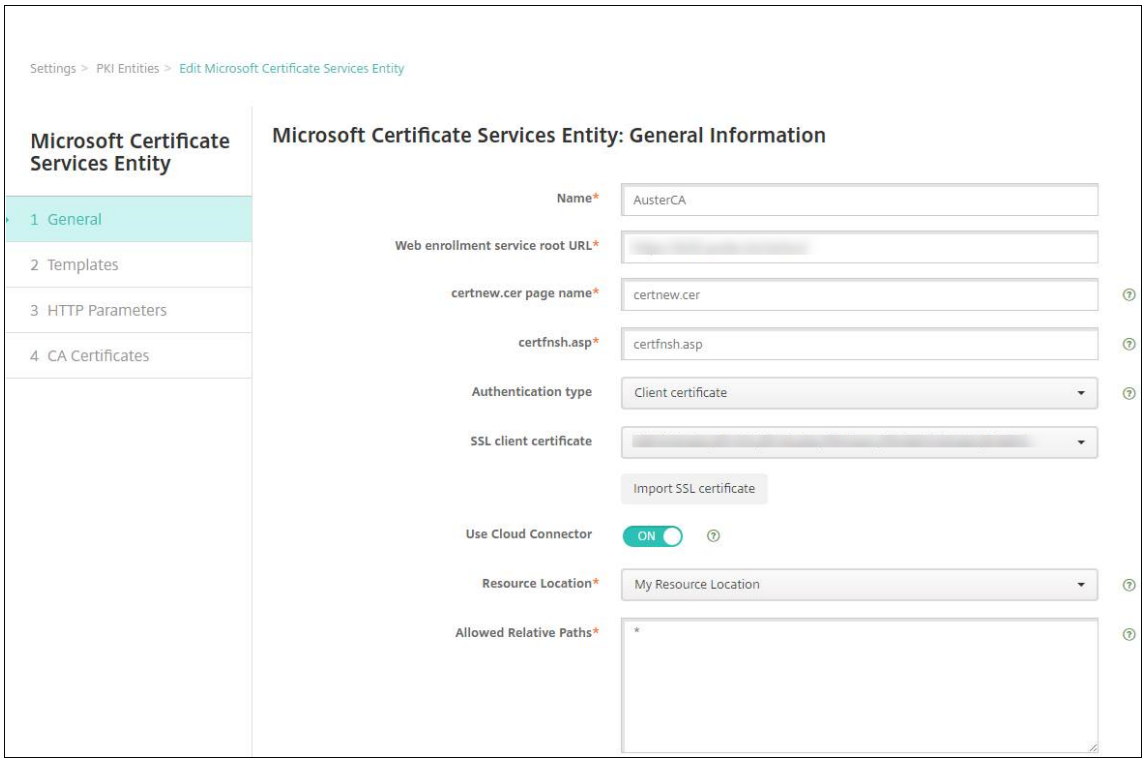
   A menu of PKI entity types appears.
3. Click **Microsoft Certificate Services Entity**.

   The **Microsoft Certificate Services Entity: General Information** page appears.
4. On the **Microsoft Certificate Services Entity: General Information** page, configure these settings:

   - **Name:** Type a name for your new entity, which you use later to refer to that entity. Entity names must be unique.
   - **Web enrollment service root URL:** Type the base URL of your Microsoft CA web enrollment service. For example: `https://192.0.0.1/certsrv/`. The URL can use plain HTTP or HTTP-over-SSL.
   - **certnew.cer page name:** The name of the certnew.cer page. Use the default name unless you have renamed it for some reason.
   - **certfnsh.asp:** The name of the certfnsh.asp page. Use the default name unless you have renamed it for some reason.
   - **Authentication type:** Choose the authentication method that you want to use.
     - **None**
     - **HTTP Basic:** Type the user name and password required to connect.
     - **Client certificate:** Choose the correct SSL client certificate.
   - **Use Cloud Connector:** Choose **On** to use Cloud Connector for connections to the PKI server. Then, specify a **Resource Location** and **Allowed Relative Paths** for the connection.
     - **Resource Location:** Choose from the resource locations defined in Citrix Cloud Connector.
     - **Allowed Relative Paths:** The relative paths allowed for the specified resource location. Specify one path per line. You can use the asterisk (*) wildcard.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Suppose that the resource location is `https://www.ServiceRoot/certsrv`. To provide access to all URLs in that path, enter `/*` in **Allowed Relative Paths**.



5. Click **Test Connection** to make sure that the server is accessible. If it is not accessible, a message appears, stating that the connection failed. Check your configuration settings.
6. Click **Next**.

   The **Microsoft Certificate Services Entity: Templates** page appears. On this page, you specify the internal names of the templates your Microsoft CA supports. When creating credential providers, you select a template from the list defined here. Every credential provider using this entity uses exactly one such template.

   For Microsoft Certificate Services template requirements, see the Microsoft documentation for your Microsoft Server version. Citrix Endpoint Management doesn't have requirements for the certificates it distributes other than the certificate formats noted in Certificates.
7. On the **Microsoft Certificate Services Entity: Templates** page, click **Add**, type the name of the template and then click **Save**. Repeat this step for each template that you want to add.
8. Click **Next**.

   The **Microsoft Certificate Services Entity: HTTP parameters** page appears. On this page, you specify custom parameters for Citrix Endpoint Management to add to the HTTP request to the Microsoft Web Enrollment interface. Custom parameters are useful only for customized scripts running on the CA.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

9. On the **Microsoft Certificate Services Entity: HTTP parameters** page, click **Add**, type the name and value of the HTTP parameters you want to add, and then click **Next**.

   The **Microsoft Certificate Services Entity: CA Certificates** page appears. On this page, you must inform Citrix Endpoint Management of the signers of the certificates that the system gets through this entity. When your CA certificate is renewed, update it in Citrix Endpoint Management. Citrix Endpoint Management applies the change to the entity transparently.

10. On the **Microsoft Certificate Services Entity: CA Certificates** page, select the certificates you want to use for this entity.

11. Click **Save**.

    The entity appears on the PKI Entities table.

NetScaler Gateway Certificate Revocation List (CRL)

Citrix Endpoint Management supports Certificate Revocation List (CRL) only for a third-party Certificate Authority. If you have a Microsoft CA configured, Citrix Endpoint Management uses NetScaler Gateway to manage revocation.

When you configure client certificate-based authentication, consider whether to configure the NetScaler Gateway Certificate Revocation List (CRL) setting **Enable CRL Auto Refresh**. This step makes sure that the user of a device in MAM-only mode can't authenticate using an existing certificate on the device.

Citrix Endpoint Management reissues a new certificate, because it doesn't restrict a user from generating a user certificate after one is revoked. This setting increases the security of PKI entities when the CRL checks for expired PKI entities.

Discretionary CAs

A discretionary CA is created when you provide Citrix Endpoint Management with a CA certificate and the associated private key. Citrix Endpoint Management handles certificate issuance, revocation, and status information internally, according to the parameters you specify.

When configuring a discretionary CA, you can activate Online Certificate Status Protocol (OCSP) support for that CA. If you enable OCSP support, the CA adds the extension `id-pe-authorityInfoAccess` to the certificates that the CA issues. The extension points to the Citrix Endpoint Management internal OCSP Responder at the following location:

```
https://<server>/<instance>/ocsp
```

When configuring the OCSP service, specify an OCSP signing certificate for the discretionary entity in question. You can use the CA certificate itself as the signer. To avoid the unnecessary exposure

© 1997–2025 Citrix Systems, Inc. All rights reserved.

of your CA private key (recommended): Create a delegate OCSP signing certificate, signed by the CA certificate, and include this extension: `id-kp-OCSPSigning extendedKeyUsage`.

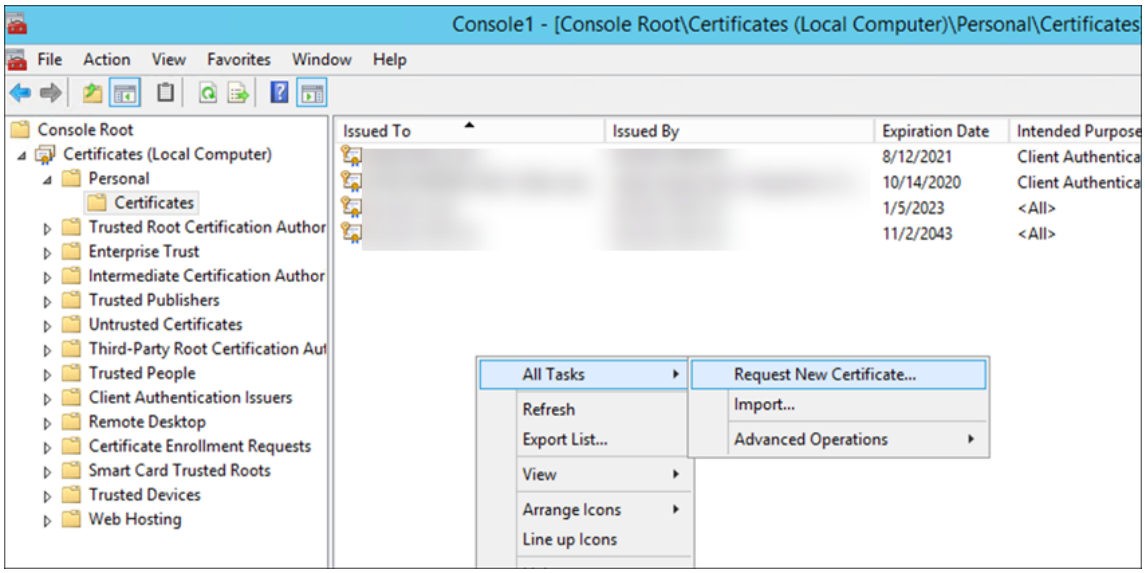
The Citrix Endpoint Management OCSP responder service supports basic OCSP responses and the following hashing algorithms in requests:

- SHA-256
- SHA-384
- SHA-512

Responses are signed with SHA-256 and the signing certificate key algorithm (DSA, RSA, or ECDSA).

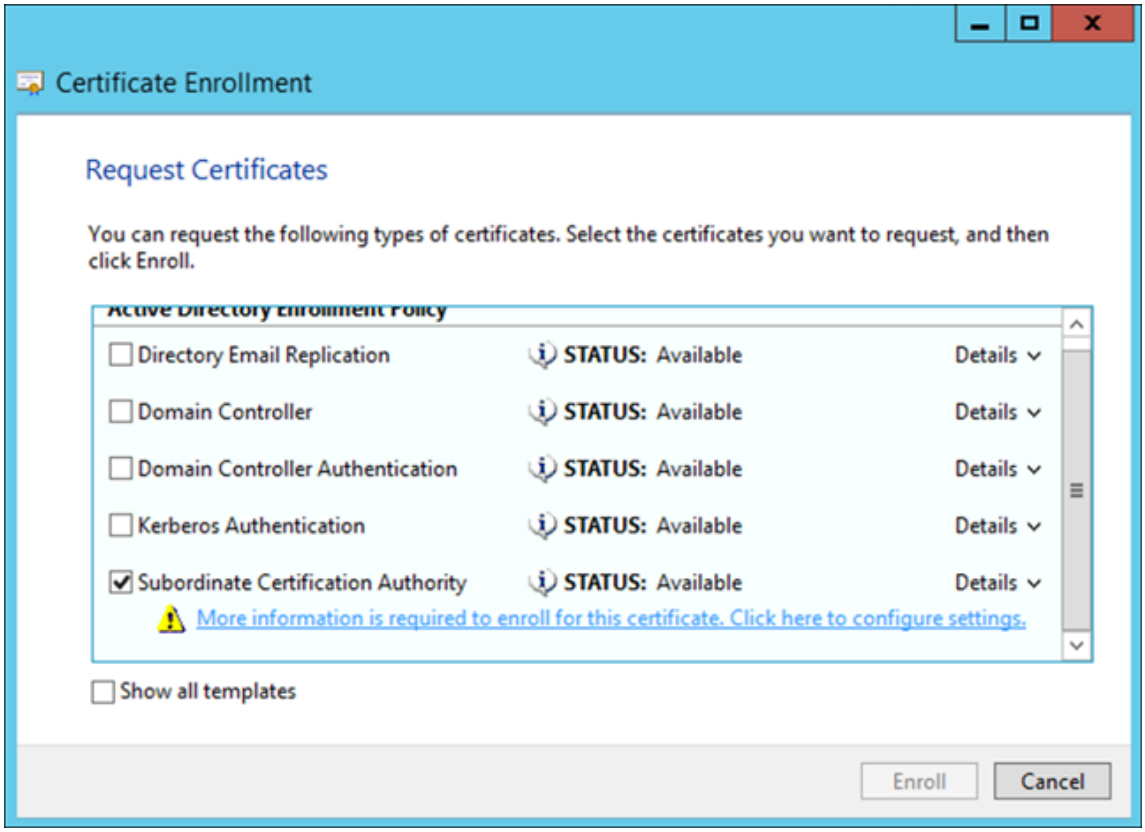
Generate and import a certificate for your CA

1. On your server, open the Microsoft Management Console (MMC) with your Local System account, and open the certificate snap-in. In the pane on the right, right-click and then click **All Tasks > Request New Certificate**.



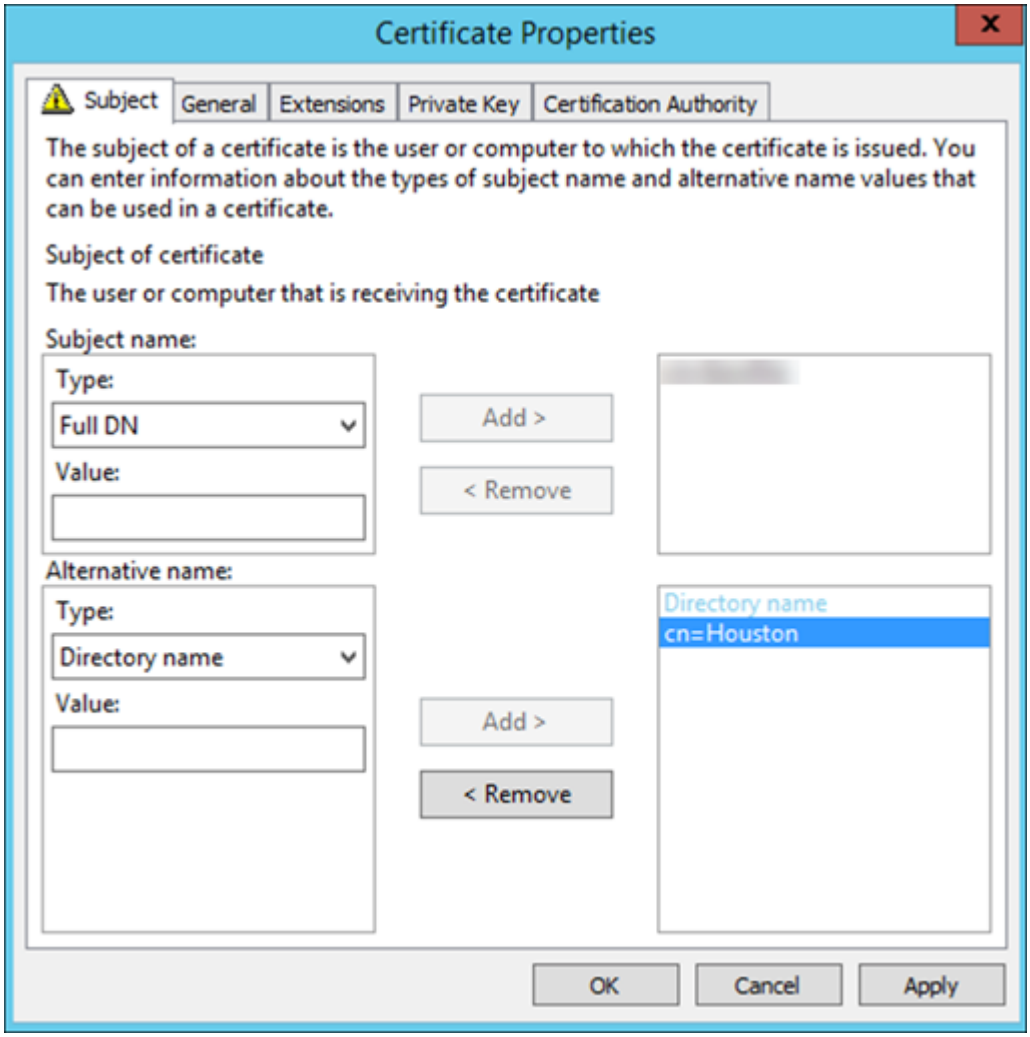
2. In the wizard that opens, click **Next** twice. In the **Request Certificates** list, select **Subordinate Certification Authority** and then click the **More information** link.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



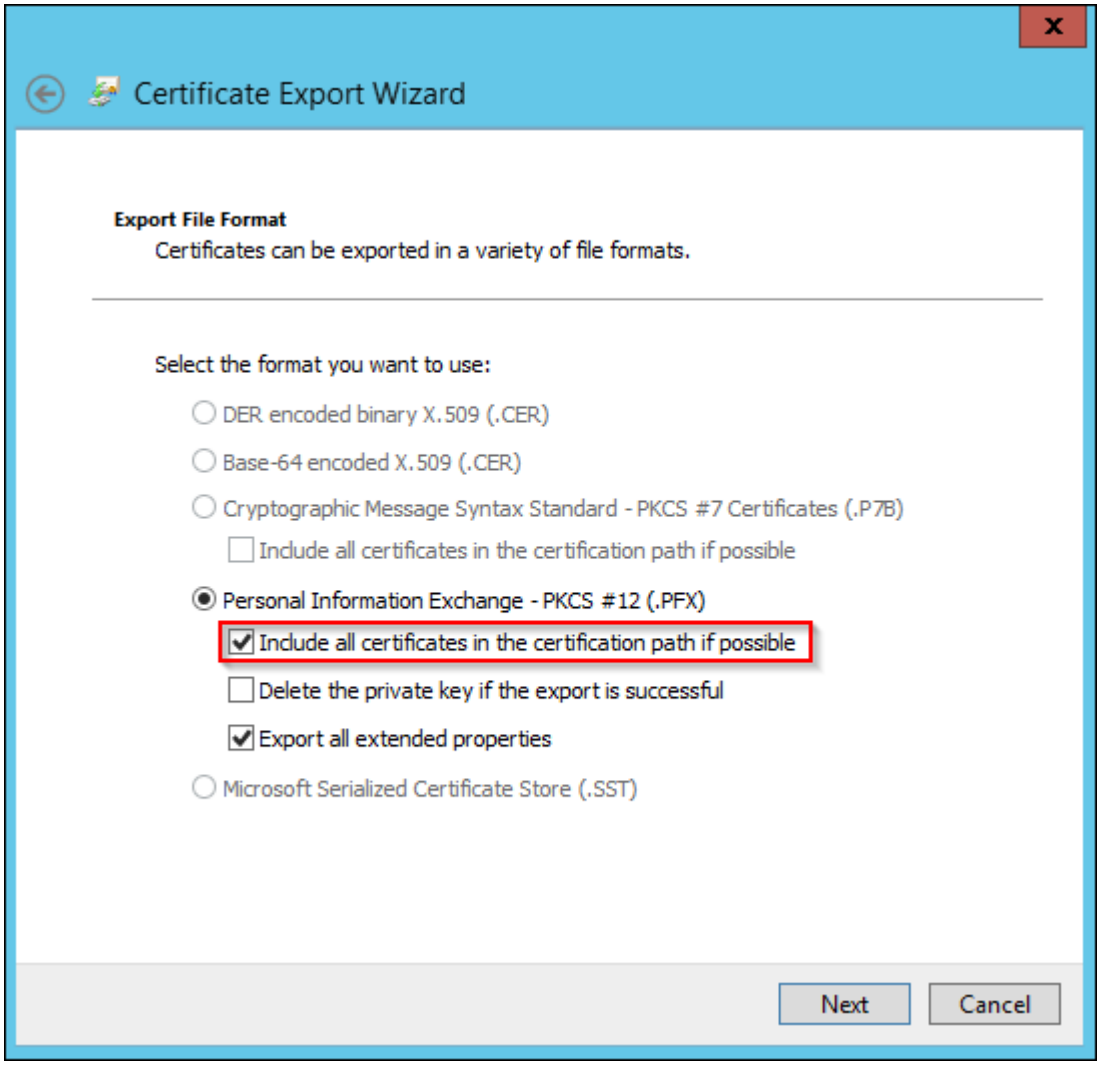
3. In the window, type a **Subject name** and **Alternative name**. Click **OK**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

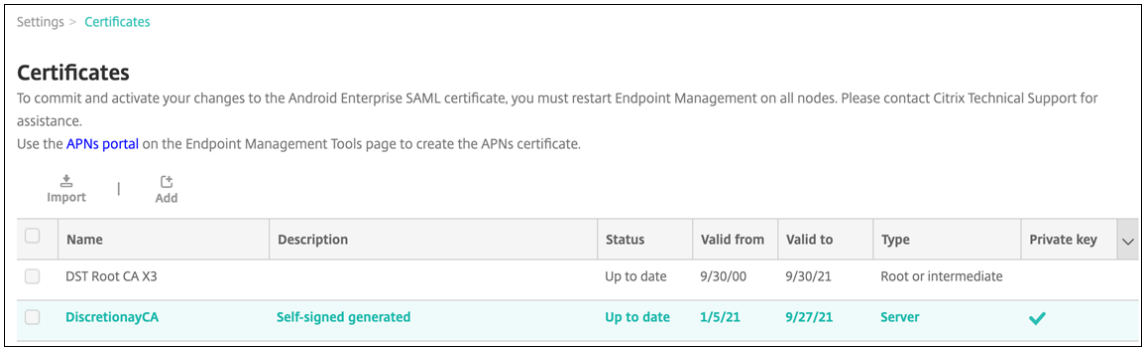


4. Click **Enroll**, and then click **Finish**.
5. In the MMC, right-click the certificate you created. Click **All Tasks > Export**. Export the certificate as a .pfx file with a private key. Select the option to **Include all certificates in the certification path if possible**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

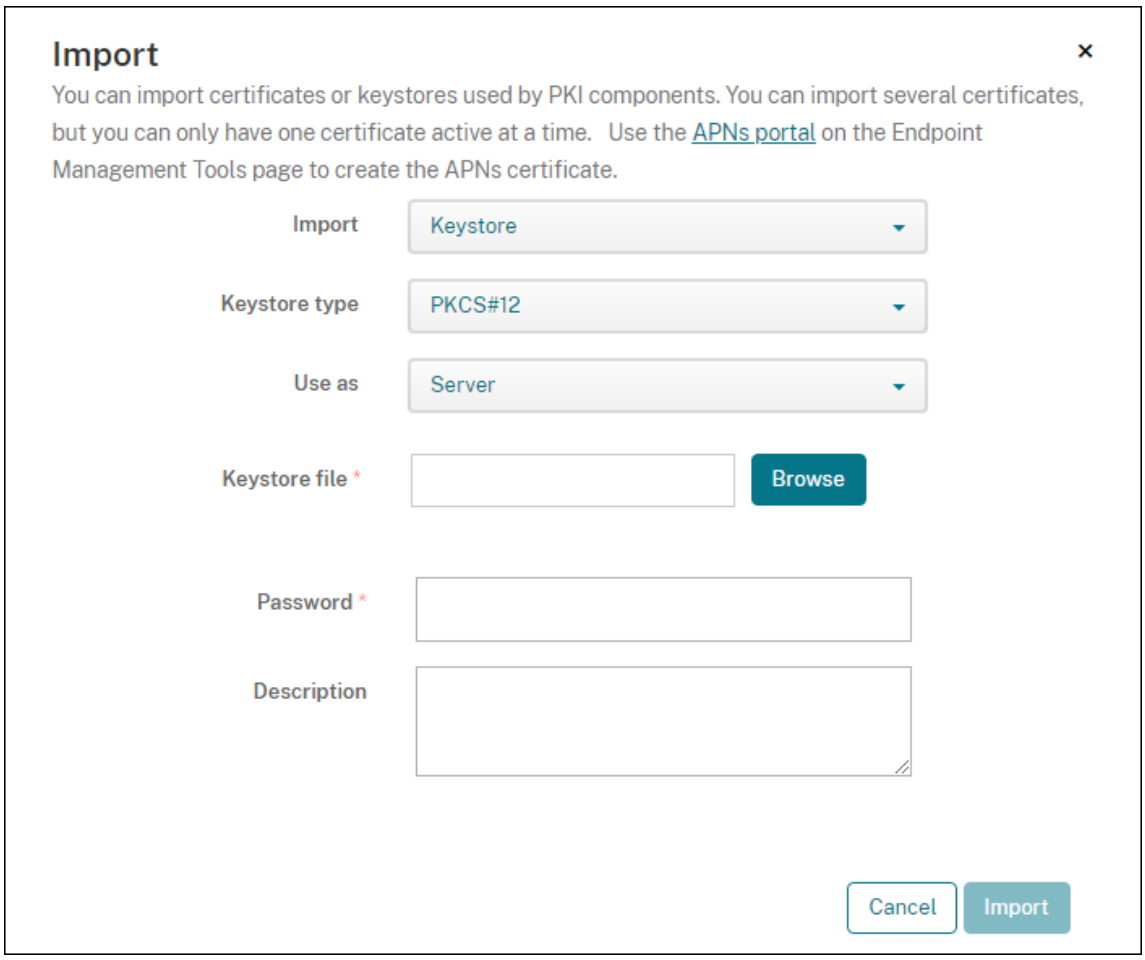


6. In the Citrix Endpoint Management console, navigate to **Settings > Certificates**.



7. Click **Import**. In the window that opens, browse for the certificate and private key files you exported previously.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

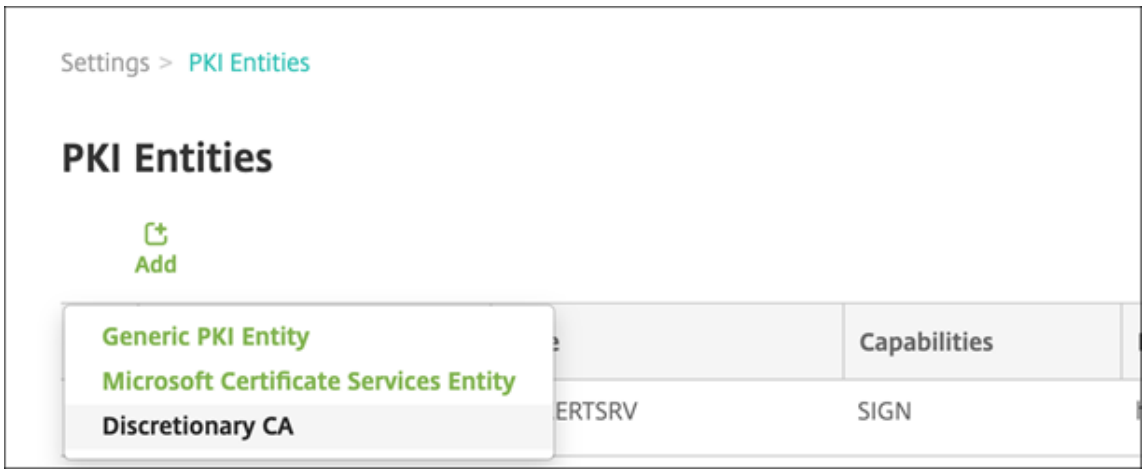


8. Click **Import**. The certificate is added to the table.

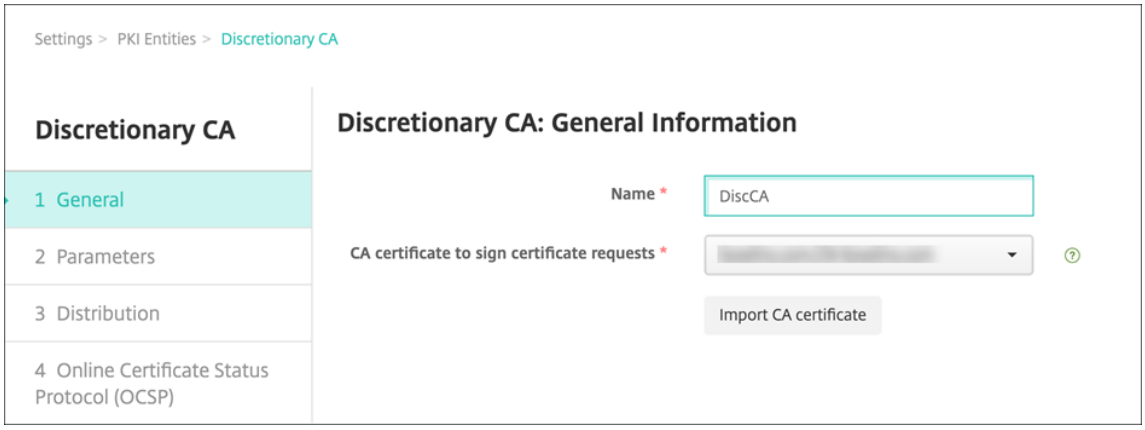
Add discretionary CAs

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console and then click **More > PKI Entities**.
2. On the **PKI Entities** page, click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Click **Discretionary CA**.



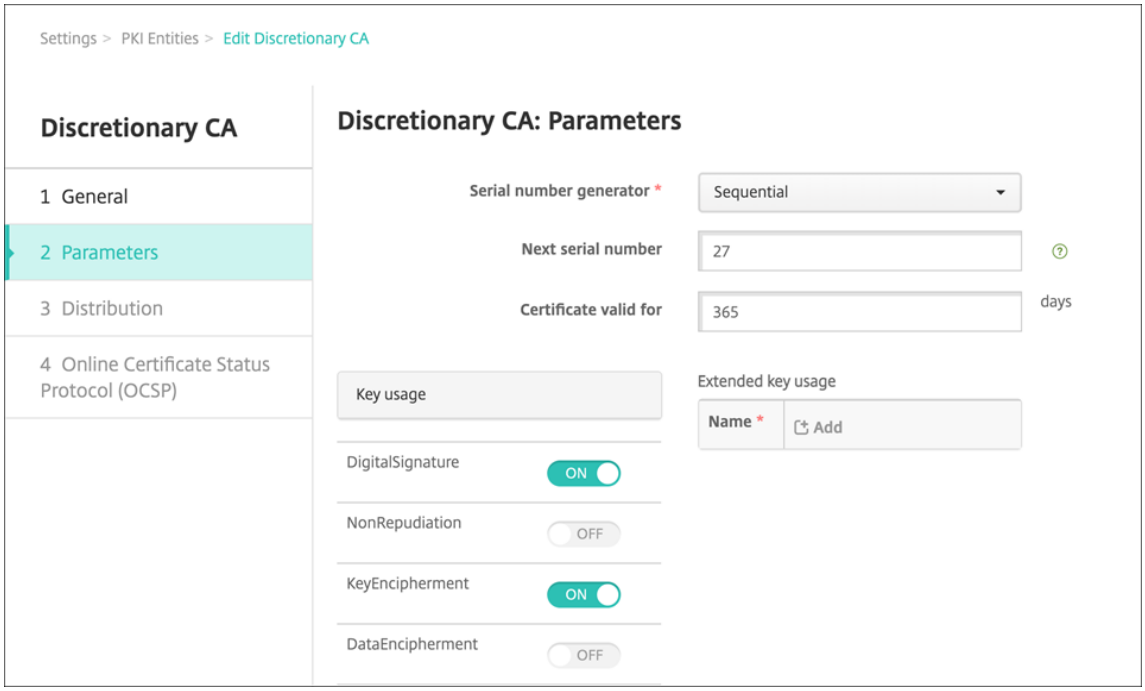
4. On the **Discretionary CA: General Information** page, configure the following:

   - **Name:** Type a descriptive name for the discretionary CA.
   - **CA certificate to sign certificate requests:** Click a certificate for the discretionary CA to use to sign certificate requests.

     This list of certificates is generated from the CA certificates with private keys you uploaded at Citrix Endpoint Management at **Configure > Settings > Certificates**.

5. Click **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

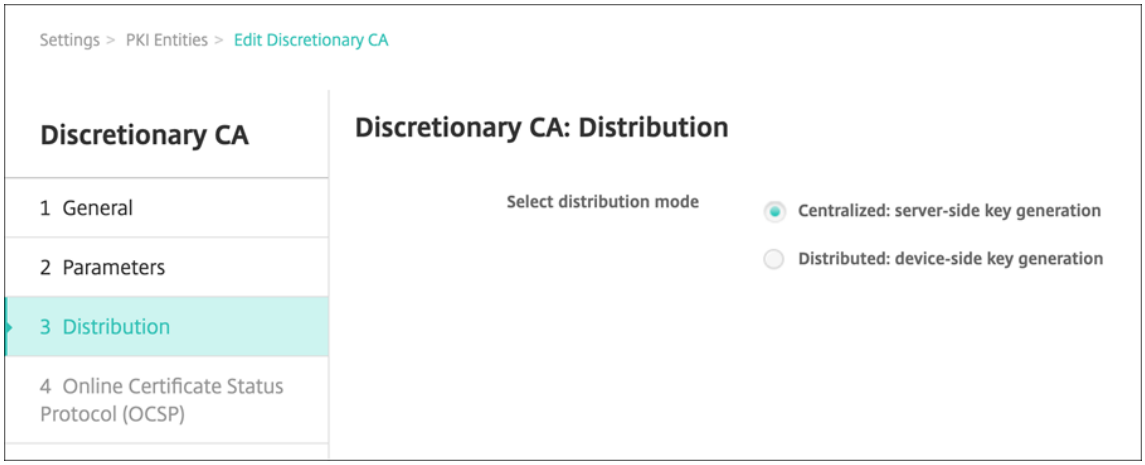


6. On the **Discretionary CA: Parameters** page, configure the following:

   - **Serial number generator:** The discretionary CA generates serial numbers for the certificates it issues. From this list, click **Sequential** or **Non-sequential** to determine how the numbers are generated.
   - **Next serial number:** Type a value to determine the next number issued.
   - **Certificate valid for:** Type the number of days the certificate is valid.
   - **Key usage:** Identify the purpose of the certificates issued by the discretionary CA by setting the appropriate keys to **On**. Once set, the CA is limited to issuing certificates for those purposes.
   - **Extended key usage:** To add more parameters, click **Add**, type the key name and then click **Save**.

7. Click **Next**.

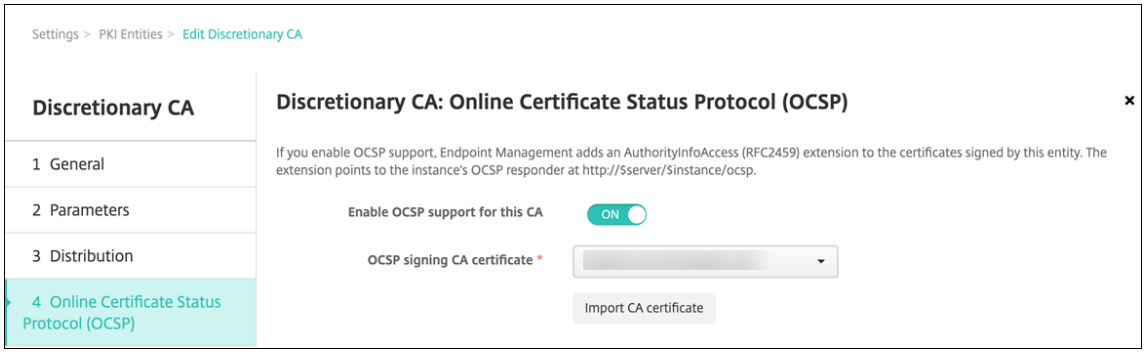
© 1997–2025 Citrix Systems, Inc. All rights reserved.



8. On the **Discretionary CA: Distribution** page, select a distribution mode:

   - **Centralized: server-side key generation**. Citrix® recommends the centralized option. The private keys are generated and stored on the server and distributed to user devices.
   - **Distributed: device-side key generation**. The private keys are generated on the user devices. This distributed mode uses SCEP and requires an RA encryption certificate with the **keyUsage keyEncryption** extension and an RA signing certificate with the **keyUsage digitalSignature** extension. The same certificate can be used for both encryption and signing.

9. Click **Next**.



10. On the **Discretionary CA: Online Certificate Status Protocol (OCSP)** page, configure the following:

    - If you want to add an `AuthorityInfoAccess` (RFC2459) extension to the certificates signed by this CA, set **Enable OCSP support for this CA** to **On**. This extension points to the CA OCSP responder at `https://<server>/<instance>/ocsp`.
    - If you enabled OCSP support, select an OSCP signing CA certificate. This list of certificates is generated from the CA certificates you uploaded to Citrix Endpoint Management.

    Enabling the feature gives the Citrix ADC an opportunity to check the status of certificates. Citrix recommends that you enable this feature.

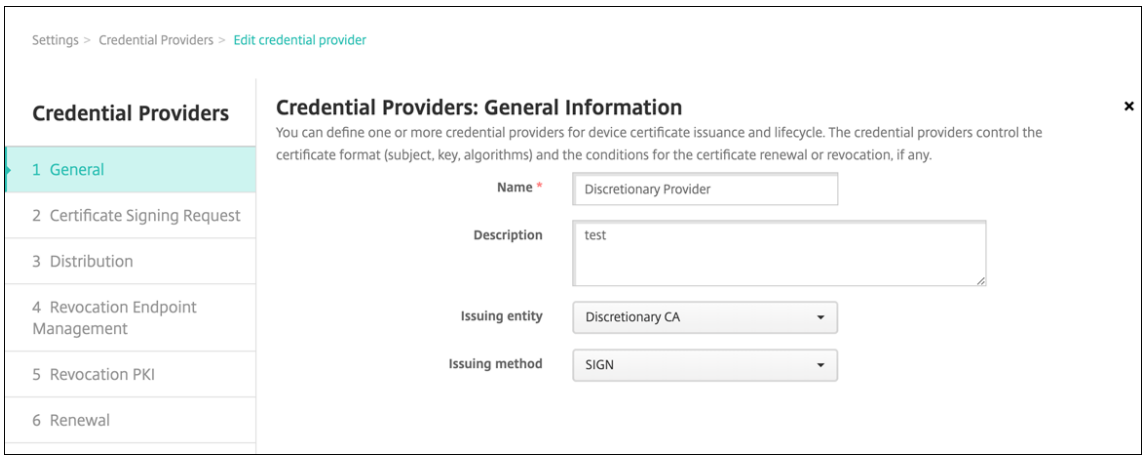
© 1997–2025 Citrix Systems, Inc. All rights reserved.

11. Click **Save**.

    The discretionary CA appears on the PKI Entities table.

Configure a credential provider

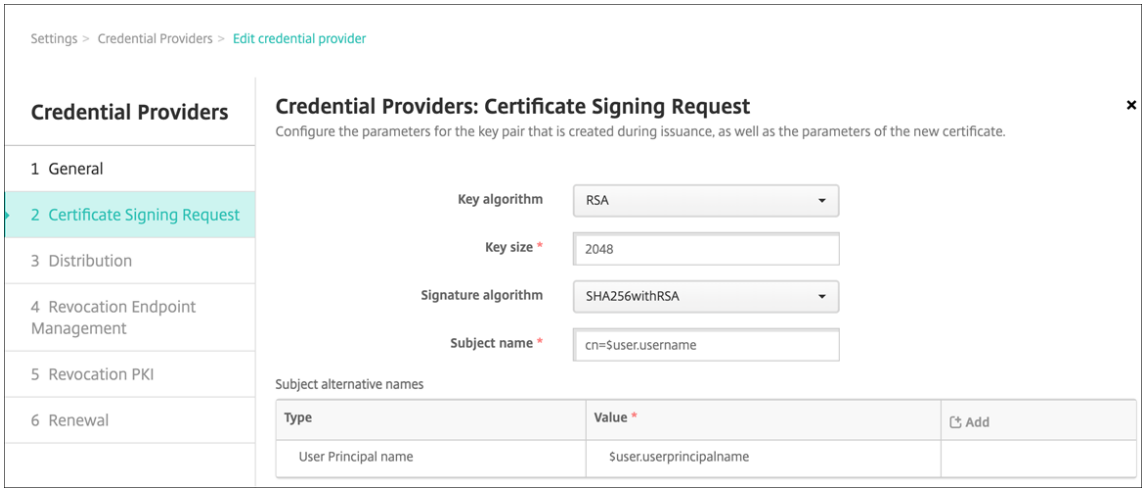
1. In the Citrix Endpoint Management console, navigate to **Settings > Credential Provider**, and click **Add**.
2. On the **Credential Providers: General Information** page, configure the following:



   - **Name:** Type a unique name for the new provider configuration. This name is used later to identify the configuration in other parts of the Citrix Endpoint Management console.
   - **Description:** Describe the credential provider. Although this field is optional, a description can provide useful details about this credential provider.
   - **Issuing entity:** Select **Discretionary CA**.
   - **Issuing method:** Click **Sign** or **Fetch** to serve as the method that the system uses to get certificates from the configured entity. For client certificate authentication, use **Sign**.

3. Click **Next**. On the **Credential Providers: Certificate Signing Request** page, configure the following according to your certificate configuration:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Key algorithm:** Choose the key algorithm for the new key pair. Available values are **RSA**, **DSA**, and **ECDSA**.
- **Key size:** Type the size, in bits, of the key pair. This field is required. Citrix recommends using **2048** bits.
- **Signature algorithm:** Click a value for the new certificate. Values depend on the key algorithm. Citrix recommends **SHA256withRSA**.
- **Subject name:** Required. Type the Distinguished Name (DN) of the new certificate subject. Use `CN=${ user.username }` for the user name or `CN=${ user.samaccountname }` to use the sAMAccountName.
- To add an entry to the **Subject alternative names** table, click **Add**. Select the type of alternative name and then type a value in the second column.

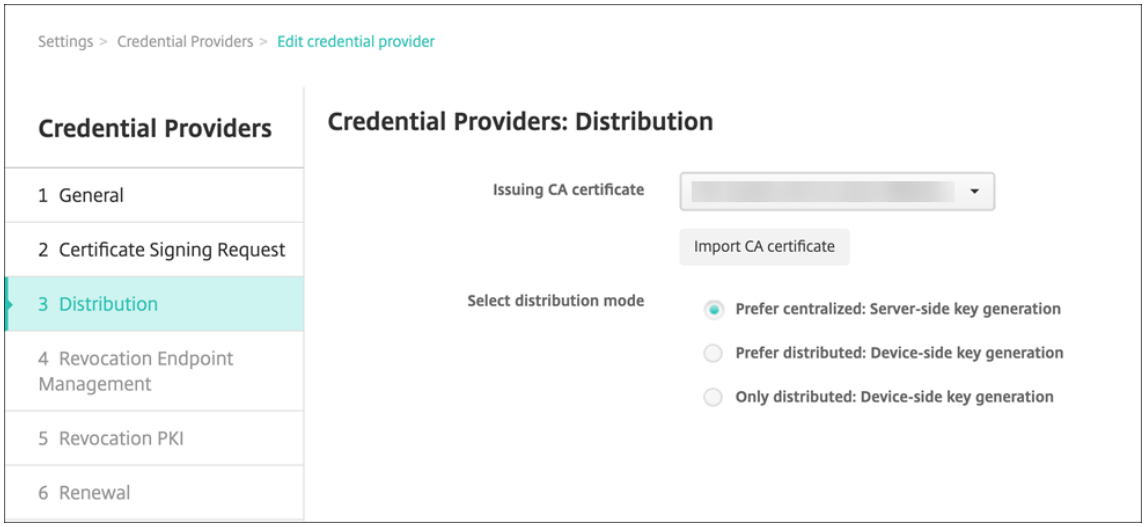
  Add the following:

  - **Type:** User Principal name
  - **Value:** `$user.userprincipalname`

  As with the subject name, you can use Citrix Endpoint Management macros in the value field.

4. Click **Next**. On the **Credential Providers: Distribution** page, configure the following:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

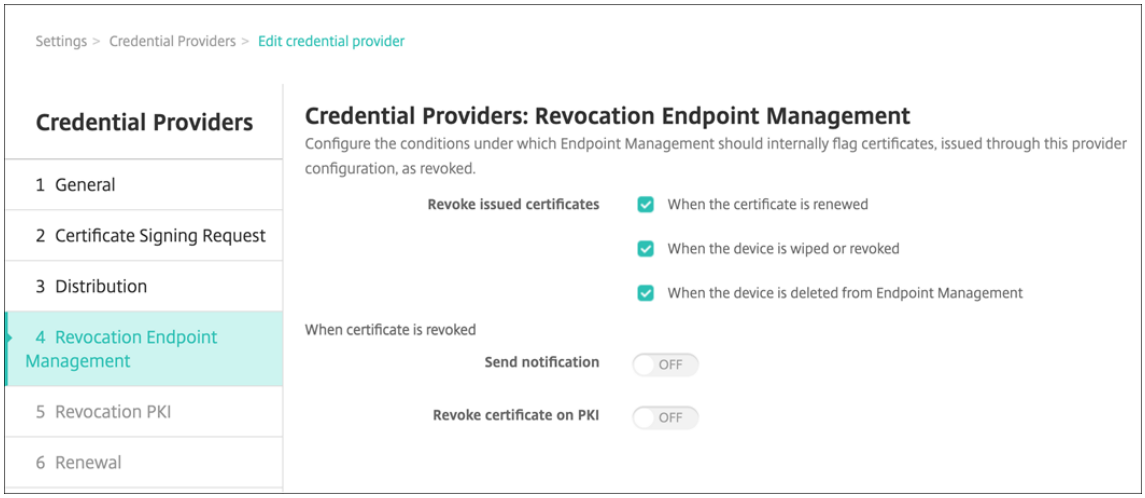


- **Issuing CA certificate:** Select the discretionary CA certificate that you added previously.
- **Select distribution mode:** Select one of the following ways of generating and distributing keys:
  - **Prefer centralized: Server-side key generation:** Citrix recommends this centralized option. It supports all platforms supported by Citrix Endpoint Management and is required when using NetScaler Gateway authentication. The private keys are generated and stored on the server and distributed to user devices.
  - **Prefer distributed: Device-side key generation:** The private keys are generated and stored on the user devices. This distributed mode uses SCEP and requires an RA encryption certificate with the keyUsage keyEncryption and an RA signing certificate with the KeyUsage digitalSignature. The same certificate can be used for both encryption and signing.
  - **Only distributed: Device-side key generation:** This option works the same as **Prefer distributed: Device-side key generation**, except that no option is available if device-side key generation fails or is unavailable.

If you selected **Prefer distributed: Device-side key generation** or **Only distributed: Device-side key generation**, click the RA signing certificate and RA encryption certificate. The same certificate can be used for both. New fields appear for these certificates.

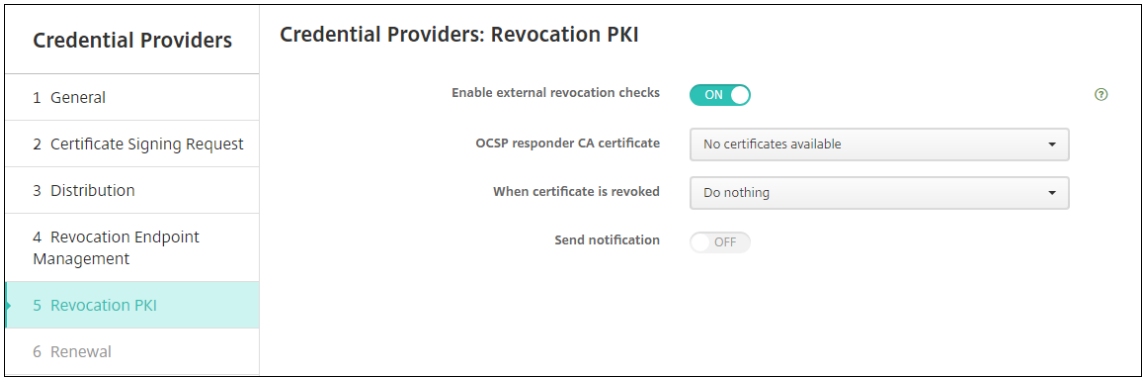
5. Click **Next**. On the **Credential Providers: Revocation Citrix Endpoint Management** page, configure the conditions under which Citrix Endpoint Management internally flags certificates, issued through this provider configuration, as revoked. Configure the following:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- In **Revoke issued certificates**, select one of the options indicating when to revoke certificates.
- To direct Citrix Endpoint Management to send a notification when the certificate is revoked: Set the value of **Send notification** to **On** and choose a notification template.
- **Revoke certificate on PKI** doesn't work when using Citrix Endpoint Management as your discretionary PKI.

6. Click **Next**. On the **Credential Providers: Revocation PKI** page, identify what actions to take on the PKI if the certificate is revoked. You also have the option of creating a notification message. Configure the following:



- **Enable external revocation checks:** Turn this setting **On**. More fields related to revocation PKI appear.
- In the **OCSP responder CA certificate** list, select the distinguished name (DN) of the certificate's subject.

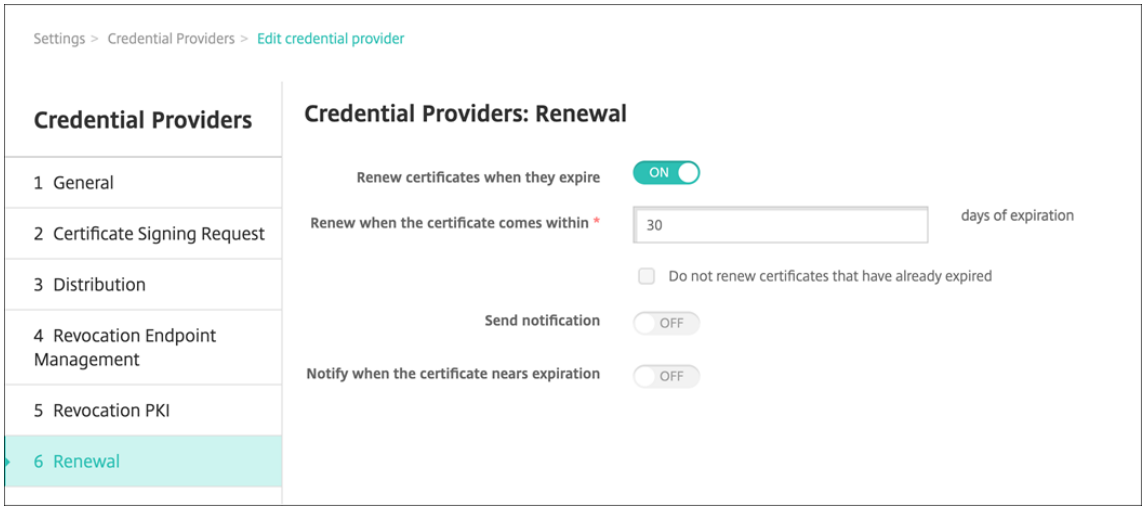
  You can use Citrix Endpoint Management macros for the DN field values. For example: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- In the **When certificate is revoked** list, click one of the following actions to take on the PKI entity when the certificate is revoked:
  - Do nothing.
  - Renew the certificate.
  - Revoke and wipe the device.
- To direct Citrix Endpoint Management to send a notification when the certificate is revoked: Set the value of **Send notification** to **On**.

  You can choose between two notification options:
  - If you select **Select notification template**, you can select a pre-written notification message which you can then customize. These templates are in the Notification template list.
  - If you select **Enter notification details**, you can write your own notification message. In addition to providing the recipient's email address and the message, you can set how often the notification is sent.

7. Click **Next**. On the **Credential Providers: Renewal** page, configure the following:



Set **Renew certificates when they expire** to **On**. More fields appear.

- In the **Renew when the certificate comes within** field, type how many days before expiration to renew the certificate.
- Optionally, select **Do not renew certificates that have already expired**. In this case, "already expired"means that the `NotAfter` date is in the past, not that it has been revoked. Citrix Endpoint Management doesn't renew certificates after they are internally revoked.

To direct Citrix Endpoint Management to send a notification when the certificate has been renewed: Set **Send notification** to **On**. To direct Citrix Endpoint Management to send a notification when the certification nears expiration: Set **Notify when certificate nears expiration** to

© 1997–2025 Citrix Systems, Inc. All rights reserved.

On.
For either of those choices, you can choose between two notification options:

- **Select notification template:** Select a pre-written notification message which you can then customize. These templates are in the Notification template list.
- **Enter notification details:** Write your own notification message. Provide the recipient's email address, a message, and a frequency for sending the notification.

8. Click **Save**.

Credential providers

September 6, 2025

Credential providers are the actual certificate configurations that you use in the various parts of the Citrix Endpoint Management system. Credential providers define the sources, parameters, and life cycles of your certificates. Those operations occur whether the certificates are part of device configurations or are standalone (that is, pushed as is to the device).

Device enrollment constrains the certificate life cycle. That is, Citrix Endpoint Management doesn't issue certificates before enrollment, although Citrix Endpoint Management might issue some certificates as part of enrollment. Also, certificates issued from the internal PKI within the context of one enrollment are revoked when the enrollment is revoked. After the management relationship terminates, no valid certificate stays.

You can use one credential provider configuration in many places, to the effect that one configuration can govern any number of certificates at the same time. The unity then is on the deployment resource and the deployment. For example, if Credential Provider P is deployed to device D as part of configuration C: The issuance settings for P determine the certificate that is deployed to D. Likewise, the renewal settings for D apply when C is updated. And, the revocation settings for D also apply when C is deleted or when D is revoked.

According to those rules, the credential provider configuration in Citrix Endpoint Management determines the following:

- The source of certificates.
- The method in which certificates are got: Signing a new certificate or fetching (recovering) an existing certificate and key pair.
- The parameters for issuance or recovery: For example, Certificate Signing Request (CSR) parameters, such as key size, key algorithm, and certificate extensions.
- The manner in which certificates are delivered to the device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Revocation conditions: Although all certificates are revoked in Citrix Endpoint Management when the management relationship is severed, the configuration might specify an earlier revocation. For instance, the configuration can specify to revoke a certificate when the associated device configuration is deleted. Also, under some conditions, the revocation of the associated certificate in Citrix Endpoint Management might be sent to the back-end public key infrastructure (PKI). That is, certificate revocation in Citrix Endpoint Management might cause certificate revocation on the PKI.
- Renewal settings: Certificates got through a given credential provider can automatically renew when they near expiration. Or, separately from that situation, notifications can be issued when that expiration approaches.

The availability of configuration options mainly depends on the type of PKI Entity and issuance method that you select for a credential provider.

Method of certificate issuance

You can get a certificate, which is known as the method of issuance, by signing.

With this method, the issuance involves creating a new private key, creating a CSR, and submitting the CSR to a Certificate Authority (CA) for signature. Citrix Endpoint Management supports the sign method for both MS Certificate Services entities and Discretionary CA entities.

A credential provider uses the sign method of issuance.

Certificate Delivery

Two modes of certificate delivery are available in Citrix Endpoint Management: centralized and distributed. Distributed mode uses the Simple Certificate Enrollment Protocol (SCEP) and is only available in situations in which the client supports the protocol (iOS only). Distributed mode is mandatory in some situations.

For a credential provider to support distributed (SCEP-assisted) delivery, a special configuration step is necessary: Setting up Registration Authority (RA) certificates. The RA certificates are required, because, if you use the SCEP protocol, Citrix Endpoint Management acts like a delegate (a registrar) to the actual certificate authority. Citrix Endpoint Management must prove to the client that it has the authority to act as such. That authority is established by uploading the previously mentioned certificates to Citrix Endpoint Management.

Two distinct certificate roles are required (although a single certificate can fulfill both requirements): RA signature and RA encryption. The constraints for these roles are as follows:

- The RA signing certificate must have the X.509 key usage digital signature.
- The RA encryption certificate must have the X.509 key usage key encipherment.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To configure the credential provider RA certificates, you upload the certificates to Citrix Endpoint Management and then link to them in the credential provider.

A credential provider is considered to support distributed delivery only if the provider has a certificate configured for certificate roles. You can configure each credential provider to either prefer centralized mode, to prefer distributed mode, or to require distributed mode. The actual result depends on the context: If the context does not support distributed mode, but the credential provider requires this mode, deployment fails. Likewise, if the context requires distributed mode, but the credential provider does not support distributed mode, deployment fails. In all other cases, the preferred setting is honored.

The following table shows SCEP distribution throughout Citrix Endpoint Management:

Context	SCEP supported	SCEP required
iOS Profile Service	Yes	Yes
iOS Mobile Device Management enrollment	Yes	No
iOS configuration profiles	Yes	No
SHTP enrollment	No	No
SHTP configuration	No	No
Windows Tablet enrollment	No	No
Windows Tablet configuration	No, except for the network device policy, which is supported for Windows 10 and Windows 11 releases	No

Certificate Revocation

There are three types of revocation.

- **Internal revocation:** Internal revocation affects the certificate status as maintained by Citrix Endpoint Management. Citrix Endpoint Management considers this status when evaluating a presented certificate, or when providing OCSP status information for a certificate. The credential provider configuration determines how this status is affected under various conditions. For instance, the credential provider might specify to flag certificates as revoked when the certificates are deleted from the device.
- **Externally propagated revocation:** Also known as Revocation Citrix Endpoint Management, this type of revocation applies to certificates got from an external PKI. The certificate is revoked

© 1997–2025 Citrix Systems, Inc. All rights reserved.

on the PKI when Citrix Endpoint Management internally revokes the certificate, under the conditions defined by the credential provider configuration.

- **Externally induced revocation:** Also known as Revocation PKI, this type of revocation also only applies to certificates got from an external PKI. Whenever Citrix Endpoint Management evaluates a given certificate status, Citrix Endpoint Management queries the PKI as to that status. If the certificate is revoked, Citrix Endpoint Management internally revokes the certificate. This mechanism uses the OCSP protocol.

These three types are not exclusive, but rather apply together. An external revocation or independent finding can cause an internal revocation. An internal revocation potentially affects an external revocation.

Certificate Renewal

A certificate renewal is the combination of a revocation of the existing certificate and an issuance of another certificate.

Citrix Endpoint Management first tries to get the new certificate before revoking the previous certificate, to avoid discontinuation of service when issuance fails. For distributed (SCEP-supported) delivery, the revocation also only happens after the certificate has been successfully installed on the device. Otherwise, the revocation occurs before the new certificate is sent to the device. That revocation is independent of the success or failure of certificate installation.

The revocation configuration requires that you specify a certain duration (in days). When the device connects, the server verifies whether the certificate `NotAfter` date is later than the current date, minus the specified duration. If the certificate meets that condition, Citrix Endpoint Management tries to renew the certificate.

Create a credential provider

Configuring a credential provider varies mostly as a factor of which issuing entity and which issuing method you select for the credential provider. You can distinguish between credential providers that use an internal entity or an external entity:

- A discretionary entity, which is internal to Citrix Endpoint Management, is an internal entity. The issuing method for a discretionary entity is always a sign. Sign means that with each issuing operation, Citrix Endpoint Management signs a new key pair with the CA certificate selected for the entity. Whether the key pair is generated on the device or on the server depends on the distribution method you select.
- An external entity, which is part of your corporate infrastructure, includes Microsoft CA.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner and then click **Settings > Credential Providers**.
2. On the **Credential Providers** page, click **Add**.

   The **Credential Providers: General Information** page appears.
3. On the **Credential Providers: General Information** page, do the following:

   - **Name:** Type a unique name for the new provider configuration. This name is used later to identify the configuration in other parts of the Citrix Endpoint Management console.
   - **Description:** Describe the credential provider. Although this field is optional, a description can provide useful details about this credential provider.
   - **Issuing entity:** Click the certificate issuing entity.
   - **Issuing method:** Click **Sign** or **Fetch** to serve as the method that the system uses to get certificates from the configured entity. For client certificate authentication, use **Sign**.
   - If the **Template** list is available, select the template that you added under the PKI entity for the credential provider.

     These templates become available when Microsoft Certificate Services Entities are added at **Settings > PKI Entities**.
4. Click **Next**.

   The **Credential Providers: Certificate Signing Request** page appears.
5. On the **Credential Providers: Certificate Signing Request** page, configure the following according to your certificate configuration:

   - **Key algorithm:** Choose the key algorithm for the new key pair. Available values are **RSA**, **DSA**, and **ECDSA**.
   - **Key size:** Type the size, in bits, of the key pair. This field is required.

     The permissible values depend on the key type. For example, the maximum size for DSA keys is 2048 bits. To avoid false negatives, which depend on the underlying hardware and software, Citrix Endpoint Management doesn't enforce key sizes. Always test credential provider configurations in a test environment before activating them in production.
   - **Signature algorithm:** Click a value for the new certificate. Values depend on the key algorithm.
   - **Subject name:** Required. Type the Distinguished Name (DN) of the new certificate subject. For example:
     `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } ,C=${ user.c } \endquotation`

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For example, for client certificate authentication, use these settings:

- **Key algorithm:** RSA
- **Key size:** 2048
- **Signature algorithm:** SHA256withRSA
- **Subject name:** `cn=$user.username`

- To add an entry to the **Subject alternative names** table, click **Add**. Select the type of alternative name and then type a value in the second column.

  For client certificate authentication, specify:

  - **Type:** User Principal name
  - **Value:** `$user.userprincipalname`

    As with Subject name, you can use Citrix Endpoint Management macros in the value field.

6. Click **Next**.

   The **Credential Providers: Distribution** page appears.

7. On the **Credential Providers: Distribution** page, do the following:

   - In the **Issuing CA certificate** list, click the offered CA certificate. Because the credential provider uses a discretionary CA entity, the CA certificate for the credential provider is always the CA certificate configured on the entity itself. The CA certificate is presented here for consistency with configurations that use external entities.
   - In **Select distribution mode**, click one of the following ways of generating and distributing keys:
     - **Prefer centralized: Server-side key generation:** Citrix recommends this centralized option. It supports all platforms supported by Citrix Endpoint Management and is required when using NetScaler Gateway authentication. The private keys are generated and stored on the server and distributed to user devices.
     - **Prefer distributed: Device-side key generation:** The private keys are generated and stored on the user devices. This distributed mode uses SCEP and requires an RA encryption certificate with the keyUsage keyEncryption and an RA signing certificate with the KeyUsage digitalSignature. The same certificate can be used for both encryption and signing.
     - **Only distributed: Device-side key generation:** This option works the same as Prefer distributed: Device-side key generation, except that since it is "Only"rather than "Prefer"no option is available if device-side key generation fails or is unavailable.

   If you selected **Prefer distributed: Device-side key generation** or **Only distributed: Device-side key generation**, click the RA signing certificate and RA encryption certificate. The same certificate can be used for both. New fields appear for these certificates.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

8. Click **Next**.

   The **Credential Providers: Revocation Citrix Endpoint Management** page appears. On this page, you configure the conditions under which Citrix Endpoint Management internally flags certificates, issued through this provider configuration, as revoked.

9. On the **Credential Providers: Revocation Citrix Endpoint Management** page, do the following:

   - In **Revoke issued certificates**, select one of the options indicating when to revoke certificates.
   - To direct Citrix Endpoint Management to send a notification when the certificate is revoked: Set the value of **Send notification** to **On** and choose a notification template.
   - To revoke the certificate on PKI when the certificate is revoked from Citrix Endpoint Management: Set **Revoke certificate on PKI** to **On** and, in the **Entity list**, click a template. The Entity list shows all available entities with revocation capabilities. When the certificate is revoked from Citrix Endpoint Management, a revocation call is sent to the PKI selected from the Entity list.

10. Click **Next**.

    The **Credential Providers: Revocation PKI** page appears. On this page, you identify what actions to take on the PKI if the certificate is revoked. You also have the option of creating a notification message.

11. On the **Credential Providers: Revocation PKI** page, do the following if you want to revoke certificates from the PKI:

    - Change the setting of **Enable external revocation checks** to **On**. More fields related to revocation PKI appear.
    - In the **OCSP responder CA certificate** list, click the distinguished name (DN) of the certificate's subject.

      You can use Citrix Endpoint Management macros for the DN field values. For example: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`

    - In the **When certificate is revoked** list, click one of the following actions to take on the PKI entity when the certificate is revoked:
      - Do nothing.
      - Renew the certificate.
      - Revoke and wipe the device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- To direct Citrix Endpoint Management to send a notification when the certificate is revoked: Set the value of **Send notification** to **On**.

  You can choose between two notification options:

- If you select **Select notification template**, you can select a pre-written notification message which you can then customize. These templates are in the Notification template list.
- If you select **Enter notification details**, you can write your own notification message. In addition to providing the recipient's email address and the message, you can set how often the notification is sent.

12. Click **Next**.

    The **Credential Providers: Renewal** page appears. On this page, you can configure Citrix Endpoint Management to do the following:

    - Renew the certificate. You can optionally send a notification on renewal, and optionally exclude already expired certificates from the operation.
    - Issue a notification for certificates that near expiration (notification before renewal).

13. On the **Credential Providers: Renewal** page, do the following if you want to renew certificates when they expire:

    Set **Renew certificates** when they expire to **On**. More fields appear.

    - In the **Renew when the certificate comes within** field, type how many days before expiration to renew the certificate.
    - Optionally, select **Do not renew certificates that have already expired**. In this case, "already expired"means that the `NotAfter` date is in the past, not that it has been revoked. Citrix Endpoint Management doesn't renew certificates after they are internally revoked.

    To direct Citrix Endpoint Management to send a notification when the certificate has been renewed: Set **Send notification** to **On**. To direct Citrix Endpoint Management to send a notification when the certification nears expiration: Set **Notify when certificate nears expiration** to **On**.
    For either of those choices, you can choose between two notification options:

    - **Select notification template:** Select a pre-written notification message which you can then customize. These templates are in the Notification template list.
    - **Enter notification details:** Write your own notification message. Provide the recipient's email address, a message, and a frequency for sending the notification.

    In the **Notify when the certificate comes within** field, type how many days before the certificate's expiration to send the notification.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

14. Click **Save**.

    The credential provider appears in the Credential Provider table.

APNs certificates

September 6, 2025

To enroll and manage Apple devices in Citrix Endpoint Management, you set up an Apple Push Notification service (APNs) certificate from Apple. The certificate enables Mobile Device Management through the Apple Push Network.

Workflow summary:

Step 1: Create a Certificate Signing Request (CSR) through any of these methods:

- Create a CSR by using Keychain Access on macOS (recommended by Citrix®)
- Create a CSR by using Microsoft IIS
- Create a CSR by using OpenSSL

Step 2: Sign the CSR in Citrix Endpoint Management Tools

Step 3: Submit the signed CSR to Apple to get the APNs certificate

Step 4: Using the same computer used for Step 1, Complete the CSR and export a PKCS #12 file:

- Create a PKCS #12 file by using Keychain Access on macOS
- Create a PKCS #12 file by using Microsoft IIS
- Create a PKCS #12 file by using OpenSSL

Step 5: Import an APNs certificate into Citrix Endpoint Management

Step 6: Renew an APNs certificate

Create a Certificate Signing Request

We recommend that you create a CSR by using Keychain Access on macOS. You can also create a CSR by using Microsoft IIS or OpenSSL.

> **Important:**
>
> - For the Apple ID used to create the certificate:
>   - The Apple ID must be a corporate ID and not a personal ID.
>   - Record the Apple ID that you use to create the certificate.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate require device re-enrollment.

- If you accidentally or intentionally revoke the certificate, you lose the ability to manage your devices.
- If you used the iOS Developer Enterprise Program to create a mobile device manager push certificate: Be sure to handle any actions for the migrated certificates in the Apple Push Certificates Portal.

Create a CSR by using Keychain Access on macOS

1. On a computer running macOS, under **Applications > Utilities**, start the Keychain Access app.
2. Open the **Keychain Access** menu and then click **Certificate Assistant > Request a Certificate From a Certificate Authority**.
3. The Certificate Assistant prompts you to enter the following information:
   - **Email Address:** Email address of the individual or role account who manages the certificate.
   - **Common Name:** Common name of the individual or a role account who manages the certificate.
   - **CA Email Address:** Email address of the Certificate Authority.
4. Select the **Saved to disk** and **Let me specify key pair information** options and then click **Continue**.
5. Enter a name for the CSR file, save the file on your computer, and then click **Save**.
6. Specify the key pair information: Select the **Key Size** of 2048 bits and the **RSA algorithm** and then click **Continue**. The CSR file is ready for you to upload as part of the APNs certificate process.
7. Click **Done** when the Certificate Assistant completes the CSR process.
8. To continue, Sign the CSR.

Create a CSR by using Microsoft IIS

The first step for generating an APNs certificate request is to create a Certificate Signing Request (CSR). For Windows, generate a CSR by using Microsoft IIS.

1. Open Microsoft IIS.
2. Double-click the Server Certificates icon for IIS.
3. In the **Server Certificates** window, click **Create Certificate Request**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. Type the appropriate Distinguished Name (DN) information. For example, you can type the fully qualified domain name (FQDN) of your Citrix Endpoint Management server, such as www.domain.com. Then click **Next**.
5. Select **Microsoft RSA SChannel Cryptographic Provider** for the Cryptographic Service Provider and **2048** for bit length and then click **Next**.
6. Enter a file name and specify a location to save the CSR and then click **Finish**.
7. To continue, Sign the CSR.

Create a CSR by using OpenSSL

If you can't use a macOS device or Microsoft IIS to generate a CSR, use OpenSSL. You can download and install OpenSSL from the OpenSSL website.

1. On the computer where you install OpenSSL, run the following command from a command prompt or shell.

   ```
   openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate
   .csr -newkey rsa:2048
   ```

2. The following message for certificate naming information appears. Enter the information as requested.

   ```
   1  You are about to be asked to enter information that will be
         incorporated into your certificate request.
   2  What you are about to enter is what is called a Distinguished Name
          or a DN.
   3  There are quite a few fields but you can leave some blank
   4  For some fields there will be a default value,
   5  If you enter '.', the field will be left blank.
   6  -----
   7  Country Name (2 letter code) [AU]:US
   8  State or Province Name (full name) [Some-State]:CA
   9  Locality Name (eg, city) []:RWC
   10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
         Customer
   11 Organizational Unit Name (eg, section) [:Marketing
   12 Common Name (eg, YOUR name) []:John Doe
   13 Email Address []:john.doe@customer.com
   ```

3. At the next message, enter a password for the CSR private key.

   ```
   1  Please enter the following 'extra' attributes
   2  to be sent with your certificate request
   3  A challenge password []:
   4  An optional company name []:
   ```

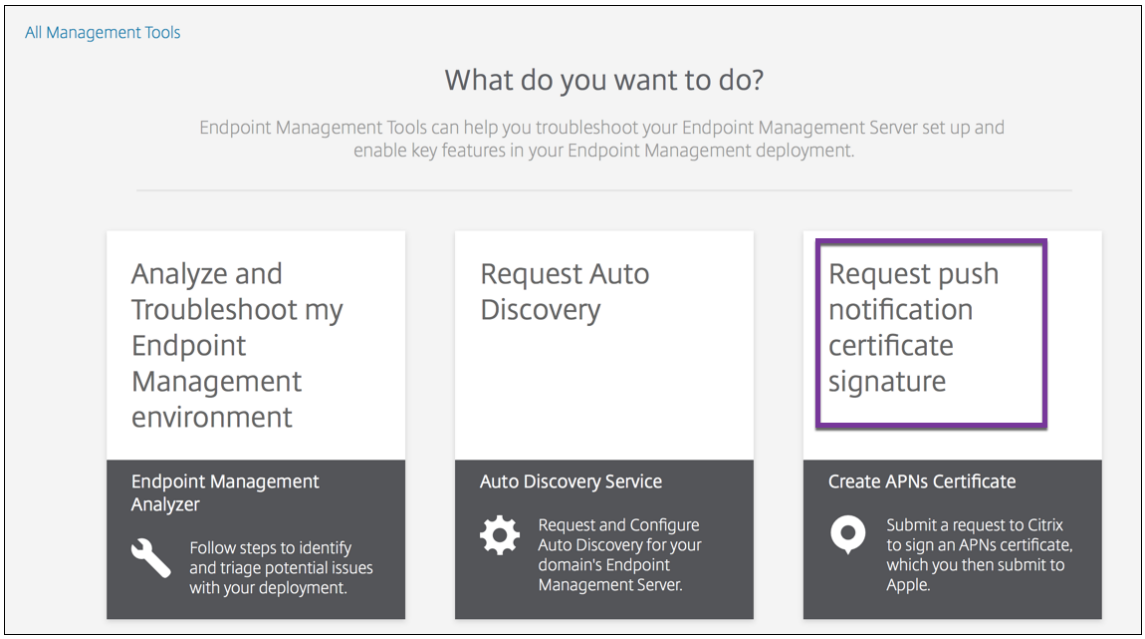
4. To continue, sign the CSR as described in the next section.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Sign the CSR

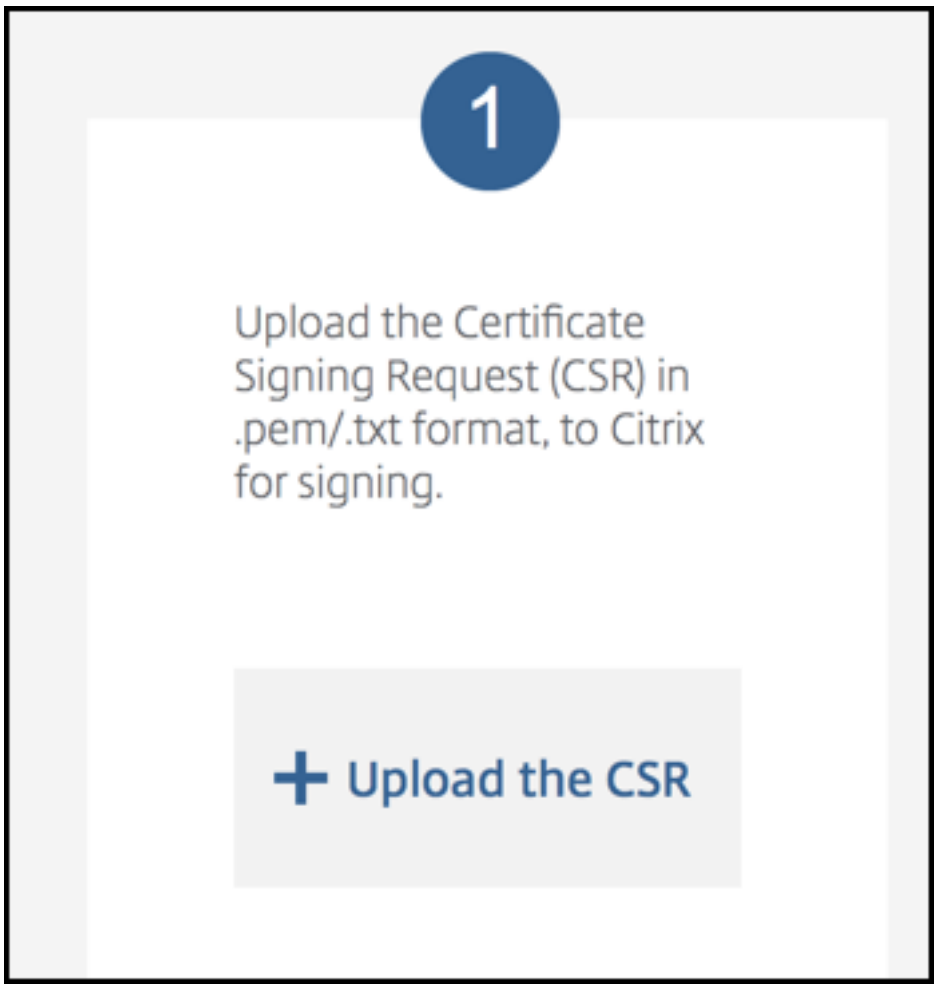
To use a certificate with Citrix Endpoint Management, you must submit it to Citrix for signing. Citrix signs the CSR with its Mobile Device Management signing certificate and returns the signed file in a `.plist` format.

1. In your browser, go to the Citrix Endpoint Management Tools website and then click **Request push notification certificate signature**.



2. On the **Creating a new certificate page**, click **Upload the CSR**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Browse to and select the certificate.

   > **Important:**
   >
   > The certificate must be in .pem/txt format. If needed, change the file name extension of the certificate to .pem or .txt by right-clicking and renaming the file.

4. On the **Citrix Endpoint Management APNs CSR Signing** page, click **Sign**. The CSR is signed and automatically saved to your configured download folder.
5. To continue, submit the signed CSR as described in the next section.

Submit the signed CSR to Apple to get the APNs certificate

After receiving your signed Certificate Signing Request (CSR) from Citrix, submit the CSR to Apple to get the APNs certificate needed to import into Citrix Endpoint Management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Some users have reported problems logging into the Apple Push Portal. As an alternative, you can log on to the Apple Developer Portal. You can then follow these steps:

1. In a browser, go to the Apple Push Certificates Portal.
2. Click **Create a Certificate**.
3. The first time that you create a certificate with Apple: Select the **I have read and agree to these terms and conditions** checkbox, and then click **Accept**.
4. Click **Choose File**, browse to the signed CSR on your computer, and then click **Upload**. A confirmation message indicates that the upload succeeds.
5. Click **Download** to retrieve the .pem certificate.
6. To continue, complete the CSR and export a PKCS #12 file as described in the next section.

Complete the CSR and export a PKCS #12 file

After you receive the APNs certificate from Apple, return to Keychain Access, Microsoft IIS, or OpenSSL to export the certificate into a PCKS #12 file.

A PKCS #12 file has the APNS certificate file and your private key. PFX files usually have the extension .pfx or .p12. You can use .pfx and .p12 files interchangeably.

> **Important:**
>
> Citrix recommends you save or export the personal and public keys from the local system. You need the keys to access the APNs certificates for reuse. Without the same keys, your certificate is invalid and you must repeat the entire CSR and APNs process.

Create a PKCS #12 file by using Keychain Access on macOS

> **Important:**
>
> Use the same macOS device for this task that you used to generate the CSR.

1. On the device, locate the Production identity (.pem) certificate that received from Apple.
2. Start the Keychain Access application and navigate to the **Login > My Certificates** tab. Drag and then drop the Product identity certificate onto the open window.
3. Click the certificate and expand the left arrow to verify that the certificate includes an associated private key.
4. To begin exporting the certificate into a PCKS #12 (.pfx) certificate, choose the certificate and private key, right-click, and select **Export 2 items**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. Give the certificate file a unique name for use with Citrix Endpoint Management. Don't include space characters in the name. Then, choose a folder location for the saved certificate, select the .pfx file format, and click **Save**.
6. Enter a password for exporting the certificate. Citrix recommends that you use a unique, strong password. Also, be sure to keep the certificate and password safe for later use and reference.
7. The Keychain Access app prompts you for the login password or selected keychain. Type the password, and then click **OK**. The saved certificate is now ready for use with the Citrix Endpoint Management server.
8. To continue, see Import an APNs certificate into Citrix Endpoint Management.

Create a PKCS #12 file by using Microsoft IIS

> **Important:**
>
> Use the same IIS server for this task that you used to generate the CSR.

1. Open Microsoft IIS.
2. Click the **Server Certificates** icon.
3. In the **Server Certificates** window, click **Complete Certificate Request**.
4. Browse to the Certificate.pem file from Apple. Then, type a friendly name or the certificate name and click **OK**. Don't include space characters in the name.
5. Select the certificate that you identified in Step 4, and then click **Export**.
6. Specify a location and file name for the .pfx certificate and a password, and then click **OK**.

   You need the password for the certificate to import it into Citrix Endpoint Management.
7. Copy the .pfx certificate to the server on which you plan to install Citrix Endpoint Management.
8. To continue, see Import an APNs certificate into Citrix Endpoint Management.

Create a PKCS #12 file by using OpenSSL

If you use OpenSSL to create a CSR, you can also use OpenSSL to create a .pfx APNs certificate.

1. At a command prompt or shell, run the following command. `Customer.privatekey.pem` is the private key from your CSR. `APNs_Certificate.pem` is the certificate that you just received from Apple.

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.
   privatekey.pem -out apns_identity.pfx
   ```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Enter a password for the .pfx certificate file. Remember this password because you use the password again when you upload the certificate to Citrix Endpoint Management.
3. Note the location for the .pfx certificate file. Then, copy the file to the Citrix Endpoint Management server so you can use the console to upload the file.
4. To continue, import an APNs certificate into Citrix Endpoint Management as described in the next section.

Import an APNs certificate into Citrix Endpoint Management

After you receive the new APNs certificate: Import the APNs certificate into Citrix Endpoint Management to either add the certificate for the first time or to replace a certificate.

1. In the Citrix Endpoint Management console, go to **Settings > Certificates**.
2. Click **Import > Keystore**.
3. From **Use as**, choose **APNs**.
4. Browse to the .pfx or .p12 file on your computer.
5. Enter a password, and then click **Import**.

For more information about certificates in Citrix Endpoint Management, see Certificates and authentication.

Renew an APNs certificate

> **Important:**
>
> If you use a different Apple ID for the renewal process, you must reenroll user devices.

To renew an APNs certificate, do the steps to create a certificate, then go to the Apple Push Certificates Portal. Use that portal to upload the new certificate. After logging on, your existing certificate or a certificate imported from your previous Apple Developers account appears.

In the Certificates Portal, the only difference when renewing the certificate is that you click **Renew**. You must have a developer account with the Certificates Portal to access the site. To renew your certificate, use the same organization name and Apple ID.

To determine when your APNs certificate expires, in the Citrix Endpoint Management console, go to **Settings > Certificates**. If the certificate expires, do not revoke it.

1. Generate a CSR using Microsoft IIS, Keychain Access (macOS), or OpenSSL. For more information on generating a CSR, see Create a Certificate Signing Request.

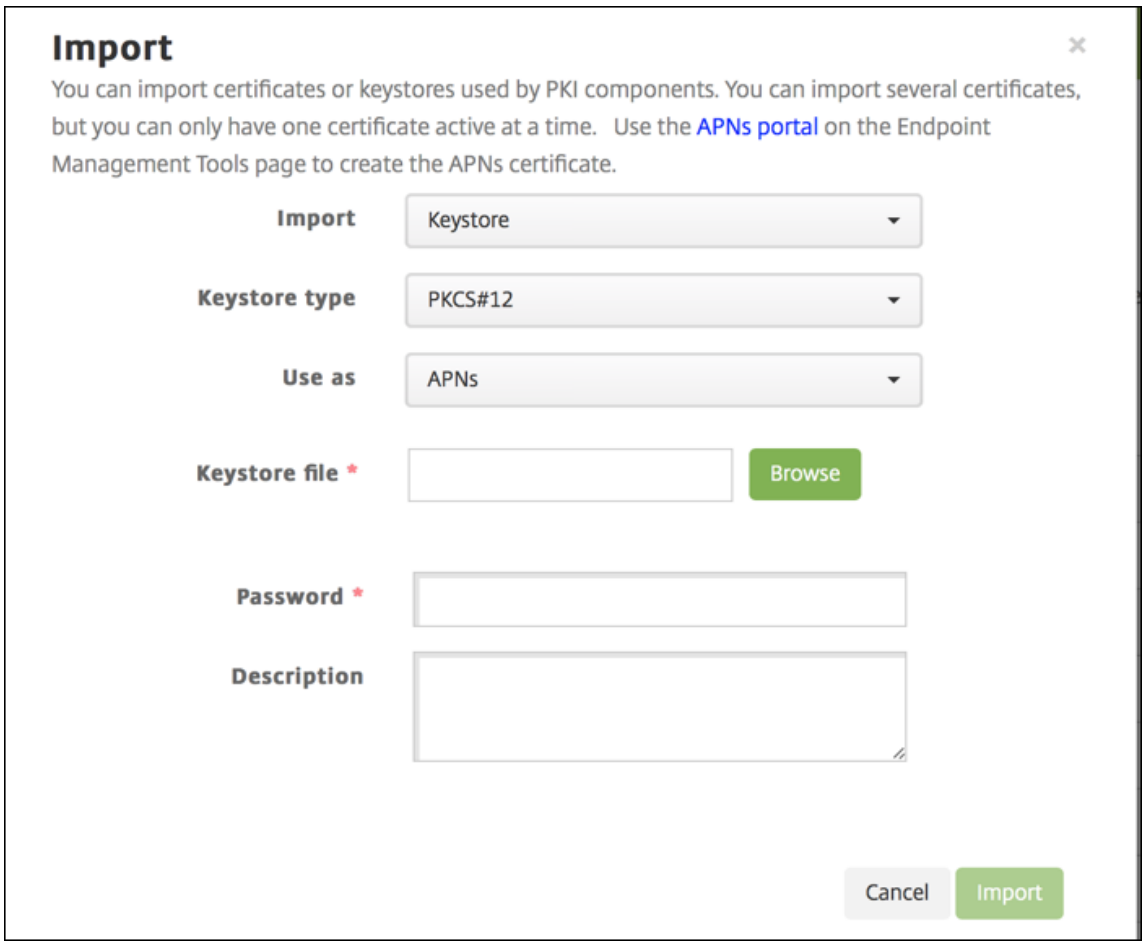
© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. In your browser, go to Citrix Endpoint Management Tools. Then, click **Request push notification certificate signature**.
3. Click **+ Upload the CSR**.
4. In the dialog box, navigate to the CSR, click **Open**, and click **Sign**.
5. When you receive a `.plist` file, save it.
6. In the step 3 title, click **Apple Push Certificates Portal** and sign on.
7. Select the certificate that you want to renew, and then click **Renew**.
8. Upload the `.plist` file. You receive a .pem file as the output. Save the .pem file.
9. Using that .pem file, complete the CSR (according to the method you used to create the CSR in Step 1).
10. Export the certificate as a .pfx file.

In the Citrix Endpoint Management console, import the .pfx file and complete the configuration as follows:

1. Go to **Settings > Certificates > Import**.
2. From the **Import menu**, choose **Keystore**.
3. From the **Keystore type** menu, choose **PKCS #12**.
4. From **Use as**, choose **APNs**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. For **Keystore file**, click **Browse** and navigate to the file.
6. In **Password**, type the certificate password.
7. Type an optional **Description**.
8. Click **Import**.

Citrix Endpoint Management redirects you back to the **Certificates** page. The **Name**, **Status**, **Valid from**, and **Valid to** fields update.

SAML for single sign-on with Citrix Files

September 6, 2025

> **Disclaimer:**
>
> This feature will be deprecated if ShareFile (now Progress) discontinues support.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

You can configure Citrix Endpoint Management and ShareFile to use the Security Assertion Markup Language (SAML) to provide single sign-on (SSO) access to Citrix Files mobile apps. This functionality includes:

- Citrix Files apps that are MAM SDK enabled or wrapped by using the MDX Toolkit
- Non-wrapped Citrix Files clients, such as the website, Outlook plug-in, or sync clients
- **For wrapped Citrix Files apps:** Users who log on to Citrix Files get redirected to Citrix Secure Hub for user authentication and to acquire a SAML token. After successful authentication, the Citrix Files mobile app sends the SAML token to ShareFile. After the initial logon, users can access the Citrix Files mobile app through SSO. They can also attach documents from ShareFile to Citrix Secure Mail mails without logging on each time.
- **For non-wrapped Citrix Files clients:** Users who log on to Citrix Files using a web browser or other Citrix Files client are redirected to Citrix Endpoint Management. Citrix Endpoint Management authenticates the users, who then acquire a SAML token which is sent to ShareFile. After the initial logon, users can access Citrix Files clients through SSO without logging on each time.

To use Citrix Endpoint Management as a SAML identity provider (IdP) to ShareFile, you must configure Citrix Endpoint Management for use with Enterprise accounts, as described in this article. Or, you can configure Citrix Endpoint Management to work only with storage zone connectors. For more information, see ShareFile use with Citrix Endpoint Management.

For a detailed reference architecture diagram, see Architecture.

Prerequisites

Complete the following prerequisites before you can configure SSO with Citrix Endpoint Management and Citrix Files apps:

- The MAM SDK or a compatible version of the MDX Toolkit (for Citrix Files mobile apps).

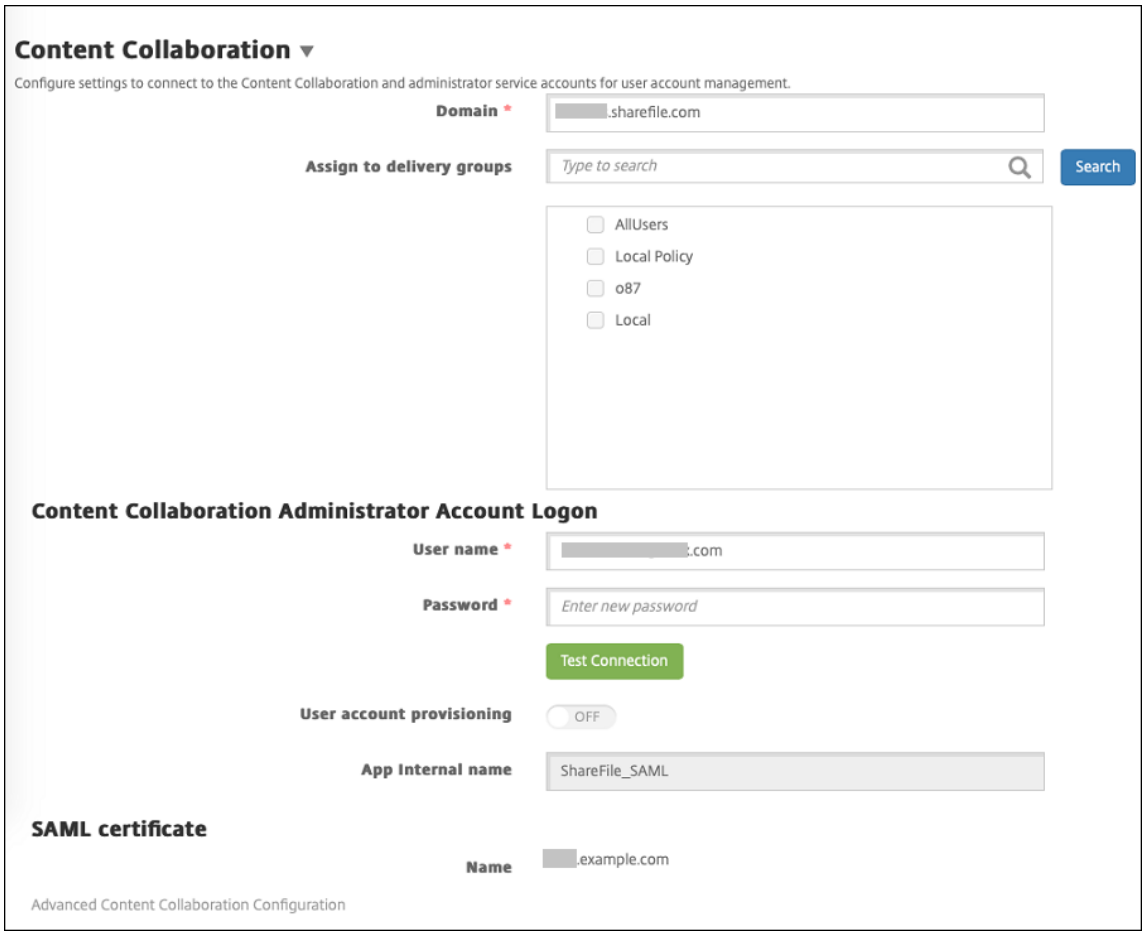
  For more information, see Citrix Endpoint Management compatibility.
- A compatible version of Citrix Files mobile apps and Citrix Secure Hub.
- ShareFile administrator account.
- Connectivity verified between Citrix Endpoint Management and ShareFile.

Configure ShareFile access

Before setting up SAML for ShareFile, provide ShareFile access information as follows:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. In the Citrix Endpoint Management web console, click **Configure > ShareFile**. The **ShareFile** configuration page appears.



2. Configure these settings:

   - **Domain:** Type your ShareFile subdomain name. For example: `example.sharefile.com`.
   - **Assign to delivery groups:** Select or search for the delivery groups that you want to be able to use SSO with ShareFile.
   - **ShareFile Administrator Account Logon**
   - **User name:** Type the ShareFile administrator user name. This user must have administrator privileges.
   - **Password:** Type the ShareFile administrator password.
   - **User account provisioning:** Leave this setting disabled. Use the ShareFile User Management Tool for user provisioning. See Provision user accounts and distribution groups.

3. Click **Test Connection** to verify that the user name and password for the ShareFile administrator account authenticate to the specified ShareFile account.

4. Click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Management syncs with ShareFile and updates the ShareFile settings **ShareFile Issuer/Entity ID** and **Login URL**.
- The **Configure > ShareFile** page shows the **App internal name**. You need that name to complete the steps described later in [Modify the Citrix Files.com SSO settings] (#modify-the-citrix-filescom-sso-settings).

Set up SAML for Wrapped Citrix Files MDX Apps

You don't need to use NetScaler Gateway for single sign-on configuration with Citrix Files apps prepared with the MAM SDK. To configure access for non-wrapped Citrix Files clients, such as the website, Outlook plug-in, or the sync clients, see Configure the NetScaler Gateway for Other Citrix Files Clients.

To configure SAML for wrapped Citrix Files MDX apps:

1. Download the ShareFile for Citrix Endpoint Management clients. See ShareFile Tool/App Downloads.
2. Prepare the Citrix Files mobile app with the MAM SDK. For details, see the MAM SDK overview.
3. In the Citrix Endpoint Management console, upload the prepared Citrix Files mobile app. For information about uploading MDX apps, see To add an MDX app to Citrix Endpoint Management.
4. Verify the SAML settings: Log on to ShareFile with the administrator user name and password you configured earlier.
5. Verify that ShareFile and Citrix Endpoint Management are configured for the same time zone. Make sure that Citrix Endpoint Management shows the correct time for the configured time zone. If not, the SSO might fail.

Validate the Citrix Files mobile app

1. On the user device, install and configure Citrix Secure Hub.
2. From the app store, download and install the Citrix Files mobile app.
3. Start the Citrix Files mobile app. Citrix Files starts without prompting for user name or password.

Validate with Citrix Secure Mail

1. On the user device, if it has not already been done, install and configure Citrix Secure Hub.
2. From the app store, download, install, and set up Citrix Secure Mail.
3. Open a new email form and then tap **Attach from ShareFile**. Files available to attach to the email are shown without asking for a user name or password.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure NetScaler Gateway for other Citrix Files clients

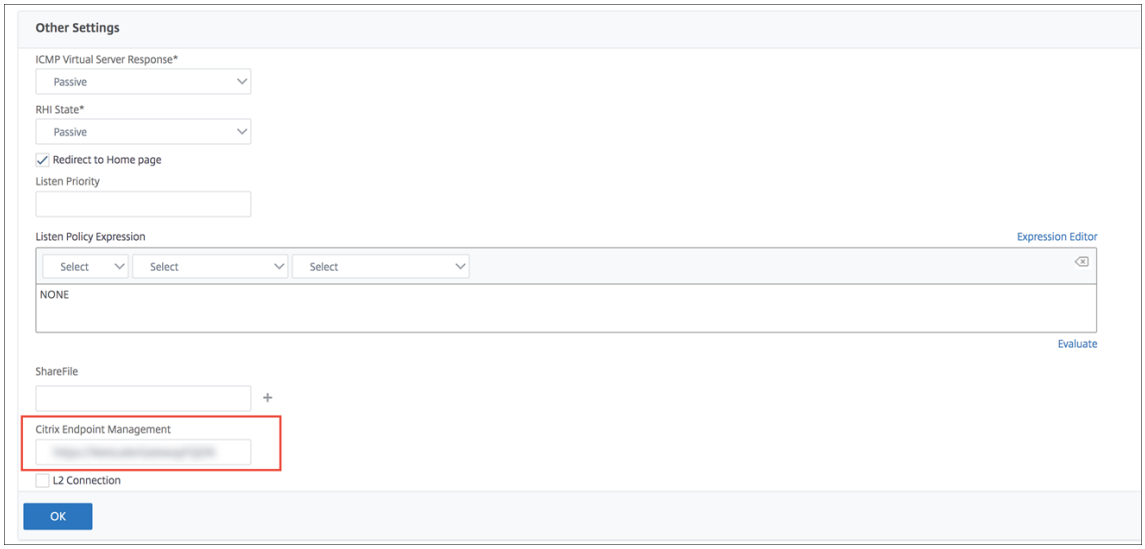
To configure access for non-wrapped Citrix Files clients, such as the website, Outlook plug-in, or the sync clients: Configure NetScaler Gateway to support the use of Citrix Endpoint Management as a SAML identity provider as follows.

- Disable home page redirection.
- Create a Citrix Files session policy and profile.
- Configure policies on the NetScaler Gateway virtual server.

Disable home page redirection

Disable the default behavior for requests that come through the /cginfra path. That action enables users to see the original requested internal URL instead of the configured home page.

1. Edit the settings for the NetScaler Gateway virtual server that is used for Citrix Endpoint Management logons. In NetScaler Gateway, go to **Other Settings** and then clear the checkbox labeled **Redirect to Home Page**.



2. Under **ShareFile** (now called ShareFile), type your Citrix Endpoint Management internal server name and port number.
3. Under **Citrix Endpoint Management**, type your Citrix Endpoint Management URL.

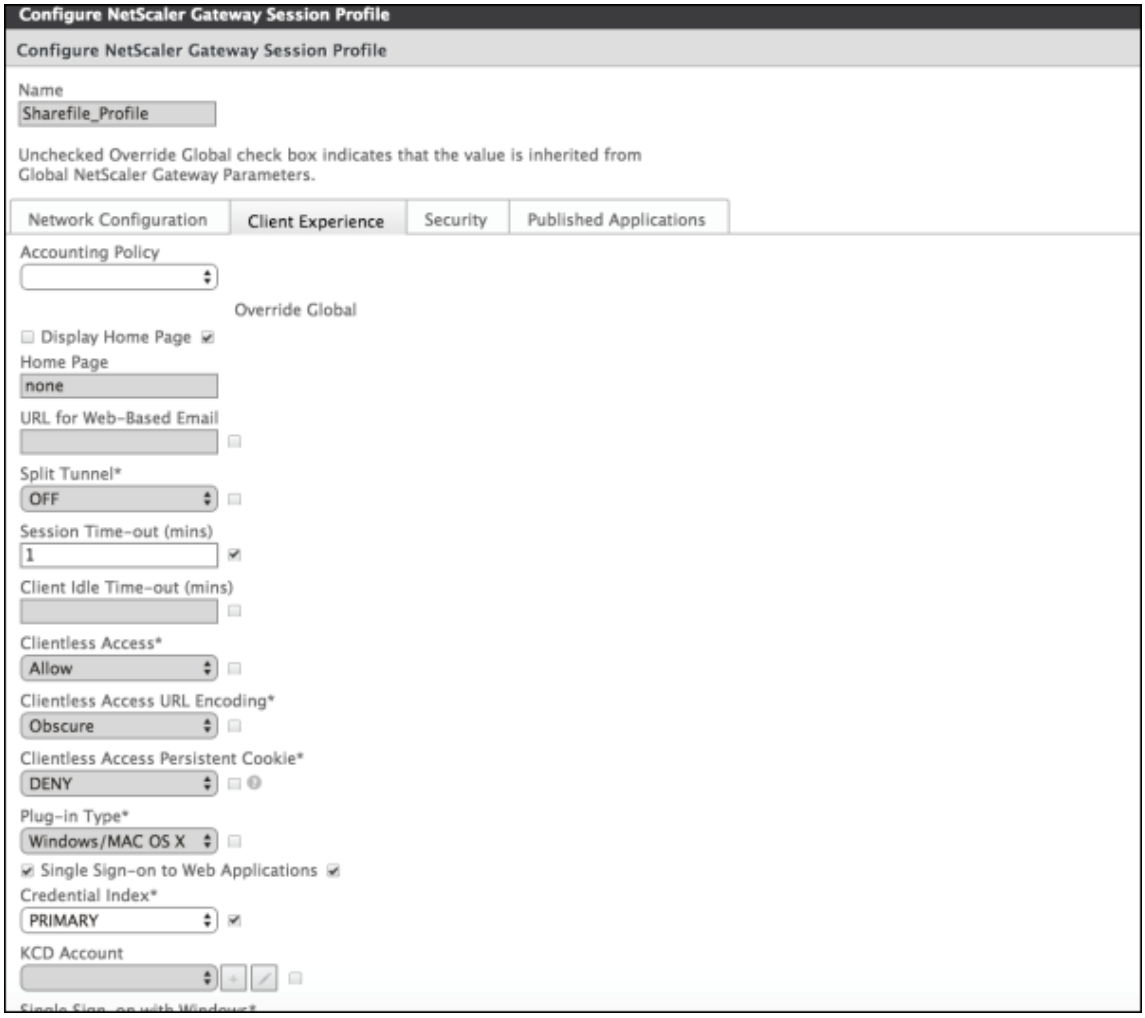
   This configuration authorizes requests to the URL that you entered through the /cginfra path.

Create a Citrix Files session policy and request profile

Configure these settings to create a Citrix Files session policy and request profile:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

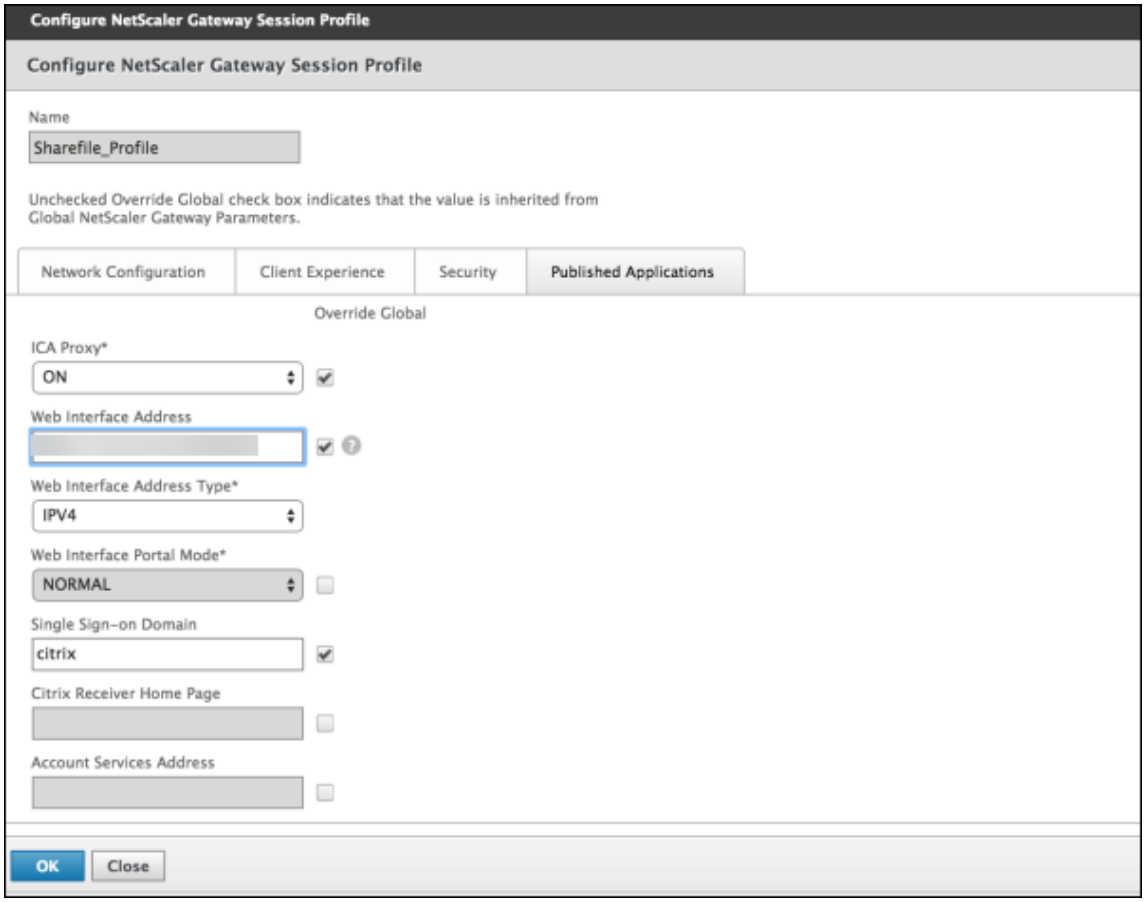
1. In the NetScaler Gateway configuration utility, in the left-hand navigation pane, click **NetScaler Gateway > Policies > Session**.
2. Create a session policy. On the **Policies** tab, click **Add**.
3. In the **Name** field, type **ShareFile_Policy**.
4. Create an action by clicking the **+** button. The **Create NetScaler® Gateway Session Profile** page appears.



Configure these settings:

- **Name:** Type **ShareFile_Profile**.
- Click the **Client Experience** tab and then configure these settings:
  - **Home Page:** Type **none**.
  - **Session Time-out (mins):** Type **1**.
  - **Single Sign-on to Web Applications:** Select this setting.
  - **Credential Index:** Click **PRIMARY**.
- Click the **Published Applications** tab.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



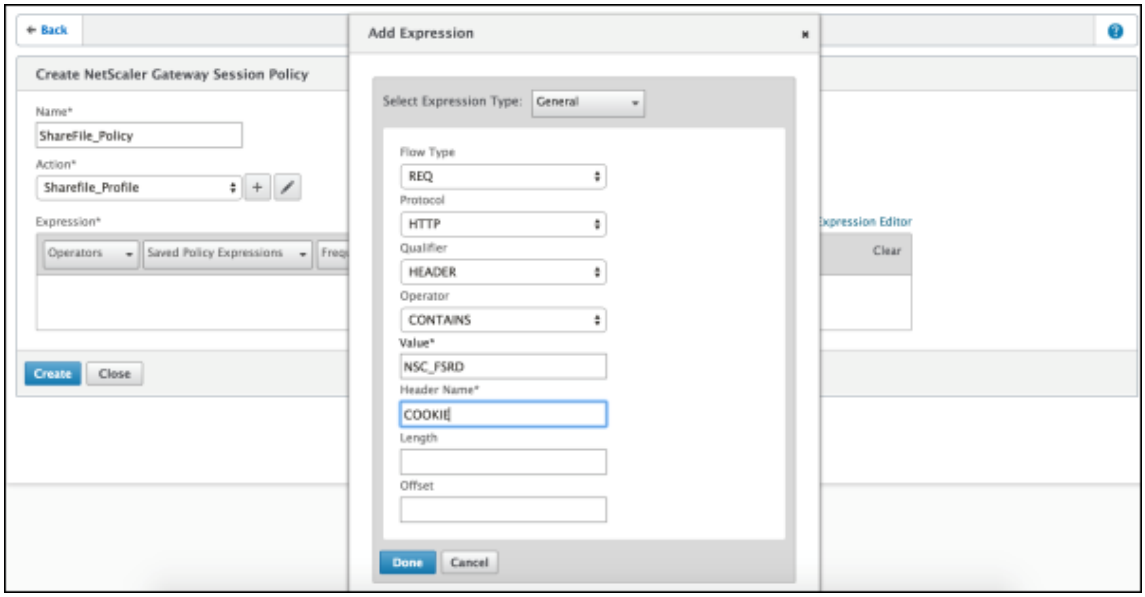
Configure these settings:

- **ICA® Proxy:** Click **On**.
- **Web Interface Address:** Type your Citrix Endpoint Management server URL.
- **Single Sign-on Domain:** Type your Active Directory domain name.

  When configuring the NetScaler Gateway Session Profile, the domain suffix for **Single Sign-on Domain** must match the Citrix Endpoint Management domain alias defined in LDAP.

5. Click **Create** to define the session profile.
6. Click **Expression Editor**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure these settings:

- **Value:** Type **NSC_FSRD**.
- **Header Name:** Type **COOKIE**.

7. Click **Create** and then click **Close**.

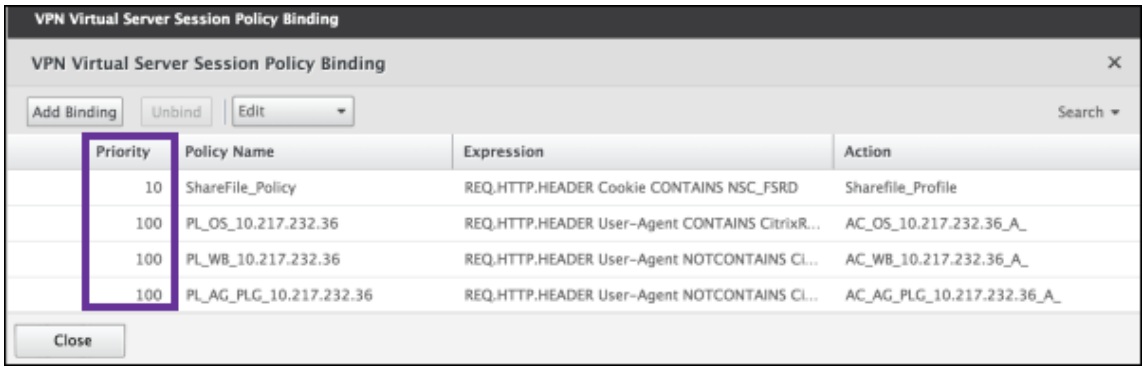
Configure policies on the NetScaler Gateway virtual server

Configure these settings on the NetScaler Gateway virtual server.

1. In the NetScaler Gateway configuration utility, in the left navigation pane, click **NetScaler Gateway > Virtual Servers**.
2. In the **Details** pane, click your NetScaler Gateway virtual server.
3. Click **Edit**.
4. Click **Configured policies > Session policies** and then click **Add binding**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. Select **ShareFile_Policy**.
6. Edit the auto-generated **Priority** number for the selected policy so that it has the highest priority (the smallest number) in relation to any other policies listed. For example:



7. Click **Done** and then save the running NetScaler Gateway configuration.

Modify the Citrix Files.com SSO settings

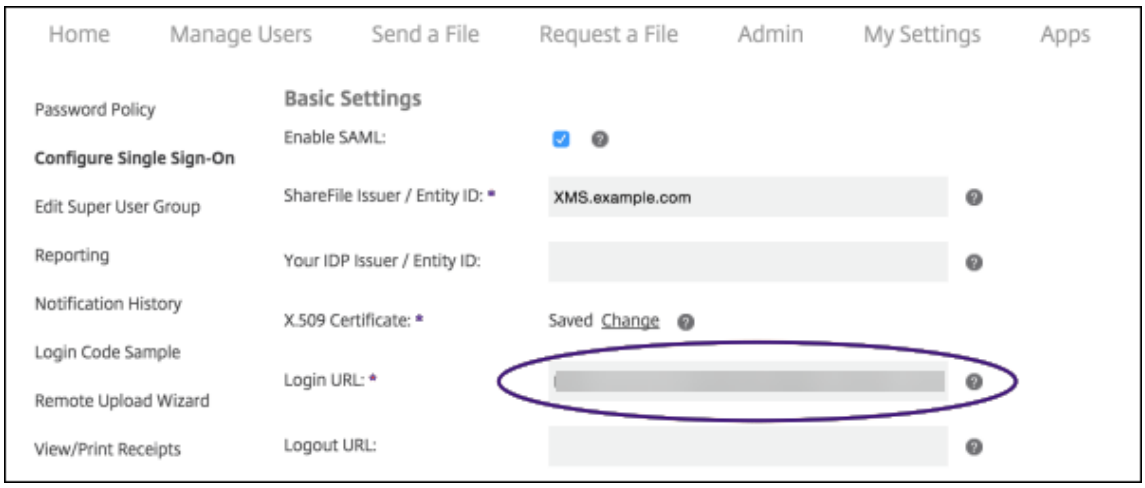
Make the following changes for both MDX and non-MDX Citrix Files apps.

> **Important:**
>
> A new number is appended to the internal application name:
>
> - Each time you edit or recreate the Citrix Files app
> - Each time you change the ShareFile settings in Citrix Endpoint Management
>
> As a result, you must also update the Login URL in the Citrix Files website to display the updated app name.

1. Log on to your ShareFile account (`https://<subdomain>.sharefile.com`) as a ShareFile administrator.
2. In the ShareFile web interface, click **Admin** and then select **Configure Single Sign-on**.
3. Edit the **Login URL** as follows:

   Here's a sample **Login URL** before the edits: `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- Insert the NetScaler Gateway virtual server external FQDN plus **/cginfra/https/** in front of the Citrix Endpoint Management server FQDN and then add **8443** after the Citrix Endpoint Management FQDN.

  Here's a sample of an edited URL: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`

- Change the parameter &app=ShareFile_SAML_SP to the internal Citrix Files application name. The internal name is ShareFile_SAML by default. However, every time you change your configuration, a number is appended to the internal name (ShareFile_SAML_2, ShareFile_SAML_3, and so on). You can look up the **App internal name** on the **Configure > ShareFile** page.

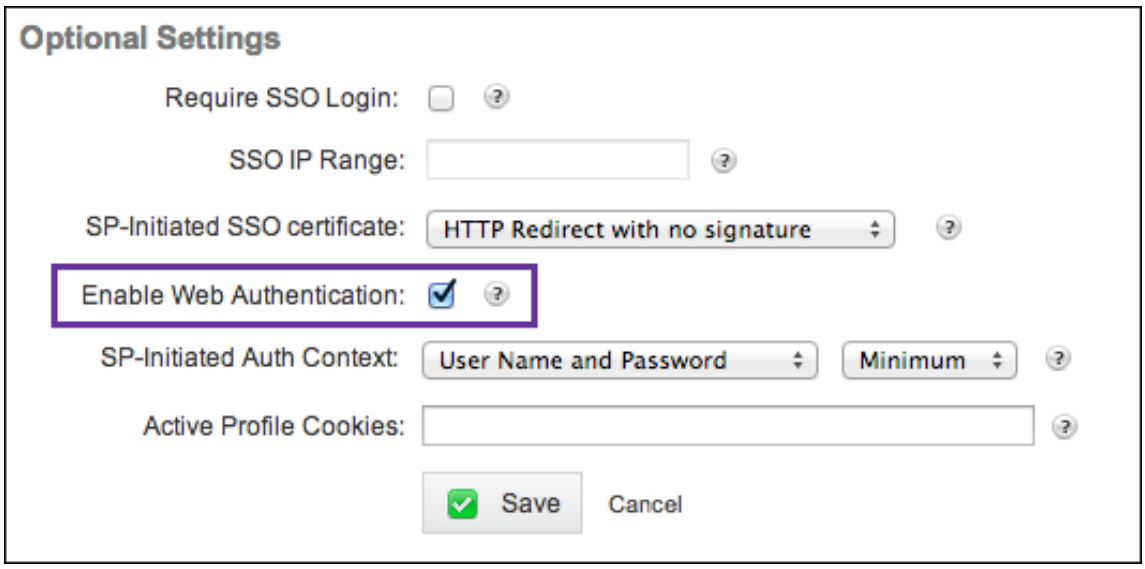
  Here's a sample of an edited URL: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- Add &nssso=**true** to the end of the URL.

  Here's a sample of the final URL: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`.

4. Under **Optional Settings**, select the **Enable Web Authentication** checkbox.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Validate the configuration

Do the following to validate the configuration.

1. Point your browser to `https://<subdomain>sharefile.com/saml/login`.

   You are redirected to the NetScaler Gateway logon form. If you are not redirected, verify the preceding configuration settings.

2. Enter the user name and password for the NetScaler Gateway and Citrix Endpoint Management environment that you configured.

   Your Citrix Files folders at `<subdomain>.sharefile.com` appear. If you do not see your Citrix Files folders, make sure that you entered the proper logon credentials.

Authentication with Azure Active Directory through Citrix Cloud

September 6, 2025

Citrix Endpoint Management supports authentication with Azure Active Directory (Azure AD) credentials through Citrix Cloud. This authentication method is available only to users enrolling in MDM through Citrix Secure Hub.

To use Citrix Secure Hub with MDM+MAM, configure Citrix Endpoint Management to use NetScaler Gateway for MAM enrollment. For more information, see NetScaler Gateway and Citrix Endpoint Management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management uses the Citrix Cloud service, Citrix identity, to federate with Azure Active Directory. Citrix recommends that you use the Citrix identity provider instead of a direct connection to Azure Active Directory.

Citrix Endpoint Management supports authentication with Azure AD for the following platforms:

- iOS and macOS devices not enrolled in the Apple Business Manager or Apple School Manager
- iOS and macOS devices enrolled in the Apple Business Manager
- Android Enterprise devices (preview), for BYOD and fully managed modes

Authentication with Azure AD through Citrix Cloud has these limitations:

- Isn't available for Citrix Endpoint Management local accounts.
- Doesn't support authentication through Azure AD for enrollment invitations. If you send users an enrollment invitation that has an enrollment URL, users authenticate through LDAP instead of Azure AD.

Prerequisites

> **Note:**
>
> Azure Active Directory Standalone is not supported, an on-premises Active Directory is required for integration with Citrix Endpoint Management.

- Azure Active Directory user credentials.
- User groups in Active Directory must match the user groups in Azure Active Directory.
- User names and email addresses in Active Directory must match the user names and email addresses in the Azure Active Directory.
- Citrix Cloud account, with Citrix Cloud Connector installed for directory service synchronization.
- NetScaler Gateway. Citrix recommends that you either enable certificate-based authentication or Azure AD for a full single sign-on experience. If you use LDAP authentication on the NetScaler Gateway for MAM registration, end users experience a dual authentication prompt during enrollment. For more information, see Client certificate or certificate plus domain authentication.
- In the enrollment profile for Android Enterprise, set **Allow users to decline device management** to **Off**. If users decline device management, they can't enroll using an identity provider to authenticate. For more information, see Enrollment security.

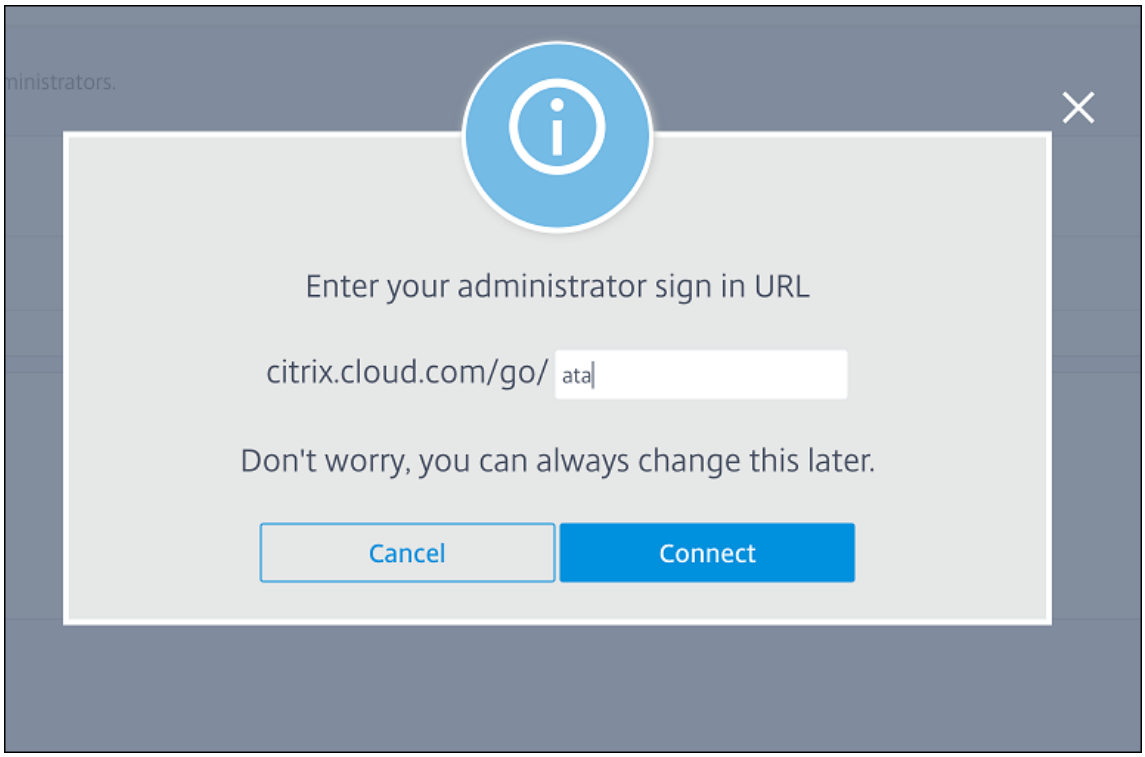
Configure Citrix Cloud to use Azure Active Directory as your identity provider

To set up this service for use with the Citrix Secure Hub, configure Azure Active Directory in Citrix Cloud.

1. Go to https://citrix.cloud.com and sign in to your Citrix Cloud account.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. From the Citrix Cloud menu, go to the **Identity and Access Management** page and connect to Azure Active Directory.
3. Type your administrator sign-in URL and then click **Connect**.



4. After you sign in, your Azure Active Directory account connects to Citrix Cloud. The **Identity and Access Management > Authentication** page shows which accounts to use to sign in to your Citrix Cloud and Azure AD accounts.
5. To enable authentication with Azure AD for users enrolling through the Citrix Secure Hub, under **Workspace Configuration > Authentication**, select **Azure Active Directory**. After you complete the configuration, you can enroll user devices through the Citrix Secure Hub.

Configure Citrix identity as the IdP type for Citrix Endpoint Management

This configuration applies only to users enrolling through Citrix Secure Hub. After you configure Azure Active Directory in Citrix Cloud, configure Citrix Endpoint Management as follows.

1. In the Citrix Endpoint Management console, go to **Settings > Identity Provider (IDP)** and then click **Add**.
2. On the **Identity Provider (IDP)** page, configure the following:

   - **IDP Name:** Type a unique name to identify the IdP connection that you're creating.
   - **IDP Type:** Choose **Citrix Identity Platform**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Authentication Domain:** Choose **Azure Active Directory**. This domain corresponds to the Identity provider domain on the Citrix Cloud **Workspace Configuration > Authentication** page.

3. Click **Next**. On the **IDP Claims Usage** page, configure the following:
   - **User Identifier type:** By default, this field is set to **userPrincipalName**. Make sure that you configure all users with the same identifier in both your on-premises Active Directory and in Azure Active Directory. Citrix Endpoint Management uses this identifier to map users on the identity provider with on-premises Active Directory users.
   - **User Identifier string:** This field is automatically filled.
4. Click **Next**, review the **Summary** page, and then click **Save**.

   Citrix Secure Hub users, Citrix Endpoint Management console, and Self-Help Portal users can now sign in with their Azure Active Directory credentials. Citrix Secure Hub users who are domain-joined can use Citrix Secure Hub to sign in with their Azure AD credentials. Citrix Secure Hub uses client certificate authentication for MAM devices.

Citrix Secure Hub authentication flow

Citrix Endpoint Management uses the following flow to authenticate users with Azure AD as an IdP on devices enrolled through Citrix Secure Hub:

1. A user starts Citrix Secure Hub.
2. Citrix Secure Hub passes the authentication request to Citrix identity, which passes the request to Azure Active Directory.
3. The user types their Azure Active Directory user name and password.
4. Azure Active Directory validates the user and sends a code to Citrix identity.
5. Citrix identity sends the code to Citrix Secure Hub, which sends the code to the Citrix Endpoint Management server.
6. Citrix Endpoint Management gets an ID token by using the code and secret and then validates the user information that's in the ID token. Citrix Endpoint Management returns a session ID.

Authentication with Azure Active Directory Group-Based Administration

September 6, 2025

Citrix Endpoint Management now supports group-based identity authentication for accessing its services through Azure Active Directory (AAD) and SAML identity providers. This update ensures that administrators can manage access at the group level using AAD group membership, offering flexibility

© 1997–2025 Citrix Systems, Inc. All rights reserved.

and enhanced security. The legacy Citrix Identity login mechanism remains available as an alternative.

Key Enhancements

- **Azure AD Group Integration**: Administrators can now manage user access to CEM services by leveraging Azure AD groups. This simplifies permissions management and allows for group-based access controls.
- **Citrix Endpoint Management Login Authentication with Azure AD Groups**: Users can authenticate through Azure AD groups, providing seamless integration with existing organizational identity infrastructure.
- **Full Support for SAML**: SAML identity providers can also be used for group-based authentication.
- **Legacy Citrix Identity Support**: Citrix Identity login is still available, ensuring users can transition at their own pace.

Feature Flags

- **Citrix Cloud™ feature flag**: `fullAccessGroups` –This feature is enabled by default to allow full access for groups.
- **Citrix Endpoint Management feature flag**: `cc.group.based.admin` –Enables group-based administration functionality in Citrix Endpoint Management.

Prerequisites

- Azure AD is configured in the Citrix Cloud portal.
- Admin Sign-in URL for Citrix Cloud needs to be set for accessing Citrix Endpoint Management through Azure AD groups.

Configuration Steps

1. Log in to the Azure Portal and access Azure Active Directory.
2. Navigate to Users and select Create new user.
3. Navigate to Groups, click New group, and add the newly created user as a member of this group.
4. Log in to Citrix Cloud using Admin credentials to sign in.
5. Navigate to Identity and Access Management, assign either full or custom permissions to the new Azure AD group.
6. The user in the Azure AD group can now log in to Citrix Endpoint Management™ using the Admin Sign-in URL.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Authentication with Azure Active Directory through NetScaler Gateway for MAM enrollment

April 17, 2025

Citrix Endpoint Management supports authentication with Azure Active Directory (Azure AD) credentials through NetScaler Gateway. This authentication method is available only for users enrolling in MAM through Citrix Secure Hub.

Prerequisites

To configure Citrix Endpoint Management to use Azure AD through NetScaler Gateway as an identity provider (IdP) for devices enrolled with MAM, make sure that the following prerequisites are met:

- Configure Citrix Endpoint Management with Azure AD through Citrix Cloud as IdP for devices enrolled with MDM. For more information about configuring Azure AD for MDM, see Authentication with Azure Active Directory through Citrix Cloud.
- Connect Azure AD to Citrix Cloud. For more information, see Connect Azure Active Directory to Citrix Cloud.
- Enable the following relevant feature flags depending on the platform respectively:
  - iOS:
    - iOS-V3Form-MAM
    - iOS-SAMLAuth-MAM
  - Android:
    - Android-V3Form-MAM
    - Android-SAMLAuth-MAM

  > **Note:**
  >
  > To enable this feature, contact your support team.

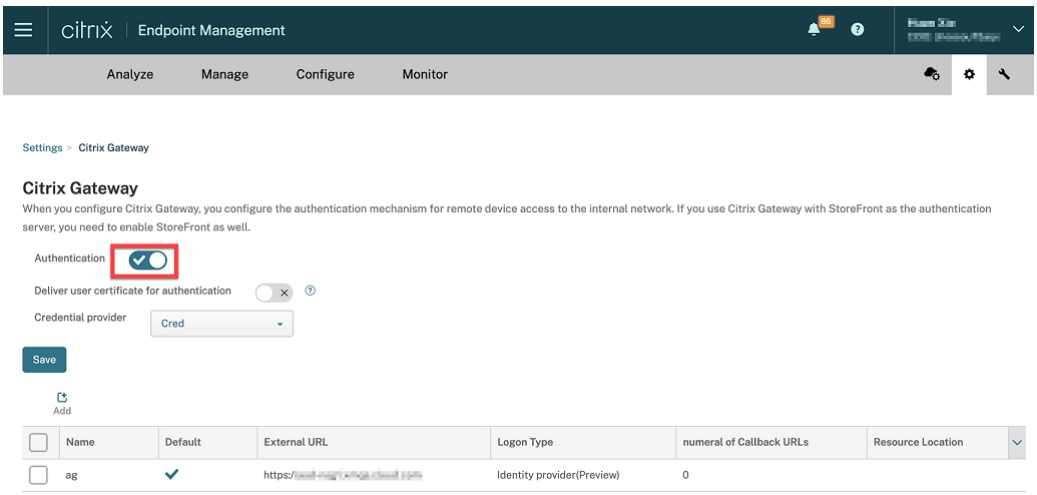
- For Android, enable **Android Enterprise**.

  > **Note:**
  >
  > This feature is not tested or verified under legacy Android Device Administrator (DA) mode. This mode is not supported.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure Azure AD for MAM as IdP

1. Configure NetScaler Gateway in Citrix Endpoint Management as follows:
   a) Sign in to the Citrix Endpoint Management console and then click the **Settings** icon.
   b) Click **NetScaler Gateway** under **Server**.
   c) Enable the **Authentication** toggle button.



   d) Make sure that the **Logon Type** of the gateway is the *Identity provider*.
   e) Click **Save**.
2. Configure Azure AD as a SAML IdP by using Configure Azure AD as a SAML IdP.
3. Configure NetScaler ADC as a SAML SP using the advanced policy by using Configure NetScaler ADC as SAML service provider (SP).
4. Create a AAA virtual server by using To set up an authentication virtual server by using the GUI.
5. Configure the AAA virtual server by using Configure the authentication virtual server.
6. Create and configure the authentication profile by using Authentication profiles.
7. Bind the authentication profile with the Gateway virtual server and save all the configurations.

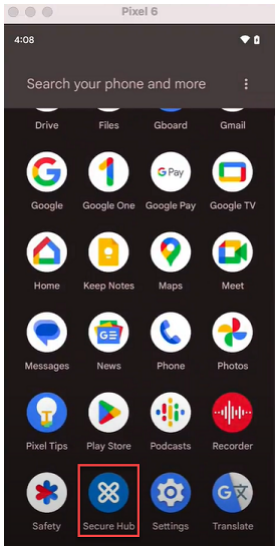
Now, Azure AD is added as an identity provider for devices enrolled with MAM and you can authenticate them using Azure AD.

Expected behavior

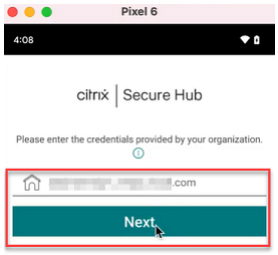
The following example is using an Android device:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. On your mobile device, open the Citrix Secure Hub app.

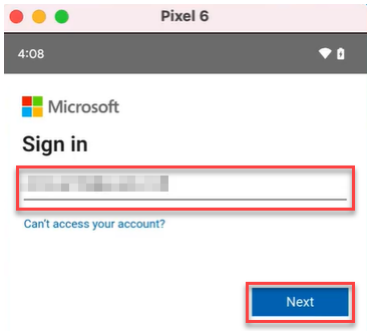


2. Provide the required permissions.
3. On the sign-in page, enter the credentials provided by your organization and then tap **Next**.



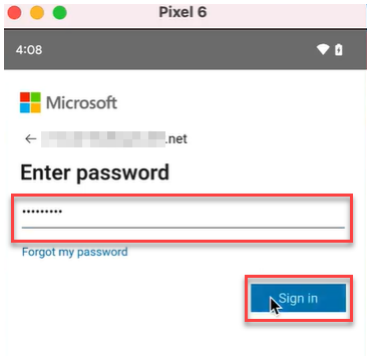
You are redirected to the Microsoft sign-in page.

4. On the Microsoft sign in page, enter your email id and then tap **Next**.

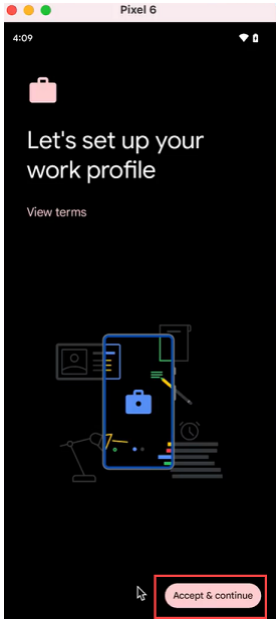


5. Enter the password and then tap **Sign in**.

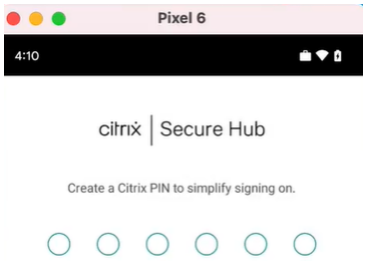
© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. On the **Let's set up your work profile** page, tap **Accept & continue**.



7. Create the pin for the Citrix Secure Hub app and confirm the same.



You are successfully redirected to the Citrix Secure Hub home page.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Authentication with Okta through Citrix Cloud

September 6, 2025

Citrix Endpoint Management supports authentication with Okta credentials through Citrix Cloud. This authentication method is available only to users enrolling in MDM through the Citrix Secure Hub.

Devices enrolling in MAM can't authenticate using Okta credentials through Citrix Cloud. To use Citrix Secure Hub with MDM+MAM, configure Citrix Endpoint Management to use NetScaler Gateway for MAM enrollment. For more information, see NetScaler Gateway and Citrix Endpoint Management.

Citrix Endpoint Management uses the Citrix Cloud service, Citrix identity, to federate with Okta. Citrix recommends that you use the Citrix identity provider instead of a direct connection to Okta.

Citrix Endpoint Management supports authentication with Okta for the following platforms:

- iOS and macOS devices not enrolled in the Apple Business Manager or Apple School Manager
- iOS and macOS devices enrolled in the Apple Business Manager
- Android Enterprise devices (preview), for BYOD and fully managed modes

Authentication with Okta through Citrix Cloud has these limitations:

- Isn't available for Citrix Endpoint Management local accounts.
- Doesn't support authentication through Okta for enrollment invitations. If you send users an enrollment invitation that has an enrollment URL, users authenticate through LDAP instead of Okta.

Prerequisites

- Okta user credentials
- User groups in the Active Directory must match the user groups at Okta.
- User names and email addresses in the active directory must match the user names and email addresses at Okta.
- Citrix Cloud account with Citrix Cloud Connector installed for directory service synchronization.
- NetScaler Gateway. Citrix recommends that you enable certificate-based authentication for a full single sign-on experience. If you use LDAP authentication on the NetScaler Gateway for MAM registration, end users experience a dual authentication prompt during enrollment. For more information, see Client certificate or certificate plus domain authentication.
- In the enrollment profile for Android Enterprise, set **Allow users to decline device management** to **Off**. If users decline device management, they can't enroll using an identity provider to authenticate. For more information, see Enrollment security.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

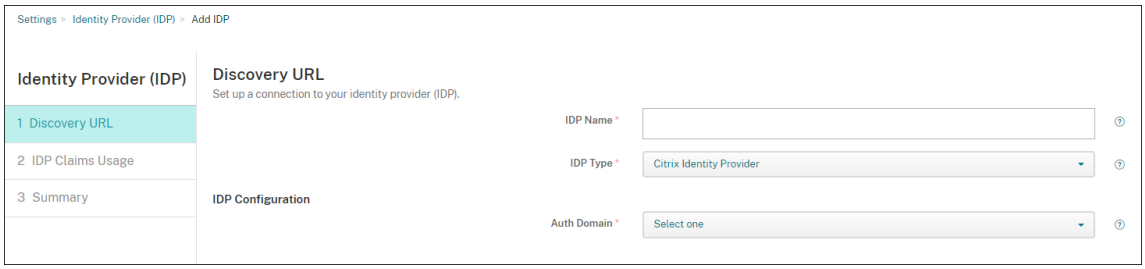
Configure Citrix Cloud to use Okta as your identity provider

To configure Okta in Citrix Cloud, see Connect Okta as an identity provider to Citrix Cloud.

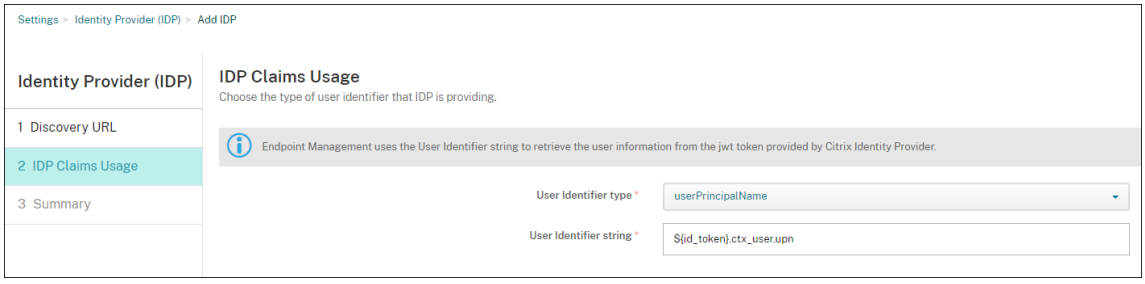
Configure Citrix identity as the IdP type for Citrix Endpoint Management

This configuration applies only to users enrolling through Citrix Secure Hub. After you configure Azure Active Directory in Citrix Cloud, configure Citrix Endpoint Management as follows:

1. In the Citrix Endpoint Management console, go to **Settings > Identity Provider (IDP)** and then click **Add**.
2. On the **Identity Provider (IDP)** page, configure the following:



   - **IDP Name:** Type a unique name to identify the IdP connection that you are creating.
   - **IDP Type:** Choose **Citrix Identity Provider**.
   - **Authentication Domain:** Choose the Citrix Cloud domain. If you aren't sure which one to choose, your domain appears on the Citrix Cloud **Identity and Access Management > Authentication** page.
3. Click **Next**. In the **IDP Claims Usage** page, configure the following:



   - **User Identifier type:** This field is set to **userPrincipalName**. Make sure that you configure all users with the same identifier in your on-premises Active Directory and at Okta. Citrix Endpoint Management uses this identifier to map users on the identity provider with on-premises Active Directory users.
   - **User Identifier string:** This field is automatically filled.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

After this configuration, Citrix Secure Hub users who are domain-joined can use Citrix Secure Hub to sign in with their Okta credentials. Citrix Secure Hub uses client certificate authentication for MAM devices.

Citrix Secure Hub authentication flow

Citrix Endpoint Management uses the following flow to authenticate users with Okta as an IdP on devices enrolled through Citrix Secure Hub:

1. A user starts Citrix Secure Hub.
2. Citrix Secure Hub passes the authentication request to Citrix identity, which passes the request to Okta.
3. The user types their user name and password.
4. Okta validates the user and sends a code to Citrix identity.
5. Citrix identity sends the code to Citrix Secure Hub, which sends the code to the Citrix Endpoint Management server.
6. Citrix Endpoint Management gets an ID token by using the code and secret, and then validates the user information that's in the ID token. Citrix Endpoint Management returns a session ID.

Authentication with Okta through NetScaler Gateway for MAM enrollment

September 6, 2025

Citrix Endpoint Management supports authentication with Okta credentials through NetScaler Gateway. This authentication method is available only for users enrolling in MAM through Citrix Secure Hub.

Prerequisites

To configure Citrix Endpoint Management to use Okta through NetScaler Gateway as an identity provider (IdP) for devices enrolled with MAM, make sure that the following prerequisites are met:

- Configure Citrix Endpoint Management with Okta through Citrix Cloud as IdP for devices enrolled with MDM. For more information about configuring Okta for MDM, see Authentication with Okta through Citrix Cloud.
- Enable the following relevant feature flags depending on the platform respectively:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

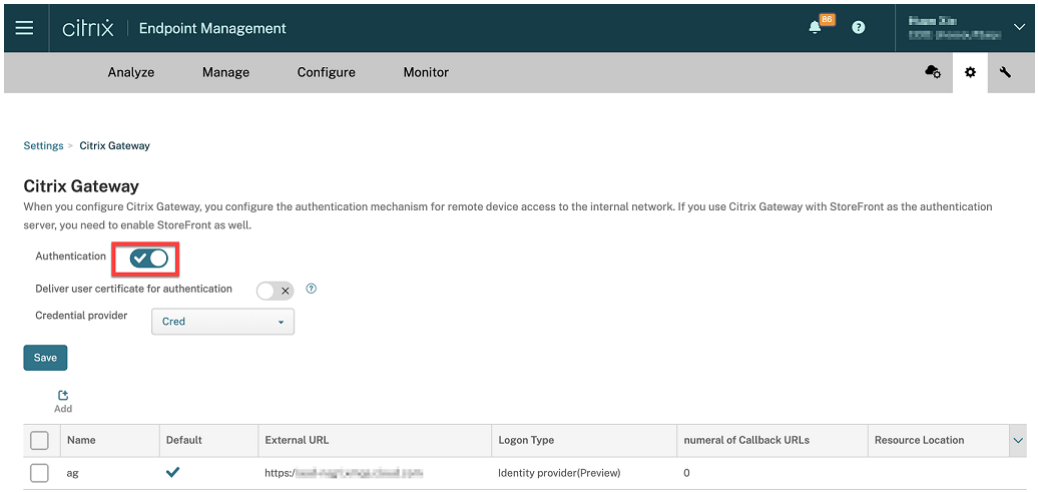
  - iOS:
    - iOS-V3Form-MAM
    - iOS-SAMLAuth-MAM
  - Android:
    - Android-V3Form-MAM
    - Android-SAMLAuth-MAM

> **Note:**
>
> To enable this feature, contact your support team.

- Download and install the latest version of Citrix Secure Hub.
- Make sure that the Okta service is available for your organization and the relevant users and groups are created or imported to Okta.

Configure NetScaler Gateway in Citrix Endpoint Management

1. Sign in to the Citrix Endpoint Management console and then click the **Settings** icon.
2. Click **NetScaler Gateway** under **Server**.
3. Enable the **Authentication** toggle button.



4. Make sure that the **Logon Type** of the gateway is the *Identity provider*.
5. Click **Save**.

Prepare on-premises NetScaler Gateway

1. If you do not have an on-premises NetScaler Gateway configured for Citrix Endpoint Management, then do the following steps:

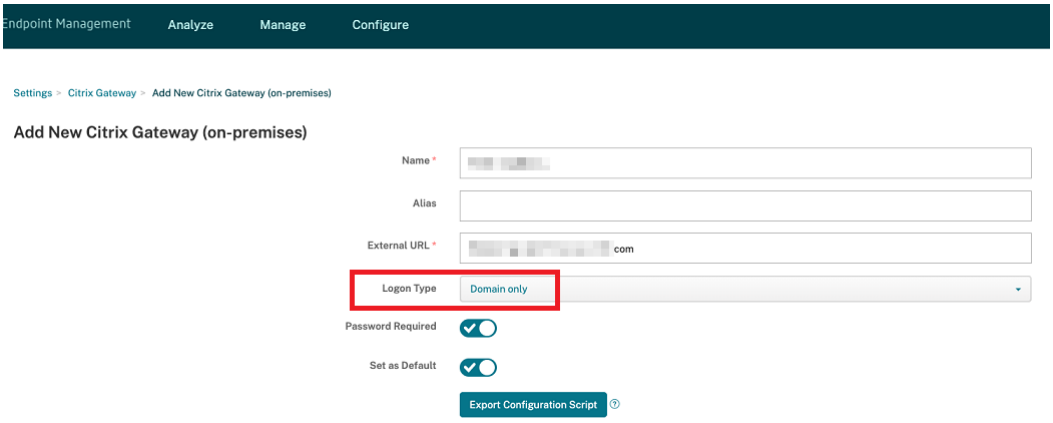
© 1997–2025 Citrix Systems, Inc. All rights reserved.

a) In the Citrix Endpoint Management console. click the **Settings** icon.

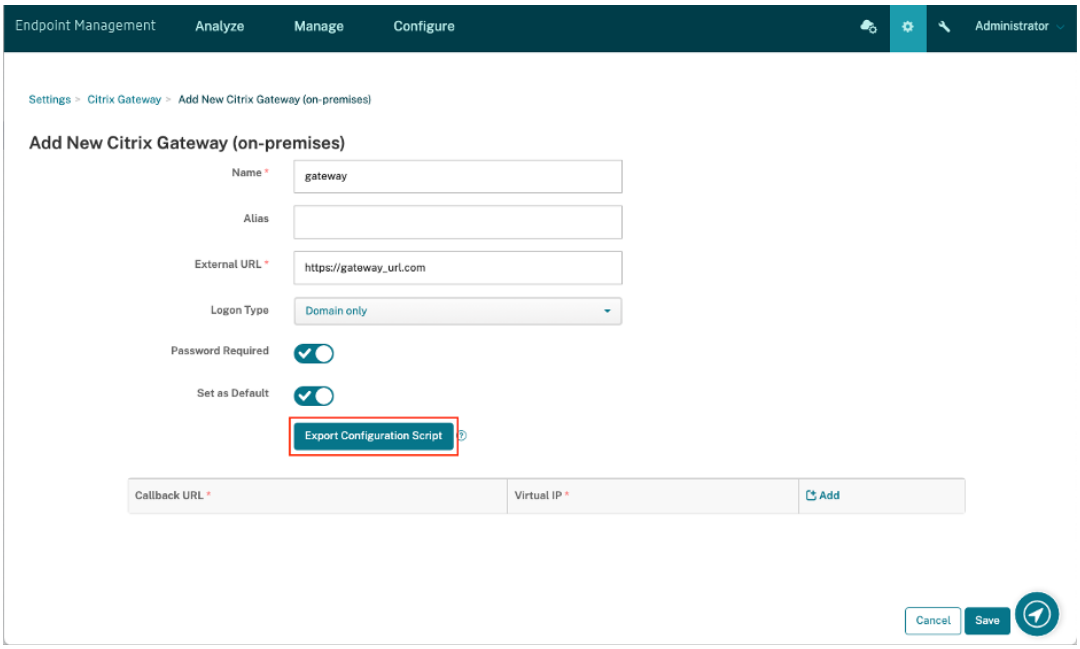
b) Click **NetScaler Gateway** under **Server**.

c) Click **Edit**.

d) Click the **Logon Type** drop-down menu and select *Domain only*.



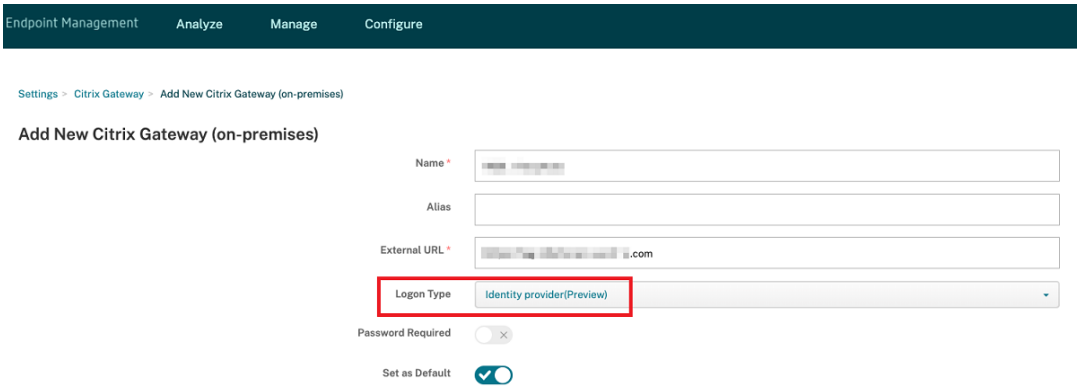
e) Click **Export Configuration Script**.



The **Export Configuration Script** is downloaded.

f) Click the **Logon Type** drop-down menu and select *Identity provider*.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



g) Click **Save**.

h) Open the downloaded zip file and extract the files from it.

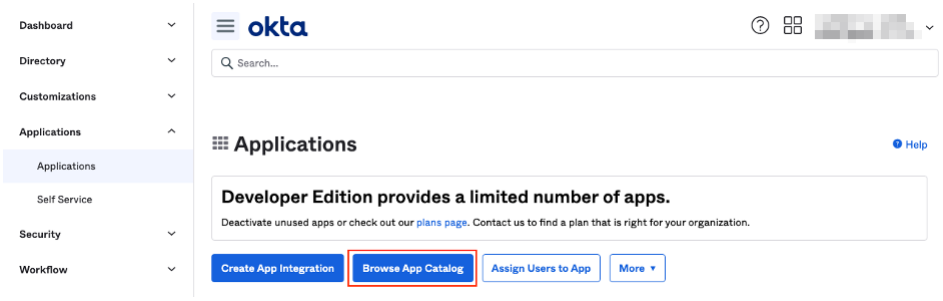
i) Run the scripts in the extracted .txt files to prepare the on-premises NetScaler Gateway.

2. Sign in to the Citrix ADC management console and then navigate to **NetScaler Gateway** > **Virtual Servers**.
3. Click the gateway relevant to your Citrix Endpoint Management setup.
4. Unbind any existing authentication policies on the on-premises NetScaler Gateway.

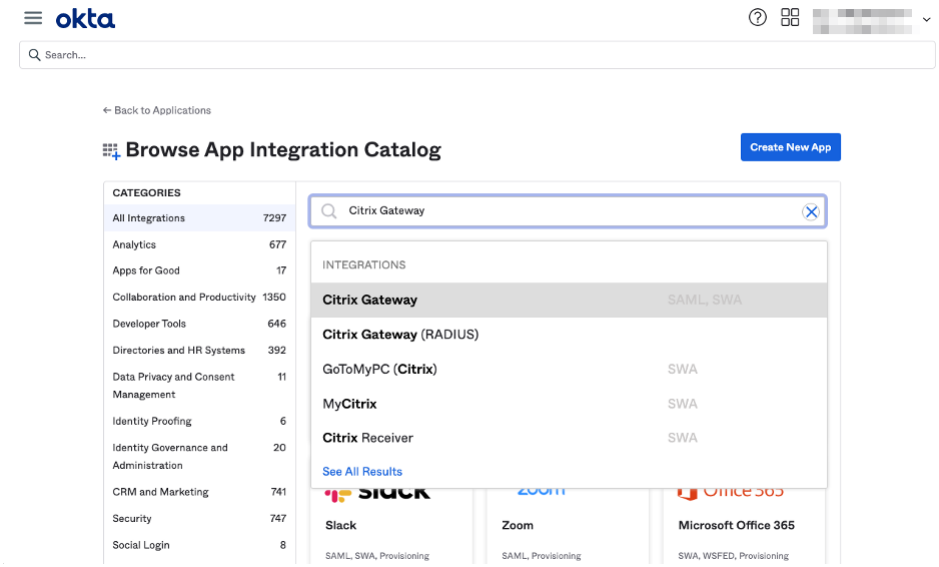
Configure Okta

1. Sign in to Okta as administrator.
2. Click **Applications** > **Applications** > **Browse App Catalog**.

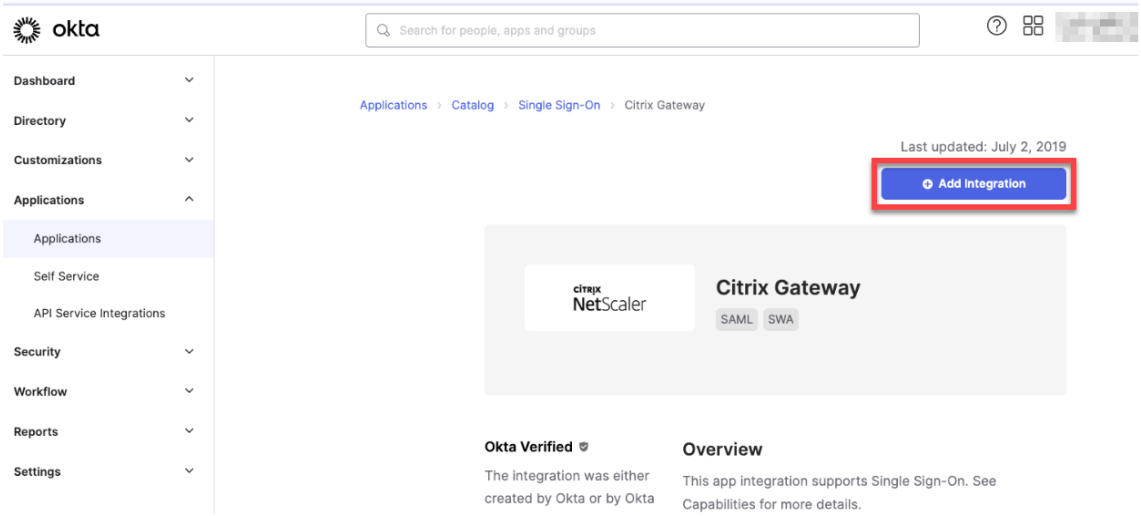
© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Type **NetScaler Gateway** in the search bar under **Browse App Integration Catalog** and then select **NetScaler Gateway (SAML, SWA)**.

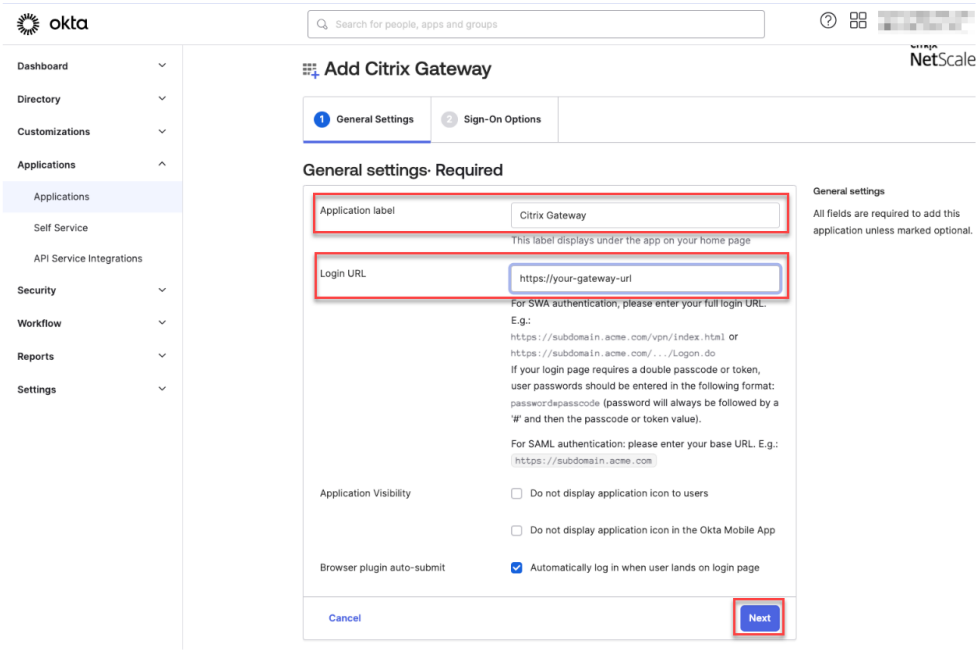


4. Click **Add Integration**.



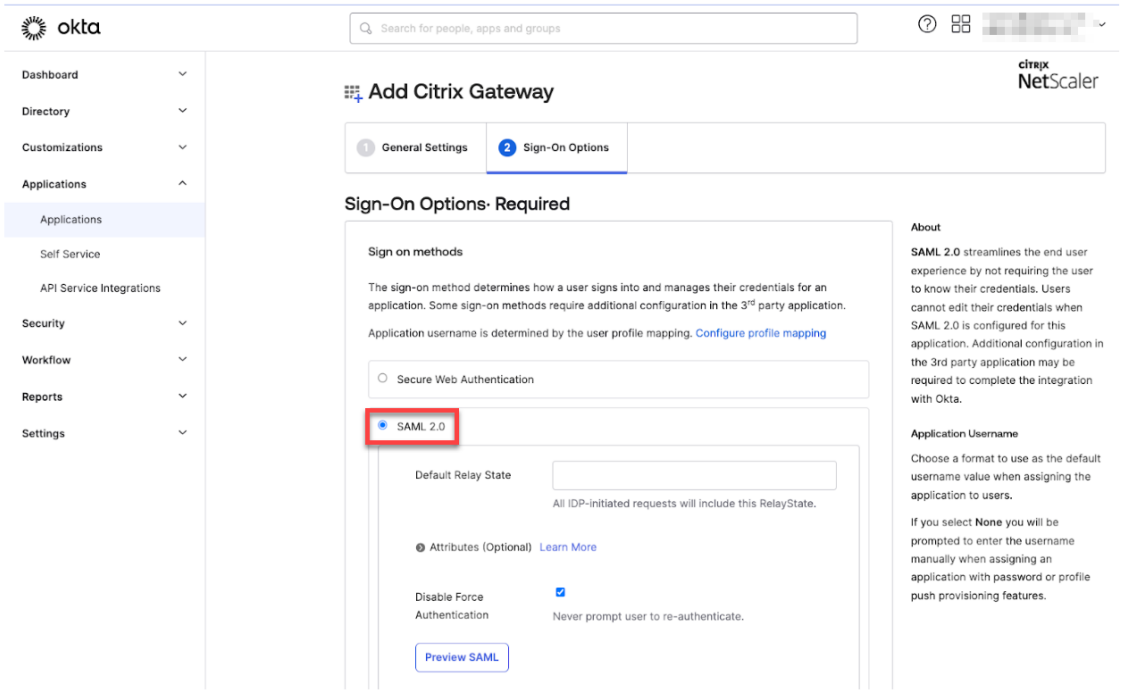
5. Enter the relevant name in the **Application label** field.
6. Enter the gateway virtual server URL in the **Login URL** field and then click **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



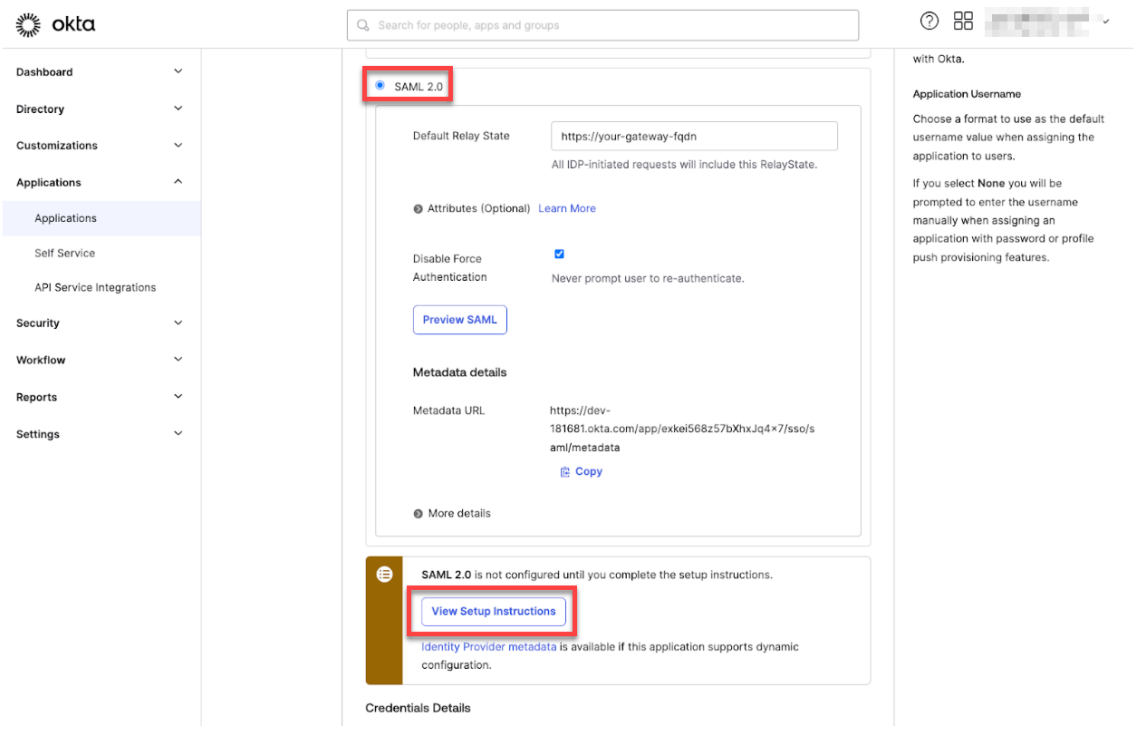
> **Note:**
>
> The URL entered in the **Login URL** field must be the same as the NetScaler Gateway URL for Citrix Endpoint Management settings.

7. Under **Sign-On Options Required** > **Sign on methods**, select **SAML 2.0**.



8. Click **View Setup Instructions** and follow the instructions provided in the page to create the SAML policy in the Citrix® on-premises gateway admin console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> - After installing the CA certificate while configuring NetScaler Gateway versions 11.1 or later, create a SAML action. To create SAML action, navigate to **Security** > **AAA - Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** > **Actions** > **SAML Actions**. Click **Add** and fill the information as provided in the preceding page. Don't follow the navigation provided in the page that is, **Netscaler Gateway** > **Policies** > **Authentication** > **SAML** > **Servers**.
> - Also, don't follow the steps provided to create SAML policy as those steps are using classic policy. We are using advanced policy now. Do the following step 9 to create a SAML policy using an advanced policy.

9. Create a corresponding SAML policy for the SAML action, and bind the policy to the authentication virtual server as follows:

   a) Navigate to **Security** > **AAA-Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** and click **Add**.

   b) On the Create Authentication Policy page, provide the following details:

   - **Name** - Specify a name for the SAML policy.
   - **Action Type** - Select *SAML* as the authentication action type.
   - **Action** - Select the SAML server profile to bind the SAML policy with.
   - **Expression** - Displays the name of the rule or expression that the SAML policy uses to determine if the user must authenticate with the SAML server. On the text box, set

© 1997–2025 Citrix Systems, Inc. All rights reserved.

the value **rule** = `true` for the SAML policy to take effect and the corresponding SAML action to be run.

c) Bind the SAML policy to the VPN virtual server and link the VPN virtual server to the authentication virtual server through an authentication profile. For more information about the binding procedure, see Bind the authentication policy.

10. Create a AAA virtual server by using To set up an authentication virtual server by using the GUI.
11. Configure the AAA virtual server by using Configure the authentication virtual server.
12. Create and configure the authentication profile by using Authentication profiles.
13. Bind the authentication profile with the Gateway virtual server and save all the configurations.
14. After creating the SAML policy in the Citrix on-premises gateway admin console, click Done.

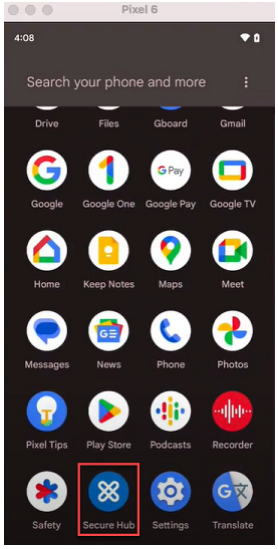
    Now, you can see two applications for Citrix Endpoint Management integration that is, a web application for Citrix Cloud and a SAML application for Citrix Endpoint Management MAM authentication.
15. Assign the relevant users and groups to the SAML application that you created.

Now, Okta is added as an identity provider for devices enrolled with MAM and you can authenticate them using Okta.

Expected behavior

The following example is using an Android device:

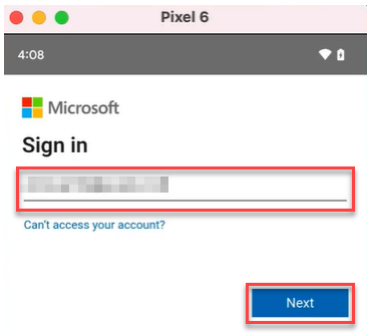
1. On your mobile device, open the Citrix Secure Hub app.



2. Provide the required permissions.

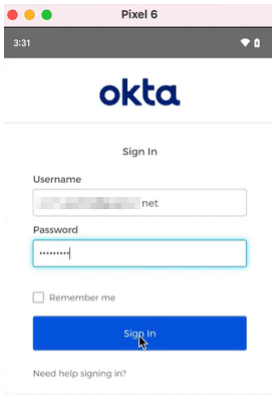
© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. On the sign-in page, enter the credentials provided by your organization and then tap **Next**.

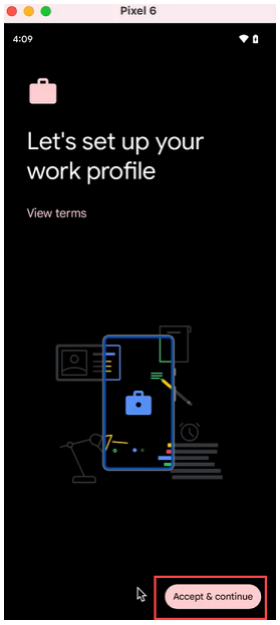


You are redirected to the Okta sign in page.

4. On the Okta sign in page, enter your credentials and then tap **Sign in**.

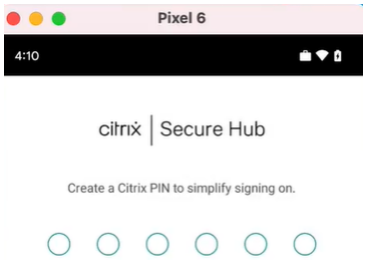


5. On the **Let's set up your work profile** page, tap **Accept & continue**.



6. Create the pin for the Citrix Secure Hub app and confirm the same.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



You are successfully redirected to the Citrix Secure Hub home page.

Authentication with an on-premises NetScaler Gateway through Citrix Cloud

September 6, 2025

Citrix Endpoint Management supports authentication with an on-premises NetScaler Gateway through Citrix Cloud. This authentication method is available only to users enrolling in MDM through the Citrix Secure Hub.

Devices enrolling in MAM can't authenticate using on-premises NetScaler Gateway credentials through Citrix Cloud. To use Citrix Secure Hub with MDM+MAM, configure Citrix Endpoint Management to use NetScaler Gateway for MAM enrollment. For more information, see NetScaler Gateway and Citrix Endpoint Management.

Citrix Endpoint Management supports authentication with an on-premises NetScaler Gateway through Citrix Cloud for the following platforms:

- iOS devices
- Android Enterprise devices, for BYOD and fully managed modes

> **Note:**
>
> Citrix Endpoint Management doesn't support authentication with an on-premises NetScaler Gateway through Citrix Cloud for enrollment invitations. If you send users an enrollment invitation that has an enrollment URL, users authenticate through LDAP instead of an on-premises NetScaler Gateway as an identity provider.

It is recommended that you enable certificate-based authentication for a full single sign-on experience. If you use LDAP authentication on the NetScaler Gateway for MAM registration, then the end users experience a dual authentication prompt during enrollment. For more information, see Client certificate or certificate plus domain authentication.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Prerequisites

- NetScaler Gateway. Citrix recommends that you enable certificate-based authentication for a full single sign-on experience. If you use LDAP authentication on the NetScaler Gateway for MAM registration, end-users experience a dual authentication prompt during enrollment. For more information, see Client certificate or certificate plus domain authentication.
- Citrix Cloud account with Citrix Cloud Connector installed for directory service synchronization.
- Citrix Secure Hub 20.5.0 and later.

Configure Citrix Cloud to use NetScaler Gateway as your identity provider

To set up NetScaler Gateway authentication in Citrix Cloud, see Connect an on-premises NetScaler Gateway as an identity provider to Citrix Cloud.

Configure the Citrix identity provider as the IdP type for Citrix Endpoint Management

This configuration applies only to users enrolling through Citrix Secure Hub. After you configure NetScaler Gateway in Citrix Cloud, configure Citrix Endpoint Management as follows.

1. In the Citrix Endpoint Management console, go to **Settings > Identity Provider (IDP)** and then click **Add**.
2. On the **Identity Provider (IDP)** page, configure the following:
   - **IDP Name:** Type a unique name to identify the IdP connection that you're creating.
   - **IDP Type:** Choose **Citrix Identity Provider**.
   - **Authentication Domain:** Choose **NetScaler Gateway**. This domain corresponds to your Identity provider domain on the Citrix Cloud **Workspace Configuration > Authentication** page.
3. Click **Next**. On the **IDP Claims Usage** page, configure the following:
   - **User Identifier type:** By default, this field is set to **userPrincipalName**.
   - **User Identifier string:** This field is automatically filled.
4. Click **Next**, review the **Summary** page, and then click **Save**.

   You can now enroll user devices through Citrix Secure Hub using an on-premises NetScaler Gateway as an identity provider.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Secure Hub authentication flow

Citrix Endpoint Management uses the following flow to authenticate users with an on-premises NetScaler Gateway as an IdP on devices enrolled through Citrix Secure Hub:

1. A user starts Citrix Secure Hub.
2. Citrix Secure Hub passes the authentication request to Citrix identity, which passes the request to an on-premises NetScaler Gateway.
3. The user types their user name and password.
4. An on-premises NetScaler Gateway validates the user and sends a code to Citrix identity.
5. Citrix identity sends the code to Citrix Secure Hub, which sends the code to the Citrix Endpoint Management server.
6. Citrix Endpoint Management gets an ID token by using the code and secret and then validates the user information that's in the ID token. Citrix Endpoint Management returns a session ID.

nFactor authentication

September 6, 2025

nFactor authentication allows you to use all the authentication modes currently possible with the NetScaler when you're using Citrix Secure Hub. It enhances the security of an application by requiring the users to provide more proofs of identity to gain access. For more information about nFactor authentication, see nFactor authentication.

Also, for more information about different authentication and authorization methods and how to configure them, see Authentication and Authorization.

Citrix Endpoint Management supports the following authentication types with nFactor authentication:

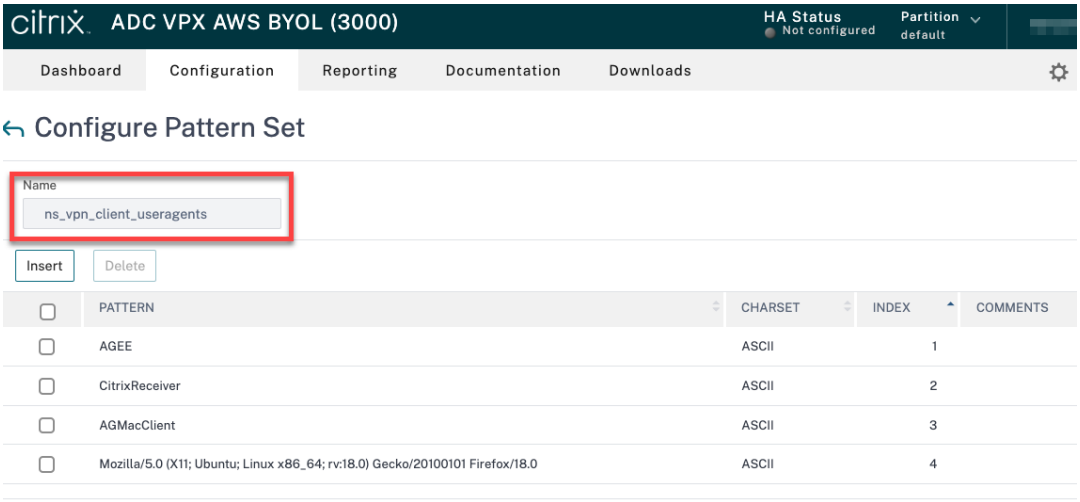
- Local
- Lightweight Directory Access Protocol (LDAP)
- RADIUS
- SAML
- Client certificate authentication

Prerequisites

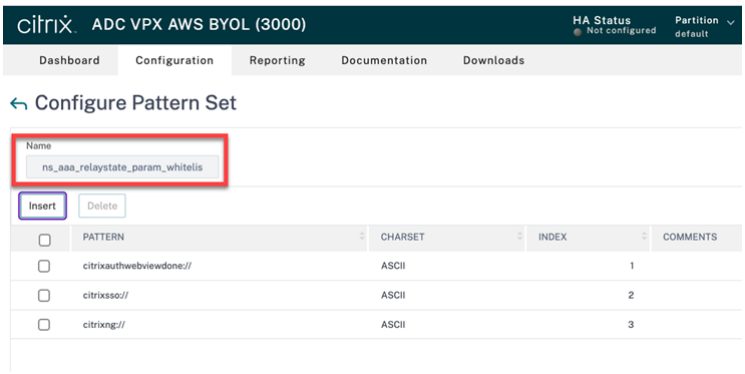
To configure Citrix Endpoint Management to use nFactor authentication, make sure that the following prerequisites are met:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Make sure that you are using NetScaler 13.0 or later.
- Make sure that you have configured the following pattern set settings in the NetScaler® for your Android and iOS devices:
  - Ns_vpn_client_useragents



  - Ns_aaa_relaystate_param_whitelist



- Make sure that you installed the latest version of Citrix Secure Hub from Apple or Google Play.
- Make sure that you are using the Advanced authentication policy in the NetScaler Gateway.
- Make sure that you set the client property **ENABLE_MAM_NFACTOR_SSO** as **True** for both on-premises and cloud. For more information about the **ENABLE_MAM_NFACTOR_SSO** property, see Client property reference.

> **Note:**
>
> If the client property **Enable nFactor SSO** is set to **False**, then make sure that the classic authentication policies are bound to the NetScaler Gateway.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure nFactor authentication

Configure nFactor authentication for Citrix Endpoint Management depending on how your NetScaler Gateway is set up as follows:

- Citrix Endpoint Management is already set up with the NetScaler Gateway using the Classic authentication policy. For more information, see Update the Classic policy to the Advanced authentication policy in the existing NetScaler Gateway.
- Citrix Endpoint Management setup with the NetScaler Gateway using the Advanced authentication policy. For more information, see Configure the NetScaler Gateway setup using the Advanced policy.

Update the Classic policy to the Advanced authentication policy in the existing NetScaler Gateway

If your Citrix Endpoint Management is already setup using the Classic authentication policy in the NetScaler Gateway, then you must update the Classic authentication policy to the Advanced authentication policy using one of the following methods:

- Create an Advanced authentication policy and change the gateway configuration to use the Advanced authentication policy. For more information, see Authentication policies.
- Update the Classic authentication policy to the Advanced authentication policy. For more information see, Converting policy expressions using the NSPEPI tool.

Configure the NetScaler Gateway setup using the Advanced policy

To configure the nFactor authentication for Citrix Endpoint Management in the NetScaler Gateway using the Advanced authentication policy, see Configure nFactor authentication.

> **Note:**
>
> - You can choose the relevant authentication type from the supported authentication types.
> - If you are using SAML authentication type, then you can configure SAML using MAM IdP using one of the following methods:
>   - To configure using Azure Active Directory, see Authentication with Azure Active Directory through NetScaler Gateway for MAM enrollment.
>   - To configure using Okta, see Authentication with Okta through NetScaler Gateway for MAM enrollment.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

User accounts, roles, and enrollment

September 6, 2025

You do user configuration tasks in the Citrix Endpoint Management console on the **Manage** tab and the **Settings** page. Unless otherwise indicated, the steps for the following tasks are provided in this article.

- Enrollment security mode and invitations
  - From **Settings > Enrollment**, configure up to seven enrollment security modes and send enrollment invitations. Each enrollment security mode has its own level of security and the number of steps users must take to enroll their devices.
- Roles for user accounts and groups
  - From **Settings > Role-Based Access Control**, assign predefined roles, or sets of permissions, to users and groups. These permissions control the level of access users have to system functions. For more information, see Configure roles with RBAC.
  - From **Settings > Notification Templates**, to create or update the notification templates to use in automated actions, enrollment, and standard notification messages sent to users. You configure the notification templates to send messages over two different channels: Citrix Secure Hub or SMTP. For more information, see: Creating and updating Notification Templates.
- User accounts and groups:
  - From **Manage > Users**, you can add local user accounts manually or use a .csv provisioning file to import the accounts and to manage local groups. However, most Citrix Endpoint Management deployments connect to LDAP for user and group information. You might prefer to create user accounts locally in use cases such as the following:
    - In environments, such as retail, where devices are shared rather than dedicated to individual users.
    - If you use an unsupported directory, such as Novell eDirectory.
  - From **Settings > Workflows**, use workflows to manage the creation and removal of user accounts.

About user accounts

An Citrix Endpoint Management user account is either for a local, Active Directory, or cloud user.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Cloud users:** A cloud user is a special user account that Citrix Cloud creates when an administrator is added to your Citrix Cloud customer account. A cloud user account uses the same user name as the administrator account on Citrix Cloud and defaults to the Admin role. The cloud user account provides a single sign-on and does other administrative functions.

  To add administrators to a Citrix Cloud account, see Invite new administrators.

For cloud users:

- You can change the roles and user properties of cloud users through the Citrix Cloud console. See Manage Citrix Cloud administrators.
- To change the password, see Administrators.
- To delete a cloud user, in Citrix Cloud, go to **Identity and access management > Administrators**. Click the ellipsis at the end of the user's row, and then select **Delete Administrator**.
- You cannot add cloud users to a local group.

Configure enrollment security modes

You configure a device enrollment security mode to specify a security level and notification template for device enrollment in Citrix Endpoint Management.

Citrix Endpoint Management offers six enrollment security modes, each with its own level of security and steps users must take to enroll their devices. You configure enrollment security modes in the Citrix Endpoint Management console from the **Manage > Enrollment Invitations** page. For information, see Enrollment invitations.

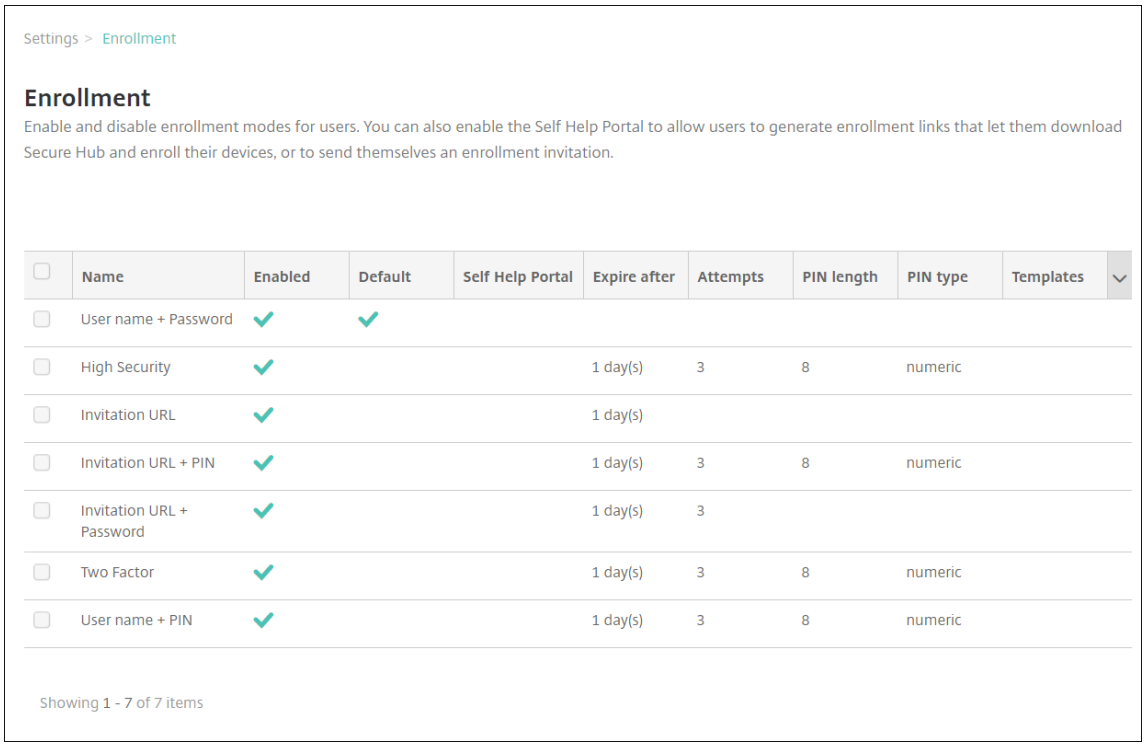
> **Note:**
>
> If you plan to use custom notification templates, you must set up the templates before you configure enrollment security modes. For more information about notification templates, see Creating or Updating Notification Templates.

1. On the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Click **Enrollment**. The **Enrollment** page appears. It has a table of all available enrollment security modes. By default, all enrollment security modes are enabled.
3. Select any enrollment security mode in the list to edit it. Then, set the mode as the default or disable the mode.

   Select the checkbox next to an enrollment security mode to view the options menu. Or, click anywhere else in the list to view the options menu on the right side of the listing.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Tip:**
>
> When you edit the enrollment security mode, you can specify an expiration deadline after which users cannot enroll their devices. For information, see To edit an enrollment security mode in this article. The value appears in the user and group enrollment invitation configuration pages.



You have the following enrollment security mode choices depending on your platform:

- User name + Password
- Invitation URL
- Invitation URL + PIN
- Invitation URL + Password
- Two Factors
- User name + PIN

For information about platform-specific enrollment security modes, see Enrollment security modes by platform.

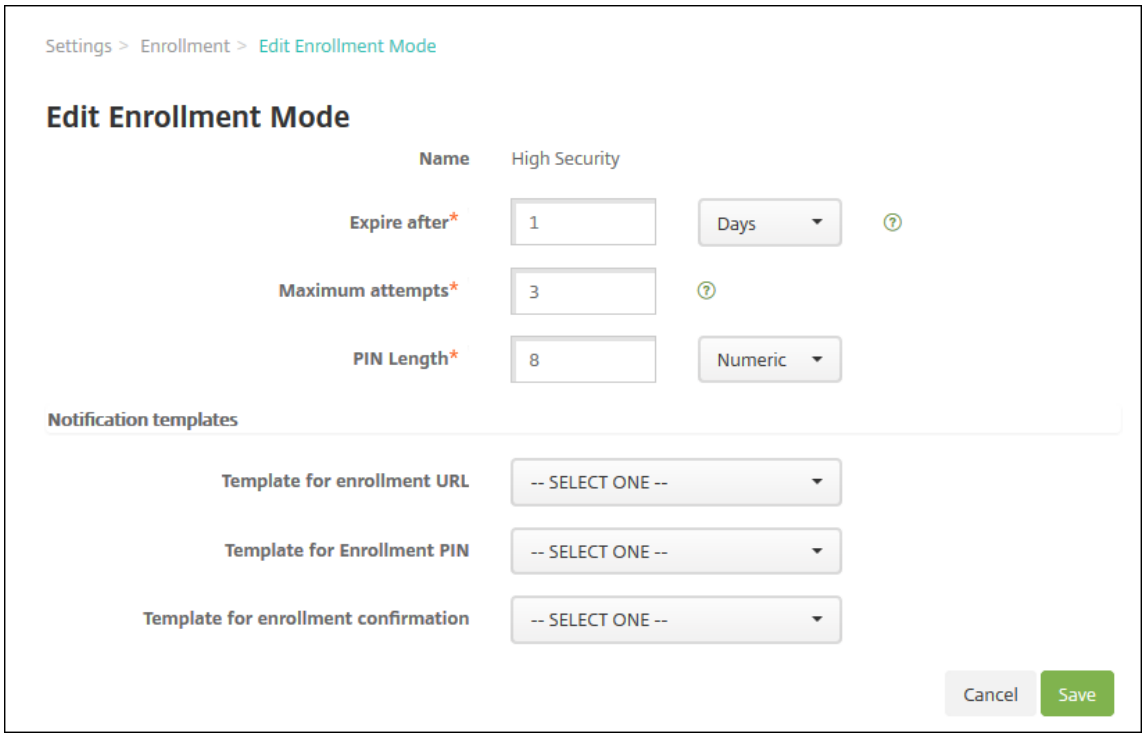
You can use enrollment invitations as an effective way to restrict the ability to enroll to specific users or groups. To send enrollment invitations, you can use only **Invitation URL**, **Invitation URL + PIN**, or **Invitation URL + Password** enrollment security modes. For devices enrolling with **User name + Password**, **Two-factor authentication**, or **User name + PIN**, users must manually enter their credentials in Citrix Secure Hub.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

You can use one-time PIN (sometimes also called OTP) enrollment invitations as a two-factor authentication solution. One-time PIN enrollment invitations control the number of devices a user can enroll. OTP invitations aren't available for Windows devices.

To edit an enrollment security mode

1. In the **Enrollment** list, select an enrollment security mode and then click **Edit**. The **Edit Enrollment Mode** page appears. Depending on the mode you select, you might see different options.



2. Change the following information as appropriate:

   - **Expire after:** Type an expiration deadline after which users cannot enroll their devices. This value appears in the user and group enrollment invitation configuration pages.

     Type **0** to prevent the invitation from expiring.

   - **Days:** Click **Days** or **Hours** in the drop-down list to correspond to the expiration deadline you entered in **Expire after**.

   - **Maximum attempts:** Type the number of attempts to enroll that a user can make before being locked out of the enrollment process. This value appears in the user and group enrollment invitation configuration pages.

     Type **0** to allow unlimited attempts.

   - **PIN length:** Type a numeral to set the length of the generated PIN.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Numeric:** Click **Numeric** or **Alphanumeric** in the drop-down list for the PIN type.
- **Notification templates:**
  - **Template for enrollment URL:** Click a template in the drop-down list to use for the enrollment URL. For example, the Enrollment invitation template sends users an email. For more information on notification templates, see Create or update notification templates.
  - **Template for enrollment PIN:** Click a template in the drop-down list to use for the enrollment PIN.
  - **Template for enrollment confirmation:** Click a template in the drop-down list to use to inform a user that they enrolled successfully.

3. Click **Save**.

To set an enrollment security mode as default

The default enrollment security mode is used for all device enrollment requests unless you select a different enrollment security mode. If no enrollment security mode is set as the default, you must create an enrollment request for each device enrollment.

1. If the enrollment security mode that you want to use as a default isn't enabled, select it and click **Enable**. The only enrollment security modes that you can use as a default are **User name + Password**, **Two Factor**, or **User name + PIN**.
2. Select the enrollment security mode and click **Default**. The selected mode is now the default. If any other enrollment security mode was set as the default, the mode is no longer the default.

To disable an enrollment security mode

Disabling an enrollment security mode makes it unavailable for use, both for group enrollment invitations and on the Self-Help Portal. You might change how you allow users to enroll their devices by disabling one enrollment security mode and enabling another.

1. Select an enrollment security mode.

   You cannot disable the default enrollment security mode. If you want to disable the default enrollment security mode, you must first remove its default status.

2. Click **Disable**. The enrollment security mode is no longer enabled.

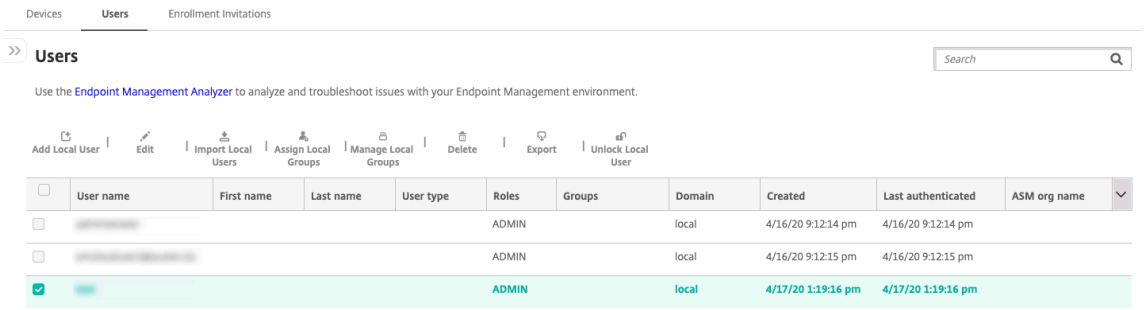
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Add, edit, unlock, or delete local user accounts

You can add local user accounts to Citrix Endpoint Management manually or you can use a provisioning file to import the accounts. For the steps to import user accounts from a provisioning file, see Import user accounts.

All Citrix Cloud administrators get created as Citrix Endpoint Management administrators. If you create a Citrix Cloud administrator with custom access, make sure that access includes Citrix Endpoint Management. For information on adding Citrix Cloud administrators, see Add administrators.

1. In the Citrix Endpoint Management console, click **Manage > Users**. The **Users** page appears.

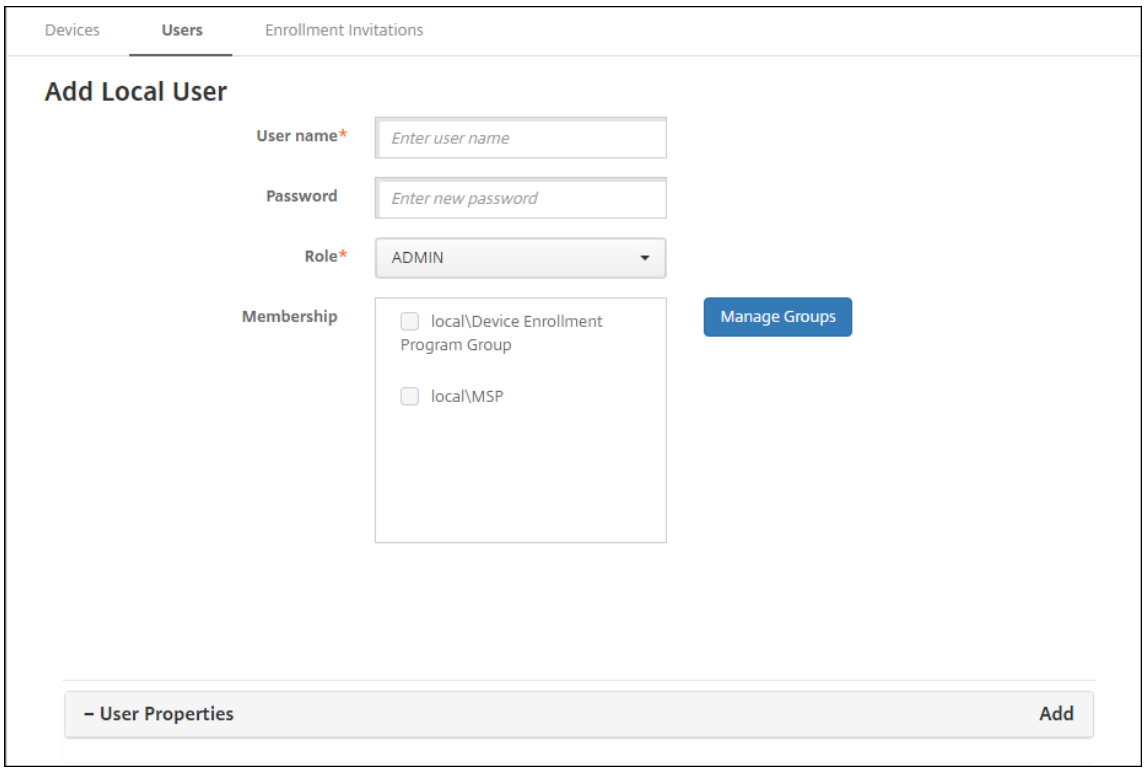


2. Click **Show filter** to filter the list.

To add a local user account

1. On the **Users** page, click **Add Local User**. The **Add Local User** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. Configure these settings:

   - **User name:** Type the name, a required field. You can include the following in names: spaces, uppercase letters, and lowercase letters.
   - **Password:** Type an optional user password. The password must be at least 14 characters long and meet all the following criteria:
     - Include at least two numbers
     - Include at least one uppercase and one lowercase letter
     - Include at least one special character
     - Don't include dictionary words or restricted words, such as your Citrix® user name or email address
     - Don't include more than three sequential and repeating characters or keyboard patterns, such as 1111, 1234, or asdf
   - **Role:** Click the user role in the drop-down list. For more information about roles, see Configure roles with RBAC. Possible options are:
     - ADMIN
     - DEVICE_PROVISIONING
     - SUPPORT
     - USER
   - **Membership:** Click the group or groups in the drop-down list to which to add the user.
   - **User Properties:** Add optional user properties. For each user property you want to add, click **Add** and do the following:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **User Properties:** Click a property in the drop-down list and then type the user property attribute in the field next to the property.
- Click **Done** to save the user property or click **Cancel**.

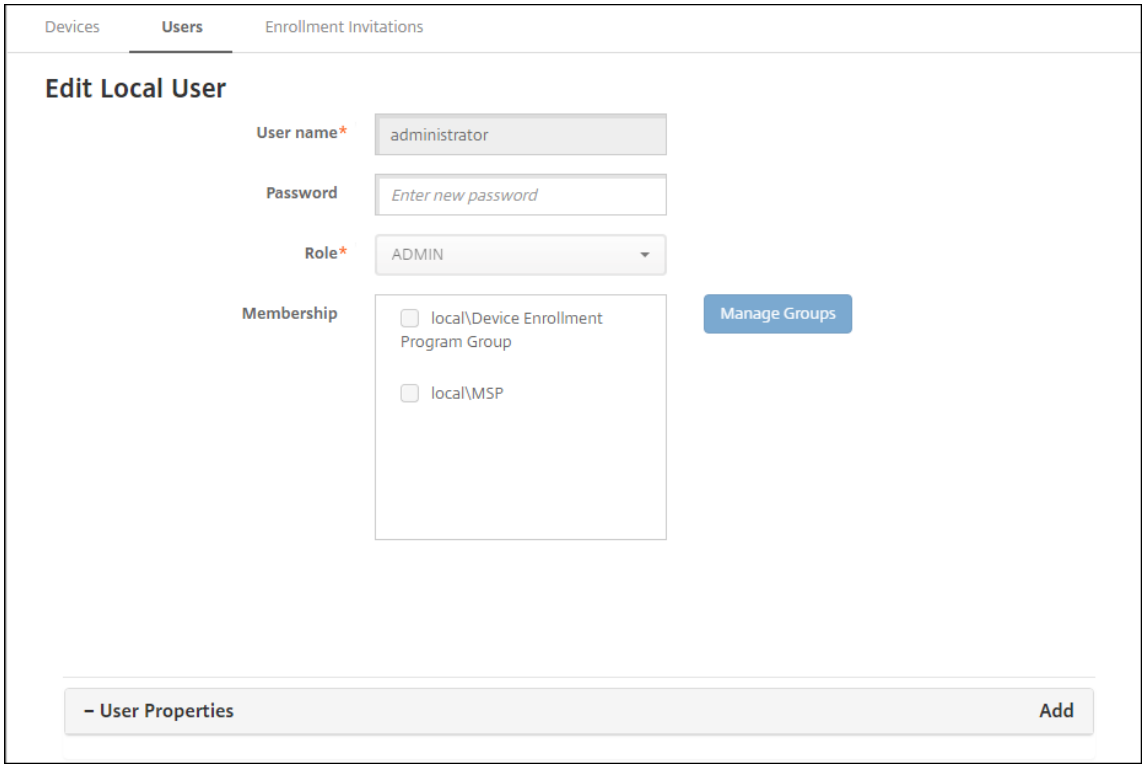
To delete an existing user property, hover over the line that has the property and then click the **X** on the right side. The property is deleted immediately.

To edit an existing user property, click the property and make changes. Click **Done** to save the changed listing or **Cancel** to leave the listing unchanged.

3. Click **Save**. After you create a user, the **User type** field for a local user account stays empty.

To edit a local user account

1. On the **Users** page, in the list of users, click to select a user and then click **Edit**. The **Edit Local User** page appears.



2. Change the following information as appropriate:

- **User name:** You cannot change the user name.
- **Password:** Change or add a user password.
- **Role:** Click the user role in the drop-down list.
- **Membership:** Click the group or groups in the drop-down list to which to add or edit the user account. To remove the user account from a group, clear the checkbox next to the group name.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **User properties:** Do one of the following:
  - For each user property you want to change, click the property and make changes. Click **Done** to save the changed listing or **Cancel** to leave the listing unchanged.
  - For each user property you want to add, click **Add** and do the following:
    * **User Properties:** Click a property in the drop-down list and then type the user property attribute in the field next to the property.
    * Click **Done** to save the user property or click **Cancel**.
  - For each existing user property you want to delete, hover over the line that has the property and then click the **X** on the right side. The property is deleted immediately.

3. Click **Save** to save your changes or click **Cancel** to leave the user unchanged.

To unlock a local user account

A local user account gets locked according to these server properties:

- `local.user.account.lockout.time`
- `local.user.account.lockout.limit`

  For more information, see Server Property Definitions.

When a local user account gets locked, you can unlock the account from the Citrix Endpoint Management console.

1. On the **Users** page, in the list of user accounts, click to select a user account.
2. Click **Unlock User**. A confirmation dialog box appears.
3. Click **Unlock** to unlock the user account or click **Cancel** to leave the user unchanged.

You can't open an Active Directory user from the Citrix Endpoint Management console. A locked Active Directory user must contact their Active Directory help desk for a password reset.

To delete a local user account

1. On the **Users** page, in the list of user accounts, click to select a user account.

   You can select more than one user account to delete by selecting the checkbox next to each user account.
2. Click **Delete**. A confirmation dialog box appears.
3. Click **Delete** to delete the user account or click **Cancel**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To delete Active Directory users

To delete one or more Active Directory users at a time, select the users and click **Delete**.

If a user that you delete has enrolled devices and you want to re-enroll those devices, delete the devices before re-enrolling them. To delete a device, go to **Manage > Devices**, select the device, and then click **Delete**.

Import user accounts

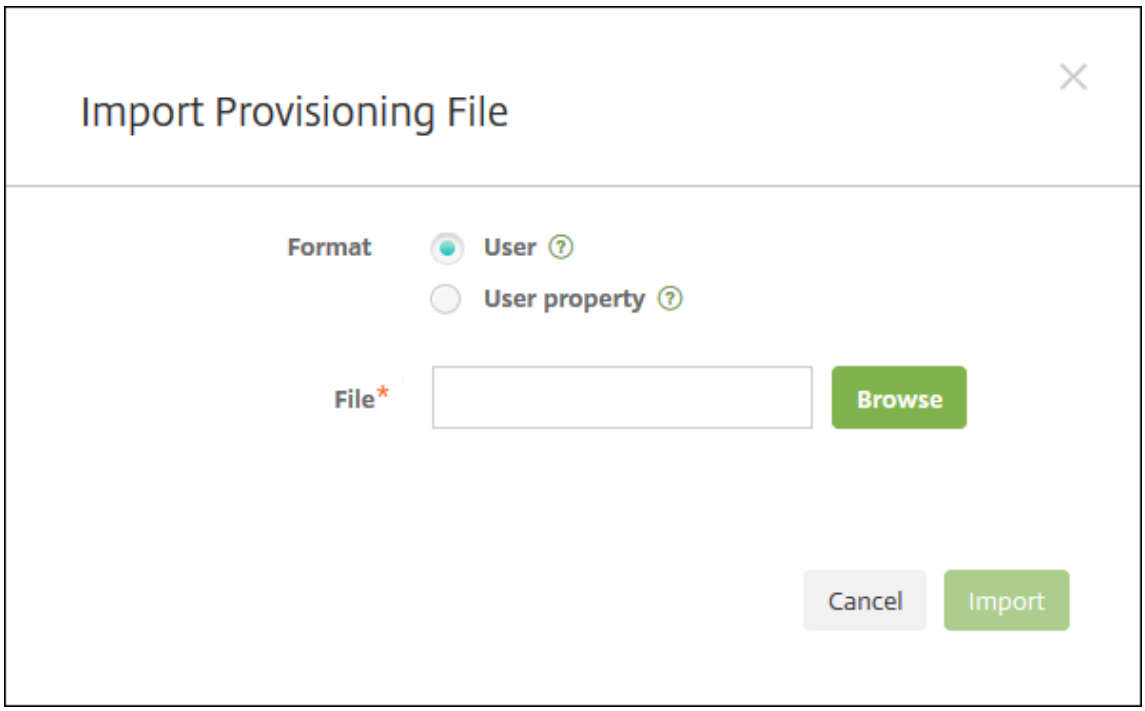
You can import local user accounts and properties from a .csv file called a provisioning file, which you can create manually. For more information about formatting provisioning files, see Provisioning file formats.

> **Note:**
>
> - For local users, use the domain name along with the user name in the import file. For example, specify `username@domain`. If the local user that you create or import is for a managed domain in Citrix Endpoint Management, the user cannot enroll by using the corresponding LDAP credentials.
> - If importing user accounts to the Citrix Endpoint Management internal user directory, disable the default domain to speed up the import process. Keep in mind that disabling the domain affects enrollments. Reenable the default domain after the import of internal users is complete.
> - Local users can be in User Principal Name (UPN) format. However, Citrix recommends that you do not use the managed domain. For example, if example.com is managed, do not create a local user with this UPN format: user@example.com.

After you prepare a provisioning file, follow these steps to import the file to Citrix Endpoint Management.

1. In the Citrix Endpoint Management console, click **Manage > Users**. The **Users** page appears.
2. Click **Import Local Users**. The **Import Provisioning File** dialog box appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Select either **User** or **Property** for the format of the provisioning file that you are importing.
4. Select the provisioning file to use by clicking **Browse** and then navigating to the file location.
5. Click **Import**.

Provisioning file formats

You can create a provisioning file and use it to import user accounts and properties to Citrix Endpoint Management. Use one of the following formats for a provisioning file:

- **User provisioning file fields:** `user;password;role;group1;group2`
- **User attribute provisioning file fields:** `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

> **Note:**
>
> - Separate the fields within the provisioning file with a semi-colon (;). If part of a field has a semi-colon, escape it with a backslash character (). For example, type the property **propertyV; test;1;2** as **propertyV\;test\;1\;2** in the provisioning file.
> - Valid values for **Role** are the predefined roles USER, ADMIN, SUPPORT, and DEVICE_PROVISIONING, plus any other roles that you defined.
> - Use the period character (.) as a separator to create a group hierarchy. Don't use a period in group names.
> - Use lowercase for property attributes in attribute provisioning files. The database is case

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> sensitive.

Example of user provisioning content The entry `user01;pwd\\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` means:

- **User:** user01
- **Password:** pwd; 01
- **Role:** USER
- **Groups:**
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

As another example, `AUser0;1.password;USER;ActiveDirectory.test.net` means:

- **User:** AUser0
- **Password:** 1.password
- **Role:** USER
- **Group:** ActiveDirectory.test.net

Example of user attribute provisioning content The entry `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` means:

- **User:** user01
- **Property 1**
  - **name:** propertyN
  - **value:** propertyV;test;1;2
- **Property 2:**
  - **name:** prop 2
  - **value:** prop2 value

Add or remove groups

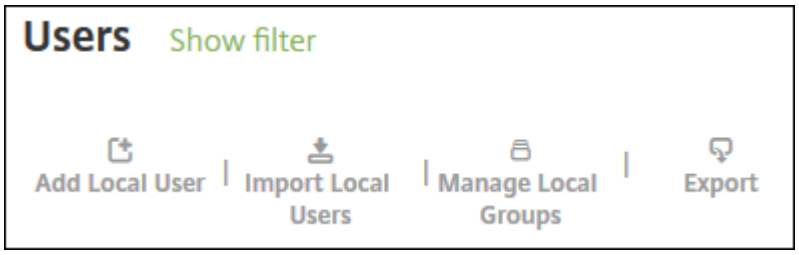
You manage groups in the **Manage Groups** dialog box in the Citrix Endpoint Management console on these pages: **Users**, **Add Local User**, or **Edit Local User**. There is no group edit command.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

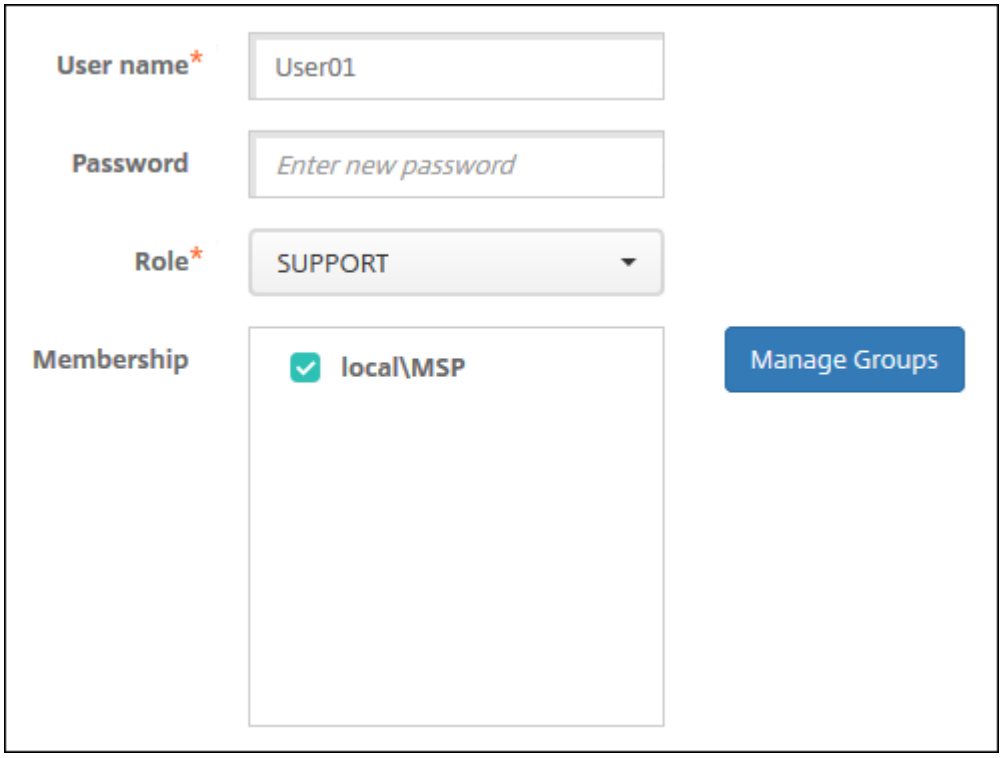
To add a local group

1. Do one of the following:

   - On the **Users** page, click **Manage Local Groups**.

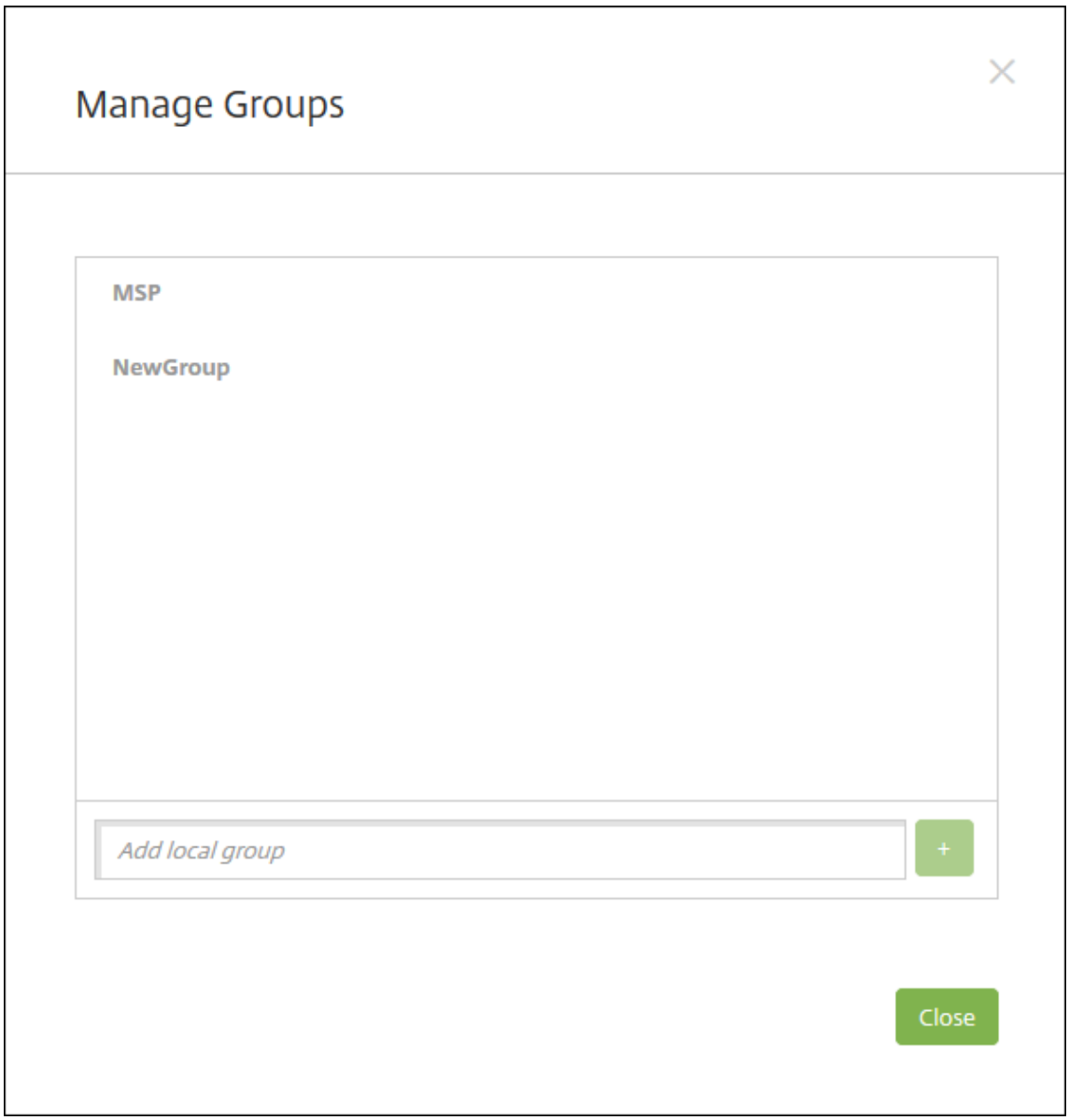


   - On either the **Add Local User** page or the **Edit Local User** page, click **Manage Groups**.



   The **Manage Group** dialog box appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. Below the group list, type a new group name and then click the plus sign (**+**). The user group is added to the list.
3. Click **Close**.

To remove a group

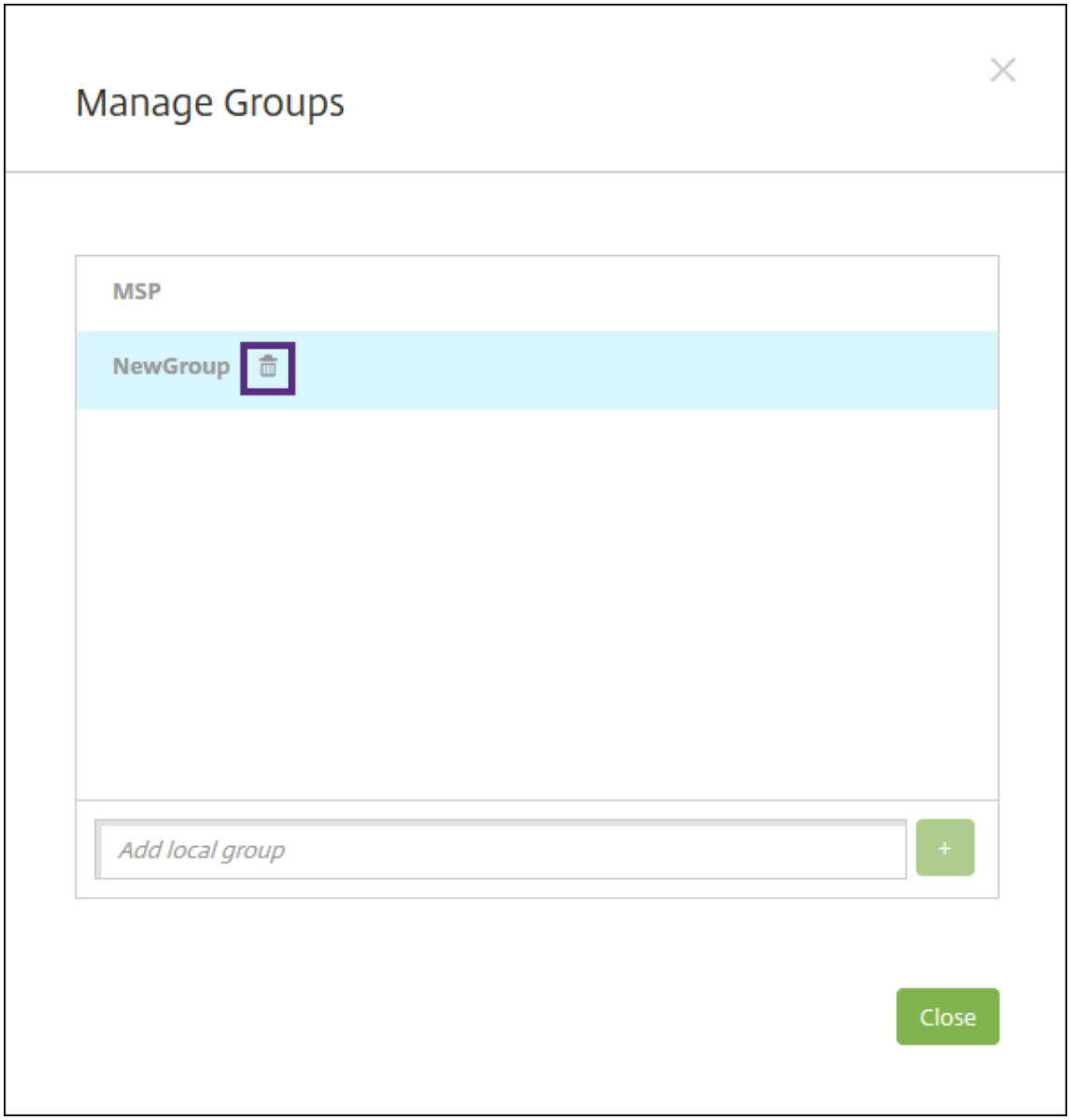
Removing a group has no effect on user accounts. Instead, removing a group only removes the user association with that group. Users also lose access to apps or profiles provided by the Delivery Groups that are associated with that group. But, any other group associations stay intact. If users aren't associated with any other local groups, they are associated at the top level.

1. Do one of the following:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- On the **Users** page, click **Manage Local Groups**.
- On either the **Add Local User** page or the **Edit Local User** page, click **Manage Groups**.

The **Manage Groups** dialog box appears.



2. On the **Manage Groups** dialog box, click the group you want to delete.
3. Click the trash can icon to the right of the group name. A confirmation dialog box appears.
4. Click **Delete** to confirm the operation and remove the group.

> **Important:**
>
> You cannot undo this operation.

5. On the **Manage Groups** dialog box, click **Close**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Create and manage workflows

You can use workflows to manage the creation and removal of user accounts. Before you create a workflow, identify individuals in your organization who have the authority to approve user account requests. Then, use the workflow template to create and approve user account requests.

When you set up Citrix Endpoint Management for the first time, you configure workflow email settings, which must be set before you can use workflows. You can change workflow email settings at any time. These settings include the email server, port, email address, and whether the request to create the user account requires approval.

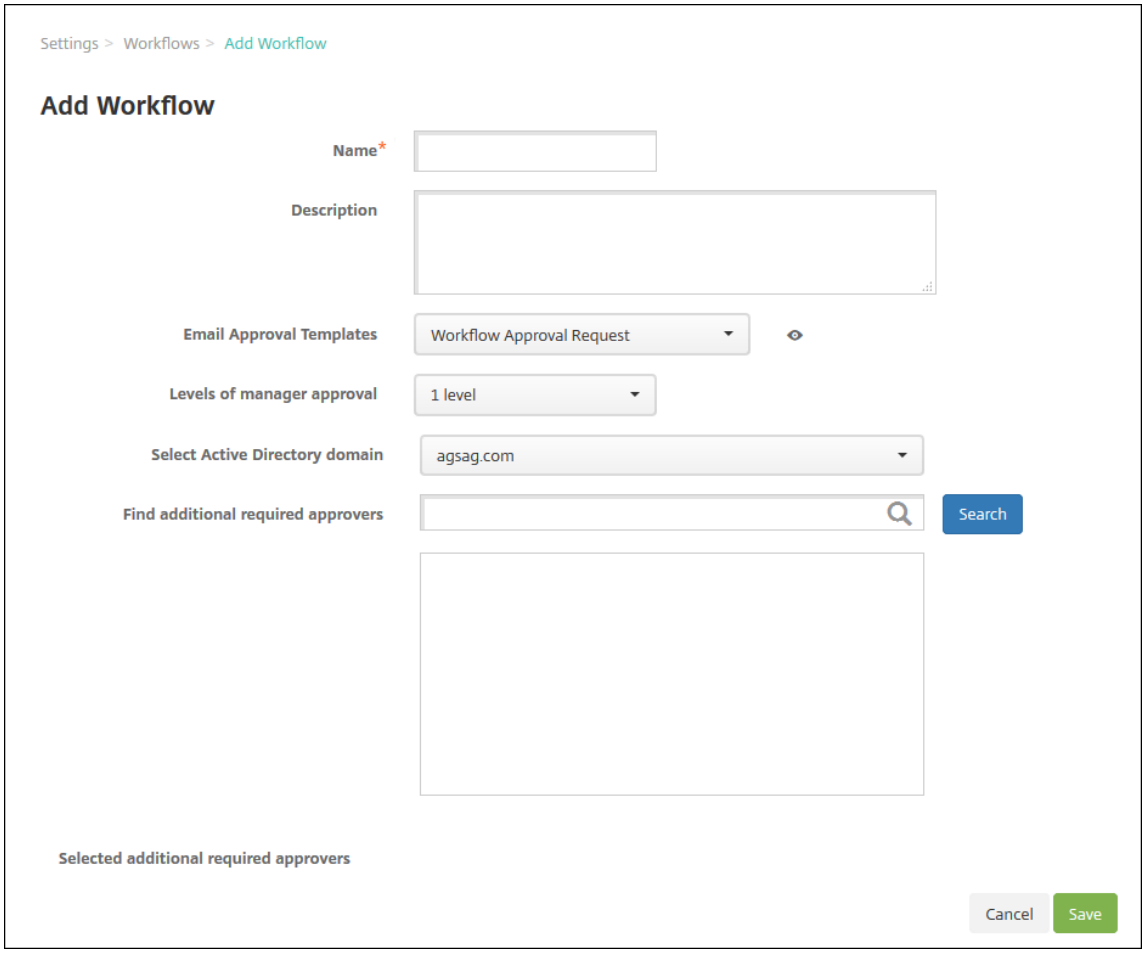
You can configure workflows in two places in Citrix Endpoint Management:

- In the **Settings > Workflows** page in the Citrix Endpoint Management console. On the **Workflows** page, you can configure multiple workflows for use with app configurations. When you configure workflows on the Workflows page, you can select the workflow when you configure the app.
- When you configure an application connector in the app, provide a workflow name and then configure the individuals to approve the user account request. See Add apps.

You can assign up to three levels for manager approval of user accounts. If you need other persons to approve the user account, you can search for and select them by using their name or email address. When Citrix Endpoint Management finds the person, you then add them to the workflow. All individuals in the workflow receive emails to approve or deny the new user account.

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Click **Workflows**. The **Workflows** page appears.
3. Click **Add**. The **Add Workflow** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Configure these settings:

   - **Name:** Type a unique name for the workflow.
   - **Description:** Optionally, type a description for the workflow.
   - **Email Approval Templates:** In the list, select the email approval template to be assigned. You create email templates in the **Notification Templates** section under **Settings** in the Citrix Endpoint Management console. When you click the eye icon to the right of this field, you see a preview of the template you are configuring.
   - **Levels of manager approval:** In the list, select the number of levels of manager approval required for this workflow. The default is **1 level**. Possible options are:
     - Not Needed
     - 1 level
     - 2 levels
     - 3 levels
   - **Select Active Directory domain:** In the list, select the appropriate Active Directory domain to be used for the workflow.
   - **Find additional required approvers:** Type a name in the search field and then click

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Search. Names originate in the Active Directory.

- When the name appears in the field, select the checkbox next to the name. The name and email address appear in the **Selected additional required approvers** list.
  - To remove a name from the list, do one of the following:
    - Click **Search** to see a list of everyone in the selected domain.
    - Type a full or partial name in the search box, and then click **Search** to limit the search results.
    - Persons in the **Selected additional required approvers** list have check marks next to their name in the search results list. Scroll through the list and clear the checkbox next to each name that you want to remove.

5. Click **Save**. The created workflow appears on the **Workflows** page.

After you create the workflow, you can view the workflow details, view the apps associated with the workflow, or delete the workflow. You cannot edit a workflow after you create the workflow. If you need a workflow with different approval levels or approvers, create another workflow.

To view details and delete a workflow

1. On the **Workflows** page, in the list of existing workflows, select a specific workflow. To do that, click the row in the table or select the checkbox next to the workflow.
2. To delete a workflow, click **Delete**. A confirmation dialog box appears. Click **Delete** again.

> **Important:**
>
> You cannot undo this operation.

Enrollment profiles

September 6, 2025

An enrollment profile specifies the following:

- Device management enrollment options for Android, iOS, and Windows devices.
- App management enrollment options for Android and iOS devices.
- Other enrollment options:
  - Whether to limit the number of devices a user can enroll.

    If the device limit is reached, an error message lets the user know that they exceeded the device registration limit.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - Whether to allow a user to decline device management.

You can use enrollment profiles to combine multiple use cases and device migration paths within a single Citrix Endpoint Management console. Some use cases include:

- Mobile Device Management (MDM only)
- MDM+Mobile Application Management (MAM)
- MAM only
- Corporate-owned enrollments
- BYOD enrollment (the ability to opt out of MDM enrollment)
- Migration of Android Device Administrator enrollments to Android Enterprise enrollments (fully managed, work profile, dedicated device)
- Automatic enrollment of Windows 10 and Windows 11 devices through Citrix Workspace app for Windows (preview)

If your current site is MDM only and you want to add MAM, you must configure a NetScaler Gateway. For more information, see NetScaler Gateway requirements.

When you create a delivery group, you can use the default enrollment profile named Global or specify a different enrollment profile.

Enrollment profile features by platform include the following.

- **For Android devices:** You specify the management and device owner mode. For example: Company-owned device, fully managed with work profile, and BYOD work profile.

  New devices enroll in Android Enterprise by default. You can opt to manage the devices using legacy Android device administrator (DA) mode. New devices also enroll in app management by default.

  For information about specifying the level of security and required enrollment steps, see User accounts, roles, and enrollment.

- **For iOS devices:** You specify the device management type: **Apple User Enrollment**, **Apple Device enrollment**, or **Do not manage devices**. This **Apple User Enrollment** mode is available as a public preview. To enable this feature, contact your support team.

  If you select Apple User Enrollment, you can choose to use a custom domain for Managed Apple IDs and configure that domain.

  New devices enroll in Apple device management by default. New devices also enroll in app management by default.

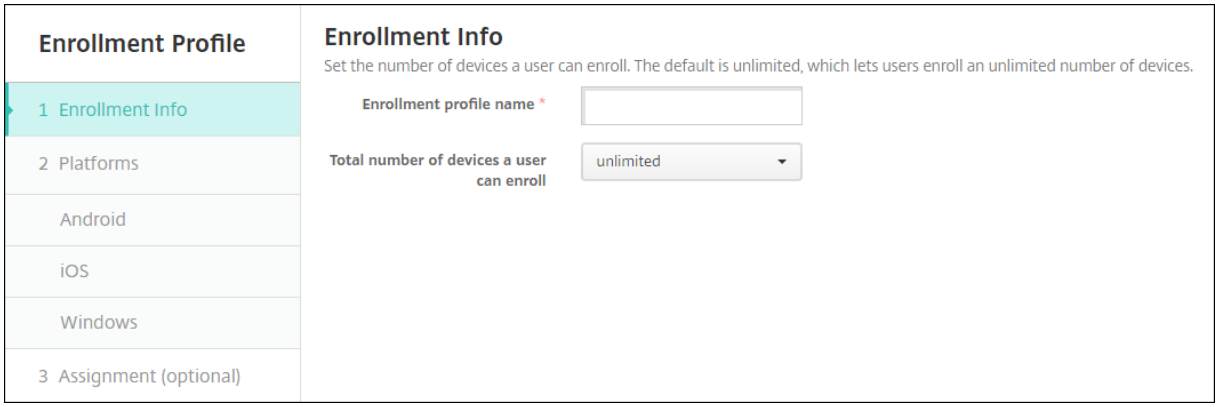
- **For Windows 10 and Windows 11 devices:** You specify whether to use Citrix® device management for Windows. New devices enroll in device management by default.

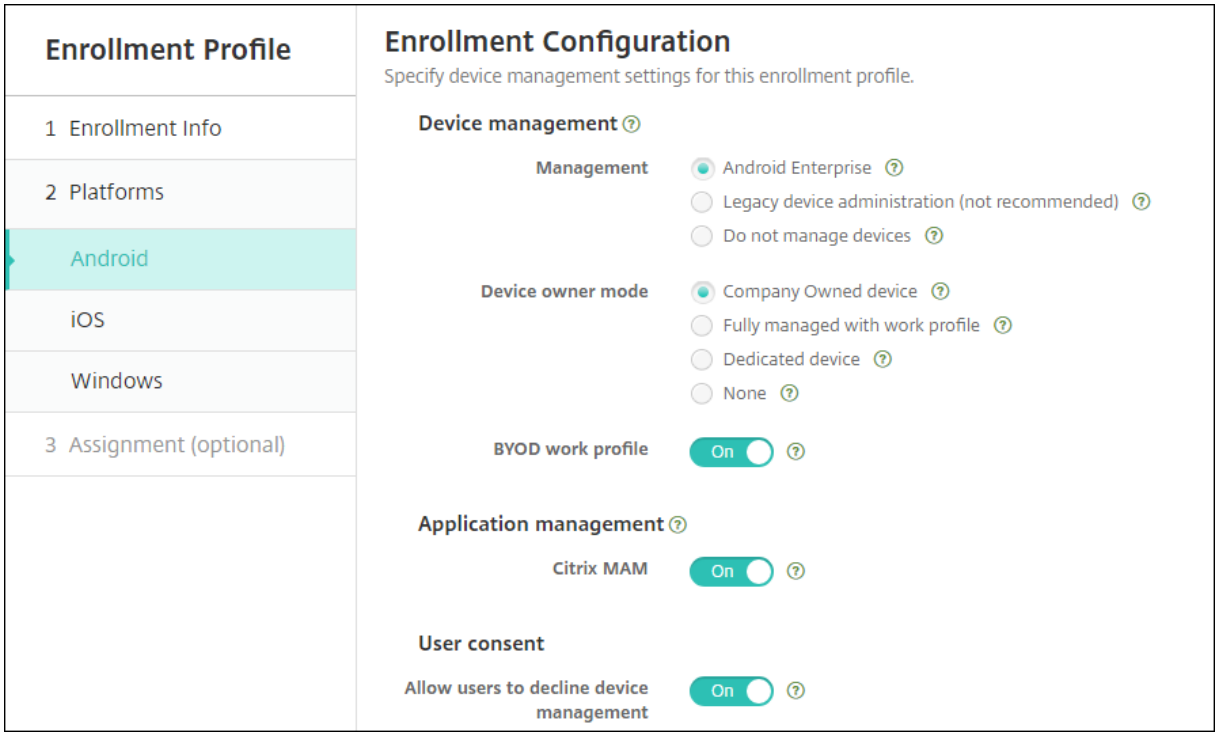
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Global enrollment profile

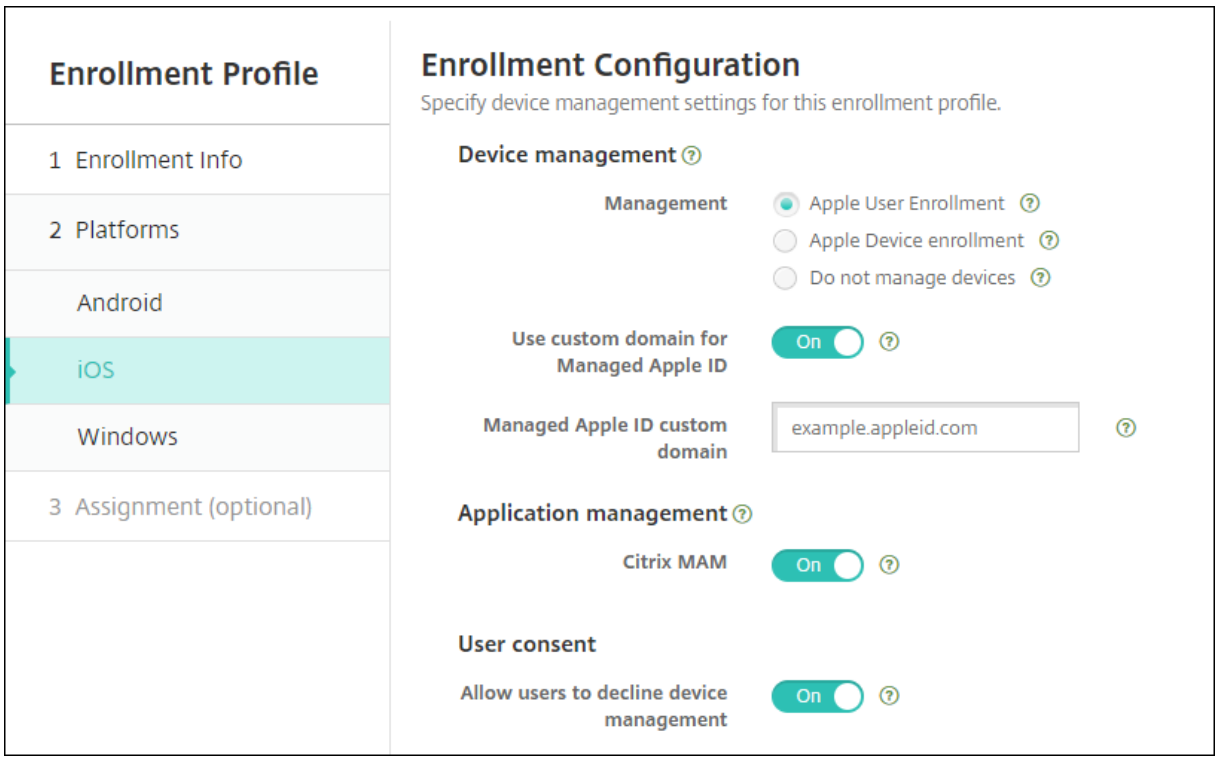
The default enrollment profile is named Global. The Global profile is useful for testing until you have a chance to create enrollment profiles.

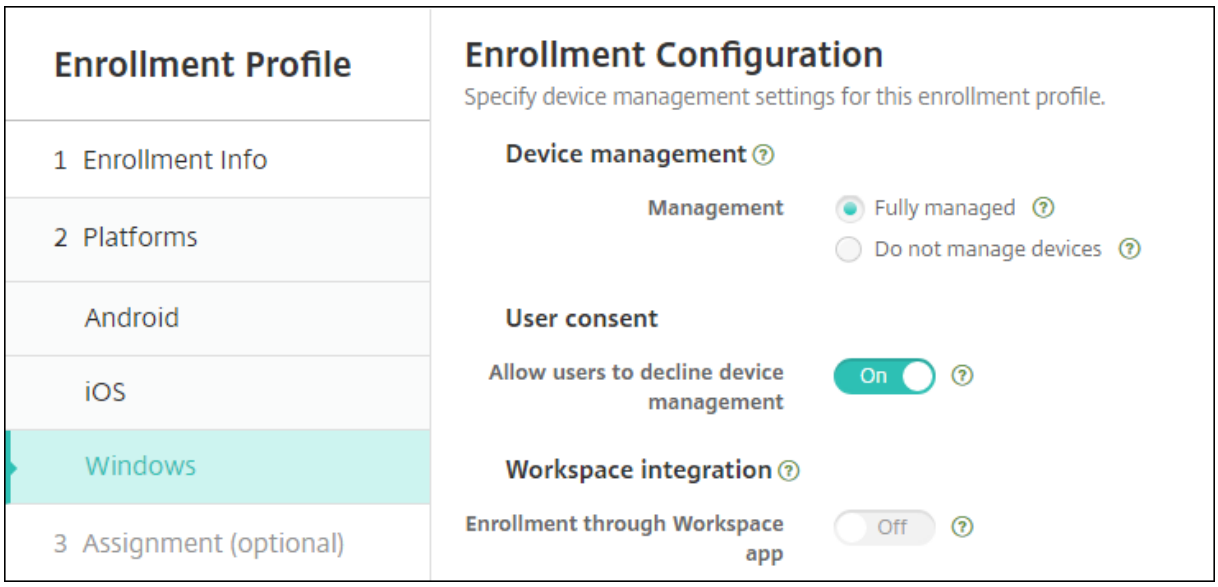
If you onboard to Citrix Endpoint Management 20.2.1 or later, the Global enrollment profile has predefined settings. The following screenshots show the default settings for the Global enrollment profile. MAM only deployments display a subset of these options.





© 1997–2025 Citrix Systems, Inc. All rights reserved.





Enrollment profiles, delivery groups, and enrollment

Enrollment profiles and delivery groups interact as follows:

- You can attach an enrollment profile to one or more delivery groups.
- If a user belongs to multiple delivery groups that have different enrollment profiles, the name of the delivery group determines the enrollment profile used. Citrix Endpoint Management selects

© 1997–2025 Citrix Systems, Inc. All rights reserved.

the delivery group that appears last in an alphabetized list of delivery groups. For example, suppose that you have the following:

- Two enrollment profiles, named "EP1"and "EP2".
- Two delivery groups, named "DG1"and "DG2".
- "DG1"is associated with "EP1".
- "DG2"is associated with "EP2".

If the enrolling user is in both the "DG1"and "DG2"delivery groups, Citrix Endpoint Management uses the "EP2"enrollment profile to determine the enrollment type for the user.

- The deployment order applies only to devices in a delivery group that has an enrollment profile configured for MDM (device management).
- After a device enrolls, some changes to an enrollment profile require re-enrollment:
  - Changing the configuration to downgrade a device from MDM+MAM to MAM or MDM enrollment. A downgrade might occur when you update an enrollment profile or move a device to a different delivery group.
  - Adding MAM to an enrollment profile that's configured for MDM.
  - Adding MDM to an enrollment profile that's configured for MAM.
- Switching to a different enrollment profile does not affect existing enrolled devices. However, users must unenroll and then reenroll those devices for the changes to take effect.

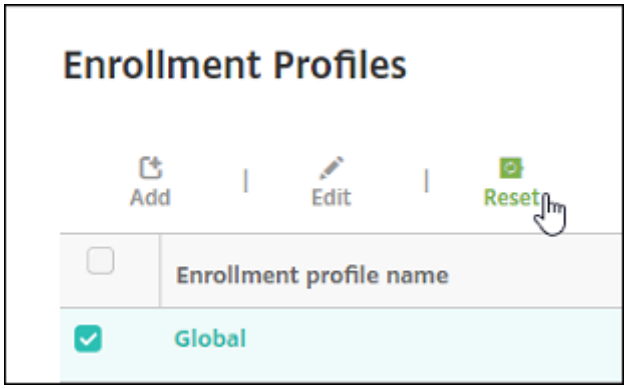
To create an enrollment profile

1. In the Citrix Endpoint Management console, go to **Configure > Enrollment Profiles**.
2. On the **Enrollment Info** page, type a descriptive name for the profile. By default, a user can enroll unlimited devices. Select a value to limit the number of devices per user. The limit applies to the sum of MAM or MDM managed Android, iOS, and Windows devices that a user enrolls.
3. Complete the platform pages. For information about enrollment settings specific to the platforms, see:
   - Android Enterprise: Creating enrollment profiles
   - iOS: Supported enrollment methods
   - Windows Desktop and Tablet: Supported enrollment methods
4. On the **Assignments** page, attach one or more delivery groups to the enrollment profile.

   A user might belong to multiple delivery groups that have different enrollment profiles. In that case, the name of the delivery group determines the enrollment profile used. Citrix Endpoint Management selects the delivery group that appears last in an alphabetized list of delivery groups. To create delivery groups, go to **Configure > Delivery Groups**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

A list of your enrollment profiles appears on the **Configure > Enrollment Profiles** page. To edit the Global profile or reset it to the original default, select the row for the Global profile and click **Reset**. You can't delete the Global profile.



Notifications

September 6, 2025

You can use notifications in Citrix Endpoint Management for the following purposes:

- To communicate with select groups of users for several system-related functions. You can also target these notifications for certain users. For example, all users with iOS devices, users whose devices are out of compliance, users with employee-owned devices, and so on.
- To enroll users and their devices
- To automatically notify users (using automated actions) when certain conditions are met. For example:
  - When a user device is about to be blocked from the corporate domain because of a compliance issue
  - When a device has been jailbroken or rooted

For details about automated actions, see Automated Actions.

To send notifications with Citrix Endpoint Management, you must configure a gateway and a notification server. You can set up a notification server in Citrix Endpoint Management to configure SMTP servers. Those servers send email notifications to users. You can use notifications to send messages over SMTP.

- SMTP is a connection-oriented, text-based protocol in which a mail sender communicates with a mail receiver. The mail sender issues command strings and supplies necessary data, typically over a TCP connection. SMTP sessions consist of commands originated by an SMTP client (the person sending the message) and corresponding responses from the SMTP server.

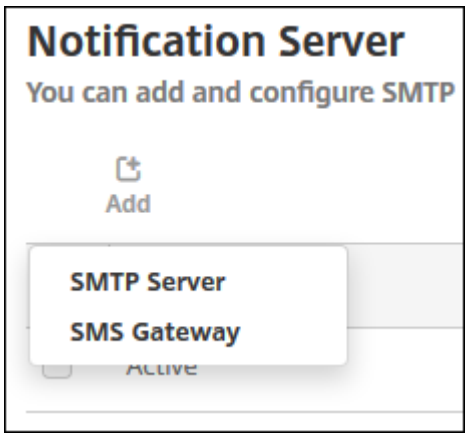
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Prerequisites

- Configure the SMTP notifications server to send messages to users. If the server is hosted on an internal server, contact your system administrator for configuration information. If the server is a hosted email service, locate the appropriate configuration information on the website of the service provider.
- You can only use one active SMTP server. This communication channel allows only one active configuration.
- Open port 25 from Citrix Endpoint Management in your network DMZ to point back to the SMTP server on your internal network. That enables Citrix Endpoint Management to send notifications successfully.

Configure an SMTP server

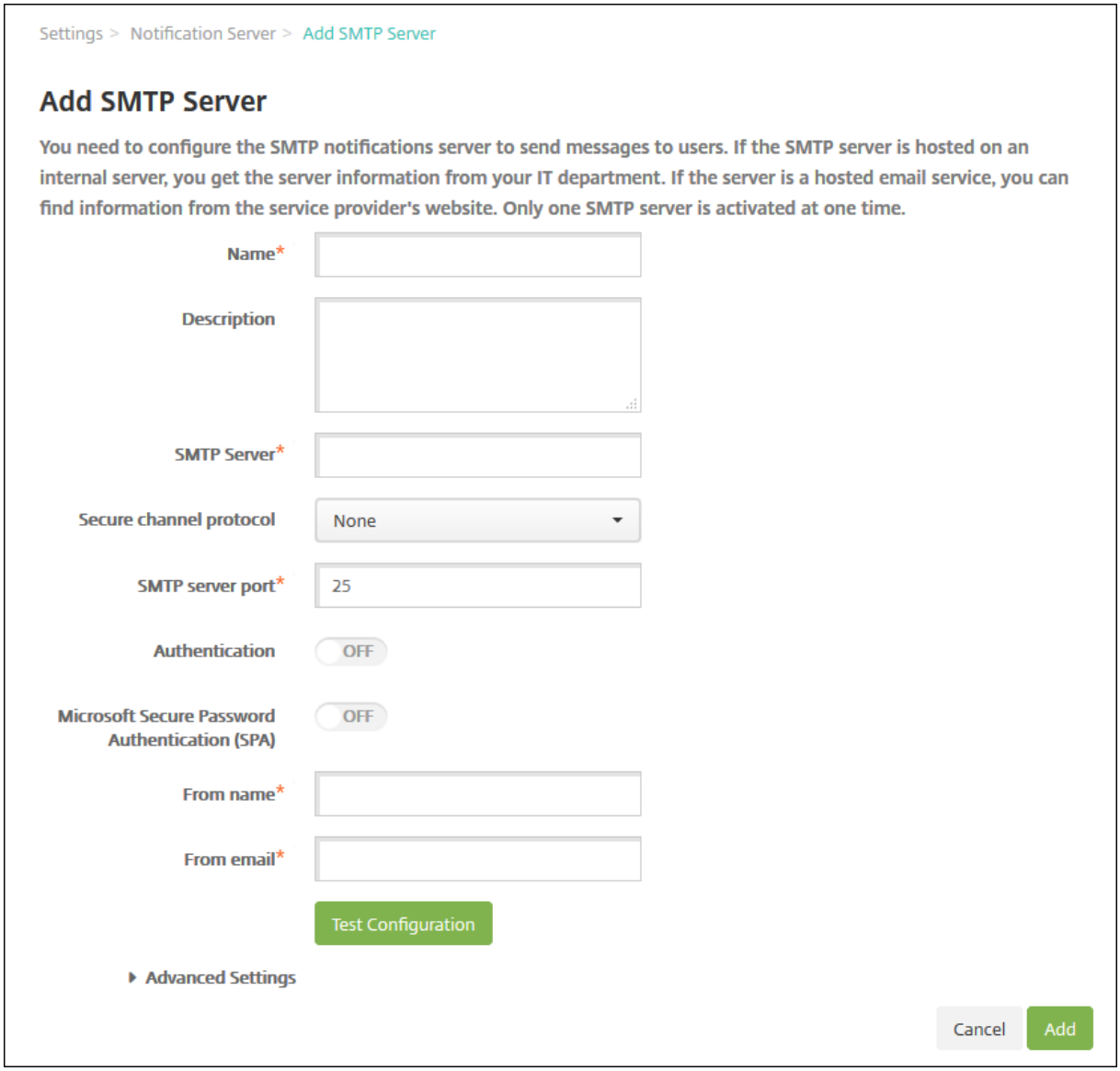
1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Under **Notifications**, click **Notification Server**. The **Notification Server** page appears.
3. Click **Add**. A menu appears with options to configure an SMTP server.



   - To add an SMTP server, click **SMTP Server** and then see Add an SMTP server for the steps to configure this setting.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Add an SMTP server



1. Configure these settings:

   - **Name:** Type the name associated with this SMTP server account.
   - **Description:** Optionally, enter a description of the server.
   - **SMTP Server:** Type the host name for the server. Specify either a fully qualified domain name (FQDN) or an IP address.
   - **Secure channel protocol:** Click **SSL**, **TLS**, or **None** in the drop-down list for the secure channel protocol used by the server (if the server is configured to use secure authentication). The default is **None**.
   - **SMTP server port:** Type the port used by the SMTP server. By default, the port is set to 25. If SMTP connections use the SSL secure channel protocol, set the port to 465.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Authentication:** Select **On** or **Off**. The default is **Off**.
- If you enable **Authentication**, configure these settings:
  - **User name:** Type the user name for authentication
  - **Password:** Type the authentication user's password.
- **Microsoft Secure Password Authentication (SPA):** If the SMTP server is using the SPA, click **On**. The default is **Off**.
- **From Name:** Type the name displayed in the **From** box when a client receives a notification email from this server. For example, Corporate IT.
- **From email:** Type the email address used if an email recipient replies to the notification sent by the SMTP server.

2. Click **Test Configuration** to send a test email notification.
3. Expand **Advanced Settings** and then configure these settings:

   - **Number of SMTP retries:** Type the number of times to retry a failed message sent from the SMTP server. The default is 5.
   - **SMTP Timeout:** Type the duration to wait (in seconds) when sending an SMTP request. Increase this value if message sending continuously fails because of timeouts. Use caution when decreasing this value, to avoid increasing the number of timed out and undelivered messages. The default is 30 seconds.
   - **Maximum number of SMTP recipients:** Type the maximum number of recipients per email message sent by the SMTP server. The default is 100.

4. Click **Add**.

Create and update notification templates

You can create or update notification templates in Citrix Endpoint Management to be used in automated actions, enrollment, and standard notification messages sent to users. You configure the notification templates to send messages over two different channels: Citrix Secure Hub or SMTP.

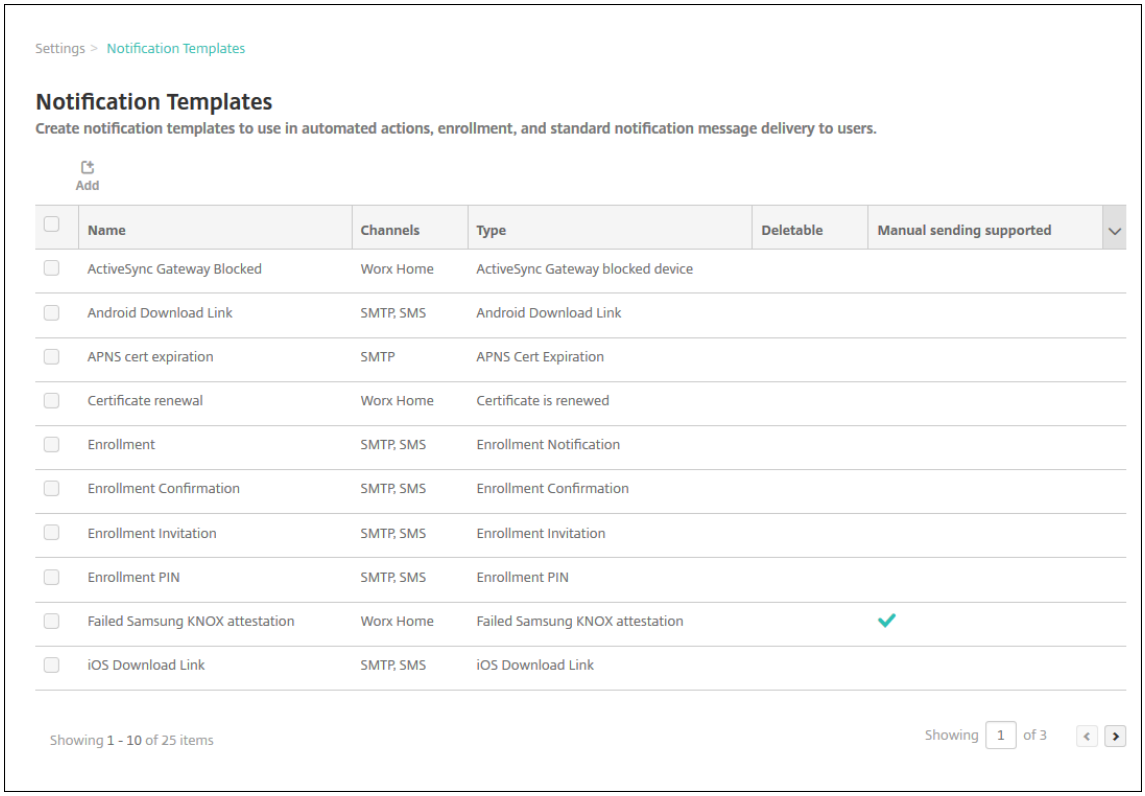
Citrix Endpoint Management includes many predefined notification templates. The templates reflect the distinct types of events that Citrix Endpoint Management automatically responds to for every device in the system.

> **Note:**
>
> If you plan to use SMTP channels to send notifications to users, you must set up the channels before you can activate them. Citrix Endpoint Management prompts you to set up the channels when you add notification templates if they aren't already set up.

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Click **Notification Templates**. The **Notification Templates** page appears.



Add a notification template

1. Click **Add**. If no SMTP server is set up, a message about the use of SMTP notifications appears. You can choose to set up the SMTP servers now or set them up later.

   If you choose to set up SMTP server settings now, you're redirected to the **Notification Server** page on the **Settings** page. After setting up the channels you want to use, you can return to the **Notification Template** page to continue adding or modifying notification templates.

   > **Important:**
   >
   > If you choose to set up SMTP server settings later, you can't activate those channels when you add or edit a notification template. As a result, those channels aren't available for sending user notifications.

2. Configure these settings:

   - **Name:** Type a descriptive name for the template.
   - **Description:** Type a description for the template.
   - **Type:** Click the notification type in the drop-down list. Only supported channels for the selected type appear. Only one APNS Cert Expiration template is allowed, which is a pre-defined template. You can't add a template of this type.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> For some template types, the phrase "Manual sending supported"appears below the type. Those template types are available in the **Notifications** list on the **Dashboard** and on the **Devices** page. From those locations you can manually send the notification to users. Manual sending isn't available in any template that uses the following macros in the Subject or Message field on any channel:

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

> **Note:**
>
> The Citrix Endpoint Management console includes the terms "blacklist"and "whitelist". We're changing those terms in an upcoming version to "block list"and "allow list".

3. Under **Channels**, configure the information for each channel to be used with this notification. You can choose any or all channels. The channels you choose depends on how you want to send notifications:

   - If you choose **Citrix Secure Hub**, only iOS and Android devices receive the notifications, which appear in the device notification tray.
   - If you choose **SMTP**, users who enrolled with their email address receive the message.

   Citrix Secure Hub:

   - **Activate:** Click to enable the notification channel.
   - **Message:** Type the message to be sent to the user. This field is required if you're using Citrix Secure Hub. For information about using macros in a message, see Macros.
   - **Sound File:** In the list, click the notification sound the user hears when the notification is received.

   SMTP:

   - **Activate:** Click to enable the notification channel.

     You can activate the SMTP notification only after you set up the SMTP server.

   - **Sender:** Type an optional sender for the notification, which can be a name, an email address, or both.
   - **Recipient:** This field has a pre-built macro for all but Ad Hoc notifications to make sure that notifications are sent to the correct SMTP recipient address. Citrix recommends that you do not modify macros in templates. You can add more recipients (such as a corporate administrator) by adding their addresses in this field. Use a semi-colon (;) to separate the

© 1997–2025 Citrix Systems, Inc. All rights reserved.

macros and other addresses. To send Ad Hoc notifications, you can enter specific recipients, or you can select devices from the **Manage > Devices** page and send notifications from there. For details, see Devices.

- **Subject:** Type a descriptive subject for the notification. This field is required.
- **Message:** Type the message to be sent to the user. For information about using macros in a message, see Macros.

4. Click **Add**. When all channels are correctly configured, they appear in this order on the **Notification Templates** page: SMTP and Citrix Secure Hub. Any channels not correctly configured appear after the correctly configured channels.

Edit a notification template

1. Select a notification template. The edit page specific to that template appears. You can edit the template, except for the **Type** field, and activate or deactivate channels.
2. Click **Save**.

Delete a notification template

You can delete only notification templates that you've added. You can't delete predefined notification templates.

1. Select an existing notification template.
2. Click **Delete**. A confirmation dialog box appears.
3. Click **Delete** to delete the notification template or click **Cancel** to cancel deleting the notification template.

Configure roles with RBAC

September 6, 2025

The role-based access control (RBAC) feature in Citrix Endpoint Management lets you assign roles to users and groups. Roles are sets of permissions that control the level of access users have to system functions.

Citrix Endpoint Management comes with the following default user roles. You can use the default roles as templates that you customize to create your own user roles.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Administrator:** Grants full system access.
- **User:** Allows users to enroll devices and access the Self-Help Portal.

You can use the RBAC feature in Citrix Endpoint Management to:

- Create and edit user roles.
- Assign roles to local user groups and Active Directory (AD) groups.
- Assign roles to administrators in Citrix Cloud through **Identity and Access Management > Administrators**. See [Add roles to Citrix Cloud administrators] (#add-roles-to-citrix-cloud-administrators).

Use the RBAC feature

You can assign roles to local users, to cloud administrators (in Citrix Cloud), and to local user groups and Active Directory groups.

- **Local users:** Assign roles to local users using **Manage > Users**. You can assign only one role to local users. To change the roles, you can manually edit the user account. Or, you can create a group for local users and assign a role to that group.
- **Cloud administrators:** A cloud administrator is a special user account that Citrix Cloud creates when an administrator is added to your Citrix Cloud customer account. A cloud administrator account uses the same user name as the administrator account on Citrix Cloud. Create RBAC roles in the Citrix Endpoint Management console and assign roles to these users through **Identity and Access Management > Administrators** in Citrix Cloud.
- **Active Directory groups:** All users in an Active Directory group have the same permissions. If a user belongs to several Active Directory groups, all the permissions merge to define the permissions for that user. For example, suppose ADGroupA users can locate manager devices and ADGroupB users can wipe employee devices. A user who belongs to both groups can locate and wipe the devices of managers and employees. If a user belongs to groups with conflicting permissions, the allowed permissions prevail.

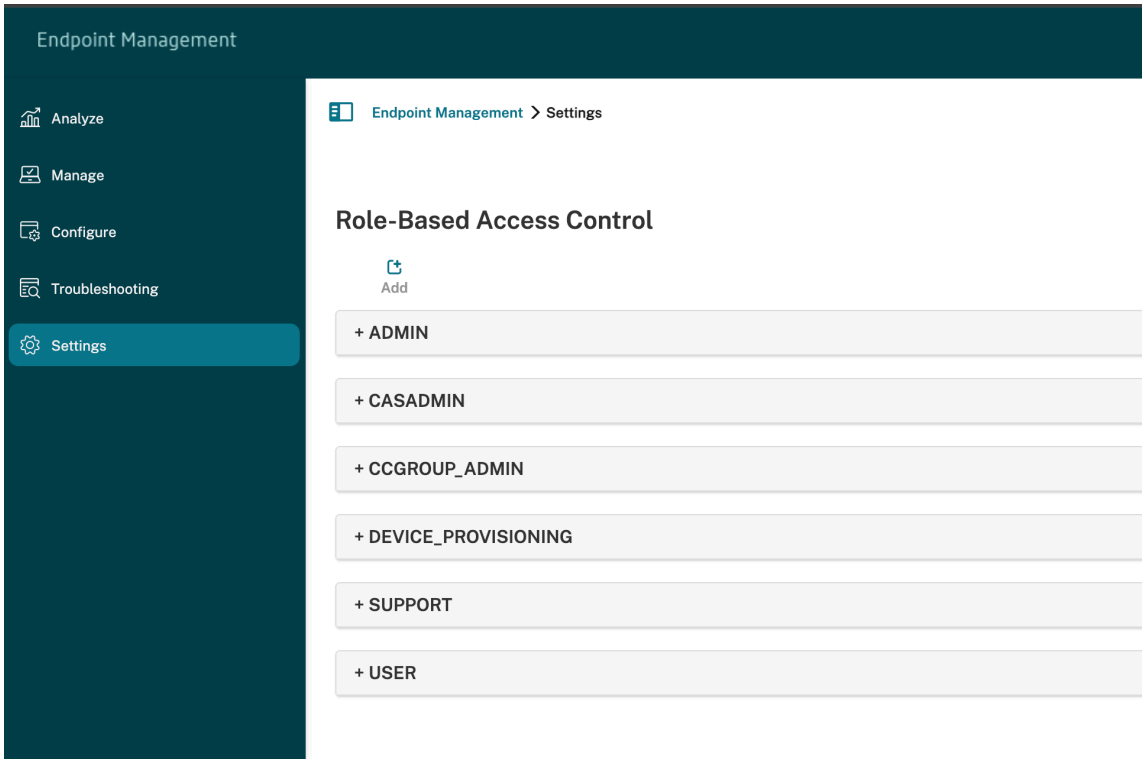
For more information, see About user accounts.

Create or edit roles

1. In the Citrix Endpoint Management console, to access the **Settings** page, click the gear icon in the upper-right corner.
2. Click **Role-Based Access Control**. The **Role-Based Access Control** page shows the default user roles and any roles that you added.

   Click the plus sign (+) next to a role to see all the permissions for that role.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. To add a role, click **Add**. Or, to edit a role, click the pen to the right of an existing role.

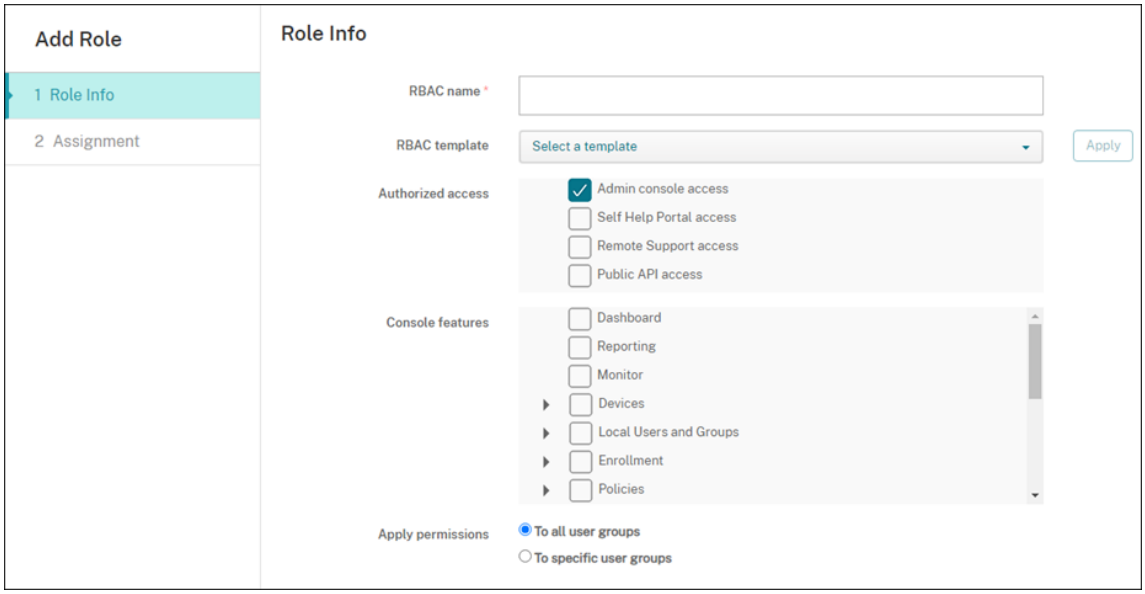
   > **Note:**
   >
   > You can delete a role by clicking the trash can to the right of a role that you defined. You can't delete the default user roles.

4. On the **Add Role** page, enter the following information:

   - **RBAC name:** Enter a descriptive name for the new user role. You can't change the name of an existing role.
   - **RBAC template:** Optionally, select a template as the starting point for the new role. (When editing a role, you can't select or change templates.) RBAC templates are the default user roles that define the access to system functions.

   Click the **Apply** button to populate the **Authorized access** and **Console features** checkboxes. Citrix Endpoint Management fills those fields with the predefined access and feature permissions for the selected template.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. To customize the role, select or clear the checkboxes in **Authorized access** and **Console features**.

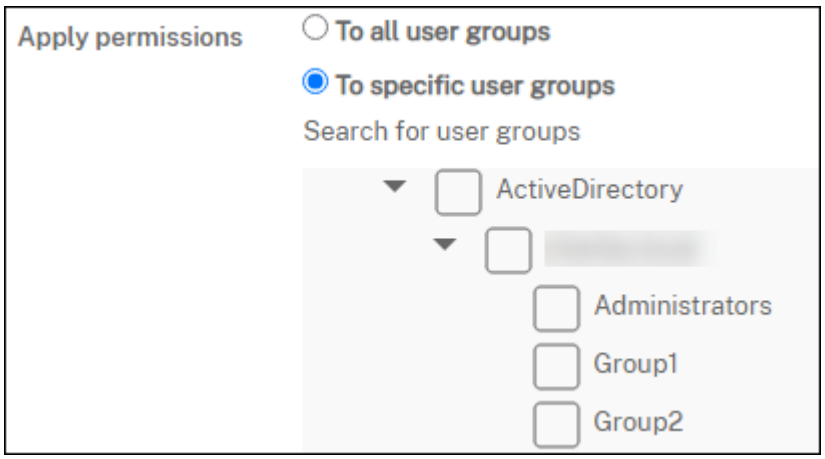
   Click the triangle next to a console feature to reveal and select permissions specific to that feature. Clicking the top-level checkbox does not select the individual permissions. Select individual options after expanding the top-level permission.

6. **Apply permissions:** Click **To specific user groups** to apply permissions to the groups you select.

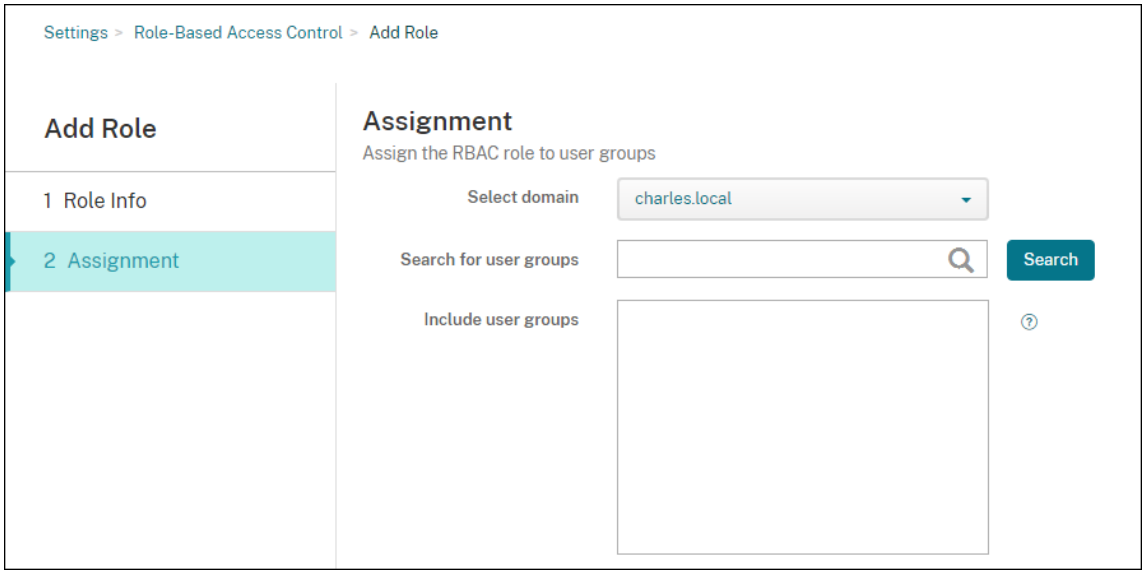
   For example, if an RBAC administrator has permission to the ActiveDirectory user group:

   - The administrator can access information only for users who are in the ActiveDirectory group.
   - The administrator can't view any other local or AD users. The administrator can view users who are members of child groups of either of those groups.
   - The administrator can send invitations to:
     - The permission groups and their child groups
     - The users who are members of permission groups and their child groups

© 1997–2025 Citrix Systems, Inc. All rights reserved.



7. Click **Next** and enter the following information to assign the role to user groups.



   - **Select domain:** From the list, select a domain.
   - **Search for user groups:** Click **Search** to see a list of all available groups. Type a full or partial group name to narrow the search.
   - **Include user groups:** In the list that appears, select the user groups you want to assign the role to.

8. Click **Save**.

Add roles to Citrix Cloud administrators

Instead of assigning RBAC roles to Citrix Cloud administrators through the Citrix Endpoint Management console, assign roles from the Citrix Cloud console.

1. In the Citrix Cloud console, navigate to **Identity and Access Management > Administrators**.

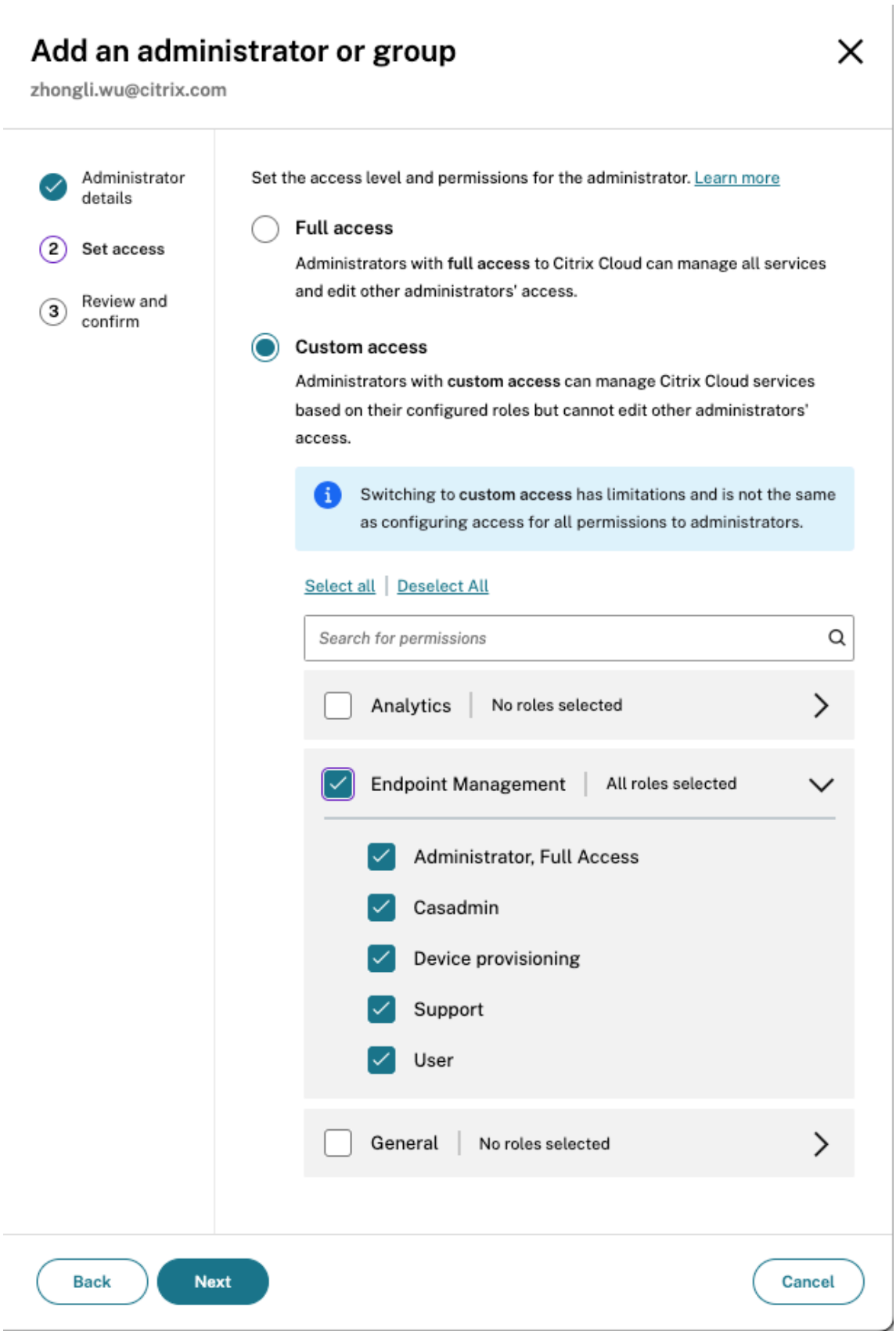
© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Selecting an identity provider, and then type an email address to add an administrator. Click **Invite**.

   Click the **...** at the end of an existing administrator row to edit those permissions.

3. Click **Custom access**. When assigning permissions to the administrator, you can select the RBAC roles created in the Citrix Endpoint Management console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. Click **Send Invite** to send an invitation to a new administrator or click **Save** to finish editing an administrator.

Predefined roles

Each predefined RBAC role has certain associated access and feature permissions. The tables that follow describe each of the permissions for the Admin role and for the User role. You can't delete or edit the predefined roles.

- For a full list of default permissions for each built-in role, download Role-Based Access Control Defaults
- For information about the Citrix Endpoint Management user accounts, see About user accounts.

> **Important:**
>
> Under the Settings permission, the RBAC permission gives Admin users full access, including the ability to assign their own permissions. Give this access only to users who you intend to give the ability to manipulate everything in the Citrix Endpoint Management system.

Admin role

The predefined Admin role provides specific access in Citrix Endpoint Management. By default, **Authorized access** (except Self-Help Portal), **Console features**, and **Apply permissions** are enabled.

You can change the role for local users who are assigned the Admin role by using **Manage > Users**. For cloud users who have the Admin role, use the Citrix Cloud console to change the role. By default, cloud and local users with the Admin role have Full access.

Authorized access for administrators

Admin console access	Administrators can access all features on the Citrix Endpoint Management console.
Self-Help Portal access	By default, administrators can't access the Self-Help Portal. (Users with the User role can access only the Self-Help portal.)
Remote Support access	Administrators can access the Remote Support feature.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Public API access	Administrators can access the public API to do actions programmatically that are available on the Citrix Endpoint Management console. The actions include administering certificates, apps, devices, delivery groups, and local users.

Console features for administrators Administrators have unrestricted access to the Citrix Endpoint Management console.

Dashboard	The **Dashboard** is the first page that administrators see after logging on to the Citrix Endpoint Management console. The **Dashboard** shows basic information about notifications and devices.
Reporting	The **Analyze > Reporting** page provides pre-defined reports that let you analyze your app and device deployments.
Devices	The **Manage > Devices** page is where you manage user devices. You can add individual devices on the page or import a device provisioning file to add multiple devices at one time.
Local Users and Groups	The **Manage > Users** page is where you can add, edit, or delete local users and local user groups.
Enrollment	The **Manage > Enrollment Invitations** page is where you manage how users are invited to enroll their devices in Citrix Endpoint Management.
Policies	The **Configure > Device Policies** page is where you manage device policies, such as VPN and network.
App	The **Configure > Apps** page is where you manage the various apps that users can install on their devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Media	The **Configure > Media** page is where you manage the various media that users can install on their devices.
Action	The **Configure > Actions** page is where you manage responses to trigger events.
Delivery Group	The **Configure > Delivery Groups** page is where you manage delivery groups and the resources associated with them.
Enrollment Profile	The **Configure > Enrollment Profiles** page is where you specify how users can enroll their devices.
Alexa for Business	The **Settings** page is where you manage your Alexa for Business profiles.
Settings	The **Settings** page is where you manage system settings, such as client and server properties, certificates, and credential providers. **Important:** These settings include the RBAC permission. The RBAC permission gives admins full access, including the ability to assign their own permissions. Give this access only to users who you intend to give the ability to manipulate everything in the Citrix Endpoint Management system.
Support	The **Troubleshooting and Support** page is where you do troubleshooting activities such as running diagnostics and generating logs.

Device restrictions for administrators Administrators access device features throughout the console by setting device restrictions, setting up and sending notifications to devices, administering apps on the devices, and so on.

Full Wipe device	Erase all data and apps from a device, including memory cards if the device has one.
Clear Restriction	Remove one or more device restrictions.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Selective Wipe device	Erase all corporate data and apps from a device, leaving personal data and apps in place.
View locations	See the location of and set geographic restrictions on a device. Includes: Locate device, Track device.
Lock device	Remotely lock a device so that users can't use the device.
Unlock device	Remotely unlock a device so that users can use the device.
Lock container	Remotely lock the corporate container on a device.
Unlock container	Remotely unlock the corporate container on a device.
Reset container password	Reset the corporate container password.
Enable ASM/Bypass activation lock	Store a bypass code on a supervised iOS device when Activation Lock is enabled. To erase the device, use this code to clear the Activation Lock automatically.
Get Resident Users	List the users that have active accounts on the current device. This action forces a sync between the device and the Citrix Endpoint Management console.
Logout Resident User	Force a log out of the current user.
Delete Resident User	Delete the current session for a specific user. The user can sign in again.
Rings the device	Remotely ring a Windows device at full volume for 5 minutes.
Reboot the device	Restart Windows devices from the Citrix Endpoint Management console.
Deploy to device	Send apps, notifications, restrictions, and other resources to a device.
Edit device	Change the settings on the device.
Notification to device	Send a notification to a device.
Add/Delete device	Add or remove devices from Citrix Endpoint Management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Devices import	Import a group of devices from a file into Citrix Endpoint Management.
Export device table	Collect device information from the Device page and export it to a .csv file.
Revoke device	Prohibit a device from connecting to Citrix Endpoint Management.
App lock	Deny access to all apps on a device. On Android, this restriction prevents users from signing in to Citrix Endpoint Management. On iOS, users can sign in, but they can't access the apps.
App wipe	On Android, this restriction deletes the user's Citrix Endpoint Management account. On iOS, this restriction deletes the encryption key required for users to access Citrix Endpoint Management features.
View software inventory	See what software is installed on a device.
Request AirPlay mirroring	Request to start AirPlay streaming.
Stop AirPlay mirroring	Stop AirPlay streaming.
Enable lost mode	On the **Manage > Devices** page, you can put a supervised device in lost mode to block a supervised device on the lock screen. You can then locate the device when the device is lost or stolen.
Disable lost mode	On the **Manage > Devices** page, you can disable lost mode for a device that is set to lost mode.
OS Update device	You can deploy an OS Update device policy to devices.
Shut down device	Shut down iOS devices from the Citrix Endpoint Management console.
Restart device	Restart iOS devices from the Citrix Endpoint Management console.
Renew Device Enrollment Certificate	Renew a device CA certificate.

Local Users and Groups Administrators manage local users and local user groups on the **Manage > Users** page in Citrix Endpoint Management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Add Local Users
Delete Local Users
Edit Local Users
Import Local Users
Export Local Users
Local User Groups
Get Local User Lock ID
Delete Local User Lock

Enrollment Administrators can add and delete enrollment invitations, send notifications to users, and export the enrollment table to a .csv file.

Add/Delete enrollment	Add or remove an enrollment invitation to a user or a group of users.
Notify user	Send and enrollment invitation to a user or group of users.
Export enrollment invitation table	Collect enrollment information from the Enrollment page and export it to a .csv file.

Policies

Add/Delete policy	Add or remove a device or app policy.
Edit policy	Change a device or app policy.
Upload Policy	Upload a device or app policy.
Clone Policy	Copy a device or app policy.
Disable Policy	Disable an existing app policy.
Export Policy	Collect device policy information from the Device Policies page and export it to a .csv file.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Assign Policy	Assign a device policy to one or more delivery groups.

App Administrators manage apps on the **Configure > Apps** page in Citrix Endpoint Management.

Add/Delete app store or enterprise app	Add or remove a public app store app or an enterprise app (not MDX-enabled).
Edit app store or enterprise app	Change a public app store app or an enterprise app (not MDX-enabled).
Add/Delete MDX, Web, and SaaS app	Add or remove an MDX-enabled app, an app from your internal network (Web app), or an app from a public network (SaaS) to Citrix Endpoint Management.
Edit MDX, Web, and SaaS app	Change an MDX-enabled app, an app from your internal network (Web app), or an app from a public network (SaaS) to Citrix Endpoint Management.
Add/Delete category	Add or delete a category in which apps can appear in the app store.
Assign public/enterprise app to delivery group	Assign a public app store app or an MDX-enabled app to a delivery group for deployment.
Assign MDX/WebLink/SaaS app to delivery group	Assign to a delivery group an app that is MDX-enabled, doesn't require single sign-on (WebLink), or that's from a public network (SaaS).
Export app table	Collect app information from the App page and export it to a .csv file.

Media Manage media from a public app store or a Volume Purchase license.

Add/Delete app store or enterprise books
Assign public/enterprise books to delivery group

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Edit app store or enterprise books	

Action

Add/delete action	Add or remove an action defined by a trigger and associated response. A trigger is an event, device or user property, or installed app name.
Edit action	Change an action defined by a trigger and associated response. A trigger is an event, device or user property, or installed app name.
Assign action to delivery group	Assign an action to a delivery group for deployment to user devices.
Export action	Collect action information from the Actions page and export it to a .csv file.

Delivery group Administrators manage delivery groups from the **Configure > Delivery Groups** page.

Add/delete delivery group	Create or remove a delivery group, which adds specified users and optional policies, apps, and actions.
Edit delivery group	Change an existing delivery group, which modifies users and optional policies, apps, and actions.
Deploy delivery group	Make the delivery group available for use.
Export delivery group	Collect delivery group information from the Delivery group page and export it to a .csv file.

Enrollment profile Manage enrollment profiles.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Add/delete enrollment profile	
Edit enrollment profile	
Assign enrollment profile to delivery group	

Alexa for Business Manage Alexa for Business profiles.

Add/delete/edit Rooms	
Add/delete/edit Room profiles	
Add/delete/edit Skill groups	

Settings for administrators Administrators configure various settings on the **Settings** pages.

RBAC	RBAC Assignment. **Important:** This permission gives admins full access, including the ability to assign their own permissions. Give this access only to users who you intend to give the ability to manipulate everything in the Citrix Endpoint Management system.
LDAP	Administer one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.
Enrollment	Enable enrollment security modes for users and the Self-Help Portal.
Release Management	View the current installed release. Includes: Release Management Update
Certificates	Edit APNS certificate
Notification Templates	Create notification templates to use in automated actions, enrollment, and standard notification message delivery to users.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Workflows	Manage the creation, approval, and removal of user accounts for use with app configurations.
Credential Providers	Add one or more credential providers authorized to issue device certificates. The credential providers control the certificate format and the conditions for renewing or revoking the certificate.
PKI Entities	Manage public key infrastructure entities (generic, Microsoft Certificate Services, or discretionary CA).
Test PKI Connection	Use the **Test Connection** button on the **Settings > PKI Entities** page to make sure that the server is accessible.
Client Properties	Manage various properties on user devices, such as passcode type, strength, and expiration.
Client Support	Set the ways in which users can contact your support services (email, phone, or support ticket email).
Client Branding	Create a custom store name and default store views for the app store. Add a custom logo that appears in the app store or Citrix Secure Hub.
Carrier SMS Gateway	Set up carrier SMS gateways to configure notifications that Citrix Endpoint Management sends through carrier SMS gateways.
Notification Server	Set up an SMTP gateway server to send an email to users.
ActiveSync Gateway	Manage user access to users and devices through rules and properties.
Google Chrome	Configure Citrix Endpoint Management to communicate with your Google Workspace account.
Apple Deployment Program	Add an Apple Deployment Program account to Citrix Endpoint Management.
Apple Configurator Device Enrollment	Configure Apple Configurator settings in the Citrix Endpoint Management console.
iOS/volume purchase Settings	Add Apple Volume Purchase accounts.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway	Configure NetScaler Gateway (now renamed NetScaler Gateway) settings in Citrix Endpoint Management.
Network Access Control	Set the conditions that determine a device is noncompliant so that it can't access the network.
Server Properties	Add or modify server properties. Requires restarting Citrix Endpoint Management on all nodes.
Virtual Apps and Desktops	Allow users to add Citrix Virtual Apps and Desktops through Citrix Workspace app.
Citrix Files	When using Citrix Endpoint Management with Enterprise accounts: Configure settings to connect to the ShareFile and administrator service accounts for user account management. Requires existing Citrix Files domain and administrator credentials. When using Citrix Endpoint Management with storage zone connectors: Configure Citrix Endpoint Management to point to network shares and SharePoint locations defined in storage zone connectors.
Android Enterprise	Configure Android Enterprise server settings.
Identity Provider (IdP)	Configure an identity provider.
Citrix Endpoint Management Tools	Access the Citrix Endpoint Management Tools page.
Windows Bulk Enrollment	Configure Windows bulk enrollment settings.

Support Administrators can do various support tasks.

NetScaler® Gateway Connectivity Checks	Do various connectivity checks for NetScaler Gateway by IP address. Requires a user name and password.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management Connectivity Checks	Do connectivity checks for selected Citrix Endpoint Management features, such as database, DNS, and Google Plan.
Citrix Product Documentation	Access the public Citrix Endpoint Management documentation site.
Citrix Knowledge Center	Access the Citrix Support site to search for knowledge-base articles.
Logs	View and download log files.
Macros	Populate user or device property data in the text field of a profile, policy, notification, or enrollment template. Configure a single policy, deploy the policy to a large user base, and have user-specific values appear for each targeted user.
PKI Configuration	Import and export PKI configuration information.
APNS Signing Utility	Submit a request for Apple Push Network signing (APNs) certificates, or upload a Citrix Secure Mail APNs certificate for iOS.
Citrix Insight Services	Upload logs to Citrix Insight Services (CIS) for assistance with various issues.
Device NetScaler Gateway connector for Exchange ActiveSync Status	Query Citrix Endpoint Management for the status of a device sent to the connector for Exchange ActiveSync. The query is based on the device ActiveSync ID.

Restrict Group Access Admin users can apply permissions to all user groups.

Console features for device provisioning Device provisioning users have the following restricted access to the Citrix Endpoint Management console. By default, each of the following features is enabled.

Device restrictions

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Edit device	Change the settings on the device.
Add/Delete device	Add or remove devices from Citrix Endpoint Management.

Settings for device provisioning Device provisioning users can access the **Settings** page, but do not have the right to configure the features.

User role

Users with the User role have the following limited access to Citrix Endpoint Management.

Authorized access for users

Self-Help Portal	Provide users access only to the Self-Help Portal in Citrix Endpoint Management.

Console features for users Users have the following restricted access to the Citrix Endpoint Management console.

Device restricted access for users

Full Wipe device	Erase all data and apps from a device, including memory cards if the device has one.
Selective Wipe device	Erase all corporate data and apps from a device, leaving personal data and apps in place.
View locations	See the location of and set geographic restrictions on a device. Included: Locate device, See the location of a device, Track device, Track device location over time
Lock device	Remotely lock a device so that it can't be used.
Unlock device	Remotely unlock a device so that It can be used.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Lock container	Remotely lock the corporate container on a device.
Unlock container	Remotely unlock the corporate container on a device.
Reset container password	Reset the corporate container password.
Enable ASM/Bypass activation lock	Store a bypass code on a supervised iOS device when Activation Lock is enabled. To erase the device, use this code to clear the Activation Lock automatically.
Get Resident Users	List the users that have active accounts on the current device. This action forces a sync between the device and the Citrix Endpoint Management console.
Logout Resident User	Force a log out of the current user.
Delete Resident User	Delete the current session for a specific user. The user can sign in again.
Rings the device	Remotely ring a Windows device at full volume for 5 minutes.
Reboot the device	Restart a Windows device.
App lock	Deny access to all apps on a device. On Android, users can't sign in to Citrix Endpoint Management. On iOS, users can sign in, but they can't access the apps.
App wipe	On Android, this restriction deletes the user's Citrix Endpoint Management account. On iOS, this restriction deletes the encryption key required for users to access Citrix Endpoint Management features.
View software inventory	See what software is installed on a device.

Enrollment restrictions for users

Add/Delete enrollment	Add or remove an enrollment invitation to a user or a group of users.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Notify user	Send and enrollment invitation to a user or group of users.

Restrict Group Access for all roles For the default roles, this permission is set by default and can be applied to all user groups. You can't edit the role.

Licenses

September 6, 2025

For information about Citrix® license usage, see:

- Monitor license and active usage for cloud services
- Monitor license and active usage for Citrix Endpoint Management

Device management

September 6, 2025

Citrix Endpoint Management can provision, manage, secure, and inventory a broad range of device types within a single management console.

- Use a common set of device policies to manage supported devices. For a quick look at the device policies available by platform:
  1. Go to the Citrix Endpoint Management console and navigate to **Configure > Device Policies**.
  2. Click **Add** and then select the platforms you want to view.

     For more information, see Filter the list of added device policies.
- Protect business information with strict security for identity, corporate-owned and BYO devices, apps, data, and network. Specify the user identity to use to authenticate to devices. Configure how to keep enterprise and personal data separate on devices.
- Deliver any app to end users, whatever device or operating system. Protect your information at the app level and provide enterprise-grade mobile application management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

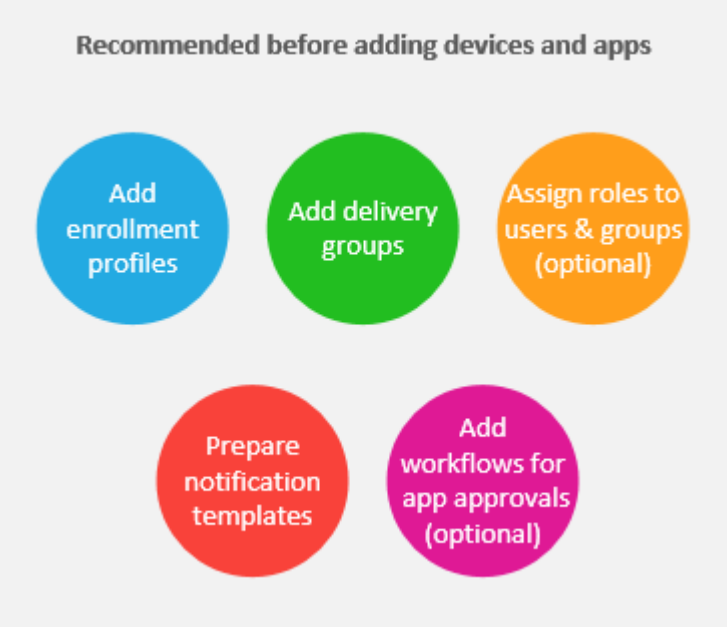
- Use provisioning and configuration controls to set up devices. Those controls include device enrollment, policy application, and access privileges.
- Use security and compliance controls to create a customized security baseline with actionable triggers. For example, lock, wipe, or notify a device in violation of defined compliance standards.
- Use OS update controls to prevent or enforce operating system updates. This feature is critical for data loss prevention against targeted operating system vulnerabilities.

To access articles about each supported platform, expand the "Device management"section in the contents list. Those articles provide details specific to each device platform. The rest of this article describes how to do general device management tasks.

Device management workflows

The workflow diagrams in this section provide a suggested sequence for device management tasks.

1. **Recommended prerequisites for adding devices and apps:** Performing the following setup in advance lets you configure devices and apps without interruption.



See:

Deploy resources

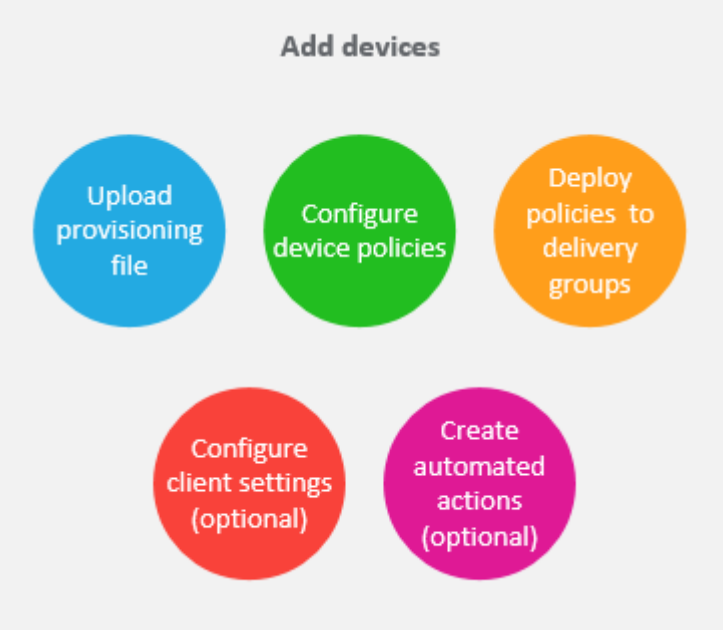
Configure roles with RBAC

Create and update notification templates

Create and manage workflows

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. **Add devices:**



   See:

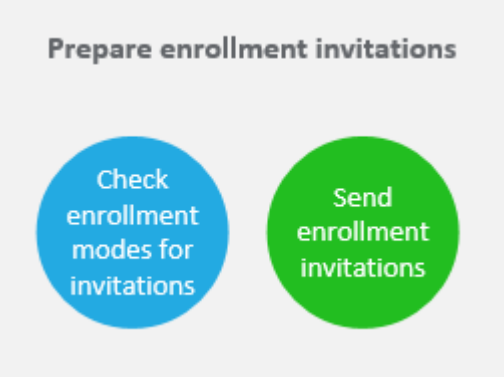
   Prepare to enroll devices and deliver resources

   Device policies

   Deploy to delivery groups

   Automated actions

3. **Prepare enrollment invitations:** You can send enrollment invitations to users with iOS, iPadOS, macOS, Android Enterprise, and legacy Android devices. Do the following if you plan to use enrollment invitations.



   See:

   Configure enrollment security modes

   Send a notification to devices

© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. **Add apps:**

   See:

   MAM SDK

   Add apps

   About app categories

   Apply workflows

   Deploy to delivery groups

5. **Perform ongoing device and app management:** In addition to using the Citrix Endpoint Management dashboard, we encourage you to review the What's new content for each version. What's new provides information about any needed actions, such as configuring new device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

See:

Monitor and support

Reports

Security actions

What's new

Device policies

Enrollment invitations

To manage user devices remotely and securely, you enroll user devices in Citrix Endpoint Management. The Citrix Endpoint Management client software is installed on the user device and the user identity is authenticated. Then, Citrix Endpoint Management and the user profile are installed. For enrollment details for supported device platforms, see the device articles under this section.

In the Citrix Endpoint Management console:

- You can send an enrollment invitation to users with iOS, iPadOS, macOS, Android Enterprise, and legacy Android devices. Enrollment invitations aren't available for Windows devices.
- You can send an invitation URL to users with iOS, iPadOS, Android Enterprise, or legacy Android devices. Invitation URLs aren't available for Windows devices.

Enrollment invitations are sent as follows:

- If Active Directory users have an email address in Active Directory, they receive the invitation. Local users receive the invitation at the email specified in user properties.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

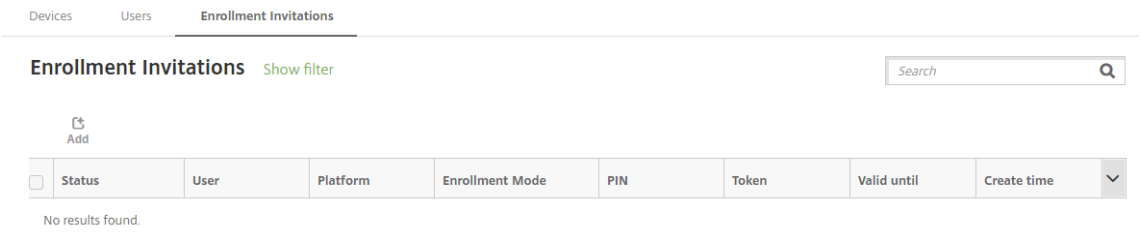
After users enroll, their devices appear as managed on **Manage > Devices**. The status of the invitation URL is shown as **Redeemed**.

Prerequisites

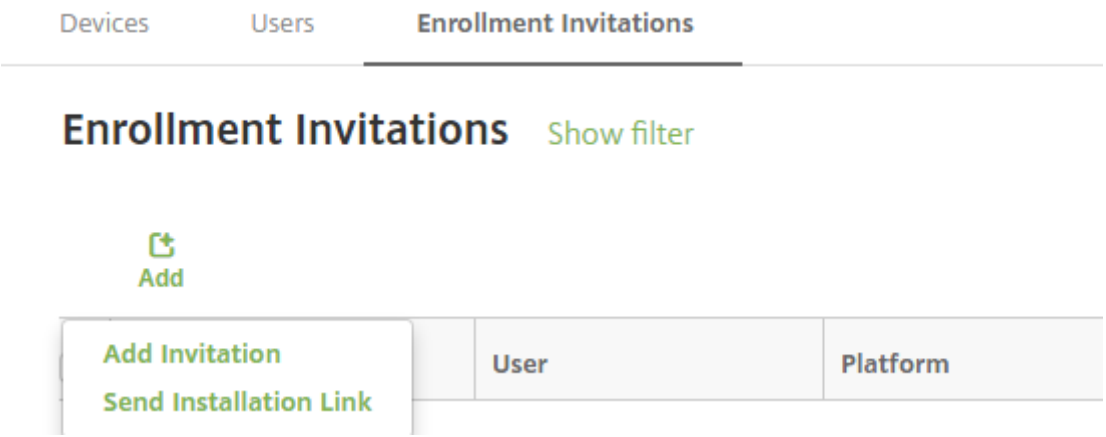
- LDAP configured
- If using local groups and local users:
  - One or more local groups.
  - Local users assigned to local groups.
  - Delivery groups are associated with local groups.
- If using Active Directory:
  - Delivery groups are associated with Active Directory groups.

Create an enrollment invitation

1. In the Citrix Endpoint Management console, click **Manage > Enrollment Invitations**. The **Enrollment Invitations** page appears.



2. Click **Add**. A menu of enrollment options appears.



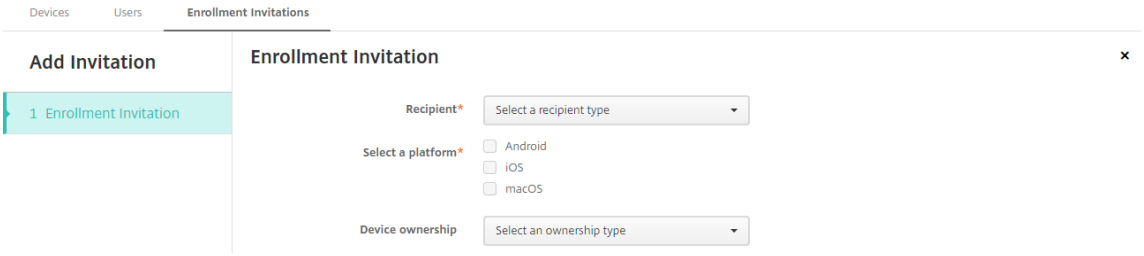
   - To send an enrollment invitation to a user or group, click **Add Invitation**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- To send an enrollment installation link to a list of recipients over SMTP, click **Send Installation Link**.

Sending enrollment invitations and installation links are described after these steps.

3. Click **Add Invitation**. The **Enrollment Invitation** screen appears.



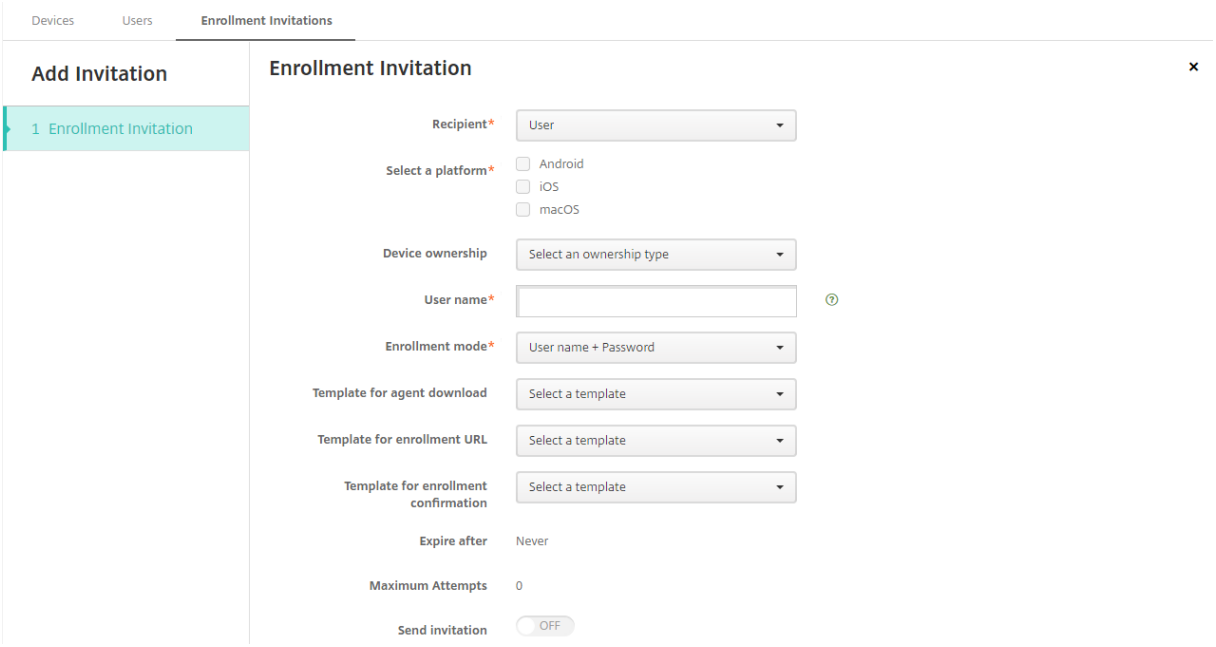
4. Configure these settings:

   - **Recipient:** Choose **Group** or **User**.
   - **Select a platform:** If **Recipient** is **Group**, all platforms are selected. You can change the platform selection. If **Recipient** is **User**, no platforms are selected. Select a platform.

     To create an enrollment invitation for Android Enterprise devices, select **Android**.
   - **Device ownership:** Select **Corporate** or **Employee**.

Settings for users or groups appear, as described in the following sections.

To send an enrollment invitation to a user



© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. Configure these **User** settings:

   - **User name:** Type a user name. The user must exist in Citrix Endpoint Management as a local or Active Directory user. If the user is local, set the email property of the user so you can send that user notifications. If the user is in the Active Directory, provided that LDAP is configured.
   - **Phone number:** This setting doesn't appear if you select more than one platform or if you select only macOS. Optionally, type the phone number of the user.
   - **Carrier:** This setting doesn't appear if you select more than one platform or if you select only macOS. Choose a carrier to associate to the phone number of the user.
   - **Enrollment mode:** Choose the enrollment security mode for users. The default is **User name + Password**. Some of the following options aren't available for all platforms:
     - **User name + Password**
     - **Invitation URL**
     - **Invitation URL + PIN**
     - **Invitation URL + Password**
     - **Two Factor**
     - **User name + PIN**

   We deprecated support for **High Security** enrollment mode. To send enrollment invitations, you can use only **Invitation URL**, **Invitation URL + PIN**, or **Invitation URL + Password** enrollment security modes. For devices enrolling with **User name + Password**, **Two Factor**, or **User name + PIN**, users must download Citrix Secure Hub and manually enter their credentials.

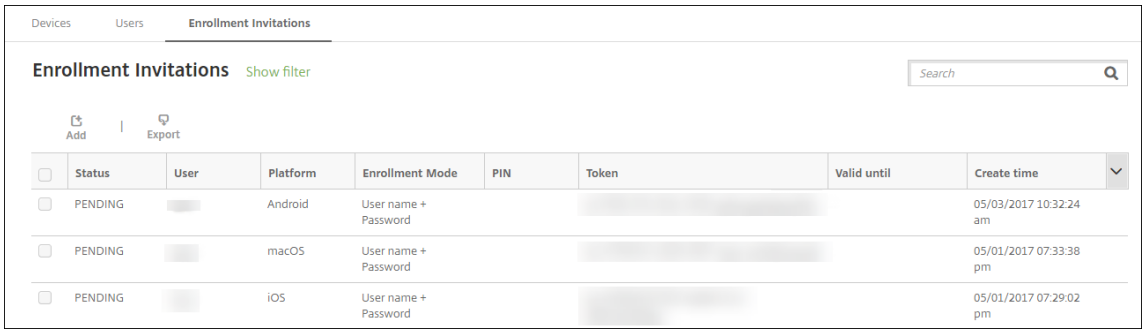
   For more information, see Enrollment security modes by platform. A PIN for enrollment is also called a one-time PIN. Such PINs are valid only when the user enrolls.

   > **Note:**
   >
   > When you select any enrollment security mode that includes a PIN, the **Template for enrollment PIN** field appears. Click **Enrollment PIN**.

   - **Template for agent download:** Choose the download link template named **Download link**. That template is for all supported platforms.
   - **Template for enrollment URL:** Choose **Enrollment Invitation**.
   - **Template for enrollment confirmation:** Choose **Enrollment Confirmation**.
   - **Expire after:** This field is set when you configure the enrollment security mode and indicates when the enrollment expires. For more information about configuring enrollment security modes, see Configure enrollment security modes.
   - **Maximum Attempts:** This field is set when you configure the enrollment security mode and indicates the maximum number of times the enrollment process occurs.
   - **Send invitation:** Select **On** to send the invitation immediately. Select **Off** to add the invitation to the table on the **Enrollment Invitations** page, but not send it.

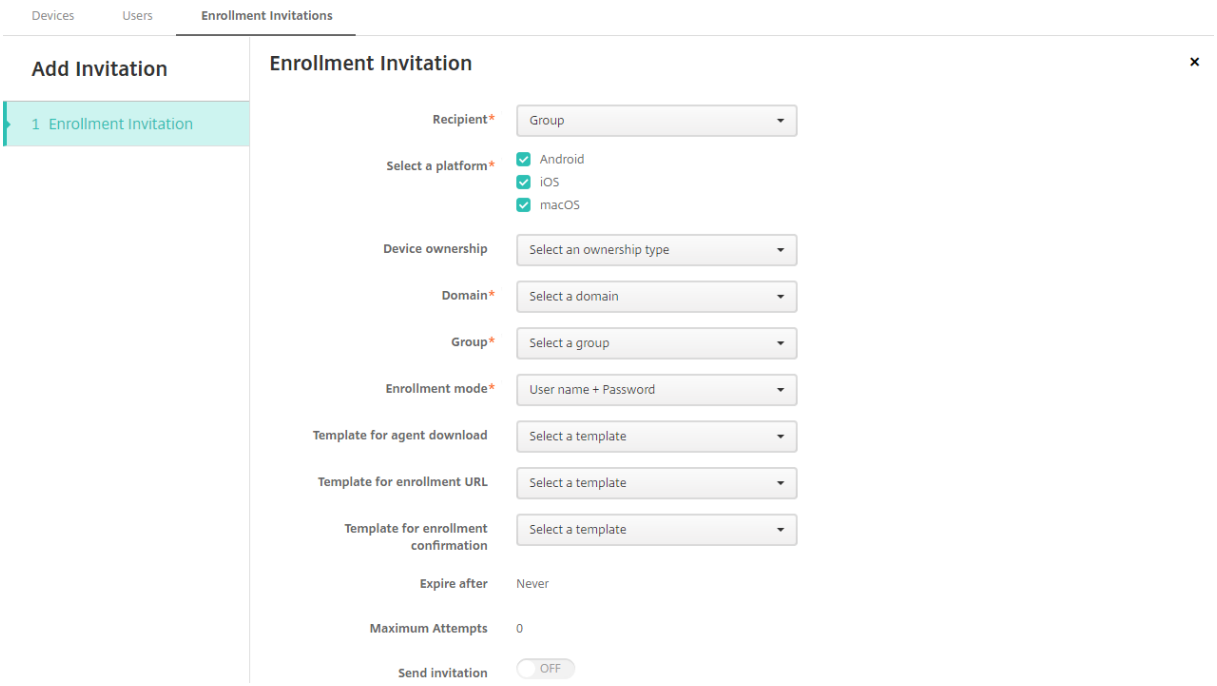
© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Click **Save and Send** if you enabled **Send invitation**. Otherwise, click **Save**. The invitation appears in the table on the **Enrollment Invitations** page.



To send an enrollment invitation to a group

The following figure shows the settings for configuring an enrollment invitation to a group.



1. Configure these settings:

   - **Domain:** Choose the domain of the group to receive the invitation.
   - **Group:** Choose the group to receive the invitation. Citrix Endpoint Management gets the user list from Active Directory. The list includes users whose names have special characters.
   - **Enrollment mode:** Choose how you want users in the group to enroll. The default is **User name + Password**. Some of the following options aren't available for all platforms:
     - **User name + Password**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Invitation URL**
- **Invitation URL + PIN**
- **Invitation URL + Password**
- **Two Factor**
- **User name + PIN**

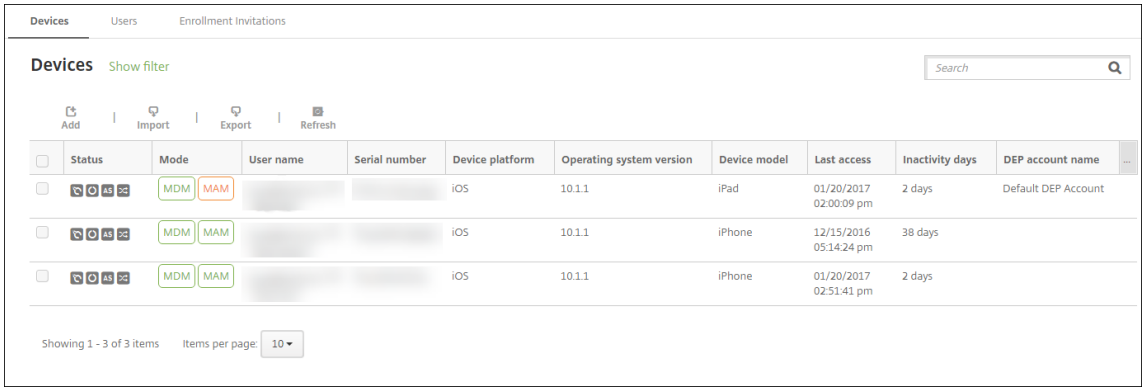
We deprecated support for **High Security** enrollment mode. To send enrollment invitations, you can use only **Invitation URL**, **Invitation URL + PIN**, or **Invitation URL + Password** enrollment security modes. For devices enrolling with **User name + Password**, **Two Factor**, or **User name + PIN**, users must download Citrix Secure Hub and manually enter their credentials.

Only the enrollment security modes that are valid for each of the selected platforms appear. For more information, see Enrollment security modes by platform.

> **Note:**
>
> When you select any enrollment security mode that includes a PIN, the **Template for enrollment PIN** field appears. Click **Enrollment PIN**.

- **Template for agent download:** Choose the download link template named **Download link**. That template is for all supported platforms.
- **Template for enrollment URL:** Choose **Enrollment Invitation**.
- **Template for enrollment confirmation:** Choose **Enrollment Confirmation**.
- **Expire after:** This field is set when you configure the enrollment security mode and indicates when the enrollment expires. For more information about configuring enrollment security modes, see Configure enrollment security modes.
- **Maximum Attempts:** This field is set when you configure the enrollment security mode and indicates the maximum number of times the enrollment process occurs.
- **Send invitation:** Select **On** to send the invitation immediately. Select **Off** to add the invitation to the table on the **Enrollment Invitations** page, but not send it.

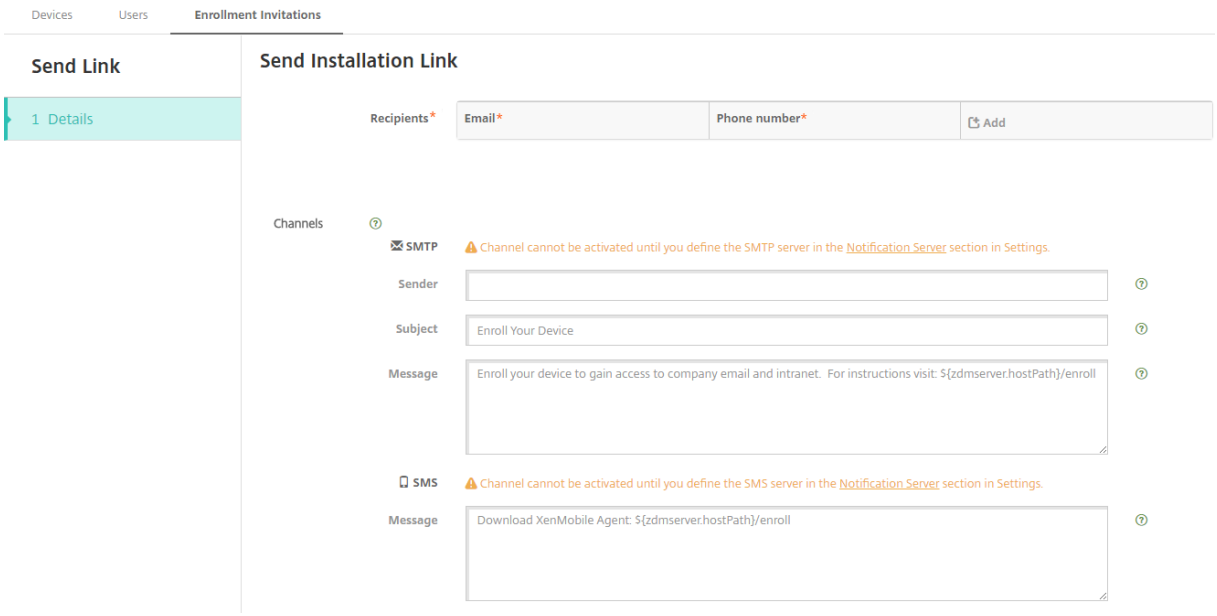
2. Click **Save and Send** if you enabled **Send invitation**. Otherwise, click **Save**. The invitation appears in the table on the **Enrollment Invitation** page.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

To send an installation link

Before you can send an enrollment installation link, you must configure channels (SMTP) on the notification server from the **Settings** page. For details, see Notifications



1. Configure these settings and then click **Save**.

   - **Recipient:** For each recipient that you want to add, click **Add** and then do the following:
     - **Email:** Type the email address of the recipient. This field is required.
     - **Phone number:** Type the phone number of the recipient. This field is required.

     > **Note:**
     >
     > To delete a recipient, hover over the line with the listing and then click the trash icon on the right side. A confirmation dialog box appears. Click **Delete** to delete the listing or click **Cancel** to keep the listing.
     >
     > To edit a recipient, hover over the line with the listing. Then, click the pen icon on the right side. Update the listing and then click **Save** to save the changed listing or **Cancel** to leave the listing unchanged.

   - **Channels:** Select a channel to use for sending the enrollment installation link. You can send notifications over **SMTP**. These channels cannot be activated until you configure the server settings on the **Settings** page in **Notification Server**. For details, see Notifications.
   - **SMTP:** Configure these optional settings. If you do not type anything in these fields, the default values specified in the notification template configured for the platform you selected are used:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Sender:** Type an optional sender.
- **Subject:** Type an optional subject for the message. For example, "Enroll your device."
- **Message:** Type an optional message to be sent to the recipient. For example, "Enroll your device to gain access to organizational apps and email."

2. Click **Send**.

> **Note:**
>
> If your environment uses sAMAccountName: After users receive the invitation and click the link, they must edit the user name to complete the authentication. The user name appears in the form of `sAMAccountName@domainname.com`. Users must remove the `@domainname.com` portion.

Enrollment security modes by platform

The following table displays security modes that you can use to enroll user devices. In the table, **Yes** indicates which device platforms support specific enrollment and management modes with different enrollment profiles.

MDM enrollment security mode	MAM enrollment security mode on NetScaler Gateway	Management modes	Support different enrollment profiles	Android (legacy)	Android Enterprise	iOS (user enrollment mode)	iOS	macOS	Windows
Azure AD and Okta as identity providers through Citrix Cloud	Client certificate	MDM+MAM or MDM	Yes	Yes	Yes	Yes	Yes	No	No

© 1997–2025 Citrix Systems, Inc. All rights reserved.

MDM enrollment security mode	MAM enrollment security mode on NetScaler Gateway	Management modes	Support different enrollment profiles	Android (legacy)	Android Enterprise	iOS (user enrollment mode)	iOS	macOS	Windows
User name + Password	LDAP, LDAP + client certificate, and client certificate only	MDM+MAM, MDM, or MAM (MAM-only mode doesn't support client certificates on NetScaler Gateway)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Invitation URL	Client certificate	MDM+MAM or MDM	Yes	Yes	Yes	No	Yes	No	No
Invitation URL + PIN	Client certificate	MDM+MAM or MDM	Yes	Yes	Yes	No	Yes	No	No

© 1997–2025 Citrix Systems, Inc. All rights reserved.

MDM enrollment security mode	MAM enrollment security mode on NetScaler Gateway	Management modes	Support different enrollment profiles	Android (legacy)	Android Enterprise	iOS (user enrollment mode)	iOS	macOS	Windows
Invitation URL + Password	LDAP, LDAP + client certificate, and client certificate only	MDM+MAM or MDM	Yes	Yes	Yes	No	Yes	No	No
Two-factor authentication (user name + password + PIN)	LDAP, LDAP + client certificate, and client certificate only	MDM+MAM or MDM	Yes	Yes	Yes	No	Yes	Yes	No
User name + PIN	Client certificate	MDM+MAM or MDM	Yes	Yes	Yes	No	Yes	Yes	No

The following describes how the enrollment security modes behave on iOS, Android, and Android Enterprise devices:

- **User name + Password** (default)
  - Sends a user a single notification that has an enrollment URL. When the user clicks the

© 1997–2025 Citrix Systems, Inc. All rights reserved.

URL, Citrix Secure Hub opens. The user then types a user name and password to enroll the device in Citrix Endpoint Management.

- **Invitation URL**
  - Sends a user a single notification that has an enrollment URL. When the user clicks the URL, Citrix Secure Hub opens. The Citrix Endpoint Management server name and the **Yes, Enroll** button appear. The user taps **Yes, Enroll** to enroll the device in Citrix Endpoint Management.
- **Invitation URL + PIN**
  - Sends a user the following emails:
    - An email with an enrollment URL, which lets the user enroll the device in Citrix Endpoint Management through Citrix Secure Hub.
    - An email with a one-time PIN that the user must type when enrolling the device, along with the user's Active Directory (or local) password.
  - With this mode, the user enrolls only by using the enrollment URL in the notification. If the user loses the notification invitation, the user can't enroll. However, you can send another invitation.
- **Invitation URL + Password**
  - Sends a user a single notification that has an enrollment URL. When the user clicks the URL, Citrix Secure Hub opens. The Citrix Endpoint Management server name appears, along with a field that lets the user type a password.
- **Two Factor**
  - Sends a user a single notification that has an enrollment URL and a one-time PIN. When the user clicks the URL, Citrix Secure Hub opens. The Citrix Endpoint Management server name appears, along with two fields that let the user type a password and the PIN.
- **User name + PIN**
  - Sends a user the following emails:
    - An email with an enrollment URL, which lets the user download and install Citrix Secure Hub. After Citrix Secure Hub opens, the user is prompted to type a user name and password to enroll the device in Citrix Endpoint Management.
    - An email with a one-time PIN that the user must type when enrolling the device, along with the user's Active Directory (or local) password.
  - If the user loses the notification invitation, the user can't enroll. However, you can send another invitation.

The following describes how the enrollment security modes behave on macOS devices:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **User name + Password**
  - Sends a user a single notification that has an enrollment URL. When the user clicks the URL, the Safari browser opens. A sign-in page appears, prompting the user to type a user name and password to enroll the device in Citrix Endpoint Management.
- **Two Factor**
  - Sends a user a single notification that has an enrollment URL and a one-time PIN. When the user clicks the URL, the Safari browser opens. A sign-in page appears, displaying two fields that let the user type a password and the PIN.
- **User name + PIN**
  - Sends a user the following emails:
    * An email with an enrollment URL. When the user clicks the URL, the Safari browser opens. A sign-in page appears, prompting the user to type a user name and password to enroll the device in Citrix Endpoint Management.
    * An email with a one-time PIN that the user must type when enrolling the device, along with the user's Active Directory (or local) password.
  - If the user loses the notification invitation, the user can't enroll. However, you can send another invitation.

You can't send enrollment invitations to Windows devices. Windows users enroll directly through their devices. For information about enrolling Windows devices, see Windows devices.

Security actions

You do device and app security actions from the **Manage > Devices** page. Device actions include revoke, lock, unlock, and wipe. App security actions include app lock and app wipe.

- **Activation Lock Bypass:** Removes the Activation Lock from supervised iOS devices before device activation. This command doesn't require the personal Apple ID or password for a user.
- **App lock:** Denies access to all apps on a device. On Android, after an app lock, users can't sign in to Citrix Endpoint Management. On iOS, users can sign in, but they can't access any apps.
- **App wipe:** Removes the user account from Citrix Secure Hub and unenrolls the device. Users can't reenroll until you use the **App unwipe** action.
- **ASM Deployment Program Activation Lock:** Creates an Activation Lock bypass code for iOS devices enrolled in Apple School Manager.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Certificate renewal:** For supported iOS, macOS, and Android devices, the Certificate Renewal security action starts certificate renewal. The next time that devices connect back to Citrix Endpoint Management, the Citrix Endpoint Management server issues new device certificates based on the new certificate authority.
- **Clear restrictions:** On supervised iOS devices, this command allows Citrix Endpoint Management to clear the restrictions password and restrictions settings configured by the user.
- **Enable/disable Lost Mode:** Puts a supervised iOS device in Lost Mode and sends the device a message, phone number, and a footnote to display. The second time that you send this command takes the device out of Lost Mode.
- **Enable tracking:** On Android or iOS devices, this command allows Citrix Endpoint Management to poll the location of specific devices at a frequency you define. To view device coordinates and location on a map, go to **Manage > Devices**, select a device, and then click **Edit**. The device info is on the **General** tab under **Security**. Use **Enable tracking** to track the device continuously. Citrix Secure Hub reports the location periodically when the device is running.
- **Full wipe:** Immediately erases all data and apps from a device, including from any memory cards. Wiped devices stay in the device list on the **Manage > Devices** page for auditing purposes. You can remove a wiped device from the device list.
  - For Android devices, this request can also include the option to wipe memory cards.
  - For Android Enterprise fully managed devices with a work profile (COPE devices), you can do a full wipe after a selective wipe removes the work profile.
  - For iOS and macOS devices, the wipe occurs immediately, even if the device is locked.

    For iOS 11 devices and iPadOS 12 devices (minimum version): When you confirm the full wipe, you can choose to preserve the cellular data plan on the device.

    For iOS 11.3 devices (minimum version): When you confirm the full wipe, you prevent iOS devices from doing proximity setup. When setting up a new iOS device, users can normally use an already configured iOS device to set up their own. You can block proximity setup on devices that are Citrix Endpoint Management managed and have been wiped.

    For iOS 17 devices (minimum version): When you confirm the full wipe, the device 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.
  - If the device user turns off the device before the memory card content is deleted, the user might still have access to device data.
  - You can cancel the wipe request until the request is sent to the device.
- **Locate:** Locates a device and reports the device location, including a map, on the **Manage > Devices** page, under **Device details > General**. Locate is a one-time action. Use **Locate** to dis-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

play the current device location at the time you do the action. To continuously track the device over a period, use **Enable tracking**.

  - When applying this action to Android (except for Android Enterprise) devices or to Android Enterprise (corporate-owned or BYOD) devices, be aware of the following behavior:
    * **Locate** requires the user to grant location permission during enrollment. The user can choose not to grant location permission. If the user doesn't grant the permission during enrollment, Citrix Endpoint Management again requests location permission when sending the **Locate** command.
  - When applying this feature to iOS or Android Enterprise devices, be aware of the following limitations:
    * For Android Enterprise devices, this request fails unless the Location device policy has set the location mode for the device to **High Accuracy** or **Battery Saving**.
    * For iOS devices, the command succeeds only if the devices are in MDM Lost Mode.

- **Lock:** Remotely locks a device. A lock is useful if a device is stolen and must be locked. Citrix Endpoint Management then generates a PIN code and sets it in the device. To access the device, the user types the PIN code. Use **Cancel Lock** to remove the lock from the Citrix Endpoint Management console.
- **Lock and Reset Password:** Remotely locks a device and resets the passcode.
  - Not supported for devices that are:
    * enrolled in Android Enterprise in work profile mode and
    * running Android versions earlier than Android 7.0
  - On devices enrolled in Android Enterprise in work profile mode and that are running Android 7.0 or greater:
    * The passcode locks the work profile. The device is not locked.
    * If a passcode isn't sent, or the passcode sent doesn't meet requirements and the work profile doesn't have a passcode: The device is locked.
    * If a passcode isn't sent, or the passcode sent doesn't meet requirements, but the work profile has a passcode: The work profile is locked but the device isn't locked.

  > **Note:**
  >
  > The reset password functionality is only supported for BYOD Samsumg devices and console admin should have `DEVICE_ACTION_CONTAINER_PASSWORD_RESET` permissions.

- **Notify (Ring):** Plays a sound on the devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> This functionality is only supported for iOS devices.

- **Reboot:** Restarts Windows 10 and Windows 11 devices. For Windows Tablet and PCs, a message about the pending reboot appears. The reboot occurs in five minutes.
- **Request/Stop AirPlay Mirroring:** Starts and stops AirPlay mirroring on supervised iOS devices.
- **Restart/Shut Down:** Immediately restarts or shuts down supervised devices.

  > **Note:**
  >
  > This functionality is only supported for iOS devices.

- **Revoke:** Prohibits a device from connecting to Citrix Endpoint Management.
- **Revoke/Authorize:** Performs the same actions as a Selective Wipe. After revocation, you can reauthorize the device to reenroll it.
- **Ring:** If the device is in Lost Mode, Ring plays a sound on a supervised iOS device. The sound plays until you removed the device from Lost Mode or the user disables the sound.
- **Rotate personal recovery key:** If you've enabled the FileVault device policy, this action generates a new personal recovery key and replaces the old key with this new key. You can cancel this request while the request is still pending. To do so, click **Cancel Rotate personal recovery key**.
- **Selective wipe:** Erases all corporate data and apps from a device, leaving personal data and apps in place. After a selective wipe, use the **Authorize** action to reauthorize the device so a user can reenroll it. Wiped devices stay in the device list on the **Manage > Devices** page for auditing purposes. You can remove a wiped device from the device list.
  - Selectively wiping an Android device does not disconnect the device from Device Manager and the corporate network. To prevent the device from accessing Device Manager, you must also revoke the device certificates.
  - Selectively wiping an Android device also revokes the device. You can reenroll the device only after reauthorizing it or deleting it from the console.
  - For Android Enterprise fully managed devices with a work profile (COPE devices), you can do a full wipe after a selective wipe removes the work profile. Or, you can re-enroll the device with the same user name. Re-enrolling the device recreates the work profile.
  - For iOS and macOS devices, this command removes any profile installed through MDM.
  - A selective wipe on a Windows device also removes the contents of the profile folder for any currently signed on user. A selective wipe doesn't remove any web clips that you deliver to users through a configuration. To remove web clips, users manually unenroll their devices. You can't reenroll a selectively wiped device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Unlock:** Clears the passcode sent to the device when it was locked. This command doesn't open the device.

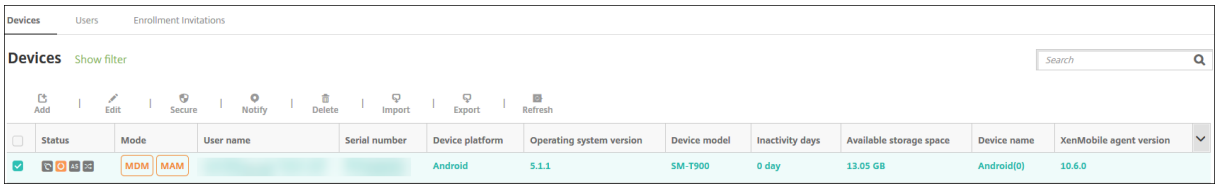
In **Manage > Devices**, the **Device details** page also lists device Security properties. Those properties include Strong ID, Lock Device, Activation Lock Bypass, and other information for the platform type. The **Full Wipe of Device** field includes the user PIN code. The user must enter that code after the device is wiped. If the user forgets the code, you can look it up here.

You can automate some actions. For more information, see Automated actions.

Remove a device from the Citrix Endpoint Management console

> **Important:**
>
> When you remove a device from the Citrix Endpoint Management console, managed apps and data stay on the device. To remove managed apps and data from the device, see "Delete a device" later in this article.

To remove a device from the Citrix Endpoint Management console, go to **Manage > Devices**, select a managed device, and then click **Delete**.



Selectively wipe a device

1. Go to **Manage > Devices**, select a managed device, and then click **Secure**.
2. In **Security Actions**, click **Selective wipe**.
3. For Android devices only, disconnect the device from the corporate network: After the device is wiped, in **Security Actions**, click **Revoke**.

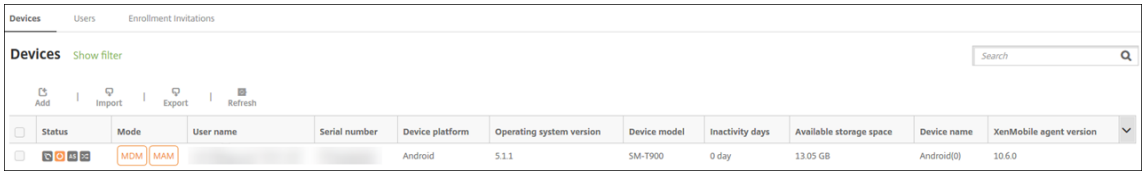
   To withdraw a selective wipe request before the wipe occurs, in **Security Actions**, click **Cancel selective wipe**.

Delete a device

This procedure removes managed apps and data from the device and deletes the device from the Devices list in the Citrix Endpoint Management console. You can use the Citrix Endpoint Management Public REST API to delete devices in bulk.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. Go to **Manage > Devices**, select a managed device, and then click **Secure**.
2. Click **Selective Wipe**. When prompted, click **Perform Selective Wipe**.
3. To verify that the wipe command succeeded, refresh **Manage > Devices**. In the **Mode** column, the amber color for MDM and MAM indicates that the wipe command succeeded.



4. On **Manage > Devices**, select the device, and then click **Delete**. When prompted, click **Delete** again.

Lock, unlock, wipe, or unwipe apps

1. Go to **Manage > Devices**, select a managed device, and then click **Secure**.
2. In **Security Actions**, click the app action.

   You can also use the **Security Actions** box to check the device status for a user whose account is disabled or deleted from Active Directory. The presence of the App Unlock or App Unwipe actions indicate apps that are locked or wiped.

App wipe and unwipe

1. Go to **Manage > Devices**. Select a device.
2. App wipe
   - Click **Secure > App Wipe**. A dialog box with the following message appears: **Are you sure you want to app wipe this device?** Click **App Wipe**.
3. App unwipe
   - Click **Secure > App Unwipe**. A dialog box with the following message appears: **Are you sure you want to app unwipe this device?** Click **Device App Unwipe**.
4. Re-enroll the device as the same user, in the same mode.
5. Launch an MDX app from **My Apps** page.
6. Launch Citrix Secure Hub.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

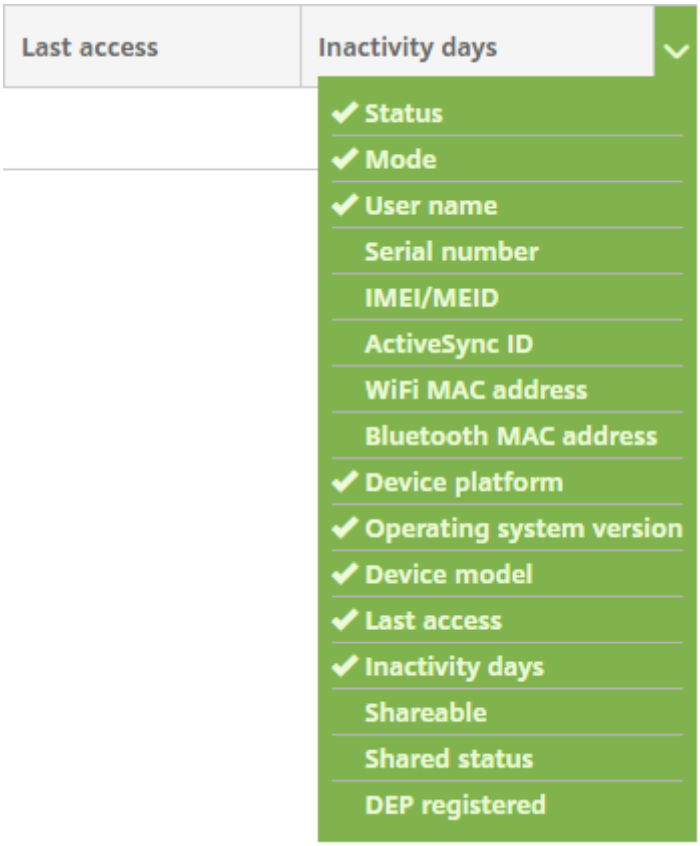
Get information about devices

The Citrix Endpoint Management database stores a list of mobile devices. To populate the Citrix Endpoint Management console with your devices, you can add the devices manually or you can import a list of devices from a file. For more information about device provisioning file formats, see Device provisioning file formats later in this article.

The **Manage > Devices** page in the Citrix Endpoint Management console lists each device and the following information:

- **Status:** Icons indicate whether the device is jailbroken, is managed, whether ActiveSync Gateway is available, and the deployment state.
- **Mode:** Indicates the device mode, such as MDM or MDM+MAM.
- Other information about the device, such as **User name**, **Device platform**, **Last access**, and **Inactivity days**. Those headings are the defaults shown.

To customize the **Devices** table, click the down arrow on the last heading. Then, select the additional headings you want to see in the table or clear any headings to remove them.



You can add devices manually, import devices from a device provisioning file, edit device details, customize the Active Directory user properties, do security actions, and send notifications to devices. You can also export all device table data to a .csv file to create a custom report. The server exports all de-

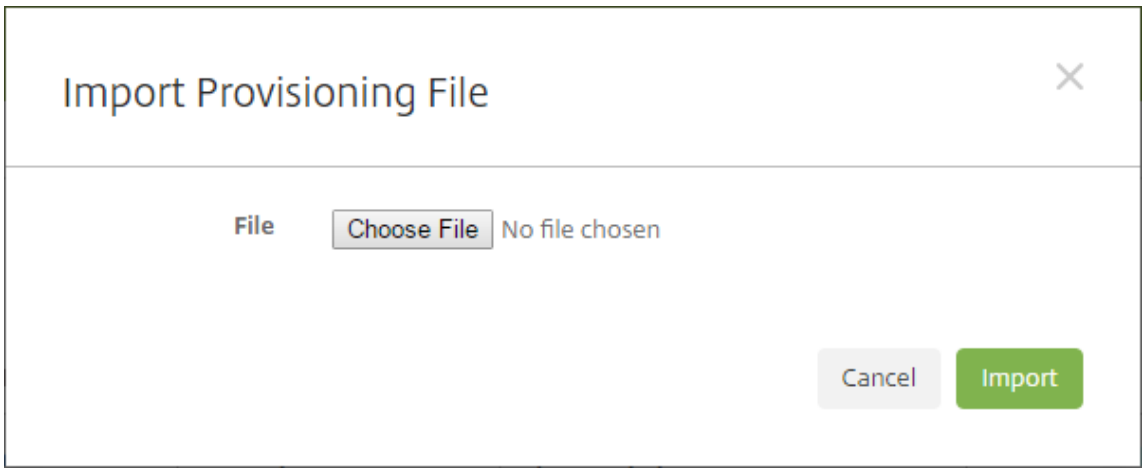
© 1997–2025 Citrix Systems, Inc. All rights reserved.

vice attributes. If you apply filters, Citrix Endpoint Management uses the filters when creating the .csv file.

Import devices from a provisioning file

You can import a file supplied by mobile operators or device manufacturers, or you can create your own device provisioning file. For details, see Device provisioning file formats later in this article.

1. Go to **Manage > Devices** and then click **Import**. The **Import Provisioning File** dialog box appears.

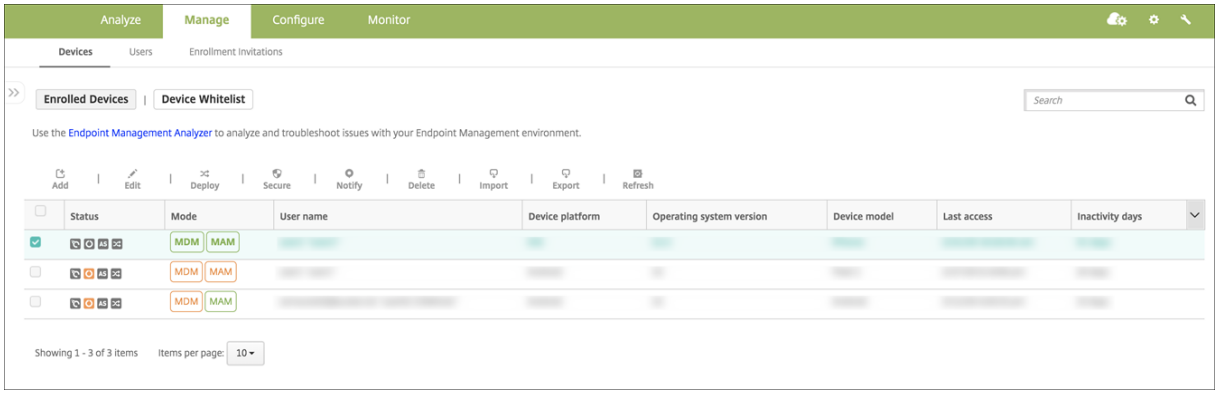


2. Click **Choose File** and then navigate to the file you want to import.
3. Click **Import**. The **Devices** table lists the imported file.
4. To edit the device information, select it and then click **Edit**. For information about the **Device details** pages, see Get information about devices.

Deploy to a device

You can force one or several devices to connect with Citrix Endpoint Management. The selected devices immediately receive resources without waiting for the next scheduled check-in.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



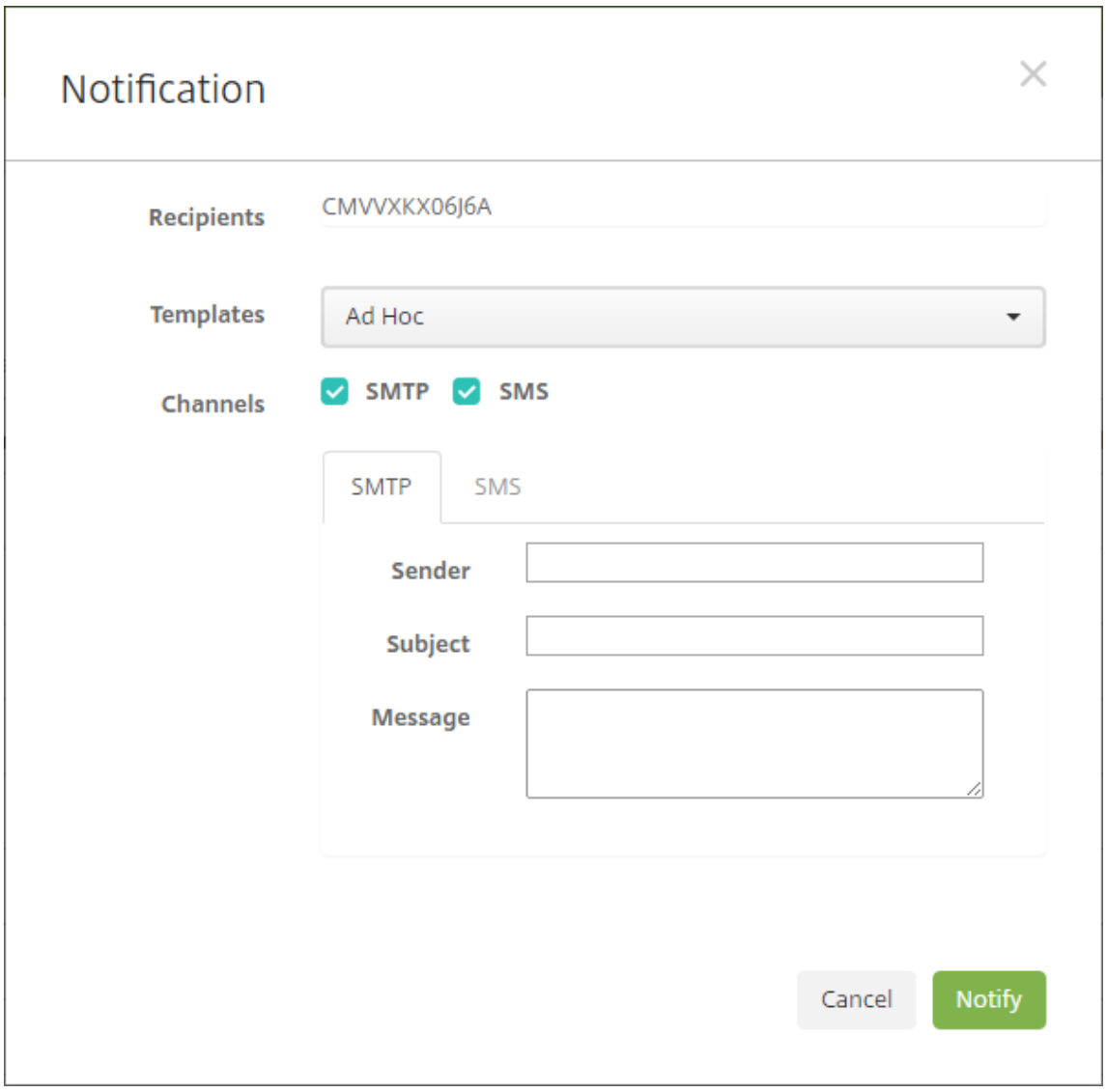
1. Go to **Manage > Devices**, select an MDM or MDM+MAM managed device, and then click **Deploy**.
2. In the dialog box, click **Deploy** to confirm your action.

Send a notification to devices

You can send notifications to devices from the Devices page. For more information about notifications, see Notifications.

1. On the **Manage > Devices** page, choose the device or devices to which you want to send a notification.
2. Click **Notify**. The **Notification** dialog box appears. The **Recipients** field lists all devices to receive the notification.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Configure these settings:

   - **Templates:** Click the type of notification that you want to send in the drop-down list. For each template except for **Ad Hoc**, the **Subject** and **Message** fields show the text configured for the template that you choose.
   - **Channels:** Select how to send the message. The default is **SMTP**. Click the tabs to see the message format for each channel.
   - **Sender:** Enter an optional sender.
   - **Subject:** Enter a subject for a **Ad Hoc** message.
   - **Message:** Enter the message for an **Ad Hoc** message.

4. Click **Notify**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Export the Devices table

1. Filter the **Devices** table according to what you want to appear in the export file.
2. Click the **Export** button above the **Devices** table. Citrix Endpoint Management extracts the information in the filtered **Devices** table and converts it to a .csv file.
3. When prompted, open or save the .csv file.

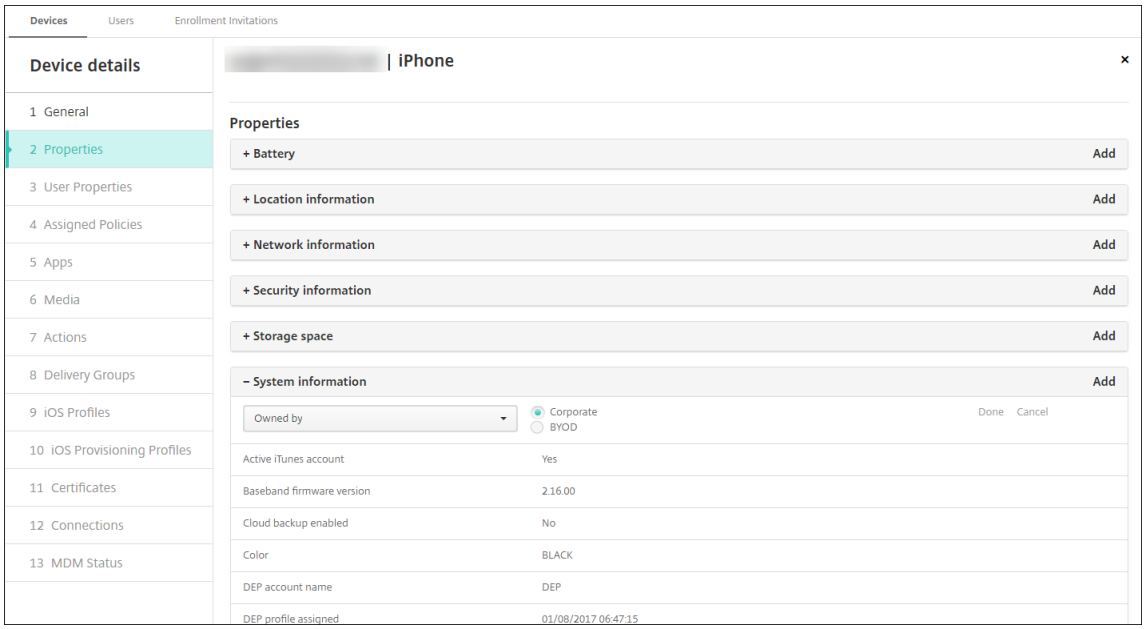
Tag user devices manually

You can manually tag a device in Citrix Endpoint Management in the following ways:

- During the invitation-based enrollment process.
- During the Self-Help Portal enrollment process.
- By adding device ownership as a device property

You have the option of tagging the device as either corporate- or employee-owned. When using the Self-Help Portal to self-enroll a device, you can tag the device as corporate- or employee-owned. You can also tag a device manually, as follows.

1. Add a property to the device from the **Devices** tab in the Citrix Endpoint Management console.
2. Add the property named **Owned by** and choose either **Corporate** or **BYOD** (employee-owned).



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Customize Active Directory user attributes

You can customize certain Active Directory user attributes to define which attributes Citrix Endpoint Management can access to create a user account.

To view the list of attributes, add the `optional.user.identity.attributes` server property as a custom key in **Settings > Server Properties**. In the **Values** field, you can remove and later restore the optional Active Directory user attributes that Citrix Endpoint Management provides by default. For more information, see Server properties.

After you edit the list of default values and save the changes, you can view the updated Active Directory user attributes in **Manage > Devices > User properties**. Citrix Endpoint Management updates the console after the user signs in to the device or during the next scheduled device check-in. If you make a spelling error or add a value that's not supported, Citrix Endpoint Management ignores your changes.

Removing the optional Active Directory user attributes can affect the following functionality:

- **Provisioning of the user account:** If you remove the first and last name values, Citrix Endpoint Management can't provision the user account for ShareFile and Salesforce.
- **Enrollment invitations:** If you remove the user's email or mobile phone details, the user can't receive an enrollment invitation.
- **Device notification actions:** If you remove the user's email details, the user can't receive the notifications through SMTP.
- **Single sign-on to Citrix Secure Mail:** If you remove the display name value, the user can't sign in to Citrix Secure Mail using single sign-on.
- **User property and deployment rules:** If you remove any of the optional attributes that you use to configure the user property and deployment rules, you can affect existing configurations.
- **Actions:** If you remove any of the optional attributes that you use to set an automated action in **Configure > Actions**, you can affect existing configurations.
- **Custom reports:** If you remove any of the optional attributes that you use in custom reports, you can affect existing configurations.

Search for devices

For fast searching, the default search scope includes the following device properties:

- Serial Number
- IMEI
- Wi-Fi MAC address
- Bluetooth MAC address
- Active Sync ID

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- User Name

You can configure the search scope through a server property **include.device.properties.during.search**, which defaults to **false**. To include all device properties in a device search, go to **Settings > Server Properties** and change the setting to **true**.

Device provisioning file formats

Many mobile operators or device manufacturers provide lists of authorized mobile devices. You can use these lists to avoid having to enter a long list of mobile devices manually. Citrix Endpoint Management supports an import file format that is common to these supported device types: Android, iOS, and Windows.

A provisioning file that you create manually must be in the following format:

```
SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;
propertyName2;propertyValue2; ... propertyNameN;propertyValueN
```

Keep in mind the following:

- For valid values for each property, see the PDF Device property names and values
- Use the UTF-8 character set.
- Use a semi-colon (;) to separate the fields within the provisioning file. If part of a field has a semi-colon, escape it with a backslash character (\).

  For example, for this property:

  ```
  propertyV;test;1;2
  ```

  Escape it as follows:

  ```
  propertyV\;test\;1\;2
  ```

- The serial number is required for iOS devices because the serial number is the iOS device identifier.
- For other device platforms, you must include either the serial number or the IMEI.
- Valid values for **OperatingSystemFamily** are **WINDOWS**, **ANDROID**, or **iOS**.

Example of a device provisioning file:

```
1 `1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;
    propertyV\;test\;1\;2;prop 2
2 2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;
    propertyV$*&&éééétest
3 3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;
4 4050BF3F5173010816100655105903 93;;iOS;test;
5 ;55244201625379903;ANDROID;test.testé;value;`
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Each line in the file describes a device. The first entry in that sample means the following:

- SerialNumber: `1050BF3F5173010816100655105903 91`
- IMEI: `15244201625379901`
- OperatingSystemFamily: `WINDOWS`
- ProertyName: `propertyN`
- PropertyValue: `propertyV\;test\;1\;2;prop 2`

Alexa for Business

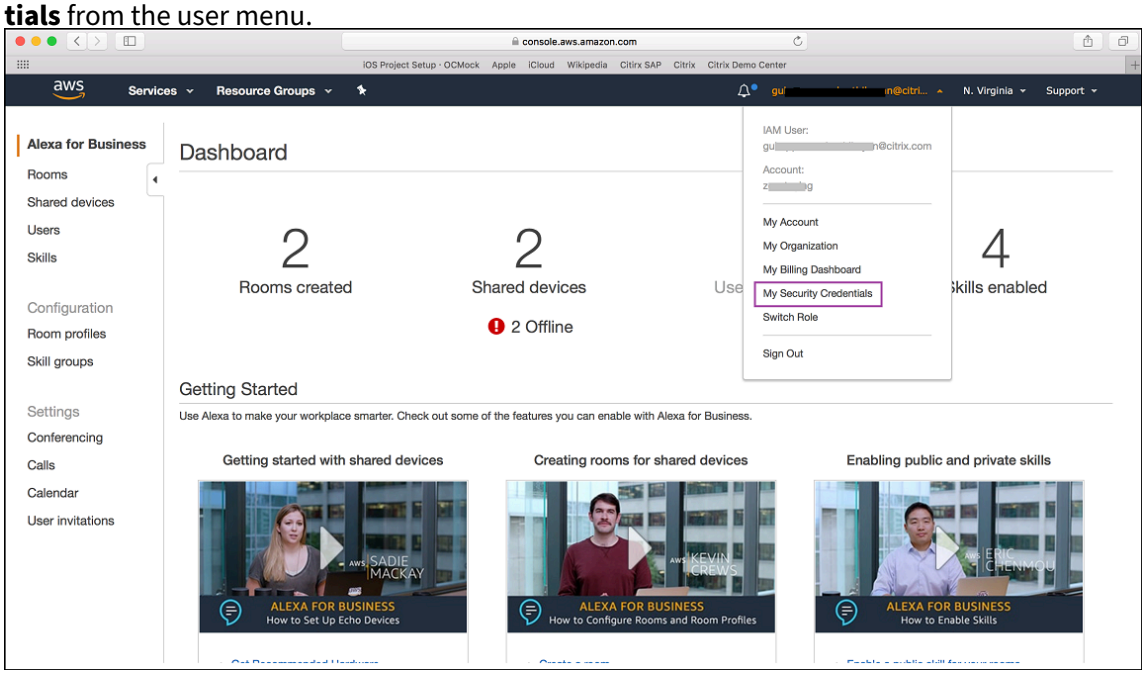
September 6, 2025

The Alexa for Business service of Amazon Web Services (AWS) lets you manage large numbers of Alexa-enabled devices for business uses, such as conference room assistance. Citrix Endpoint Management lets you configure and manage these devices in the Citrix Endpoint Management console. Citrix Endpoint Management doesn't deploy policies directly to Alexa devices. Instead, Citrix Endpoint Management updates AWS services and AWS deliver the configurations to Alexa devices.

For information about using Alexa for Business, see the Alexa for Business Administration Guide.

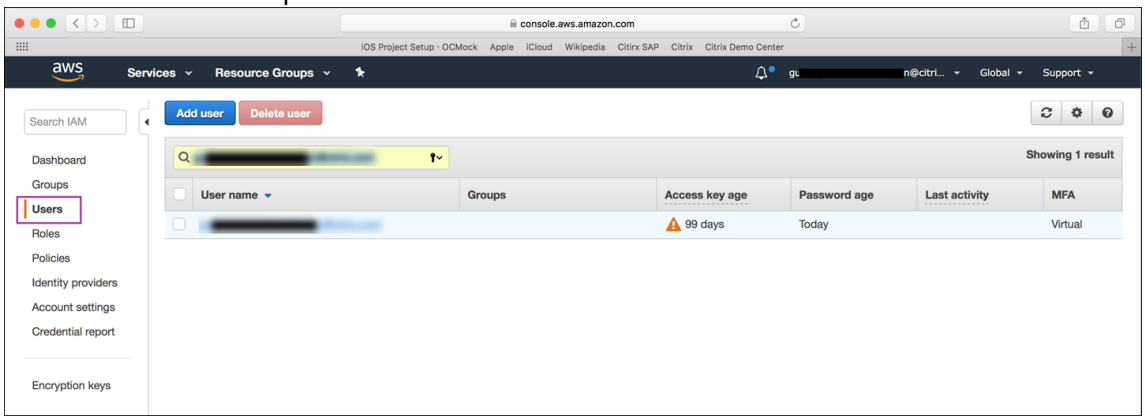
Authenticate your AWS account to Citrix Endpoint Management

1. To get your AWS account credentials, log in to the AWS console and select **My Security Credentials** from the user menu.

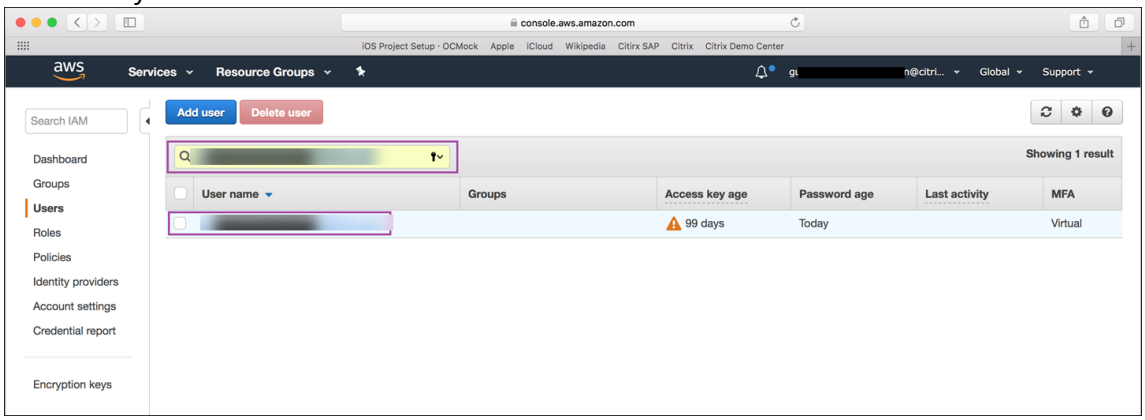


© 1997–2025 Citrix Systems, Inc. All rights reserved.

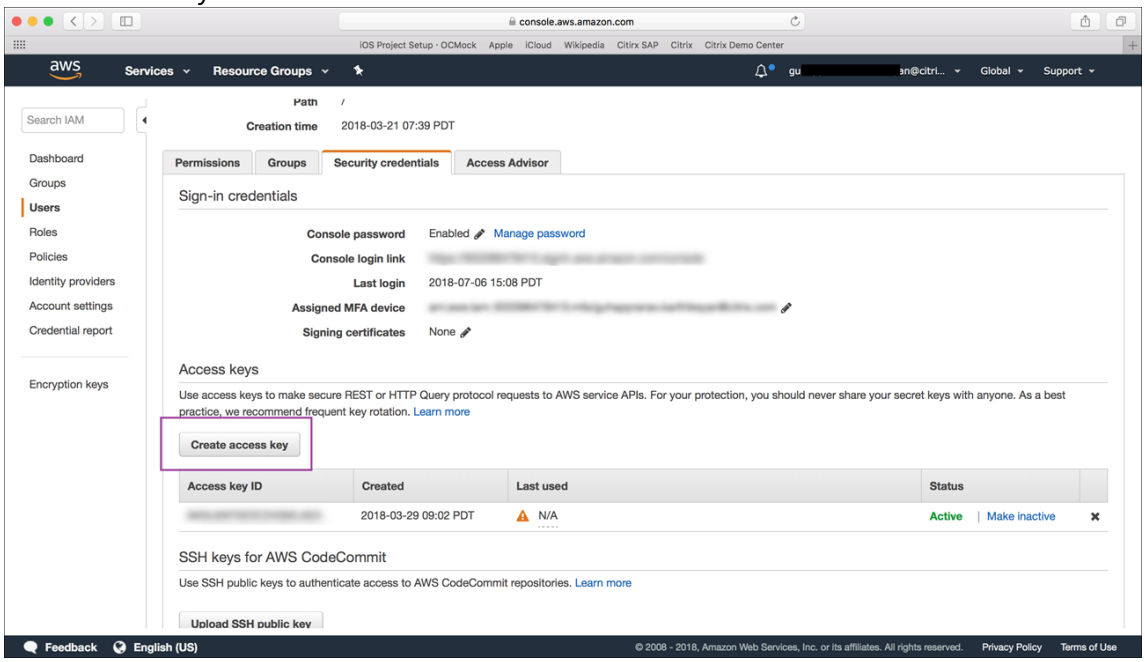
2. Select **Users** in the left panel.



3. Search for your user name and then select it.

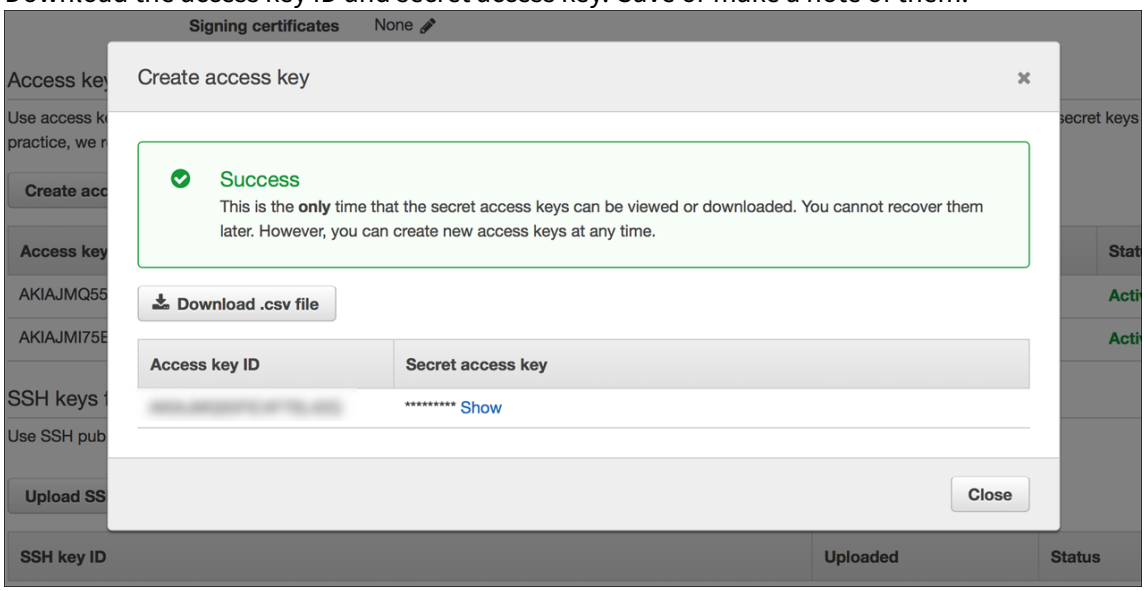


4. In the **Security Credentials** tab, click **Create access key** to generate your access key ID and secret access key.



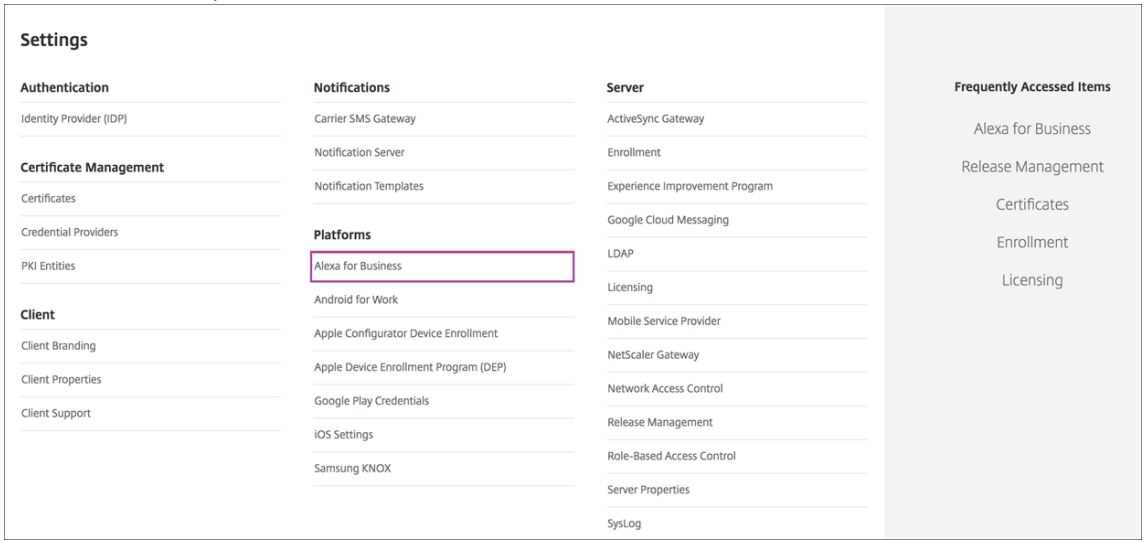
© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. Download the access key ID and secret access key. Save or make a note of them.

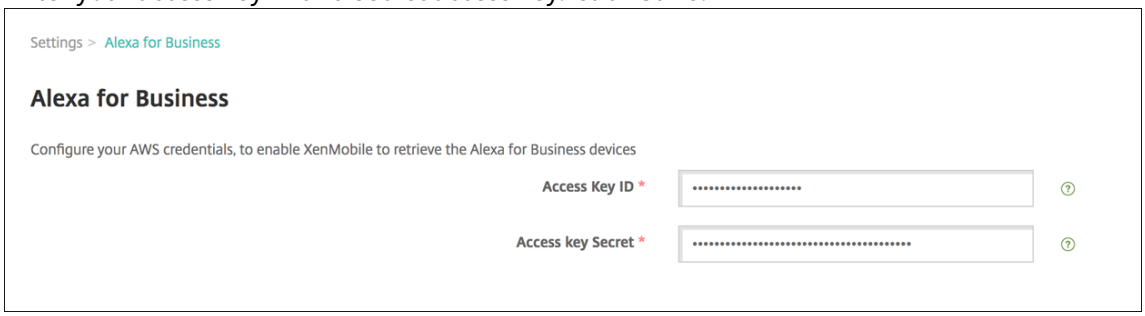


6. In the Citrix Endpoint Management console, click the gear icon to go to **Settings**.

7. Under **Platforms**, select **Alexa for Business**.



8. Enter your access key ID and secret access key. Click **Save**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure Alexa for Business on Citrix Endpoint Management

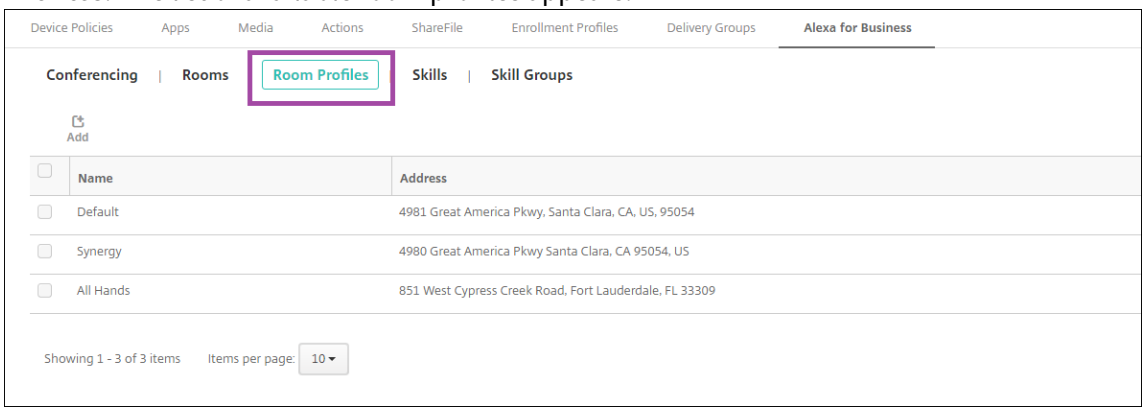
Citrix Endpoint Management lets you configure:

- Room profiles of settings that you apply to rooms that have Alexa devices
- Rooms that represent the physical rooms that have the devices
- Skill groups that you assign to rooms or devices
- Alexa skills from the Alexa skill store that can be added to skill groups
- Conferencing features that let you choose a conferencing provider and control how people schedule and join meetings in your rooms

Configure room profiles

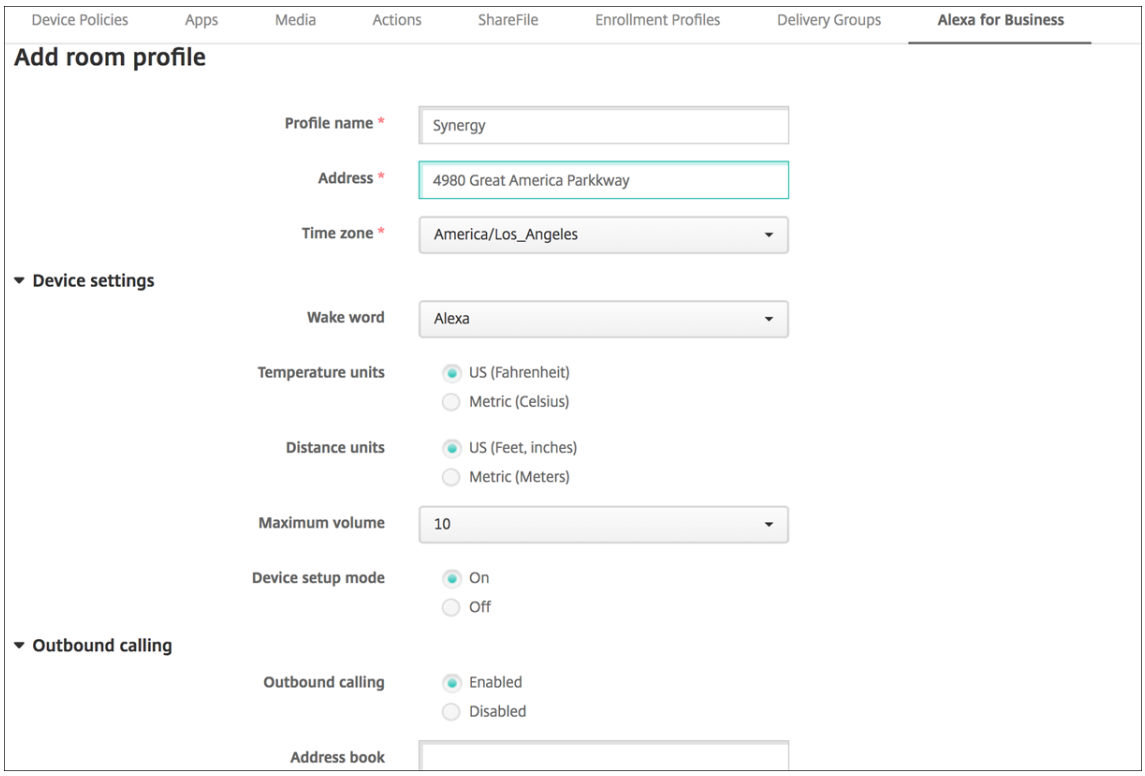
A room profile is a set of common configurations that can be applied to a collection of rooms that have Alexa devices. You can add, edit, and delete room profiles.

1. In the Citrix Endpoint Management console, select **Configure > Alexa for Business > Room Profiles**. The list of available room profiles appears.



2. To add a room profile, click **Add**. To edit a room profile, select the room profile you want to edit and click **Edit**.
3. Enter the room profile settings:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Profile Name:** Type the name of the profile.
- **Address:** Type the physical (street) address of the building where the rooms that have the Alexa devices are.
- **Time zone:** Choose the time zone of the place.
- **Wake word:** Choose the wake word that Alexa devices respond to.
- **Temperature units:** Select the units in which Alexa devices report the temperature.
- **Distance units:** Select the units in which Alexa devices report the distance.
- **Maximum volume:** Choose the maximum volume setting for Alexa.
- **Device setup mode:** Select whether the Alexa devices can be reconfigured by forcing them to the device setup mode.
- **Outbound calling:** Enable or disable the outbound calling capability of Alexa devices.
- **Address book:** Set up the address book configuration for Alexa devices.

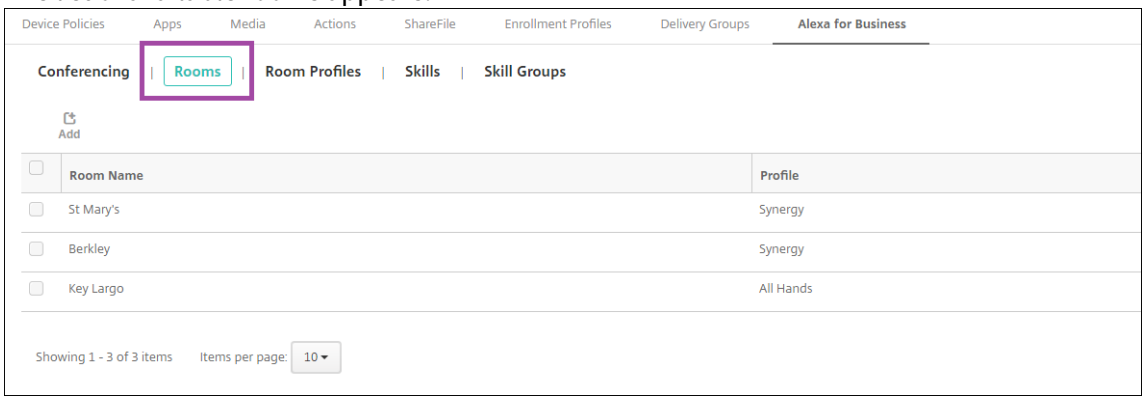
4. Click **Save**.

Configure rooms

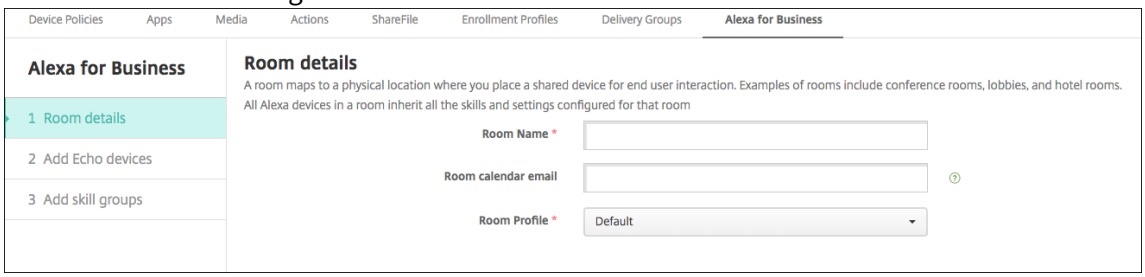
The rooms you configure in the Citrix Endpoint Management console represent the physical conference rooms, meeting rooms, and other rooms in the building. While configuring a room, you associate an Alexa device for the room and add a skills group to the device. You can add, edit, and delete rooms.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. In the Citrix Endpoint Management console, select **Configure > Alexa for Business > Rooms**. The list of available rooms appears.

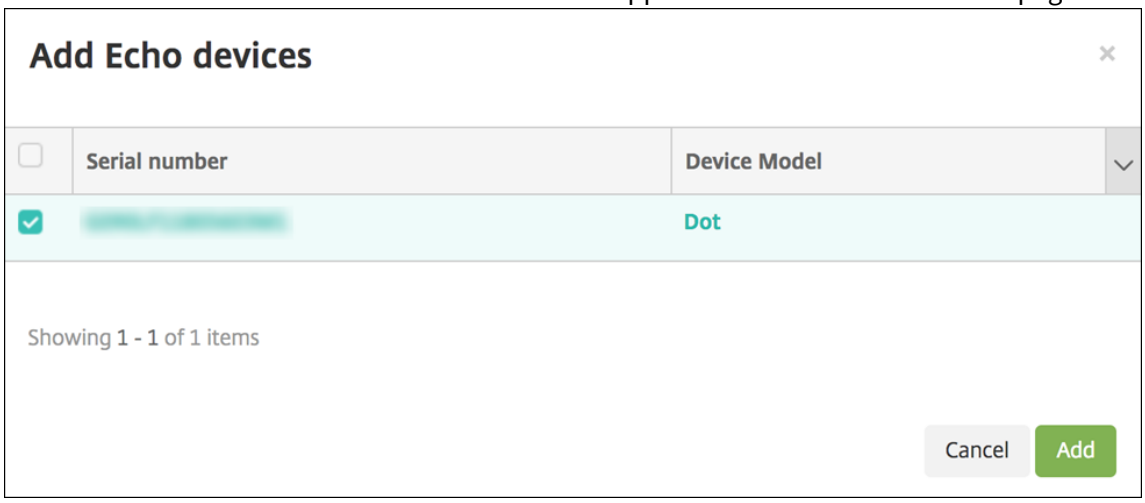


2. To add a room, click **Add**. To edit a room, select the room you want to edit and click **Edit**.
3. Enter these room settings:



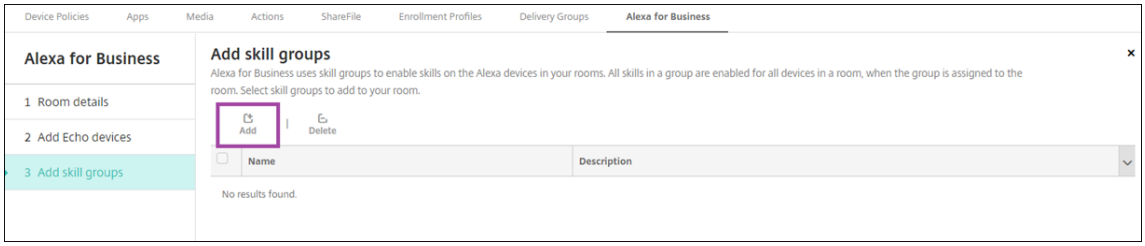
   - **Room Name:** Type the name of the conference room, meeting room, or other room.
   - **Room calendar email:** Type the calendar email address of the room.
   - **Room Profile:** Choose the name of the room profile configuration for the room.

4. Click **Next**.
5. To associate an Alexa device with the room, click **Add**.
6. Select a device and click **Add**. The selected device appears in the **Add Echo devices** page.

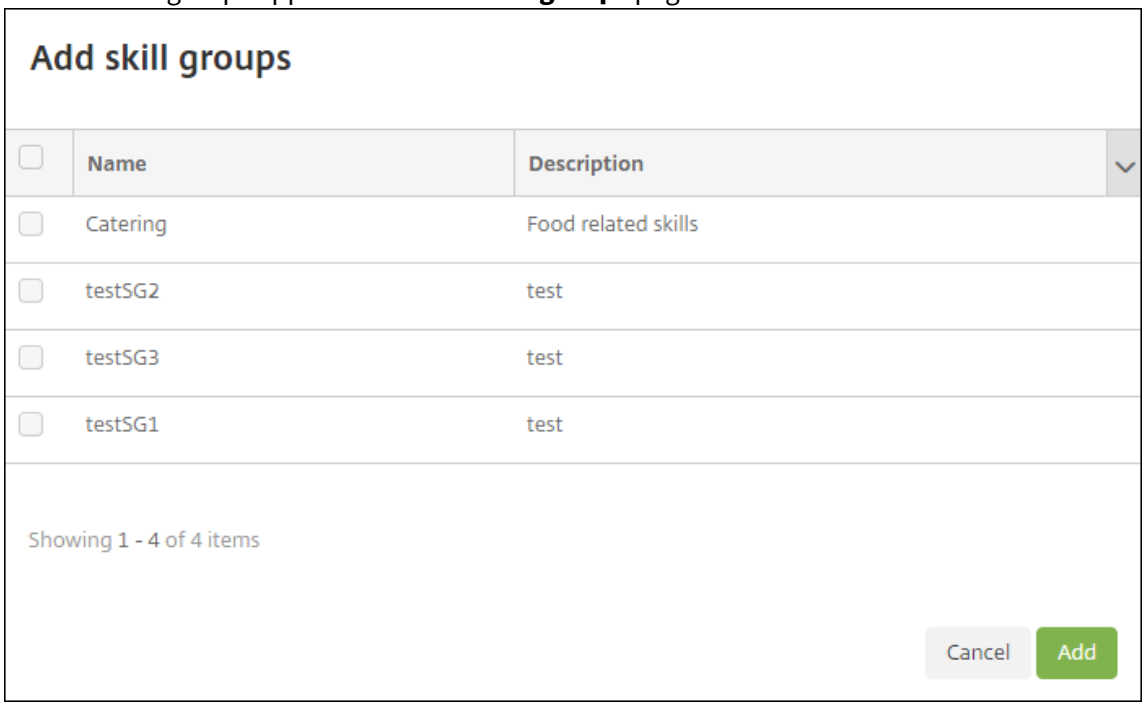


7. Click **Next**.
8. To add skill groups to the Alexa devices in the room, click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



9. Select the skill groups that you want to add to the Alexa devices in the room. Click **Add**. The selected skill groups appear in the **Add skill groups** page.



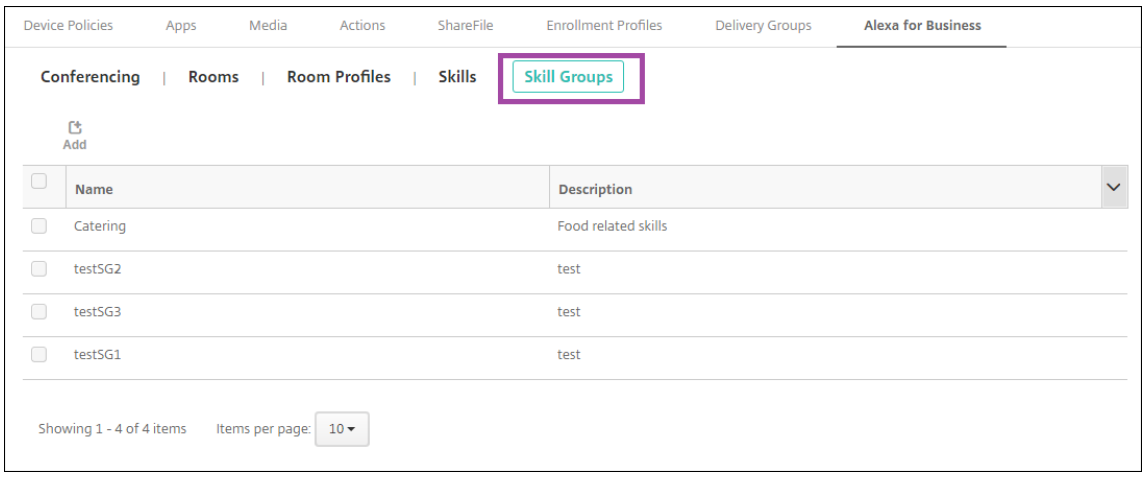
10. Click **Save**.

Configure skill groups

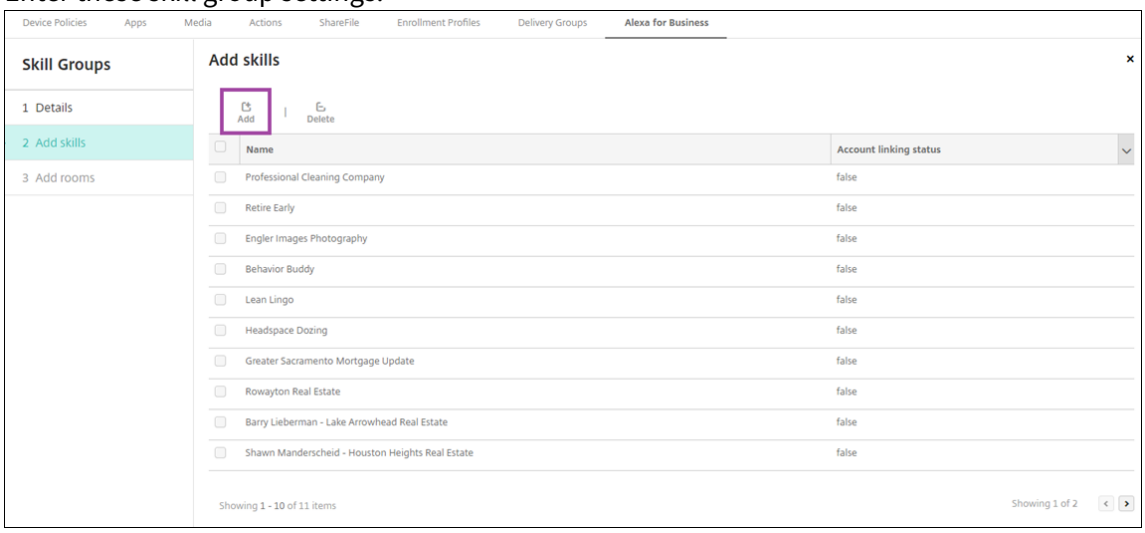
Skill groups are collections of skills that can be applied to a room. You can create a skill group and then assign it to a room. Skills let you use an Alexa device to do things like start and end an online meeting or review a list of agenda items. You can add, edit, and delete skill groups.

1. In the Citrix Endpoint Management console, select **Configure > Alexa for Business > Skill Groups**. The list of available skill groups appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



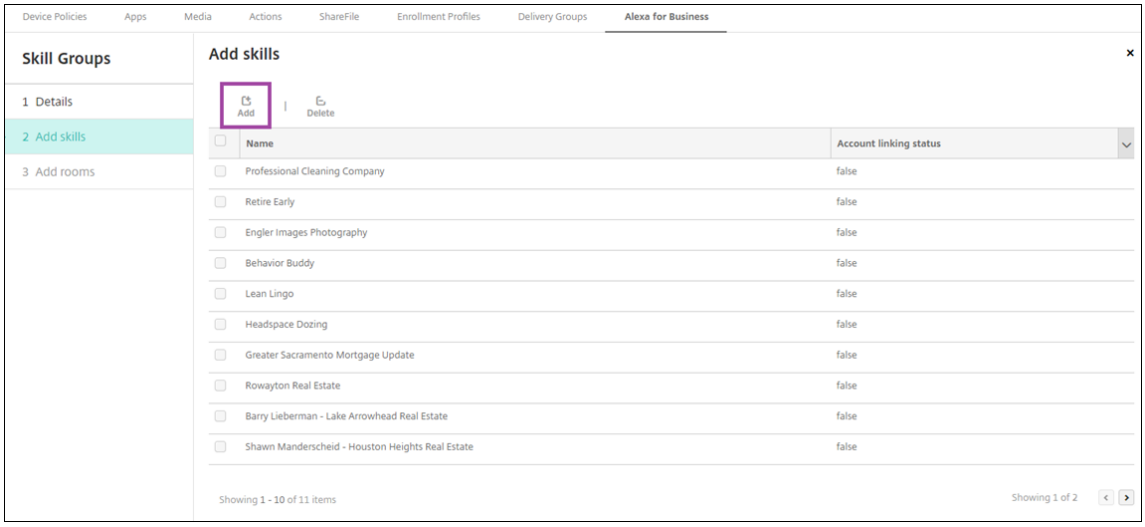
2. To add a skill group, click **Add**. To edit a skill group, select the skill group you want to edit and click **Edit**.
3. Enter these skill group settings:



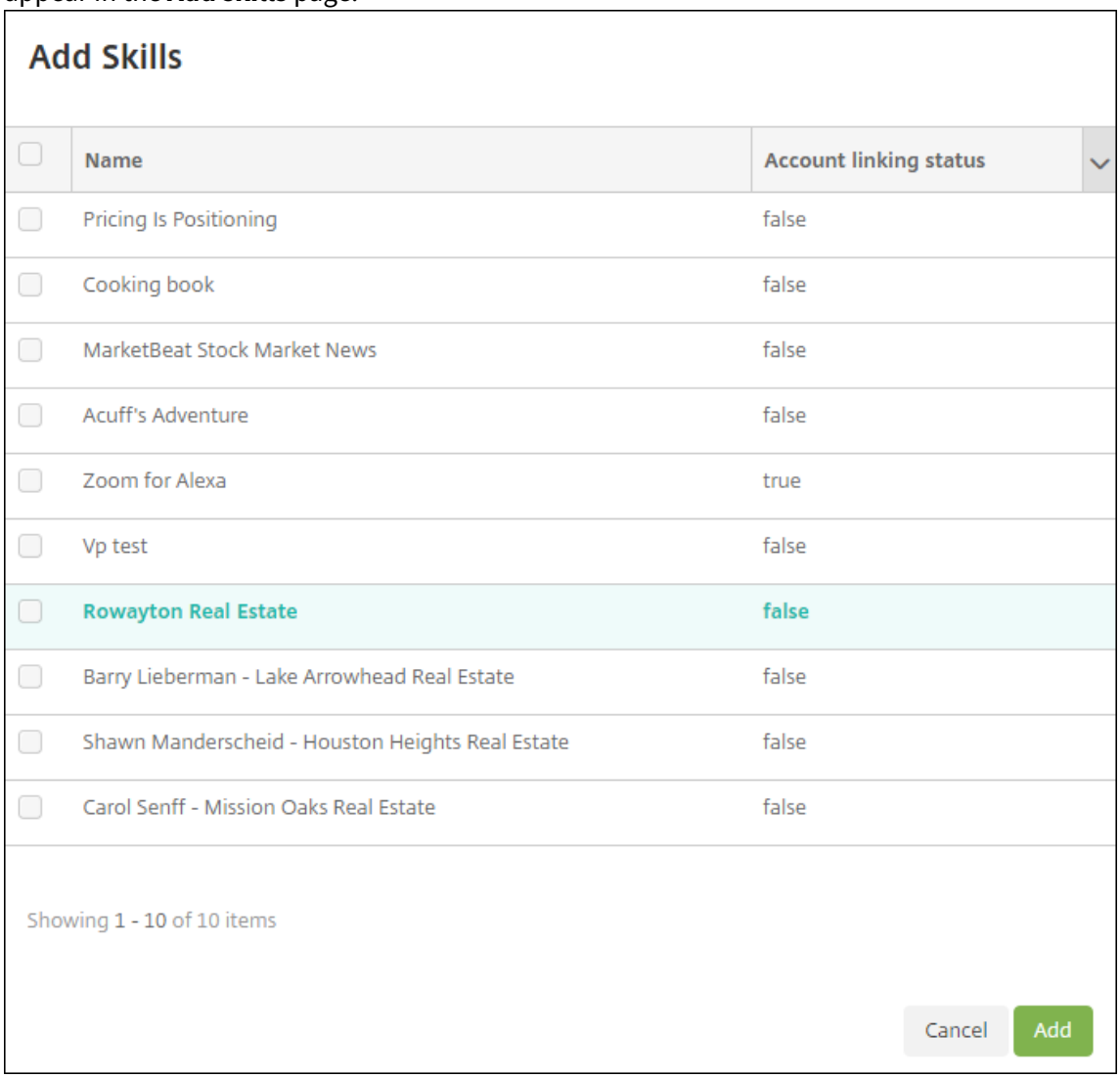
   - **Name:** Type the name of the skill group.
   - **Description:** Type a brief description of the skill group.

4. Click **Next**.
5. To add skills to the skill group, click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

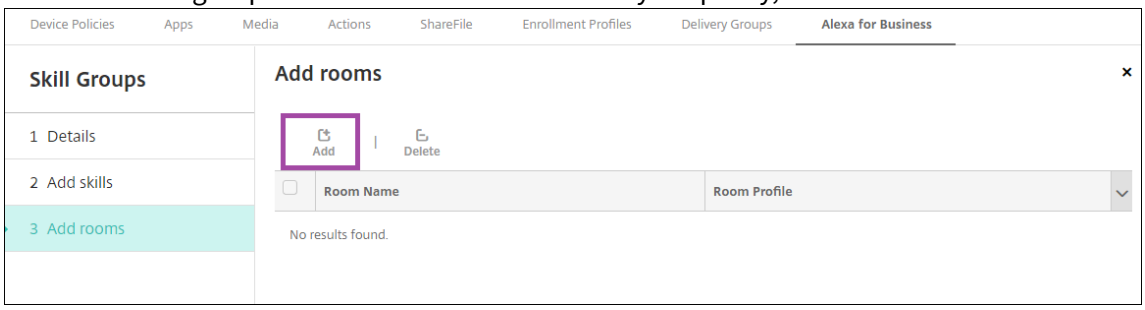


6. Select the skills that you want to include in the skill group and click **Add**. The selected skills appear in the **Add skills** page.

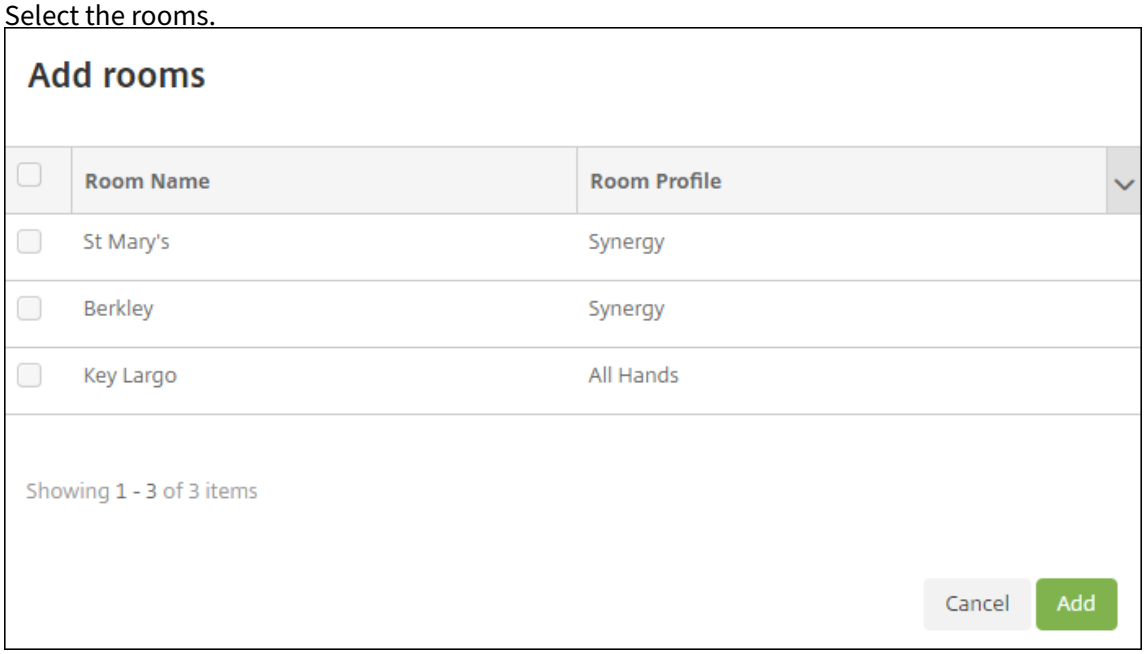


© 1997–2025 Citrix Systems, Inc. All rights reserved.

7. To add the skill group to Alexa devices in rooms that you specify, click **Add**.



8. Select the rooms.



9. Click **Save**.

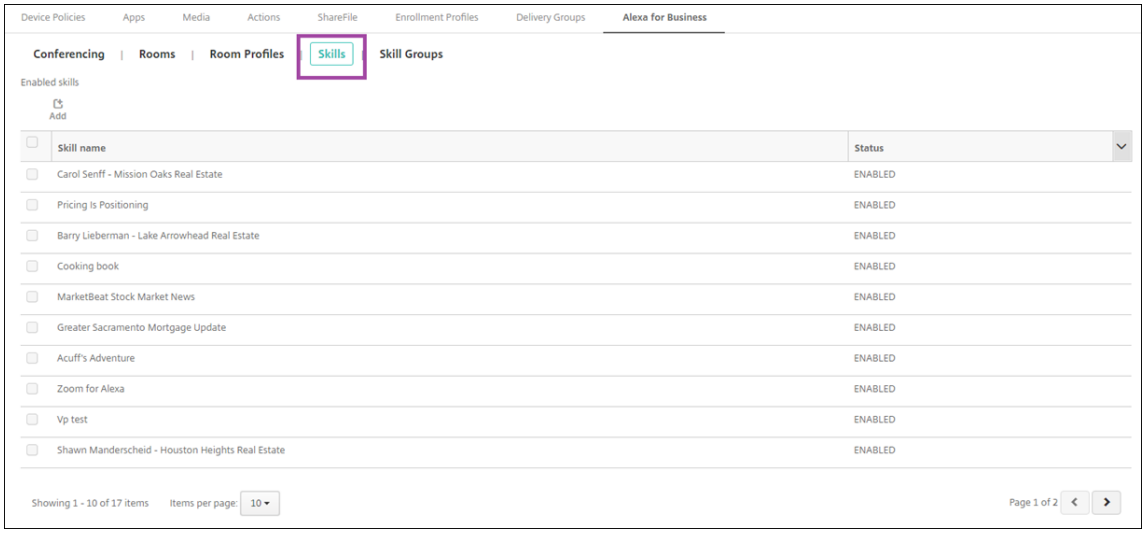
Make skills available for skill groups

You configure the list of Alexa skills available to be included in skill groups in your Alexa for Business organization. These skills are from the public Alexa skills store or private skills published to your organization.

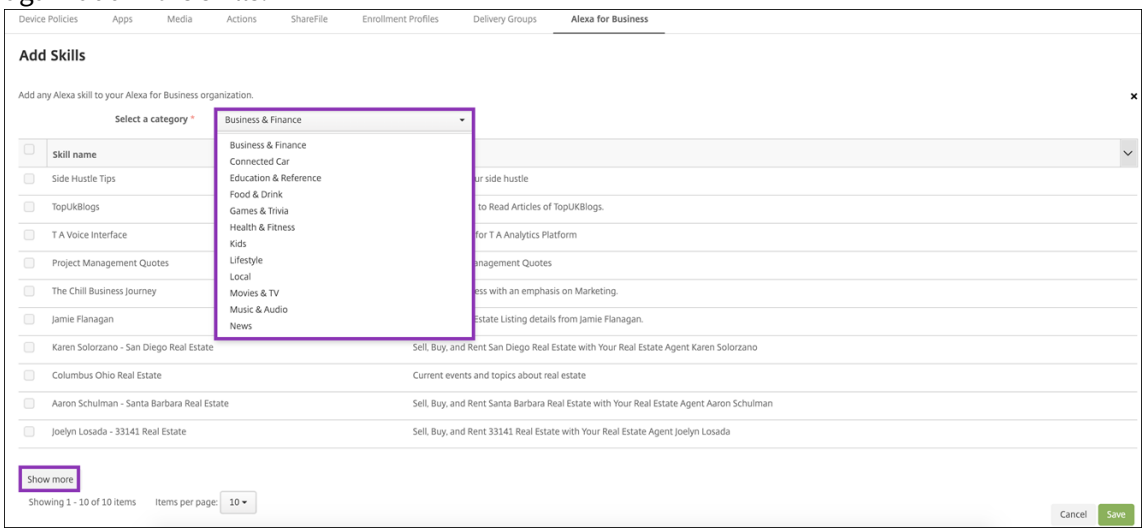
Add skills to your organization

1. In the Citrix Endpoint Management console, select **Configure > Alexa for Business > Skills**. The list of enabled skills appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. To add a skill, click **Add**.
3. To see more Alexa skills, select a category and click **Show more**. Clicking **Show more** adds up to 10 more skills to the list of skills available to add to your organization. Click **Show more** again add more skills.

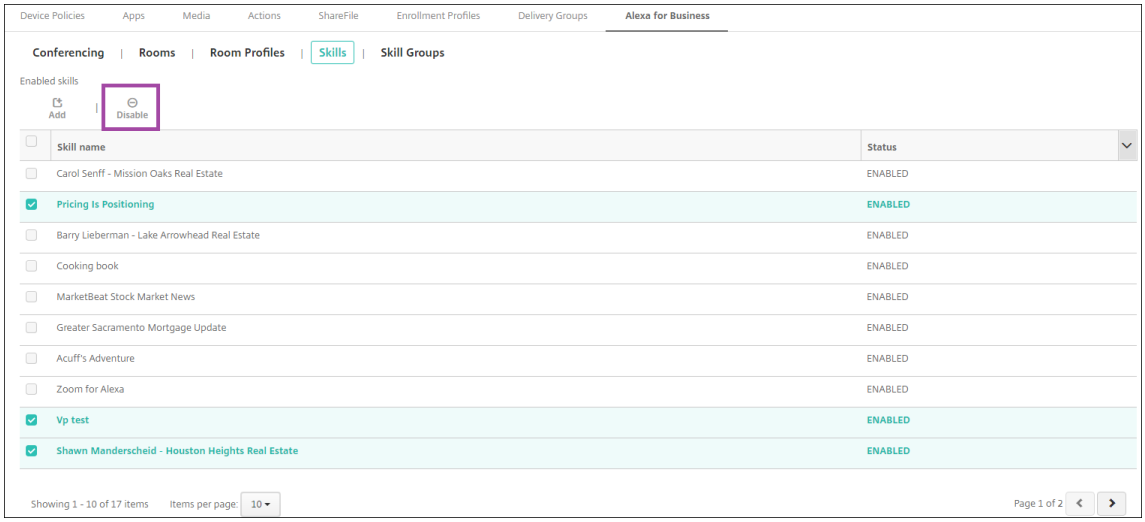


4. Select the skills that you want to add to your organization.
5. Click **Save**.

Remove skills from your organization

1. In the Citrix Endpoint Management console, select **Configure > Alexa for Business > Skills**. The list of enabled skills appears.
2. Select the skills that you want to remove from your organization.
3. Click **Disable**.

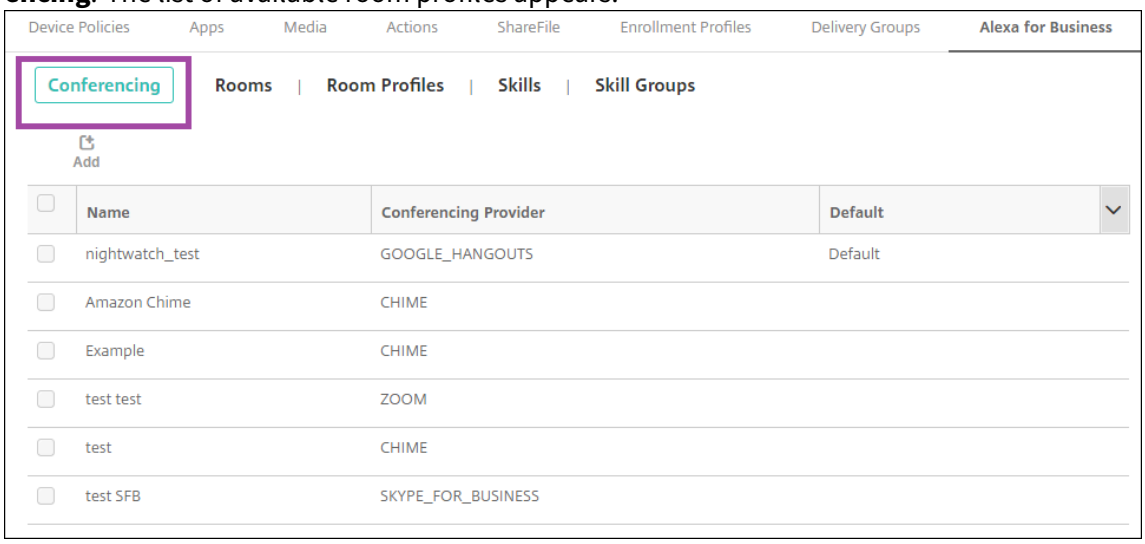
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure conferencing

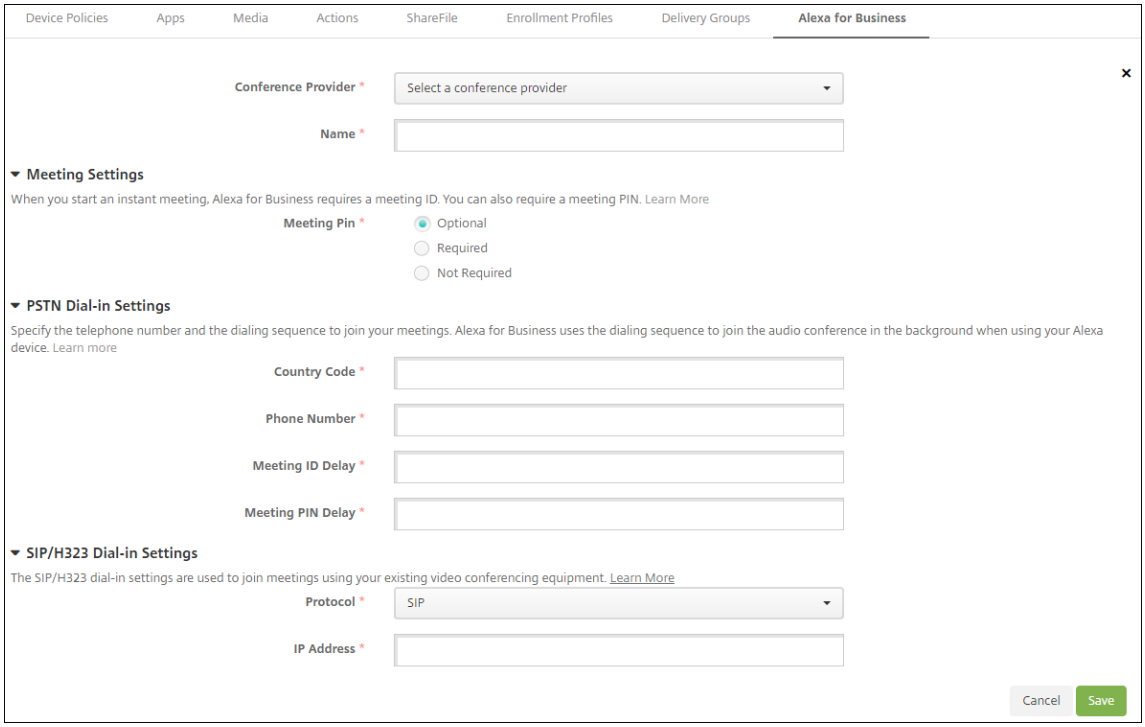
Conferencing features let you configure conferencing providers, like Google Hangout or Amazon Chime that control how people join conferences in rooms that have Alexa devices. You can add, edit, and delete conferencing providers. You can also set a default conferencing provider.

1. In the Citrix Endpoint Management console, select **Configure > Alexa for Business > Conferencing**. The list of available room profiles appears.



2. To add a conferencing provider, click **Add**. To edit a conferencing provider, select the room profile you want to edit and click **Edit**.
3. Enter the room profile settings:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Conferencing provider:** Select a conferencing provider from the list.
- **Name:** Type the name that you want to give the conferencing provider.
- **Meeting PIN:** Specify whether to require a PIN to join the meeting.
- **PSTN dial-in settings**
  - **Country code:** Type the country code.
  - **Phone number:** Type the phone number.
  - **Meeting ID delay:** Specify the number of seconds before the meeting ID is sent.
  - **Meeting PIN delay:** Specify the number of seconds before the PIN is sent.
- **SIP/H323 dial-in settings** The SIP/H323 dial-in settings are used to join meetings using your existing video conferencing equipment.
  - **Protocol:** Select a protocol.
  - **IP address:** Type the IP address.

4. Click **Save**.

If you configure more than one conferencing provider, set the default provider.

1. In the Citrix Endpoint Management console, select **Configure > Alexa for Business > Conferencing**. The list of available room profiles appears.
2. Select the conferencing provider that you want to set as the default.
3. Click **Set Default**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Migrate from device administration to Android Enterprise

September 6, 2025

This article discusses considerations and recommendations for migrating from legacy Android device administration to Android Enterprise. Google is deprecating the Android Device Administration API. That API supported enterprise apps on Android devices. Android Enterprise is the modern management solution recommended by Google and Citrix.

Citrix Endpoint Management is changing to Android Enterprise as the default enrollment method for Android devices. After Google deprecates the APIs, enrollment will fail for Android Q devices in device administration mode.

Android Enterprise includes support for fully managed and work profile device modes. The Google publication, Android Enterprise Migration Bluebook, explains in detail about how legacy device administration and Android Enterprise differ. We recommend that you read the migration information from Google.

We recommend that you also refer to the Citrix Tech Zone article, Migration from Android Device Administrator to Android Enterprise with Citrix Endpoint Management.

Impact of device administration deprecation

Google has deprecated the Device Administrator APIs and won't support them from November 2, 2020. These APIs won't work on devices running Android 10+ after we upgrade Citrix Secure Hub to target Android API level 29:

- **Disable camera:** Controls access to device cameras.
- **Keyguard features:** Controls features that are related to device locking, such as biometrics and patterns.
- **Expire password:** Forces users to change their password after a configurable time period.
- **Limit password:** Sets restrictive password requirements.

Requirements and recommendations

- If you can upgrade a device to Android 10+, you must enroll that device in Android Enterprise.
  - You must enroll Android 11 devices into Android Enterprise.
  - From September 2020, for Android 10 devices: Citrix doesn't support new enrollments or device re-enrollments into device administration mode. Devices already enrolled continue to work until November 2, 2020, as noted in the preceding section.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- For devices running Android 9 and lower, we support the legacy device administration mode. However, we recommend moving those devices to Android Enterprise as soon as possible.
- For new or existing devices enrolled in Citrix MAM-only mode, no action is needed. The deprecated Google APIs have no impact on devices in MAM-only mode. However, with the move to platform encryption, we highly recommend moving from MAM-only mode to Android Enterprise work profile mode (BYOD). Work profile mode provides MAM functionality, but in a container on the device.

Analysis

The analysis phase of migration consists of:

- Understanding your legacy Android setup
- Documenting your legacy setup so you can map legacy features to Android Enterprise features

Recommended analysis

1. Evaluate Android Enterprise on Citrix Endpoint Management: Fully managed, fully managed with work profile, dedicated device, work profile (BYOD).
2. Analyze your current device administration features against Android Enterprise.
3. Document your device administration use cases.

To document your device administration use cases:

1. Create a spreadsheet and list the current policy groups in your Citrix Endpoint Management console.
2. Create separate use cases based on the existing policy groups.
3. For each use case, document the following:
    - Name
    - Business owner
    - User identity model
    - Device Requirements
        - Security
        - Management
        - Usability
    - Device inventory
        - Make and model

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    - OS Version
  - Apps

4. For each app, list:

   - App name
   - Package name
   - Hosting method
   - Whether the app is public or private
   - Whether the app is mandatory (true/false)

Requirements mapping

Based on the completed analysis, determine your Android Enterprise feature requirements.

Recommended requirements mapping

1. Determine the management mode and enrollment method:

   - Work profile (BYOD): Requires re-enrollment. No factory reset needed.
   - Fully managed: Requires factory reset. Enroll devices by using QR code, Near field communication (NFC) bump, device policy controller (DPC) identifier, zero touch.

2. Create an app migration strategy.
3. Map use case requirements to Android Enterprise features. Document the feature for each device requirement that most closely matches the requirement and its corresponding Android version.
4. Determine the minimum Android OS based on feature requirements (7.0, 8.0, 9.0).
5. Choose an identity model:

   - Recommended: Managed Google Play Account
   - Use Google Workspace accounts only if you're a Google Cloud Identity Customer

6. Create a device strategy:

   - No action: If devices meet the minimum OS level
   - Upgrade: If devices support and can be updated to the supported OS
   - Replace: If devices can't be updated to the supported OS level

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Recommended app migration strategy

After you complete the requirements mapping, move the apps from the Android platform to the Android Enterprise platform. For details about publishing apps, see Add apps.

- Public store apps

  1. Select the apps to migrate and then edit the apps to clear the Google Play setting and select **Android Enterprise** as the platform.
  2. Select the delivery group. If an app is mandatory, move the app to the **Required Apps** list in the delivery group.

  After you save an app, it appears in the Google Play Store. If you have a work profile, apps appear in the Google Play Store in the work profile.

- Private (enterprise) apps

  Private apps are developed in-house or by a third-party developer. We recommend that you publish private apps by using Google Play.

  1. Select the apps to migrate and then edit the apps to select **Android Enterprise** as the platform.
  2. Upload the APK file and then configure the app settings.
  3. Publish the app to the required delivery group.

- MDX apps

  1. Select the apps to migrate and then edit the apps to select **Android Enterprise** as the platform.
  2. Upload the MDX File. Go through the app approval process.
  3. Select the MDX policies.

  For Enterprise MDX apps, we recommend changing them to MDX SDK mode wrapped apps:

  - Option 1: Host the APK in Google Play with a developer account assigned privately to your organization. Publish the MDX file in Citrix Endpoint Management.
  - Option 2: Publish the app from Citrix Endpoint Management as an enterprise app. Publish the APK in Citrix Endpoint Management and select the platform **Android Enterprise** for the MDX file.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix device policy migration

For policies that are available for both the **Android (legacy DA)** and **Android Enterprise** platforms: Edit the policy and select the platform **Android Enterprise**.

- For Android Enterprise, consider the device enrollment method. Some policy options are available only for devices in work profile mode or fully managed mode. See Configure Android Enterprise device and app policies.
- If you use the Exchange device policy for legacy DA devices, create a Managed configurations policy device policy instead to configure email settings.
- To make sure that you target a policy to the intended devices (Android Enterprise versus legacy DA), add a deployment rule to the policy. For example, for the legacy DA platform, use this deployment rule:

```
Limit by known device property name Android Enterprise
Enabled Device? Isn't equal to true
```

That deployment rule checks if the device is NOT enabled for Android Enterprise and delivers the policy along with the apps to devices enabled for legacy DA.

Proof of concept

After you migrate the apps to Android Enterprise, you can set up a migration test to verify that the features are working as intended.

Recommended proof-of-concept setup

1. Set up the deployment infrastructure:
   - Create a Delivery Group for your Android Enterprise testing.
   - Configure Android Enterprise in Citrix Endpoint Management.
2. Set up user apps.
3. Configure Android Enterprise features.
4. Assign policies to the Android Enterprise delivery group.
5. Test and confirm features.
6. Complete a device setup walkthrough for each use case.
7. Document user setup steps.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Deployment

You can now deploy your Android Enterprise setup and prepare your users for migration.

Recommended deployment strategy

The recommended Citrix deployment strategy is to test all of your production systems for Android Enterprise, then complete device migration later.

- In this scenario, users continue to use legacy devices with their current configuration. You set up new devices for Android Enterprise management.
- Migrate existing devices only when an upgrade or replacement is necessary.
- Migrate existing devices to Android Enterprise management at the end of their usual lifecycle. Or, migrate those devices when they need replacement because of loss or breakage.

Android Enterprise

September 6, 2025

Android Enterprise is a set of tools and services provided by Google as an enterprise management solution for Android devices. With Android Enterprise:

- You use Citrix Endpoint Management to manage company-owned and bring your own device (BYOD) Android devices.
- You can manage the entire device or a separate profile on the device. The separate profile isolates business accounts, apps, and data from personal accounts, apps, and data.
- You can also manage devices dedicated to a single use, such as inventory management. For an overview from Google of what Android Enterprise can do, see Android Enterprise Management.

Resources:

- For a list of terms and definitions related to Android Enterprise, see the Google Android Enterprise developers guide article, Android Enterprise terminology. Google updates these terms frequently.
- For a list of Android operating systems supported for Citrix Endpoint Management, see Supported device operating systems.
- For information about the outbound connections to consider when setting up network environments for Android Enterprise, see the Google support article, Android Enterprise Network Requirements.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- For information about deploying Android Enterprise, see Deploy resources).

Getting started with Android Enterprise

> **Important:**
>
> Device administration mode is no longer supported. If your users have devices in device administration mode, see Migrate from device administration to Android Enterprise. After your devices are migrated to Android Enterprise, use the following steps to set up Android Enterprise devices.

One-time setup

1. Create a managed Google Play account.

   See Using managed Google Play with Citrix Endpoint Management and Requirements.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Bind your Google Play account to Citrix Endpoint Management.

   See Connecting Citrix Endpoint Management to Google Play.

3. Plan how you want to manage devices.

   See Device deployment scenarios and profiles.

4. Plan enrollment security for user devices.

   See Enrollment security.

5. Prepare to deliver MDX-enabled apps.

   Use the MAM SDK to develop apps. Or, if you aren't ready to transition to the new SDK, use the command-line based MDX Toolkit to wrap the apps.

   See MAM SDK overview.

At this point, you're prepared to configure your Android Enterprise devices with app and devices policies, enrollment profiles, and apps. See the following section for guidance.

Configure devices

1. Create delivery groups.

   Control who gets what resources and when they get them. See Deploy resources.

   We stop delivering apps published for the legacy DA platform to devices enrolled in Android Enterprise. For Android Enterprise devices, publish apps for the Android Enterprise platform. To continue to publish legacy DA apps to devices in DA mode, create a separate delivery group for those apps. See Deprecation.

2. Add apps. You can approve the apps in Google Play directly from the Citrix Endpoint Management console.

   See the Google support article, Manage apps in your organization.

3. Create enrollment profiles.

   Specify device and app management enrollment options. See Device deployment scenarios and profiles and Creating enrollment profiles.

   - When you deploy an Android Enterprise public app store app to an Android device user, that user is automatically enrolled in Android Enterprise.
   - Zero-touch enrollment allows you to configure devices to enroll automatically when they're first powered on. See Zero-touch enrollment.

4. Configure device and app policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Balance enterprise security with user privacy and user experience. See Configure Android Enterprise device and app policies.

5. Distribute apps.

   You use managed Google Play to add, buy, and approve apps for deployment to the Android Enterprise workspace on a device. Users can only install apps from managed Google Play that you make available for them.

   See:

   - Distribute Android Enterprise apps
   - Managed configurations policy
   - App permissions policy

6. Configure security actions to monitor and provide compliance.

   See Security actions.

Using managed Google Play with Citrix Endpoint Management

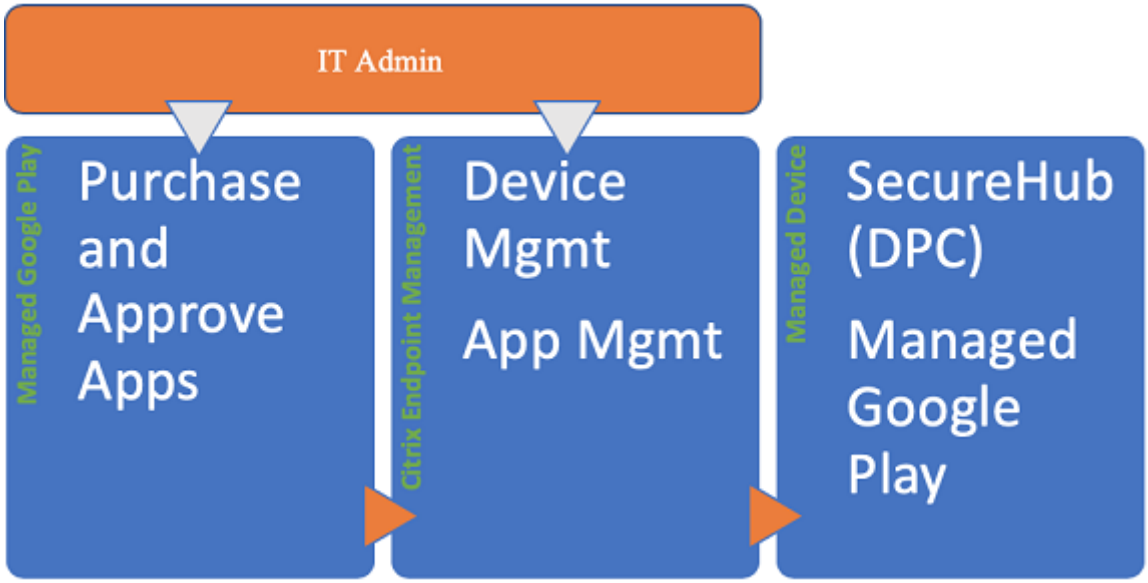
When you integrate Citrix Endpoint Management with managed Google Play to use Android Enterprise, you create an enterprise. Google defines an enterprise as binding between the organization and your enterprise mobile management (EMM) solution. All the users and devices that the organization manages through your solution belong to its enterprise.

An enterprise for Android Enterprise has three components: an EMM solution, a device policy controller (DPC) app, and a Google enterprise app platform. When you integrate Citrix Endpoint Management with Android Enterprise, the complete solution has these components:

- **Citrix Endpoint Management:** The Citrix EMM. Citrix Endpoint Management is the unified Citrix Endpoint Management for a secure digital workspace. Citrix Endpoint Management provides the means for IT administrators to manage devices and apps for their organizations.
- **Citrix Secure Hub:** The Citrix DPC app. Citrix Secure Hub is the launchpad for Citrix Endpoint Management. Citrix Secure Hub enforces policies on the device.
- **Managed Google Play:** A Google enterprise app platform that integrates with Citrix Endpoint Management. The Google Play EMM API sets app policies and distributes apps.

This illustration shows how administrators interact with these components and how the components interact with each other:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> You can use either managed Google Play or Google Workspace (formerly G Suite) to register Citrix as your EMM provider. This article discusses using Android Enterprise with managed Google Play. If your organization uses Google Workspace to provide access to apps, you can use it with Android Enterprise. See Legacy Android Enterprise for Google Workspace customers.

When you use managed Google Play, provision managed Google Play Accounts for devices and end users. Managed Google Play Accounts provide access to managed Google Play, allowing users to install and use the apps you make available. If your organization uses a third-party identity service, you can link managed Google Play Accounts with your existing identity accounts.

Because this type of enterprise isn't tied to a domain, you can create more than one enterprise for a single organization. For example, each department or region within an organization can enroll as a different enterprise. Using different enterprises lets you manage separate sets of devices and apps.

For Citrix Endpoint Management administrators, managed Google Play combines the user experience and app store features of Google Play with a set of management features designed for enterprises. You use managed Google Play to add, buy, and approve apps for deployment to the Android Enterprise workspace on a device. You can use Google Play to deploy public apps, private apps, and third-party apps.

For users of managed devices, managed Google Play is the enterprise app store. Users can browse apps, view app details, and install them. Unlike the public version of Google Play, users can only install apps from managed Google Play that you make available for them.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device deployment scenarios and profiles

Device deployment scenarios refer to who owns the devices you deploy and how you manage them. Device profiles refer to how the DPC manages and enforces policies on devices.

A work profile isolates business accounts, apps, and data from personal accounts, apps, and data. Work profiles and personal profiles are separated at an OS level. For more details about work profiles, see What is a work profile.

> **Important:**
>
> When Android Enterprise devices update to Android 11, Google migrates devices managed as "fully managed with a work profile" to a new security-enhanced work profile experience. The new enrollment mode is called "work profile on corporate-owned devices." For more information, see Changes ahead for Android Enterprise's Fully Managed with Work Profile.
> For Android 12 devices, see Security and privacy enhancements for work profile.

Device management	Use cases	Work profile	Personal profile	Notes
Company-owned devices (fully managed)	Company-owned devices intended only for work use	No	No	For new or factory reset devices only. See Provisioning Android Enterprise fully managed devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device management	Use cases	Work profile	Personal profile	Notes
Fully managed with a work profile / Work profile on corporate-owned devices	Company-owned devices intended for work and personal use	Yes	Yes. Two copies of the DPC run on these devices: One manages the device in device owner mode and the other manages the work profile in profile owner mode. You can apply separate policies to the device and the work profile.	See Provisioning Android Enterprise fully managed devices with a work profile or work profile on corporate-owned devices.
Dedicated devices*	Company-owned devices configured for a single use case, such as digital signage or ticket printing	No	No	See Provisioning dedicated Android Enterprise devices.
BYOD work profile**	Personal devices enrolled with work profile management (also known as profile owner mode)	Yes	Yes. The DPC manages only the work profile, not the whole device.	These devices don't need to be new or factory reset. See Provisioning Android Enterprise work profile devices.

* Users can share a dedicated device. When a user signs on to an app on a dedicated device, the state of their work is with the app, not the device.

** Citrix Endpoint Management does not support Zebra devices as in BYOD work profile mode. Citrix Endpoint Management supports Zebra devices as fully managed devices using Android Enterprise.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Enrollment security

Enrollment profiles determine whether Android devices enroll in MAM, MDM, or MDM+MAM, with the option for users to opt out of MDM.

For information about specifying the level of security and required enrollment steps, see User accounts, roles, and enrollment.

Citrix Endpoint Management supports the following authentication methods for Android devices enrolled in MDM or MDM+MAM. For information, see the following articles:

- Domain or domain plus security token authentication
- Client certificate or certificate plus domain authentication
- Identity providers:
  - Authentication with Azure Active Directory through Citrix Cloud (Preview)
  - Authentication with Okta through Citrix Cloud (Preview)

A rarely used authentication method is a client certificate plus security token. For information, see https://support.citrix.com/article/CTX215200.

Requirements

Before you start using Android Enterprise, you need:

- Accounts and credentials:
  - To set up Android Enterprise with managed Google Play, a corporate Google account
  - To download the latest MDX files, a Citrix® customer account
- Firebase Cloud Messaging (FCM) and a Connection scheduling device policy configured for Citrix Endpoint Management. See Firebase Cloud Messaging and Connection scheduling device policy.

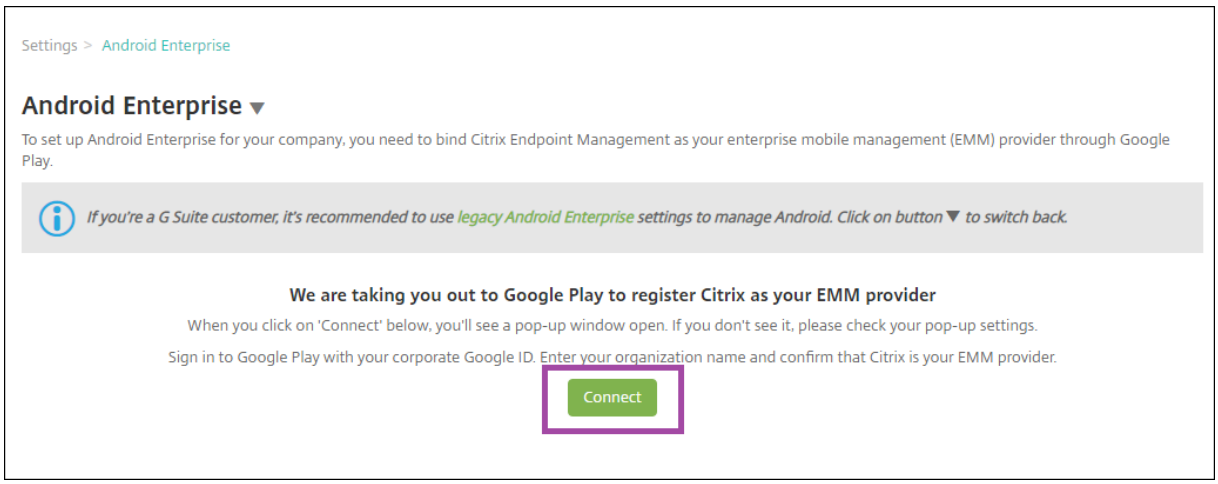
Connecting Citrix Endpoint Management to Google Play

To set up Android Enterprise for your organization, register Citrix as your EMM provider through managed Google Play. That setup connects managed Google Play to Citrix Endpoint Management and creates an enterprise for Android Enterprise in Citrix Endpoint Management.

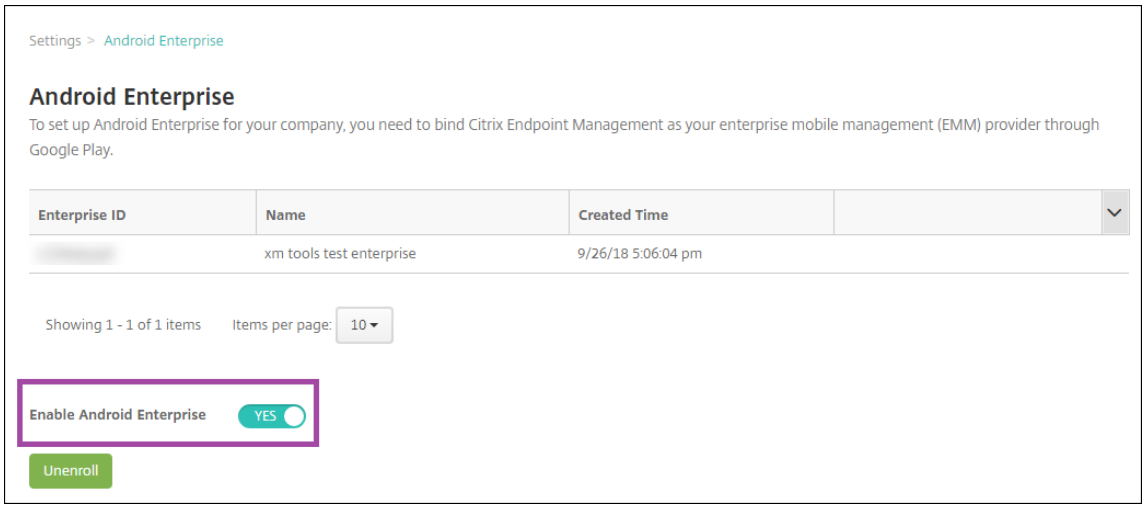
You need a corporate Google account to sign in to Google Play.

1. In the Citrix Endpoint Management console, go to **Settings > Android Enterprise**.
2. Click **Connect**. Google Play opens.

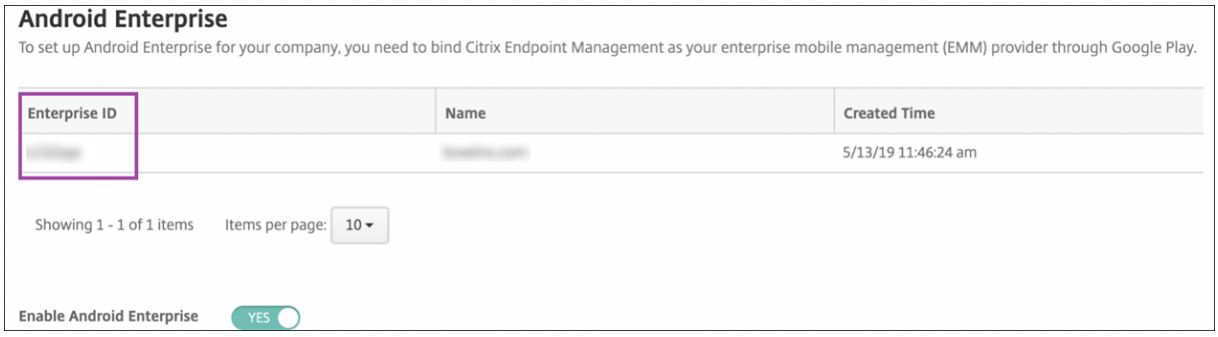
© 1997–2025 Citrix Systems, Inc. All rights reserved.



1. Sign in to Google Play with your corporate Google account credentials. Enter your organization name and confirm that Citrix is your EMM provider.
2. An enterprise ID is added for Android Enterprise. To enable Android Enterprise, slide **Enable Android Enterprise** to **Yes**.



Your Enterprise ID appears in the Citrix Endpoint Management console.



Your environment is connected to Google and is ready to manage the devices. You can now provide apps for users.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management can provide users with Citrix mobile productivity apps, MDX apps, public app store apps, web and SaaS apps, enterprise apps, and web links. For more information on giving these types of apps to users, see Distribute Android Enterprise apps.

The following section shows how to provide mobile productivity apps.

Providing Citrix mobile productivity apps to Android Enterprise users

Giving Citrix mobile productivity apps to Android Enterprise users requires these steps.

1. Publish the apps as MDX apps. See Configure apps as MDX apps.
2. Configure the rules for the security challenges your users use to access the work profiles on their devices. See Configure security challenge policy.

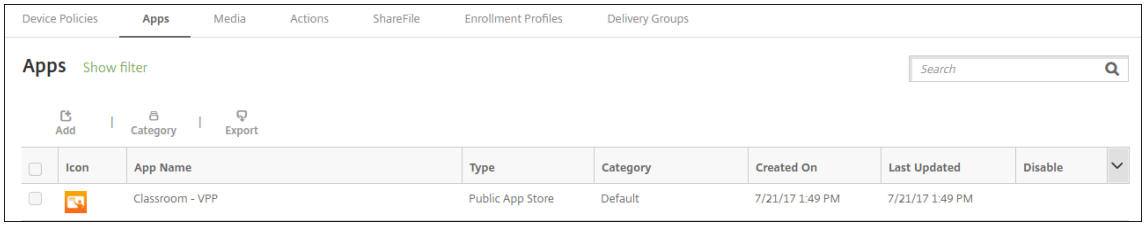
The apps you publish are available to devices enrolled in your Android Enterprise enterprise.

> **Note:**
>
> When you deploy an Android Enterprise public app store app to an Android user, that user is automatically enrolled in Android Enterprise.

Configure apps as MDX apps

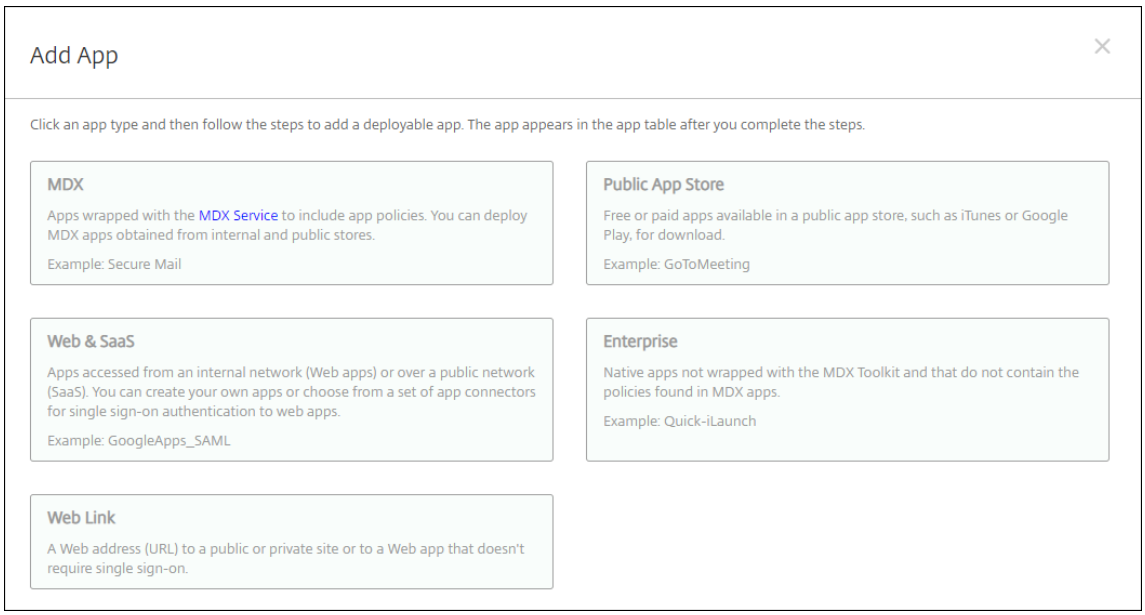
To configure a Citrix productivity app as an MDX app for Android Enterprise:

1. In the Citrix Endpoint Management console, click **Configure > Apps**. The **Apps** page appears.

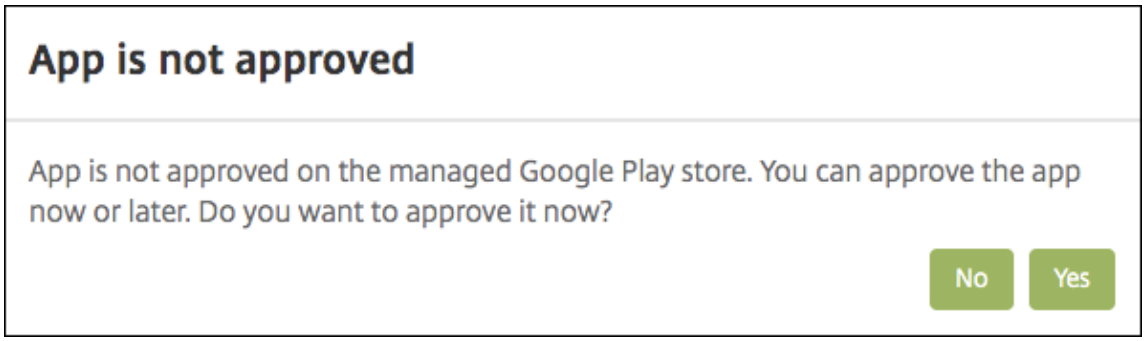


2. Click **Add**. The **Add App** dialog box appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

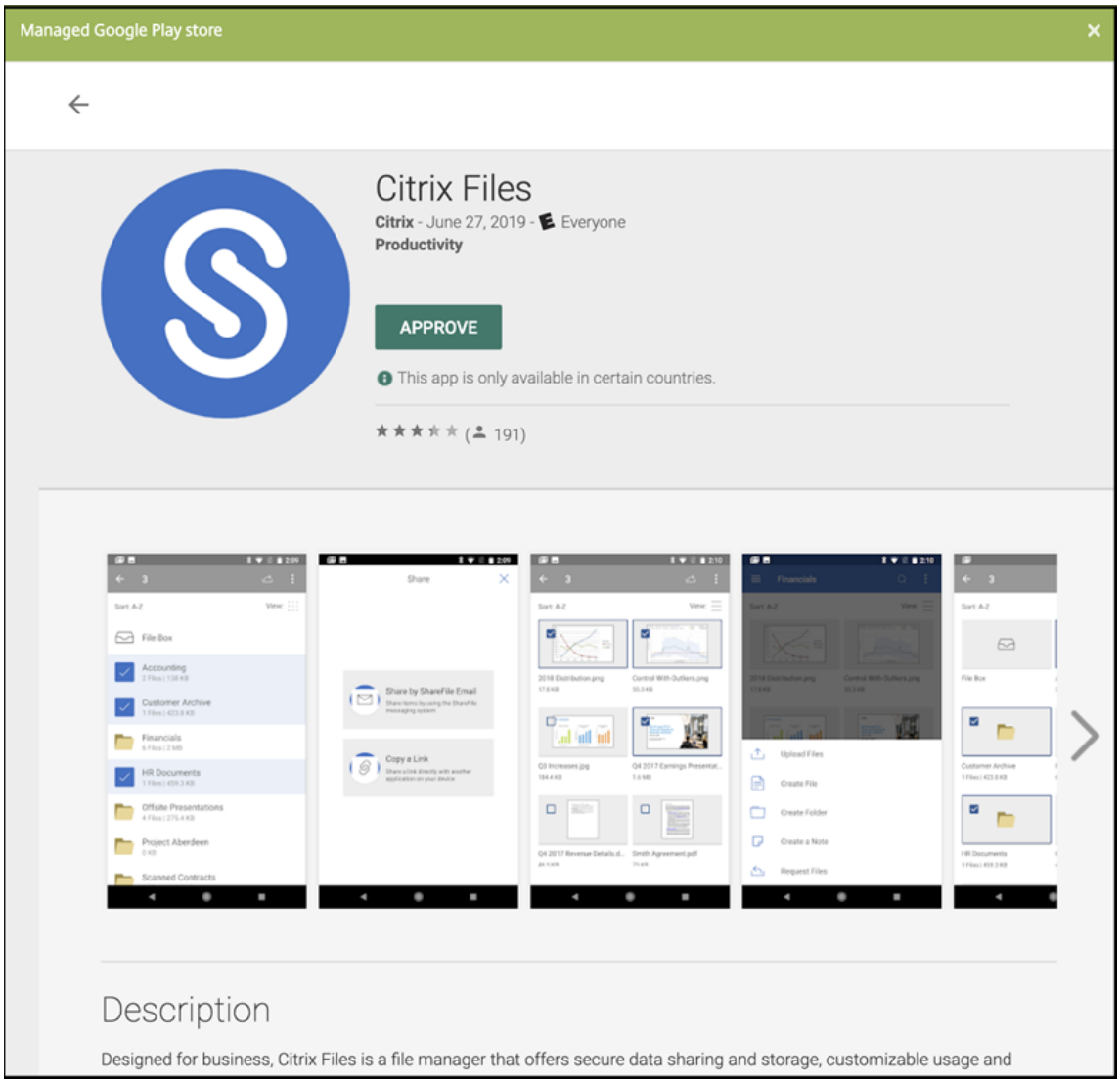


3. Click **MDX**. The **App Information** page appears.
4. On the left side of the page, select **Android Enterprise** as the platform.
5. On the **App Information** page, type the following information:
   - **Name:** Type a descriptive name for the app. This name appears under **App Name** on the **Apps** table.
   - **Description:** Type an optional description of the app.
   - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see About app categories.
6. Click **Next**. The **Android Enterprise MDX App** page appears.
7. Click **Upload** and navigate to the file location of the .mdx files for the app. Select the file and click **Open**.
8. The UI notifies you if the attached application requires approval from the managed Google Play store. To approve the application without leaving the Citrix Endpoint Management console, click **Yes**.



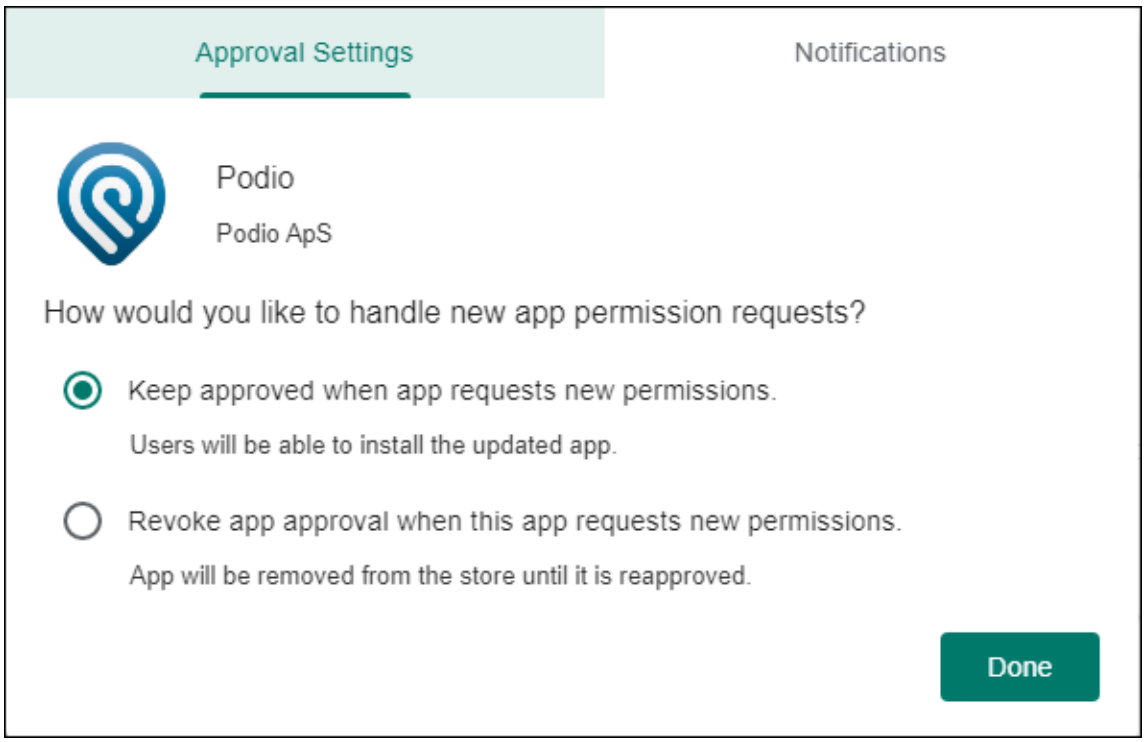
© 1997–2025 Citrix Systems, Inc. All rights reserved.

9. When the managed Google Play store page opens, click **Approve**.



10. Click **Approve** again.
11. Select **Keep approved when app requests new permissions**. Click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



12. When the app is approved and saved, more settings appear on the page. Configure these settings:

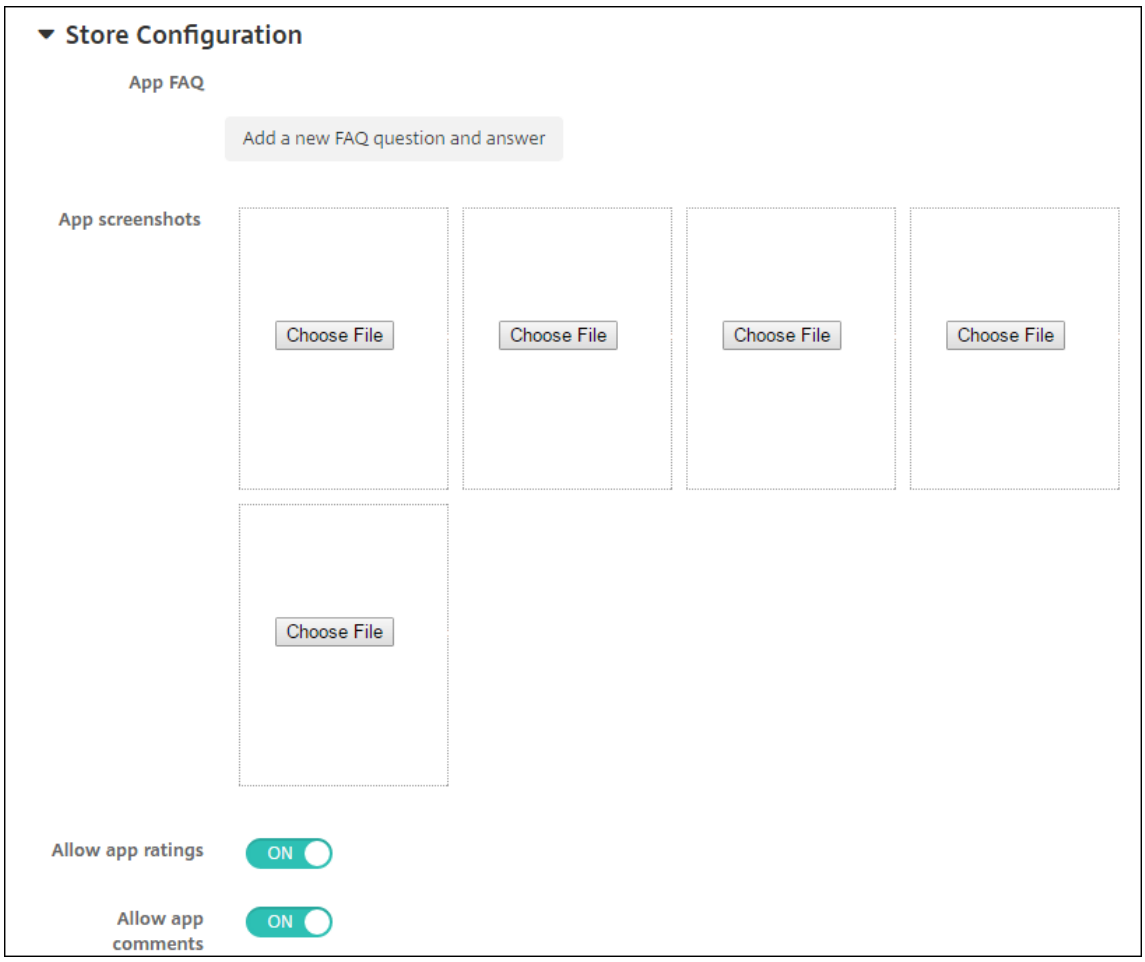
    - **File name:** Type the file name associated with the app.
    - **App Description:** Type a description for the app.
    - **Product track:** Specify which product track that you want to push to user devices. If you have a track designed for testing, you can select and assign it to your users. The default is Production.
    - **App version:** Optionally, type the app version number.
    - **Package ID:** The URL of the app in the Google Play store.
    - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
    - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
    - **Excluded devices:** Optionally, type the manufacturer or models of devices that can't run the app.

13. Configure the **MDX Policies**. For more information about app policies for MDX apps, see MDX Policies at a Glance and MAM SDK overview.

14. Configure the deployment rules. For information, see Deploy resources.

15. Expand **Store Configuration**. This setting doesn't apply to Android Enterprise apps, which appear only in managed Google Play.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

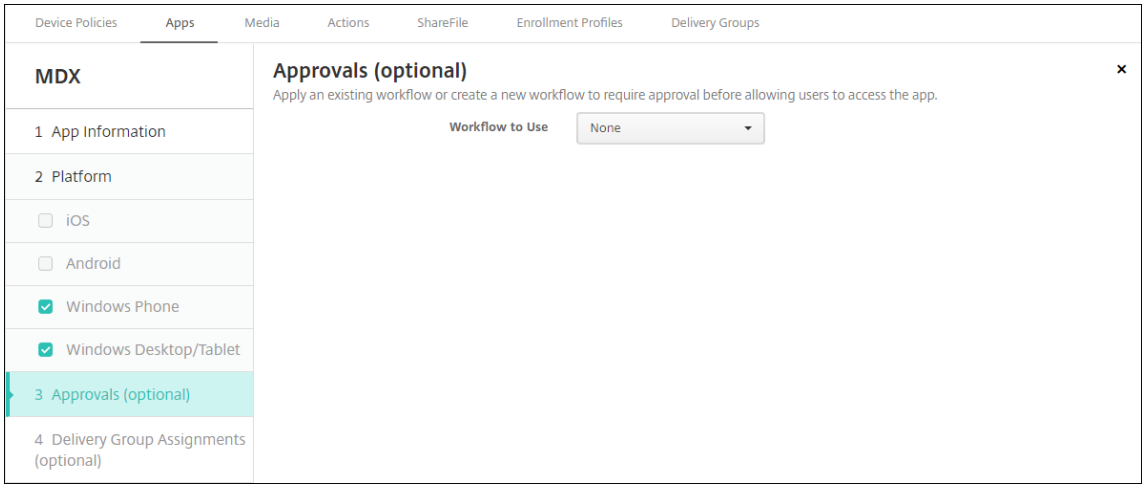


Optionally, you can add an FAQ for the app or screen captures that appear in the app store. You can also set whether users can rate or comment on the app.

- Configure these settings:
  - **App FAQ:** Add FAQ questions and answers for the app.
  - **App screenshots:** Add screen captures to help classify the app in the app store. The graphic you upload must be a PNG. You can't upload a GIF or JPEG image.
  - **Allow app ratings:** Select whether to allow a user to rate the app. The default is **On**. **Allow app comments:** Select whether to allow users to comment about the selected app. The default is **On**.

16. Click **Next**. The **Approvals** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



You use workflows when you need approval when creating user accounts. If you don't want to set up approval workflows, you can skip to Step 15.

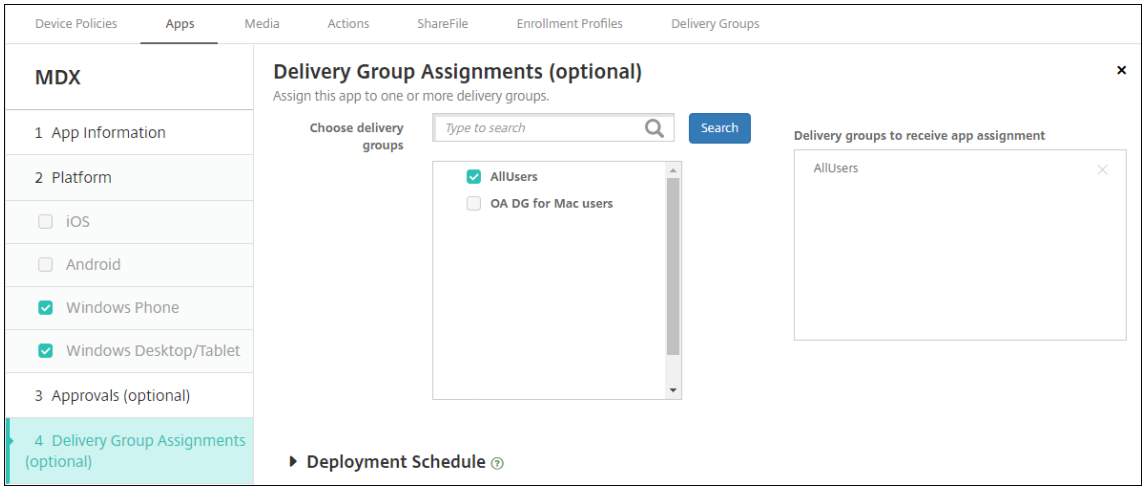
Configure these settings to assign or create a workflow:

- **Workflow to Use:** Click an existing workflow in the drop-down list or click **Create a new workflow**. The default is **None**.
- If you select **Create a new workflow**, configure these settings. For more information, see Create and manage workflows.
- **Name:** Type a unique name for the workflow.
- **Description:** Optionally, type a description for the workflow.
- **Email Approval Templates:** In the list, select the email approval template to be assigned. When you click the eye icon to the right of this field, a dialog box appears where you can preview the template.
- **Levels of manager approval:** In the list, select the number of levels of manager approval required for this workflow. The default is 1 level. Possible options are:
  - Not Needed
  - 1 level
  - 2 levels
  - 3 levels
- **Select Active Directory domain:** In the list, select the appropriate Active Directory domain to be used for the workflow.
- **Find additional required approvers:** Type the name of the additional required person in the search field and then click **Search**. Names originate in the Active Directory.
- When the name appears in the field, select the checkbox next to the name. The name and email address appear in the **Selected additional required approvers** list.
  - To remove a person from the **Selected additional required approvers** list, do one of the following:
    - Click **Search** to see a list of all the persons in the selected domain.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

* Type a full or partial name in the search box, and then click **Search** to limit the search results.
* Persons in the **Selected additional required approvers** list have check marks next to their name in the search results list. Scroll through the list and clear the checkbox next to each name you want to remove.

17. Click **Next**. The **Delivery Group Assignment** page appears.



18. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.
19. Expand **Deployment Schedule** and then configure the following settings:

    - Next to **Deploy**, click **On** to schedule deployment or click **Off** to prevent deployment. The default option is set as **On**.
    - Next to Deployment schedule, click **Now**, or **Later**. The default option is set as **Now**.
    - If you click **Later**, click the calendar icon and then select the date and time for deployment.
    - Next to **Deployment condition**, click **On every connection**, or click **Only when previous deployment has failed**. The default option is set as **On every connection**.
    - Next to **Deploy for always-on connection**, make sure that **Off** is selected. The default option is set as **Off**. The always-on connections aren't available for Android Enterprise to customers who began using Citrix Endpoint Management with version 10.18.19 or later. We don't recommend the connections for customers who began using Citrix Endpoint Management before version 10.18.19.

      This option applies when you've configured the scheduling background deployment key in **Settings > Server Properties**.

      The deployment schedule that you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

20. Click **Save**.

Repeat the steps for each mobile productivity app.

Configure security challenge policy

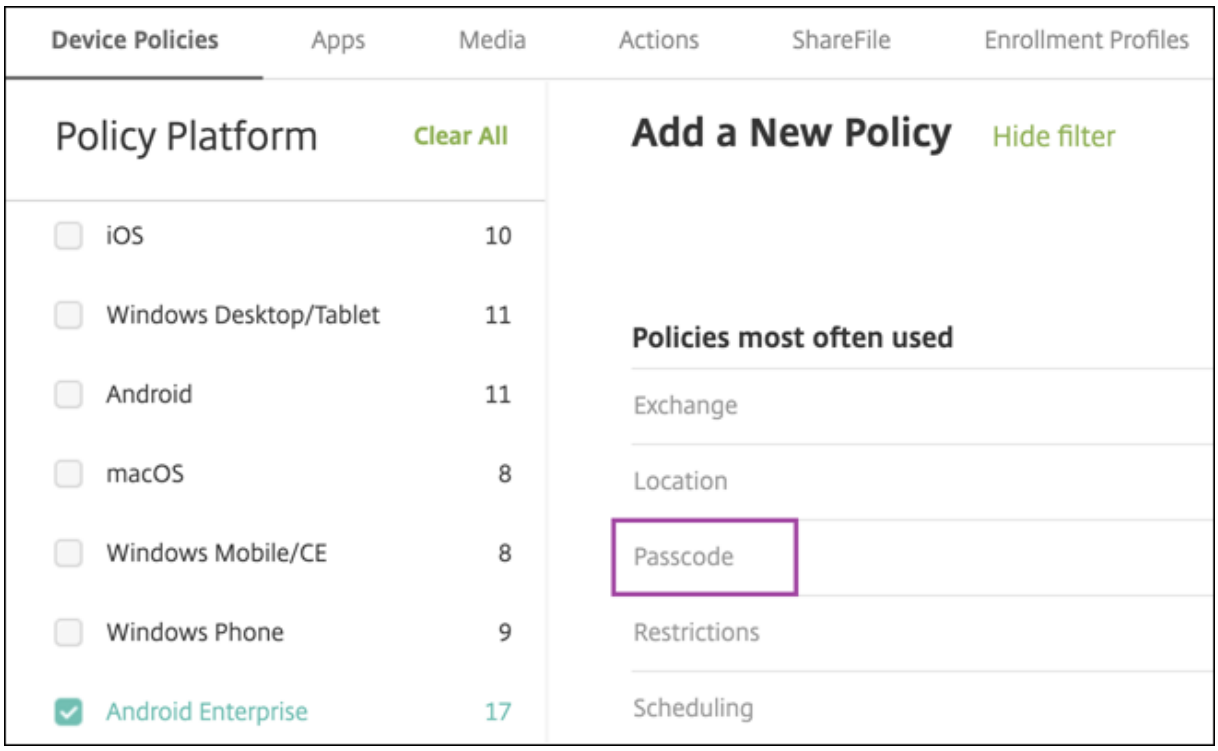
The Citrix Endpoint Management Passcode device policy configures security challenge rules. The challenges appear when users access their devices or the Android Enterprise work profiles on their devices. A security challenge can be a passcode or biometric recognition. For more information about the Passcode policy, see Passcode device policy.

- If your Android Enterprise deployment includes BYOD devices, configure the passcode policy for the work profile.
- If your deployment includes company-owned, fully managed devices, configure the passcode policy for the device itself.
- If your deployment includes both types of devices, configure both types of passcode policy.

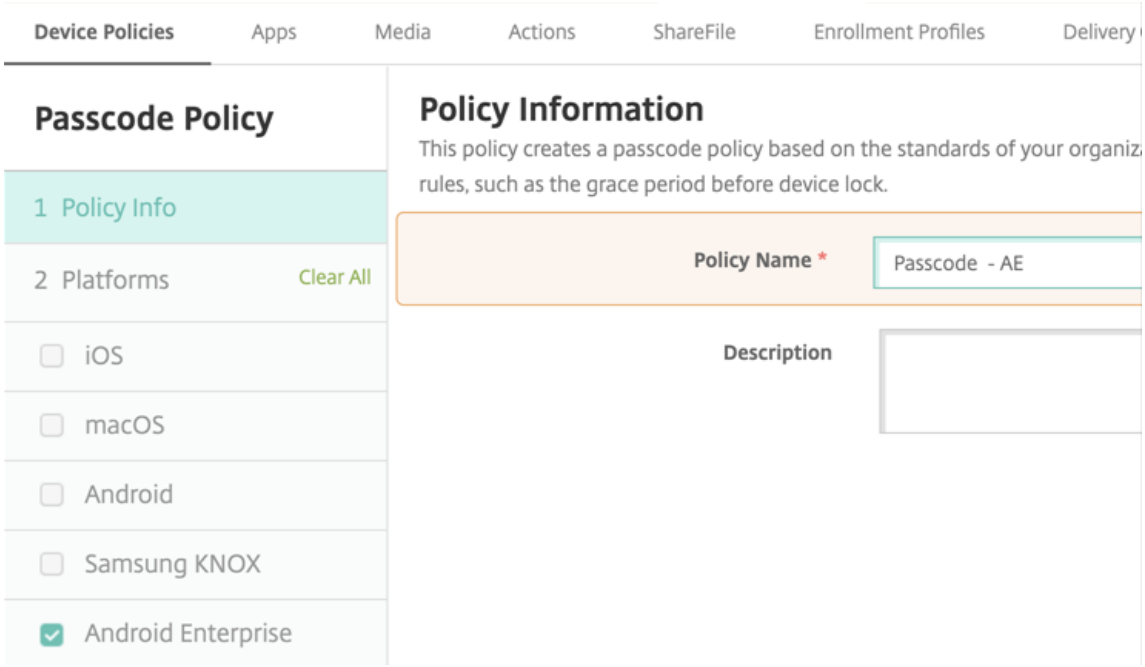
To configure the passcode policy:

1. In the Citrix Endpoint Management console, go to **Configure > Device Policies**.
2. Click **Add**.
3. Click **Show filter** to show the **Policy Platform** pane. In the **Policy Platform** pane, select **Android Enterprise**.
4. Click **Passcode** on the right pane.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



1. Enter a **Policy Name**. Click **Next**.



2. Configure the Passcode policy settings.

   - Set **Device passcode required** to **On** to see the settings available for security challenges for the device itself.
   - Set **Work profile security challenge** to **On** to see the settings available for work profile

© 1997–2025 Citrix Systems, Inc. All rights reserved.

security challenges.

3. Click **Next**.
4. Assign the policy to one or more delivery groups.
5. Click **Save**.

Creating enrollment profiles

Enrollment profiles control how Android devices are enrolled if Android Enterprise is enabled for your Citrix Endpoint Management deployment. When you create an enrollment profile to enroll Android Enterprise devices, you can configure the enrollment profile to enroll new and factory reset devices as:

- Fully managed devices
- Dedicated devices
- Fully managed devices with a work profile/Work profile on corporate-owned devices

You can also configure each of these Android Enterprise enrollment profiles to enroll BYOD Android devices as work profile devices.

If Android Enterprise is enabled for your Citrix Endpoint Management deployment, all newly enrolled or reenrolled Android devices are enrolled as Android Enterprise devices. By default, the Global enrollment profile enrolls new and factory reset Android devices as fully managed devices and enrolls BYOD Android devices as work profile on corporate-owned devices.

When you create enrollment profiles, you assign delivery groups to them. If a user belongs to many delivery groups that have different enrollment profiles, the name of the delivery group determines the enrollment profile used. Citrix Endpoint Management selects the delivery group that appears last in an alphabetized list of delivery groups. For more information, see Enrollment profiles.

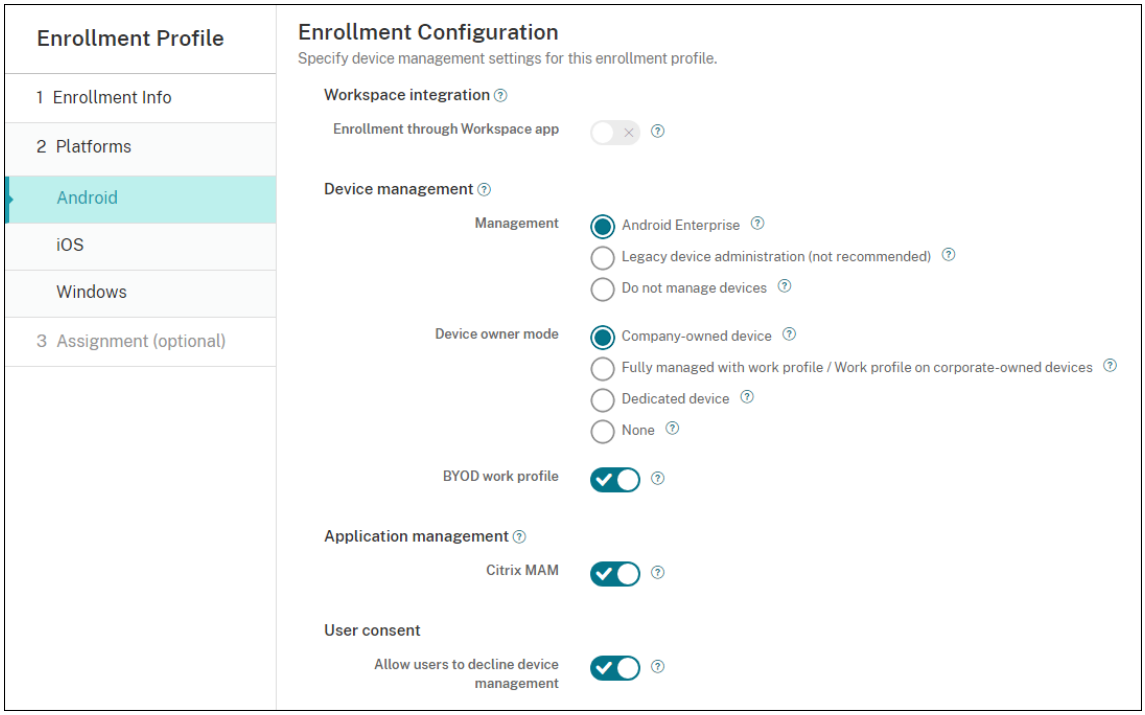
Add an enrollment profile for fully managed devices

The Global enrollment profile enrolls fully managed devices by default, but you can create more enrollment profiles to enroll fully managed devices.

1. In the Citrix Endpoint Management console, go to **Configure > Enrollment Profiles**.
2. To add an enrollment profile, click **Add**. In the Enrollment Info page, type a name for the enrollment profile.
3. Set the number of devices that members with this profile can enroll.
4. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. Set **Management** to **Android Enterprise**.
6. Set **Device owner mode** to **Company-owned device**.



7. **BYOD work profile** allows you to configure the enrollment profile to enroll BYOD devices as work profile devices. New and factory reset devices are enrolled as fully managed devices. Set **BYOD work profile** to **On** to allow enrollment of BYOD devices as work profile devices. Set **BYOD work profile** to **Off** to restrict enrollment to fully managed devices. Default is **On**.
8. Choose whether to enroll devices in Citrix MAM.
9. If you set **BYOD work profile** to **On**, configure user consent. To allow users of BYOD work profile devices to decline device management when they enroll their devices, set **Allow users to decline device management** to **On**.

   If **BYOD work profile** is set to **On**, the default value of **Allow users to decline device management** is **On**. If **BYOD work profile** is set to **Off**, then **Allow users to decline device management** is disabled.
10. Select **Assignment (options)**. The Delivery Group Assignment screen appears.
11. Choose the delivery group or delivery groups that have the administrators who enroll fully managed devices. Then click **Save**.

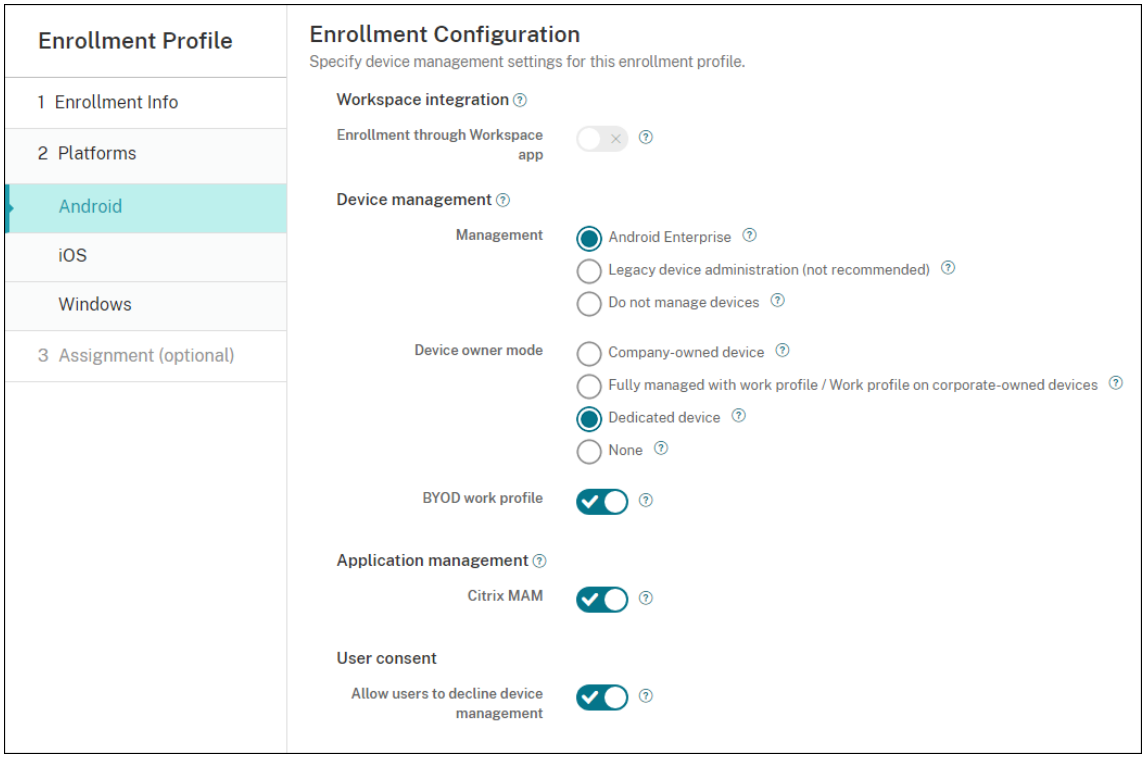
    The Enrollment Profile page appears with the profile that you added.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Add a dedicated device enrollment profile

When your Citrix Endpoint Management deployment includes dedicated devices, a single Citrix Endpoint Management administrator or small group of administrators enroll many dedicated devices. To make sure that these administrators can enroll all the devices required, create an enrollment profile for them with unlimited devices allowed per user.

1. In the Citrix Endpoint Management console, go to **Configure > Enrollment Profiles**.
2. To add an enrollment profile, click **Add**. In the Enrollment Info page, type a name for the enrollment profile. Set to **Unlimited** the number of devices members with this profile can enroll.
3. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
4. Set **Management** to **Android Enterprise**.
5. Set **Device owner mode** to **Dedicated device**.



6. **BYOD work profile** allows you to configure the enrollment profile to enroll BYOD devices as work profile devices. New and factory reset devices are enrolled as dedicated devices. Set **BYOD work profile** to **On** to allow enrollment of BYOD devices as work profile devices. Set **BYOD work profile** to **Off** to restrict enrollment to company-owned devices. Default is **On**.
7. Choose whether to enroll devices in Citrix MAM.
8. If you set **BYOD work profile** to **On**, configure user consent. To allow users of BYOD work profile devices to decline device management when they enroll their devices, set **Allow users to**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

decline device management to **On**.

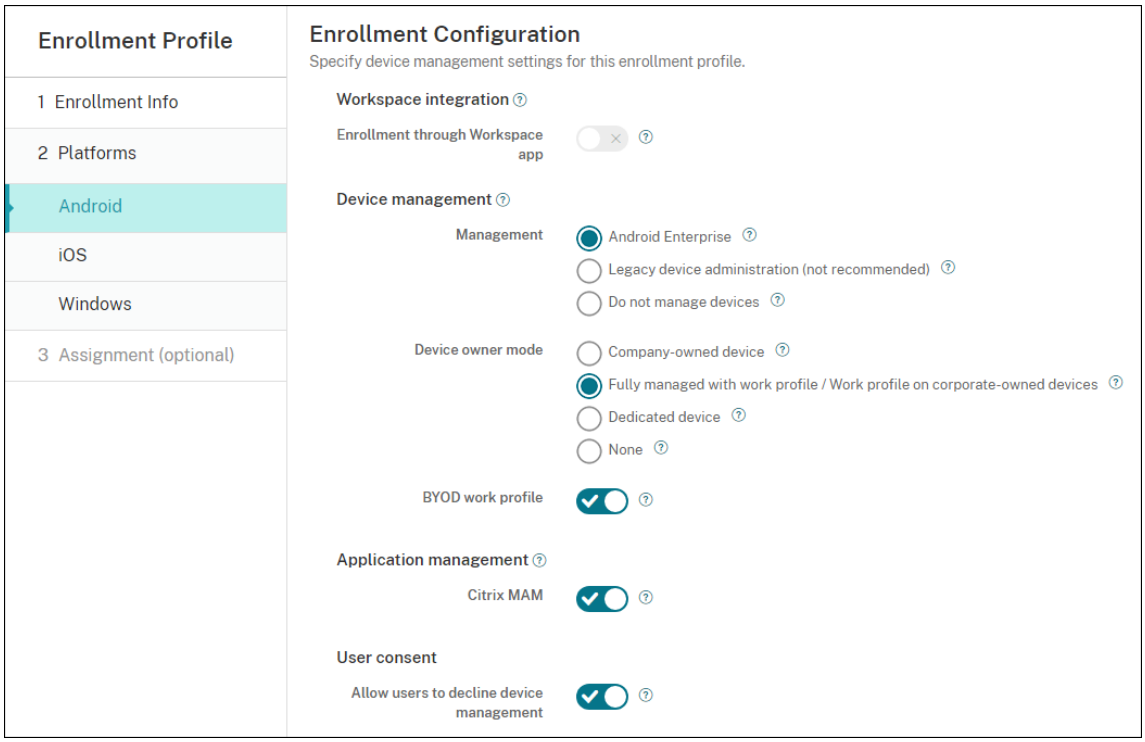
If **BYOD work profile** is set to **On**, the default value of **Allow users to decline device management** is **On**. If **BYOD work profile** is set to **Off**, then **Allow users to decline device management** is disabled.

9. Select **Assignment (options)**. The Delivery Group Assignment screen appears.
10. Choose the delivery group or delivery groups that have the administrators who enroll the dedicated devices. Then click **Save**.

    The Enrollment Profile page appears with the profile that you added.

Add an enrollment profile for fully managed devices with a work profile / work profile on corporate-owned devices

1. In the Citrix Endpoint Management console, go to **Configure > Enrollment Profiles**.
2. To add an enrollment profile, click **Add**. In the Enrollment Info page, type a name for the enrollment profile.
3. Set the number of devices that members with this profile can enroll.
4. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
5. Set **Management** to **Android Enterprise**. Set **Device owner mode** to **Fully managed with work profile / Work profile on corporate-owned devices**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

6. **BYOD work profile** allows you to configure the enrollment profile to enroll BYOD devices as work profile devices. New and factory reset devices are enrolled as fully managed devices with a work profile. Set **BYOD work profile** to **On** to allow enrollment of BYOD devices as work profile devices. Set **BYOD work profile** to **Off** to restrict enrollment to dedicated devices. Default is **Off**.
7. Choose whether to enroll devices in Citrix MAM.
8. If you set **BYOD work profile** to **On**, configure user consent. To allow users of BYOD work profile devices to decline device management when they enroll their devices, set **Allow users to decline device management** to **On**.

   If **BYOD work profile** is set to **On**, the default value of **Allow users to decline device management** is **On**. If **BYOD work profile** is set to **Off**, then **Allow users to decline device management** is disabled.
9. Select **Assignment (options)**. The Delivery Group Assignment screen appears.
10. Choose the delivery group or delivery groups that have the administrators who enroll fully managed devices with a work profile. Then click **Save**.

    The Enrollment Profile page appears with the profile that you added.

Adding an enrollment profile for legacy devices

Google deprecated the device administrator mode of device management. Google encourages customers to manage all Android devices in device owner mode or profile owner mode. (See Device admin deprecation in the Google Android Enterprise developer guides.)

To support this change:

- Citrix made Android Enterprise the default enrollment option for Android devices.
- If Android Enterprise is enabled for your Citrix Endpoint Management deployment, all newly enrolled or re-enrolled Android devices are enrolled as Android Enterprise devices.

Your organization might not be ready to begin managing legacy Android devices using Android Enterprise. In that case, you can continue to manage them in device administrator mode. For devices already enrolled in device administrator mode, Citrix Endpoint Management continues to manage them in device administrator mode.

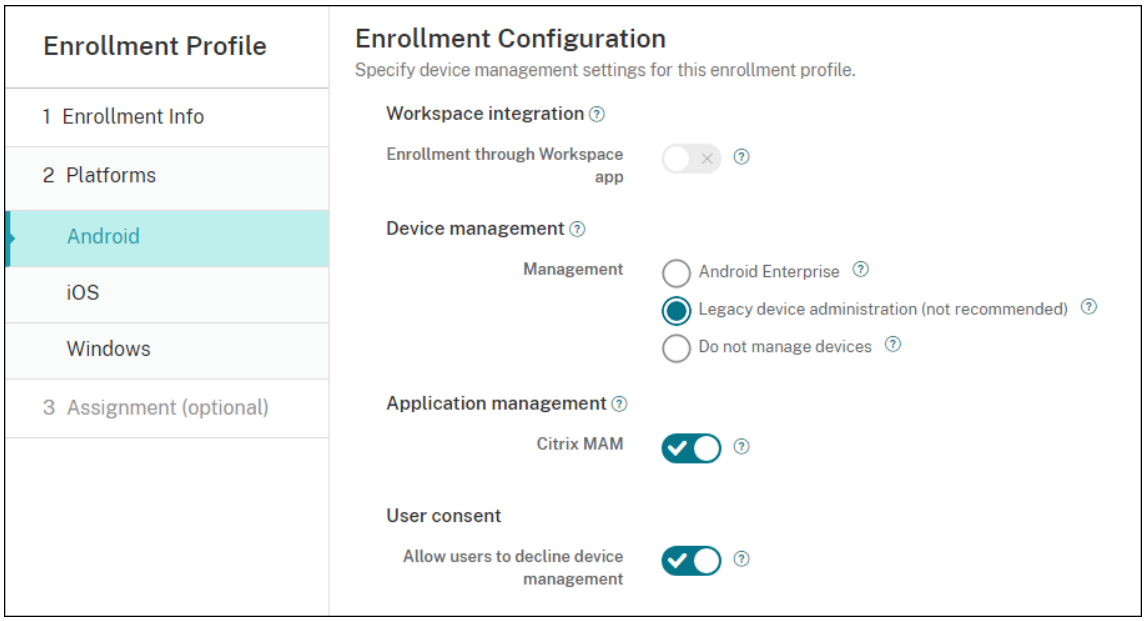
Create an enrollment profile for legacy devices to allow new Android device enrollments to use device administrator mode.

To create an enrollment profile for legacy devices:

1. In the Citrix Endpoint Management console, go to **Configure > Enrollment Profiles**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. To add an enrollment profile, click **Add**. In the Enrollment Info page, type a name for the enrollment profile.
3. Set the number of devices that members with this profile can enroll.
4. Select **Android** under **Platforms** or click **Next**. The Enrollment Configuration page appears.
5. Set **Management** to **Legacy device administration (not recommended)**. Click **Next**.



6. Choose whether to enroll devices in Citrix MAM.
7. To allow users to decline device management when they enroll their devices, set **Allow users to decline device management** to **On**. Default is **On**.
8. Select **Assignment (options)**. The Delivery Group Assignment screen appears.
9. Choose the delivery group or delivery groups that have the administrators who enroll the dedicated devices. Then click **Save**.

The Enrollment Profile page appears with the profile that you added.

To continue managing legacy devices in device administrator mode, enroll or re-enroll them using this profile. You enroll device administrator devices similar to work profile devices, by having users download Citrix Secure Hub and giving an enrollment server URL.

Provisioning Android Enterprise work profile devices

Android Enterprise work profile devices are enrolled in profile owner mode. These devices do not need to be new or factory reset. BYOD devices are enrolled as work profile devices. The enrollment experience is similar to Android enrollment in Citrix Endpoint Management. Users download Citrix Secure Hub from Google Play and enroll their devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

By default, the **USB Debugging and Unknown Sources** settings get disabled on a device when you enroll the device in Android Enterprise as a work profile device.

When enrolling devices in Android Enterprise as work profile devices, always go to Google Play. From there, enable Citrix Secure Hub to appear in the user's personal profile.

Provisioning Android Enterprise fully managed devices

You can enroll fully managed devices in the deployment you set up in the previous sections. Fully managed devices are company-owned devices and are enrolled in device owner mode. Only new or factory reset devices can be enrolled in device owner mode.

You can enroll devices in device owner mode using any of these enrollment methods:

- **DPC identifier token:** With this enrollment method, users enter the characters `afw#xenmobile` when setting up the device. `afw#xenmobile` is the Citrix DPC identifier token. This token identifies the device as managed by Citrix Endpoint Management and downloads Citrix Secure Hub from the Google Play store. See Enrolling devices using the Citrix DPC identifier token.
- **Near field communication (NFC) bump:** The NFC bump enrollment method transfers data through between two devices using near-field communication. Bluetooth, Wi-Fi, and other communication modes are disabled on a new or factory-reset device. NFC is the only communication protocol that the device can use in this state. See Enrolling devices with NFC bump.
- **QR code:** QR code enrollment can be used to enroll a distributed fleet of devices that do not support NFC, such as tablets. The QR code enrollment method sets up and configures the device profile mode by scanning a QR code from the setup wizard. See Enrolling devices using a QR code.
- **Zero-touch:** Zero-touch enrollment allows you to configure devices to enroll automatically when they're first powered on. Zero-touch enrollment is supported on some Android devices running Android 9.0 or later. See Zero-touch enrollment.
- **Google Accounts:** Users enter their Google Account credentials to start the provisioning process. This option is for enterprises using Google Workspace.

Enrolling devices using the Citrix DPC identifier token

Users enter `afw#xenmobile` when prompted to enter a Google account after powering on new or factory reset devices for initial setup. This action downloads and installs Citrix Secure Hub. Users then follow the Citrix Secure Hub set-up prompts to complete the enrollment.

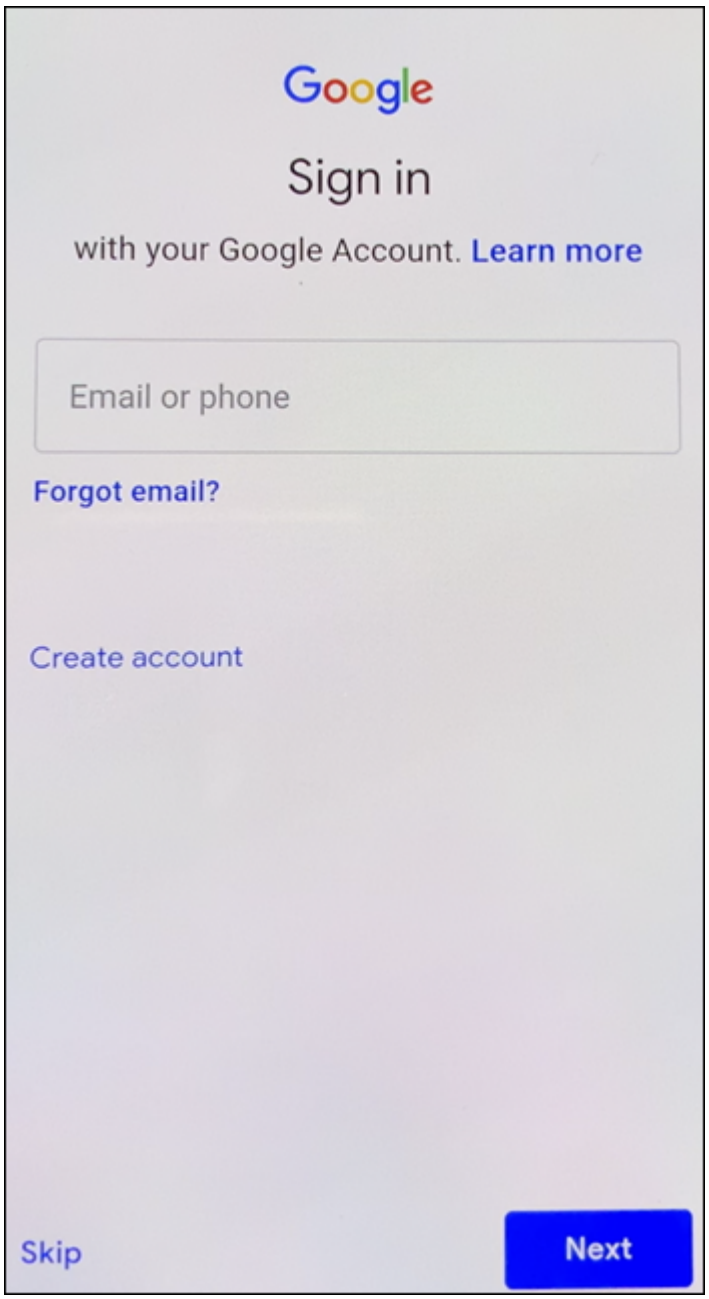
System requirements

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Supported on all Android devices running the Android OS.

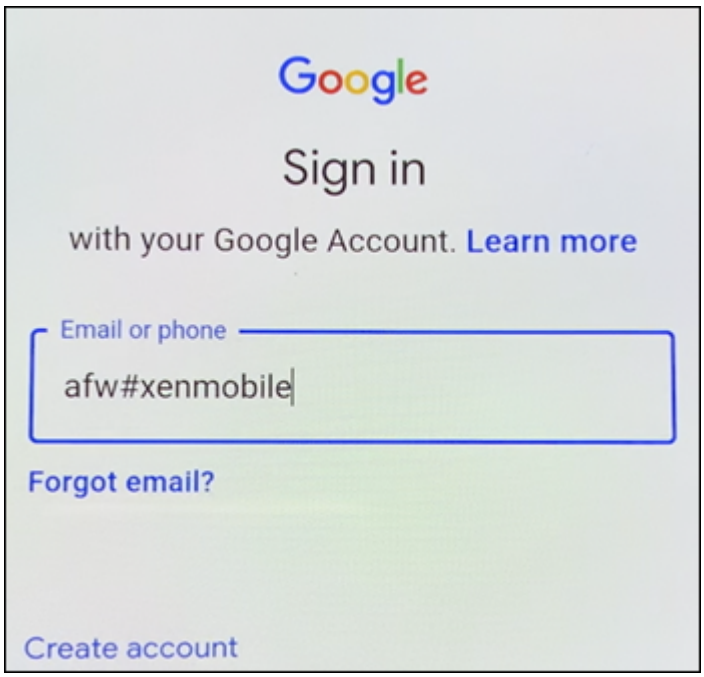
To enroll the device

1. Power on a new or factory reset device.
2. The initial device setup loads and prompts for a Google account. If the device loads the home screen of the device, check the notification bar for a **Finish Setup** notification.



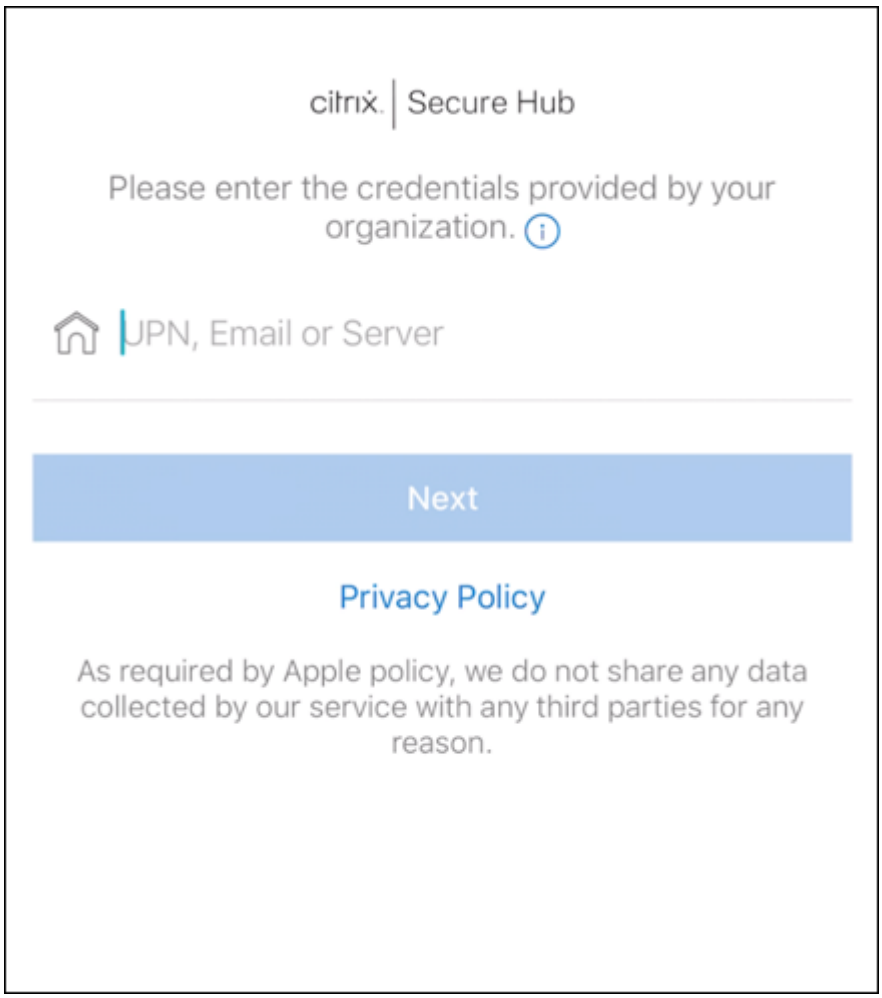
3. Enter `afw#xenmobile®` in the **Email or phone** field.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



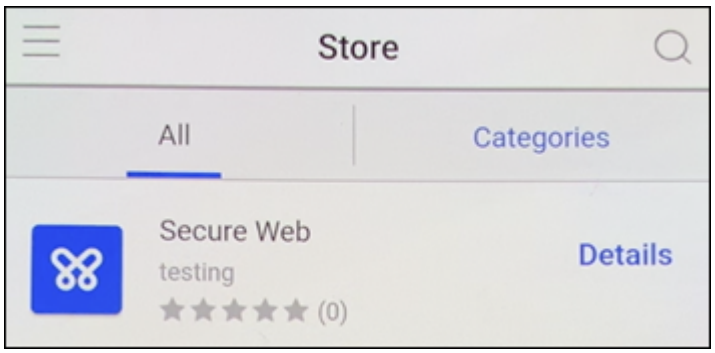
4. Tap **Install** on the Android Enterprise screen prompting to install Citrix Secure Hub.
5. Tap **Install** on the Citrix Secure Hub installer screen.
6. Tap **Allow** for all app permission requests.
7. Tap **Accept & Continue** to install Citrix Secure Hub and allow it to manage the device.
8. Citrix Secure Hub is now installed and on the default enrollment screen. In this example, AutoDiscovery isn't set up. If it is, the user can enter their user name/email and a server can be found for them. Instead, enter the enrollment URL for the environment and tap **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

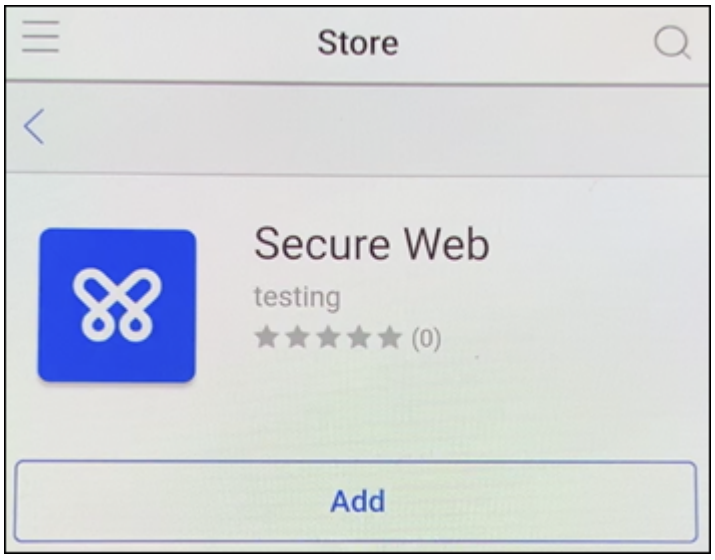


9. The default configuration for Citrix Endpoint Management allows users to choose if they use MAM or MDM+MAM. If prompted in this way, tap **Yes, Enroll** to choose MDM+MAM.
10. Enter the user email address and password, then tap **Next**.
11. The user is prompted to configure a device passcode. Tap **Set** and enter a passcode.
12. The user is prompted to configure a work profile unlock method. For this example, tap **Password**, tap **PIN**, and enter a PIN.
13. The device is now on the Citrix Secure Hub **My Apps** landing screen. Tap **Add apps from Store**.
14. To add Citrix Secure Web, tap **Citrix Secure Web**.

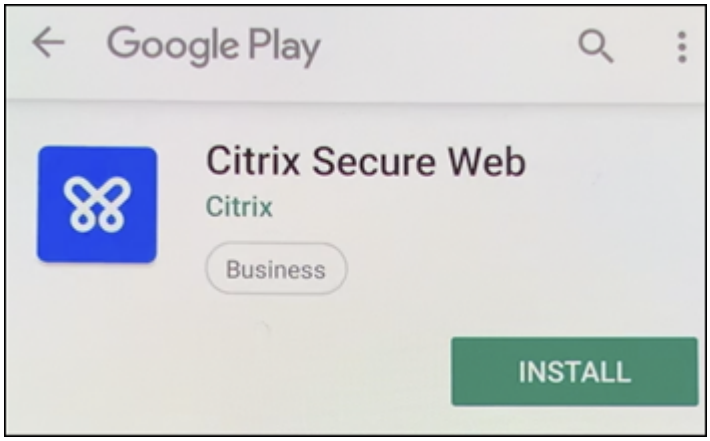
© 1997–2025 Citrix Systems, Inc. All rights reserved.



15. Tap **Add**.

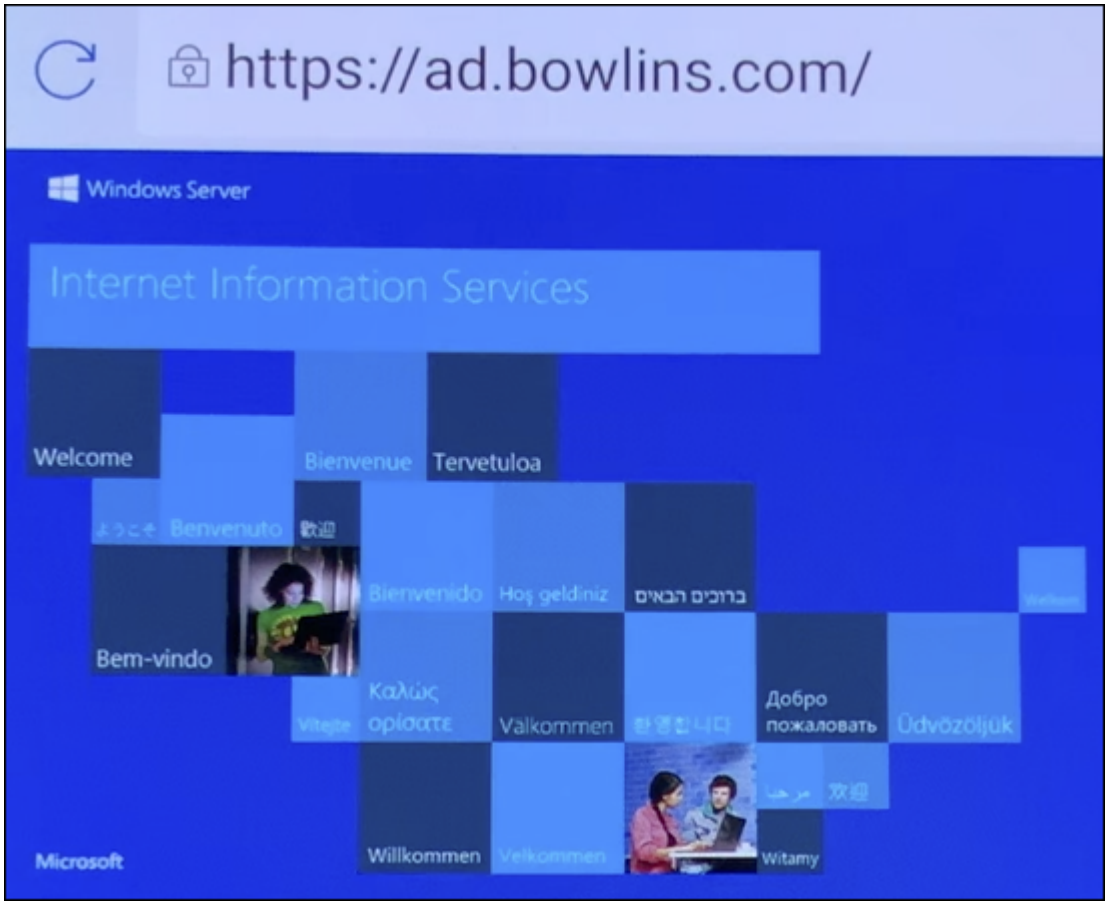


16. Citrix Secure Hub directs the user to the Google Play store to install Citrix Secure Web. Tap **Install**.



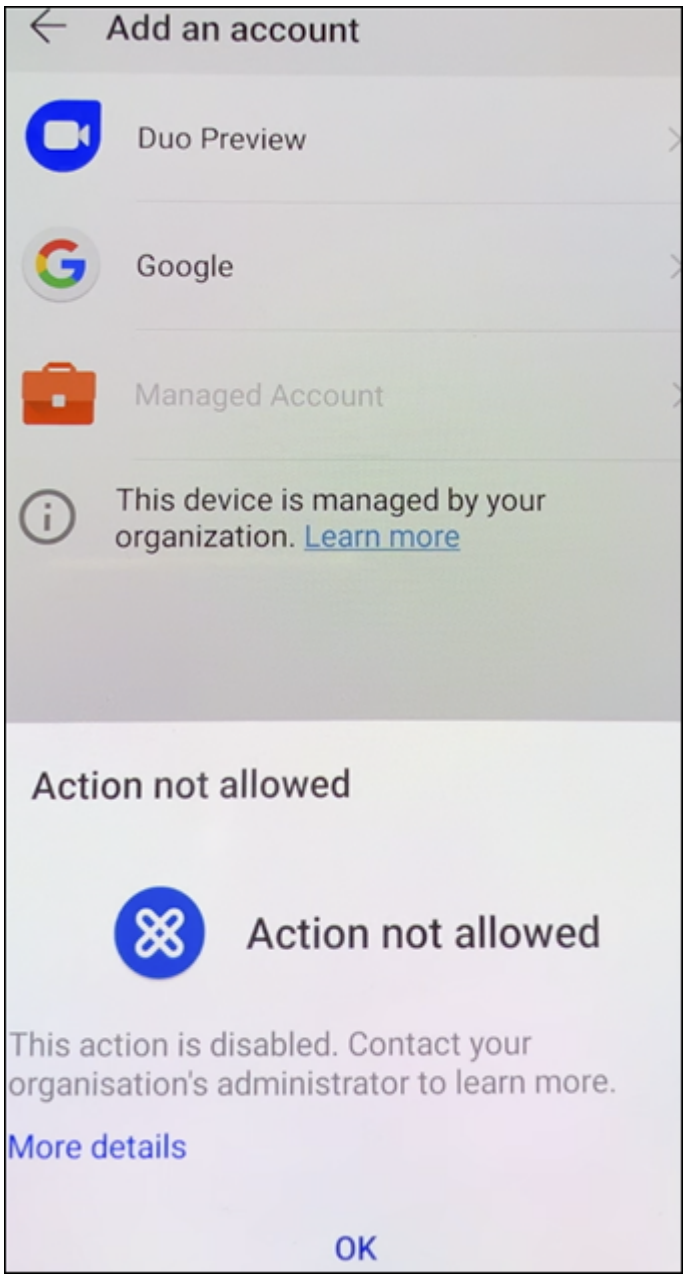
17. After Citrix Secure Web is installed, tap **Open**. Enter a URL from an internal site in the address bar and verify that the page loads.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



18. Go to **Settings > Accounts** on the device. Observe that the **Managed Account** can't be modified. The developer options for sharing screen or remote debugging are also blocked.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Enrolling devices with NFC bump

To enroll a device as a fully managed device using NFC bumps requires two devices: One that is reset to its factory settings and one running the Citrix Endpoint Management Provisioning Tool.

System requirements and prerequisites

- Supported Android devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- A new or factory-reset device with the NFC feature, provisioned for Android Enterprise as a fully managed device. See the section on Provisioning Android Enterprise fully managed devices.
- Another device with the NFC feature, running the configured Provisioning Tool. The Provisioning Tool is available in Citrix Secure Hub or on the Citrix downloads page.

Each device can have only one Android Enterprise profile. In this case, the profile is for a managed Citrix Secure Hub. Trying to add a second DPC app removes the installed Citrix Secure Hub.

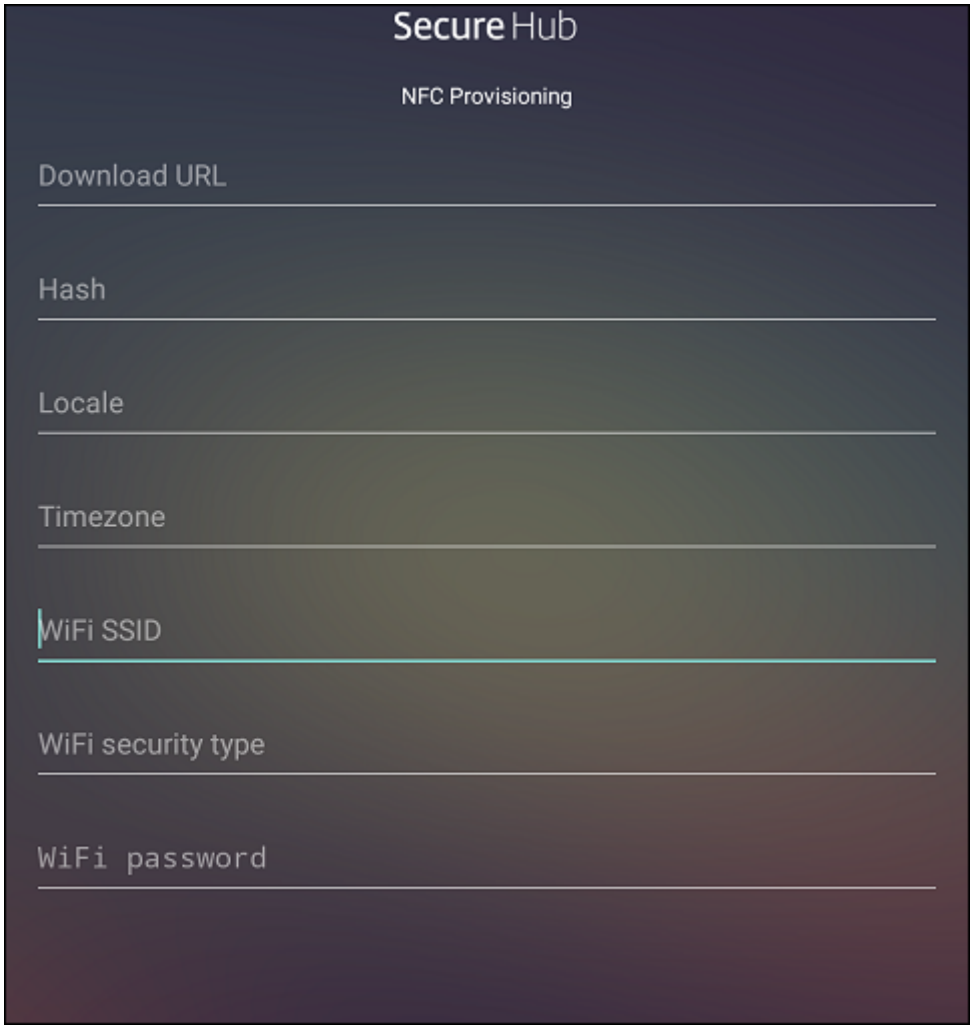
Data transferred through the NFC bump Provisioning a factory-reset device requires you to send the following data through an NFC bump to start the Android Enterprise:

- Package name of the DPC app that acts as device owner (in this case, Citrix Secure Hub).
- Intranet/Internet location from which the device can download the DPC app.
- SHA-256 hash of the DPC app to verify if the download is successful.
- Wi-Fi connection details so that a factory-reset device can connect and download the DPC app. Note: Android now does not support 802.1x Wi-Fi for this step.
- Time zone for the device (optional).
- Geographic location for the device (optional).

When the two devices are bumped, the data from the Provisioning Tool is sent to the factory-reset device. That data is then used to download Citrix Secure Hub with administrator settings. If you don't enter time zone and location values, Android automatically configures the values on the new device.

Configuring the Citrix Endpoint Management Provisioning Tool Before doing an NFC bump, you must configure the Provisioning Tool. This configuration is then transferred to the factory-reset device during the NFC bump.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



You can type data into the required fields or populate them by using a text file. The steps in the next procedure describe how to configure the text file with descriptions for each field. The app doesn't save information after you type it, so you might want to create a text file to keep the information for future use.

To configure the Provisioning Tool by using a text file Name the file nfcprovisioning.txt and place the file in the `/sdcard/` folder on the SD card of the device. The app can then read the text file and populate the values.

The text file must have the following data:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

This line is the intranet/internet location of the EMM provider app. After the factory-reset device connects to Wi-Fi following the NFC bump, the device must have access to this location for downloading. The URL is a regular URL, with no special formatting required.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>

This line is the checksum of the EMM provider app. This checksum is used to verify that the download is successful. Steps to get the checksum are discussed later in this article.

android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>

This line is the connected Wi-Fi SSID of the device on which the Provisioning Tool is running.

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>

Supported values are WEP and WPA2. If the Wi-Fi is unprotected, this field must be empty.

android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>

If the Wi-Fi is unprotected, this field must be empty.

android.app.extra.PROVISIONING_LOCALE=<locale>

Enter language and country codes. The language codes are two-letter lowercase ISO language codes (such as en) as defined by ISO 639-1. The country codes are two-letter uppercase ISO country codes (such as US) as defined by ISO 3166-1. For example, type en_US for English as spoken in the United States. If you don't type any codes, the country and language are automatically populated.

android.app.extra.PROVISIONING_TIME_ZONE=<timezone>

The time zone in which the device is running. Type the database name of the area/location. For example, type **America/Los_Angeles** for Pacific time. If you don't type a name, the time zone automatically populates.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<**package** name>

This data isn't required, because the value is hardcoded into the app as Citrix Secure Hub. It's mentioned here only for the sake of completion.

If there's Wi-Fi protected using WPA2, a completed nfcprovisioning.txt file might look like the following:

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

If there's unprotected Wi-Fi, a completed nfcprovisioning.txt file might look like the following:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

To get the checksum of Citrix Secure Hub The checksum of Citrix Secure Hub is a constant value: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`. To download an APK file for Citrix Secure Hub, use the following Google Play store link: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

To get an app checksum Prerequisites:

- The **apksigner** tool from the Android SDK Build Tools
- OpenSSL command line

To get the checksum of any app, follow these steps:

1. Download the app's APK file from the Google Play store.
2. In the OpenSSL command line, navigate to the **apksigner** tool: `android-sdk/build-tools/<version>/apksigner` and type the following:

   ```
   apksigner verify -print-certs <apk_path> | perl -nle 'print $& if
      m{
    (?<=SHA-256 digest:) .* }
    '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
   ```

   The command returns a valid checksum.

3. To generate the QR code, enter the checksum in the `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHE` field. For example:

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.
     zenprise/com.zenprise.configuration.AdminFunction",
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
4   "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"
       qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
5   "android.app.extra.
       PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
       play.google.com/managed/downloadManagingApp?identifier=xenmobile",
6   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
7
8       "serverURL": "https://supportablility.xm.cloud.com"
9     }
10
11  }
```

Libraries used The Provisioning Tool uses the following libraries in its source code:

- v7 `appcompat` library, Design Support library, and v7 palette support library by Google under Apache license 2.0

  For information, see Support Library Features Guide.

- Butter Knife by Jake Wharton under Apache license 2.0

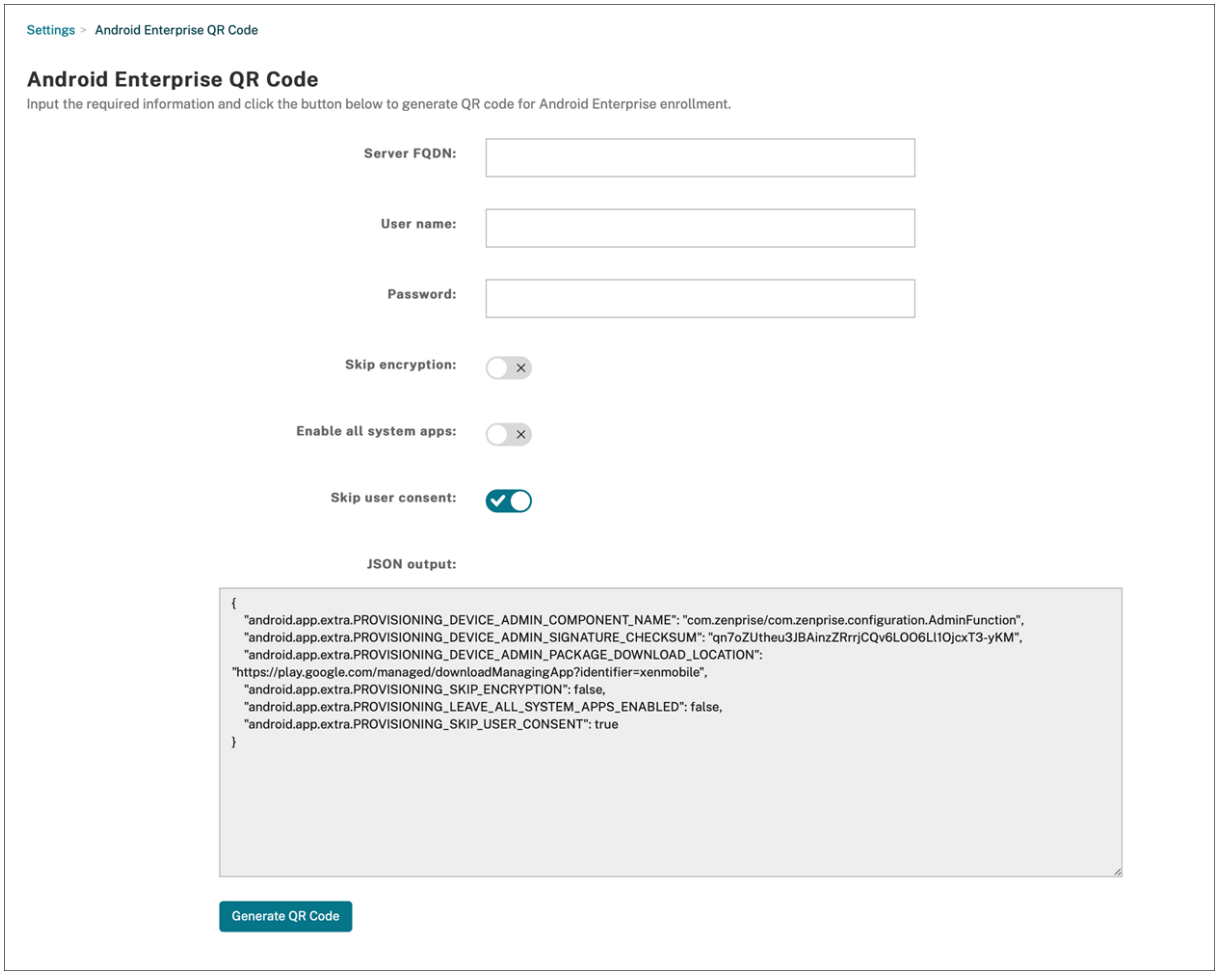
Enrolling devices using a QR code

Users can enroll a fully managed device by using the QR code you generate for them.

System requirements Android devices that run Android 7.0 or later.

Create a QR code You generate a QR code by specifying enrollment information as needed. After you generate a QR code, save the QR code locally. Citrix Endpoint Management doesn't store it.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



1. Navigate to **Settings > Android Enterprise QR Code**.
2. If needed, specify the following enrollment information:

    - **Server FQDN:** Type the FQDN of the Citrix Endpoint Management server (for example, `example.cem.cloud.com`). This field is optional. If you leave it empty, users must populate this information when they enroll.
    - **User name:** Type the user name used to enroll. If you plan on distributing the QR code to more than one user, we recommend leaving this field empty. Configuring a QR code with a user name and password is useful for enrolling kiosk devices. If you leave the field empty, users must populate this information when they enroll.
    - **Password:** Type the password associated with the user name you typed. If you leave the field empty, users must populate this information when they enroll.
    - **Skip encryption:** If **On**, the device isn't encrypted during enrollment. The default is **Off**.
    - **Enable all system apps:** If **On**, allows access to all the system apps on the device. The default is **Off**.
    - **Skip user consent:** If **Off**, users can opt out of device management. The default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The **JSON output** box displays the JSON content that corresponds to the information you specified.

3. To add more enrollment information, edit the JSON content in the **JSON output** box.
4. Click **Generate QR Code**. The QR code appears to the right of the JSON output.
5. Right-click the QR code image and save it.
6. Send the image to the users for device enrollment.

A factory-reset device scans this QR code to enroll as a fully managed device.

To enroll the device After powering up a new or factory reset device:

1. Tap the screen six times on the welcome screen to launch the QR code enrollment flow.
2. When prompted, connect to Wi-Fi. The download location for Citrix Secure Hub in the QR code is accessible over this Wi-Fi network.

   Once the device successfully connects to Wi-Fi, it downloads a QR code reader from Google and launches the camera.
3. Point the camera to the QR code to scan the code.

   Android downloads Citrix Secure Hub from the download location in the QR code, validates the signing certificate signature, installs Citrix Secure Hub, and sets it as the device owner.

For more information, see this Google guide for Android EMM developers: https://developers.google.com/android/work/prov-devices#qr_code_method.

Zero-touch enrollment

Zero-touch enrollment lets you set up devices to provision themselves as fully managed devices when they're powered on for the first time.

Your device reseller creates an account for you on the Android zero-touch portal, an online tool that lets you apply configurations to devices. Using the Android zero-touch portal, create one or more zero-touch enrollment configurations and apply the configurations to the devices assigned to your account. When your users power up these devices, the devices are automatically enrolled in Citrix Endpoint Management. The configuration assigned to the device defines its automatic enrollment process.

System requirements

- Support for zero-touch enrollment begins with Android 9.0.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Devices and account information from your reseller

- Devices eligible for zero-touch enrollment are bought from an enterprise reseller or Google partner. For a list of Android Enterprise zero-touch partners, see the Android website.
- An Android Enterprise zero-touch portal account, created by your reseller.
- Android Enterprise zero-touch portal account login information, provided by your reseller.

Create a zero-touch configuration When you create a zero-touch configuration, include a custom JSON to specify details of the configuration.

Use this JSON to configure the device to enroll on the Citrix Endpoint Management server you specify. Replace the URL of your server for 'URL'in this example.

```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
  {

        "serverURL":"URL"
    }

 }
```

You can use an optional JSON with more parameters to further customize your configuration. This example specifies the Citrix Endpoint Management server and the user name and password that devices using this configuration use to log on to the server.

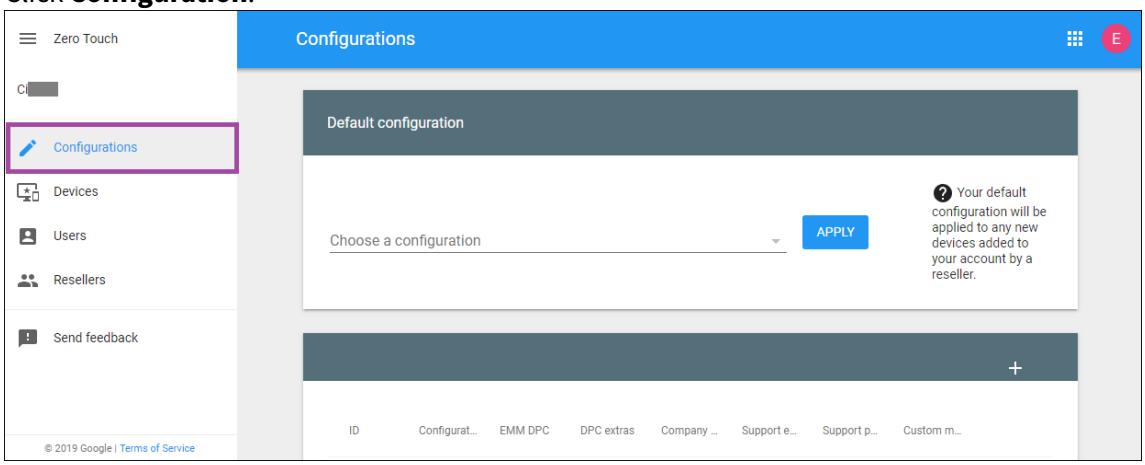
```
{

   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
     {

        "serverURL":"URL",
        "xm_username":"username",
        "xm_password":"password"
      }

        }
```

> **Important:**
>
> To enroll devices in the work profile on corporate-owned devices mode, add `{ "desiredProvisioningMo` `": "managedProfile"}` to the custom JSON under `PROVISIONING_ADMIN_EXTRAS_BUNDLE` .

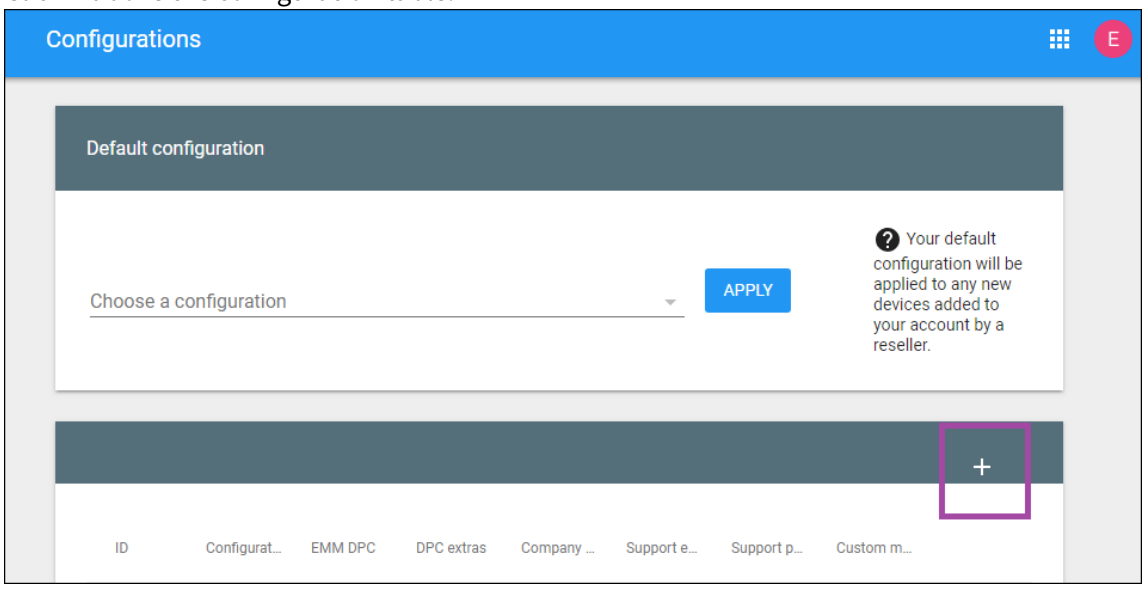
1. Go to the Android zero-touch portal at https://partner.android.com/zerotouch. Log in with the account information from your zero-touch device reseller.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Click **Configuration**.

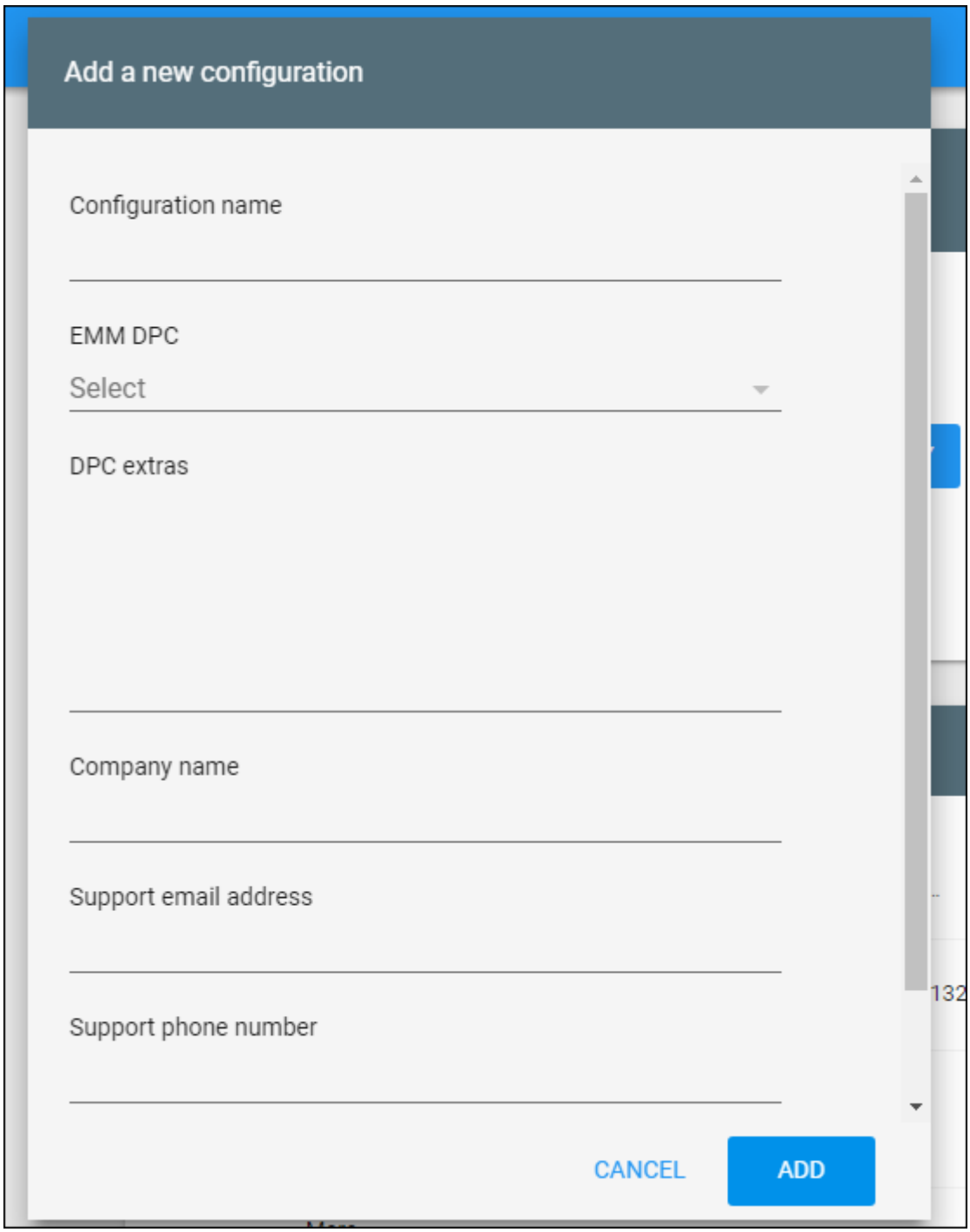


3. Click **+** above the configuration table.



4. Enter your configuration information in the configuration window that appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Configuration name:** Type the name that you choose for this configuration.
- **EMM DPC:** Choose **Citrix Secure Hub**.
- **DPC extras:** Paste your custom JSON text in this field.
- **Company name:** Type the name that you want to appear on your Android Enterprise zero-touch devices during device provisioning.
- **Support email address:** Type an email address that your users can contact for help. This

© 1997–2025 Citrix Systems, Inc. All rights reserved.

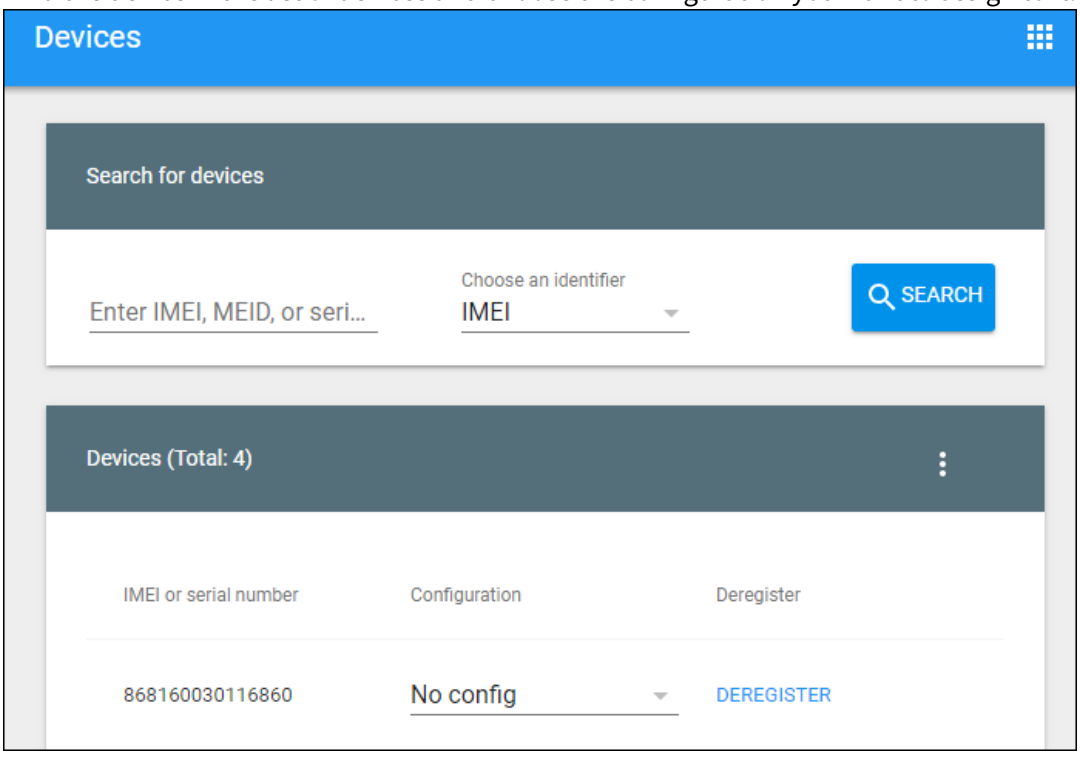
address appears on your Android Enterprise zero-touch devices before device provisioning.

- **Support phone number:** Type a phone number that your users can contact for help. This phone number appears on your Android Enterprise zero-touch devices before device provisioning.
- **Custom Message:** Optionally, add one or two sentences to help your users contact you or give them more details about what's happening to their device. This custom message appears on your Android Enterprise zero-touch devices before device provisioning.

5. Click **Add**.
6. To create more configurations, repeat steps 2 through 4.
7. To apply a configuration to a device:

   a) In the Android zero-touch portal, click **Devices**.

   b) Find the device in the list of devices and choose the configuration you want to assign to it.



   c) Click **Update**.

You can apply a configuration to many devices using a CSV file.

For information on how to apply a configuration to many devices, see Zero-touch enrollment for IT admins. This Android Enterprise topic has more information on how to manage configurations and apply them to devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Provisioning dedicated Android Enterprise devices

Dedicated Android Enterprise devices are fully managed devices that are dedicated to fulfill a single use case. You restrict these devices to one app or a small set of apps required to do the tasks needed for this use case. You also prevent users from enabling other apps or doing other actions on the device.

Enroll dedicated devices using any of the enrollment methods used for other fully managed devices, as described in Provisioning Android Enterprise fully managed devices. Provisioning dedicated devices require more setup before enrollment.

To provision dedicated devices:

- Add an enrollment profile for Citrix Endpoint Management administrators that you allow to enroll dedicated devices to your Citrix Endpoint Management deployment. See Creating enrollment profiles.
- To enable a dedicated device to access apps, add them to the allow list.
- Optionally, set the allowed app to allow lock task mode. When an app is in lock task mode, the app is pinned to the device screen when the user opens it. No Home button appears and the Back button is disabled. The user exits the app using an action programmed into the app, such as signing out.
- Enroll each device in the enrollment profile that you added.

System requirements

- Support for enrolling dedicated devices begins with Android 6.0.

Allow apps and set lock task mode

The Kiosk device policy lets you allow apps and set lock task mode. By default, Citrix Secure Hub and Google Play services are on the allow list.

To add the Kiosk policy:

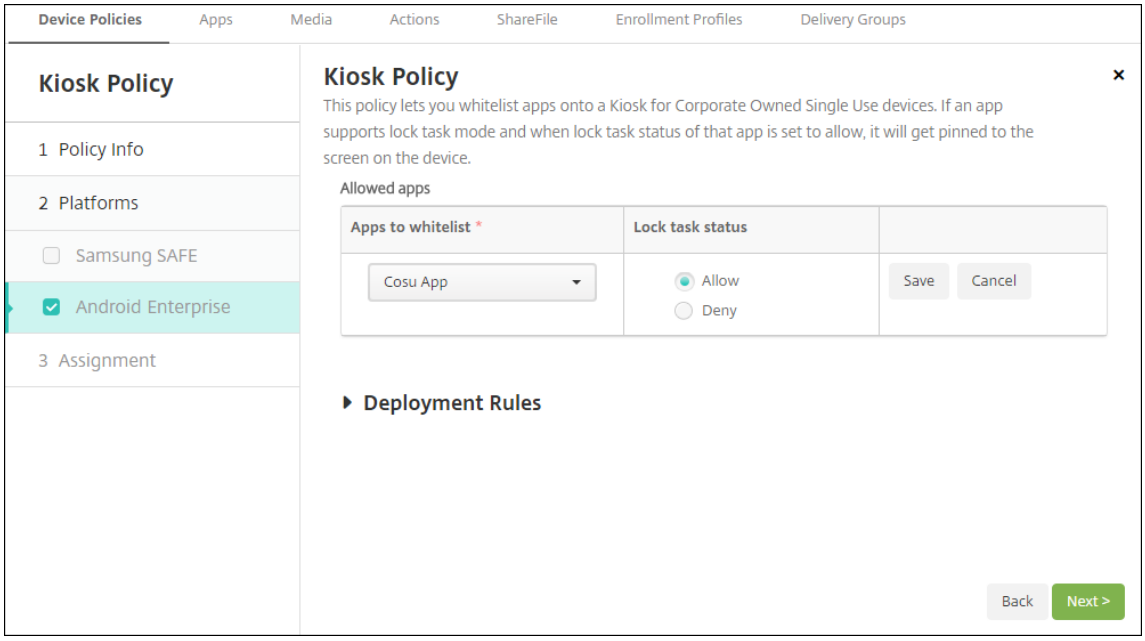
1. In the Citrix Endpoint Management console, click **Configure > Device Policies**. The **Device Policies** page appears.
2. Click **Add**. The **Add a New Policy** dialog box appears.
3. Expand **More** and then, under Security, click **Kiosk**. The **Kiosk Policy** page appears.
4. Under Platforms, select **Android Enterprise**. Clear other platforms.
5. In the Policy Information pane, type the **Policy Name** and an optional **Description**.
6. Click **Next** and then click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

7. To allow an app and allow or deny lock task mode for that app:

   Select the app that you want to allow from the list.

   Choose **Allow** to set the app to be pinned to the device screen when the user starts the app. Choose **Deny** to set the app not to be pinned. Default is **Allow**.



8. Click **Save**.
9. To allow another app and allow or deny lock task mode for that app, click **Add**.
10. Configure deployment rules and choose delivery groups. For more information, see Device policies.

Provisioning Android Enterprise fully managed devices with a work profile or work profile on corporate-owned devices

Devices running Android 9.0-10.x enroll as “fully managed with a work profile.”Starting with Android 11+, devices enroll as “work profile on corporate-owned devices.”All of these devices are company-owned devices that are used for both work and personal purposes. Your organization manages the entire device. You can apply one set of policies to the device and a separate set of policies to the work profile.

In the Citrix Endpoint Management console, fully managed devices with a work profile appear with these terms:

- The device ownership is “Corporate”.
- The device Android Enterprise install type is “Corporate Owner Personally Enabled”.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

System requirements

- Support for enrolling fully managed devices with work profiles begins with Android 9.0.

To enroll the device

New and factory reset devices enroll as fully managed devices with a work profile. Those devices use any of the enrollment methods used for other fully managed devices, as described in Provisioning Android Enterprise fully managed devices. Devices running Android 11 can enroll in the work profile on corporate-owned devices mode using the QR code or zero-touch enrollment methods described in that section.

> **Important:**
>
> When enrolling devices in the work profile on corporate-owned devices mode using the QR code method, add the following to the JSON output, above the `serverURL` field:
> `"desiredProvisioningMode": "managedProfile",`

JSON output

```
{
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
    "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
    "android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": false,
    "android.app.extra.PROVISIONING_SKIP_USER_CONSENT": true,
    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
        "desiredProvisioningMode": "managedProfile",
        "serverURL": "https://testServer.xmqa.cloud.com",
        "username": "username",
        "password": "password"
    }
```

Devices that aren't new or factory reset are enrolled as work profile devices as described in Provisioning Android Enterprise work profile devices.

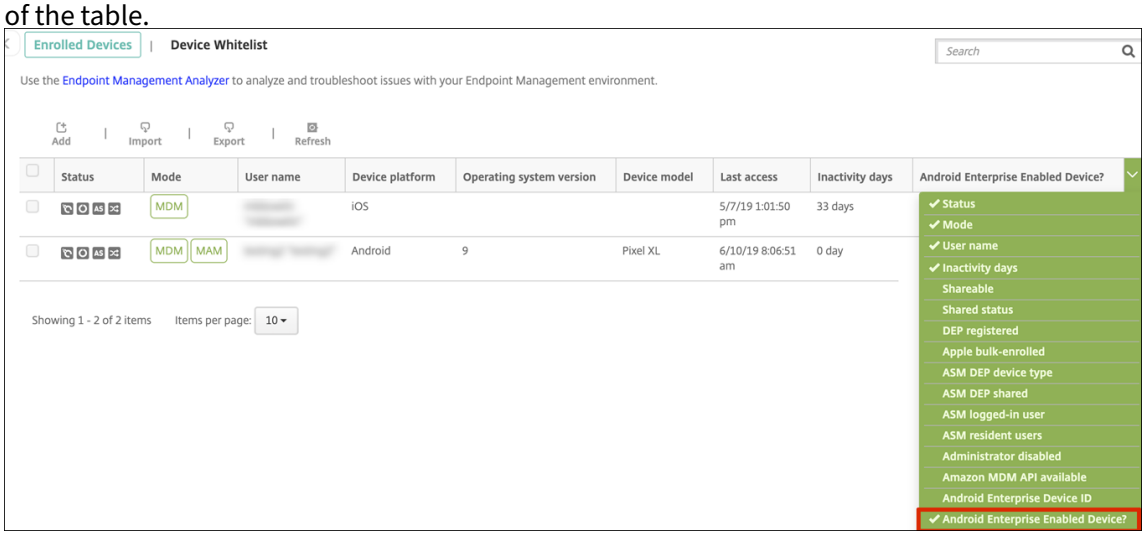
Viewing Android Enterprise devices in the Citrix Endpoint Management console

To view Android Enterprise fully managed devices, dedicated devices, and fully managed devices with a work profile:

1. In the Citrix Endpoint Management console, go to **Manage > Devices**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Add the **Android Enterprise Enabled Device?** column by clicking the menu on the right edge of the table.



3. To view available security actions, select a fully managed device and click **Secure**. When the device is fully managed, the **Full Wipe** action is available but **Selective Wipe** isn't. That difference is because the device only allows apps from the managed Google Play store. There isn't an option for the user to install applications from the public store. Your organization manages all the content on the device.

Configure Android Enterprise device and app policies

For an overview of the policies controlled at both the device and app levels, see Supported device policies and MDX policies for Android Enterprise.

What to know about policies:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Device restrictions:** Dozens of device restrictions let you control features such as:
  - Use of the device camera
  - Use of copy and paste between work and personal profiles
- **Per-app VPN:** Use the Managed configurations device policy to configure VPN profiles for Android Enterprise.
- **Email policy:** We recommend using the Managed configurations device policy to configure apps.

Device policies

This table lists all device policies available for Android Enterprise devices.

> **Important:**
>
> For devices that enroll in Android Enterprise and use MDX apps: You can control some settings through MDX and Android Enterprise. Use the least restrictive policy settings for MDX and control the policy through Android Enterprise.

App permissions	App inventory	App uninstall
Automatically update managed apps	Connection scheduling	Credentials
Custom XML	Citrix Endpoint Management options	Files
Keyguard management	Kiosk	Launcher configuration
Location	Managed configurations	Network
OS update	Passcode	Restrictions

Device policies for fully managed devices with work profile (COPE devices)

For fully managed devices with work profiles, you can use some device policies to apply separate settings to the entire device and the work profile. You can use other device policies to apply settings only to the entire device or only to the work profile of fully managed devices with work profiles. For

© 1997–2025 Citrix Systems, Inc. All rights reserved.

devices enrolled in the work profile on corporate-owned devices mode, policies apply only to the work profile and not the entire device.

Policy	Applies to
App permissions	Work profile
App inventory	Work profile
App uninstall	Work profile
Automatically update managed apps	Work profile
Connection scheduling	Work profile
Credentials	Work profile
Custom XML	N/A
Citrix Endpoint Management options	Work profile
Files	Work profile
Keyguard management	Device and work profile
Kiosk	N/A
Launcher configuration	Device and work profile
Location	Device (location mode only)
Managed configurations	Work profile
Network	Device
OS update	N/A
Passcode	Device and work profile
Restrictions	Device and work profile (create separate policies for the device and the work profile)
VPN	N/A

See also, Supported device policies and MDX policies for Android Enterprise and MAM SDK overview.

Security actions

Android Enterprise supports the following security actions. For a description of each security action, see Security actions.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Security action	Work profile	Fully managed
Certificate Renewal	Yes	Yes
Full Wipe	Yes (after a selective wipe)	Yes
Locate	Yes	Yes
Lock	Yes	Yes
Lock and Reset Password	No	Yes
Notify (Ring)	Yes	Yes
Revoke	Yes	Yes
Selective Wipe	Yes	Yes

Security action notes

- The locate security action fails unless the Location device policy sets the location mode for the device to **High Accuracy** or **Battery Saving**. See Location device policy.
- On work profile devices that are running versions of Android earlier than Android 9.0:
  - The lock and reset password action isn't supported.
- On work profile devices with Android 9.0 or greater:
  - The passcode sent locks the work profile. The device itself isn't locked.
  - If no passcode is set on the work profile:
    - If no passcode is sent, or the passcode sent doesn't meet passcode requirements: The device is locked.
  - If a passcode is set on the work profile:
    - If no passcode is sent, or the passcode sent doesn't meet passcode requirements: The work profile is locked but the device itself isn't locked.

Unenroll an Android Enterprise enterprise

If you no longer want to use your Android Enterprise enterprise, you can unenroll the enterprise.

> **Warning:**
>
> After you unenroll an enterprise, Android Enterprise apps on devices already enrolled through it reset to their default states. Google no longer manages the devices. If you enroll into a new Android Enterprise enterprise, you must approve apps for the new organization from managed

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> Google Play. You can then update the apps from the Citrix Endpoint Management console.

After the Android Enterprise enterprise is unenrolled:

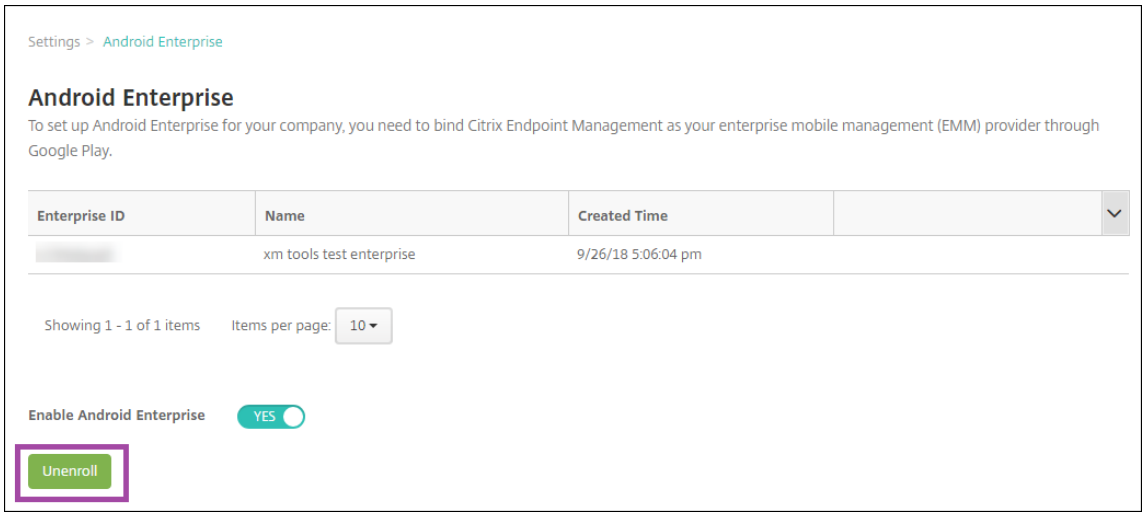
- Devices and users enrolled through the enterprise have the Android Enterprise apps reset to their default state. Managed configurations policies previously applied no longer affect operations.
- Citrix Endpoint Management manages devices enrolled through the enterprise. From the perspective of Google, those devices are unmanaged. You can't add new Android Enterprise apps. You can't apply Managed configurations policies. You can apply other policies, such as Scheduling, Password, and Restrictions, to these devices.
- If you try to enroll devices in Android Enterprise, they're enrolled as Android devices, not Android Enterprise devices.

Unenroll an Android Enterprise enterprise using the Citrix Endpoint Management server console and Citrix Endpoint Management Tools.

When you do this task, Citrix Endpoint Management opens a Tools popup window. Before you begin, make sure that your browser has permission to open popup windows. Some browsers, such as Google Chrome, require you to disable popup blocking and add the address of the Citrix Endpoint Management site to the popup allow list.

To unenroll an Android Enterprise enterprise:

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The Settings page appears.
2. On the Settings page, click **Android Enterprise**.
3. Click **Unenroll**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Distribute Android Enterprise apps

September 6, 2025

Citrix Endpoint Management manages apps deployed to devices. You can organize and deploy the following types of Android Enterprise apps.

- **Managed app store apps:** These apps include free apps available in the managed Google Play Store. For example, GoToMeeting.
- **MDX:** Apps prepared with the MAM SDK or wrapped with the MDX Toolkit. These apps include MDX policies. You get MDX apps from internal sources and public stores. Deploy Citrix mobile productivity apps as MDX apps.
- **Enterprise:** Private apps you develop or get from another source. You provide these apps to your users through the managed Google Play Store. The managed Google Play Store is the Google enterprise app store.
- **MDX-enabled private apps:** Enterprise apps prepared with the MAM SDK or wrapped with the MDX Toolkit.

You can add enterprise apps and MDX-enabled private apps two different ways.

- Add the apps to the Citrix Endpoint Management console as enterprise apps, as described in the Enterprise apps and MDX-enabled private apps sections in this article.
- Publish the apps directly to the managed Google Play Store using your Google developer account. Then add the apps to the Citrix Endpoint Management console as managed app store apps. See Managed app store apps.

If you publish apps using your Google developer account and then switch to using the Citrix Endpoint Management console, the ownership of the apps differs. You need to manage your apps in both locations, in this case. Citrix recommends adding your apps using one method or the other.

If you need to remove self-managed apps from the managed Google Play Store, open a ticket with Google. Developers can disable, but not delete, apps from the managed Google Play Store.

The following sections provide more in-depth information for Android Enterprise app configuration. For information about distributing apps, see Add Apps. That article includes:

- The general workflows for adding web and SaaS apps or web links
- The required app workflow for enterprise and public store apps
- How to deliver enterprise apps from the Citrix Content Delivery Network (CDN) for Enterprise Apps

© 1997–2025 Citrix Systems, Inc. All rights reserved.

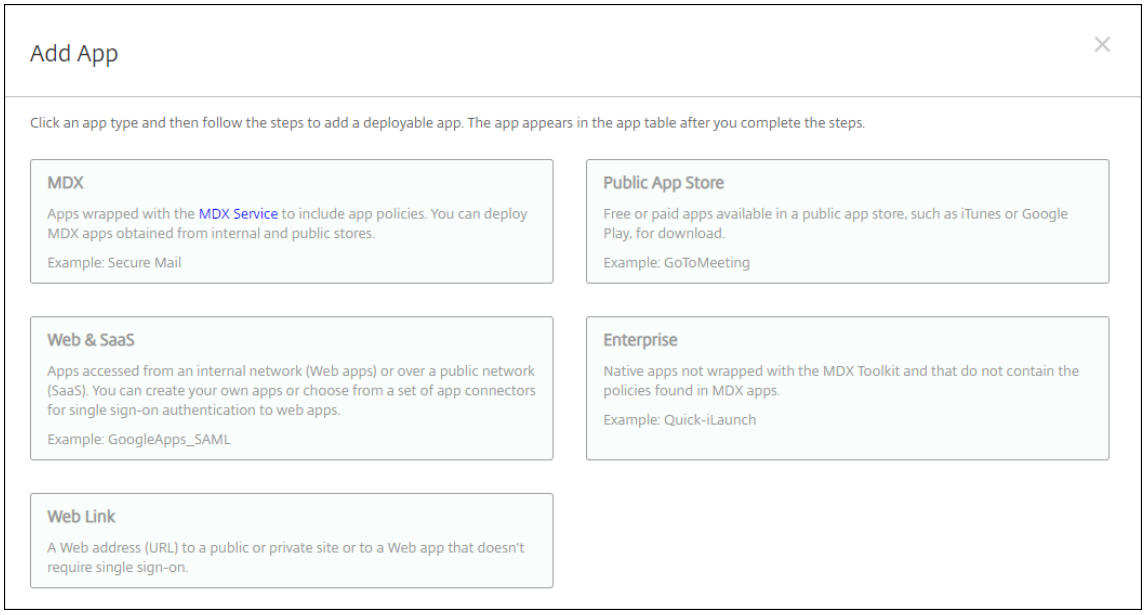
Managed app store apps

You can add free apps available on the managed Google Play Store to Citrix Endpoint Management.

> **Note:**
>
> To make all apps in the Google Play store accessible from managed Google Play, use the **Access all apps in the managed Google Play store** server property. See Server properties. Setting this property to **true** allows all Android Enterprise users to access public Google Play store apps. You can then use the Restrictions device policy to control access to these apps.

Step 1: Add and configure apps

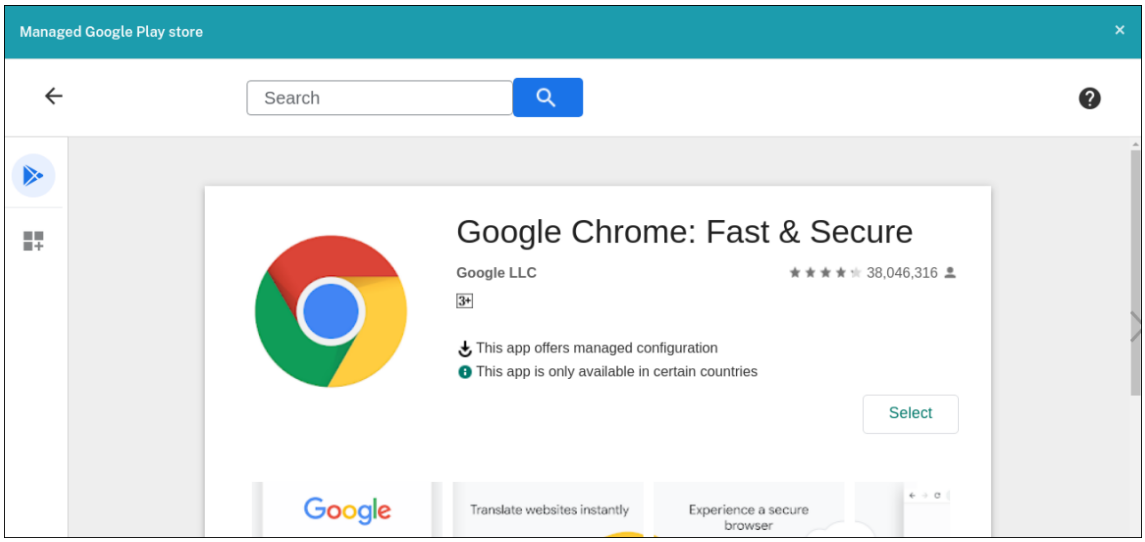
1. In the Citrix Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.
2. Click **Public App Store**.



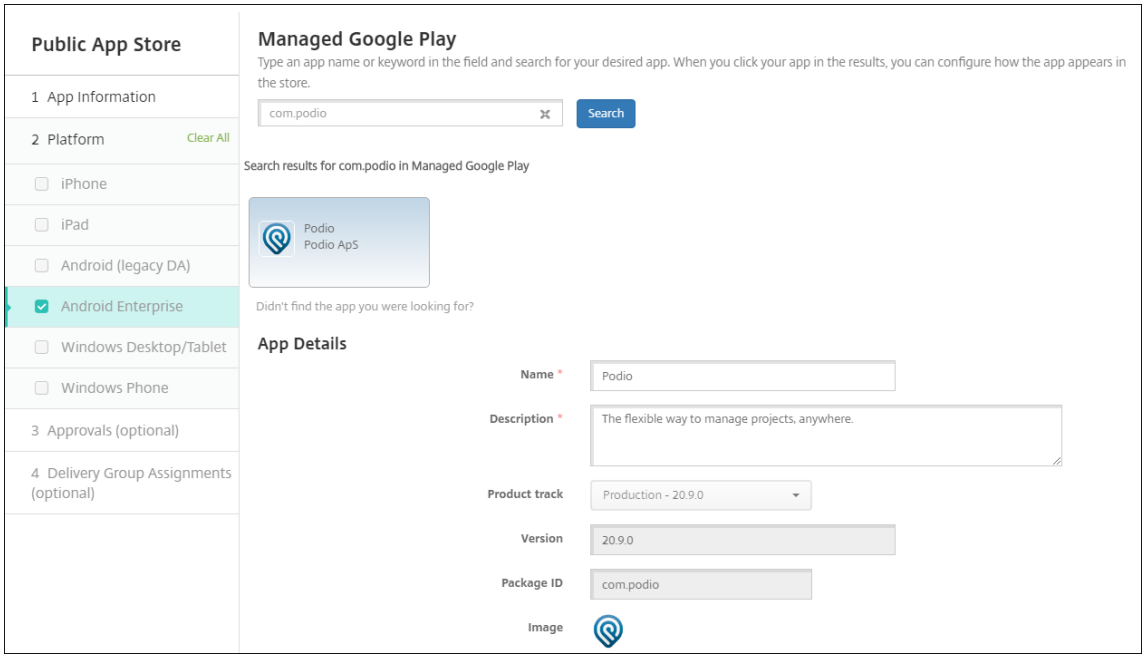
3. In the **App Information** pane, type the following information:
   - **Name:** Type a descriptive name for the app. The name appears under **App Name** on the **Apps** table.
   - **Description:** Type an optional description of the app.
4. Select **Android Enterprise** as the platform.
5. Type the app name or package ID in the search box and click **Search**. You can locate the package ID in the Google Play store. The ID is in the URL of the app. For example, `com.Slack` is the package ID in `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

6. Apps matching the search criteria appear. Click the desired app then click **Select**.



7. Click **Select** again.
8. Click the app icon and configure the app **Name** and **Description**.



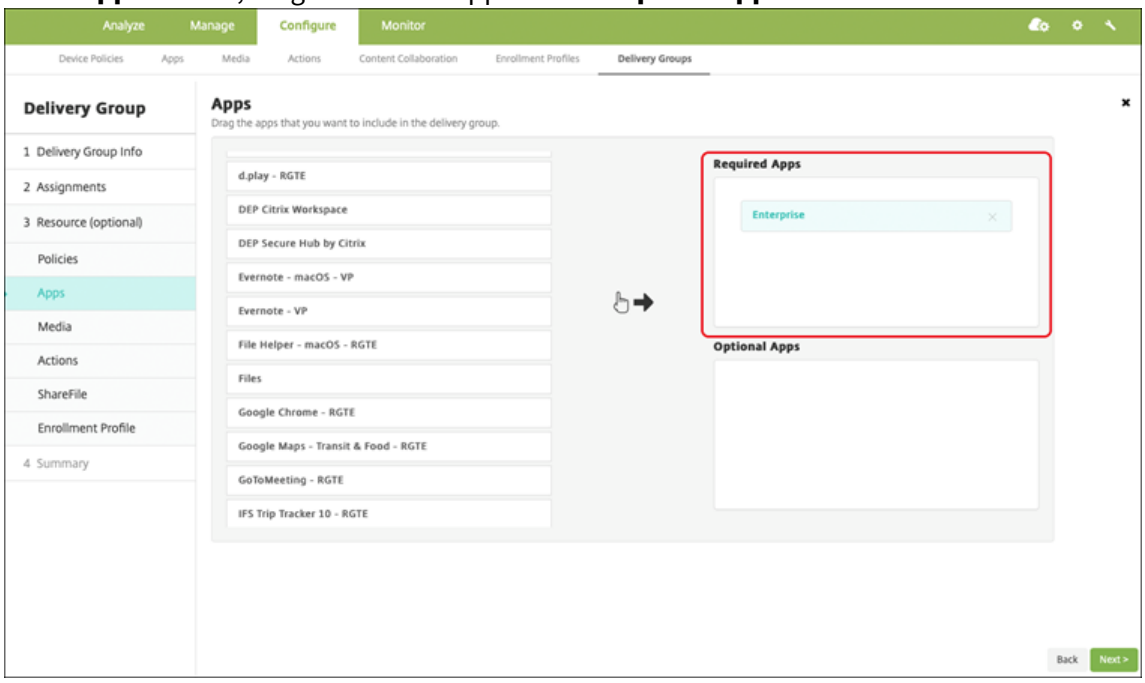
9. Assign any delivery groups to the app and click **Save**. For information, see Deploy resources.

Step 2: Configure app deployment

1. Navigate to **Configure > Delivery Groups** and select the delivery group you configured. Click **Edit**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. In the **Apps** section, drag the desired apps to the **Required Apps** box.



3. On the **Summary** page, click **Save**.
4. On the **Delivery Groups** page, select the delivery group and click **Deploy**.

MDX apps

Add MDX files to Citrix Endpoint Management and configure app details and policy settings. To configure Citrix mobile productivity apps for Android Enterprise, add them as MDX apps. For information about the app policies that are available for each device platform type, see:

- MAM SDK overview
- MDX Policies at a Glance

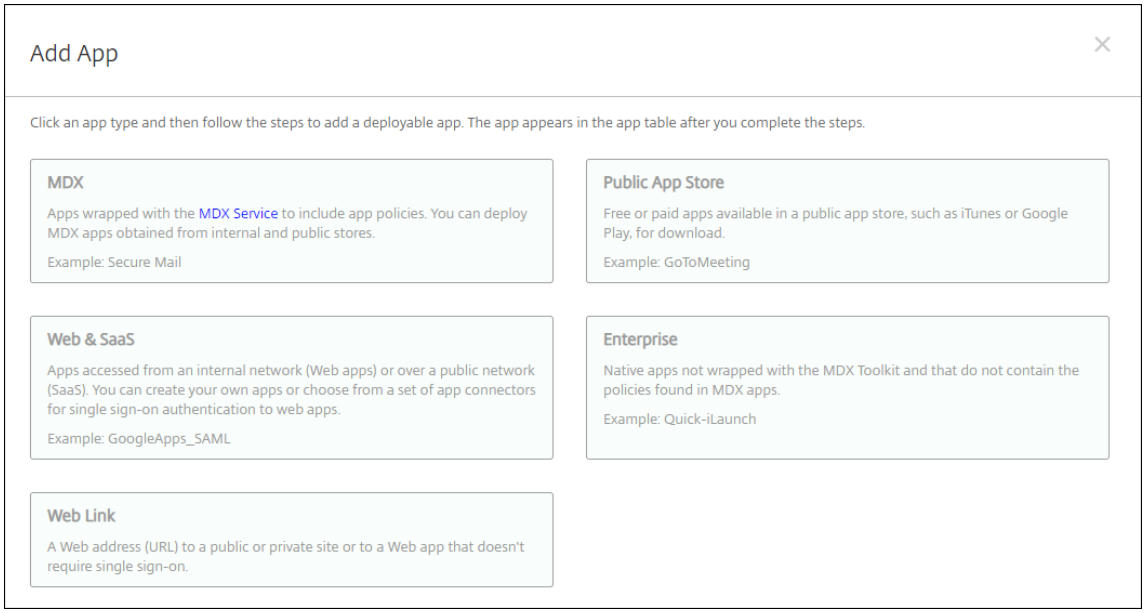
Step 1: Add and configure apps

1. For Citrix mobile productivity apps, download the public-store MDX files: Go to https://www.citrix.com/downloads. Navigate to **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.

   For other types of MDX apps, get the MDX file.

2. In the Citrix Endpoint Management console, click **Configure > Apps**. Click **Add**. The **Add App** dialog box appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



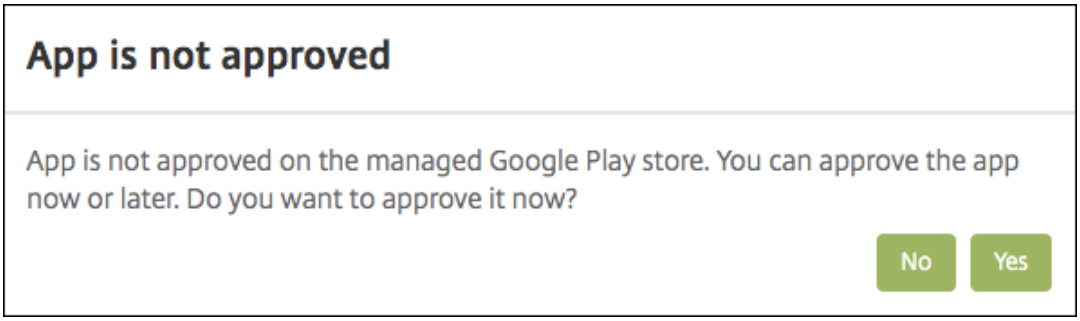
3. Click **MDX**. The **MDX App Information** page appears. In the **App Information** pane, type the following information:

   - **Name:** Type a descriptive name for the app. The name appears under **App Name** on the **Apps** table.
   - **Description:** Type an optional description of the app.

4. Select **Android Enterprise** as the platform.

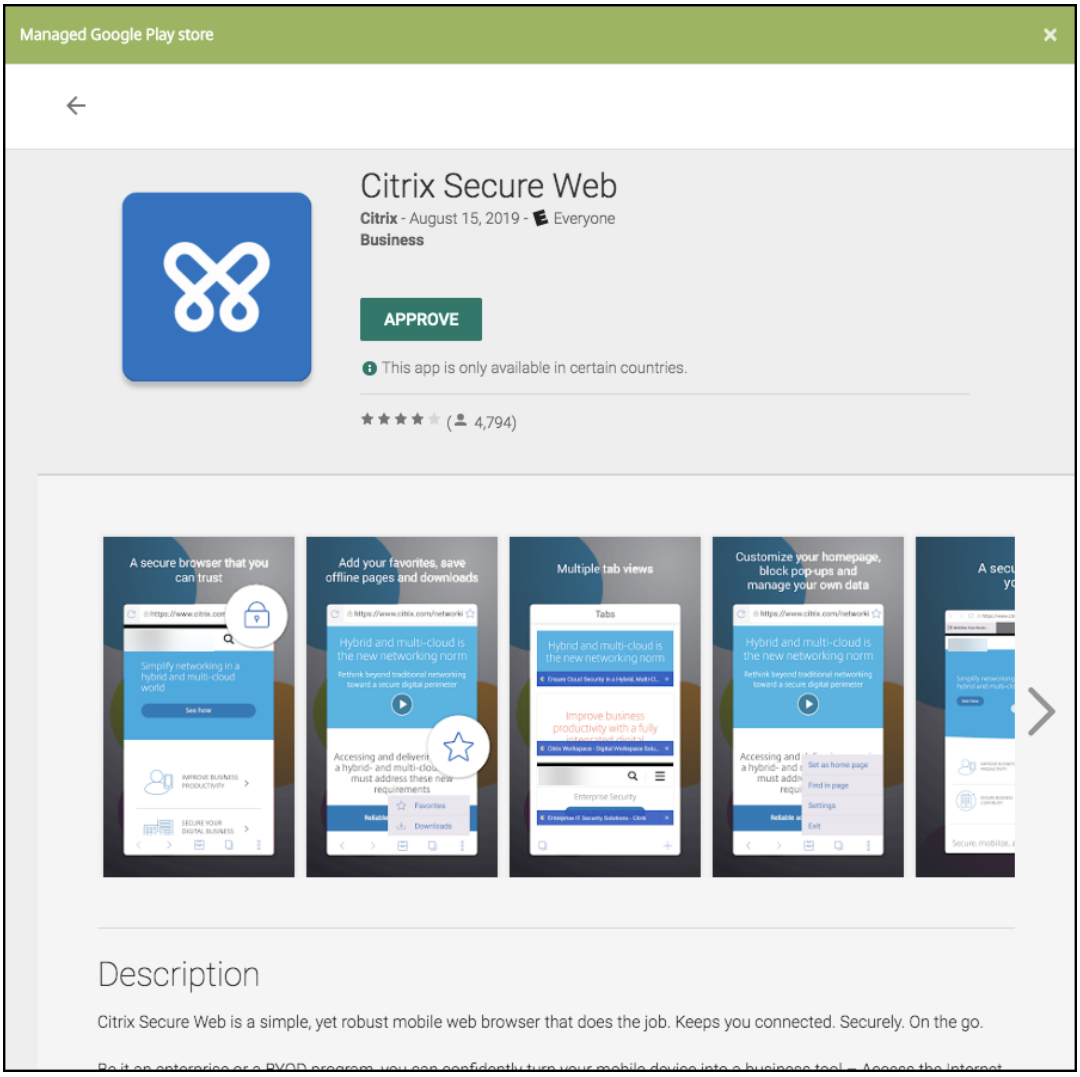
5. Click **Upload** and navigate to the MDX file. Android Enterprise only supports apps prepared with the MAM SDK or MDX Toolkit.

   - The UI notifies you if the attached application requires approval from the managed Google Play Store. To approve the application without leaving the Citrix Endpoint Management console, click **Yes**.

     After the managed Google Play Store opens, follow the instructions to approve and save the app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



When you successfully add the app, the **App details** page appears.

6. Configure these settings:

   - **File name:** Type the file name associated with the app.
   - **App Description:** Type a description for the app.
   - **App version:** Optionally, type the app version number.
   - **Package ID:** Type the package ID for the app got from the managed Google Play Store.
   - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
   - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
   - **Excluded devices:** Optionally, type the manufacturer or models of devices that can't run the app.

7. Configure the **MDX Policies**. MDX policies vary by platform and include options for policy ar-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

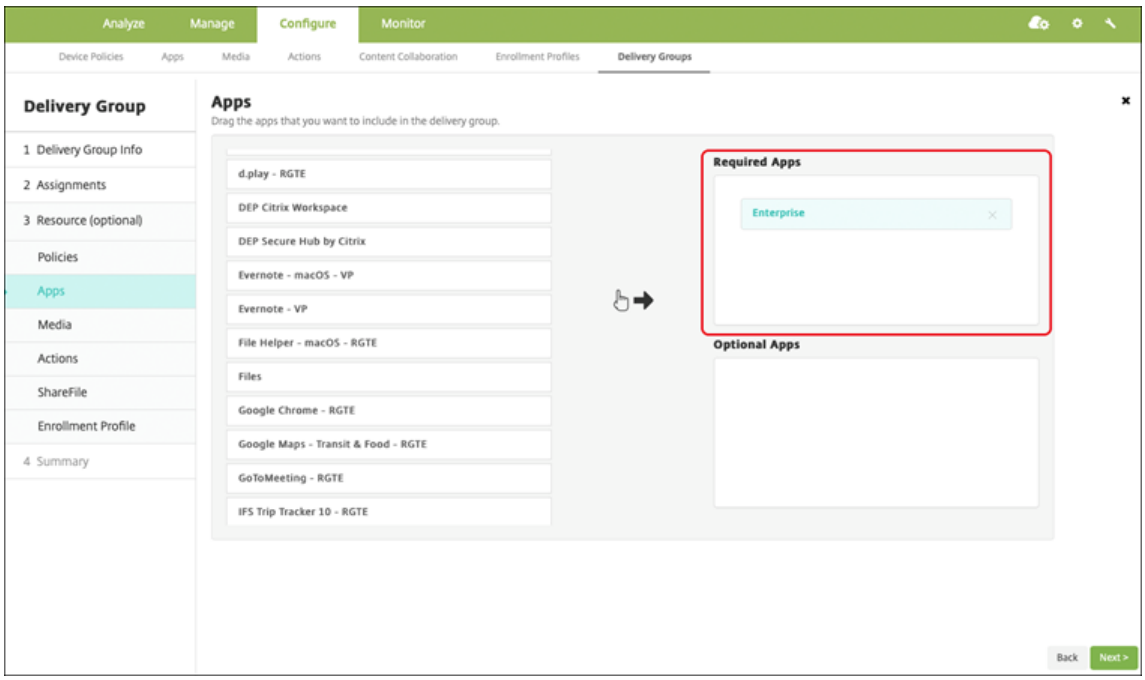
eas, including authentication, device security, and app restrictions. In the console, each of the policies has a tooltip that describes the policy. For information about the app policies that are available for each device platform type, see:

- MAM SDK overview
- MDX Policies at a Glance

8. Configure the deployment rules and store configuration.
9. Assign any delivery groups to the app and click **Save**. For information, see Deploy resources.

Step 2: Configure app deployment

1. Navigate to **Configure > Delivery Groups** and select the delivery group you configured. Click **Edit**.
2. In the **Apps** section, drag the desired apps to the **Required Apps** box.



3. On the **Summary** page, click **Save**.
4. On the **Delivery Groups** page, select the delivery group and click **Deploy**.

Enterprise apps

Enterprise apps represent private apps that aren't prepared with the MAM SDK or MDX Toolkit. You develop these apps yourself or get them directly from other sources. To add an enterprise app, you

© 1997–2025 Citrix Systems, Inc. All rights reserved.

need the APK file associated with the app. Make sure that you follow Google Best practices for private apps.

Watch this video to learn more:

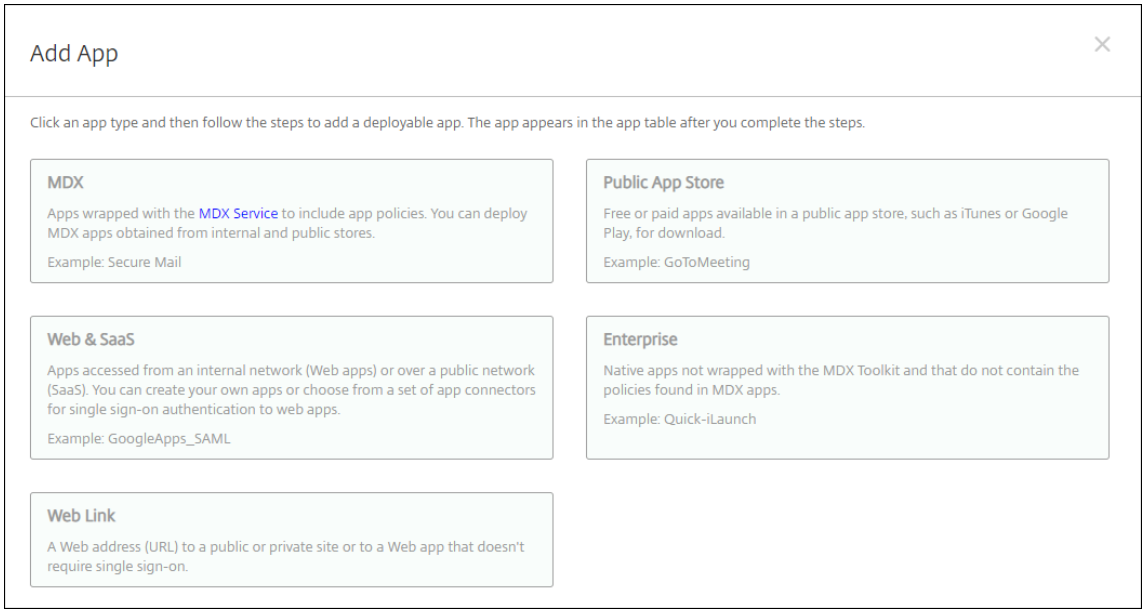
Step 1: Add and configure apps

Add the app one of two ways:

- Publish the app directly to the managed Google Play Store and add it to the Citrix Endpoint Management console as a Managed play store app. Follow the Google documentation on how to Publish private apps, and then follow the steps in the Managed app store apps section.
- Add the app to the Citrix Endpoint Management console as an enterprise app. Do the following steps:

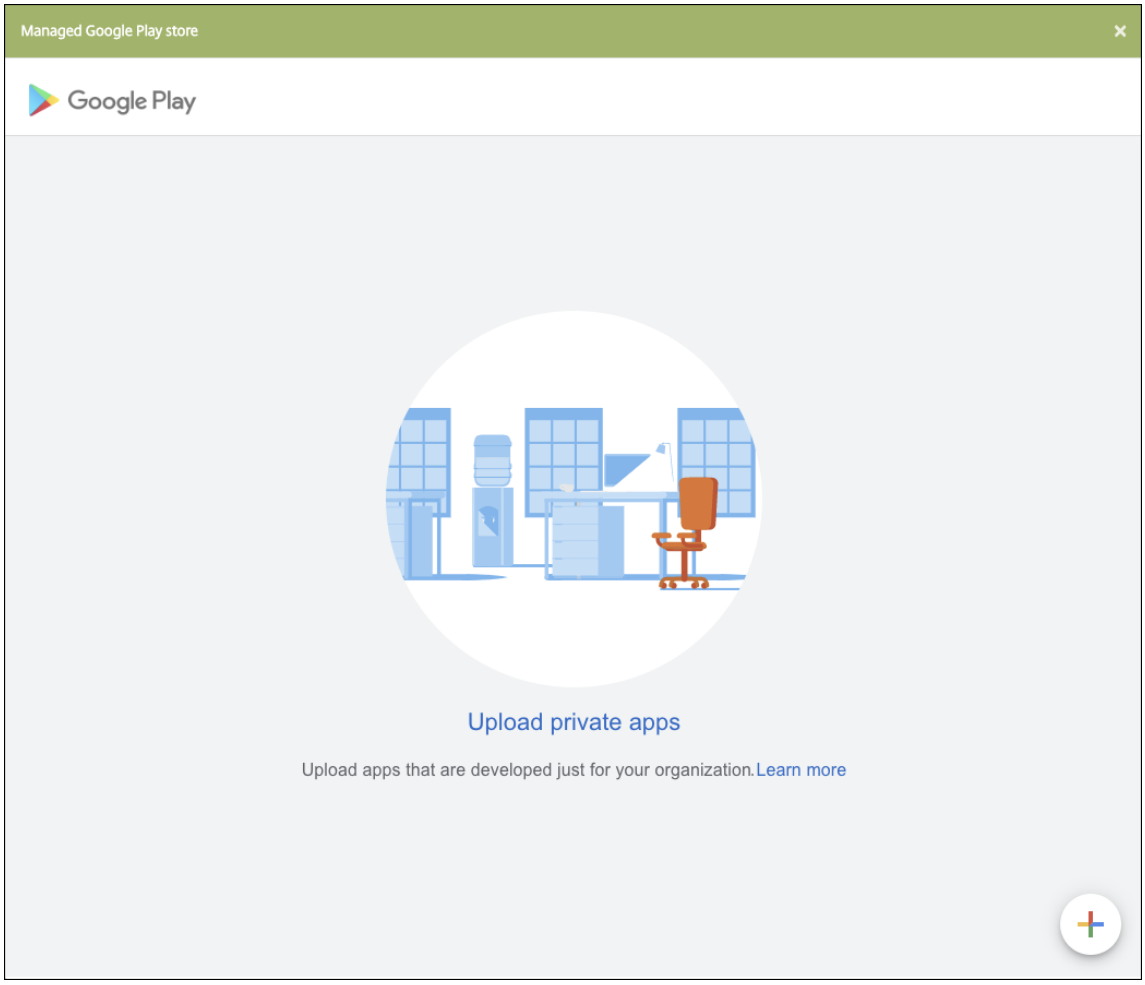
1. In the Citrix Endpoint Management console, click **Configure > Apps**. Click **Add**. The **Add App** dialog box appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



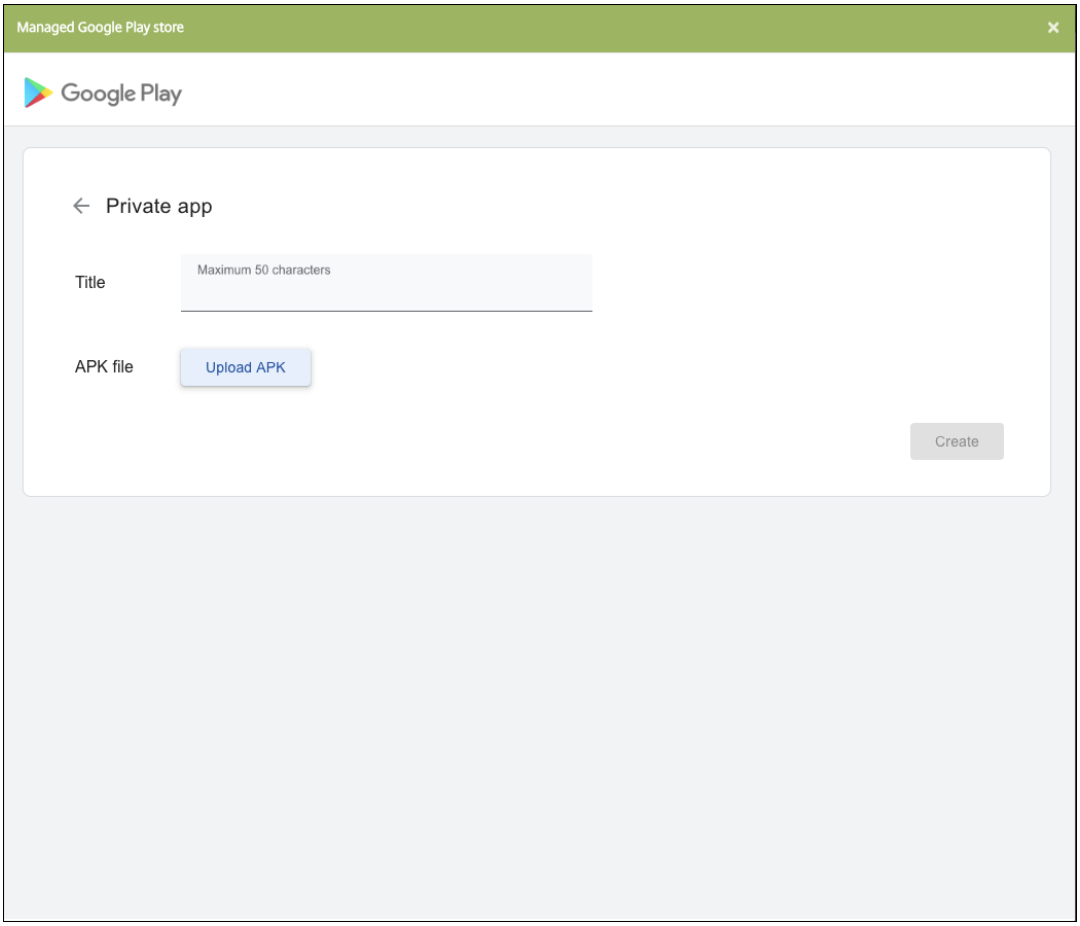
2. Click **Enterprise**. In the **App Information** pane, type the following information:
   - **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
   - **Description:** Type an optional description of the app.
3. Select **Android Enterprise** as the platform.
4. The **Upload** button opens the managed Google Play Store. You do not need to register for a developer account to publish a private app. Click the **Plus** icon in the lower right corner to continue.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



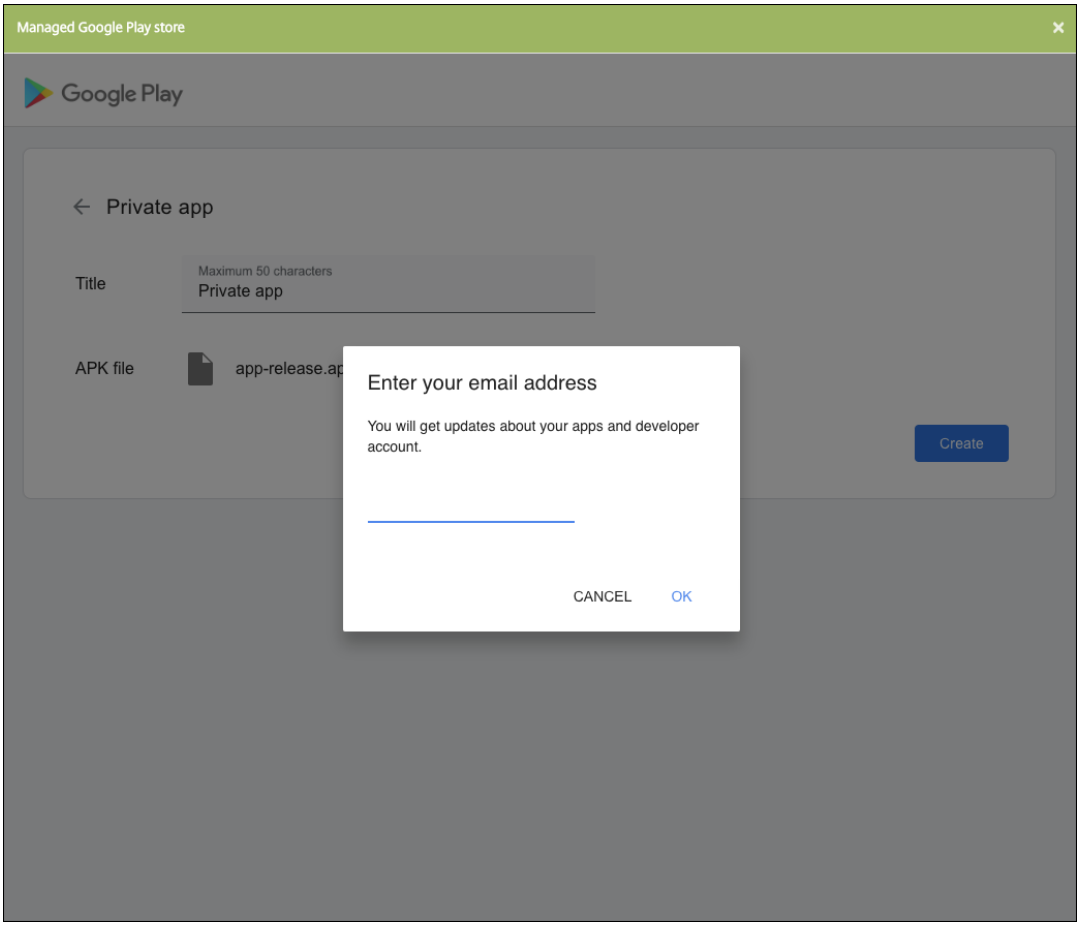
a) Type the name for your app and upload the .apk file. When finished, click **Create**. It might take up to 10 minutes for your private app to publish.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



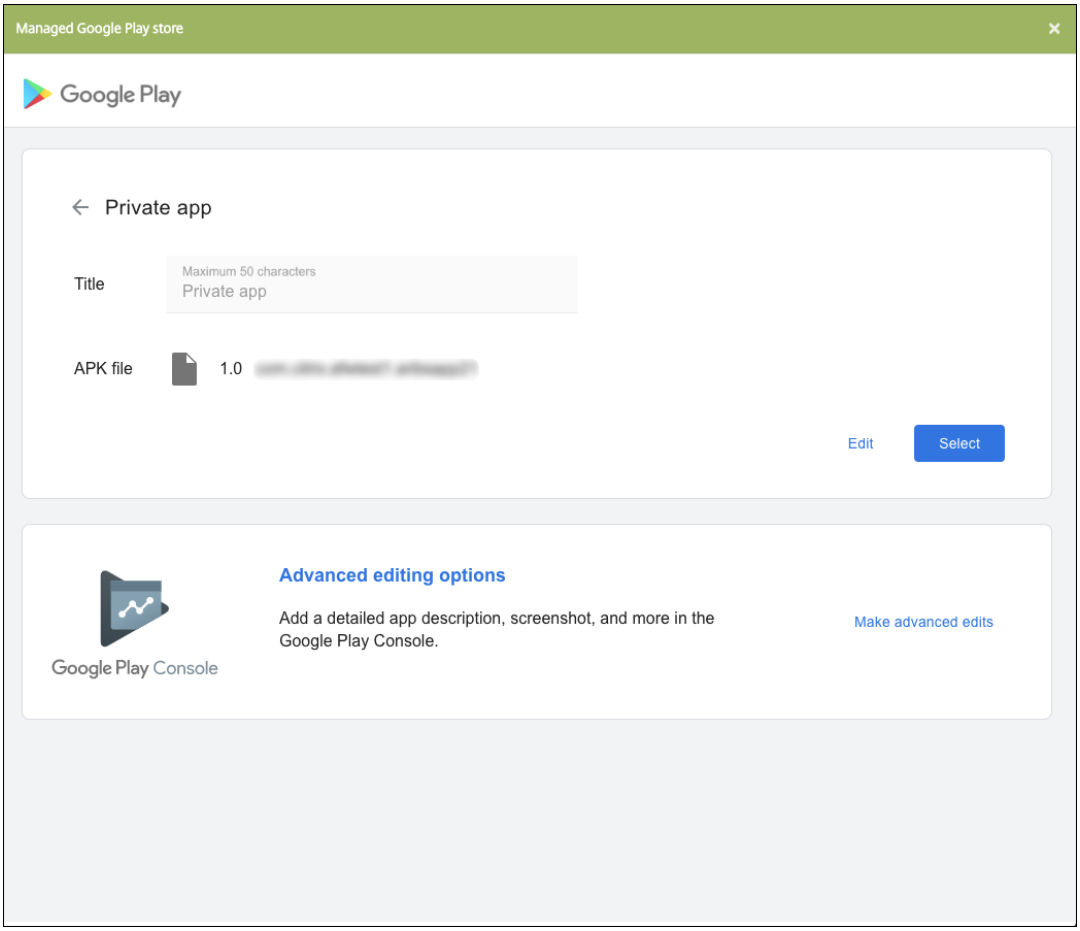
b) Enter an email address to get updates about your apps.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



c) After your application is published, click the icon for the private app. If you want to add an app description, change the app icon, and other actions, click **Make advanced edits**. Otherwise, click **Select** to open the app information page.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

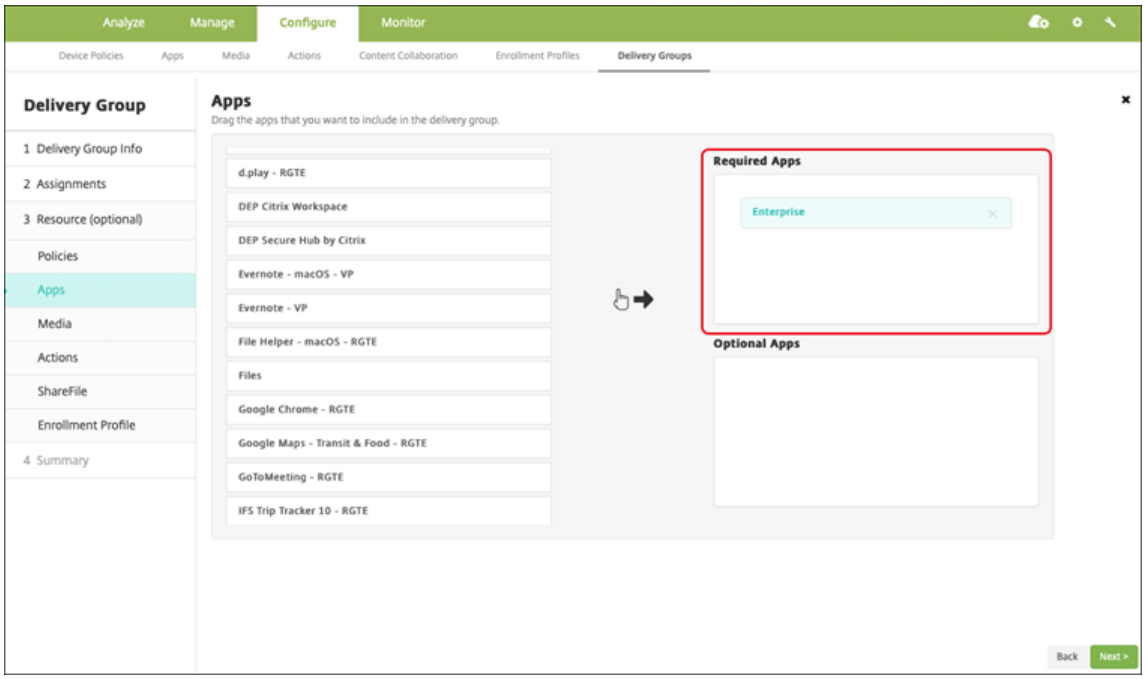


5. Click **Next**. The app information page for the platform appears.
6. Configure the settings for the platform type, such as:
   - **File name:** Optionally, type a new name for the app.
   - **App description:** Optionally, type a new description for the app.
   - **App version:** You can't change this field.
   - **Package ID:** Unique identifier of your app.
   - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
   - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
   - **Excluded devices:** Optionally, type the manufacturer or models of devices that can't run the app.
7. Configure the deployment rules and store configuration.
8. Assign any delivery groups to the app and click **Save**. For information, see Deploy resources.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Step 2: Configure app deployment

1. Navigate to **Configure > Delivery Groups** and select the delivery group you configured. Click **Edit**.
2. In the **Apps** section, drag the desired apps to the **Required Apps** box.



3. On the **Summary** page, click **Save**.
4. On the **Delivery Groups** page, select the delivery group and click **Deploy**.

MDX-enabled private apps

To add Android Enterprise apps as MDX-enabled enterprise apps:

1. Create a private Android Enterprise app and MDX-enable the app.
2. Add the app to the Citrix Endpoint Management console.
    - Host and publish the app on the managed Google Play Store.
    - Add the app to the Citrix Endpoint Management console as an Enterprise app.
3. Add the MDX file to Citrix Endpoint Management.

If you decide to host and publish apps through the Google Play Store, don't opt in for Google certificate signing. Sign the app with the same certificate used to MDX-enable the app. For more information on publishing apps, see Google documentation on Publishing your app and Signing your app. The MAM SDK doesn't wrap apps, so it doesn't require a certificate other than the one used to develop the app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For more information about publishing private apps through the Google Play Console, see the Google documentation on how to Publish private apps from the Play Console.

To publish an app through Citrix Endpoint Management, see the following sections.

Prepare an Android Enterprise app

When you create an Android Enterprise app, make sure that you follow Google Best practices for private apps.

After you create an Android Enterprise app, integrate the MAM SDK with the app or wrap the app by using the MDX Toolkit. Then, add the resulting files to XenMobile.

You can update the app by uploading an updated.apk file. The following steps cover app wrapping with the MDX Toolkit.

1. Create your Android Enterprise app and generate a signed .apk file.
2. The following sample file has all known policies, some of which might not be applicable for your environment. Any unusable settings are ignored. Create an XML file with the following parameters:

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileAppPolicies>
    <PolicySchemaVersion>
        1.0
    </PolicySchemaVersion>
    <Policies>
        <DevicePasscode>false</DevicePasscode>
        <AppPasscode>false</AppPasscode>
        <MaxOfflinePeriod>72</MaxOfflinePeriod>
        <StepupAuthAddress/>
        <RequireUserEntropy>false</RequireUserEntropy>
        <BlockRootedDevices>true</BlockRootedDevices>
        <BlockDebuggerAccess>false</BlockDebuggerAccess>
        <RequireDeviceLock>false</RequireDeviceLock>
        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
           NonCompliantDeviceBehavior>
        <WifiOnly>false</WifiOnly>
        <RequireInternalNetwork>false</RequireInternalNetwork>
        <InternalWifiNetworks/>
        <AllowedWifiNetworks/>
        <UpgradeGracePeriod>168</UpgradeGracePeriod>
        <WipeDataOnAppLock>false</WipeDataOnAppLock>
        <ActivePollPeriod>60</ActivePollPeriod>
        <PublicFileAccessLimitsList/>
        <CutAndCopy>Unrestricted</CutAndCopy>
        <Paste>Unrestricted</Paste>
        <DocumentExchange>Unrestricted</DocumentExchange>
        <OpenInExclusionList/>
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
28          <InboundDocumentExchange>Unrestricted</
                InboundDocumentExchange>
29          <InboundDocumentExchangeWhitelist/>
30          <connectionSecurityLevel>TLS</connectionSecurityLevel>
31          <DisableCamera>false</DisableCamera>
32          <DisableGallery>false</DisableGallery>
33          <DisableMicrophone>false</DisableMicrophone>
34          <DisableLocation>false</DisableLocation>
35          <DisableSms>false</DisableSms>
36          <DisableScreenCapture>false</DisableScreenCapture>
37          <DisableSensor>false</DisableSensor>
38          <DisableNFC>false</DisableNFC>
39          <BlockLogs>false</BlockLogs>
40          <DisablePrinting>false</DisablePrinting>
41          <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
                MvpnNetworkAccess>
42          <MvpnSessionRequired>False</MvpnSessionRequired>
43          <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
44          <DisableLocalhostConnections>false</
                DisableLocalhostConnections>
45          <CertificateLabel/>
46          <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
47          <DefaultLoggerLevel>15</DefaultLoggerLevel>
48          <MaxLogFiles>2</MaxLogFiles>
49          <MaxLogFileSize>2</MaxLogFileSize>
50          <RedirectSystemLogs>false</RedirectSystemLogs>
51          <EncryptLogs>false</EncryptLogs>
52          <GeofenceLongitude>0</GeofenceLongitude>
53          <GeofenceLatitude>0</GeofenceLatitude>
54          <GeofenceRadius>0</GeofenceRadius>
55          <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
56          <Authentication>OfflineAccessOnly</Authentication>
57          <ReauthenticationPeriod>480</ReauthenticationPeriod>
58          <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
59      </Policies>
60  </MobileAppPolicies>
```

3. Wrap the app using the MDX Toolkit. For information about using the MDX Toolkit, see Wrapping Android mobile apps.

   Set the **apptype** parameter to **Premium**. Use the XML file from the previous step in the command described next.

   If you know the store URL for the app, set the **storeURL** parameter to the store URL. Users download the app from the store URL after you publish the app.

   Here is an example of an MDX Toolkit command used to wrap an app called SampleAEapp:

```
1  ```
2   java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -
        Duser.variant
3   -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
4   -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
  -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
  -MinPlatform 5.0
  -keystore /MyKeystore
  -storepass mystorepwd123
  -keyalias key0
  -keypass mykeypwd123
  -storeURL "https://play.google.com/store/apps/details?id=
     SampleAEappPackage"
  -appType Premium
  -premiumMdxPolicies <Path to Premium policy XML>
```

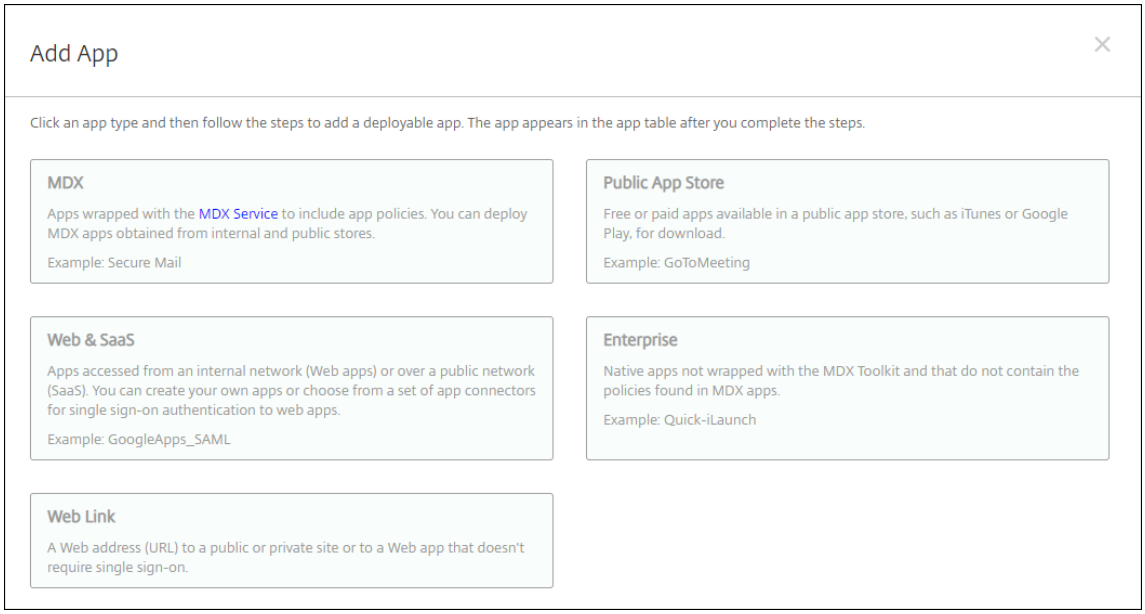
Wrapping the app generates a wrapped .apk file and an .mdx file.

Add the wrapped .apk file

Add the app one of two ways:

- Publish the app directly to the managed Google Play Store and add it to the Citrix Endpoint Management console as a Managed play store app. Follow the Google documentation on how to Publish private apps, and then follow the steps in the Managed app store apps section.
- Add the app to the Citrix Endpoint Management console as an enterprise app. Do the following steps:

1. In the Citrix Endpoint Management console, click **Configure > Apps**. The **Apps** page opens.
2. Click **Add**. The **Add App** dialog box appears.

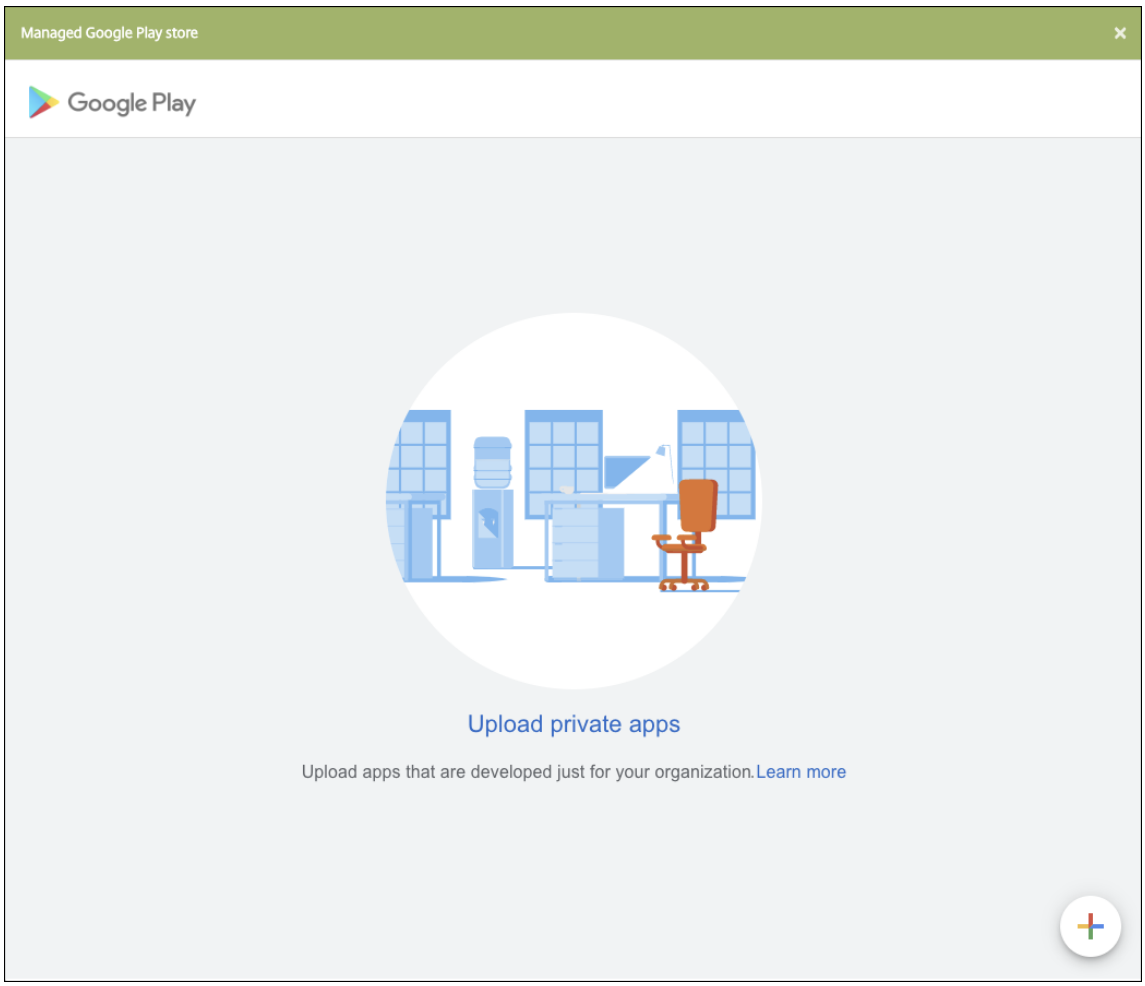


3. Click **Enterprise**. In the **App Information** pane, type the following information:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

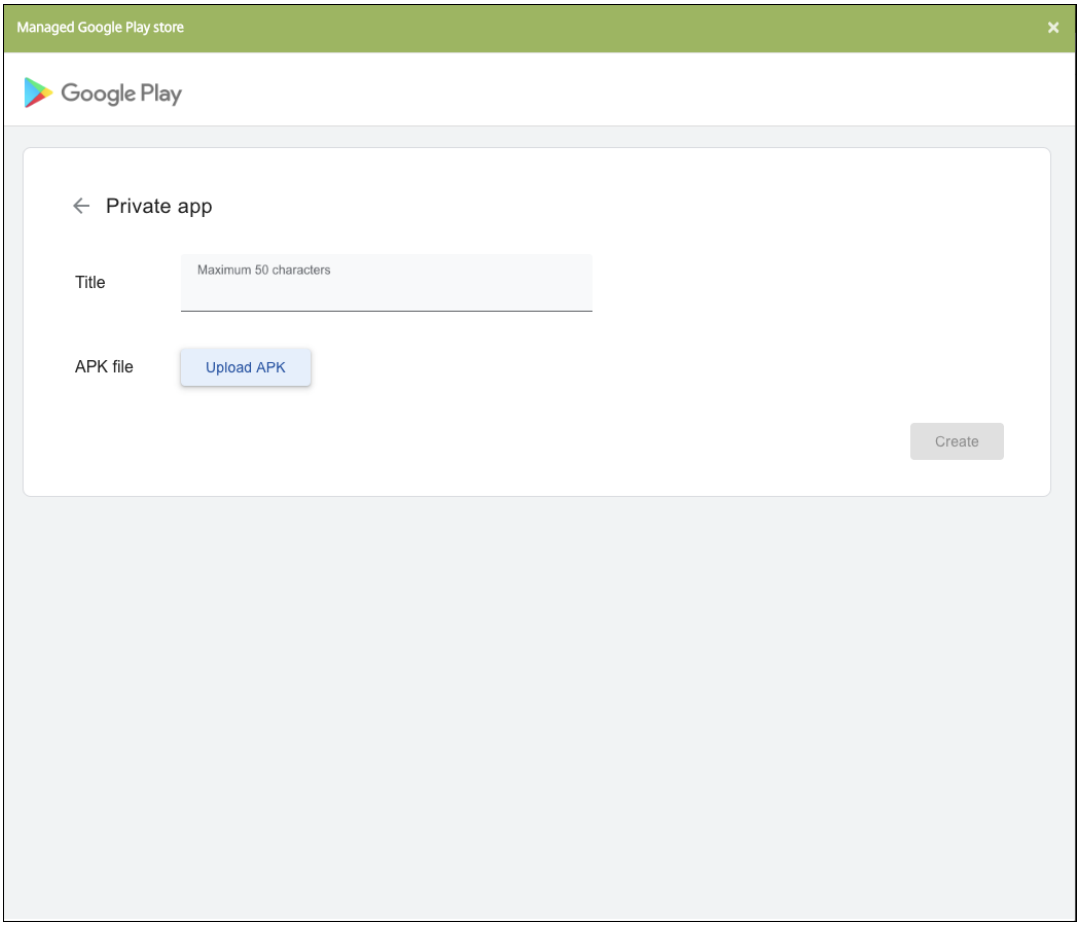
- **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
- **Description:** Type an optional description of the app.

4. Select **Android Enterprise** as the platform.
5. The **Upload** button opens the managed Google Play Store. You do not need to register for a developer account to publish a private app. Click the **Plus** icon in the lower right corner to continue.



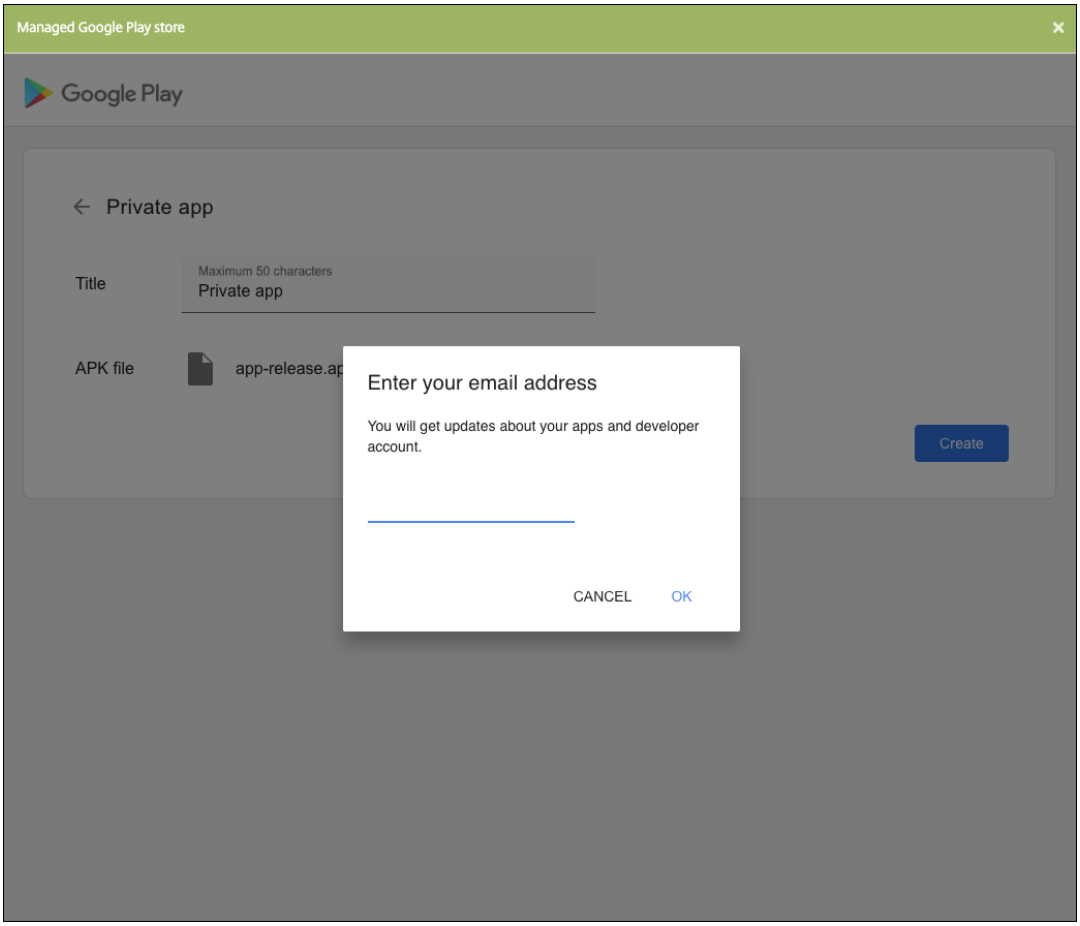
a) Type the name for your app and upload the .apk file. When finished, click **Create**. It might take up to 10 minutes for your private app to publish.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



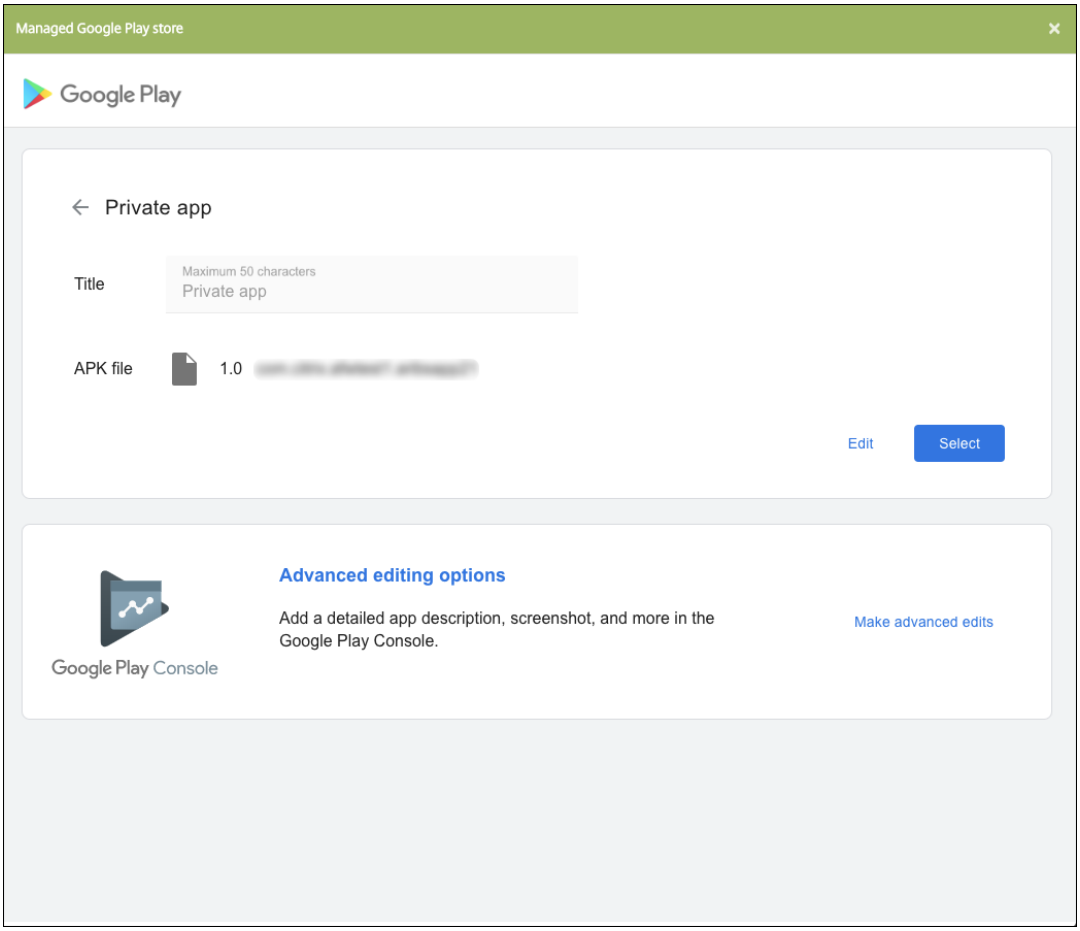
b) Enter an email address to get updates about your apps.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



c) After your application is published, click the icon for the private app and click **Select** to open the app information page.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. Click **Next**. The app information page for the platform appears.
7. Configure the settings for the platform type, such as:
   - **File name:** Optionally, type a new name for the app.
   - **App description:** Optionally, type a new description for the app.
   - **App version:** You can't change this field.
   - **Package ID:** Unique identifier of your app.
   - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
   - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
   - **Excluded devices:** Optionally, type the manufacturer or models of devices that can't run the app.
8. Configure the deployment rules and store configuration.
9. In the **Enterprise App** page, click **Next**. The **Approvals** page appears.

   To use workflows to require approval before allowing users to access the app, see Apply workflows. If you don't need an approval workflow, you can skip to Step 13.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

10. Click **Next**.
11. The **Delivery Group Assignment** page appears. No action is needed on this page. You configure the delivery groups and deployment schedule for this app when you add the .mdx file. Click **Save**.

Optional: Add or change the store URL

If you didn't know the store URL when you wrapped the app, add the store URL now.

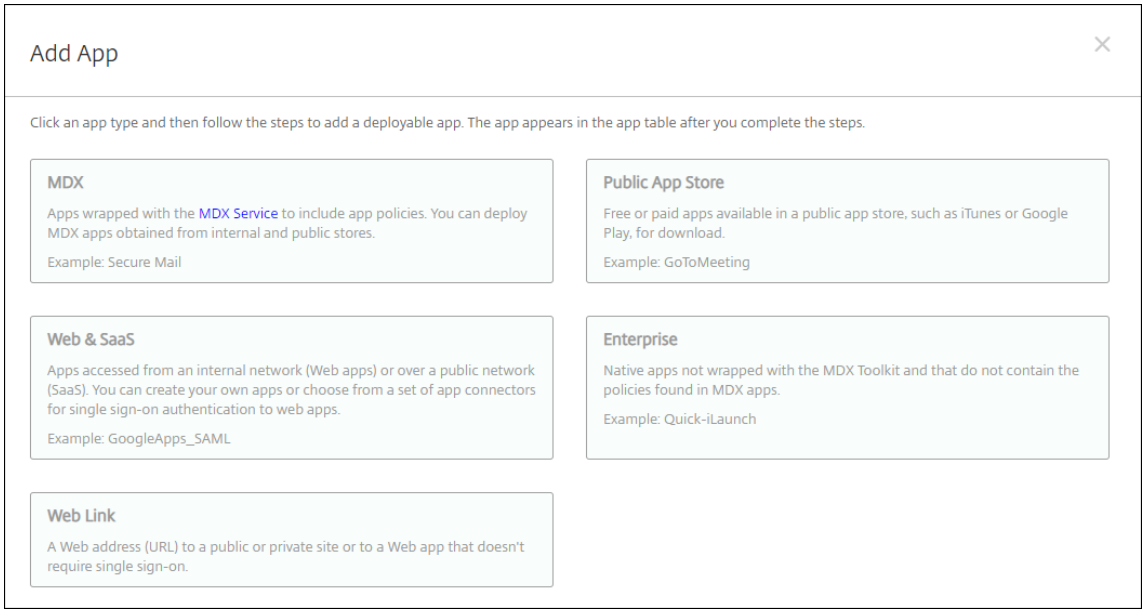
1. View the app in the managed Google Play Store. When you select the app, the store URL appears in the address bar of your browser. Copy the package name of the app from the URL form. For example: `https://play.google.com/store/apps/details?id=SampleAEappPackage`. The URL you copy might begin with `https://play.google.com/work/`. Make sure that you change `work` to `store`.
2. Use the MDX Toolkit to add the store URL to the .mdx file:

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \
setinfo \
-in ~/Desktop/SampleApps/Sample.mdx \
-out ~/Desktop/SampleApps/wrapped/Sample.mdx \
-storeURL "https://play.google.com/store/apps/details?id=
   SampleAEappPackage"
```

Add the .mdx file

1. In the Citrix Endpoint Management console, click **Configure > Apps**. Click **Add**. The **Add App** dialog box appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



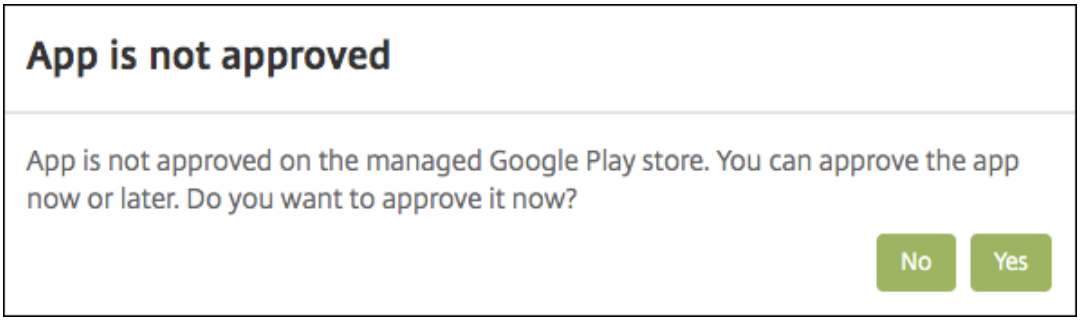
2. Click **MDX**. The **MDX App Information** page appears. In the **App Information** pane, type the following information:

   - **Name:** Type a descriptive name for the app. The name appears under **App Name** on the **Apps** table.
   - **Description:** Type an optional description of the app.

3. Select **Android Enterprise** as the platform.

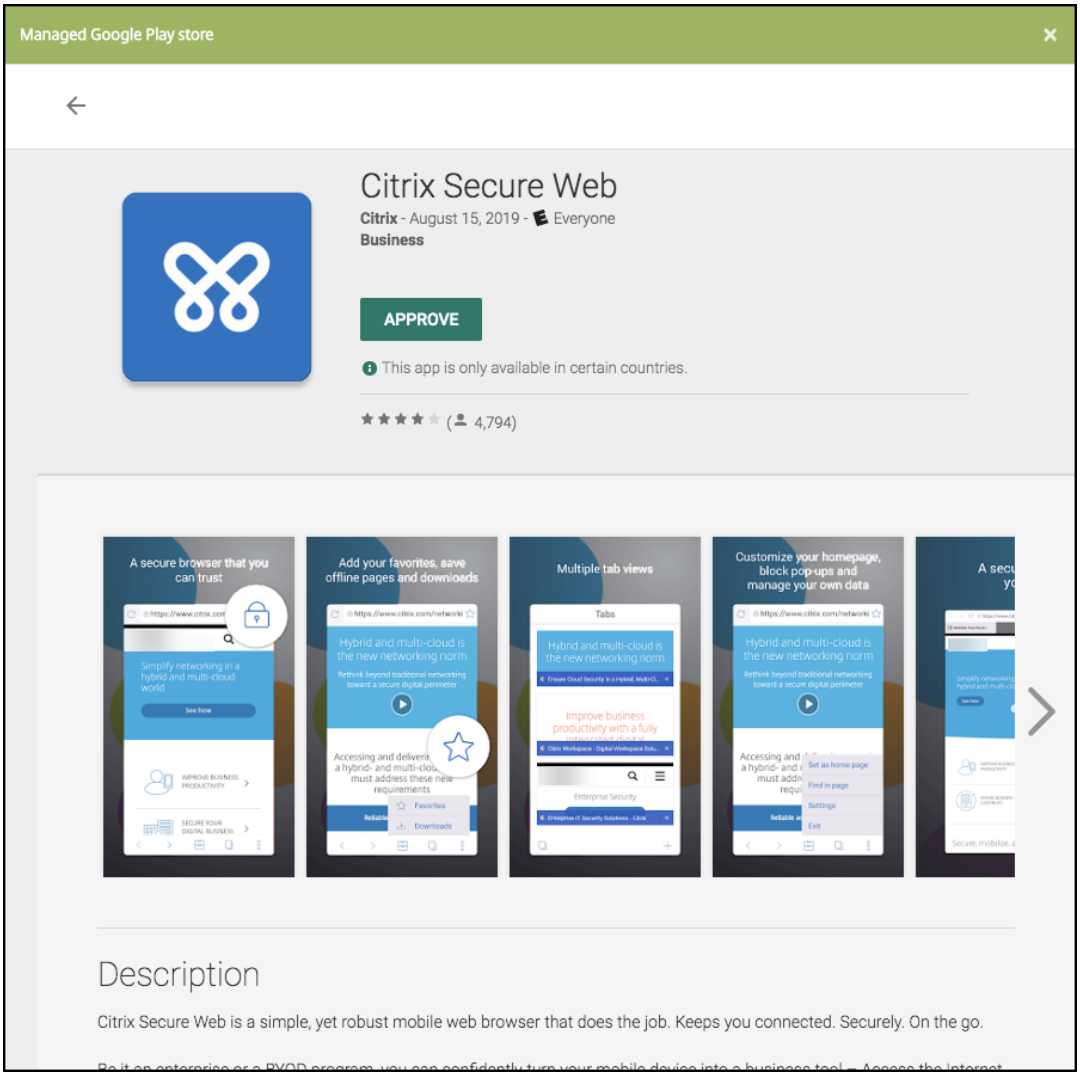
4. Click **Upload** and navigate to the MDX file. Android Enterprise only supports apps wrapped with the MDX Toolkit.

   - The UI notifies you if the attached application requires approval from the managed Google Play Store. To approve the application without leaving the Citrix Endpoint Management console, click **Yes**.

     After the managed Google Play Store opens, follow the instructions to approve and save the app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



When you successfully add the app, the **App details** page appears.

5. Configure these settings:

   - **File name:** Type the file name associated with the app.
   - **App Description:** Type a description for the app.
   - **App version:** Optionally, type the app version number.
   - **Package ID:** Type the package ID for the app got from the managed Google Play Store.
   - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
   - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
   - **Excluded devices:** Optionally, type the manufacturer or models of devices that can't run the app.

6. Configure the **MDX Policies**. MDX policies vary by platform and include options for policy ar-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

eas, including Authentication, Device Security, and App Restrictions. In the console, each of the policies has a tooltip that describes the policy. For information about the app policies that are available for each device platform type, see:

- MAM SDK overview
- MDX third-party app policies at a glance

7. Configure the deployment rules and store configuration.

   The **Deploy for always-on connection** applies when you've configured the scheduling background deployment key in **Settings > Server Properties**.

   The always-on option:

   - Isn't available for iOS devices
   - Isn't available for Android and Android Enterprise customers who began using Citrix Endpoint Management with version 10.18.19 or later
   - Isn't recommended for Android and Android Enterprise customers who began using Citrix Endpoint Management before version 10.18.19

   The deployment schedule that you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

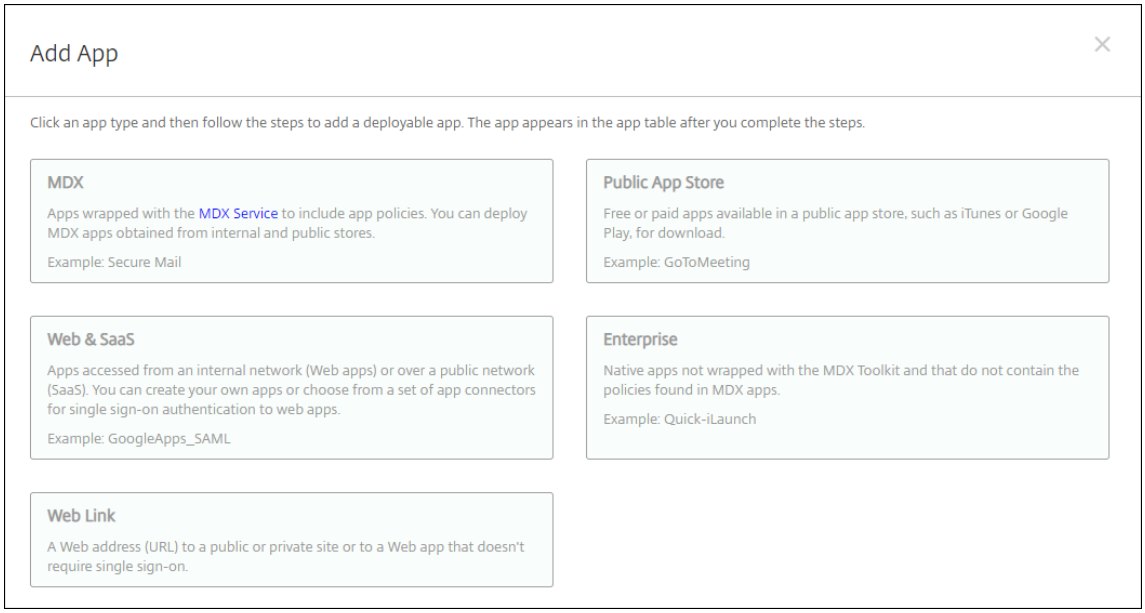
8. Assign any delivery groups to the app and click **Save**. For information, see Deploy resources.

Update the app

To update the Android Enterprise app, wrap and upload an updated .apk file:

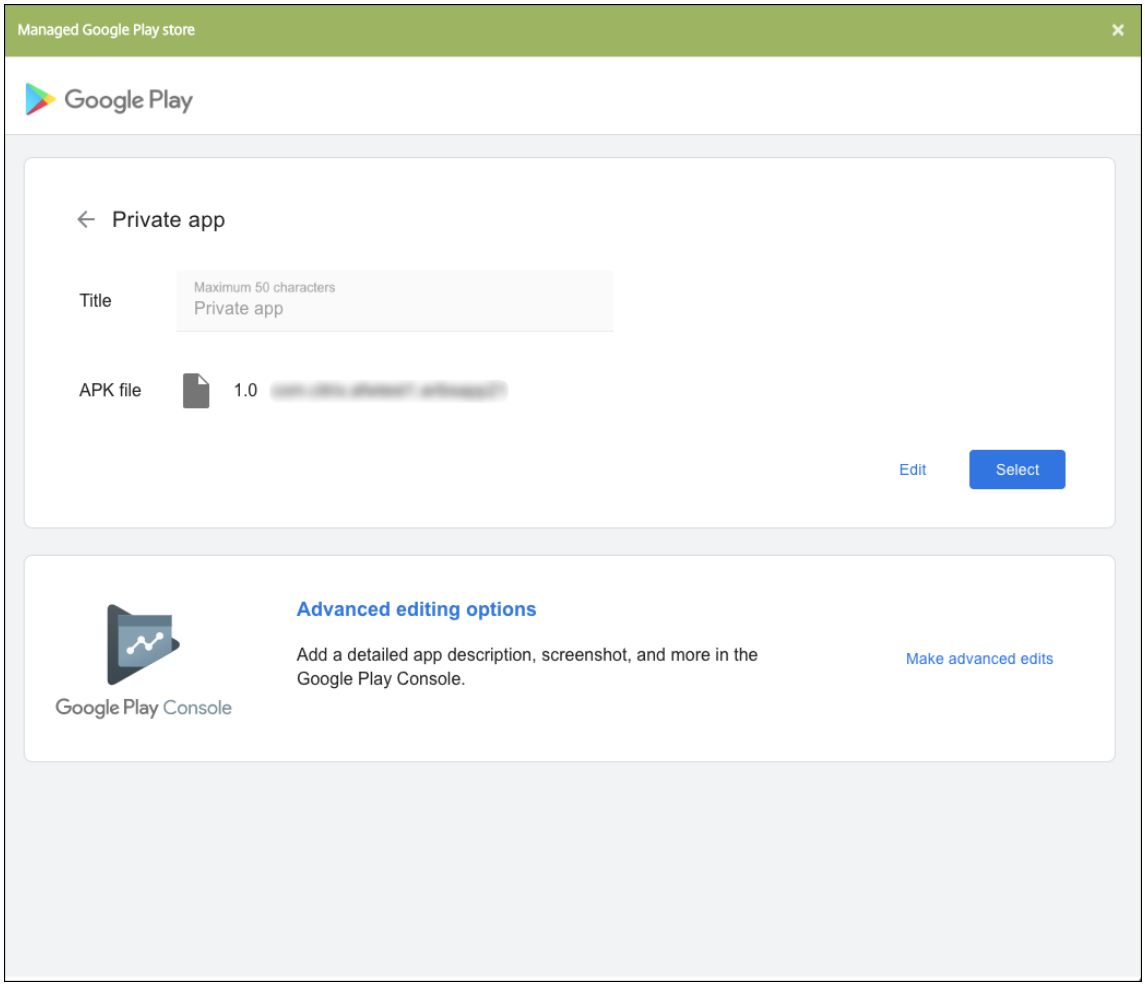
1. Wrap the .apk file for the updated app using the MAM SDK or MDX Toolkit.
2. In the Citrix Endpoint Management console, click **Configure > Apps**. The **Apps** page opens.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Click **Add**. The **Add App** dialog box appears.
4. Click **Enterprise**. In the **App Information** pane, type the following information:
   - **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
   - **Description:** Type an optional description of the app.
5. Select **Android Enterprise** as the platform.
6. Click **Next**. The **Enterprise App** page appears.
7. Click **Upload**.
8. In the managed Google Play Store page, select the app you want to update.
9. In the app information page, click **edit** next to the .apk file name.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



10. Navigate to the new .apk file and upload it.
11. In the managed Google Play Store page, click **Save**.

Legacy Android Enterprise for Google Workspace (formerly G Suite) customers

September 6, 2025

Google Workspace customers must use the legacy Android Enterprise settings to configure legacy Android Enterprise. Google recently renamed G Suite to Google Workspace.

If your organization already uses Google Workspace to provide users access to Google apps, you can use Google Workspace to register Citrix as your EMM. If your organization uses Google Workspace, it has an existing enterprise ID and existing Google Accounts for users. To use Citrix Endpoint Management with Google Workspace, you sync with your LDAP directory and retrieve Google Account

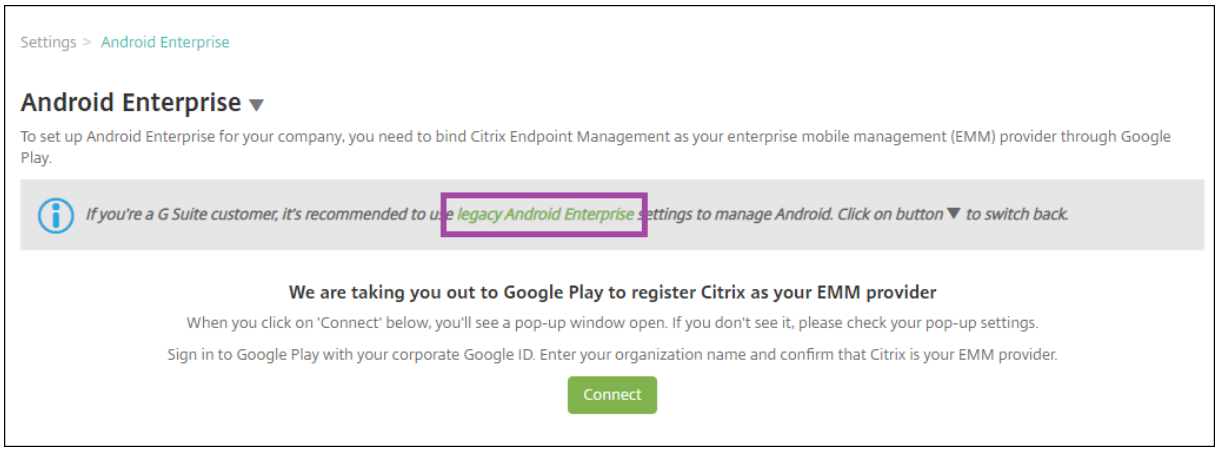
© 1997–2025 Citrix Systems, Inc. All rights reserved.

information from Google using the Google Directory API. Because this type of enterprise is tied to an existing domain, each domain can only create one enterprise. To enroll a device in Citrix Endpoint Management, each user must manually sign in with their existing Google Account. The account gives them access to managed Google Play in addition to any other Google services provided by your Google Workspace plan.

Requirements for legacy Android Enterprise:

- A publicly accessible domain
- A Google administrator account
- Android devices that have managed profile support
- A Google account that has Google Play installed
- A Work profile set up on the device

To start configuring the legacy Android Enterprise, click **legacy Android Enterprise** in the **Android Enterprise** page in Citrix Endpoint Management Settings.



Create an Android Enterprise Account

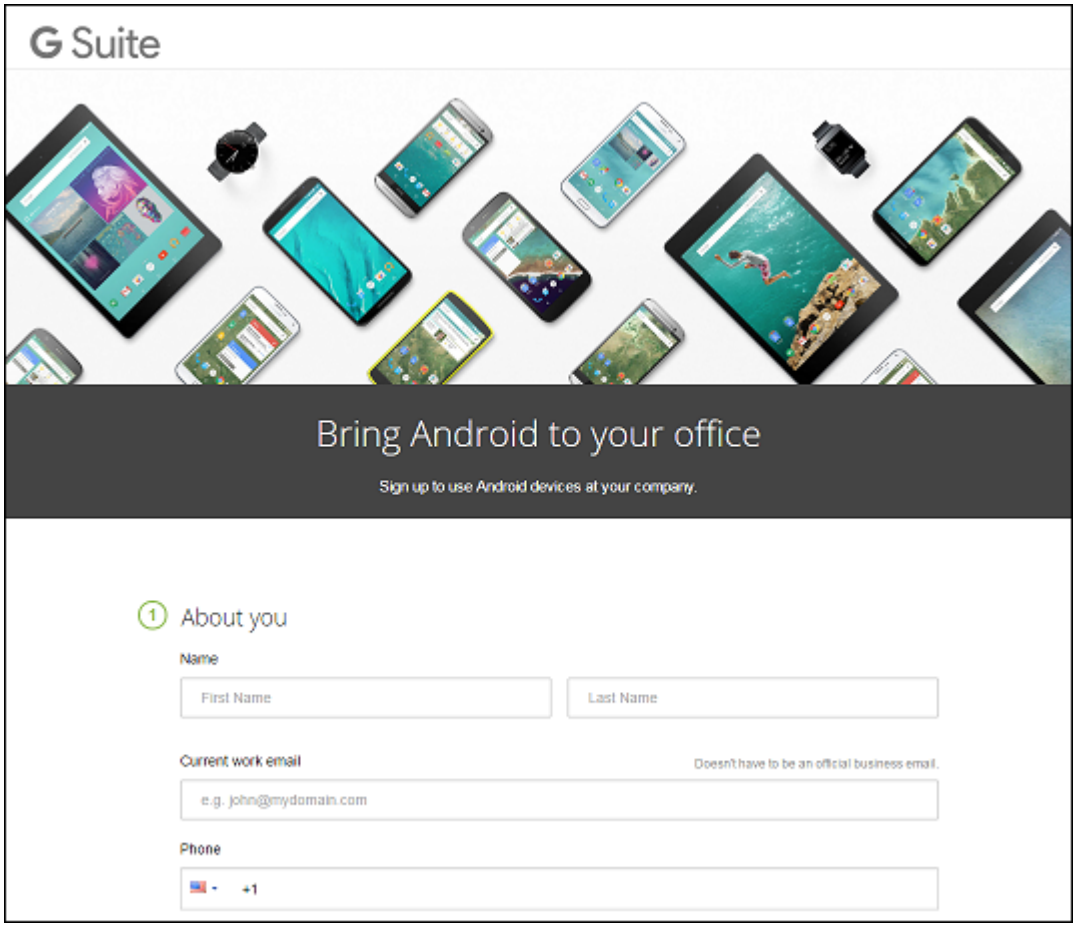
Before you can set up an Android Enterprise account, you must verify your domain name with Google.

If you have already verified your domain name with Google, you can skip to this step: Set up an Android Enterprise service account and download an Android Enterprise certificate.

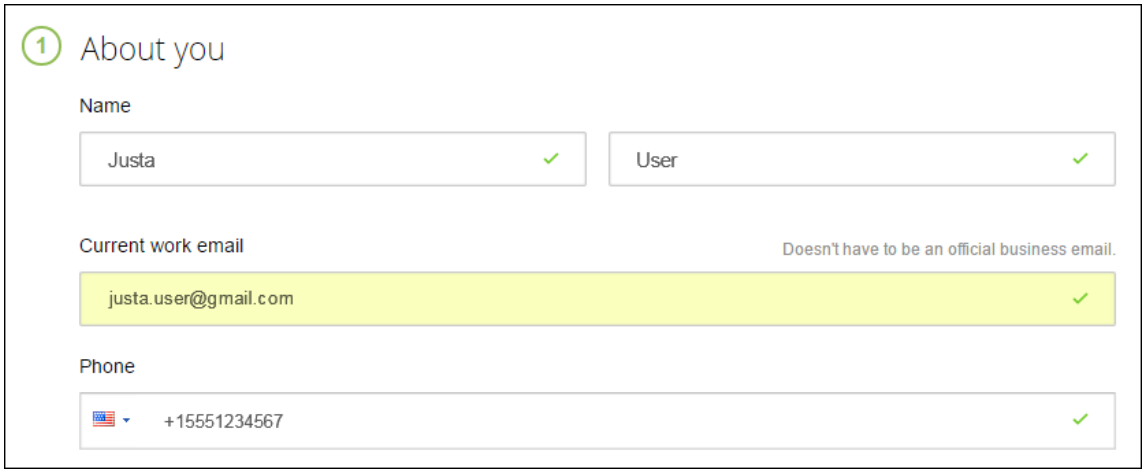
1. Navigate to https://gsuite.google.com/signup/basic/welcome.

   The following page displays where you type your administrator and company information.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

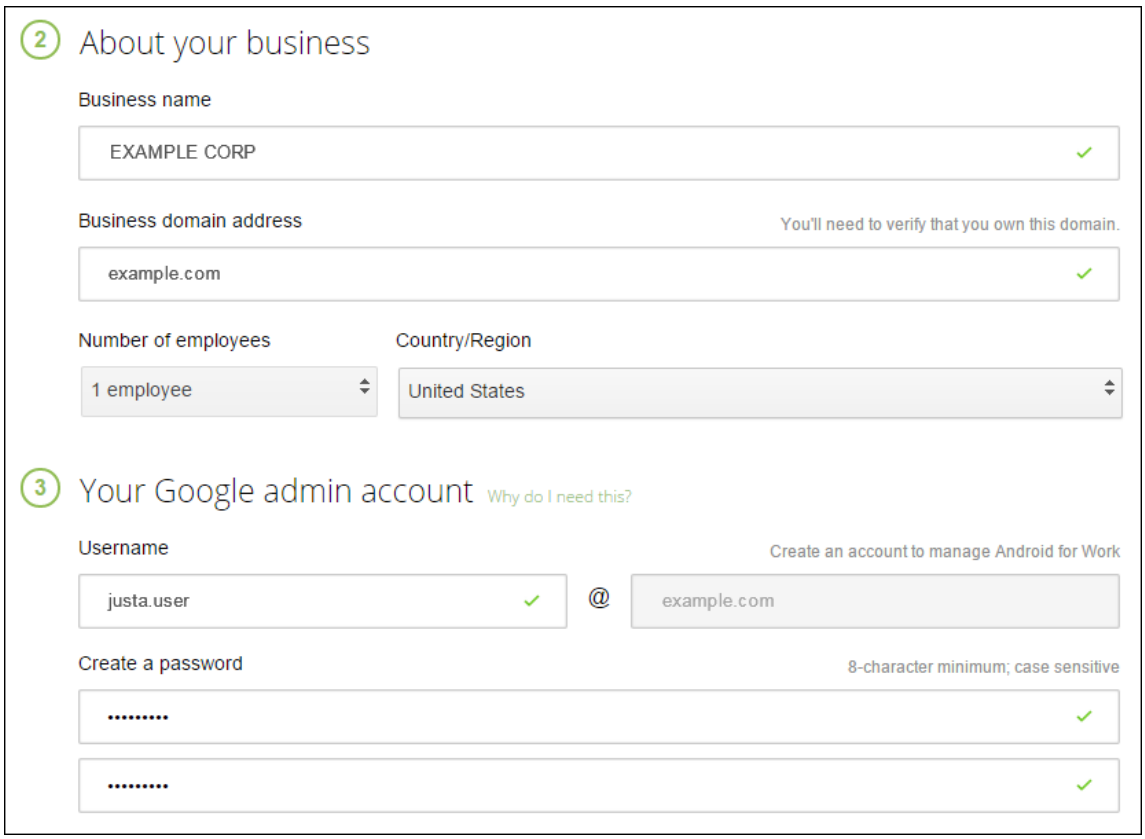


2. Type your administrator user information.



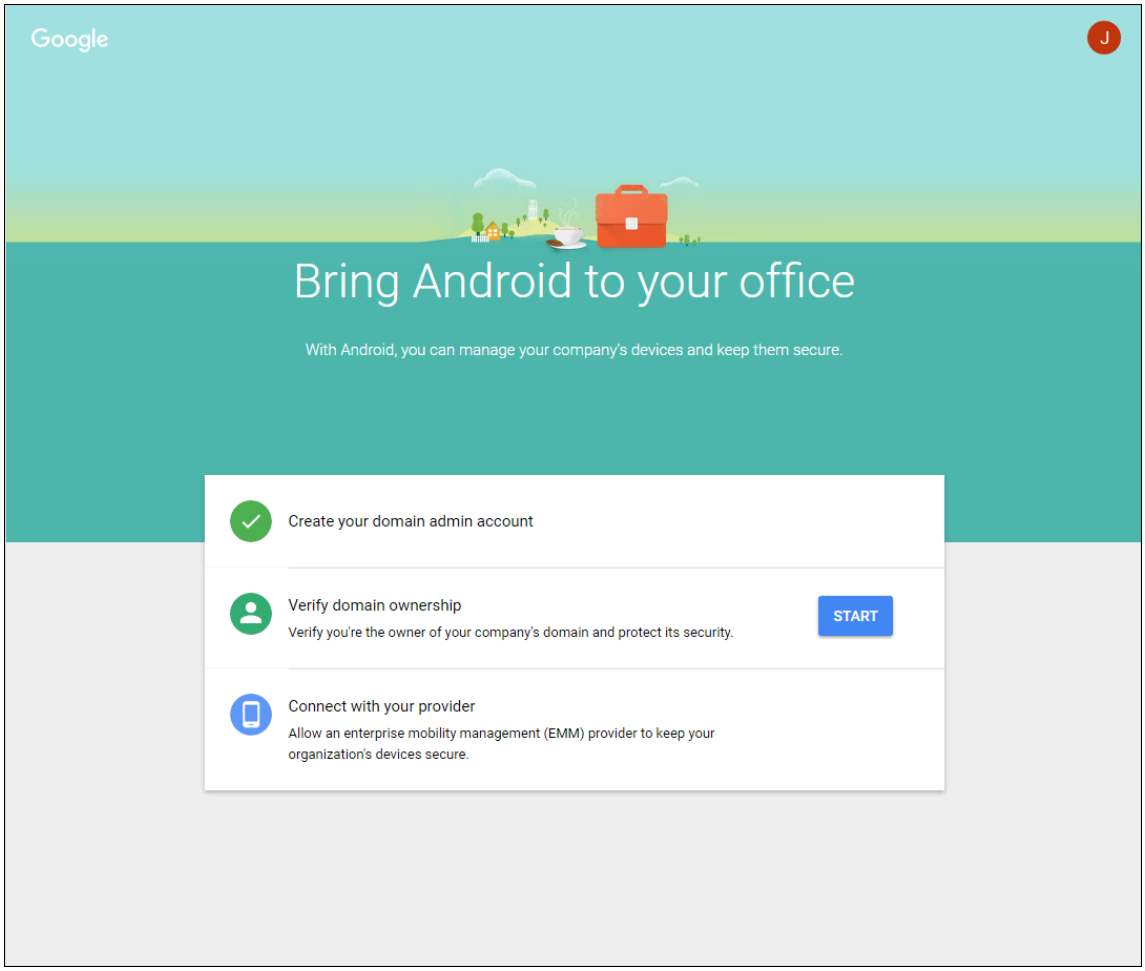
3. Type your company information, in addition to your administrator account information.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The first step in the process is complete and you see the following page.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Verify domain ownership

Allow Google to verify your domain in one of the following ways:

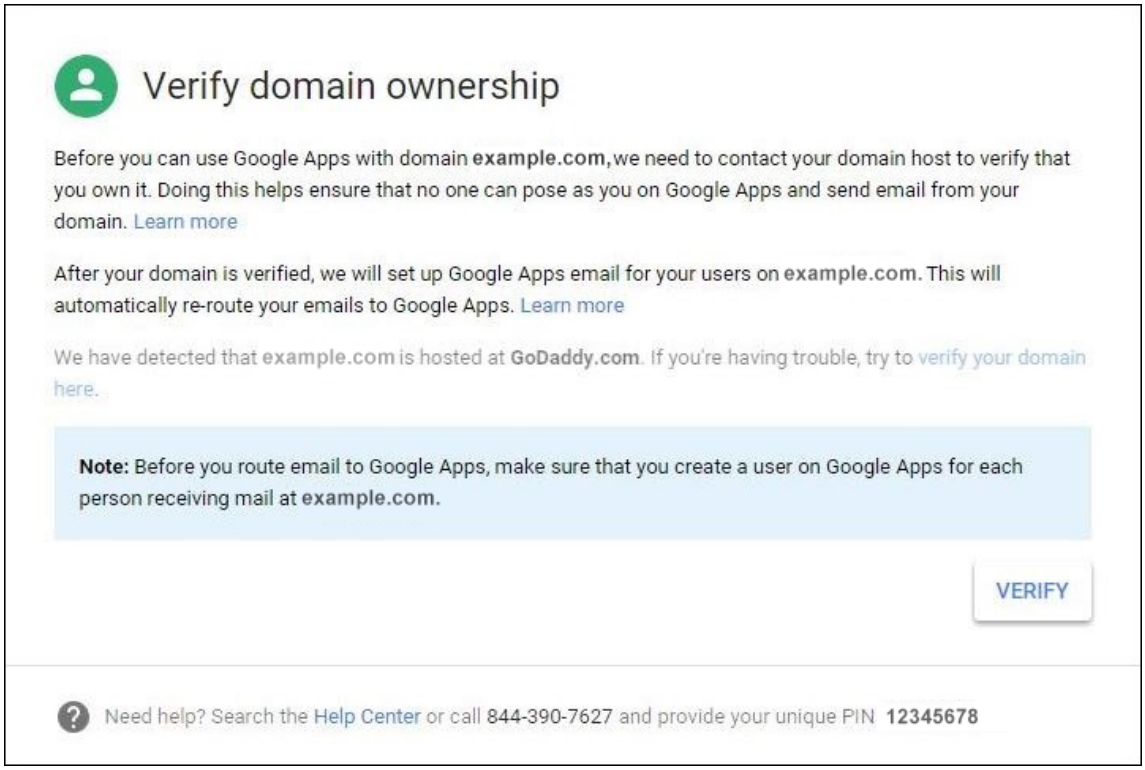
- Add a TXT or CNAME record to the website of your domain host.
- Upload an HTML file to the web server of your domain.
- Add a `<meta>` tag to your home page. Google recommends the first method. This article does not cover the steps to verify your domain ownership, but you can find the information you need here: https://support.google.com/a/answer/6248925.

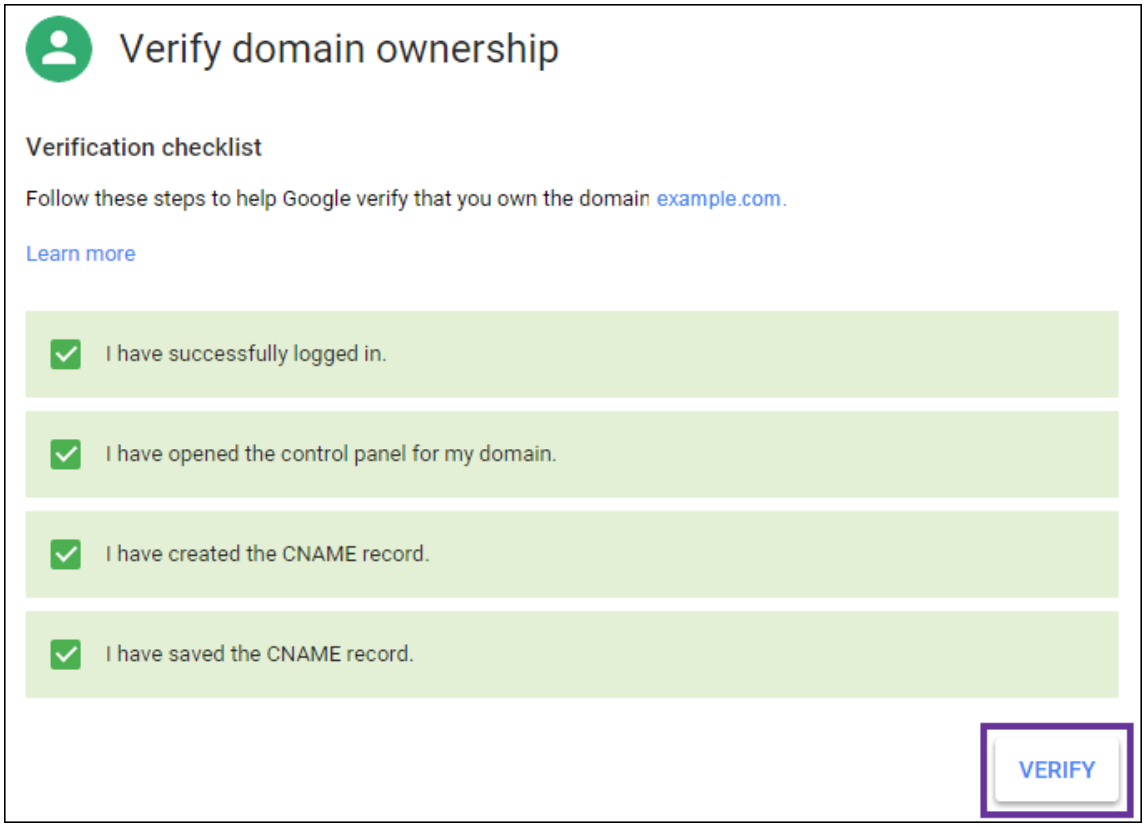
1. Click **Start** to begin the verification of your domain.

   The **Verify domain ownership** page appears. Follow the instructions on the page to verify your domain.

2. Click **Verify**.

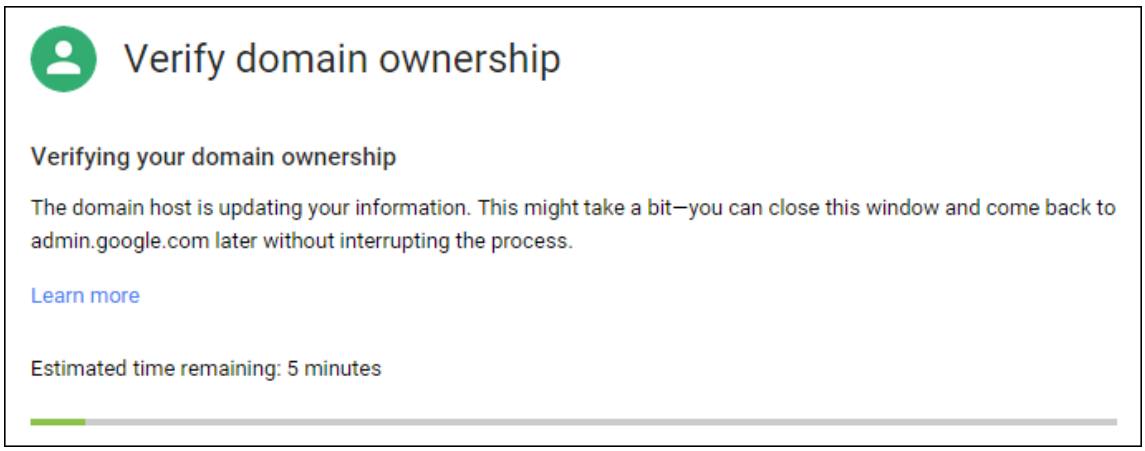
© 1997–2025 Citrix Systems, Inc. All rights reserved.



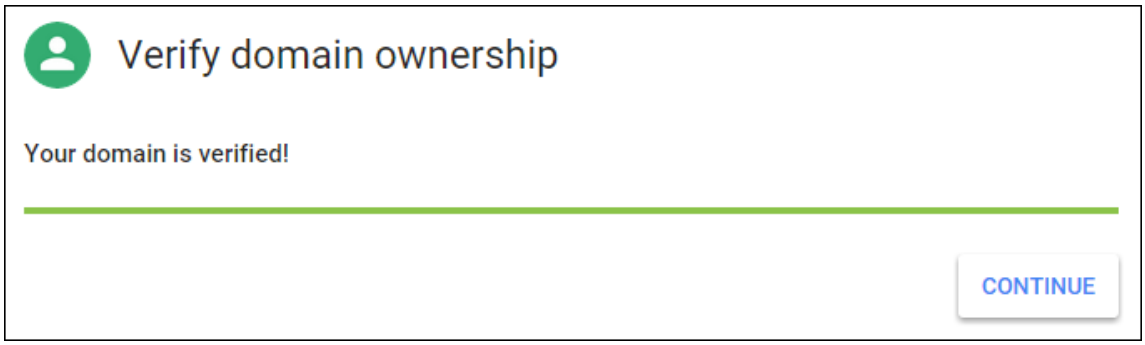


3. Google verifies your domain ownership.

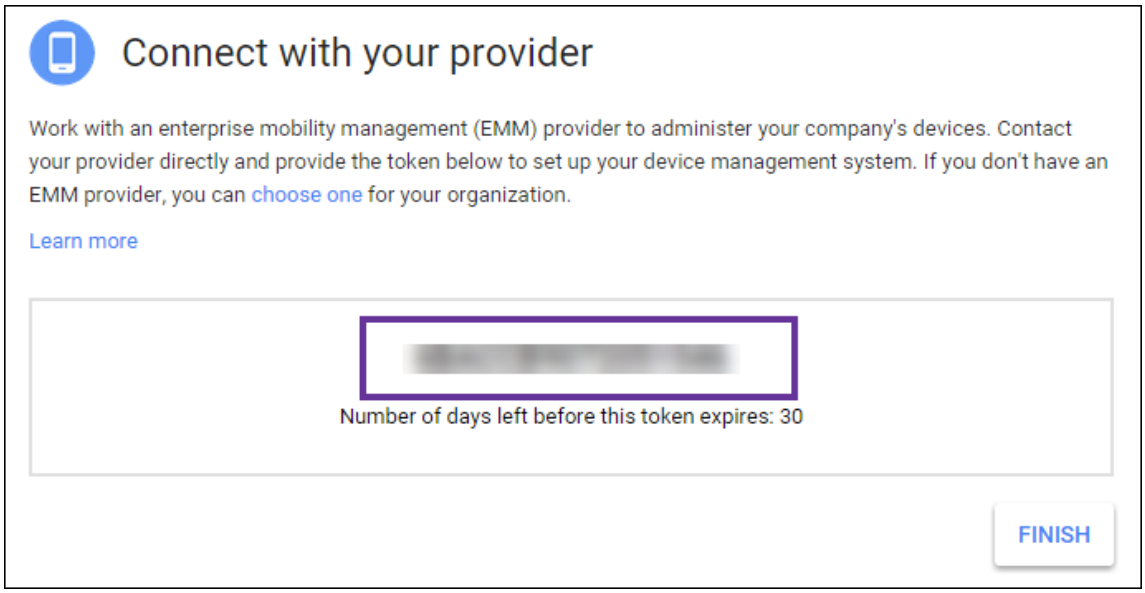
© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. After successful verification, the following page appears. Click **Continue**.



5. Google creates an EMM binding token that you provide to Citrix® and use when you configure Android Enterprise settings. Copy and save the token; you need it later in the setup procedure.



6. Click **Finish** to complete setting up Android Enterprise. A page appears, indicating that you've successfully verified your domain.

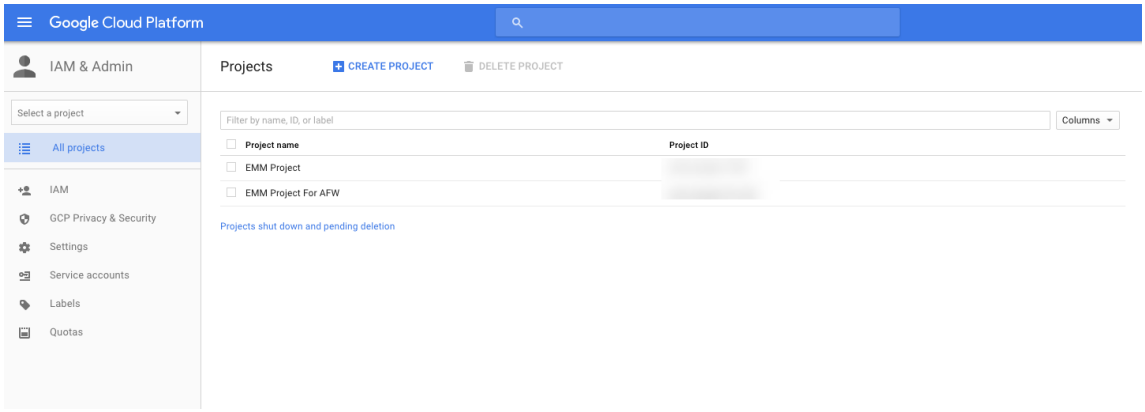
© 1997–2025 Citrix Systems, Inc. All rights reserved.

After you create an Android Enterprise service account, you can sign in to the Google Admin console to manage your mobility management settings.

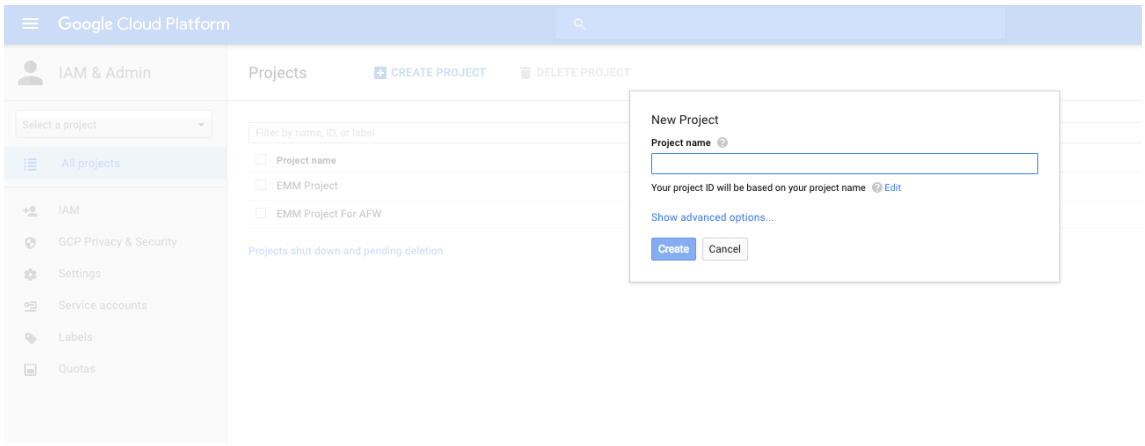
Set up an Android Enterprise service account and download an Android Enterprise certificate

To allow Citrix Endpoint Management to contact Google Play and Directory services, you must create a service account using the Google Project portal for developers. This service account is used for server-to-server communication between Citrix Endpoint Management and Google services for Android. For more information about the authentication protocol being used, go to https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

1. In a web browser, go to https://console.cloud.google.com/project and sign in with your Google administrator credentials
2. In the **Projects** list, click **Create Project**.

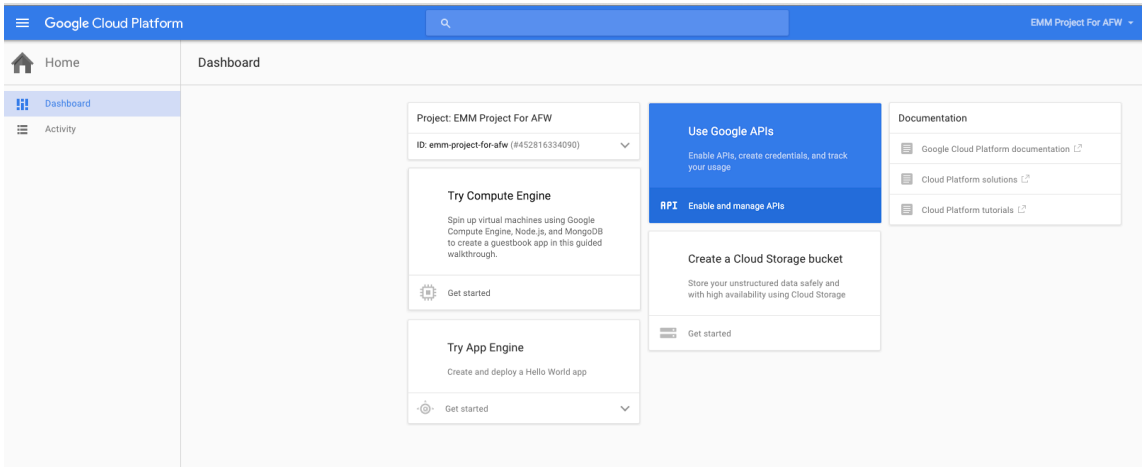


3. In **Project name**, type a name for the project.

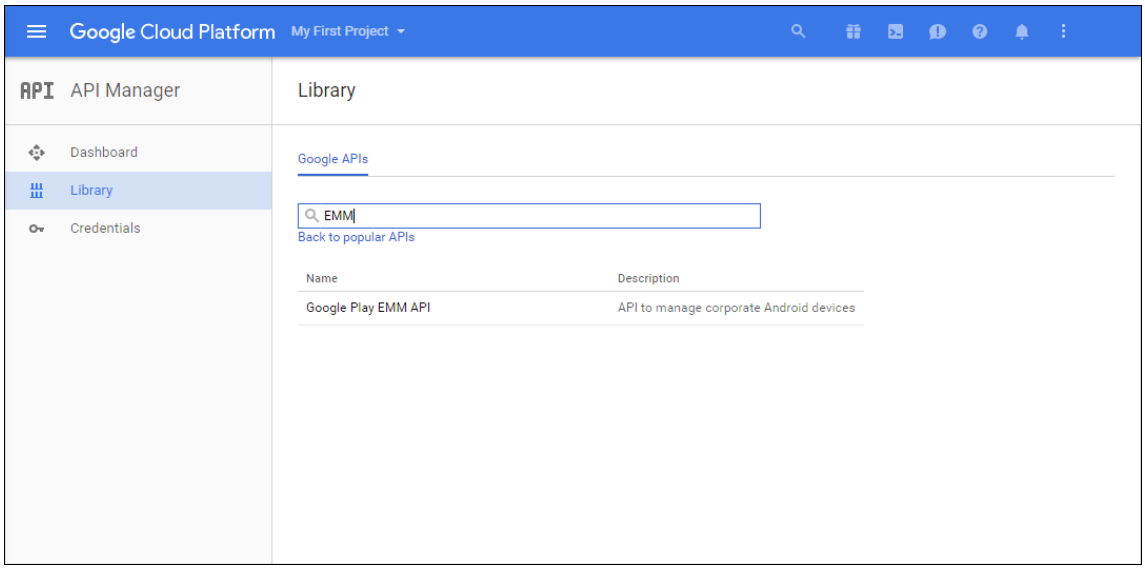


4. On the Dashboard, click **Use Google APIs**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

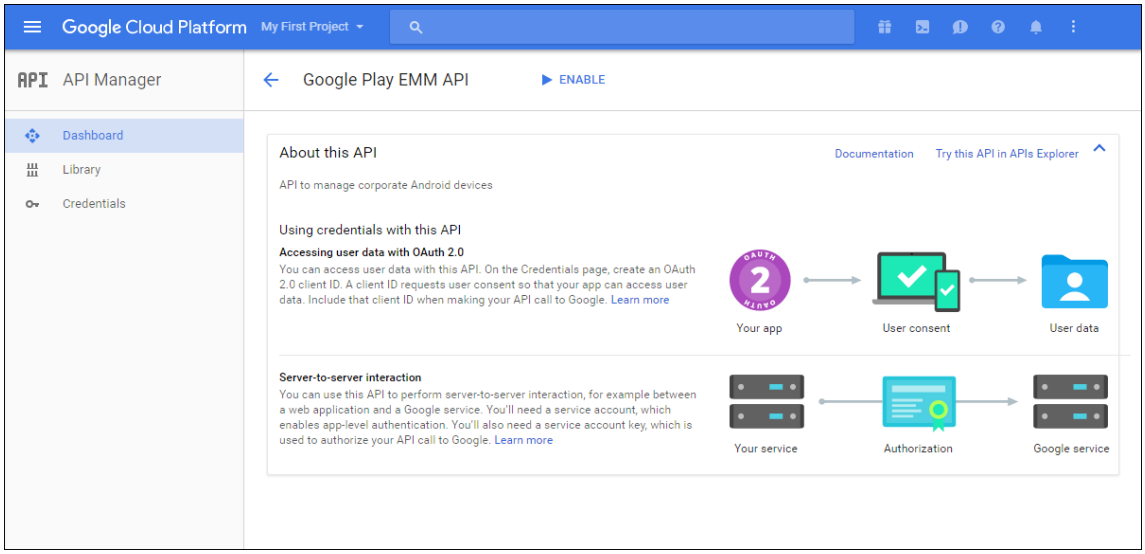


5. Click **Library**, in **Search**, type **EMM** and then click the search result.

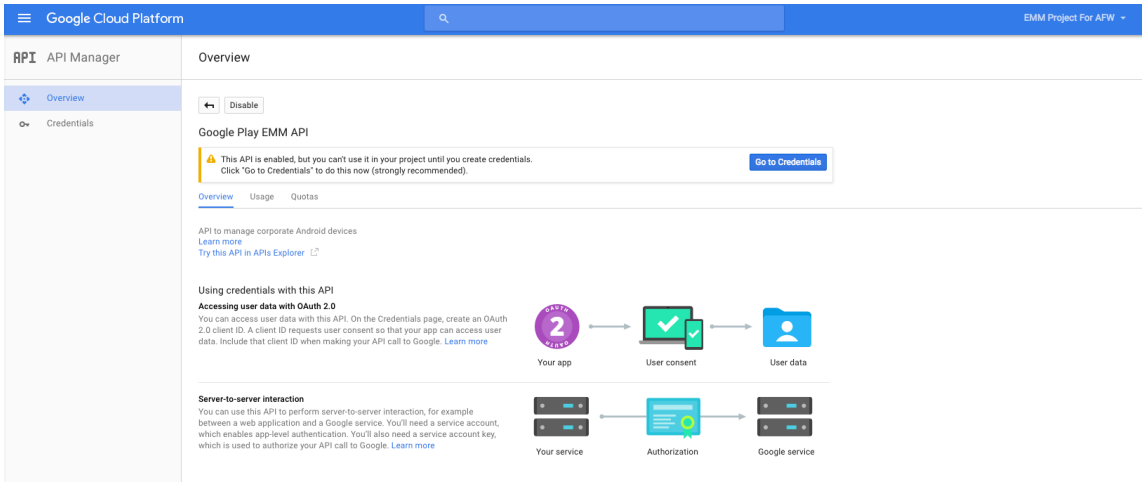


6. On the **Overview** page, click **Enable**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

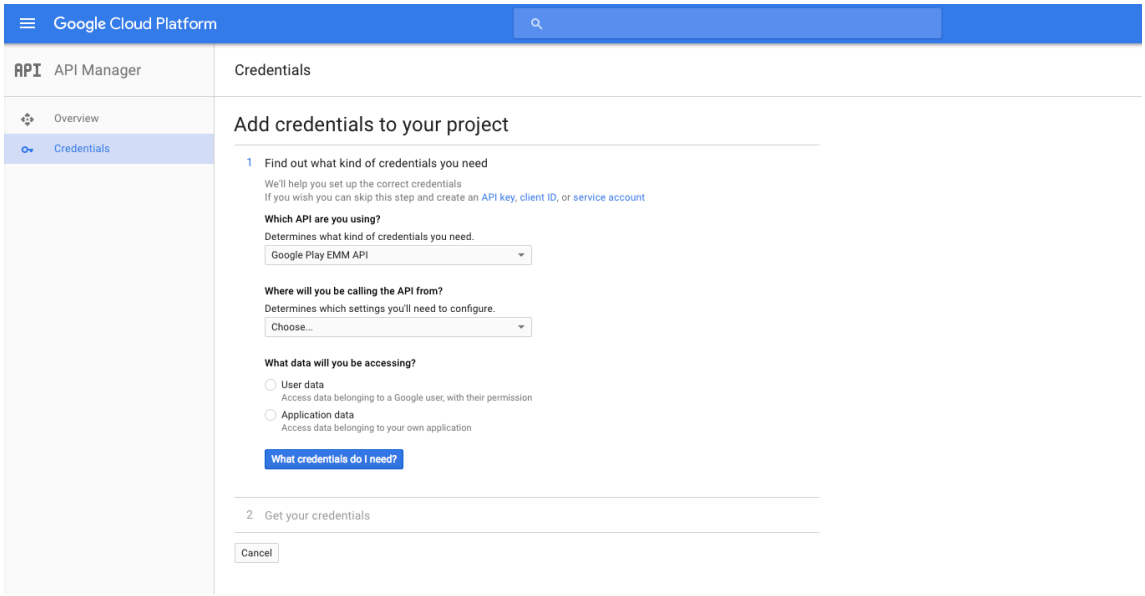


7. Next to **Google Play EMM API**, click **Go to Credentials**.

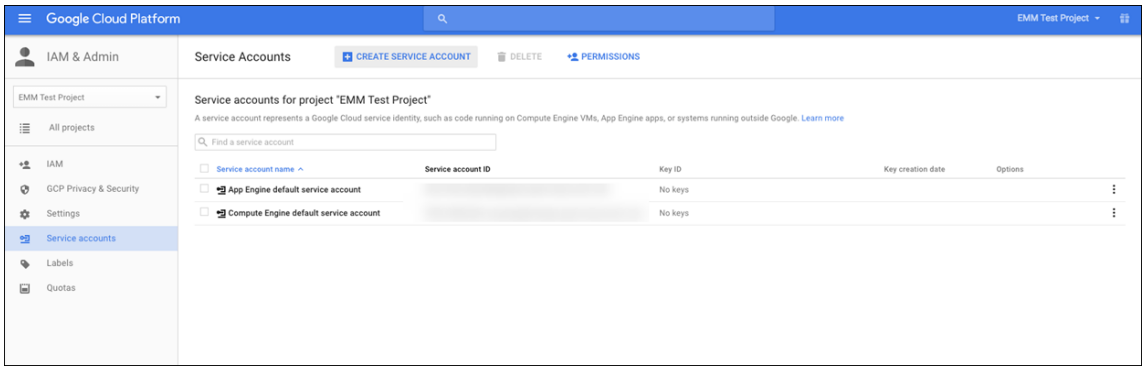


8. In the **Add credentials to our project** list, in step 1, click **service account**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

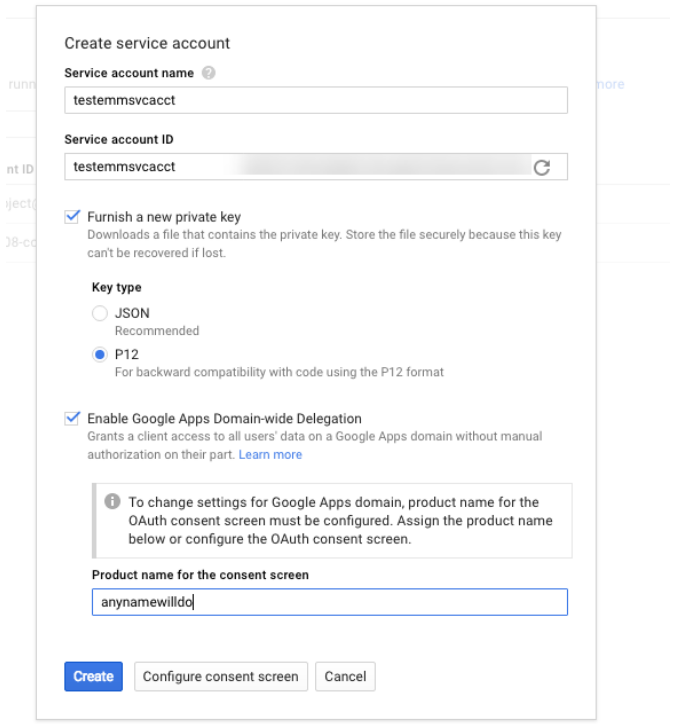


9. On the **Service Accounts** page, click **Create Service Account**.



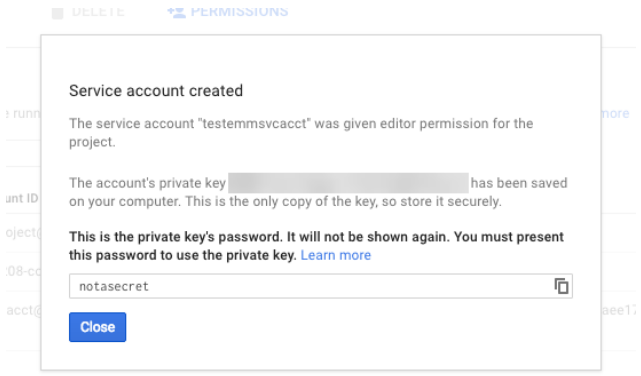
10. In **Create service account**, name the account, and select the **Furnish a new private key** checkbox. Click **P12**, select the **Enable Google Apps Domain-wide Delegation** checkbox and then click **Create**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



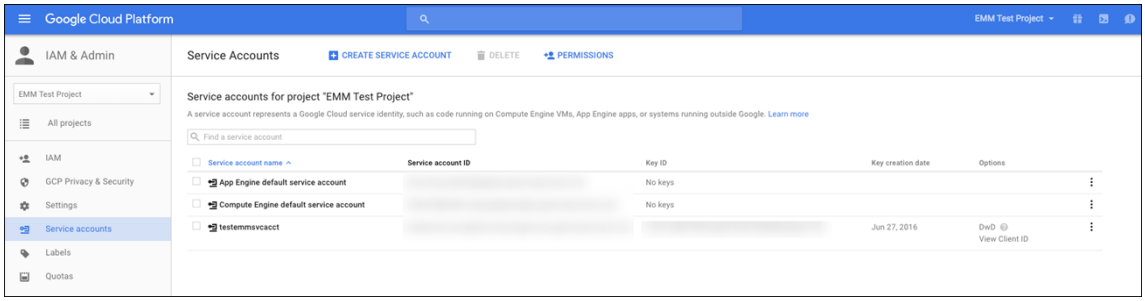
The certificate (P12 file) is downloaded to your computer. Be sure to save the certificate in a secure location.

11. On the **Service account created** confirmation page, click **Close**.

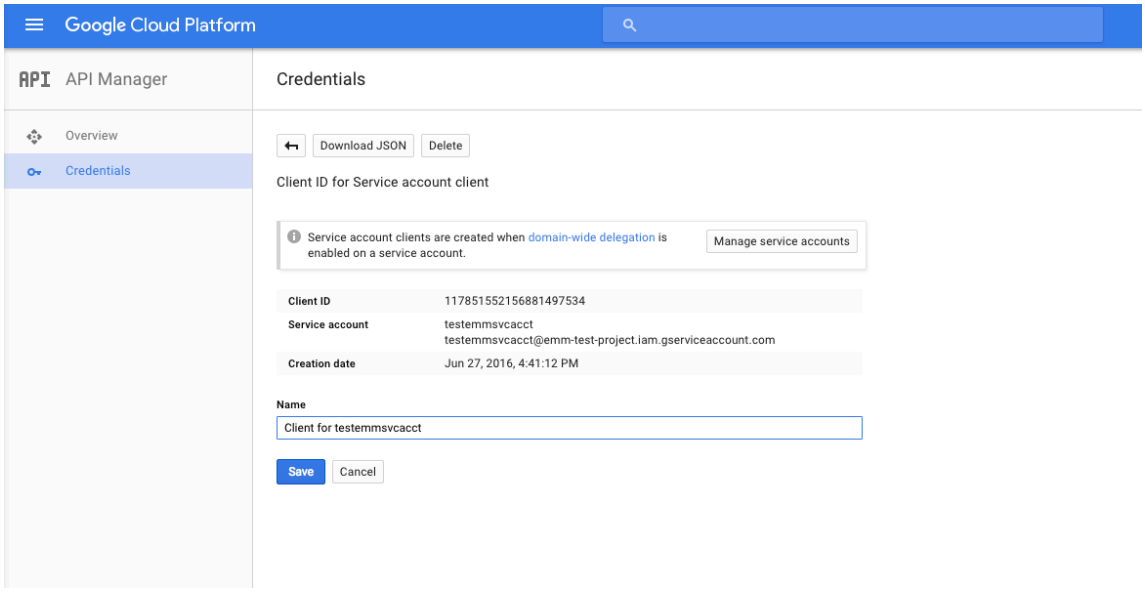


12. In **Permissions**, click **Service accounts** and then under **Options** for your service account, click **View Client ID**.

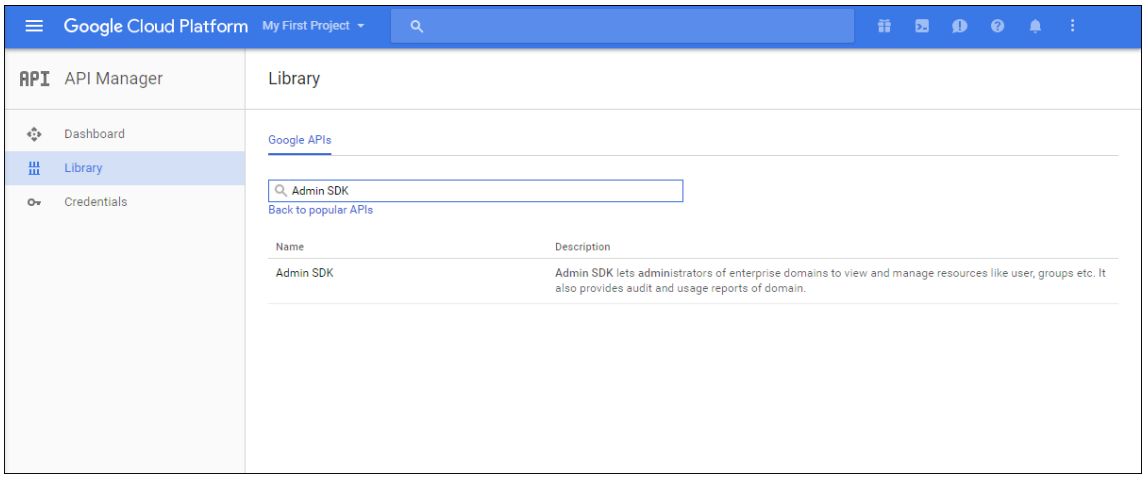
© 1997–2025 Citrix Systems, Inc. All rights reserved.



13. The details required for account authorization on the Google admin console display. Copy the **Client ID** and **Service account ID** to a location where you can retrieve the information later. You need this information, along with the domain name to send to Citrix support to add to an allow list.

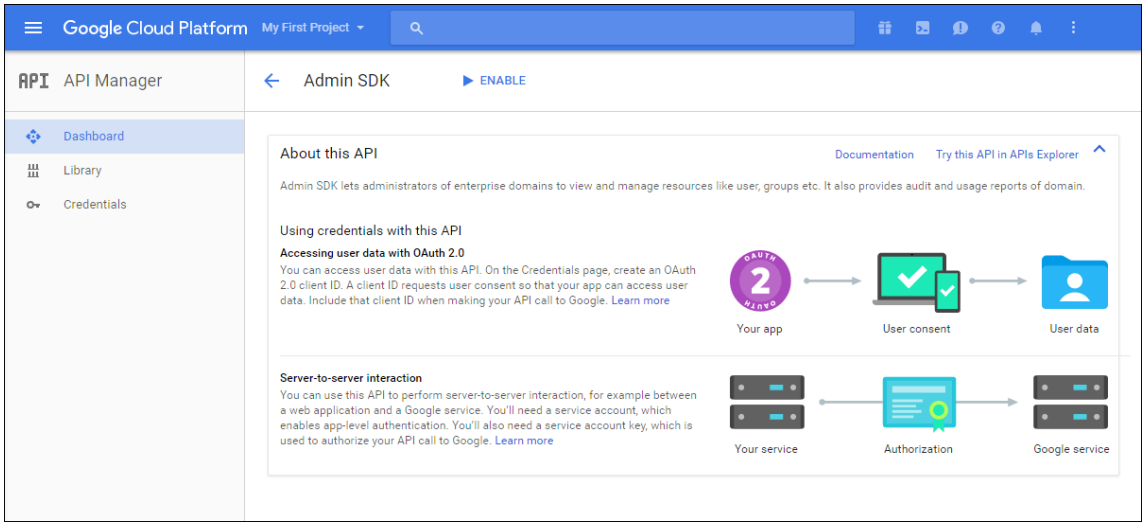


14. On the **Library** page, search for **Admin SDK** and then click the search result.

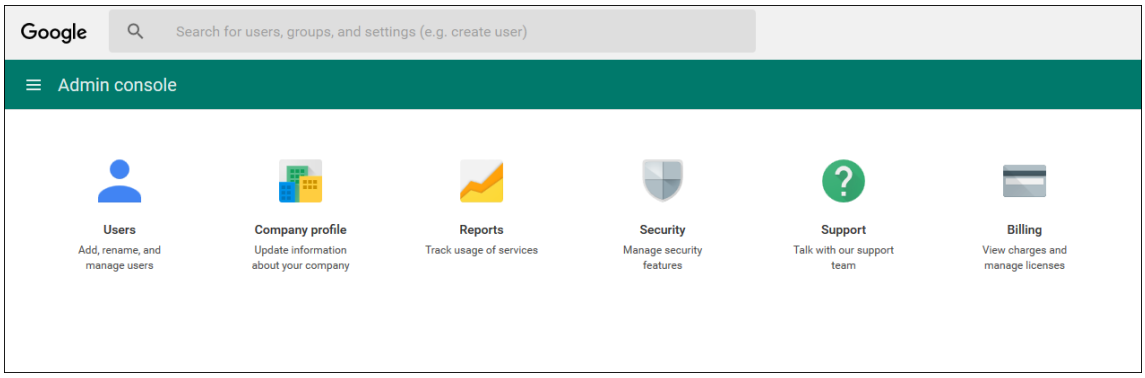


15. On the **Overview** page, click **Enable**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

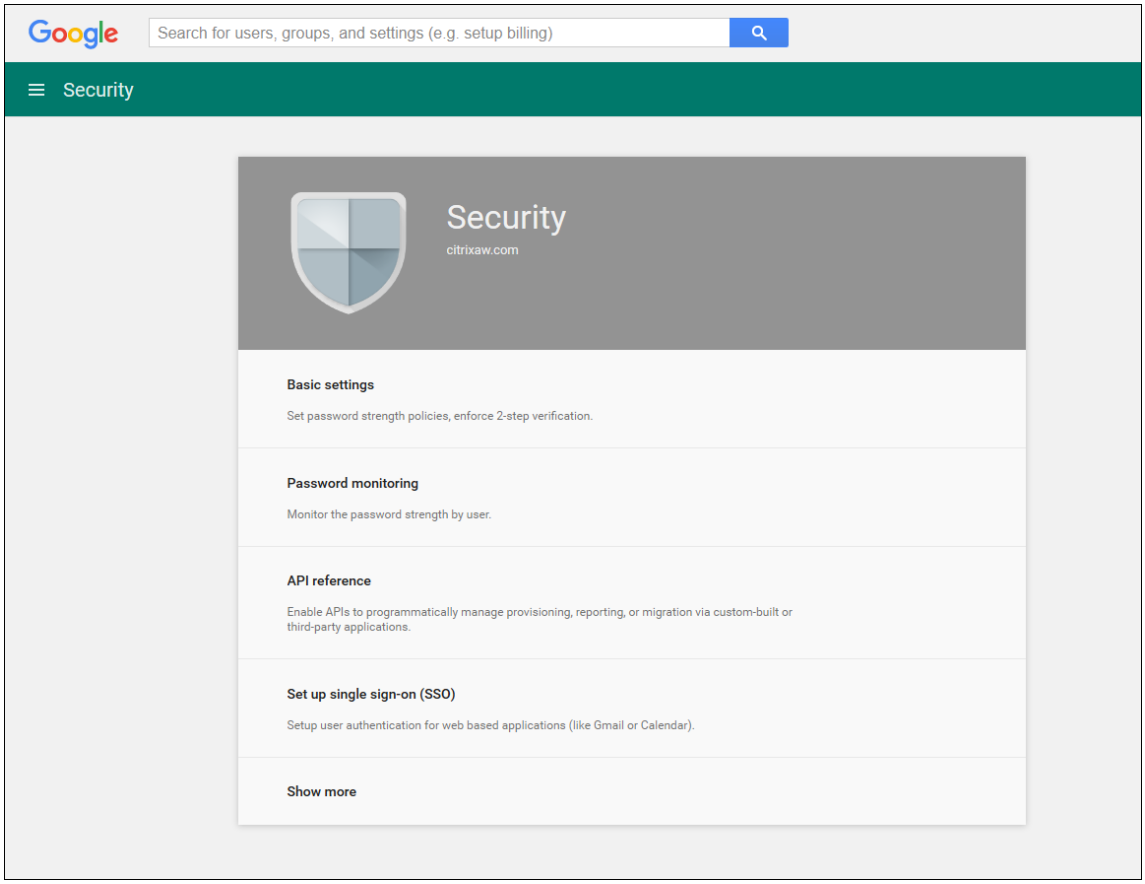


16. Open the Google admin console for your domain and then click **Security**.

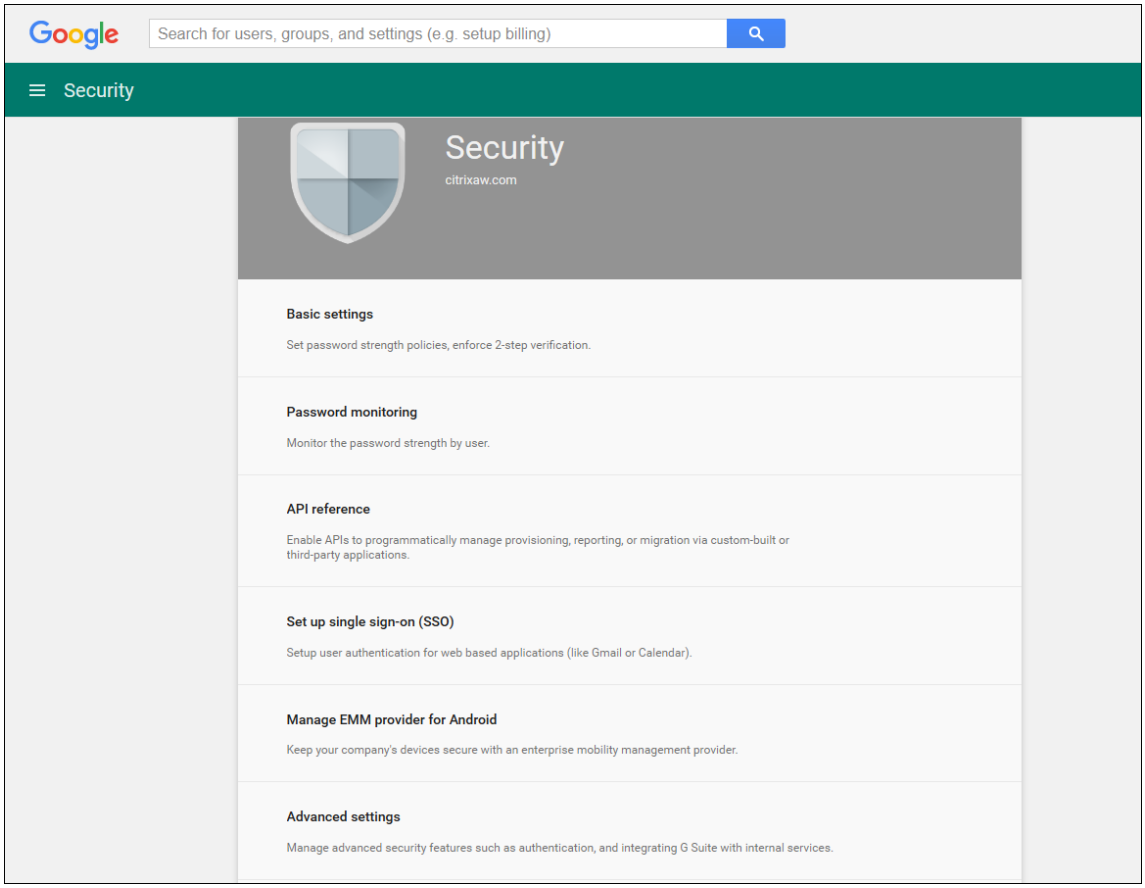


17. On the **Settings** page, click **Show more** and then click **Advanced settings**.

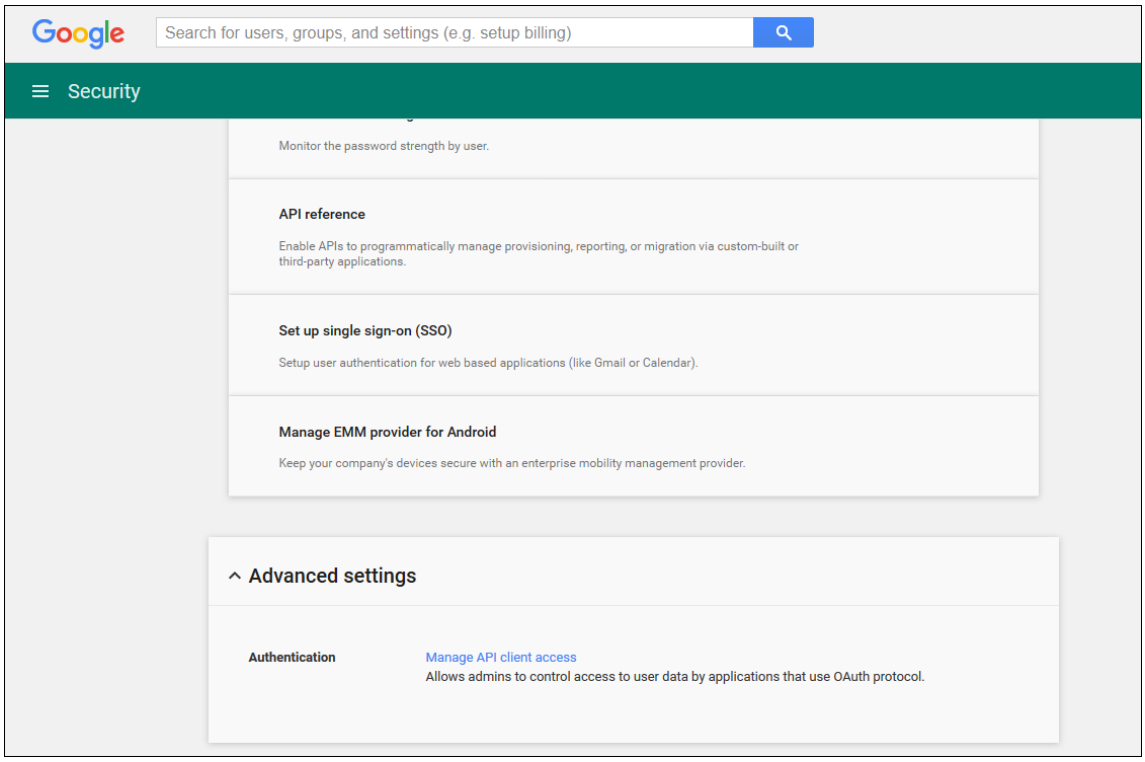
© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

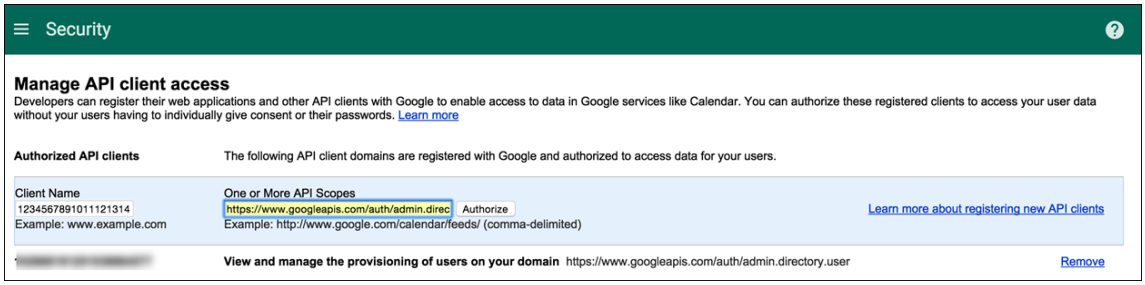


18. Click **Manage API client access**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

19. In **Client Name**, type the client ID that you saved earlier, in **One or More API Scopes**, type `https://www.googleapis.com/auth/admin.directory.user` and then click **Authorize**.



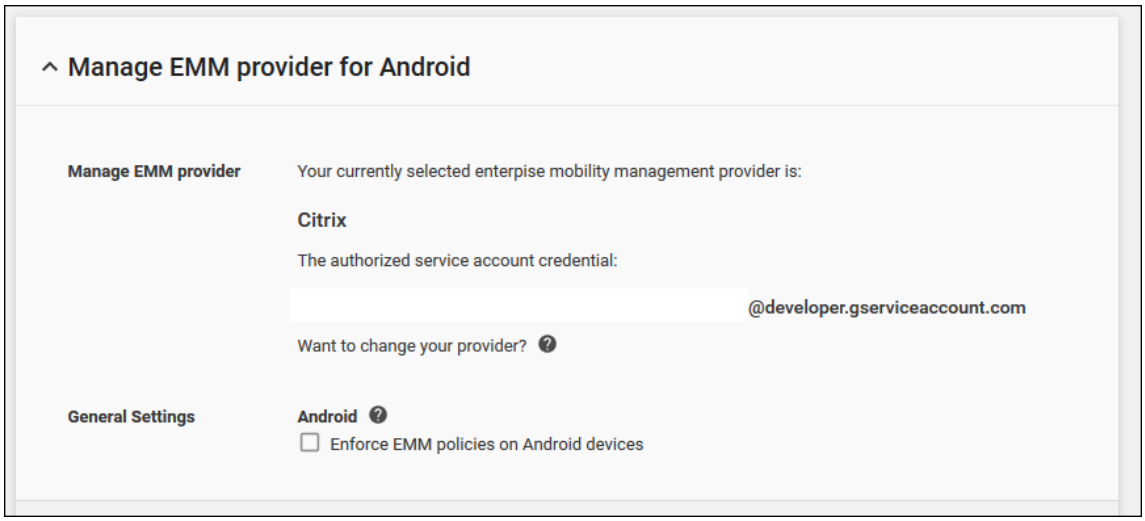
Binding to EMM

Before you can use Citrix Endpoint Management to manage your Android devices, you must contact Citrix Technical Support and provide your domain name, service account, and binding token. Citrix binds the token to Citrix Endpoint Management as your enterprise mobility management (EMM) provider. For contact information for Citrix Technical Support, see Citrix Technical Support.

1. To confirm the binding, sign in to the Google Admin portal and then click **Security**.
2. Click **Manage EMM provider for Android**.

   You see that your Google Android Enterprise account is bound to Citrix as your EMM provider.

   After you confirm the token binding, you can start using the Citrix Endpoint Management console to manage your Android devices. Import the P12 certificate that you generated in step 14. Set up Android Enterprise server settings, enable SAML-based single-sign-on (SSO), and define at least one Android Enterprise device policy.

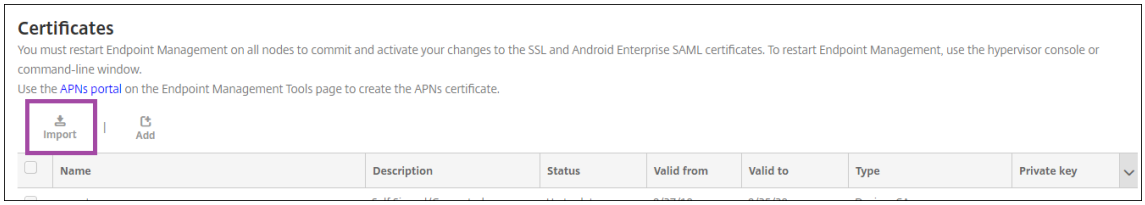


© 1997–2025 Citrix Systems, Inc. All rights reserved.

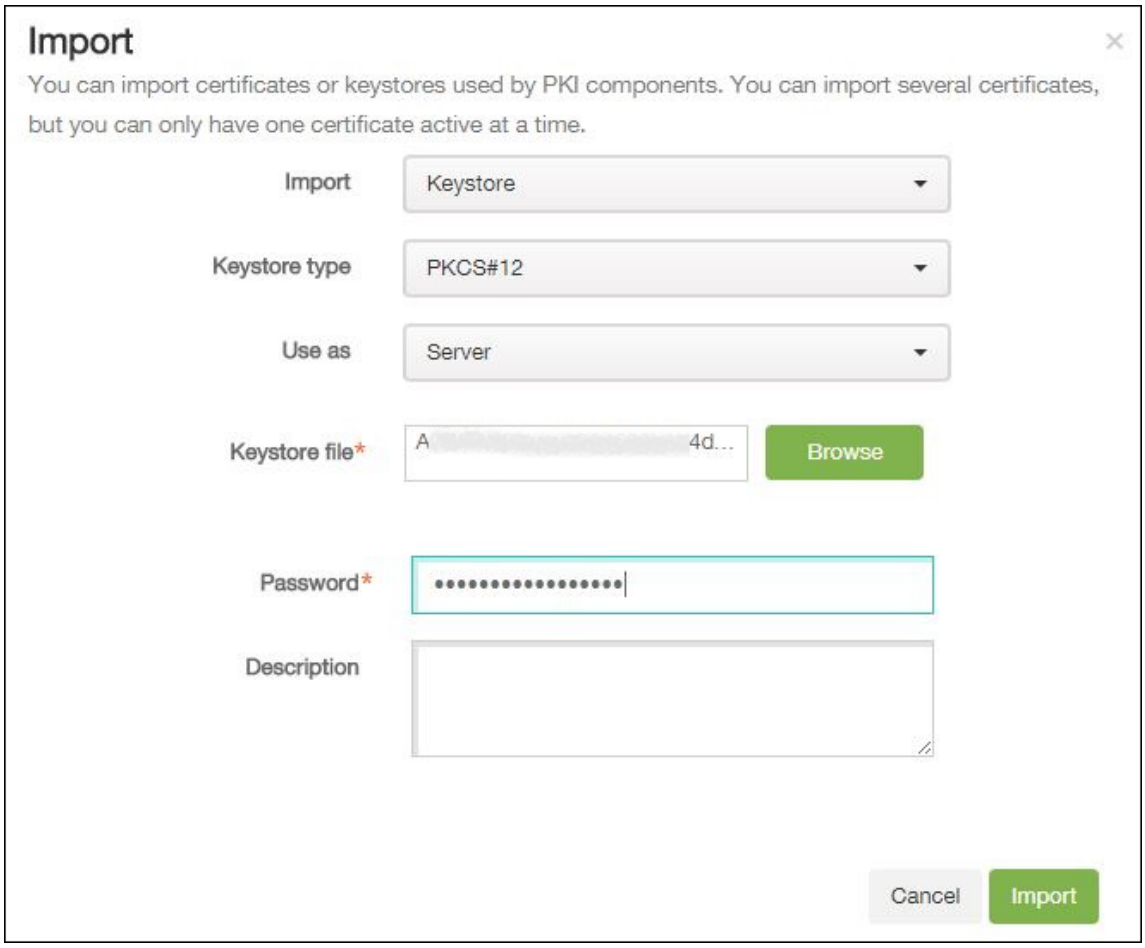
Import the P12 certificate

Follow these steps to import your Android Enterprise P12 certificate:

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console to open the **Settings** page and then click **Certificates**. The **Certificates** page appears.



2. Click **Import**. The **Import** dialog box appears.



Configure the following settings:

- **Import:** Click **Keystore** in the drop-down list.
- **Keystore type:** Click **PKCS#12** in the drop-down list.
- **Use as:** Click **Server** in the drop-down list.
- **Keystore file:** Click **Browse** and navigate to the P12 certificate.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Password:** Type the certificate password. This password is the private key password that you created when setting up your Android Enterprise account.
- **Description:** Optionally, type a description of the certificate.

3. Click **Import**.

Set up Android Enterprise server settings

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Under **Platforms**, click **Android Enterprise**. The **Android Enterprise** page appears.

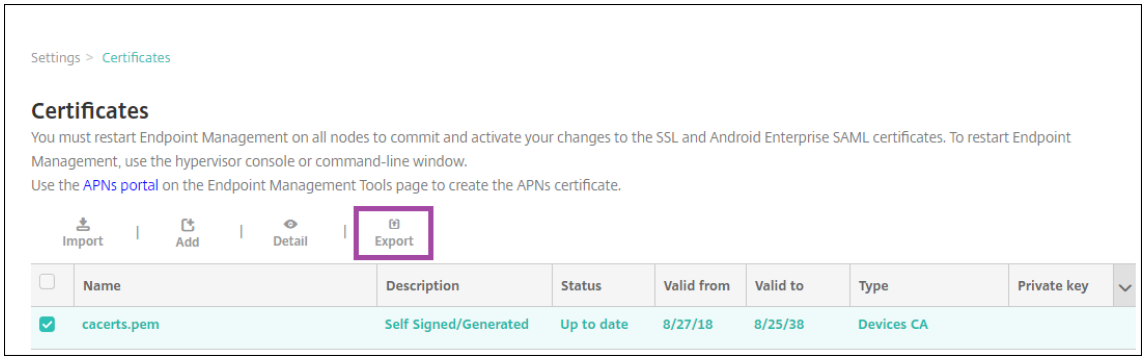
Configure the following settings and then click **Save**.

- **Domain name:** Type your Android Enterprise domain name; for example, domain.com.
- **Domain Admin Account:** Type your domain administrator user name; for example, the email account used for the Google Developer Portal.
- **Service Account ID:** Type your service account ID; for example, the email associated in the Google Service Account (`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`).
- **Client ID:** Type the numerical client ID of your Google service account.
- **Enable Android Enterprise:** Select to enable or disable Android Enterprise.

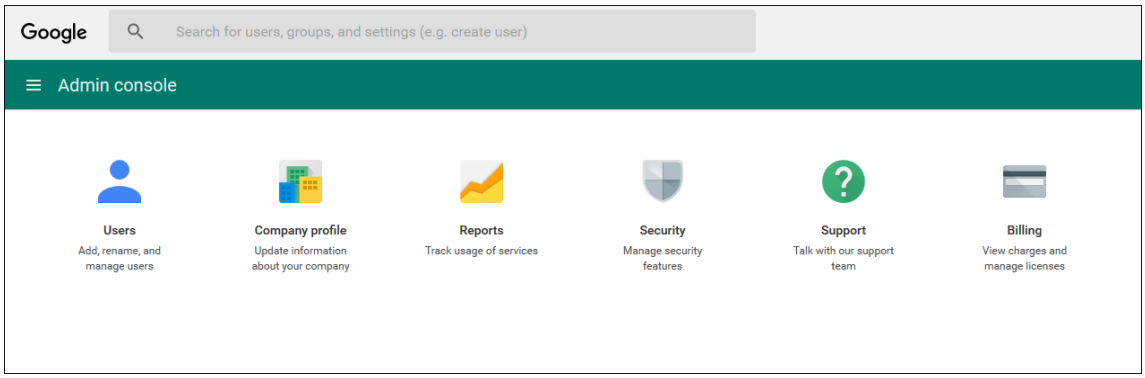
Enable SAML-based single-sign-on

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **Certificates**. The **Certificates** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

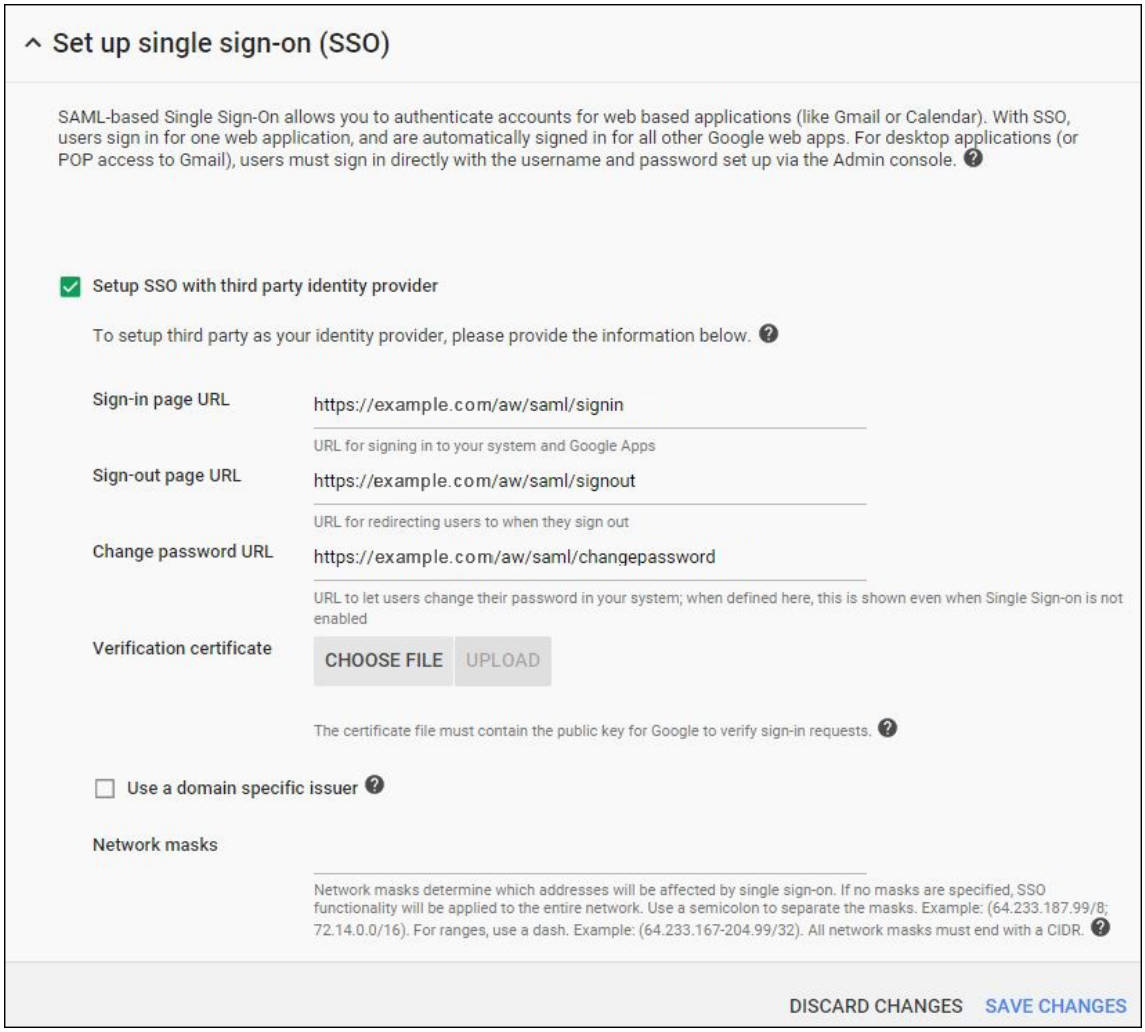


3. In the list of certificates, click the SAML certificate.
4. Click **Export** and save the certificate to your computer.
5. Sign in to the Google Admin portal by using your Android Enterprise administrator credentials. For access to the portal, see the Google Admin portal.
6. Click **Security**.



7. Under **Security**, click **Set up single sign-on (SSO)** and then configure the following settings.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



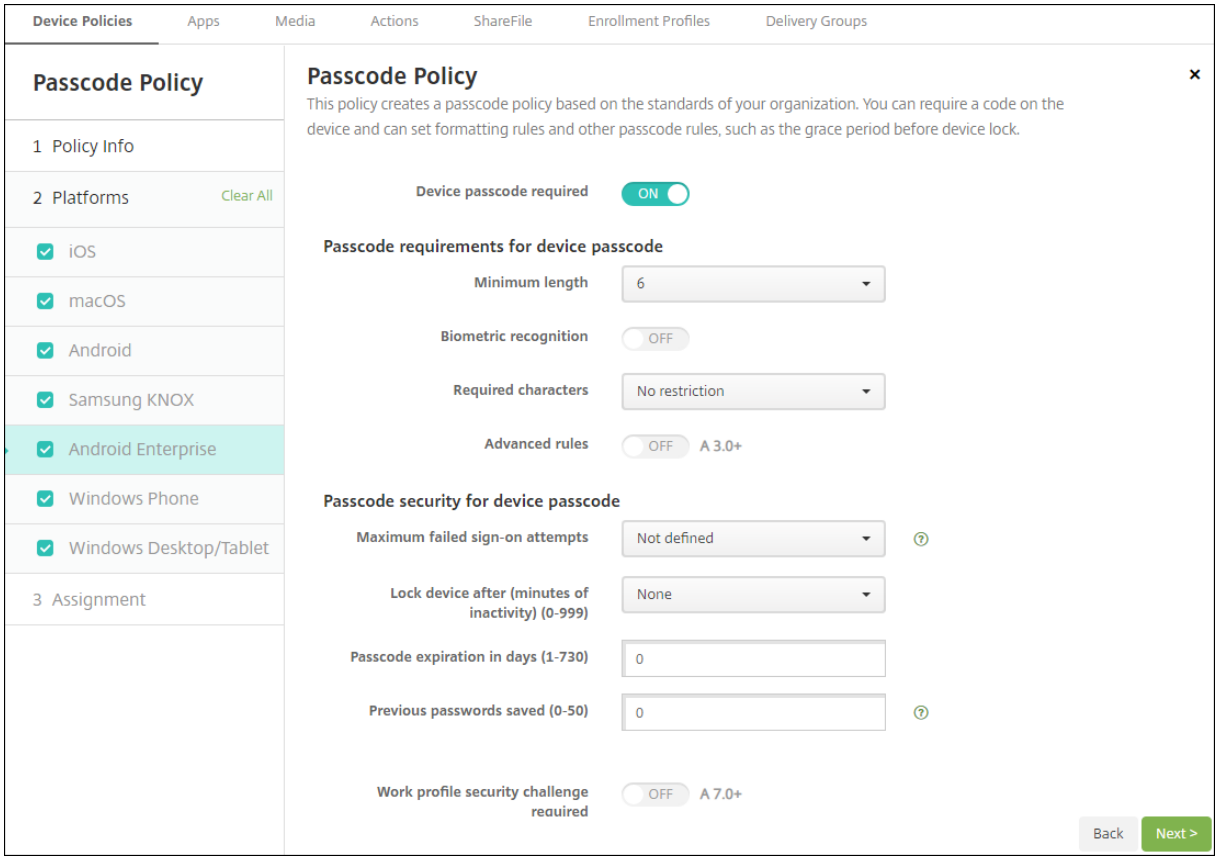
- **Sign-in page URL:** Type the URL for users signing in to your system and Google Apps. For example: `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **Sign out page URL:** Type the URL to which users are redirected when they sign out. For example: `https://<Xenmobile-FQDN>/aw/saml/signout`.
- **Change password URL:** Type the URL to let users change their password in your system. For example: `https://<Xenmobile-FQDN>/aw/saml/changepassword`. If this field is defined, users see this prompt even when SSO isn't available.
- **Verification certificate:** Click **CHOOSE FILE** and then navigate to the SAML certificate exported from Citrix Endpoint Management.

8. Click **SAVE CHANGES**.

Set up an Android Enterprise device policy

Set up a Passcode policy so that users must establish a passcode on their devices when they first enroll.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The basic steps to setting up any device policy are as follows.

1. In the Citrix Endpoint Management console, click **Configure**, and then click **Device Policies**.
2. Click **Add**.
3. On the **Add a New Policy** dialog box, select the policy you want to add. In this example, you click **Passcode**.
4. Complete the **Policy Information** page.
5. Click **Android Enterprise** and then configure the settings for the policy.
6. Assign the policy to a Delivery Group.

Configure Android Enterprise account settings

Before you can start managing Android apps and policies on devices, you must set up an Android Enterprise domain and account information in Citrix Endpoint Management. First, complete the Android Enterprise setup tasks on Google to set up a domain administrator and to get a service account ID and a binding token.

1. In the Citrix Endpoint Management web console, click the gear icon in the upper-right corner. The **Settings** page displays.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Under **Platforms**, click **Android Enterprise**. The **Android Enterprise** configuration page appears.

1. On the **Android Enterprise** page, configure the following settings:

   - **Domain Name:** Type your domain name.
   - **Domain Admin Account:** Type your domain administrator user name.
   - **Service Account ID:** Type your Google Service Account ID.
   - **Client ID:** Type the client ID of your Google service account.
   - **Enable Android Enterprise:** Select whether to enable Android Enterprise or not.

2. Click **Save**.

Set up Google Workspace partner access for Citrix Endpoint Management

Some Citrix Endpoint Management features for Chrome use Google partner APIs to communicate between Citrix Endpoint Management and your Google Workspace domain. For example, Citrix Endpoint Management requires the APIs for device policies that manage Chrome features such as Incognito mode and Guest mode.

To enable the partner APIs, you set up your Google Workspace domain in the Citrix Endpoint Management console and then configure your Google Workspace account.

Set up your Google Workspace domain in Citrix Endpoint Management

To enable Citrix Endpoint Management to communicate with the APIs in your Google Workspace domain, go to **Settings > Google Chrome Configuration** and configure the settings.

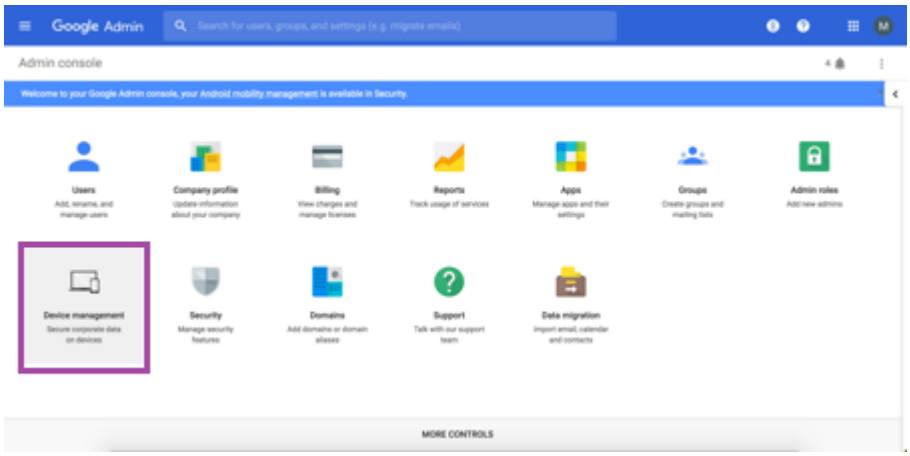
- **Google Workspace domain:** The Google Workspace domain that hosts the APIs needed by Citrix Endpoint Management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Google Workspace admin account:** The administrator account for your Google Workspace domain.
- **Google Workspace client ID:** The client ID for Citrix. Use this value to configure partner access for your Google Workspace domain.
- **Google Workspace enterprise ID:** The enterprise ID for your account, filled in from your Google enterprise account.

Enable partner access for devices and users in your Google Workspace domain

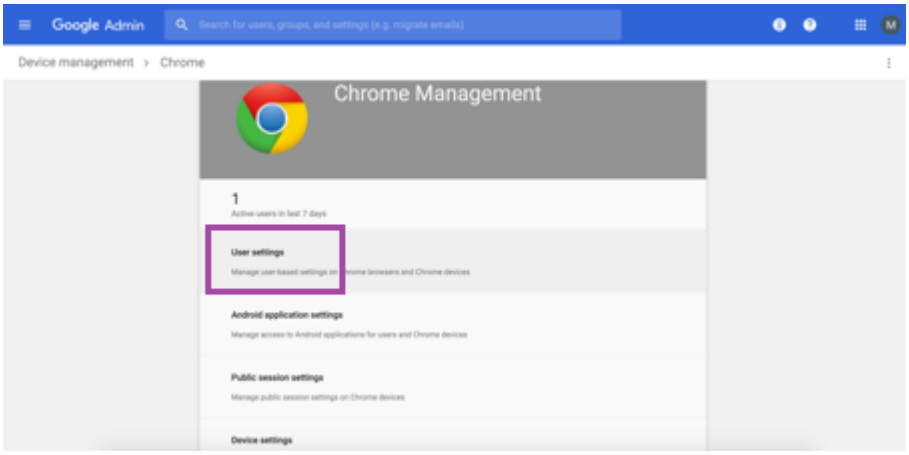
1. Log in into the Google admin console: https://admin.google.com
2. Click **Device Management**.



3. Click **Chrome management**.

4. Click **User settings**.

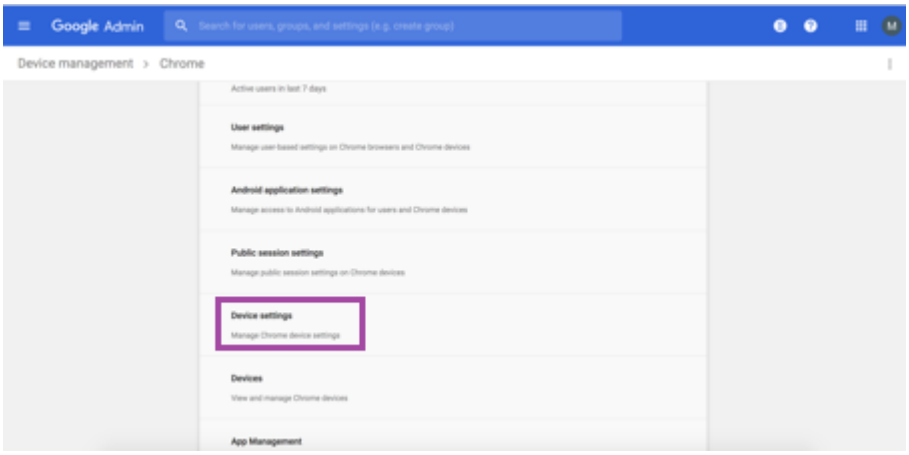
© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. Search for **Chrome Management - Partner Access**.

6. Select the **Enable Chrome Management - Partner Access** checkbox.
7. Agree that you understand and want to enable partner access. Click **Save**.
8. In the Chrome management page, click **Device Settings**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

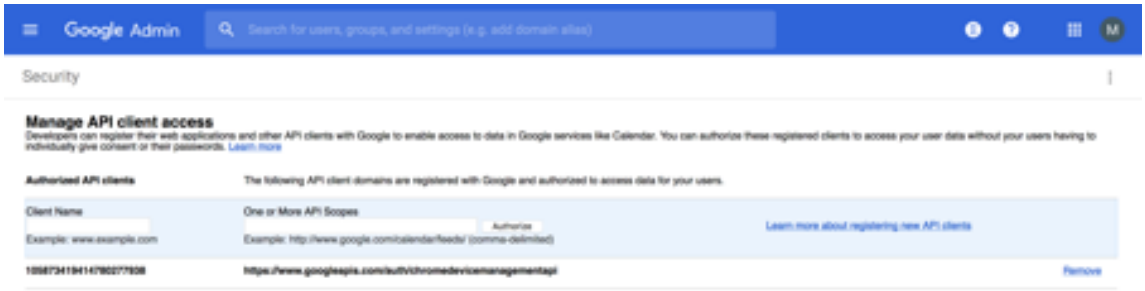


9. Search for **Chrome Management - Partner Access**.

10. Select the **Enable Chrome Management - Partner Access** checkbox.
11. Agree that you understand and want to enable partner access. Click **Save**.
12. Go to the **Security** page and then click **Advanced Settings**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

13. Click **Manage API client Access**.
14. In the Citrix Endpoint Management console, go to **Settings > Google Chrome Configuration** and copy the value of G Suite Client ID. Then, return to the **Manage API client Access** page and paste the copied value to the **Client Name** field.
15. In **One or More API Scopes**, add the URL: `https://www.googleapis.com/auth/chromedevicemanagementapi`



16. Click **Authorize**.

    The message "Your settings have been saved"appears.

Enrolling Android Enterprise devices

If your device enrollment process requires users to enter a user name or user ID, the format accepted depends on how the Citrix Endpoint Management server is configured to search for users by User Principal Name (UPN) or SAM account name.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

If the Citrix Endpoint Management server is configured to search for users by UPN, users must enter a UPN in the format:

- *username@domain*

If the Citrix Endpoint Management server is configured to search for users by SAM users must enter a SAM in one of these formats:

- *username@domain*
- *domain\username*

To determine which type of user name your Citrix Endpoint Management server is configured for:

1. In the Citrix Endpoint Management server console click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **LDAP** to view the configuration of the LDAP connection.
3. Near the bottom of the page, view the **User search by** field:
    - If it is set to **userPrincipalName**, the Citrix Endpoint Management server is set for UPN.
    - If it is set to **sAMAccountName**, the Citrix Endpoint Management server is set for SAM.

Unenrolling an Android Enterprise enterprise

You can unenroll an Android Enterprise enterprise using the Citrix Endpoint Management server console and Citrix Endpoint Management Tools.

When you do this task, the Citrix Endpoint Management server opens a popup window for Citrix Endpoint Management Tools. Before you begin, make sure that the Citrix Endpoint Management server has permission to open popup windows in the browser you are using. Some browsers, such as Google Chrome, require you to disable popup blocking and add the address of the Citrix Endpoint Management site to the popup allow list.

> **Warning:**
>
> After an enterprise is unenrolled, Android Enterprise apps on devices already enrolled through it are reset to their default states. The devices are no longer managed by Google. Re-enrolling them in an Android Enterprise enterprise might not restore previous functionality without further configuration.

After the Android Enterprise enterprise is unenrolled:

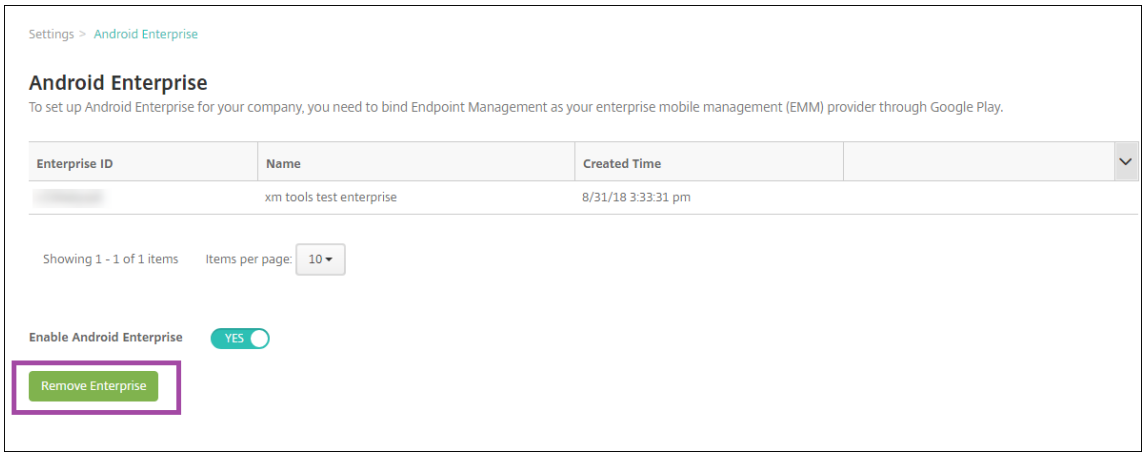
- Devices and users enrolled through the enterprise have the Android Enterprise apps reset to their default state. App permissions and Managed configurations policies previously applied no longer have an effect.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

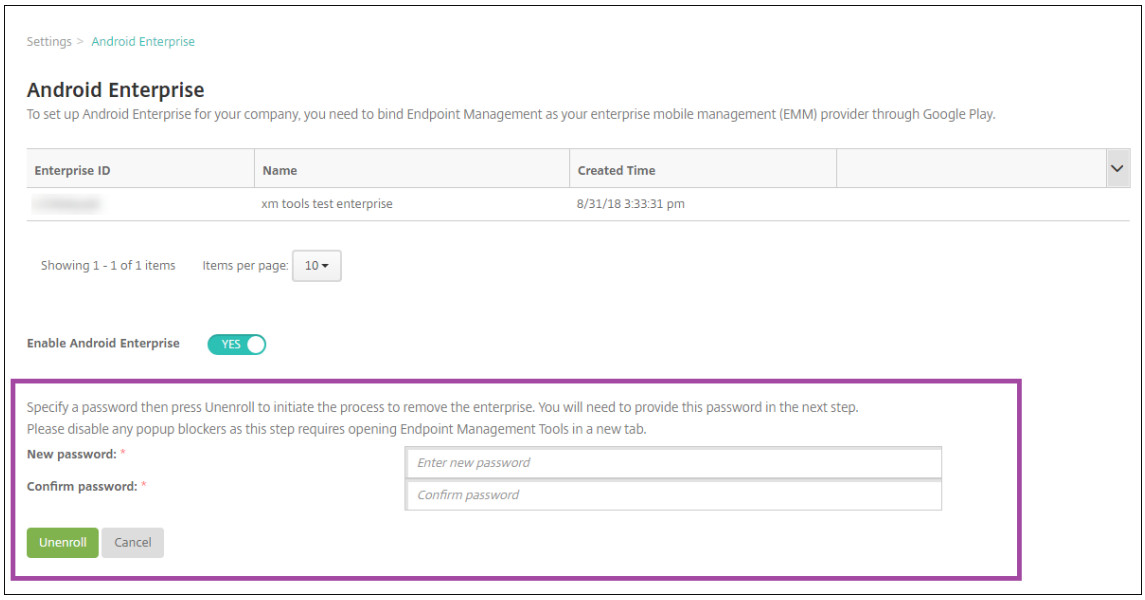
- Devices enrolled through the enterprise are managed by Citrix Endpoint Management, but are unmanaged from the Google perspective. No new Android Enterprise apps can be added. No App permissions or Managed configurations policies can be applied. Other policies, such as Scheduling, Password, and Restrictions can still be applied to these devices.
- If you try to enroll devices in Android Enterprise, they're enrolled as Android devices, not Android Enterprise devices.

To unenroll an Android Enterprise enterprise:

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The Settings page appears.
2. On the Settings page, click **Android Enterprise**.
3. Click **Remove Enterprise**.

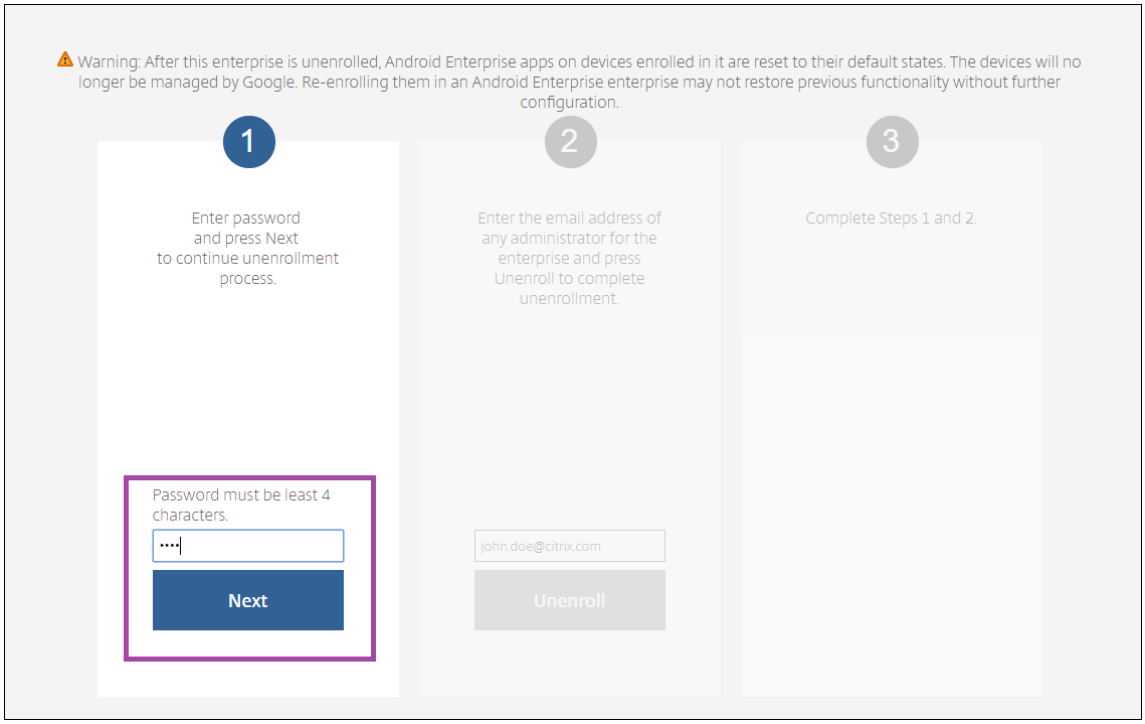


4. Specify a password. You'll need this for the next step to complete the unenrollment. Then click **Unenroll**.

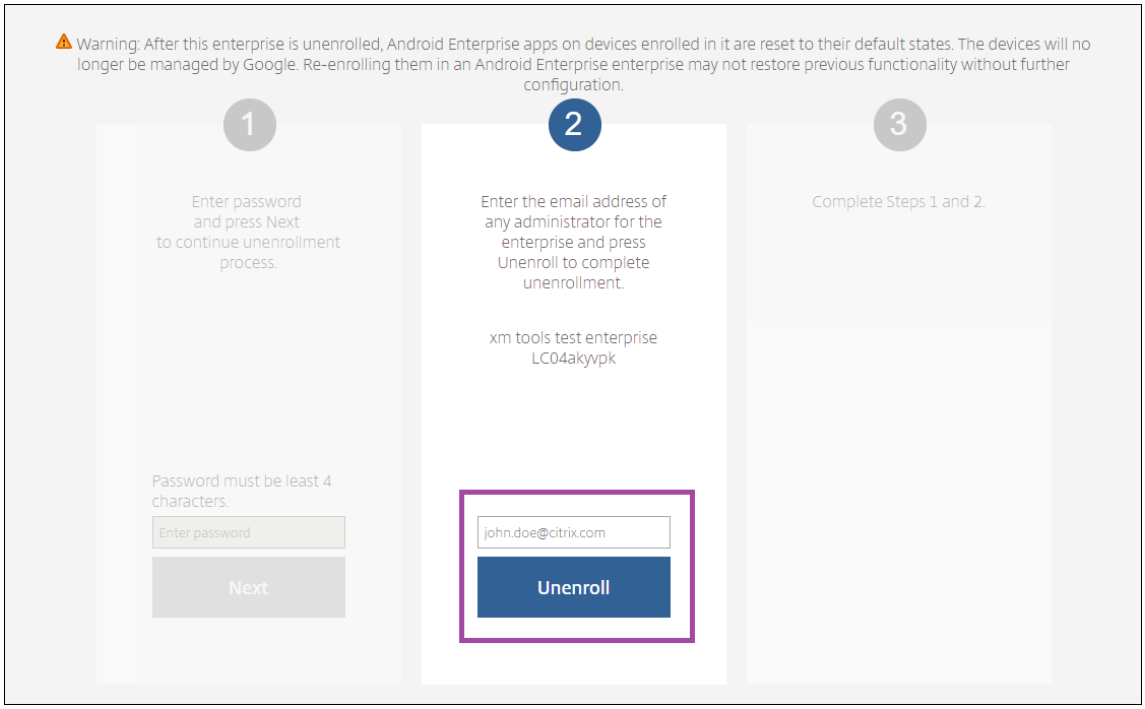


© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. When the Citrix Endpoint Management Tools page opens, enter the password you created in the previous step.



6. Click **Unenroll**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Provisioning fully managed devices in Android Enterprise

Only company-owned devices can be fully managed devices in Android Enterprise. On fully managed devices the entire device, not just the work profile, is controlled by the company or organization. Fully managed devices are also known as work-managed devices.

Citrix Endpoint Management supports these methods of enrollment for fully managed devices:

- **afw#xenmobile:** With this enrollment method, the user enters the characters `afw#xenmobile` when setting up the device. This token identifies the device as managed by Citrix Endpoint Management and downloads Citrix Secure Hub.
- **QR code:** QR code provisioning is an easy way to provision a distributed fleet of devices that do not support NFC, such as tablets. The QR code enrollment method can be used on fleet devices that have been reset to their factory settings. The QR code enrollment method sets up and configures fully managed devices by scanning a QR code from the setup wizard.
- **Near field communication (NFC) bump:** The NFC bump enrollment method can be used on fleet devices that have been reset to their factory settings. An NFC bump transfers data through between two devices using near-field communication. Bluetooth, Wi-Fi, and other communication modes are disabled on a factory-reset device. NFC is the only communication protocol that the device can use in this state.

`afw#xenmobile`®

The enrollment method is used after powering on a new or factory reset devices for initial setup. Users enter `afw#xenmobile` when prompted to enter a Google account. This action downloads and installs Citrix Secure Hub. Users then follow the Citrix Secure Hub set-up prompts to complete the enrollment.

This enrollment method is recommended for most customers because the latest version of Citrix Secure Hub is downloaded from the Google Play store. Unlike with other enrollment methods, you do not provide Citrix Secure Hub for download from the Citrix Endpoint Management server.

Prerequisites:

- Supported on all Android devices running Android OS.

QR code

To enroll a device in device mode using a QR code, you generate a QR code by creating a JSON and converting the JSON to a QR code. Device cameras scan the QR code to enroll the device.

Prerequisites:

- Supported on all Android devices running Android 7.0 and above.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Create a QR code from a JSON Create a JSON with the following fields.

These fields are required:

Key: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Value: com.zenprise/com.zenprise.configuration.AdminFunction

Key: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Value: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Key: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Value: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

These fields are optional:

- **android.app.extra.PROVISIONING_LOCALE:** Enter language and country codes.

  The language codes are two-letter lowercase ISO language codes (such as en) as defined by ISO 639-1. The country codes are two-letter uppercase ISO country codes (such as US) as defined by ISO 3166-1. For example, enter en_US for English as spoken in the United States.

- **android.app.extra.PROVISIONING_TIME_ZONE:** The time zone in which the device is running.

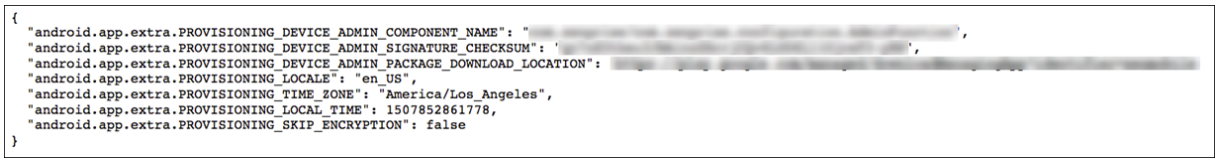
  Type the database name of the area/location. For example, type **America/Los_Angeles** for Pacific time. If you don't type a name, the time zone automatically populates.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Time in milliseconds since the Epoch.

  The Unix epoch (or Unix time, POSIX time, or Unix timestamp) is the number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT). The time doesn't include leap seconds (in ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** Set to **true** to skip encryption during profile creation. Set to **false** to force encryption during profile creation.

A typical JSON looks like the following:



Validate the JSON that is created using any JSON validation tool, such as https://jsonlint.com. Convert that JSON string to a QR code using any online QR code generator.

This QR code gets scanned by a factory-reset device to enroll the device as a fully managed device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To enroll the device

To enroll a device as a fully managed device, the device must be in factory reset state.

1. Tap the screen six times on the welcome screen to launch the QR code enrollment flow.
2. When prompted, connect to Wi-Fi. The download location for Citrix Secure Hub in the QR code (encoded in the JSON) is accessible over this Wi-Fi network.

   Once the device successfully connects to Wi-Fi, it downloads a QR code reader from Google and launches the camera.
3. Point the camera to the QR code to scan the code.

   Android downloads Citrix Secure Hub from the download location in the QR code, validate the signing certificate signature, install Citrix Secure Hub, and sets it as device owner.

For more information about provisioning devices using the QR code method, see the Google API documentation for Android EMM developers.

NFC bump

To enroll a device as a fully managed device using NFC bumps requires two devices: One that is reset to its factory settings and one running the Citrix Endpoint Management Provisioning Tool.

Prerequisites:

- Supported Android devices
- Citrix Endpoint Management enabled for Android Enterprise
- A new or factory-reset device, provisioned for Android Enterprise as a fully managed device. You can find steps to complete this prerequisite later in this article.
- Another device with NFC capability, running the configured Provisioning Tool. The Provisioning Tool is available in Citrix Secure Hub or on the Citrix downloads page.

Each device can have only one Android Enterprise profile, managed by an enterprise mobility management (EMM) app. In Citrix Endpoint Management, Citrix Secure Hub is the EMM app. Only one profile is allowed on each device. Trying to add a second EMM app removes the first EMM app.

Data transferred through the NFC bump Provisioning a factory-reset device requires you to send the following data through an NFC bump to initialize the Android Enterprise:

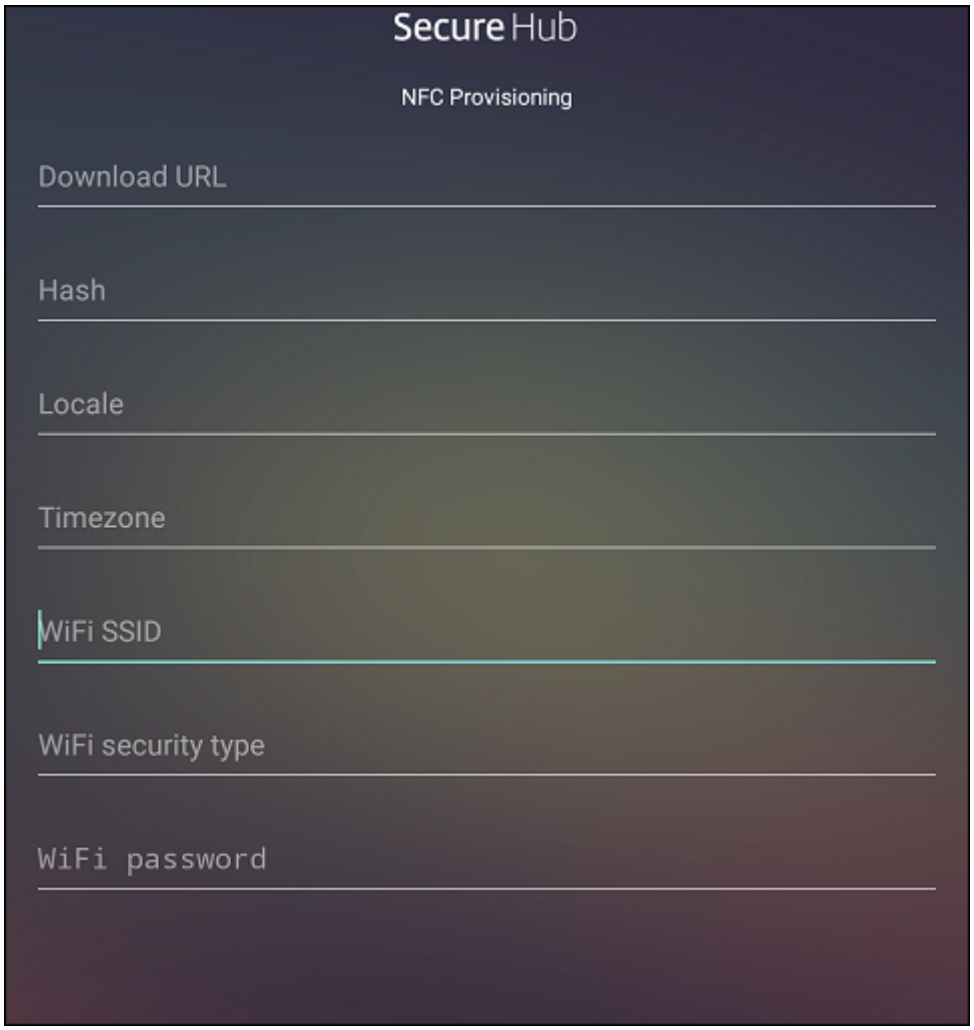
- Package name of the EMM provider app that acts as device owner (in this case, Citrix Secure Hub).
- Intranet/Internet location from which the device can download the EMM provider app.
- SHA-256 hash of EMM provider app to verify if the download is successful.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Wi-Fi connection details so that a factory-reset device can connect and download the EMM provider app. Note: Android now does not support 802.1x Wi-Fi for this step.
- Time zone for the device (optional).
- Geographic location for the device (optional).

When the two devices are bumped, the data from the Provisioning Tool is sent to the factory-reset device. That data is then used to download Citrix Secure Hub with administrator settings. If you don't enter time zone and location values, Android automatically configures the values on the new device.

Configuring the Citrix Endpoint Management Provisioning Tool Before doing an NFC bump, you must configure the Provisioning Tool. This configuration is then transferred to the factory-reset device during the NFC bump.



You can type data into the required fields or populate them via a text file. The steps in the next procedure describe how to configure the text file and have descriptions for each field. The app doesn't

© 1997–2025 Citrix Systems, Inc. All rights reserved.

save information after you type it, so you might want to create a text file to keep the information for future use.

To configure the Provisioning Tool by using a text file Name the file nfcprovisioning.txt and place the file in the **/sdcard/** folder on the SD card of the device. The app can then read the text file and populate the values.

The text file must have the following data:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

This line is the intranet/internet location of the EMM provider app. After the factory-reset device connects to Wi-Fi following the NFC bump, the device must have access to this location for downloading. The URL is a regular URL, with no special formatting required.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>`

This line is the checksum of the EMM provider app. This checksum is used to verify that the download is successful. Steps to get the checksum are discussed later in this article.

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

This line is the connected Wi-Fi SSID of the device on which the Provisioning Tool is running.

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

Supported values are WEP and WPA2. If the Wi-Fi is unprotected, this field must be empty.

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

If the Wi-Fi is unprotected, this field must be empty.

`android.app.extra.PROVISIONING_LOCALE=<locale>`

Enter language and country codes. The language codes are two-letter lowercase ISO language codes (such as en) as defined by ISO 639-1. The country codes are two-letter uppercase ISO country codes (such as US) as defined by ISO 3166-1. For example, type en_US for English as spoken in the United States. If you don't type any codes, the country and language are automatically populated.

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

The time zone in which the device is running. Type the database name of the area/location. For example, type **America/Los_Angeles** for Pacific time. If you don't type a name, the time zone automatically populates.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

© 1997–2025 Citrix Systems, Inc. All rights reserved.

This data isn't required, because the value is hardcoded into the app as Citrix Secure Hub. It's mentioned here only for the sake of completion.

If there is a Wi-Fi protected by using WPA2, a completed nfcprovisioning.txt file might look like the following:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

If there is an unprotected Wi-Fi, a completed nfcprovisioning.txt file might look like the following:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

To get the checksum of Citrix Secure Hub The checksum of Citrix Secure Hub is a constant value: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`. To download an APK file for Citrix Secure Hub, use the following Google Play store link: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

To get an app checksum Prerequisites:

- The **apksigner** tool from the Android SDK Build Tools
- OpenSSL command line

To get the checksum of any app, follow these steps:

1. Download the app's APK file from the Google Play store.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. In the OpenSSL command line, navigate to the **apksigner** tool: `android-sdk/build-tools/<version>/apksigner` and type the following:

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{
 (?<=SHA-256 digest:) .* }
 ' | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
```

   The command returns a valid checksum.

3. To generate the QR code, enter the checksum in the `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHE` field. For example:

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"
    }

 }
```

Libraries used The Provisioning Tool uses the following libraries in its source code:

- v7 `appcompat` library, Design Support library, and v7 palette support library

  For information, look for the Support Library Features Guide in the Android developers documentation.

- Butter Knife by Jake Wharton under Apache license 2.0

Provision work profile devices in Android Enterprise

On work profile devices in Android Enterprises, you securely separate the corporate and personal areas on a device. For example, BYOD devices can be work profile devices. The enrollment experience for work profile devices is similar to Android enrollment in Citrix Endpoint Management. Users download Citrix Secure Hub from Google Play and enroll their devices.

By default, the USB Debugging and Unknown Sources settings are disabled on a device when it is enrolled in Android Enterprise as a work profile device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Tip:**
>
> When enrolling devices in Android Enterprise as work profile devices, always go to Google Play. From there, enable Citrix Secure Hub to appear in the user's personal profile.

Android OS

February 29, 2024

> **Note:**
>
> This article doesn't apply to devices that are managed with Android Enterprise. For information about those devices, see other articles in this section.

Citrix Endpoint Management also supports Android OS devices that aren't managed through an Android or Samsung enterprise program. To control how and when Android devices connect to the Citrix Endpoint Management service, use Firebase Cloud Messaging (FCM). For information, see Firebase Cloud Messaging.

Enrollment profiles determine whether Android devices enroll in MAM, MDM, or MDM+MAM, with the option for users to opt out of MDM. Citrix Endpoint Management supports the following authentication types for Android devices in MDM+MAM. For information, see the following articles:

- Domain or domain plus security token authentication
- Client certificate or certificate plus domain authentication
- Identity providers:
  - Authentication with Azure Active Directory through Citrix Cloud
  - Authentication with Okta through Citrix Cloud

Another rarely used authentication method is a client certificate plus security token. For information, see https://support.citrix.com/article/CTX215200.

A general workflow for starting Android device management is as follows:

1. Complete the onboarding process. See Onboarding and resource setup and Prepare to enroll devices and deliver resources.
2. Choose and configure an enrollment method. See Supported enrollment methods.
3. Configure Android device policies.
4. Enroll Android devices.
5. Set up device and app security actions. See Security actions.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For supported operating systems, see Supported device operating systems.

Supported enrollment methods

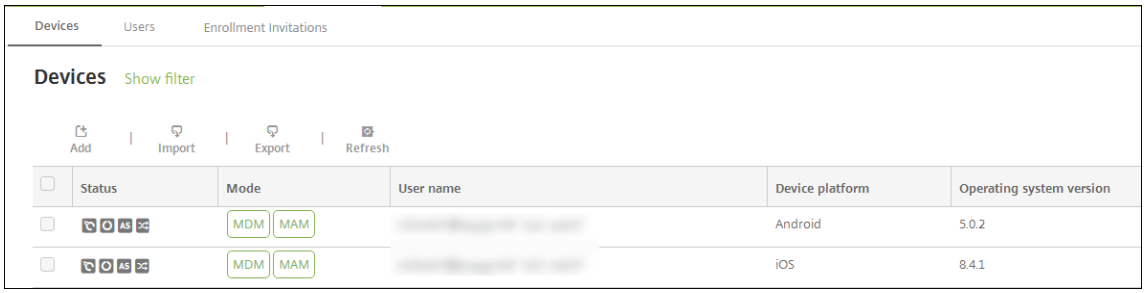
The following table lists the enrollment methods that Citrix Endpoint Management supports for Android devices:

Method	Supported
Bulk enrollment	No
Manual enrollment	Yes
Enrollment invitations	Yes

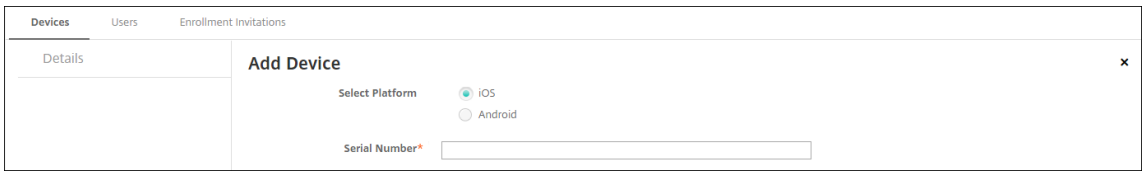
Add an Android device manually

If you want to add an Android or iOS device manually, such as for testing purposes, follow these steps.

1. In the Citrix Endpoint Management console, click **Manage > Devices**. The **Devices** page appears.



2. Click **Add**. The **Add Device** page appears.



3. Configure these settings:

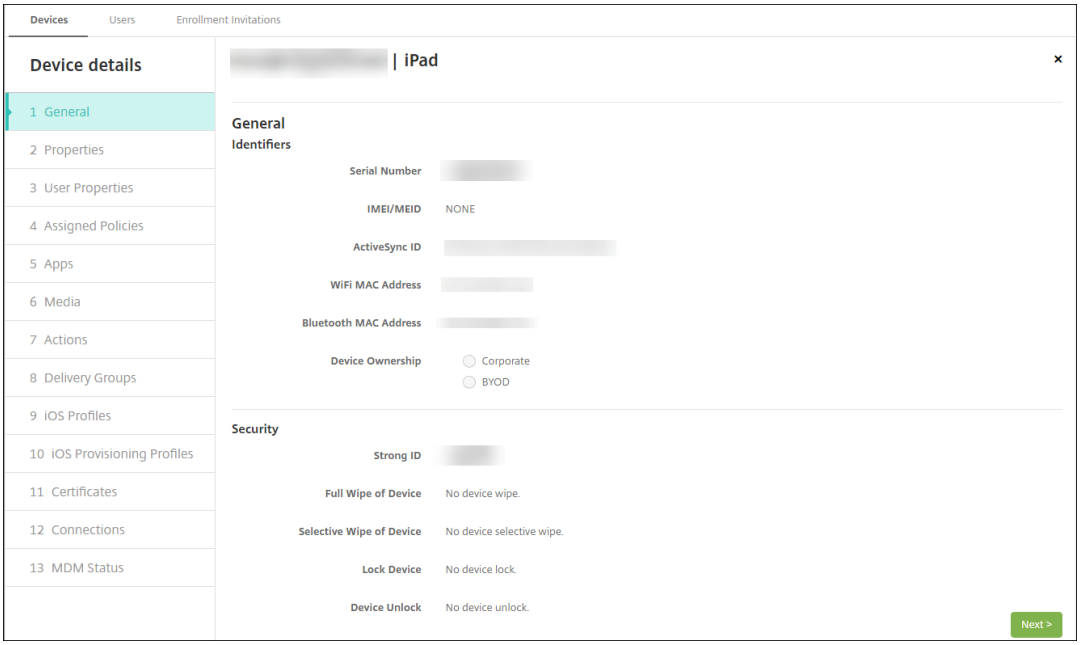
   - **Select platform:** Click **Android**.
   - **Serial Number:** Type the device serial number.
   - **IMEI/MEID:** Optionally, type the device IMEI/MEID information.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. Click **Add**. The **Devices** table appears with the device added to the bottom of the list. To view and confirm the device details: Choose the device that you added and then, in the menu that appears, click **Edit**.

> **Note:**
>
> When you select the checkbox next to a device, the options menu appears above the device list. When you click anywhere else in the list, the options menu appears on the right side of the listing.

- LDAP configured
- If using local groups and local users:
  - One or more local groups.
  - Local users assigned to local groups.
  - Delivery groups are associated with local groups.
- If using Active Directory:
  - Delivery groups are associated with Active Directory groups.



5. The **General** page lists the device **Identifiers**, such as the serial number and other information for the platform type. For **Device Ownership**, select **Corporate** or **BYOD**.

   The **General** page also lists device **Security** properties, such as Strong ID, Lock Device, Activation Lock Bypass, and other information for the platform type. The **Full Wipe of Device** field includes the user PIN code. The user must enter that code after the device is wiped. If the user forgets the code, you can look it up here.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

6. The **Properties** page lists the device properties that Citrix Endpoint Management is to provision. This list shows any device properties included in the provisioning file used to add the device. To add a property, click **Add** and then select a property from the list. For valid values for each property, see the PDF Device property names and values.

   When you add a property, it initially appears under the category where you added it. After you click **Next** and then return to the **Properties** page, the property appears in the appropriate list.

   To delete a property, hover over the listing and then click the **X** on the right side. Citrix Endpoint Management deletes the item immediately.

7. The remaining **Device Details** sections have summary information for the device.

   - **User Properties:** Displays RBAC roles, group memberships, managed Google Play accounts, and properties for the user. You can retire a managed Google Play account from this page.
   - **Assigned Policies:** Displays the number of deployed, pending, and failed policies. Provides the policy name, type, and last deployed information for each policy. Lets you reset the deployment status to pending and redeploy policies that the user removed.
   - **Apps:** Displays, for the last inventory, the number of installed, pending, and failed app deployments. Provides the app name, identifier, type, and other information. For a description of iOS and macOS inventory keys, such as **HasUpdateAvailable**, see Mobile Device Management (MDM) Protocol.
   - **Media:** Displays, for the last inventory, the number of deployed, pending, and failed media deployments.
   - **Actions:** Displays the number of deployed, pending, and failed actions. Provides the action name and time of the last deployment.
   - **Delivery Groups:** Displays the number of successful, pending, and failed delivery groups. For each deployment, provides the delivery group name and deployment time. Select a delivery group to view more detailed information, including status, action, and channel or user.
   - **iOS Profiles:** Displays the last iOS profile inventory, including name, type, organization, and description.
   - **iOS Provisioning Profiles:** Displays enterprise distribution provisioning profile information, such as the UUID, expiration date, and managed status.
   - **Certificates:** Displays, for valid, expired, or revoked certificates, information such as the type, provider, issuer, serial number, and the number of remaining days before expiration.
   - **Connections:** Displays the first connection status and the last connection status. Provides for each connection, the user name, penultimate (next to last) authentication time, and last authentication time.
   - **MDM Status:** Displays information such as the MDM status, last push time, and last device reply time.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure Android device policies

Use these policies to configure how Citrix Endpoint Management interacts with devices running Android. This table lists all device policies available for Android devices.

APN	App access	App inventory
App lock	App uninstall	Credentials
Citrix Endpoint Management options	Citrix Endpoint Management uninstall	Files
Launcher configuration	Location	Network
Passcode	Restrictions	Scheduling
Store	Terms and Conditions	Tunnel
VPN	Web clip	

Enroll Android devices

1. Go to the Google Play store on your Android device, download the Citrix Secure Hub app, and then tap the app.
2. When prompted to install the app, click **Next** and then click **Install**.
3. After Citrix Secure Hub installs, tap **Open**.
4. For devices running Android 6.0 and greater, accept the required permissions:
    - Allow Citrix Secure Hub to make and manage phone calls? (required)
    - Allow Citrix Secure Hub to access photos, media, and files on your device? (required)
    - Allow Citrix Secure Hub to access this device's location? (optional)
5. Enter your corporate credentials, such as your Citrix Endpoint Management server name, User Principal Name (UPN), or email address. Then, click **Next**.
6. Choose how to enroll your device:
    - To enroll in MDM+MAM, tap **Yes, enroll**.
    - To enroll in MAM, tap **No**.
7. In the **Activate device administrator** screen, tap **Activate**.
8. Enter your corporate password and then tap **Sign On**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

9. Depending on the way Citrix Endpoint Management is configured, you might be asked to create a Citrix PIN. You can use the PIN to sign on to Citrix Secure Hub and other Citrix Endpoint Management-enabled apps, such as Citrix Secure Mail and Citrix Files. You enter your Citrix PIN twice. On the **Create Citrix PIN** screen, enter a PIN.
10. Reenter the PIN. Citrix Secure Hub opens. You can then access the app store to view the apps you can install on your Android device.
11. If you configured Citrix Endpoint Management to push apps to devices automatically after enrollment, users are prompted to install the apps. Also, the policies that you configure in Citrix Endpoint Management are deployed to the device. Tap **Install** to install the app.

To unenroll and reenroll an Android device

Users can unenroll from within Citrix Secure Hub. When users unenroll by using the following procedure, the device still appears in the device inventory in the Citrix Endpoint Management console. You can't do the actions on the device, however. For example, you can't track the device or monitor device compliance.

1. Tap to open the Citrix Secure Hub app.
2. Depending on whether you have a phone or a tablet, do the following:

   On a phone:

   - Swipe from the left of the screen to open a settings pane.
   - Tap **Preferences**, tap **Accounts**, and then tap **Delete Account**.

   On a tablet:

   - Tap the arrow next to your email address on the upper-right corner.
   - Tap **Preferences**, tap **Accounts**, and then tap **Delete Account**.
3. In the **Delete Account?** window, tap **Yes, delete**.
   Citrix Secure Hub unenrolls your device. Follow the on-screen instructions to re-enroll your device.

Security actions

Android supports the following security actions. For a description of each security action, see Security actions.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App Lock	App Wipe	Certificate Renewal
Full Wipe	Locate	Lock
Lock and Reset Password	Notify	Revoke
Selective Wipe		

> **Note:**
>
> For devices running Android 6.0 and greater, the Locate security action requires the user to grant Location permission during enrollment. The user can opt not to grant Location permission. If the user doesn't grant the permission during enrollment, Citrix Endpoint Management again requests location permission when sending the Locate command.

Firebase Cloud Messaging

September 6, 2025

> **Note:**
>
> Firebase Cloud Messaging (FCM) was previously known as Google Cloud Messaging (GCM). Some Citrix Endpoint Management console labels and messages use the GCM terminology.

Citrix recommends that you use Firebase Cloud Messaging (FCM) to control how and when Android devices connect to Citrix Endpoint Management. Citrix Endpoint Management, when configured for FCM sends connection notifications to Android devices that are enabled for FCM. Any security action or deploy command triggers a push notification to prompt the user to reconnect to the Citrix Endpoint Management server.

After you complete the configuration steps in this article and a device checks in, the device registers with the FCM service in Citrix Endpoint Management. That connection enables near real-time communication from your Citrix Endpoint Management service to your device by using FCM. FCM registration works for new device enrollments and previously enrolled devices.

When Citrix Endpoint Management needs to start a connection to the device, it connects to the FCM service. Then, the FCM service notifies the device to connect. This type of connection is similar to what Apple uses for its Push Notification Service.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Prerequisites

- Latest Citrix Secure Hub client
- Google developer account credentials
- Google Play services installed on FCM-enabled Android devices

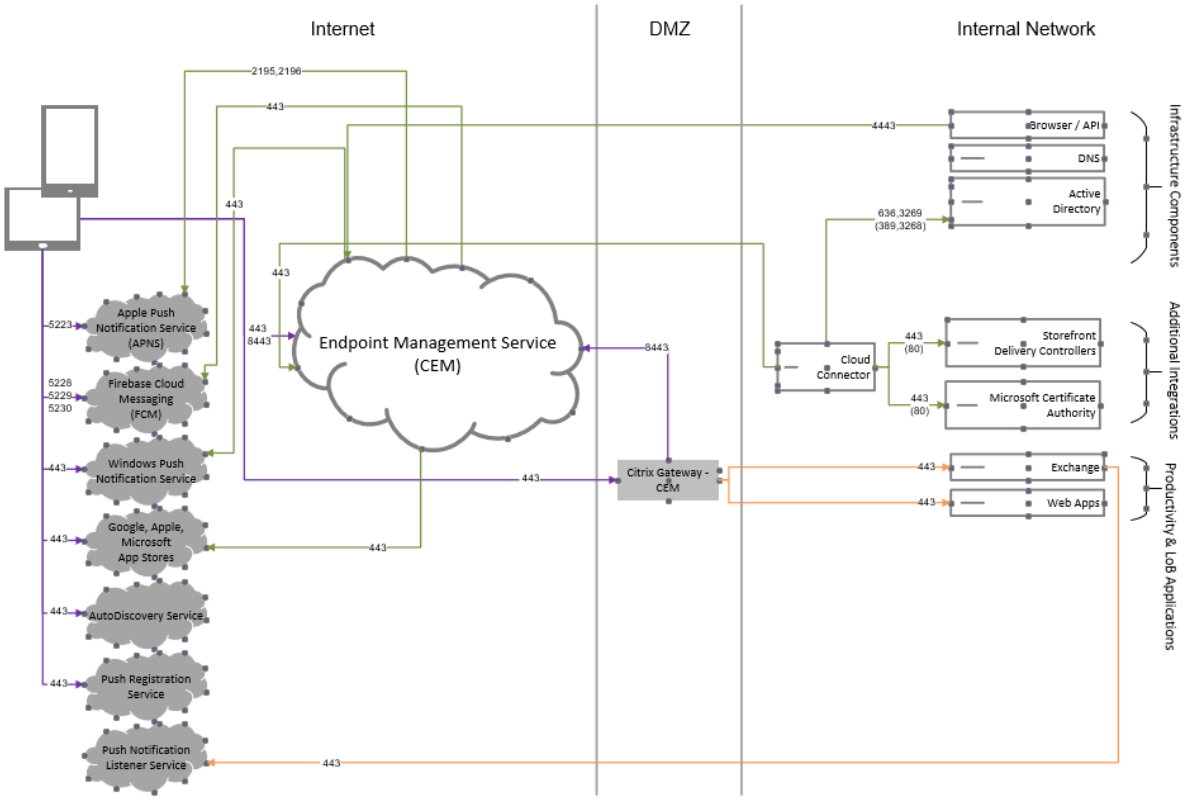
Firewall ports

- Open port 443 on Citrix Endpoint Management to `fcm.googleapis.com` and `Google.com`.
- Open outgoing Internet communication for device Wi-Fi on ports 5228, 5229, and 5230.
- To allow outgoing connections, FCM recommends adding ports 5228 through 5230 to an allow list, with no IP restrictions. However, if you require IP restrictions, FCM recommends adding all the IP addresses in the IPv4 and IPv6 blocks to an allow list. Those blocks are listed in the Google ASN of 15169. Update that list monthly.

For more information, see Port requirements.

Architecture

This diagram shows the communication flow for FCM in the external and internal network.



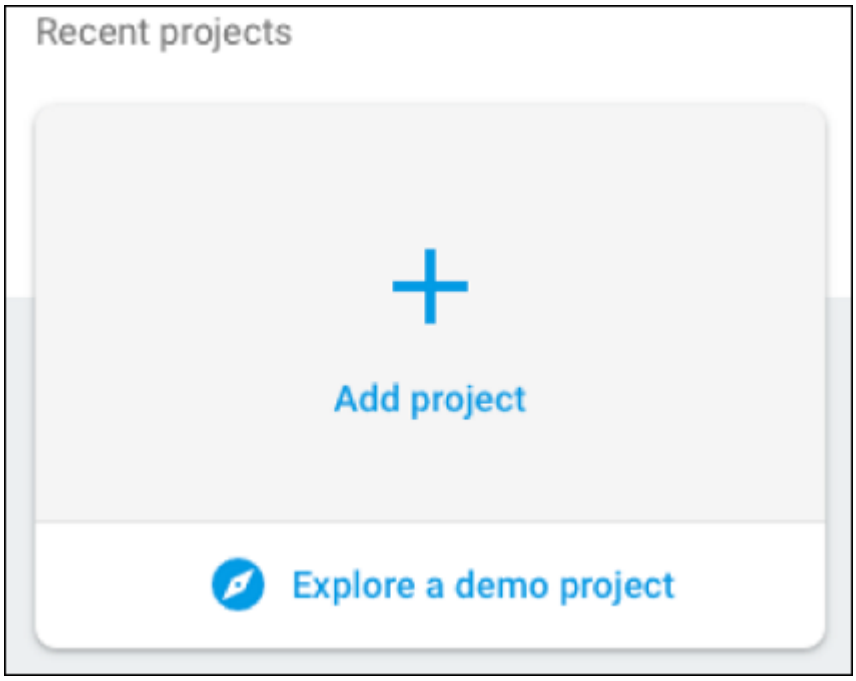
© 1997–2025 Citrix Systems, Inc. All rights reserved.

To configure your Google account for FCM

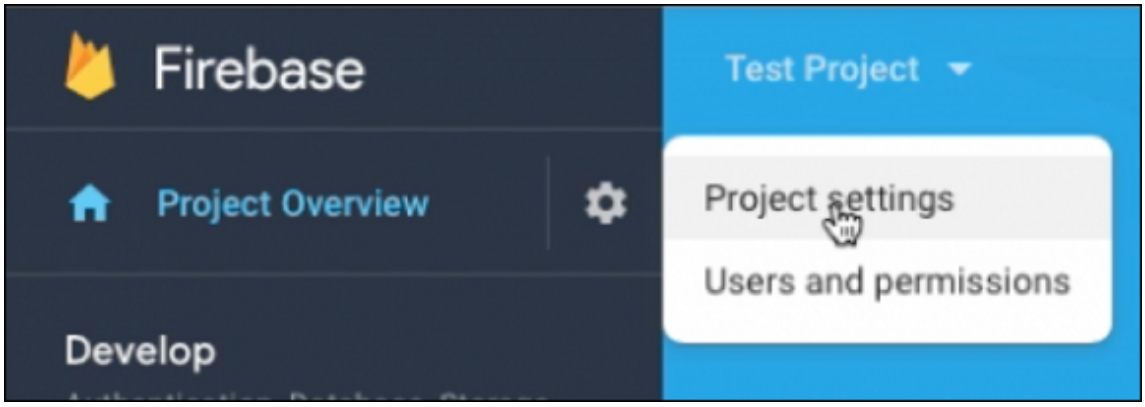
1. Sign in to the following URL using your Google developer account credentials:

   https://console.firebase.google.com/

2. Click **Add project**.



3. After you create the project, click **Project settings**.



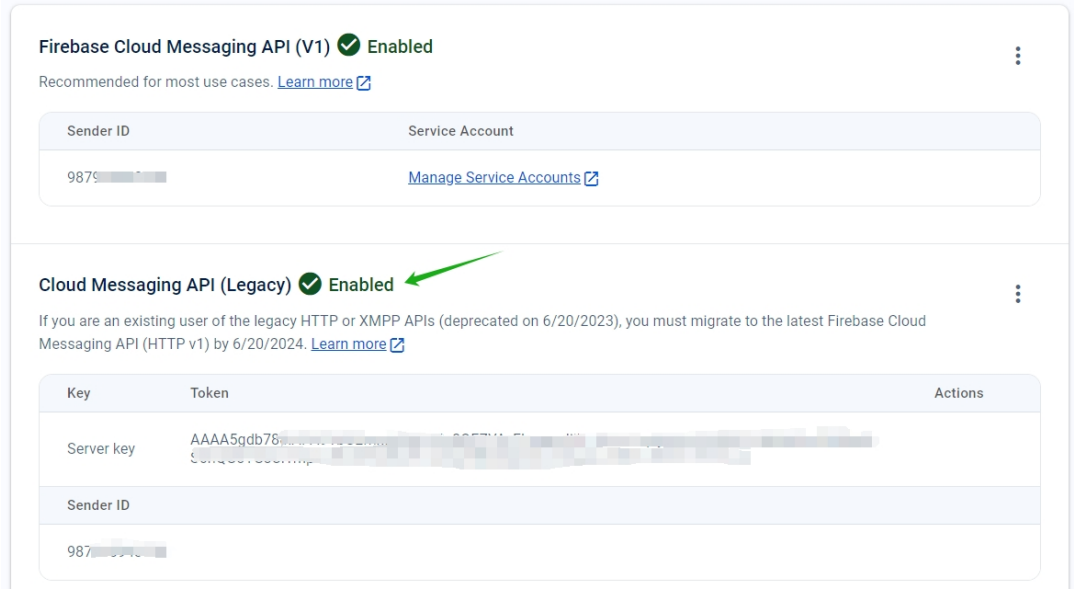
> **Note:**
>
> Google is going to deprecate the FCM legacy APIs for HTTP, which is currently used in our FCM implementation. The migration deadline is on June 21, 2024. We need to migrate the FCM from legacy FCM API to HTTP v1 API. For more information, see Migrate from legacy FCM APIs to HTTP v1.

4. Click the **Cloud Messaging** tab. Verify that the Firebase Cloud Messaging API is enabled and

© 1997–2025 Citrix Systems, Inc. All rights reserved.

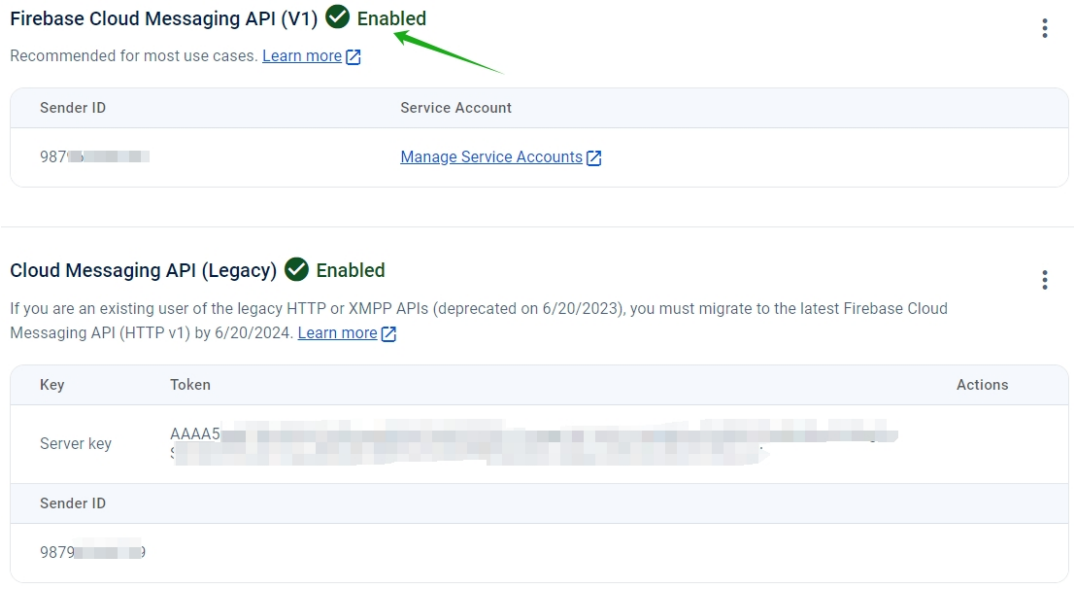
click **Manage Service Accounts**.

a) Before migration, you could use the legacy API, ensure the Cloud Messaging API (Legacy) is enabled. Copy the values from **Key** and **Sender ID** fields.



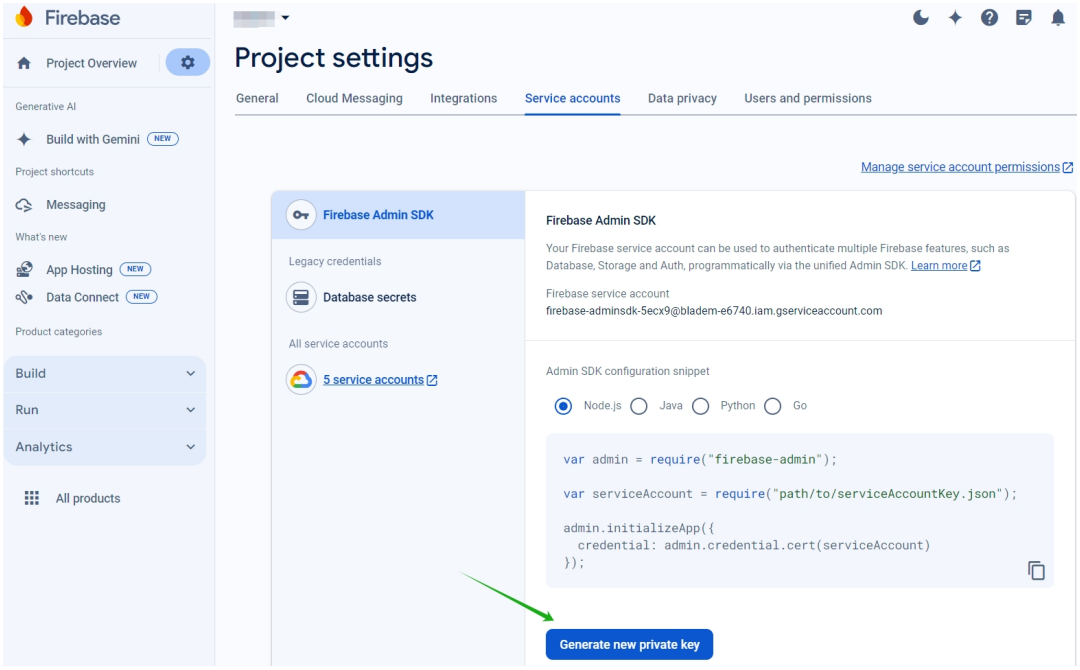
If you don't have a key listed, click the ellipsis under **Actions** to add a key.

b) After migration, the legacy API is deprecated from Google. You have to enable the Firebase Cloud Messaging API(V1). For more information, see Migrate from legacy FCM APIs to HTTP v1.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Download the service account JSON file from **Service accounts** under **Project settings**. See Provide credentials manually section to generate a private key file for your service account. Click **Generate new private key** to download the service account key JSON file.



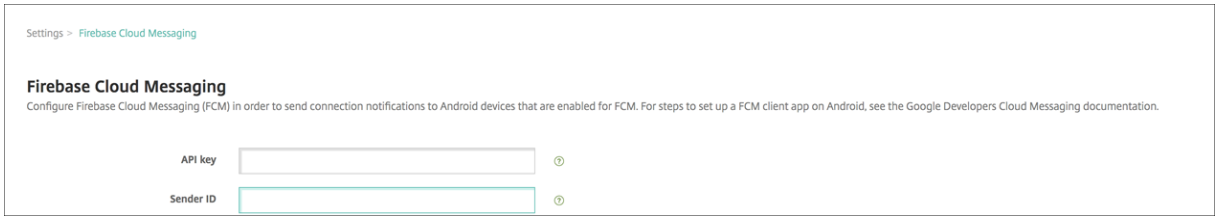
For steps to set up an FCM client app on Android, see this Google Developers Cloud Messaging article: https://firebase.google.com/docs/cloud-messaging/android/client.

To configure Citrix Endpoint Management for FCM

In the Citrix Endpoint Management console, go to **Settings > Firebase Cloud Messaging**.

For Cloud Messaging API (Legacy)

1. Enter the Firebase Cloud Messaging **Key** from the last step of the Firebase Cloud Messaging configuration in **API key** field.
2. Enter the **Sender ID** value from the previous procedure.

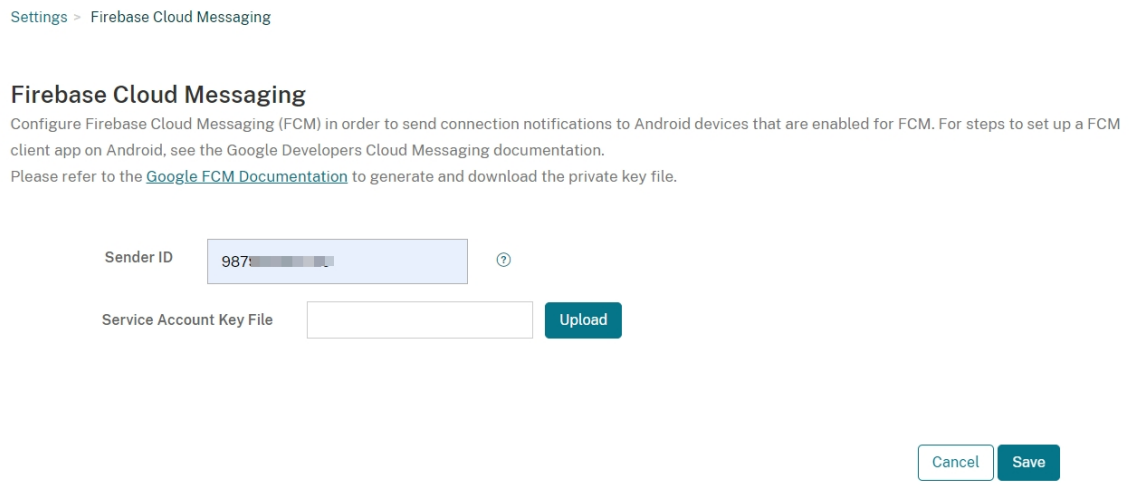


© 1997–2025 Citrix Systems, Inc. All rights reserved.

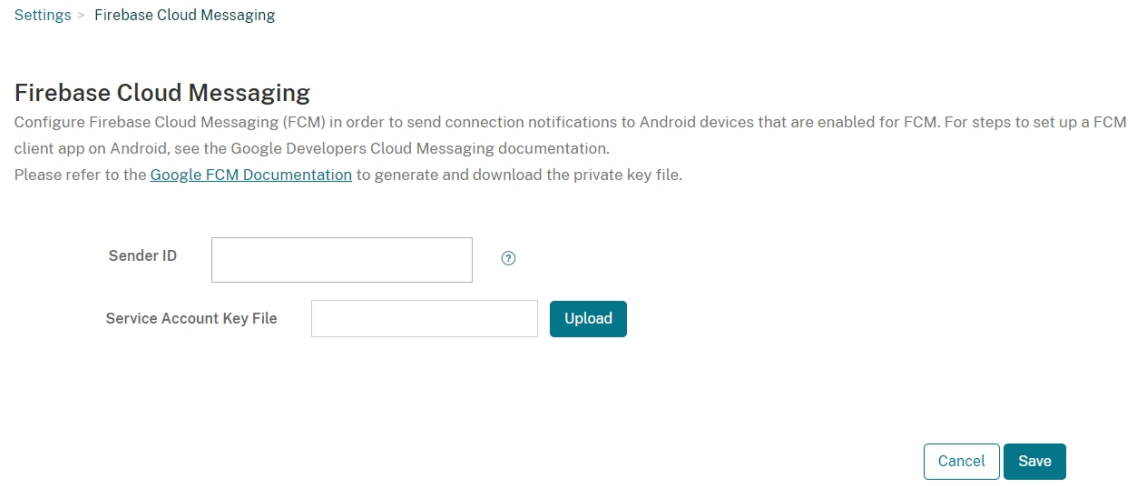
For Firebase Cloud Messaging API (V1)

> **Notes:**
>
> - To enable FCM API V1 for Citrix Endpoint Management version 24.6.0 and later, see the Knowledge Center article CTX677031.
> - If you are a new FCM user, skip step 1 and proceed from step 2.

1. If you are already using FCM, you will notice that the Sender ID is auto-populated with your current FCM project and a new option to upload the **Service Account Key File**.

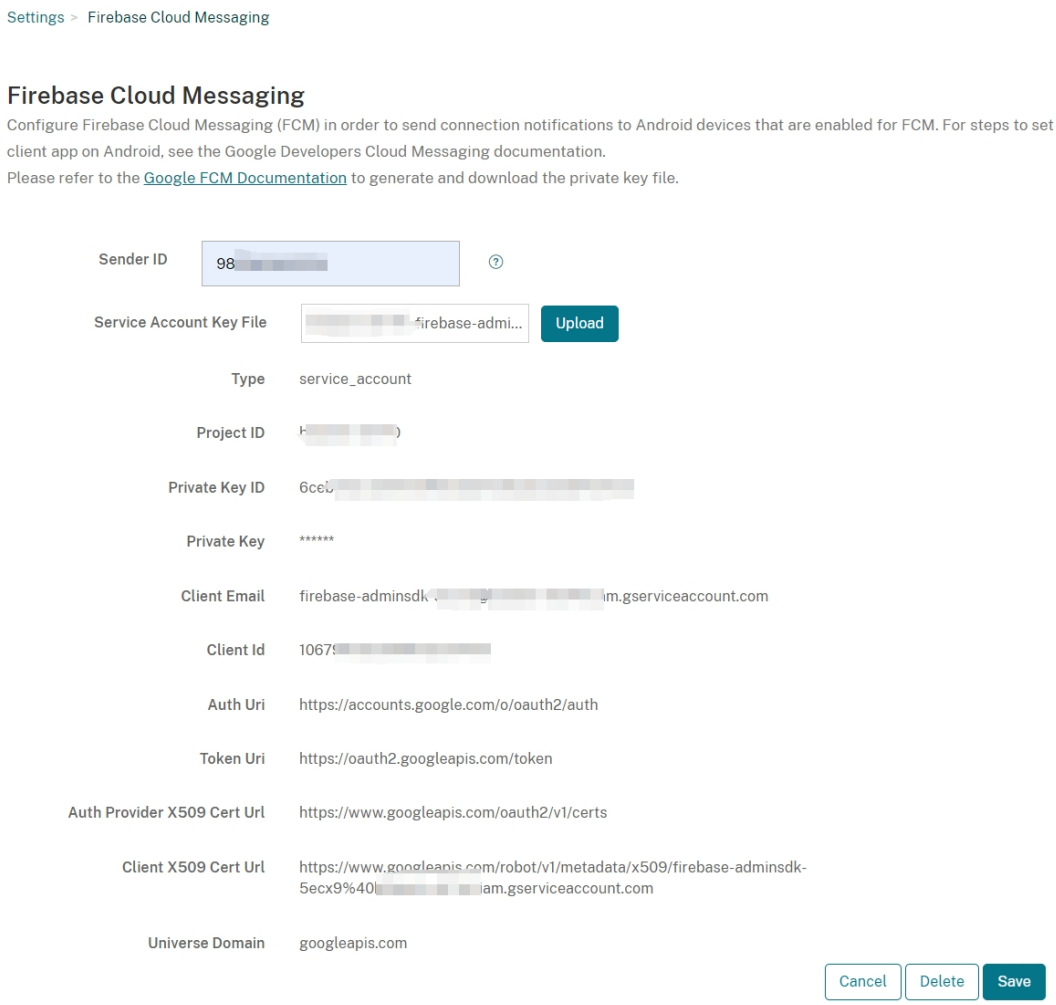


2. If you are a new FCM user, enter the **Sender ID** and upload the **Service Account Key File** from the previous procedure.



3. The uploaded file will be parsed and the corresponding fields will be auto-generated.

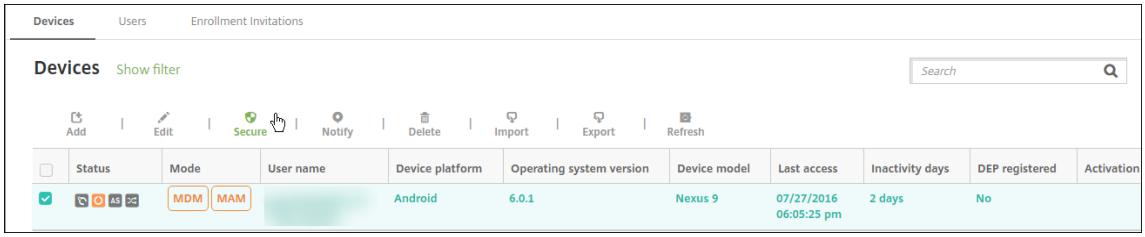
© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Verify the information and click **Save**.

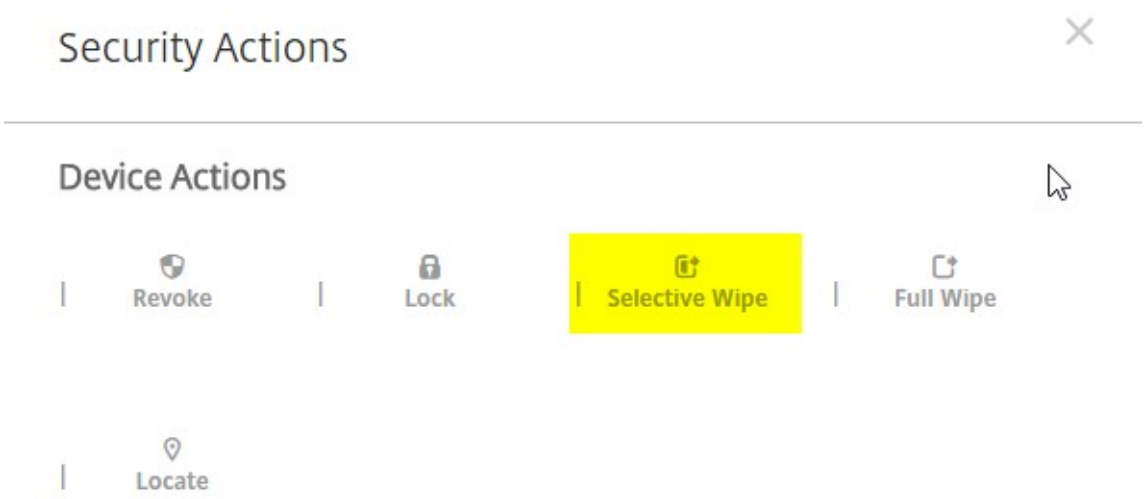
To test your configuration

1. Enroll an Android device.
2. Leave the device idle for some time, so that it disconnects from Citrix Endpoint Management.
3. From the Citrix Endpoint Management console, click **Manage**, select the Android device, and then click **Secure**.



4. Under **Device Actions**, click **Selective Wipe**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



In a successful configuration, selective wipe occurs on the device.

Support managed configurations feedback (Technical Preview)

September 6, 2025

> **Note:**
>
> Features in the Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. You can provide feedback on this feature by clicking **Send us your feedback**. Citrix might act on feedback based on its severity, criticality, and importance.

The managed configuration feedback feature allows administrators to obtain feedback on app states from Android devices that are configured with managed configuration policies. This feedback can be used to monitor the effectiveness and status of these policies.

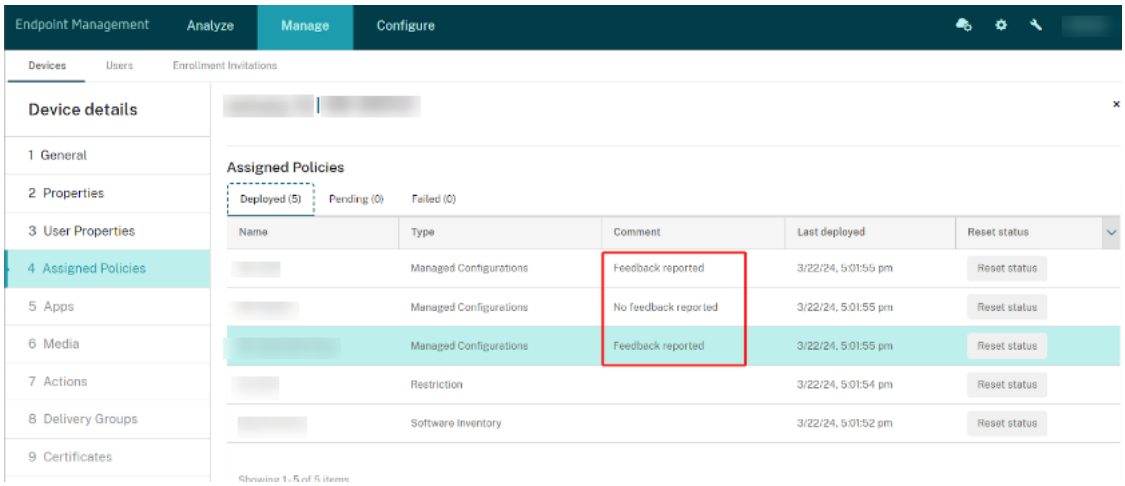
Prerequisites

1. `App Support`: The application must support managed configuration policies.
2. `Keyed App States`: The app must also support keyed app states. For detailed information on how app feedback operates, see Send app feedback to EMMs.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

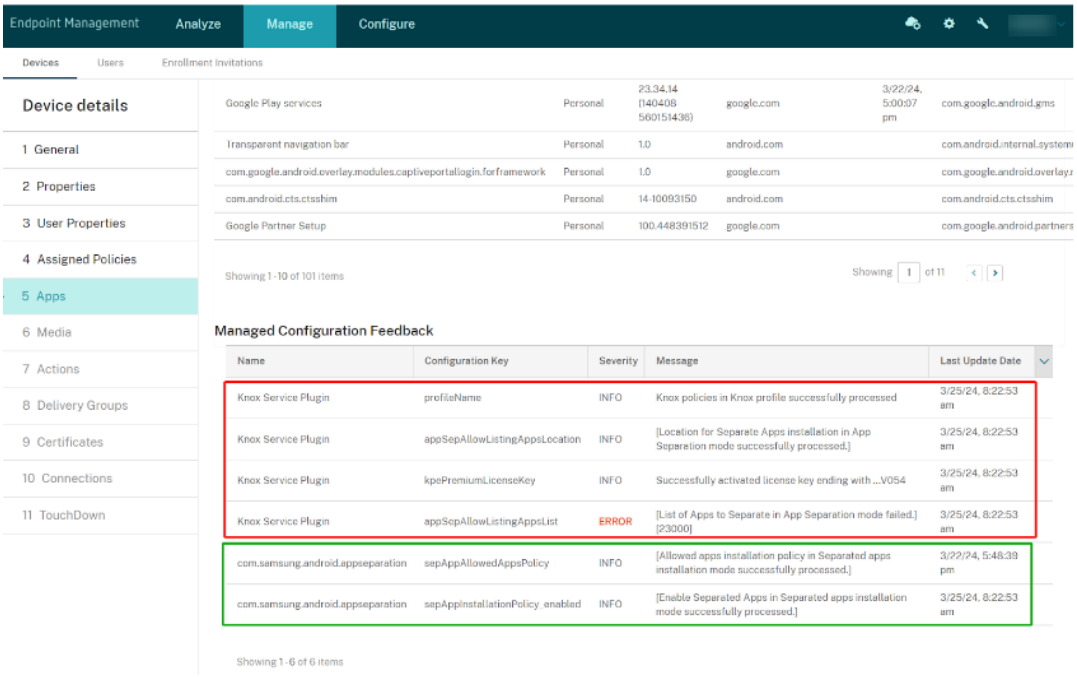
Procedure to manage and utilize Configuration feedback

1. Enable the Feature Flag `afw.app_managed_configurations.feedback` for specified (Citrix Endpoint Management) CEM server.
2. Verify managed configuration policy.
   - Confirm that the Android device is enrolled and that the managed configuration policy has been applied successfully.
   - Navigate to **Device details** and click **Assigned Policies**. The related comments to the managed configuration policy are displayed.
     - **Feedback reported**: Indicates that feedback is available for this policy-related app.
     - **No feedback reported**: Indicates that no feedback has been reported for this policy-related app.



   - Navigate to **Device details** and click **Apps**. The detailed feedback is displayed under the **Managed Configuration Feedback** table containing all the apps data.

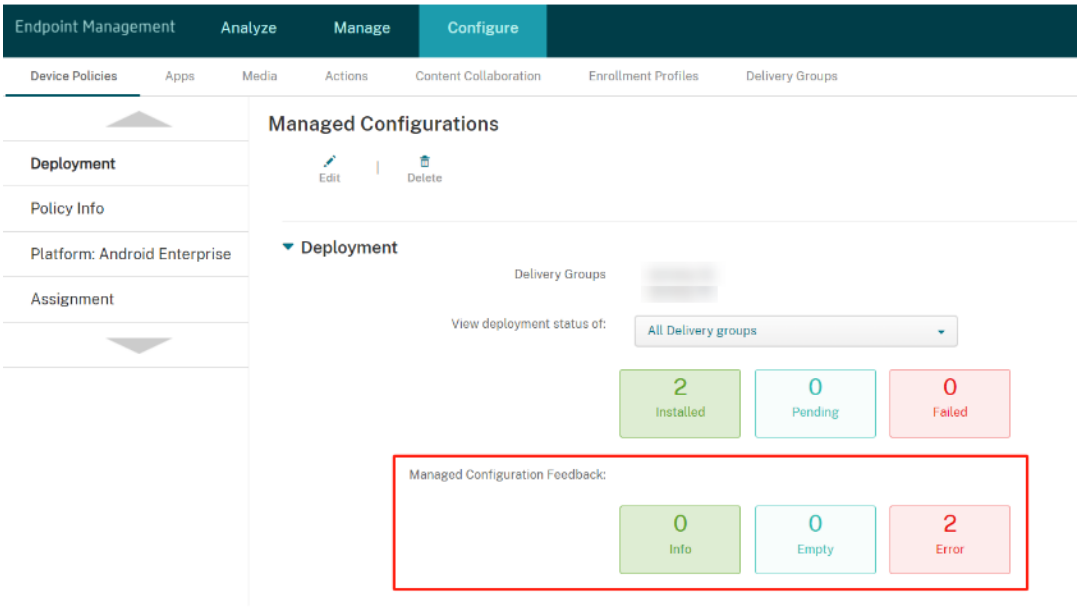
© 1997–2025 Citrix Systems, Inc. All rights reserved.



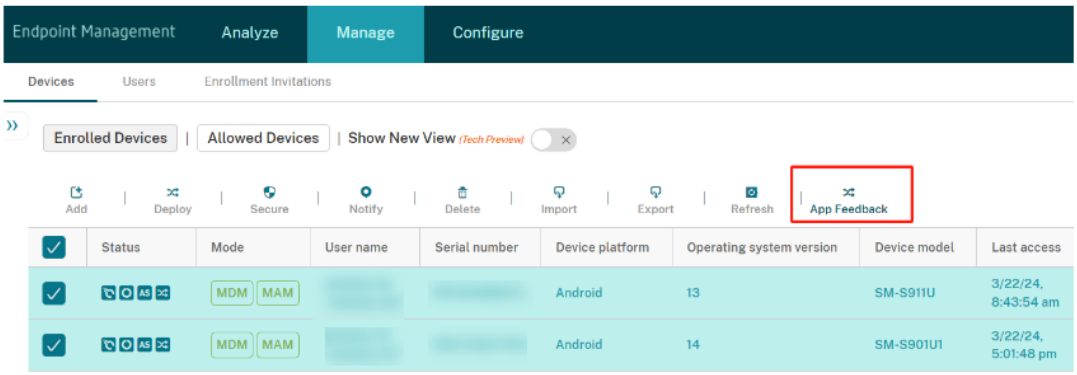
> **Note:**
>
> In the screenshot above, the red box highlights the Know Service Plugin, while the green box indicates the separated apps.

- For single managed configuration policy, you can check the feedback details for all the assigned devices:
  - **Info**: All the devices with feedback data reported containing no errors.
  - **Error**: All the devices with feedback data reported containing errors.
  - **Empty**: all the devices with no feedback data reported.

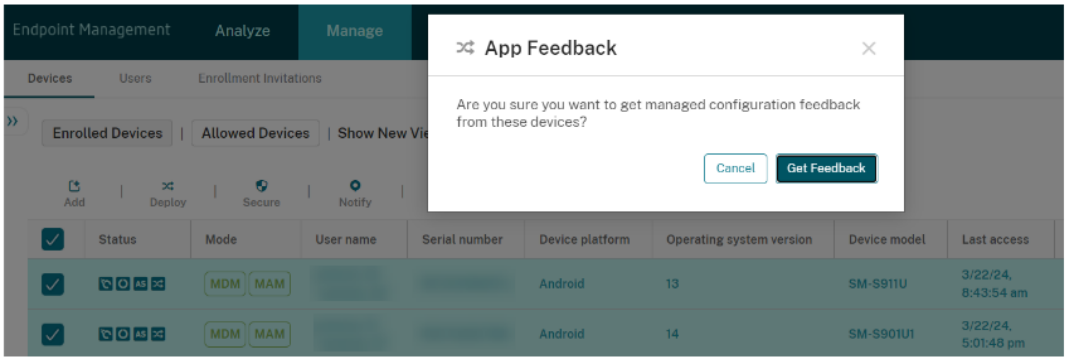
© 1997–2025 Citrix Systems, Inc. All rights reserved.



- To get the feedback manually, click **Manage** and select the checkbox to locate the corresponding devices. For example, you can select the corresponding checkboxes and click **App Feedback**.



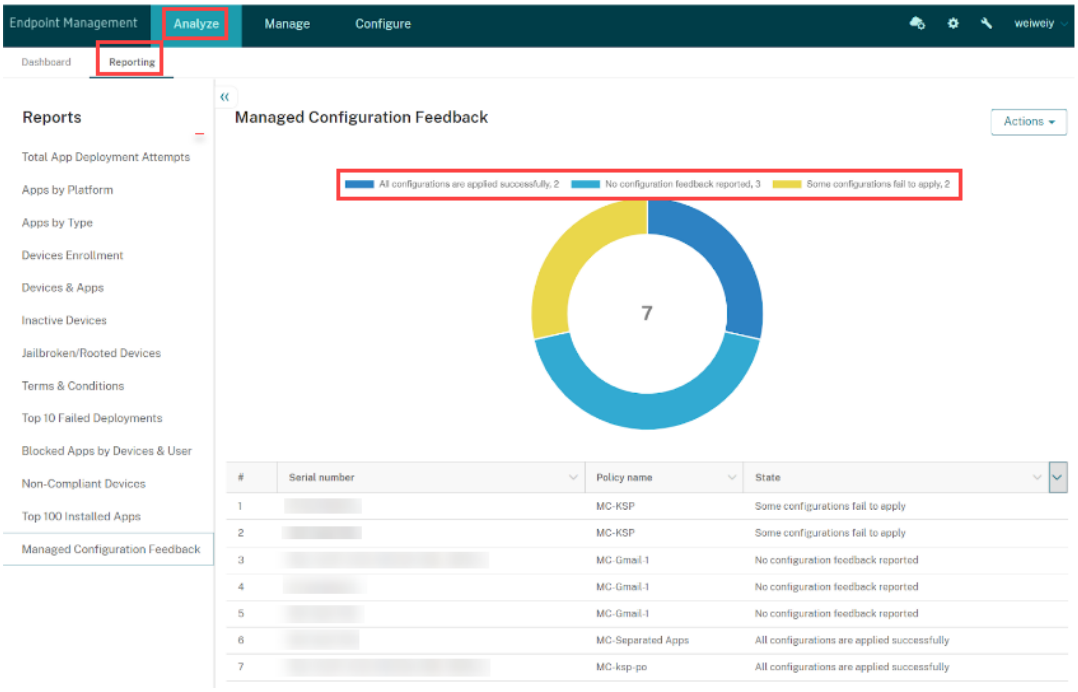
- Click **Get Feedback** to get the managed configuration feedback from the selected devices.



- From Managed Configuration Feedback report, select **Analyze** and click **Reporting** to get an overall feedback. You can see the reports for all the devices, manage configuration

© 1997–2025 Citrix Systems, Inc. All rights reserved.

policies, and the concerned configuration failures.



3. Two server properties have been introduced to adjust the feedback schedule. Use the cloud admin tools to modify these properties and control when the feedback data is saved to the database.

    a) Batch Size to Update Android Enterprise Managed Configuration Feedback database:

    - key: `android.managed.configuration.feedback.db.update.batch.size`
    - You can define the batch size of reports to be stored to DB, only for the data stored in DB will be able to show in the UI. The default value is 100 and the maximum value is 1000.

    b) Android Enterprise Managed Configuration Feedback DB Update Time Interval:

    - key: `android.managed.configuration.feedback.db.update.time.interval`
    - You can specify how long reports are stored in the database, even if the size doesn't reach the batch limit. The default value is six hours.

Troubleshooting

By default, feedback reports are retrieved during each device check-in (when Secure Hub connects to the server). However, you can manually fetch the report for specific devices using the App Feedback button.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Android SafetyNet

September 6, 2025

You can use the Android SafetyNet feature to assess the compatibility and security of Android devices that have Citrix Secure Hub installed. Android SafetyNet isn't available for MAM deployments.

When this feature is enabled, the SafetyNet Attestation API examines software and hardware information on a device to create a profile of that device. The API then looks for the same profile within a list of device models that have passed Android compatibility testing. The API also uses this information to determine whether an unknown source has modified Citrix Secure Hub.

When the Android SafetyNet feature is enabled, Citrix Secure Hub sends the SafetyNet Attestation API request to Google Play services and the result is reported back to Citrix Endpoint Management. Citrix Endpoint Management then updates device information with the attestation results. You can set automated actions that use the attestation results to trigger actions on the device.

For more information about how the SafetyNet Attestation API works, see the Android developers documentation.

Estimate how many SafetyNet Attestation API requests you need

SafetyNet Attestation API requests are sent:

- When a device is enrolled in Citrix Endpoint Management
- When a Citrix Secure Hub online authentication occurs

  Online authentication occurs when a server session expires or when a user signs off the server and then signs back on. Citrix Secure Hub prompts the user to provide credential to authenticate with the server.
- When a device is rebooted
- At a recurring time interval you configure, between 24 and 1,000 hours.

If your Citrix Endpoint Management deployment makes more than 10,000 requests per day, fill out this quota request form.

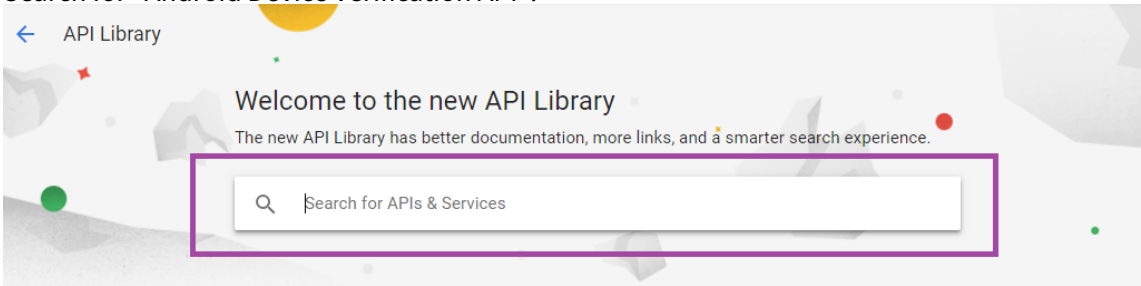
Get the SafetyNet API key

To enable Android SafetyNet in Citrix Endpoint Management, you need the **SafetyNet API** key.

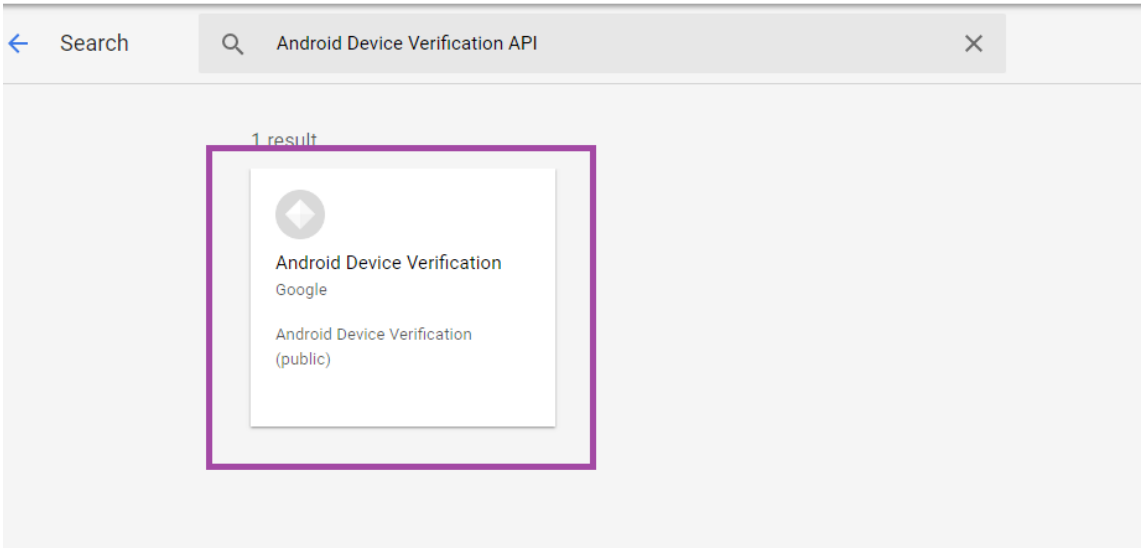
1. Log in to the Google API console with your Google administrator account credentials.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

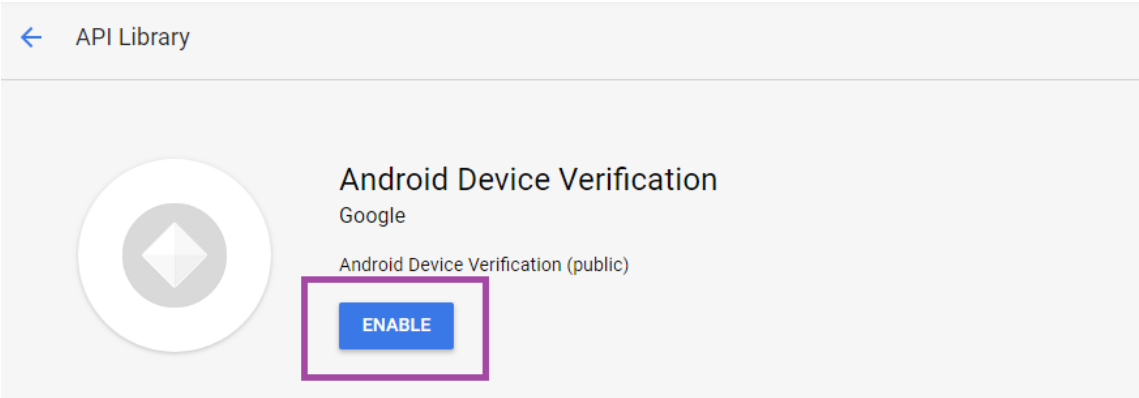
2. Go to the Library page.
3. Search for “Android Device Verification API”.



4. Click **Android Device Verification API**.

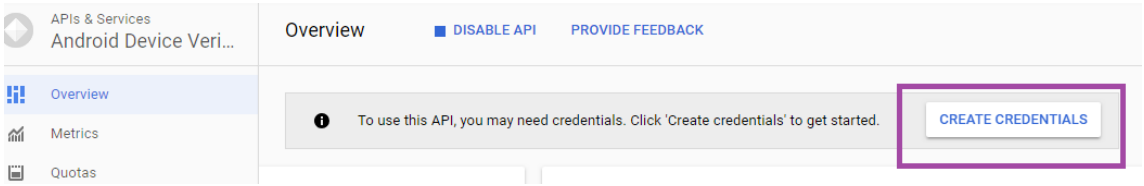


5. If the API isn’t already enabled, click **Enable**.

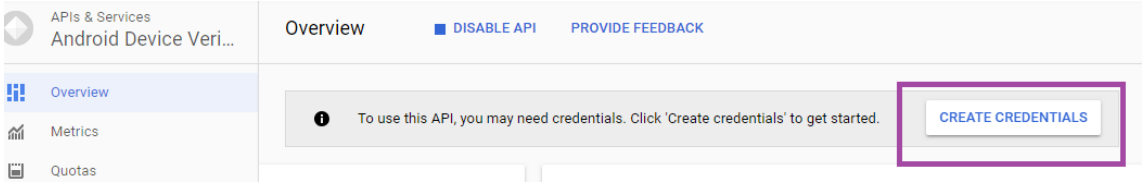


6. Click **Manage**.
7. Click **Create Credentials** to generate an API key.

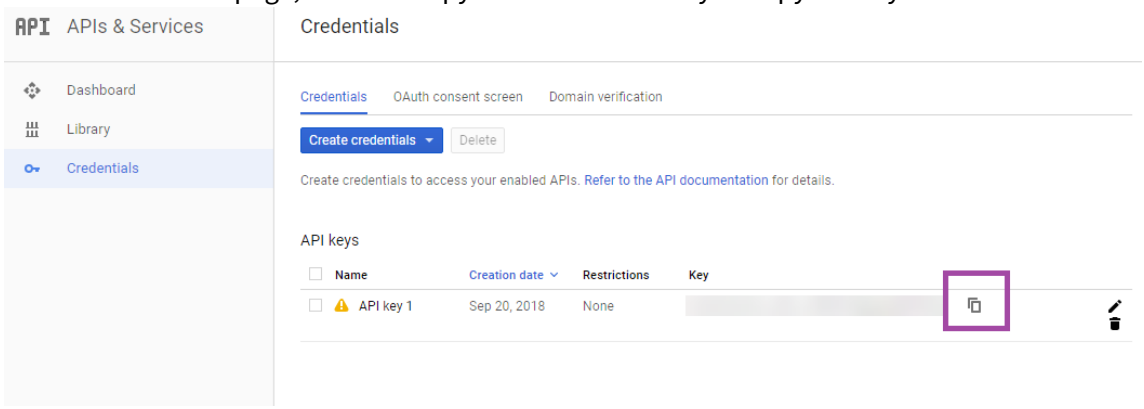
© 1997–2025 Citrix Systems, Inc. All rights reserved.



8. Select **Android Device Verification** click **What credentials to I need**. Then click **Done**.



9. In the **Credentials** page, click the copy icon next to the key to copy the key.

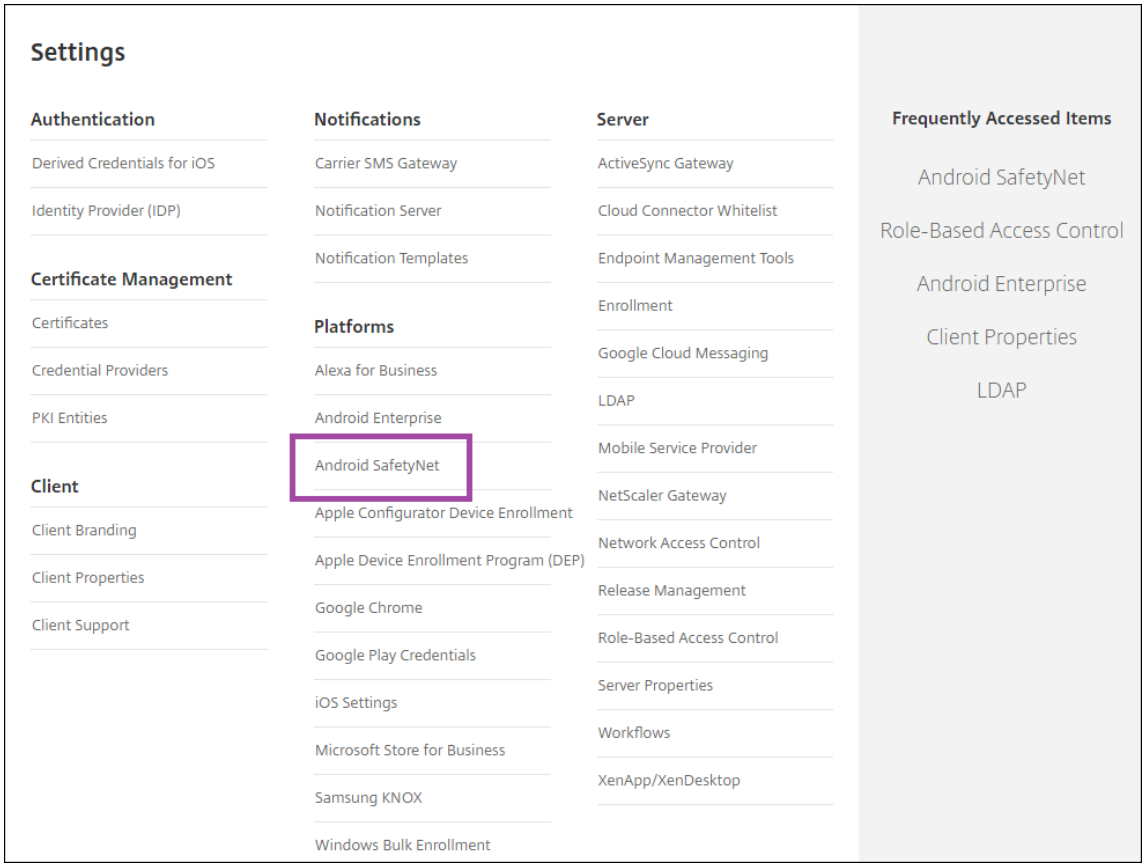


10. Save the key so you can paste it into the Citrix Endpoint Management console when you enable the Android SafetyNet.

Enable Android SafetyNet

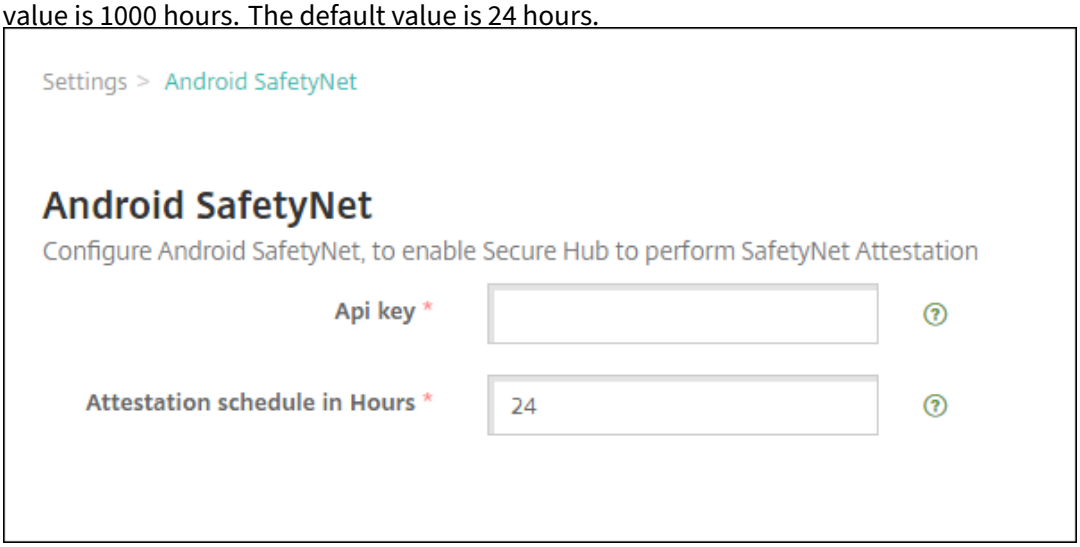
1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. On the **Settings** page, click **Android SafetyNet**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Configure these settings:

   - **API Key**. Paste in the SafetyNet API key that you got from the Google API console.
   - **Attestation schedule in hours**. Type interval at which the SafetyNet Attestation API assesses your Android devices, in hours. The minimum value is 24 hours. The maximum value is 1000 hours. The default value is 24 hours.



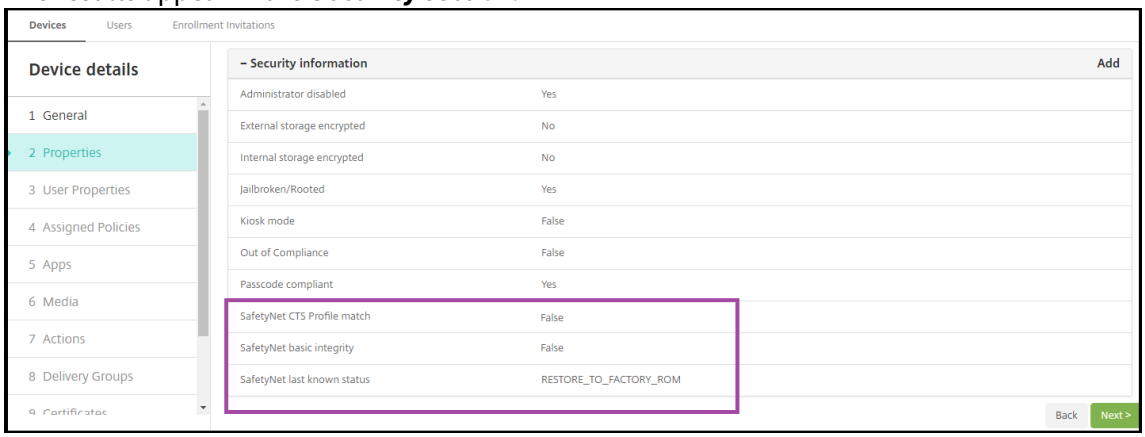
4. Click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

View Android SafetyNet results

To view the results of the SafetyNet Attestation API assessment for a device:

1. In the Citrix Endpoint Management console, click **Manage > Devices**.
2. Select Android devices to see the SafetyNet Attestation API results. Then click **Show more**.
3. In the **Device details** page, select **Properties**.
4. The results appear in the **Security** section.



The SafetyNet Attestation API returns these statuses for each device:

- **SafetyNet CTS profile match:** If this value is **True**, the device has a profile that matches one that has passed the Android Compatibility Test Suite (CTS). If this value is set as **False**, the device does not have a profile that matches one that has passed Android CTS.
- **SafetyNet basic integrity:** If this value is **True**, the SafetyNet Attestation API found no evidence that an unknown source has modified the Citrix Secure Hub on the device. If this value is set as **False**, an unknown source has modified the Citrix Secure Hub on the device.
- **SafetyNet last known status:** This value shows the last know SafetyNet status of the device:
  - **Success:** The SafetyNet Attestation API found no evidence that an unknown source has modified the Citrix Secure Hub on the device.
  - **LOCK_BOOTLOADER:** The user must lock the bootloader of the device. An unknown source has modified the Citrix Secure Hub on the device.
  - **RESTORE_TO_FACTORY_ROM:** The user must restore the device to a clean factory ROM. An unknown source has modified the Citrix Secure Hub on the device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Play Integrity API

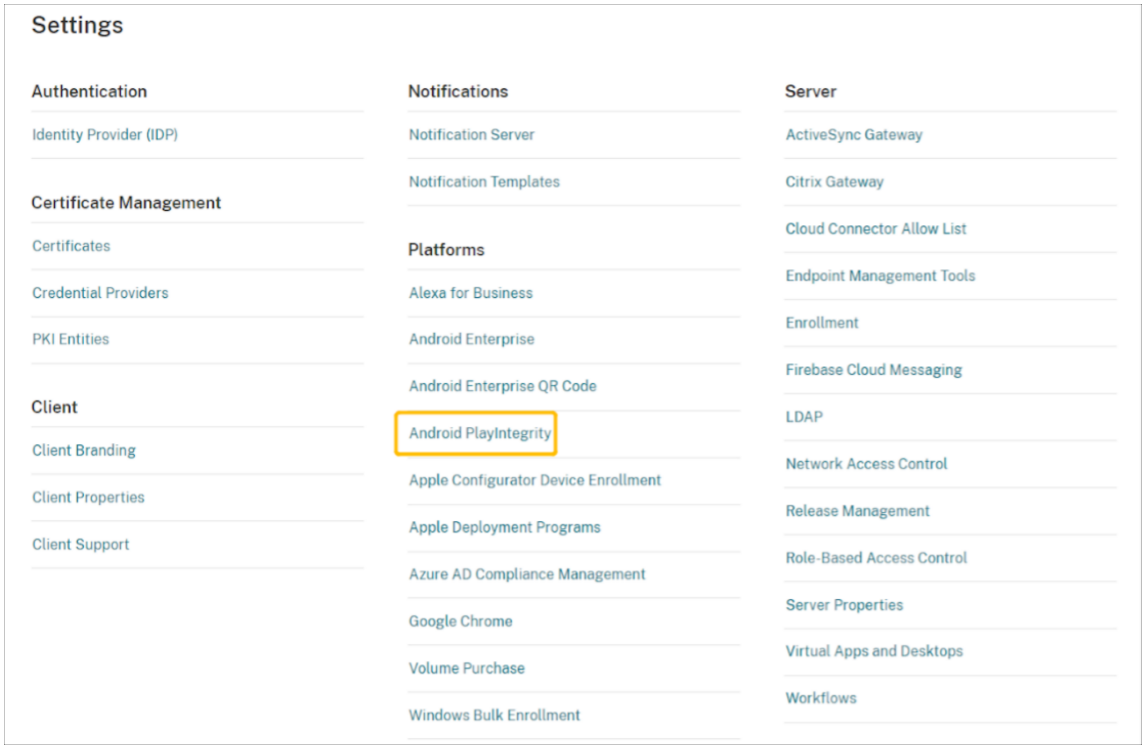
February 29, 2024

The Play Integrity API helps protect your apps and games from potentially risky and fraudulent interactions, such as cheating and unauthorized access, allowing you to respond with appropriate actions to prevent attacks and reduce abuse. For more information, see Play Integrity API.

Enable the Play Integrity API

Follow these steps to switch to the Play Integrity API.

1. Turn on the *afw.safetynet.attestation.api.* deprecation feature flag for the specified Citrix Endpoint Management server.
2. On the Citrix Endpoint Management console, select **Android PlayIntegrity** from the **Settings** page.

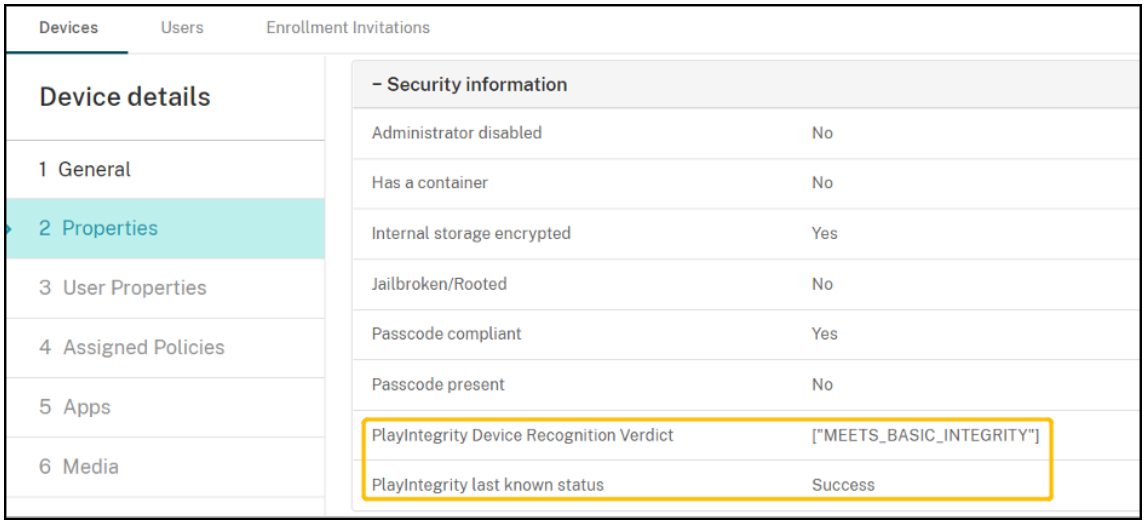


3. Enter a value in the Attestation schedule in the hours field. It is the interval time at which the PlayIntegrity Attestation API assesses your device. The minimum value is 24 hours, and the maximum value is 1000 hours. The default value is 24 hours. Click **Save**.
4. Upgrade to Citrix Secure Hub Android version 23.7.0. Sign off from your device, and sign into Citrix Secure Hub to trigger the Attest via Play Integrity API.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

View and analyze Play Integrity API attestation results

1. On the Citrix Endpoint Management console, go to **Manage > Devices**.
2. Select the device for which you want to see the Play Integrity API Attestation results. Click **Show More**.
3. In the **Devices** tab, select **Properties**. The results appear in the **Security information** section.



4. The Play Integrity API attestation returns the following statuses:
   - If the **PlayIntegrity Device Recognition Verdict** field has **"MEETS_BASIC_INTEGRITY"** , it means that Citrix Secure Hub running on the device at least passes the basic system integrity.
   - If the **PlayIntegrity Device Recognition Verdict** field doesn't have **"MEETS_BASIC_INTEGRITY"** , it means that Citrix Secure Hub on the device might be running on an unrecognized version of Android, might have an unlocked bootloader, or might not have been certified by the manufacturer.
   - If the **PlayIntegrity last known status** is **Success**, it means that the PlayIntegrity API attestation is successfully run.
   - If the **PlayIntegrity last known status** is **Failure**, it means that the PlayIntegrity API attestation has failed to run.

> **Note:**
>
> Admin can clear the feature flag that allows you to use SafetyNet, before the final turndown of SafetyNet Attestation - the end of November 2023.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Limitations

1. Newly enrolled COSU devices and DO devices are marked incompliant, even if the devices are compliant.

   Play Integrity API returns empty for the first attest during DO enrollment, which makes the device seem incompliant. This limitation is a known issue from Google. DPC Support Lib 20230418 is published to fix this issue.

   The fix is available from the 23.9.0 version. Until then use these steps as a workaround:

   - Clear the feature flag, and continue using the SafetyNet API to continue using the SafetyNet Attestation API.
   - Sign off and re-sign in to trigger an attestation after enrollment. You can also wait for the next periodic attest, which is the default of 24 hours.

   This issue only occurs during enrollment. The Play Integrity API works well after enrollment.

2. Newly enrolled WPCOD devices are marked incompliant even when the devices are compliant. Google is reviewing this issue.

Samsung

September 6, 2025

Samsung offers several solutions that are compatible with Citrix Endpoint Management.

To control how and when Android devices connect to the Citrix Endpoint Management service, use Firebase Cloud Messaging (FCM). For information, see Firebase Cloud Messaging.

Enrollment profiles determine whether Android devices enroll in MAM, MDM, or MDM+MAM, with the option for users to opt out of MDM. Citrix Endpoint Management supports the following authentication types for Android devices enrolled in MDM+MAM. For information, see the following articles:

- Domain or domain plus security token authentication
- Client certificate or certificate plus domain authentication
- Identity providers:
  - Authentication with Azure Active Directory through Citrix Cloud
  - Authentication with Okta through Citrix Cloud

Another rarely used authentication method is a client certificate plus security token. For information, see https://support.citrix.com/article/CTX215200.

A general workflow for starting Android device management is as follows:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. Complete the onboarding process. See Onboarding and resource set up and Prepare to enroll devices and deliver resources.
2. Choose and configure an enrollment method. See Supported enrollment methods.
3. Deploy Samsung license keys.
4. Configure Samsung device policies.
5. Set up device and app security actions. See Security actions.

For supported operating systems, see Supported device operating systems.

Supported enrollment methods

The following table lists the enrollment methods that Citrix Endpoint Management supports for Android devices:

Method	Supported
Manual enrollment	Yes
Enrollment invitations	Yes

For information about enrolling devices, see Enroll Android devices.

Deploy Samsung license keys

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

Configure Samsung device policies

Device policies:

App Restrictions	App Uninstall	Passcode
Restrictions	VPN	

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Security actions

Android supports the following security actions. For a description of each security action, see Security actions.

App Lock	App Wipe	Certificate Renewal
Full Wipe	Locate	Lock
Lock and Reset Password	Notify	Revoke
Selective Wipe		

> **Note:**
>
> For devices running Android 6.0 and greater, the **Locate** security action requires the user to grant Location permission during enrollment. The user can opt not to grant Location permissions. If the user doesn't grant the permission during enrollment, Citrix Endpoint Management again requests location permissions when sending the Locate command.

Network Access Control

September 6, 2025

You can use your Network Access Control (NAC) solution to extend the Citrix Endpoint Management device security assessment for Android and Apple devices. Your NAC solution uses the Citrix Endpoint Management security assessment to facilitate and handle authentication decisions. After you configure your NAC appliance, the device policies and NAC filters that you configure in Citrix Endpoint Management get enforced.

Using Citrix Endpoint Management with a NAC solution adds QoS and more granular control over devices that are internal to your network. For a summary of the advantages of integrating NAC with Citrix Endpoint Management, see Access control.

Citrix supports these solutions for integration with Citrix Endpoint Management:

- NetScaler Gateway
- ForeScout

Citrix® doesn't guarantee integration for other NAC solutions.

With a NAC appliance in your network:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Management supports NAC as an endpoint security feature for iOS, Android Enterprise, and Android devices.
- You can enable filters in Citrix Endpoint Management to set devices as compliant or non-compliant for NAC, based on rules or properties. For example:
  - If a managed device in Citrix Endpoint Management doesn't meet the specified criteria, Citrix Endpoint Management marks the device as non-compliant. A NAC appliance blocks non-compliant devices on your network.
  - If a managed device in Citrix Endpoint Management has non-compliant apps installed, a NAC filter can block the VPN connection. As a result, a non-compliant user device cannot access apps or websites through the VPN.
  - If you use NetScaler Gateway for NAC, you can enable split tunneling to prevent the NetScaler Gateway plug-in from sending unnecessary network traffic to NetScaler Gateway. For more information on split tunneling, see Configuring Split Tunneling.

Supported NAC compliance filters

Citrix Endpoint Management supports the following NAC compliance filters:

Anonymous Devices: Checks if a device is in anonymous mode. This check is available if Citrix Endpoint Management can't reauthenticate the user when a device tries to reconnect.

Forbidden Apps: Checks if a device has forbidden apps, as defined in an App Access policy. For more information about that policy, see App access device policies.

Inactive Devices: Checks if a device is inactive as defined by the **Device Inactivity Days Threshold** setting in **Server Properties**. For details, see Server properties.

Missing Required Apps: Checks if a device is missing any required apps, as defined in an App Access policy.

Non-suggested Apps: Checks if a device has non-suggested apps, as defined in an App Access policy.

Noncompliant Password: Checks if the user password is compliant. On iOS and Android devices, Citrix Endpoint Management can determine whether the password currently on the device is compliant with the passcode policy sent to the device. For instance, on iOS, the user has 60 minutes to set a password if Citrix Endpoint Management sends a passcode policy to the device. Before the user sets the password, the passcode might be non-compliant.

Out of Compliance Devices: Checks whether a device is out of compliance, based on the Out of Compliance device property. Typically, automated actions or third parties using Citrix Endpoint Management APIs change that property.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Revoked Status: Checks whether the device certificate is revoked. A revoked device cannot re-enroll until it is authorized again.

Rooted Android and Jailbroken iOS Devices: Checks whether an Android or iOS device is jailbroken.

Unmanaged Devices: Check whether Citrix Endpoint Management is managing a device. For example, a device enrolled in MAM or an unenrolled device is not managed.

> **Note:**
>
> The Implicit Compliant/Not Compliant filter sets the default value only on devices that Citrix Endpoint Management is managing. For example, any devices that have a blocked app installed or are not enrolled, get marked as Not Compliant. The NAC appliance blocks those devices from your network.

Configuration overview

We recommend that you configure the NAC components in the order listed.

1. Configure device policies to support NAC:

   For iOS devices: See Configure the VPN device policy to support NAC.

   For Android Enterprise devices: See Create an Android Enterprise managed configuration for Citrix SSO.

   For Android devices: See Configure the Citrix SSO protocol for Android.

2. Enable NAC filters in Citrix Endpoint Management.
3. Configure a NAC solution:

   - NetScaler Gateway, detailed in Update NetScaler Gateway policies to support NAC.

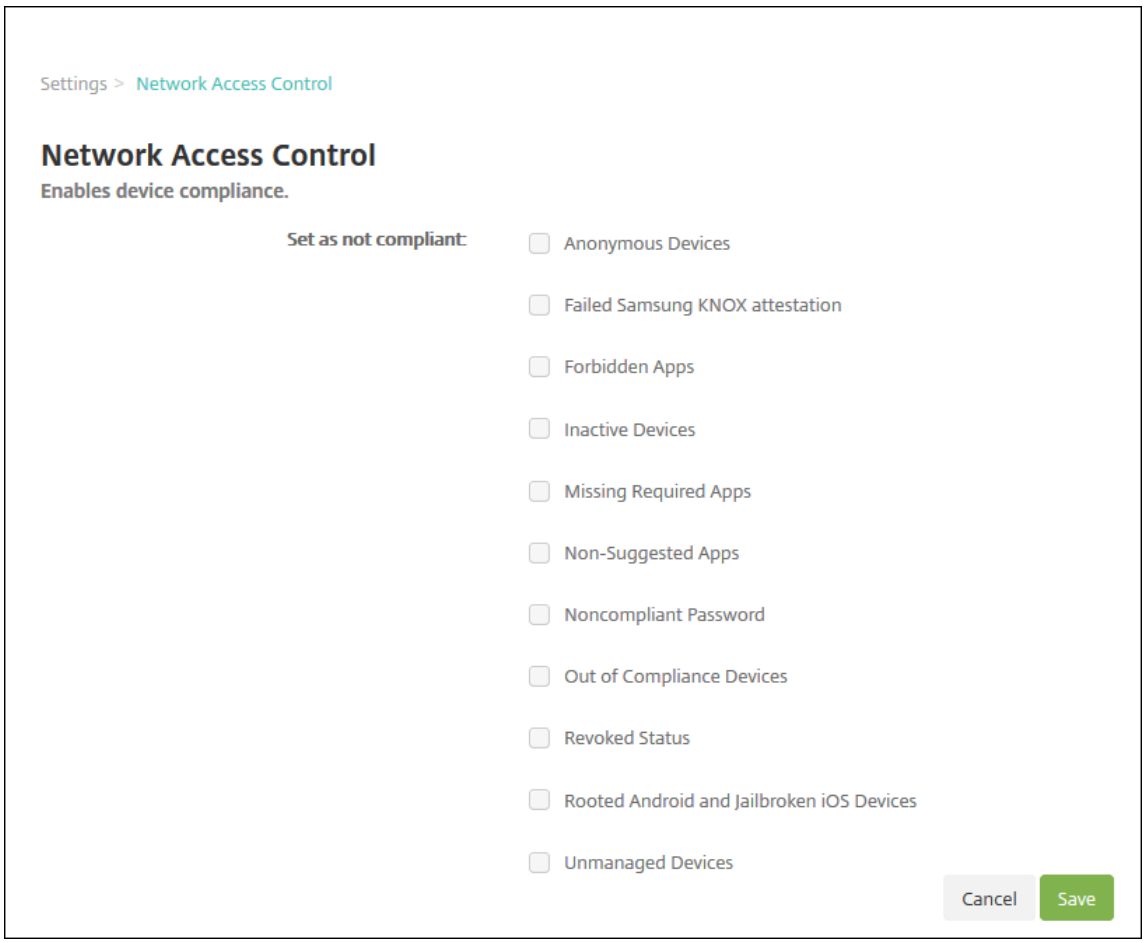
     Requires that you install Citrix SSO on devices. See NetScaler Gateway Clients.

   - ForeScout: See the ForeScout documentation.

Enable NAC filters in Citrix Endpoint Management

1. In the Citrix Endpoint Management console, go to **Settings > Network Access Control**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. Select the checkboxes for the **Set as not compliant** filters you want to enable.
3. Click **Save**.

Update NetScaler Gateway policies to support NAC

You must configure advanced (not classic) authentication and VPN sessions policies on your VPN virtual server.

These steps update a NetScaler Gateway with either of these characteristics:

- Is integrated with Citrix Endpoint Management.
- Or, is set up for VPN, not part of the Citrix Endpoint Management environment, and can reach Citrix Endpoint Management.

On your virtual VPN server from a console window, do the following. The FQDNs and IP addresses in the commands and examples are fictitious.

1. If you are using classic policies on your VPN virtual server, remove and unbind all classic policies. To check, type:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
show vpn vserver <VPN_VServer>
```

Remove any result that has the word **Classic**. For example: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

To remove the policy, type:

```
unbind vpn vserver <VPN_VServer> -policy <policy_name>
```

2. Create the corresponding advanced session policy by typing the following.

   ```
   add vpn sessionPolicy <policy_name> <rule> <session action>
   ```

   For example: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. Bind the policy to your VPN virtual server by typing the following.

   ```
   bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100
   ```

4. Create an authentication virtual server by typing the following.

   ```
   add authentication vserver <authentication vserver name> <service type> <ip address>
   ```

   For example: `add authentication vserver authvs SSL 0.0.0.0`
   In the example, `0.0.0.0` means that the authentication virtual server is not public facing.

5. Bind an SSL certificate with the virtual server by typing the following.

   ```
   bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>
   ```

   For example: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Associate an authentication profile to the authentication virtual server from the VPN virtual server. First, create the authentication profile by typing the following.

   ```
   add authentication authnProfile <profile name> -authnVsName <authentication vserver name>
   ```

   For example:

   ```
   add authentication authnProfile xm_nac_prof -authnVsName authvs
   ```

7. Associate the authentication profile with the VPN virtual server by typing the following.

   ```
   set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
   ```

   For example:

   ```
   set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof
   ```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

8. Check the connection from NetScaler Gateway to a device by typing the following.

   ```
   curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
   ```

   For example, this query verifies connectivity by getting the compliance status for the first device (`deviceid_1`) enrolled in the environment:

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"
   ```

   A successful result is similar to the following example.

   ```
   1 HTTP/1.1 200 OK
   2 < Server: Apache-Coyote/1.1
   3 < X-Citrix-Device-State: Non Compliant
   4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   ```

9. When the preceding step is successful, create the web authentication action to Citrix Endpoint Management. First, create a policy expression to extract the device ID from the iOS VPN plug-in. Type the following.

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. Send the request to Citrix Endpoint Management by typing the following. In this example, the Citrix Endpoint Management IP is `10.207.87.82` and the FQDN is `example.em.cloud.com:4443`.

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort 4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n"+ "Host: example.em.cloud.com:4443\r\n"+ "X-Citrix-VPN-Device-ID: "+ xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ(\"Compliant\")"
    ```

    The successful output for the Citrix Endpoint Management NAC is `HTTP status 200 OK`. The `X-Citrix-Device-State` header must have the value of `Compliant`.

11. Create an authentication policy with which to associate the action by typing the following.

    ```
    add authentication Policy <policy name> -rule <rule> -action <web authentication action>
    ```

    For example: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. Convert the existing LDAP policy to an advanced policy by typing the following.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
add authentication Policy <policy_name> -rule <rule> -action <
LDAP action name>
```

For example: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Add a policy label with which to associate the LDAP policy by typing the following.

```
add authentication policylabel <policy_label_name>
```

For example: `add authentication policylabel ldap_pol_label`

14. Associate the LDAP policy to the policy label by typing the following.

```
bind authentication policylabel ldap_pol_label -policyName
ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
```

15. Connect a compliant device to do a NAC test to confirm successful LDAP authentication. Type the following.

```
bind authentication vserver <authentication vserver> -policy <web
 authentication policy> -priority 100 -nextFactor <ldap policy
label> -gotoPriorityExpression END
```

16. Add the UI to associate with the authentication virtual server. Type the following command to retrieve the device ID.

```
add authentication loginSchemaPolicy <schema policy>-rule <rule>
-action lschema_single_factor_deviceid
```

17. Bind the authentication virtual server by typing the following.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -
priority 100 -gotoPriorityExpression END
```

18. Create an LDAP advanced authentication policy enable the Citrix Secure Hub connection. Type the following.

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER
(\"User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
```

```
bind authentication vserver authvs -policy ldap_xm_test_pol -
priority 110 -gotoPriorityExpression NEXT
```

iOS

September 6, 2025

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To manage iOS devices in Citrix Endpoint Management, you set up an Apple Push Notification service (APNs) certificate from Apple. For information, see APNs certificates.

Enrollment profiles determine whether iOS devices enroll in MDM+MAM, with the option for users to opt out of Mobile Device Management (MDM). Citrix Endpoint Management supports the following authentication types for iOS devices in MDM+MAM. For information, see the following articles:

- Domain or domain plus security token authentication
- Client certificate or certificate plus domain authentication
- Identity providers:
  - Authentication with Azure Active Directory through Citrix Cloud
  - Authentication with Okta through Citrix Cloud

> **Requirements for trusted certificates in iOS 13:**
>
> Apple has new requirements for TLS server certificates. Verify that all certificates follow the new Apple requirements. See the Apple publication, https://support.apple.com/en-us/HT210176. For help with managing certificates, see Upload certificates.

A general workflow for starting iOS device management is as follows:

1. Complete the onboarding process. See Onboarding and resource setup and Prepare to enroll devices and deliver resources.
2. Choose and configure an enrollment method. See Supported enrollment methods.
3. Configure iOS device policies.
4. Enroll iOS devices.
5. Set up device and app security actions. See Security actions.

For supported operating systems, see Supported device operating systems.

iOS 14 compatibility

Citrix Endpoint Management and Citrix mobile apps are compatible with iOS 14 but don't currently support the new iOS 14 features.

For supervised iOS devices, you can postpone software upgrades for up to 90 days. In the restrictions device policy for iOS, use these settings:

- **Force delayed software updates**
- **Enforce software update delay**

See iOS settings. Those settings aren't available for devices in user enrollment mode or unsupervised (full MDM) mode.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Apple host names that must remain open

Some Apple host names must be open to make sure proper operation of iOS, macOS, and Apple App Store. Blocking those host names can affect the installation, update, and proper operation of the following: iOS, iOS apps, MDM operation, and device and app enrollment. For more information, see https://support.apple.com/en-us/HT201999.

Supported enrollment methods

You specify how to manage iOS devices in enrollment profiles. You can choose between the following enrollment settings:

- **Apple User Enrollment:** For BYOD devices, offers a balance of privacy for personal data and security for corporate data. This enrollment mode is available as a public preview. To enable this feature, contact your support team.
- **Apple Device Enrollment:** For supervised iOS devices, with separate personal and corporate profiles on the device.
- **Do not manage devices:** Exclude these devices from MDM if you want to manage apps only.

For more information about creating enrollment profiles, see Enrollment profiles.

Citrix Endpoint Management supports the following enrollment methods for iOS devices:

Method	Supported
Apple Business Manager	Yes
Apple School Manager	Yes
Apple Configurator	Yes
Manual enrollment	Yes
Enrollment invitations	Yes

The Apple Deployment Programs include Apple Business Manager (ABM) for business organizations and Apple School Manager (ASM) for educational organizations. For more information, see Deploy devices through the Apple Deployment Programs.

Apple School Manager is a type of Education Apple Deployment Program. See Integrate with Apple Education features.

Use the Apple Deployment Programs to bulkly enroll iOS, iPadOS, and macOS devices. You can buy those devices directly from Apple, a participating Apple Authorized Reseller, or a carrier. Whether you buy iOS devices directly from Apple, you can use the Apple Configurator to enroll those devices. See Enroll Apple devices in bulk.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Managed Apple IDs

User enrollment tightly integrates with Managed Apple IDs. You can create a Managed Apple ID manually using ABM/ASM or dynamically with Azure Active Directory (AAD).

For non-federated authentication, create Managed Apple IDs using ABM/ASM to add an account. For information about adding an account in ABM/ASM, see Apple documentation at `https://support.apple.com/guide/apple-business-manager/welcome/web` and ASM at `https://support.apple.com/guide/apple-school-manager/welcome/web`. We recommend the following to avoid extra steps when users enroll:

- Use an email matching the corporate email address when creating a Managed Apple ID.
- Set the user role to **Staff**.
- Have users manually change their password before enrolling. Let users know that we recommend they use the same password as the corporate account.

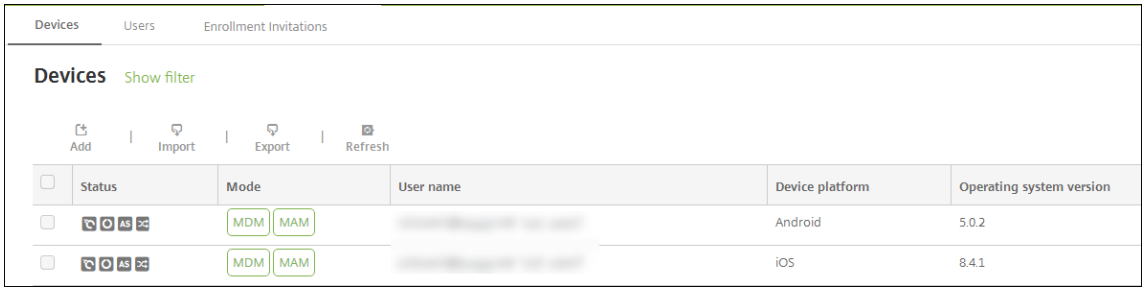
To dynamically create Managed Apple IDs, configure Citrix Cloud to use AAD as its identity provider. For more information about configuring Citrix Cloud to use AAD, see Authentication with Azure Active Directory through Citrix Cloud. Also, configure federated authentication in ABM/ASM. To learn more about configuring federated authentication in ABM or ASM, see the Apple Business Manager User Guide and the Apple School Manager User Guide.

When you manually create Managed Apple IDs, you can configure a custom domain to use in place of the default domain. The custom domain that you configure replaces the existing domain. For example, your corporate email addresses follow the format `first.last@company.com`, but you want to use `mycompany.website.com` as the domain for the Managed Apple ID instead. When creating the Managed Apple ID on ABM/ASM, the email address becomes `first.last@mycompany.website.com`.

Add an iOS device manually

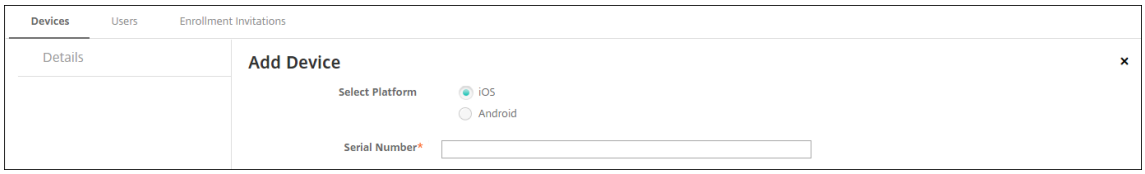
If you want to add an iOS device manually, such as for testing purposes, follow these steps.

1. In the Citrix Endpoint Management console, click **Manage > Devices**. The **Devices** page appears.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Click **Add**. The **Add Device** page appears.



3. Configure these settings:

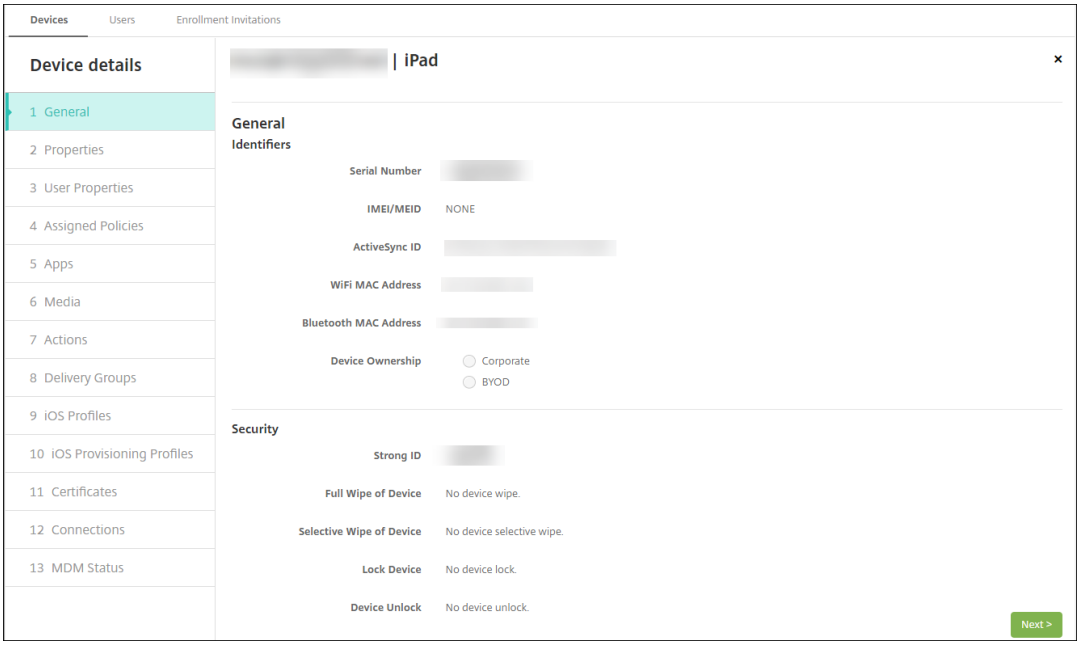
   - **Select platform:** Click **iOS**.
   - **Serial Number:** Type the device serial number.

4. Click **Add**. The **Devices** table appears with the device added to the bottom of the list. To view and confirm the device details: Choose the device that you added and then, in the menu that appears, click **Edit**.

> **Note:**
>
> When you select the checkbox next to a device, the options menu appears above the device list. If you click anywhere else in the list, the options menu appears on the right side of the listing.

   - LDAP configured
   - If using local groups and local users:
     - One or more local groups.
     - Local users assigned to local groups.
     - Delivery groups are associated with local groups.
   - If using Active Directory:
     - Delivery groups are associated with Active Directory groups.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. The **General** page lists the device **Identifiers**, such as the serial number and other information for the platform type. For **Device Ownership**, select **Corporate** or **BYOD**.

   The **General** page also lists device **Security** properties, such as Strong ID, Lock Device, Activation Lock Bypass, and other information for the platform type. The **Full Wipe of Device** field includes the user PIN code. The user must enter that code after the device is wiped. If the user forgets the code, you can look it up here.

6. The **Properties** page lists the device properties that Citrix Endpoint Management provisions. This list shows any device properties included in the provisioning file used to add the device. To add a property, click **Add** and then select a property from the list. For valid values for each property, see the PDF Device property names and values.

   When you add a property, it initially appears under the category where you added it. After you click **Next** and then return to the **Properties** page, the property appears in the appropriate list.

   To delete a property, hover over the listing and then click the **X** on the right side. Citrix Endpoint Management deletes the item immediately.

7. The remaining **Device Details** sections have summaries for the device.

   - **User Properties:** Displays RBAC roles, group memberships, Volume Purchase accounts, and properties for the user. You can retire a Volume Purchase account from this page.
   - **Assigned Policies:** Displays the number of deployed, pending, and failed policies. Provides the policy name, type, and last deployed information for each policy. Lets you reset the deployment status to pending and redeploy policies that the user removed.
   - **Apps:** Displays, for the last inventory, the number of installed, pending, and failed app deployments. Provides the app name, identifier, type, and other information. For a descrip-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

tion of iOS and macOS inventory keys, such as **HasUpdateAvailable**, see Mobile Device Management (MDM) Protocol.

- **Media:** Displays, for the last inventory, the number of deployed, pending, and failed media deployments.
- **Actions:** Displays the number of deployed, pending, and failed actions. Provides the action name and time of the last deployment.
- **Delivery Groups:** Displays the number of successful, pending, and failed delivery groups. For each deployment, provides the delivery group name and deployment time. Select a delivery group to view more detailed information, including status, action, and channel or user.
- **iOS Profiles:** Displays the last iOS profile inventory, including name, type, organization, and description.
- **iOS Provisioning Profiles:** Displays enterprise distribution provisioning profile information, such as the UUID, expiration date, and managed status.
- **Certificates:** Displays, for valid, expired, or revoked certificates, information such as the type, provider, issuer, serial number, and the number of remaining days before expiration.
- **Connections:** Displays the first connection status and the last connection status. Provides for each connection, the user name, penultimate (next to last) authentication time, and last authentication time.
- **MDM Status:** Displays information such as the MDM status, last push time, and last device reply time.

Configure iOS device policies

Use these policies to configure how Citrix Endpoint Management interacts with devices running iOS or iPadOS. This table lists all device policies available for iOS and iPadOS devices.

AirPlay mirroring	AirPrint	APN
App access	App attributes	App configuration
App inventory	App lock	App uninstall
Apps notifications	Bluetooth	Calendar (CalDAV)
Cellular	Contacts (CardDAV)	Credentials
Device name	Education configuration	Exchange
Font	Home screen layout	Import iOS & macOS profile

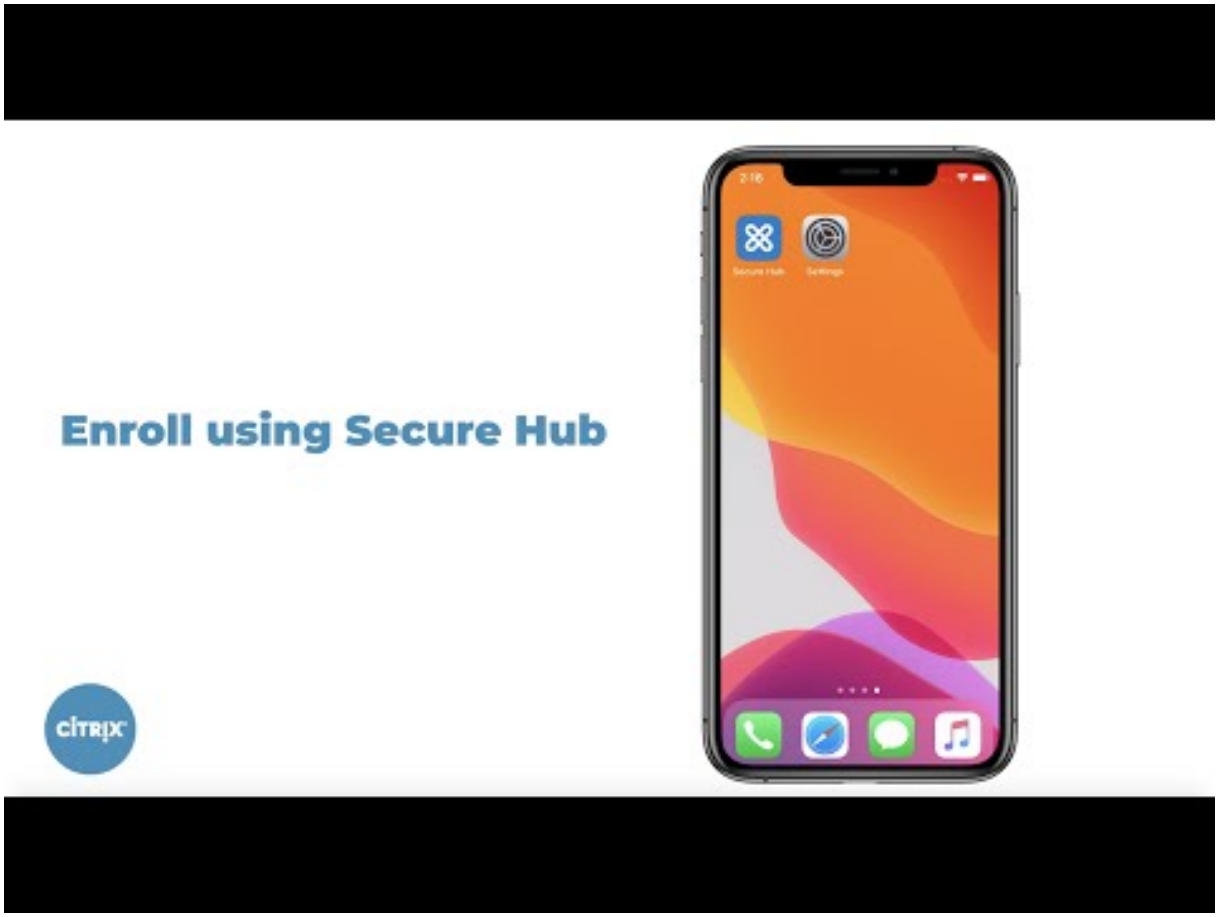
© 1997–2025 Citrix Systems, Inc. All rights reserved.

LDAP	Location	Lock screen message
Mail	Managed domains	Maximum resident users
MDM options	Network	Network usage
Organization info	OS update	Passcode
Passcode lock grace period	Personal hotspot	Profile removal
Provisioning profile	Provisioning profile removal	Proxy
Restrictions	Roaming	SCEP
SSO account	Store	Subscribed calendars
Terms and conditions	VPN	Wallpaper
Web content filter	Web clip	

Enroll iOS devices

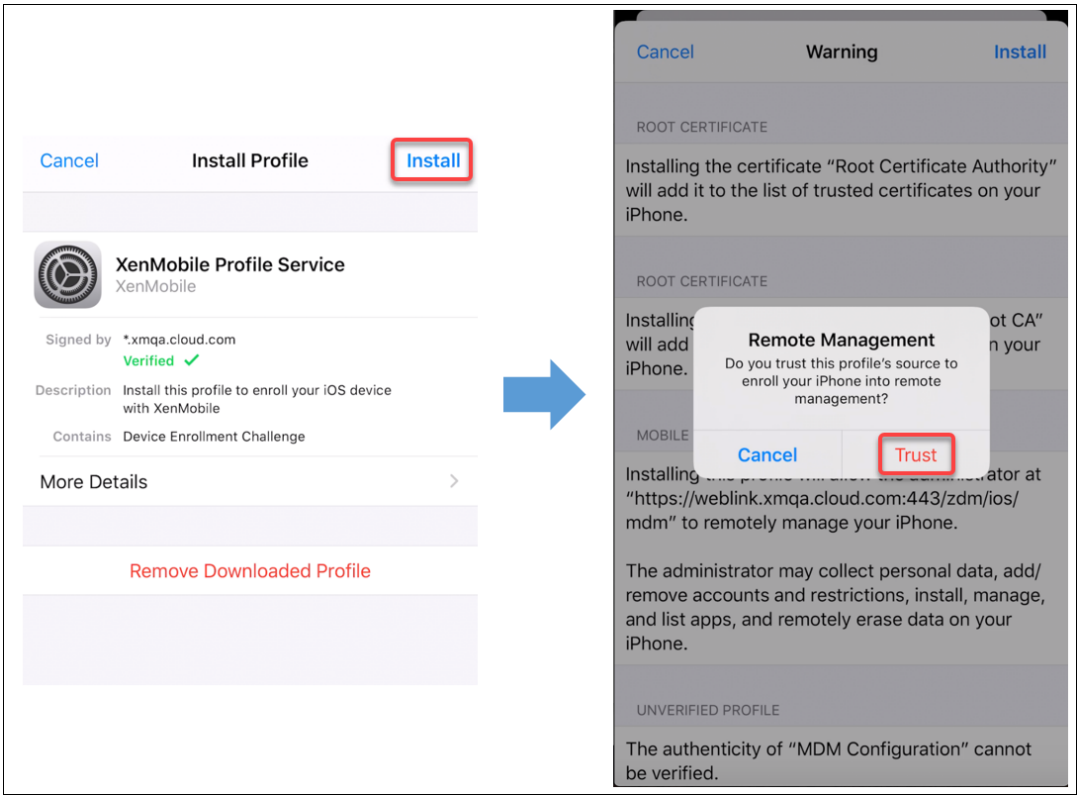
This section shows how users enroll iOS devices (12.2 or later) into Citrix Endpoint Management. For more information about the iOS enrollment, watch the following video:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



1. Go to the Apple store on your iOS device, download the Citrix Secure Hub app, and then tap the app.
2. When prompted to install the app, tap **Next** and then tap **Install**.
3. After Citrix Secure Hub installs, tap **Open**.
4. Enter your corporate credentials, such as your Citrix Endpoint Management server name, User Principal Name (UPN), or email address. Then, click **Next**.
5. Tap **Yes, Enroll** to enroll your iOS device.
6. A list of the data Citrix Endpoint Management collects appears. Click **Next**. An explanation of how an organization uses that data appears. Click **Next**.
7. After you type your credentials, tap **Allow** when prompted, to download the configuration profile. After you download the configuration profile, tap **Close**.
8. In your device settings, install the XenMobile® profile.
    - Go to **Settings > General > Profile > XenMobile Profile Service** and tap **Install** to add the profile.
    - In the notification window, tap **Trust** to enroll your device into remote management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



9. Once enrollment succeeds, open Citrix Secure Hub. If you're enrolling into MDM+MAM: After your credentials validate, create and confirm your Citrix PIN when prompted.
10. After the workflow completes, the device is enrolled. You can then access the app store to view the apps you can install on your iOS device.

Security actions

Device enrollment for iOS supports the following security actions. For a description of each security action, see Security actions.

- Activation Lock Bypass
- App Lock
- App Wipe
- ASM Activation Lock
- Certificate Renewal
- Clear Restrictions
- Enable/Disable Lost Mode
- Enable/Disable Tracking
- Full Wipe
- Locate
- Lock

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Ring
- Request/Stop AirPlay Mirroring
- Restart/Shut Down
- Revoke/Authorize
- Selective Wipe
- Unlock

User enrollment for iOS supports the following security actions:

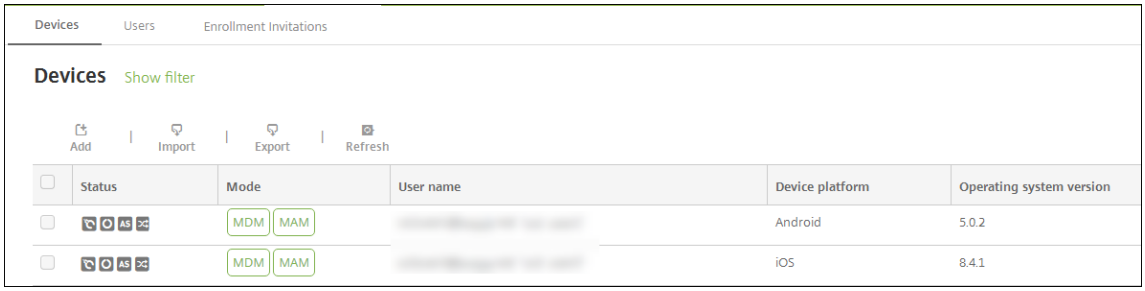
- Revoke
- Lock
- Selective wipe
- Certificate renewal

Lock iOS devices

You can lock a lost iOS device with an accompanying display of a message and phone number that displays on the device lock screen.

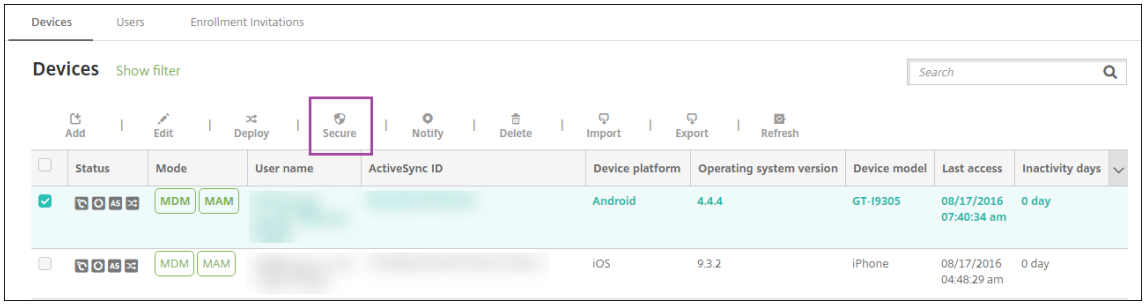
To display a message and phone number on a locked device, set the Passcode policy to **true** in the Citrix Endpoint Management console. Instead users can enable the passcode on the device manually.

1. Click **Manage > Devices**. The **Devices** page appears.

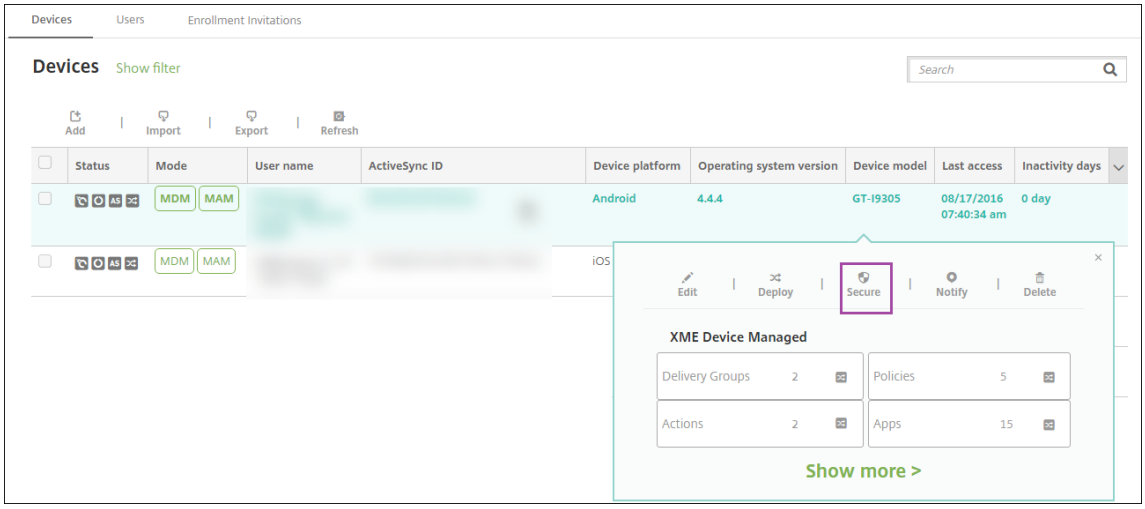


2. Select the iOS device that you want to lock.

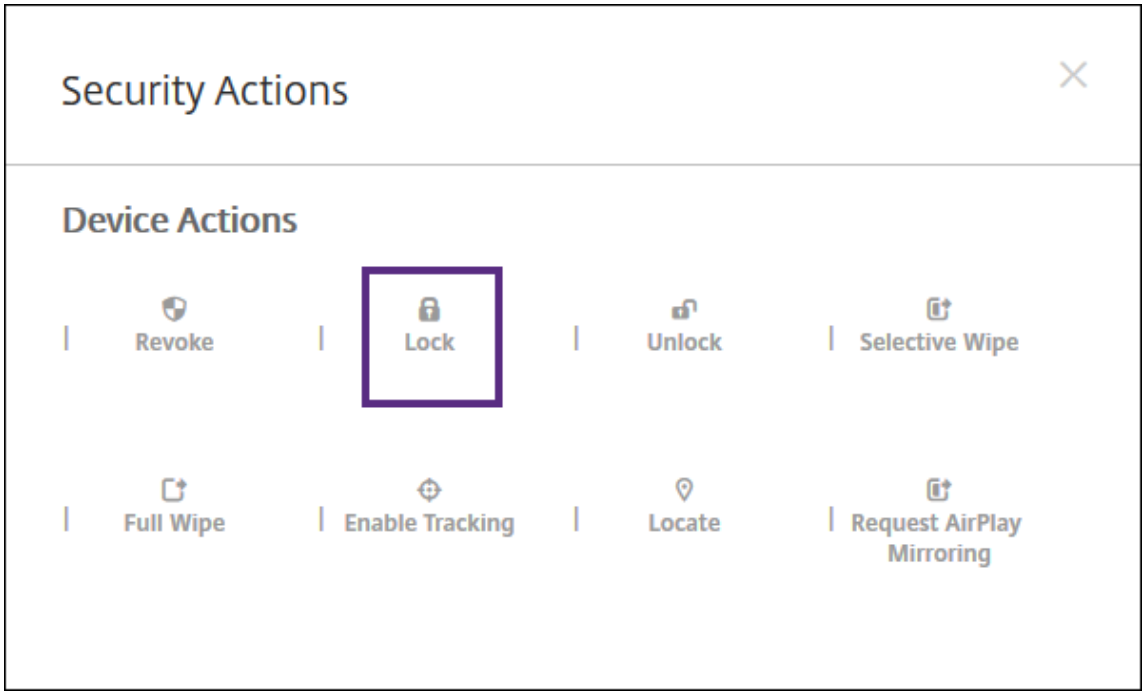
   Select the checkbox next to a device to show the options menu above the device list. Click anywhere else in the list to show the options menu on the right side of the listing.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

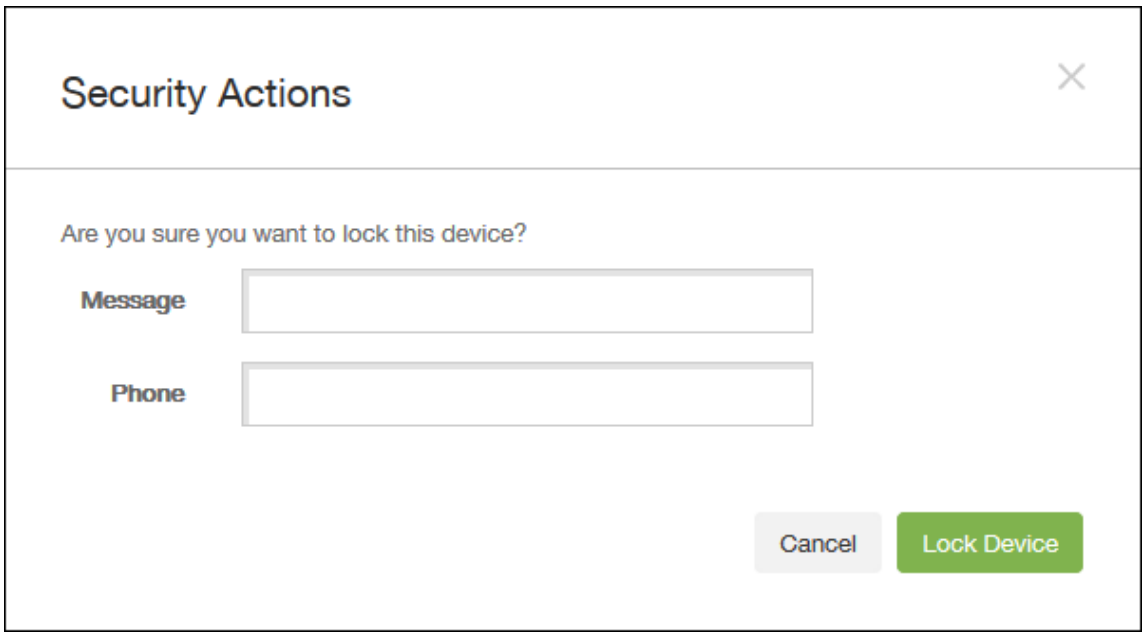


3. In the options menu, click **Secure**. The **Security Actions** dialog box appears.



4. Click **Lock**. The **Security Actions** confirmation dialog box displays.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. Optionally, type a message and phone number that appears on the lock screen of the device.

   iOS appends the words "Lost iPad" to what you type in the **Message** field.

   If you leave the **Message** field empty and provide a phone number, Apple displays the message "Call owner" on the device lock screen.

6. Click **Lock Device**.

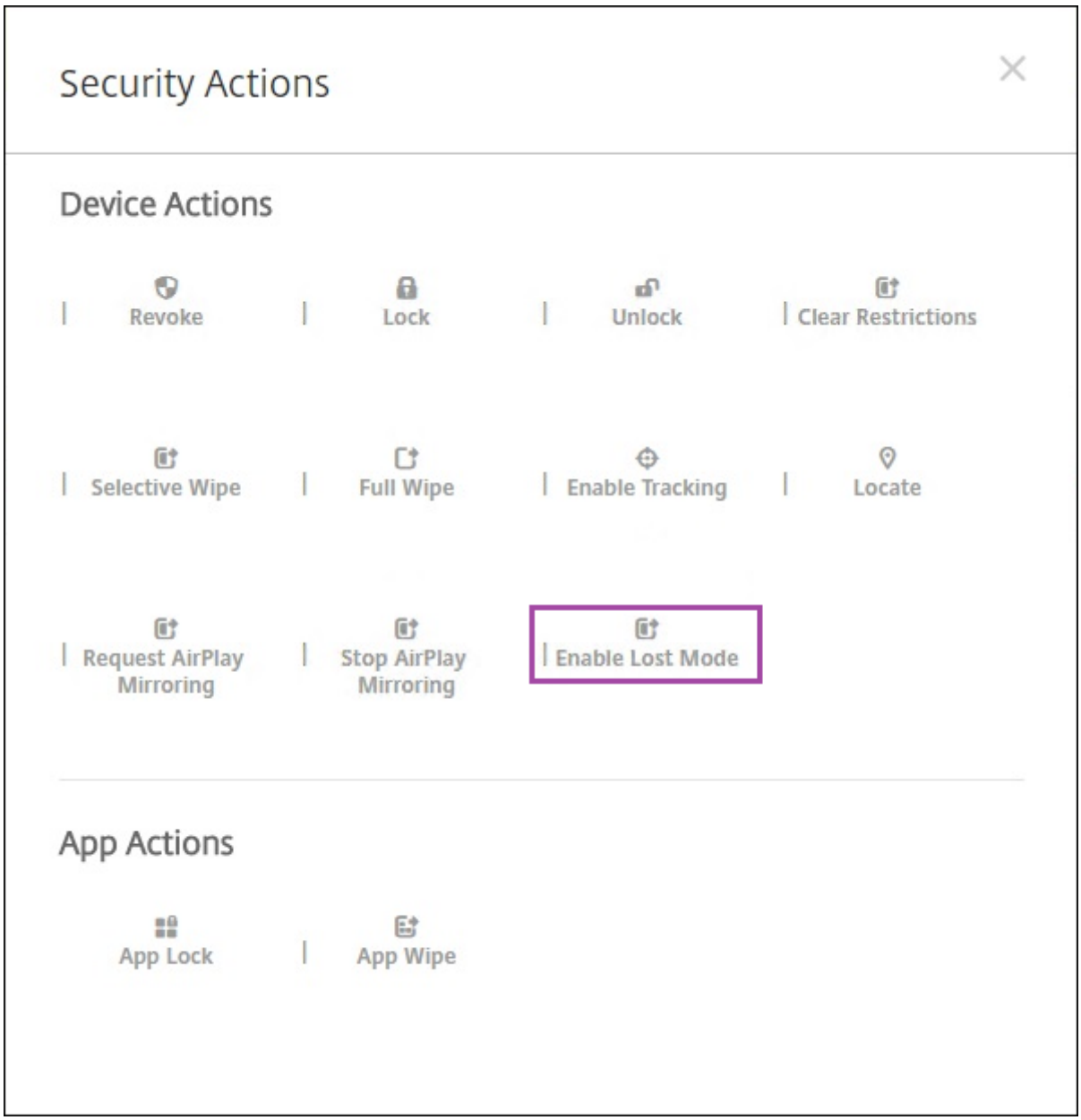
Put iOS devices in Lost Mode

The Citrix Endpoint Management Lost Mode device property puts an iOS device in Lost Mode. Unlike Apple Managed Lost Mode, Citrix Endpoint Management Lost Mode doesn't require a user to do either of the following actions to enable locating their device: Configure the **Find My iPhone/iPad** setting or enable the Location Services for Citrix Secure Hub.

In Citrix Endpoint Management Lost Mode, only Citrix Endpoint Management can unlock the device. (In contrast, if you use the Citrix Endpoint Management device lock feature, users can unlock the device directly by using a PIN code that you provide.

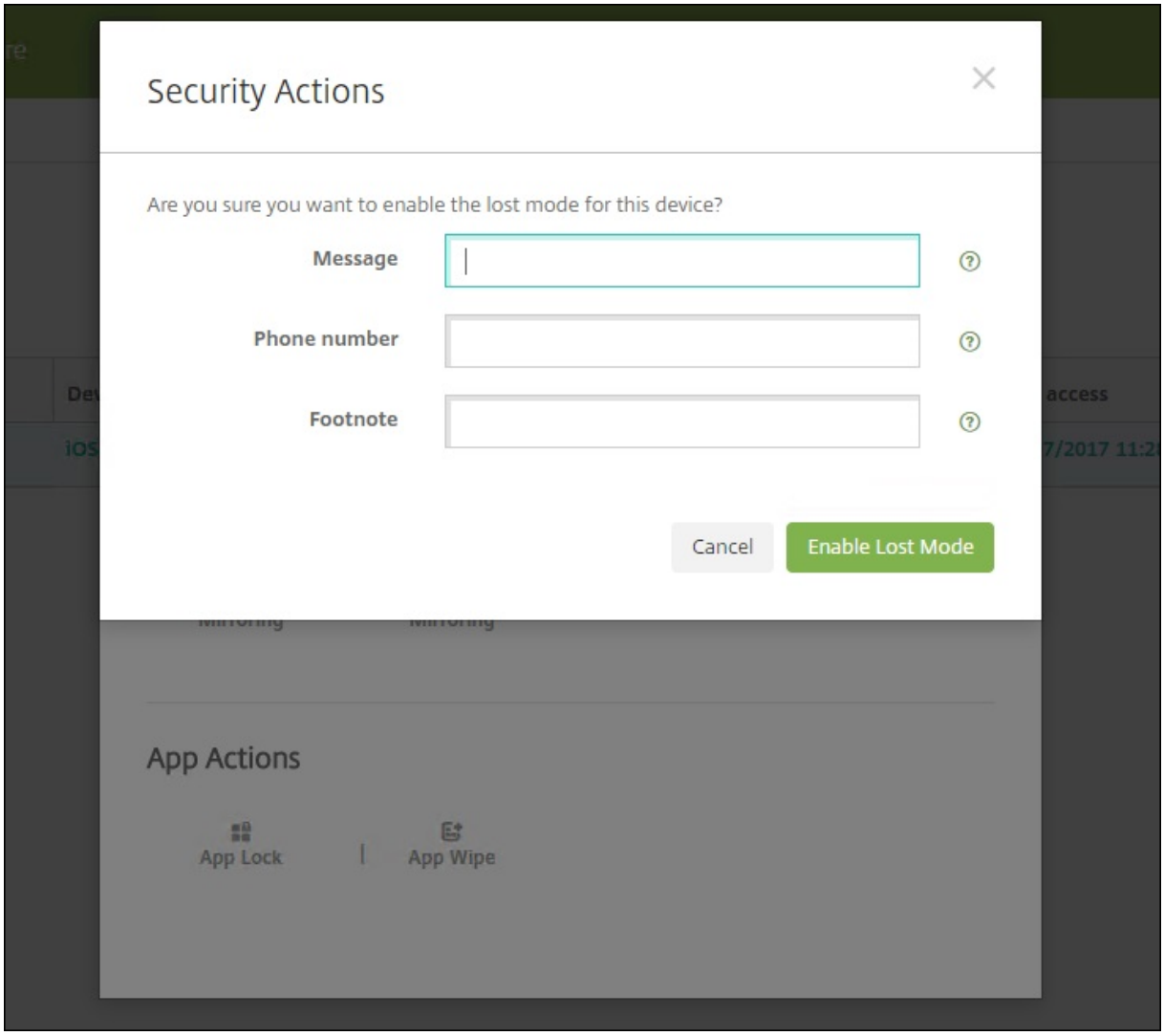
To enable or disable lost mode: Go to **Manage > Devices**, choose a supervised iOS device, and then click **Secure**. Then, click **Enable Lost Mode** or **Disable Lost Mode**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



If you click **Enable Lost Mode**, type information to appear on the device when it's in lost mode.

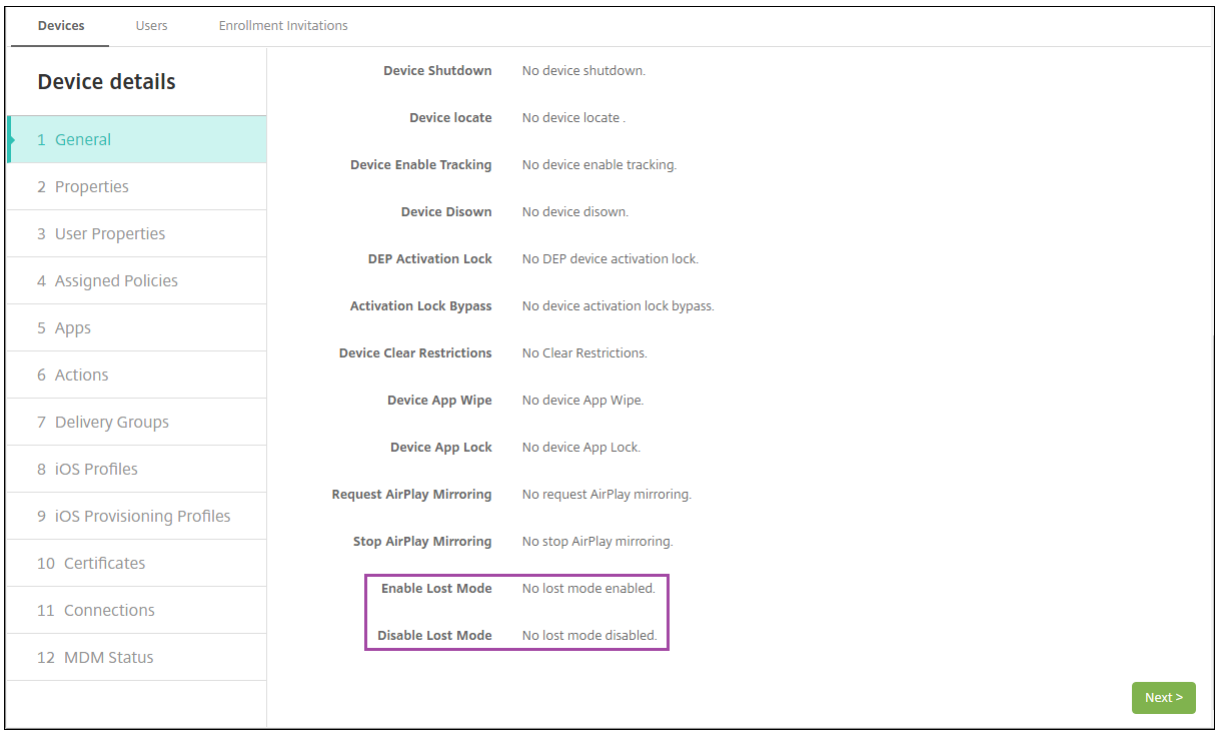
© 1997–2025 Citrix Systems, Inc. All rights reserved.



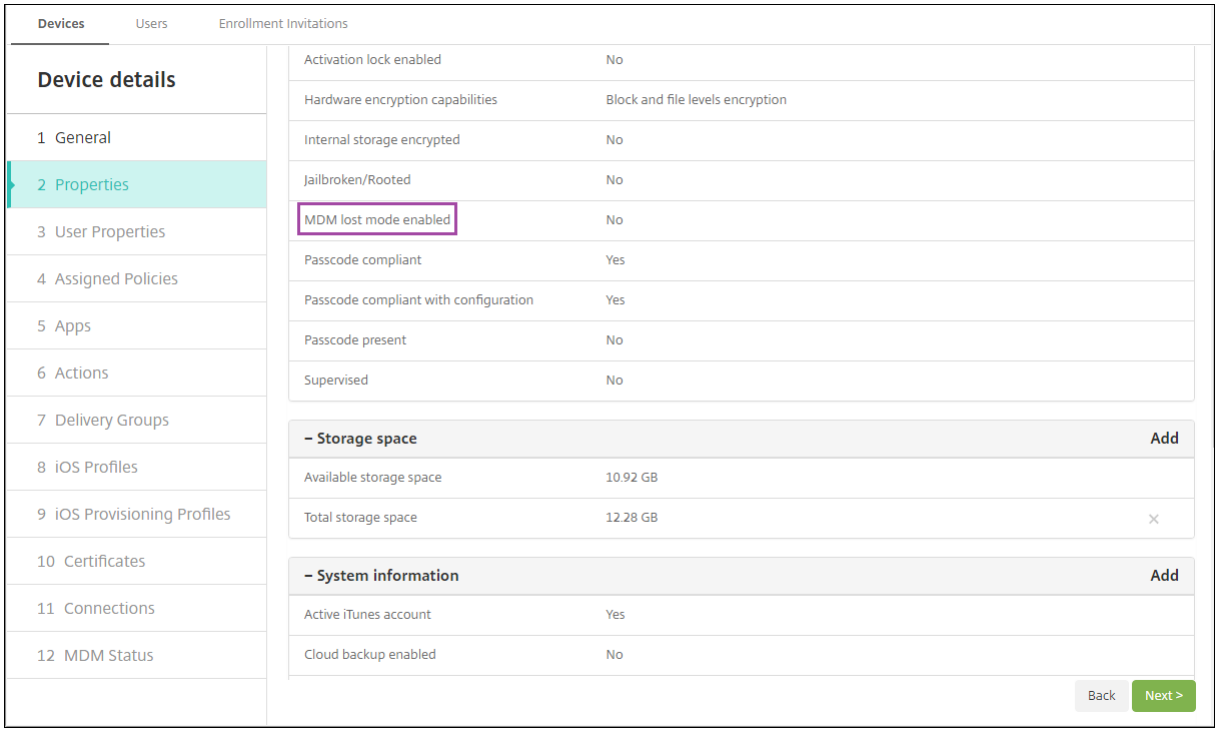
Use any of the following methods to check Lost Mode status:

- In the **Security Actions** window, verify if the button is set as **Disable Lost Mode**.
- From **Manage > Devices**, on the **General** tab under **Security**, see the last Enable Lost Mode or Disable Lost Mode action.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- From **Manage > Devices**, on the **Properties** tab, verify that the value of the **MDM lost mode enabled** setting is correct.



If you enable Citrix Endpoint Management Lost Mode on an iOS device, the Citrix Endpoint Management console also changes as follows:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- In **Configure > Actions**, the **Actions** list doesn't include these automated actions: **Revoke the device**, **Selectively wipe the device**, and **Completely wipe the device**.
- In **Manage > Devices**, the **Security Actions** list no longer includes the **Revoke** and **Selective Wipe** device actions. You can still use a security action to do a **Full Wipe** action, as needed.

iOS appends the words "Lost iPad"to what you type in the **Message** in the **Security Actions** screen.

If you leave the **Message** empty and provide a phone number, Apple shows the message "Call owner" on the device lock screen.

Bypass an iOS activation lock

Activation Lock is a feature of Find My iPhone/iPad that prevents reactivation of a lost or stolen supervised device. Activation Lock requires the user Apple ID and password before anyone can do these actions: Turn off Find My iPhone/iPad, erase the device, or reactivate the device. For the devices that your organization owns, bypassing an Activation Lock is necessary to, for example, reset or reallocate devices.

To enable Activation Lock, you configure and deploy the Citrix Endpoint Management MDM Options device policy. You can then manage a device from the Citrix Endpoint Management console without the Apple credentials of the user. To bypass the Apple credential requirement of an Activation Lock, issue the Activation Lock Bypass security action from the Citrix Endpoint Management console.

For example, if the user returns a lost phone or to set up the device before or after a Full Wipe: When the phone prompts for the Apple App Store account credential, bypass that step by issuing the Activation Lock Bypass security action.

Device requirements for activation lock bypass

- Supervised through Apple Configurator or Apple Deployment Program
- Configured with an iCloud account
- Find My iPhone/iPad enabled
- Enrolled in Citrix Endpoint Management
- MDM Options device policy, with activation lock enabled, is deployed to devices

To bypass an activation lock before issuing a Full Wipe of a device:

1. Go to **Manage > Devices**, select the device, click **Secure**, and then click **Activation Lock Bypass**.
2. Wipe the device. The activation lock screen doesn't appear during device setup.

To bypass an activation lock after issuing a Full Wipe of a device:

1. Reset or wipe the device. The activation lock screen appears during device setup.
2. Go to **Manage > Devices**, select the device, click **Secure**, and then click **Activation Lock Bypass**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. Tap the Back button on the device. The home screen appears.

Keep in mind the following:

- Advise your users not to turn off Find My iPhone/iPad. Don't do a full wipe from the device. In either of those cases, the user is prompted to enter the iCloud account password. After account validation, the user won't see an Activate iPhone/iPad screen after erasing all content and settings.
- For a device that has a generated Activation lock bypass code and has the Activation lock enabled: If you can't bypass the Activate iPhone/iPad page after a Full Wipe, you don't need to delete the device from Citrix Endpoint Management. Either you or the user can contact Apple support to unblock the device directly.
- During a hardware inventory, Citrix Endpoint Management queries a device for an Activation lock bypass code. If a bypass code is available, the device sends it to Citrix Endpoint Management. Then, to remove the bypass code from the device, send the Activation Lock Bypass security action from the Citrix Endpoint Management console. At that point, Citrix Endpoint Management and Apple have the bypass code required to unblock the device.
- The Activation Lock Bypass security action relies on the availability of an Apple service. If the action doesn't work, you can unblock a device using one of the following ways:
  - On the device, manually enter the credentials of the iCloud account.
  - Leave the user name field empty and type the bypass code in the password field. To look up the bypass code, go to **Manage > Devices**, select the device, click **Edit**, and click **Properties**. The **Activation lock bypass code** is under **Security information**.

macOS

March 4, 2024

To manage macOS devices in Citrix Endpoint Management, you set up an Apple Push Notification service (APNs) certificate from Apple. For information, see APNs certificates.

Citrix Endpoint Management enrolls macOS devices into MDM. Citrix Endpoint Management supports the following enrollment authentication types for macOS devices in MDM.

- Domain
- Domain plus one-time password
- Invitation URL plus one-time password

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Requirements for trusted certificates in macOS 15:**
>
> Apple has new requirements for TLS server certificates. Verify that all certificates follow the new Apple requirements. See the Apple publication, https://support.apple.com/en-us/HT210176. For help with managing certificates, see Upload certificates.

A general workflow for starting macOS device management is as follows:

1. Complete the onboarding process. See Onboarding and resource setup and Prepare to enroll devices and deliver resources.
2. Choose and configure an enrollment method. See Supported enrollment methods.
3. Configure macOS device policies.
4. Enroll macOS devices.
5. Set up device and app security actions. See Security actions.

For supported operating systems, see Supported device operating systems.

Apple host names that must remain open

Some Apple host names must be open to make sure proper operation of iOS, macOS, and Apple App Store. Blocking those host names can affect the installation, update, and proper operation of the following: iOS, iOS apps, MDM operation, and device and app enrollment. For more information, see https://support.apple.com/en-us/HT201999.

Supported enrollment methods

The following table lists the enrollment methods that Citrix Endpoint Management supports for macOS devices:

Method	Supported
Apple Deployment Program	Yes
Apple School Manager	Yes
Apple Configurator	No
Manual enrollment	Yes
Enrollment invitations	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Apple has device enrollment programs for business and education accounts. For business accounts, you enroll in the Apple Deployment Program to use the Apple Deployment Program for device enrollment and management in Citrix Endpoint Management. That program is for iOS, macOS, and Apple TV devices. See Deploy devices through Apple Deployment Program.

For education accounts, you create an Apple School Manager account. Apple School Manager unifies the Deployment Program and Volume Purchase. Apple School Manager is a type of Education Apple Deployment Program. See Integrate with Apple Education features.

You can use the Apple Deployment Program to bulkly enroll iOS, macOS, and Apple TV devices. You can buy those devices directly from Apple, a participating Apple Authorized Reseller, or a carrier.

Configure macOS device policies

Use these policies to configure how Citrix Endpoint Management interacts with devices running macOS. This table lists all device policies available for macOS devices.

AirPlay mirroring	App inventory	App uninstall
Calendar (CalDAV)	Contacts (CardDAV)	Credentials
Device name	Exchange	FileVault
Firewall	Font	Import iOS & macOS profile
LDAP	Mail	Network
OS update	Passcode	Profile removal
Restrictions	SCEP	VPN
Web clip		

Enroll macOS devices

Citrix Endpoint Management provides two methods to enroll devices that are running macOS. Both methods enable macOS users to enroll over the air, directly from their devices.

- **Send users an enrollment invitation:** This enrollment method enables you to set any of the following enrollment security modes for macOS devices:
  - User name + password
  - User name + PIN
  - Two-factor authentication

© 1997–2025 Citrix Systems, Inc. All rights reserved.

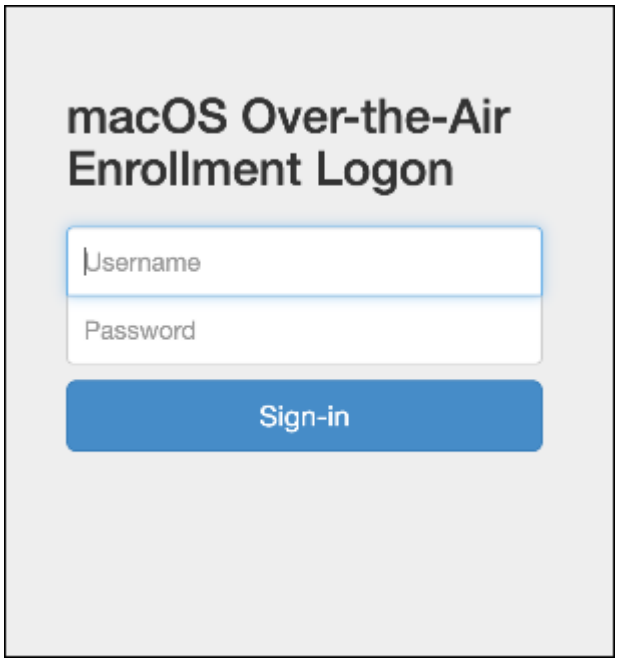
When the user follows the instructions in the enrollment invitation, a sign-on screen with the user name filled in appears.

- **Send users an enrollment link:** This enrollment method for macOS devices sends users an enrollment link, which they can open in Safari or Chrome browsers. A user then enrolls by providing their user name and password.

  To prevent the use of an enrollment link for macOS devices, set the server property **Enable macOS OTAE** to **false**. As a result, macOS users can enroll only by using an enrollment invitation.

Send macOS users an enrollment invitation

1. Add an invitation for macOS user enrollment. See Enrollment invitations.
2. After users receive the invitation and click the link, the following screen appears in the Safari browser. Citrix Endpoint Management fills in the user name. If you chose **Two Factor** for the enrollment security mode, another field appears.



3. Users install certificates as necessary. Whether users see the prompt to install certificates depends on whether you configured the following for macOS: A publicly trusted SSL certificate and a publicly trusted digital signing certificate. For information about certificates, see Certificates and authentication.
4. Users provide the requested credentials.

   The Mac device policies install. You can now start managing macOS devices with Citrix Endpoint Management just as you manage mobile devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Send macOS users an installation link

1. Send the enrollment link `https://serverFQDN:8443/instanceName/macos/otae`, which users can open in Safari or Chrome browsers.

   - **serverFQDN** is the fully qualified domain name (FQDN) of the server running Citrix Endpoint Management.
   - Port **8443** is the default secure port. If you configured a different port, use that port instead of 8443.
   - The **instanceName**, often shown as `zdm`, is the name specified during server installation.

   For more information about sending installation links, see To send an installation link.

2. Users install certificates as necessary. If you configured a publicly trusted SSL certificate and digital signing certificate for iOS and macOS, users see the prompt to install the certificates. For information about certificates, see Certificates and authentication.

3. Users sign on to their Macs.

   The Mac device policies install. You can now start managing macOS devices with Citrix Endpoint Management just as you manage mobile devices.

Security actions

macOS supports the following security actions. For a description of each security action, see Security actions.

Revoke	Lock	Selective Wipe
Full Wipe	Certificate renewal	Rotate personal recovery key

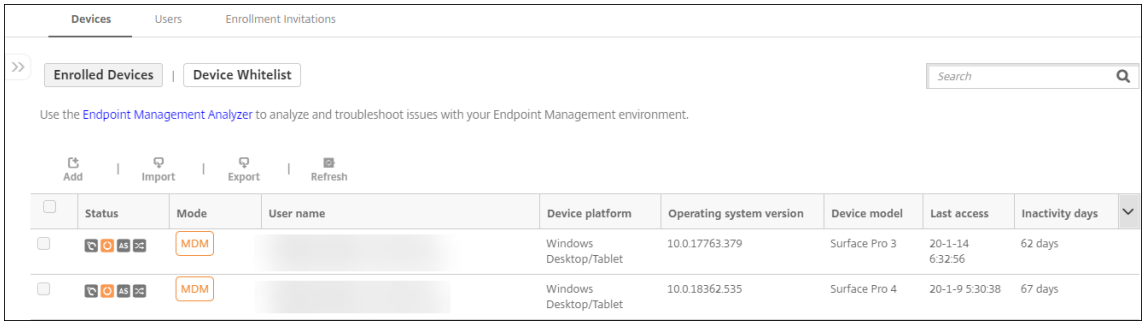
Lock macOS devices

You can remotely lock a lost macOS device. Citrix Endpoint Management locks the device. It then generates a PIN code and sets it in the device. To access the device, the user types the PIN code. Use **Cancel Lock** to remove the lock from the Citrix Endpoint Management console.

You can use the Passcode device policy to configure more settings associated with the PIN code. For more information, see macOS settings.

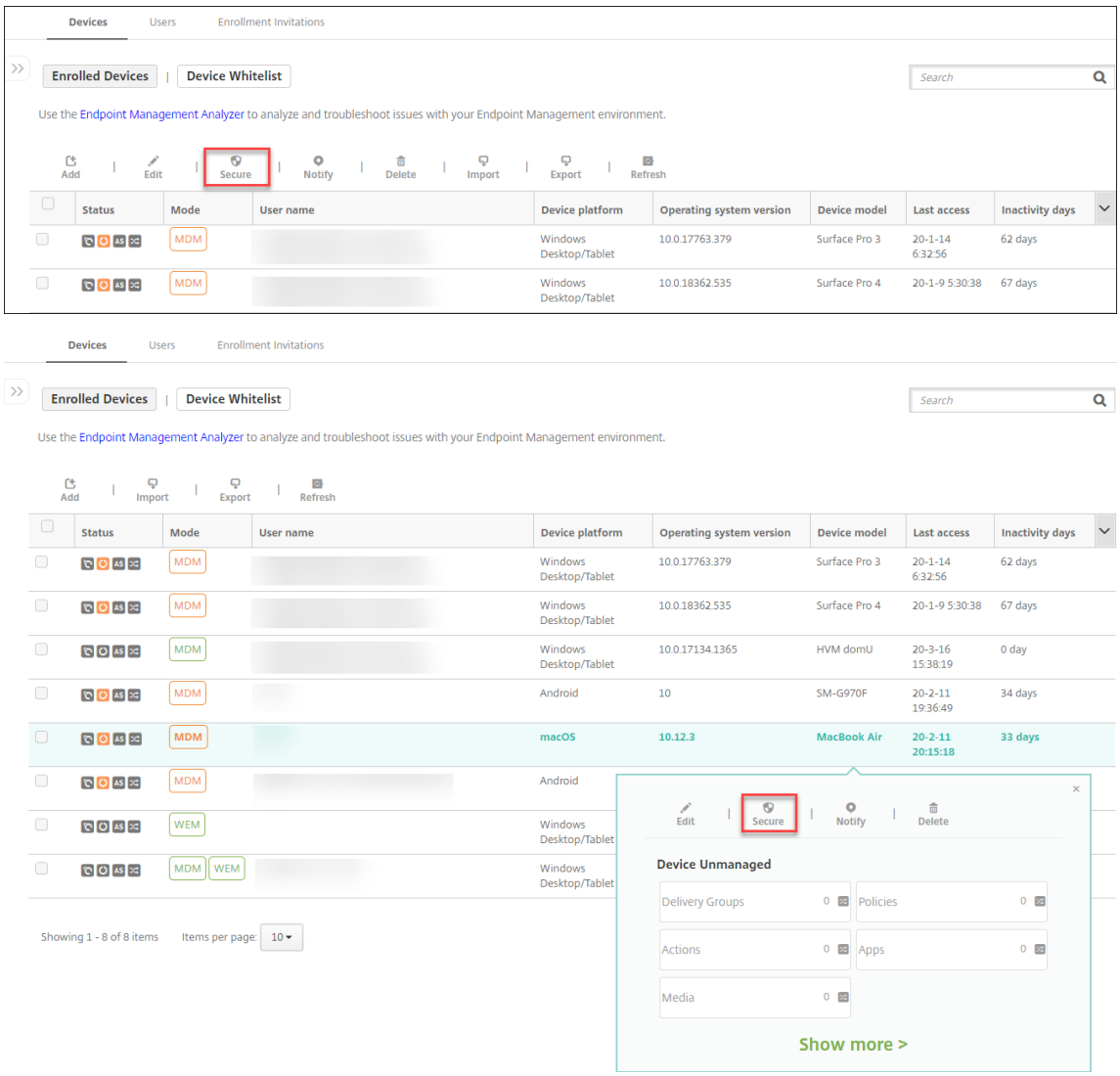
1. Click **Manage > Devices**. The **Devices** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. Select the macOS device that you want to lock.

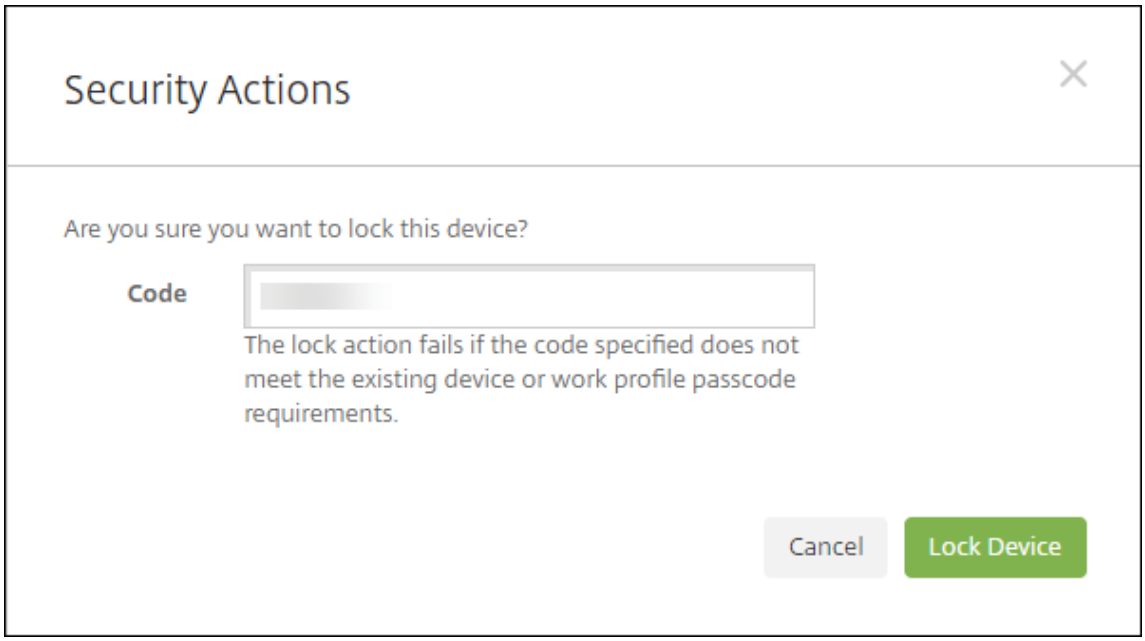
   Select the checkbox next to a device to show the options menu above the device list. You can also click anywhere else on a listed item to show the options menu on the right side of the list.



3. In the options menu, click **Secure**. The **Security Actions** dialog box appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. Click **Lock**. The **Security Actions** confirmation dialog box displays.



5. Click **Lock Device**.

> **Important:**
>
> You can also specify a passcode instead of using the code that Citrix Endpoint Management generates. The lock action fails if the code specified does not meet the code requirements of the device or existing work profile.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Bootstrap token

A bootstrap token assists with granting the SecureToken macOS attribute to accounts when you sign on to a macOS device. SecureToken passes down from one trusted account to another. SecureToken-enabled accounts can do cryptographic operations on the device. Without the bootstrap token, you need to follow complex workflows to create accounts on that device before adding individual user accounts.

Citrix Endpoint Management supports escrowing bootstrap tokens for macOS devices that are enrolled through the Apple Deployment Program. You use the Apple Deployment Program to enroll macOS devices that you buy directly from Apple, a participating Apple Authorized Reseller, or a carrier. For information about enrolling in the Apple Deployment Program, see Deploy devices through Apple Deployment Program.

Bootstrap tokens are generated during the Setup Assistant workflow. Specifically, they are generated during local user account creation. The Setup Assistant runs the first time users start their devices. The tokens are saved in the Citrix Endpoint Management database and not visible to you and end users. Deleting the devices from your Citrix Endpoint Management site deletes the tokens. Doing a factory reset doesn't delete them.

Prerequisites:

- macOS 11.0 or later
- macOS devices that have the Apple T2 Security Chip
- macOS devices enrolled through Apple Deployment Program

One benefit of escrowing bootstrap tokens with Citrix Endpoint Management is that remote accounts can be enabled for FileVault and able to unlock the FileVault volume. For information about FileVault, see FileVault device policy.

Deploy devices through the Apple Deployment Programs

September 5, 2025

The Apple Deployment Programs (ADPs) let you automatically enroll Apple devices in Citrix Endpoint Management without having to touch or prepare the devices before users get them. After a user unboxes and activates the device, the device automatically enrolls in Citrix Endpoint Management, and all management settings, apps, and books are ready for the user.

The ADPs include Apple Business Manager (ABM) for business organizations and Apple School Manager (ASM) for educational organizations. ABM and ASM are available for iOS, iPadOS, and macOS

© 1997–2025 Citrix Systems, Inc. All rights reserved.

devices. For more information about device eligibility, see Apple Business Manager User Guide and Apple School Manager User Guide.

> **Note:**
>
> ABM and ASM combine the previous Device Enroll Program and Volume Purchase Program from Apple.

This article walks you through the general deployment workflow with ABM or ASM:

1. Enroll in ABM or ASM
2. Connect your ABM or ASM account to Citrix Endpoint Management
3. Order devices
4. Assign devices to Citrix Endpoint Management
5. Buy content in volume and synchronize it with Citrix Endpoint Management
6. Configure deployment rules for device policies and apps
7. Add delivery groups that have users and resources assigned to them

After you complete this deployment process, the devices are ready to be unboxed and activated for an automated device enrollment.

Prerequisites

Open required ports for connectivity between Citrix Endpoint Management and Apple. For more information, see Port requirements.

Enroll in ABM or ASM

To begin deploying devices at Apple, enroll in ABM or ASM.

ABM and ASM are available for organizations and not individuals. You must provide many organization details and information to create an account. It might take time to request and receive approval for accounts.

Enroll in ABM

To enroll in ABM, go to business.apple.com. Click **Enroll now** to apply for a new account.

Best practice is to use an email address for your organization, such as `deployment@company.com`. The enrollment process might take a few days. After you receive your logon credentials, follow the steps provided in ABM to create an account.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Enroll in ASM

To create your ASM account, go to Apple School Manager and follow the instructions to enroll. The first time that you log in to ASM, the Setup Assistant opens.

- For information about ASM prerequisites, the Setup Assistant, and management tasks, see the Apple School Manager User Guide.
- When setting up an ASM user account, use a domain name that differs from the domain name for Active Directory. For example, prefix the domain name for ASM with something like `appleid`.
- When you connect ASM to your roster data, ASM creates Managed Apple IDs for instructors and students. Your roster data includes instructors, students, and classes. For information about adding roster data to ASM, see the Apple School Manager User Guide, linked earlier in this list.
- You can customize the Managed Apple ID format for your institution, as described in the Apple School Manager User Guide, linked earlier in this list.

  > **Important:**
  >
  > Don't change Managed Apple IDs after you import ASM information into Citrix Endpoint Management.

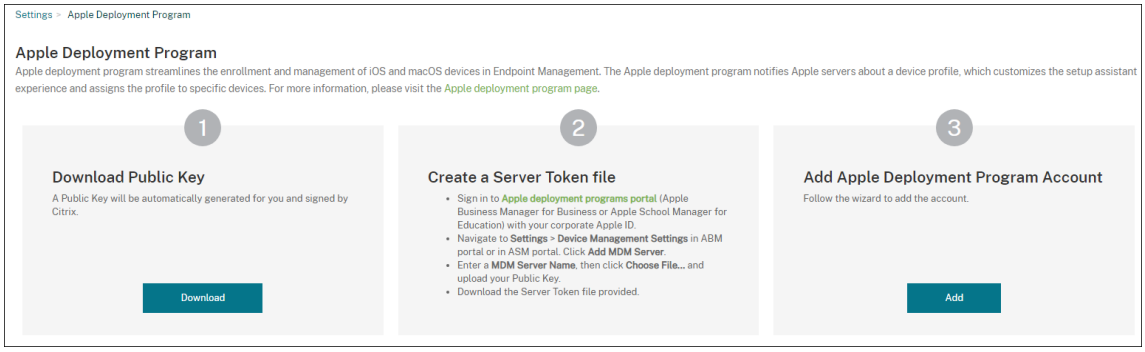
- If you bought devices through resellers or carriers, link those devices to ASM. For information, see the Apple School Manager User Guide, linked earlier in this list.

Connect your ABM or ASM account to Citrix Endpoint Management

After you create your ABM or ASM account, connect it with your Citrix Endpoint Management server deployment.

Step 1: Download a public key from your Citrix Endpoint Management server

1. In the Citrix Endpoint Management console, go to **Settings > Apple Deployment Programs**.



2. Under **Download Public Key**, click **Download**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Step 2: Create and download a server token file from your Apple account

1. Sign in to Apple Business Manager or Apple School Manager using an administrator or device enrollment manager account.
2. At the bottom of the sidebar, click **Settings** and then click **Device Management Settings > Add MDM Server**.
3. In the **MDM Server Name** setting, type a name for the Citrix Endpoint Management server. The server name that you type is for your reference. It's not the server URL or name.
4. Under **Upload Public Key**, click **Choose File**. Upload the public key that you downloaded from Citrix Endpoint Management and then save the changes.
5. Click **Download Token** to download the server token file to your computer.

   You upload the server token file when adding the ABM or ASM account to Citrix Endpoint Management. Your token information appears in the Citrix Endpoint Management console after you import the token file.
6. Under **Default Device Assignment**, click **Change**. Choose how you want to assign devices and then provide the information requested. For more information, see the ABM User Guide or Apple School Manager User Guide.

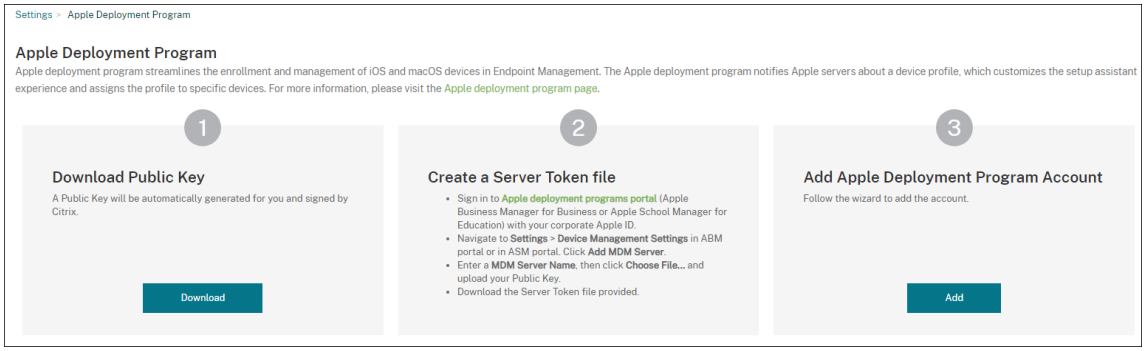
Step 3: Add your account to Citrix Endpoint Management

You can add multiple ABM or ASM accounts to Citrix Endpoint Management. This feature enables you to use different enrollment settings and setup assistant options by country, department, and so on. You then associate ABM or ASM accounts with different device policies.

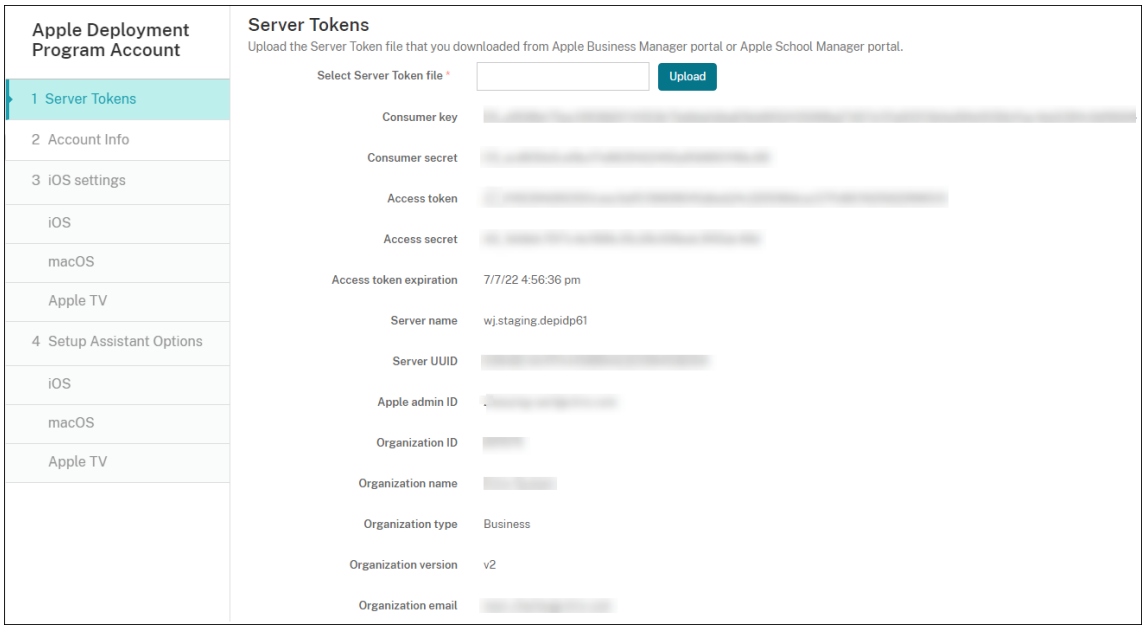
For example, you might centralize all of your ABM or ASM accounts from different countries on the same Citrix Endpoint Management server to import and supervise all ABM or ASM devices. You first customize enrollment settings and setup assistant options per department, organizational hierarchy, or other structure. You then configure policies to provide appropriate functionality across your organization and let users receive the appropriate assistance.

1. In the Citrix Endpoint Management console, go to **Settings > Apple Deployment Program** and, under **Add Apple Deployment Program Account**, click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



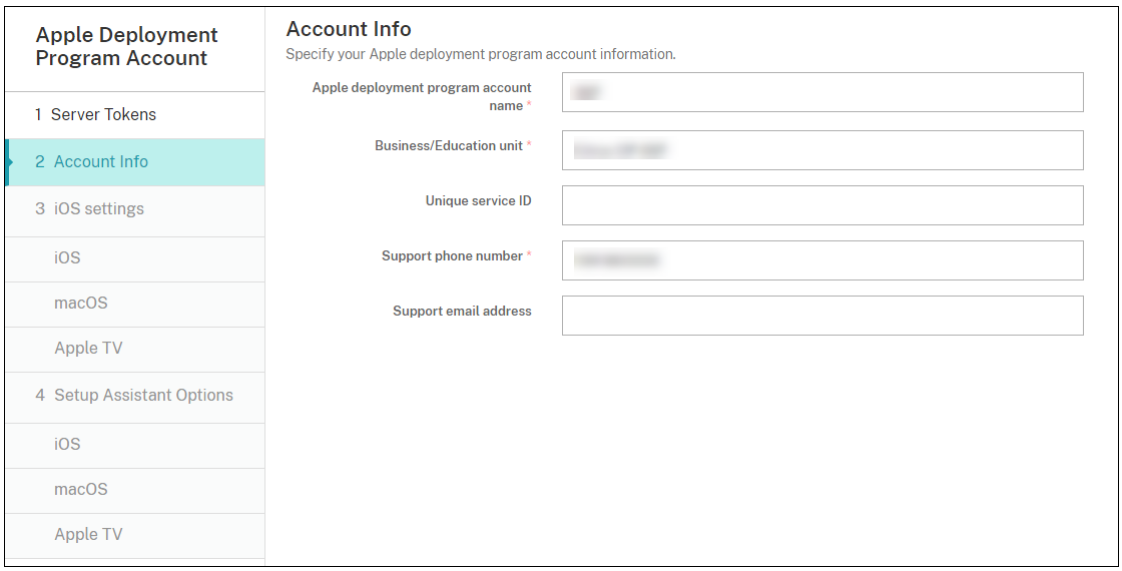
2. In the **Server Tokens** page, specify your server token file and then click **Upload**.



Your server token information appears.

3. In the **Account Info** page, specify these settings:

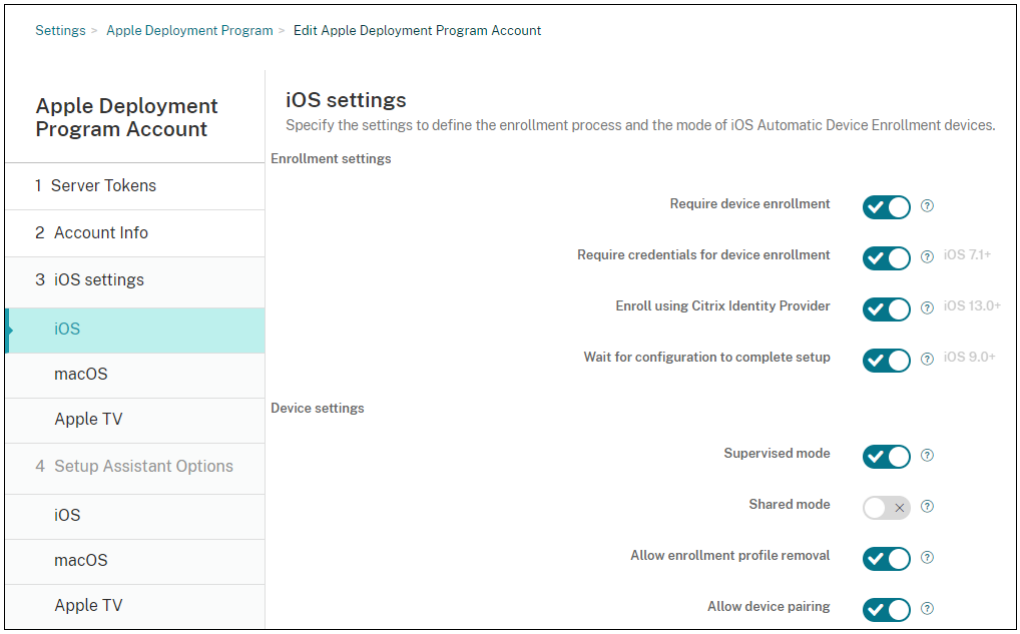
© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Apple Deployment Program account name:** A unique descriptive name for this ADP account, identifying how you organize ADP accounts, such as by country or organizational hierarchy.
- **Business/Education unit:** The business unit or department to which the device is assigned. This field is required.
- **Unique service ID:** An optional unique ID to help you further identify the account.
- **Support phone number:** A support phone number that users call for help during setup. This field is required.
- **Support email address:** An optional support email address available to end users.
- **Education suffix:** For ASM accounts. Type the suffix assigned to devices enrolled through this account.

4. In **iOS Settings**, specify these settings:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Enrollment settings:

- **Require device enrollment:** Whether to require users to enroll their devices. The default is **On**.
- **Require credentials for device enrollment:** Whether to require users to enter their credentials during ABM and ASM setup. We recommend that you require all users to enter their credentials during device enrollment, allowing only authorized users to enroll devices. The default is **On**.

  When you enable ABM or ASM before first-time setup and you don't select this option, Citrix Endpoint Management creates the ABM or ASM components. This creation includes components such as user, Citrix Secure Hub, software inventory, and deployment group. If you select this option, Citrix Endpoint Management doesn't create the components. As a result, if you later clear this option, users who haven't entered their credentials can't enroll in ABM or ASM because these components don't exist. To add ABM or ASM components, in that case, disable and then enable the ABM or ASM account.
- **Enroll using Citrix Identity Provider:** Whether to enroll using Citrix Identity Provider. This setting is available only to ABM accounts. If **On**, ADP-enabled iOS devices enroll only by using the Citrix identity provider. The default is **Off**.

  To turn on the setting, you must first configure Citrix Identity Provider as your identity provider. Go to **Settings > Identity Provider (IDP)**, click **Add**, and select **Citrix Identity Provider**.

  If this setting is set as **On**, be aware of the following considerations:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

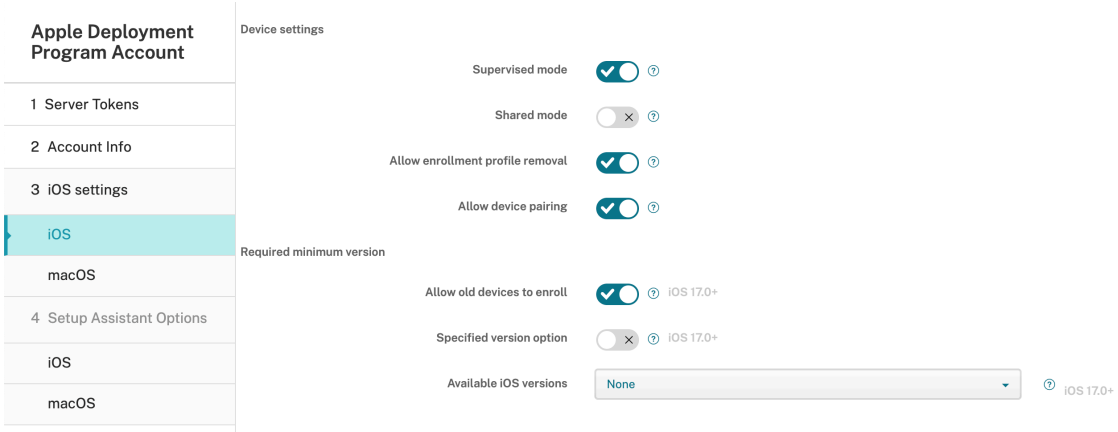
  - You can't delete the corresponding Citrix Identity Provider configuration on the **Settings > Identity Provider (IDP)** page.
  - When editing the corresponding Citrix Identity Provider configuration, you can't switch to a different identity provider.

- **Wait for configuration to complete setup:** Whether to require users'devices to be in Setup Assistant mode until all MDM resources deploy to the device. This setting is available for devices in supervised mode. The default is **Off**.
- Apple documentation states that the following commands might not work while a device is in Setup Assistant mode:
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

Device settings:

- **Supervised mode:** Set to **On** if you're using the Apple Configurator to manage enrolled devices or when **Wait for configuration to complete setup** is enabled. The default is **On**. For details on placing an iOS device in supervised mode, see Deploy devices using Apple Configurator 2.
- **Allow enrollment profile removal:** Whether to allow devices to use a profile that you can remove remotely. The default is **Off**.
- **Allow device pairing:** Whether you can manage enrolled devices through Apple Music and the Apple Configurator. The default is **Off**.

Required minimum Version



- **Allow old devices to enroll:** If enabled, devices can enroll even if they could not upgrade

© 1997–2025 Citrix Systems, Inc. All rights reserved.

to the current required minimum version. The default is On. This option is available only on iOS 17.0 and later.

- **Specified version option:** Whether to allow admin to input specified version manually. The default is **Off**. This option is available only on iOS 17.0 and later.
- **Available iOS versions:** You can choose available iOS versions from the list. If the device has an iOS version lower than the current version, it will kick off update process on device. If the version expires in the future, a minimum version of the available version list is used. The default is None, it will not take effect when set as None. This option is available only on iOS 17.0 and later.
- **Specified version:** If the device has an iOS version lower than the current version, it will kick off update process on device. If the version expires in the future, a minimum version of the available version list is used. Enter the correct version number, otherwise unknown errors may occur.

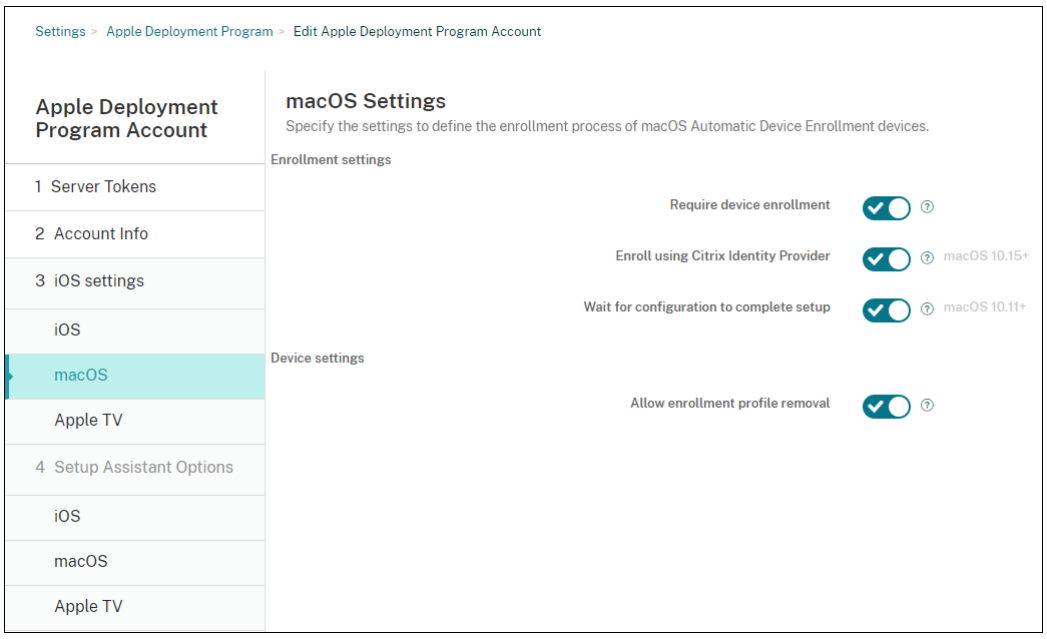
Supervision Identities

If you use the GroundControl tool, you can add a certificate to do the following:

- Override pairing restrictions to avoid the "Trust this host"prompt.
- Escalate managed device actions over USB to do activities such as profile installation without user interaction. Doing so allows GroundControl to enable single app mode and device lock for checkout.
- Restore a backup to ABM or ASM devices.

For more information on GroundControl, see The GroundControl website.

5. In **macOS Settings**, specify these settings:



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Enrollment settings:

- **Require device enrollment:** Whether to require users to enroll their devices. The default is **On**.
- **Enroll using Citrix Identity Provider:** Whether to enroll using Citrix Identity Provider. This setting is available only to ABM accounts. If **On**, ADP-enabled macOS devices enroll only by using the Citrix identity provider. The default is **Off**.

  To turn on the setting, you must first configure Citrix Identity Provider as your identity provider. Go to **Settings > Identity Provider (IDP)**, click **Add**, and select **Citrix Identity Provider**.

  If this setting is set as **On**, be aware of the following considerations:

  - You can't delete the corresponding Citrix Identity Provider configuration on the **Settings > Identity Provider (IDP)** page.
  - When editing the corresponding Citrix Identity Provider configuration, you can't switch to a different identity provider.
- **Wait for configuration to complete setup:** If **On**, the macOS device doesn't continue in the setup assistant until the MDM resource passcode gets deployed to the device. That deployment occurs before the creation of the local account. This setting is available for macOS 10.11 and higher devices. The default is **Off**.

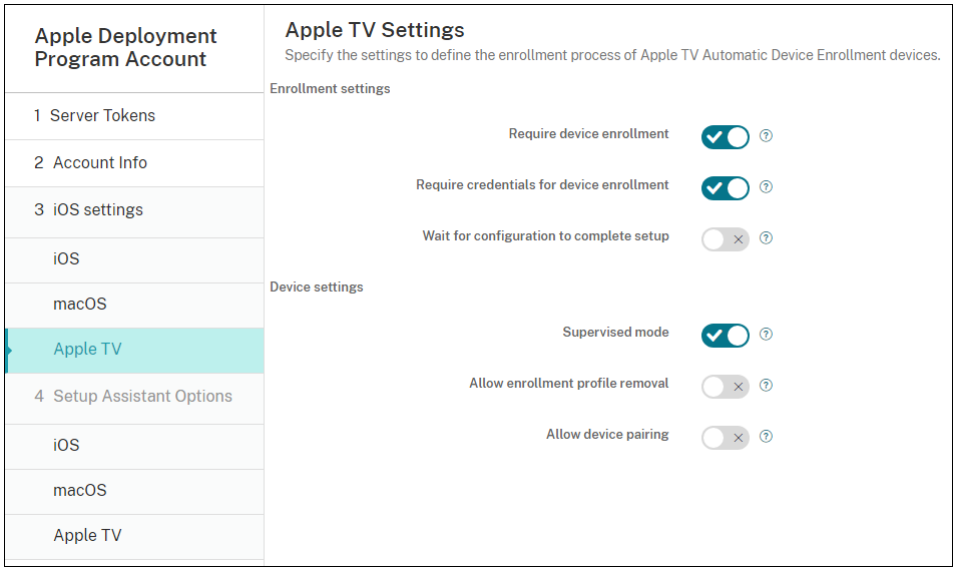
Device settings:

- **Allow enrollment profile removal:** Whether to allow devices to use a profile that you can remove remotely. The default is **Off**.

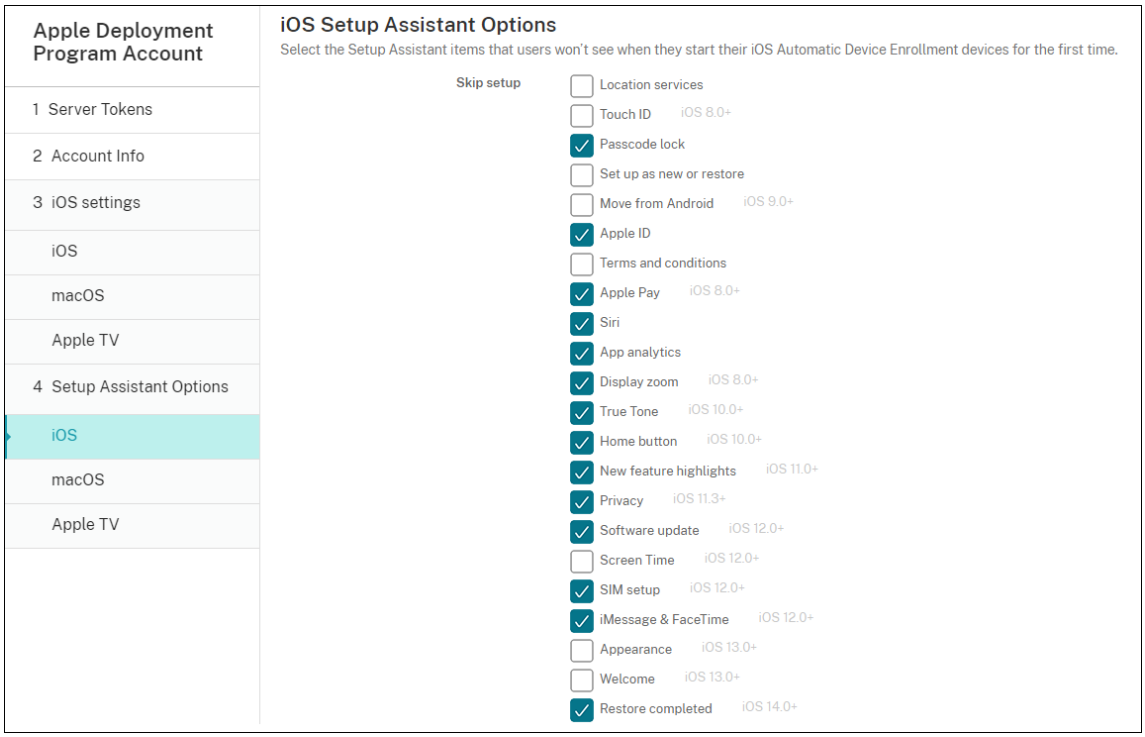
6. In **Apple TV Settings**, specify these settings:

   - **Require device enrollment:** Prevents users from skipping enrollment.
   - **Require Credentials for device enrollment:** Challenges for credentials during enrollment. When this setting is off, Apple TV gets enrolled as the default "Device Enrollment Program user".
   - **Wait for configuration to complete setup:** The device waits in the **Setup Assistant** screen until all resources deploy.
   - **Supervised mode:** Gives more capability to the administrator while configuring restrictions.
   - **Allow enrollment profile removal:** Allows users to remove the enrollment profiles.
   - **Allow device pairing:** Allows devices enrolled through the Device Enrollment Program to be managed through Apple tools, such as the Apple App Store and the Apple Configurator.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



7. In **iOS Setup Assistant Options**, select the steps that the iOS Setup Assistant skips when users start their devices the first time. When a screen is skipped, the related feature uses default settings. Users can configure the skipped features after setup completes unless you restrict access to those features completely. For more information about restricting access to features, see Restrictions device policy. The default for all items is cleared. The following descriptions explain what occurs when a setting is selected.



- **Location services:** Prevents users from setting up the location service on the device.
- **Touch ID:** Prevents users from setting up Touch ID or Face ID on iOS devices. Deprecated

© 1997–2025 Citrix Systems, Inc. All rights reserved.

in iOS 15.

- **Passcode lock:** Prevents users from setting up a passcode for the device. If no passcode exists, users can't use Touch ID or Apple Pay.
- **Set up as new or restore:** Prevents users from setting up the device as new or from an iCloud or Apple App Store backup.
- **Move from Android:** Prevents users from transferring data from an Android device to an iOS device. This option is available only when **Set up as new or restore** is selected (that is, the step is skipped).
- **Apple ID:** Prevents users from setting up a Managed Apple ID account for the device.
- **Terms and conditions:** Prevents users from reading and accepting terms and conditions for use of the device.
- **Apple Pay:** Prevents users from setting up Apple Pay. If this setting is cleared, users must set up Touch ID and Apple ID. Make sure that those settings are cleared.
- **Siri:** Prevents the user from configuring Siri.
- **App analytics:** Prevents users from setting up whether to share crash data and usage statistics with Apple.
- **Display zoom:** Prevents users from setting up the display resolution (either standard or zoomed) on iOS devices. Deprecated in iOS 17.
- **True Tone:** Prevents users from setting up four-channel sensors to dynamically adjust the white balance of the display.
- **Home button:** Prevents users from setting up the Home button style of feedback. Deprecated in iOS 15.
- **New feature highlights:** Prevents users from seeing screens that display information about new features of Apple software.
- **Privacy:** Prevent users from seeing the data and privacy pane. For iOS 11.3 and later.
- **Software update:** Prevents users from updating iOS to the latest version. For iOS 12.0 and later.
- **Screen Time:** Prevents users from enabling Screen Time. For iOS 12.0 and later.
- **SIM setup:** Prevents users from setting up a cellular plan. For iOS 12.0 and later.
- **iMessage & FaceTime:** Prevents users from enabling iMessage and FaceTime. For iOS 12.0 and later.
- **Appearance:** Prevents users from selecting the appearance mode. For iOS 13.0 and later.
- **Welcome:** Prevents the user from seeing the **Get Started** screen. For iOS 13.0 and later.
- **Restore completed:** Prevents users from seeing whether a restore completes during setup. For iOS 14.0 and later.
- **Update completed:** Prevents users from seeing whether a software update completes during setup. For iOS 14.0 and later.
- **App Store:** Prevents users from setting up the App Store. For iOS 11.1 and later.
- **Action Button:** Prevents users from seeing the Action Button configuration pane. For iOS

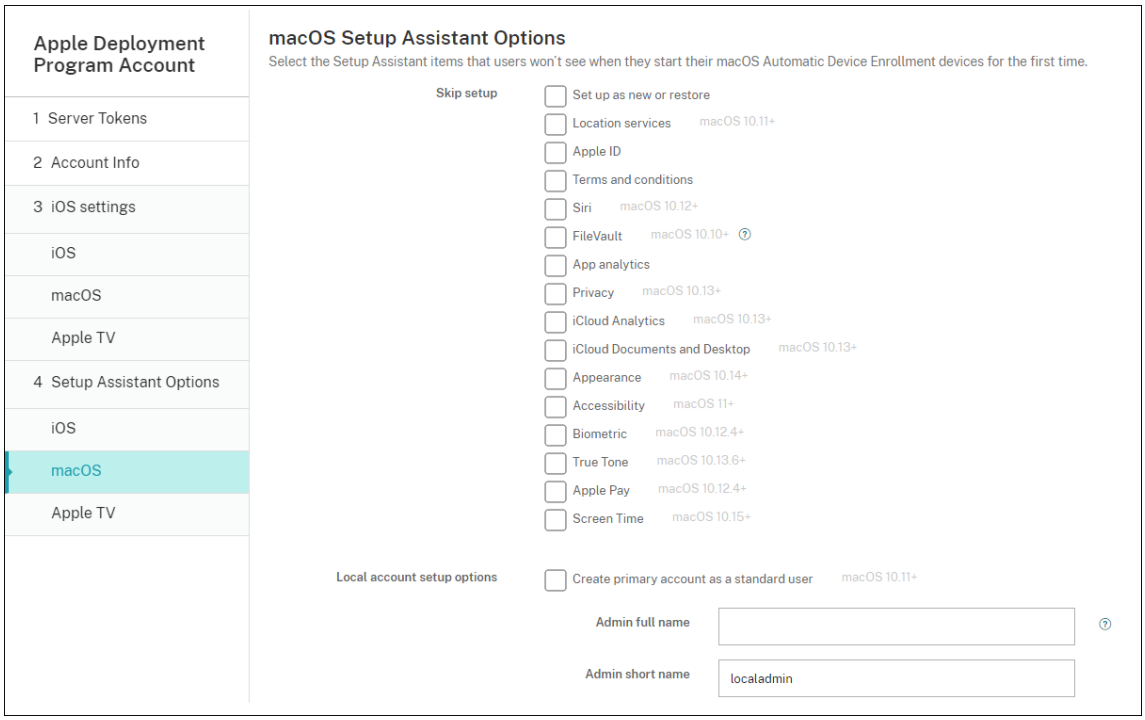
© 1997–2025 Citrix Systems, Inc. All rights reserved.

17.0 and later.

- **Lockdown Mode:** Prevents users from seeing the Lockdown Mode pane if an Apple Account is set up. For iOS 17.1 and later.
- **Intelligence:** Prevents users from seeing the Intelligence pane. For iOS 18.0 and later.
- **Camera button:** Prevents users from seeing the Camera Button pane. For iOS 18.0 and later.

The account appears on **Settings > Apple Deployment Program**.

8. In **macOS Setup Assistant Options**, select the steps that the macOS Setup Assistant skips when users start their devices the first time. When a screen is skipped, the related feature uses default settings. Users can configure the skipped features after setup completes unless you restrict access to those features completely. For more information about restricting access to features, see Restrictions device policy. The default for all items is cleared. The following descriptions explain what occurs when a setting is selected.



- **Set up as new or restore:** Prevents users from setting up the device as new or from a Time Machine backup or do a system migration.
- **Location services:** Prevents users from setting up the location service on the device. For macOS 10.11 and later.
- **Apple ID:** Prevents users from setting up a Managed Apple ID account for the device.
- **Terms and conditions:** Prevents users from reading and accepting terms and conditions for use of the device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Siri:** Prevents the user from configuring Siri. For macOS 10.12 and later.
- **FileVault:** Use FileVault to encrypt the startup disk. Citrix Endpoint Management only applies the FileVault setting if the system has a single local user account and that account is signed into iCloud.

  You can use the macOS FileVault Disk Encryption feature to protect the system volume by encrypting its contents (https://support.apple.com/en-us/HT204837). If you run the Setup assistant on a late-model portable Mac that doesn't have FileVault turned on, you might be prompted to turn on this feature. The prompt appears on both new systems and systems upgraded to OS X 10.10 or 10.11, but only if the system has a single local administrator account and that account is signed into iCloud.
- **App analytics:** Prevents users from setting up whether to share crash data and usage statistics with Apple.
- **Privacy:** Prevent users from seeing the Data and privacy pane. For macOS 10.13 and later.
- **iCloud Analytics:** Prevent users from choosing whether to send diagnostic iCloud data to Apple. For macOS 10.13 and later.
- **iCloud Documents and Desktop:** Prevent users from setting up the iCloud Desktop and Documents. For macOS 10.13 and later.
- **Appearance:** Prevents users from selecting the appearance mode. For macOS 10.14 and later.
- **Accessibility:** Prevents the user from hearing Voice Over automatically. Only available if the device is connected to Ethernet. For macOS 11 and later.
- **Biometric:** Prevents the user from setting up Touch ID and Face ID. For macOS 10.12.4 and later.
- **True Tone:** Prevents users from setting up four-channel sensors to dynamically adjust the white balance of the display. For macOS 10.13.6 and later.
- **Apple Pay:** Prevents users from setting up Apple Pay. If this setting is cleared, users must set up Touch ID and Apple ID. Make sure that the **Apple ID** and **Biometric** settings are cleared.
- **Screen Time:** Prevents users from enabling Screen Time. For macOS 10.15 and later.
- **App Store:** Prevents the user from setting up the App Store. For macOS 11.1 and later.
- **Unlock with Apple Watch:** Prevents users from unlocking their Mac with an Apple Watch. For macOS 12 and later.
- **Local account setup options:** Specify the settings to create an account on the device. Citrix Endpoint Management first creates the local administrator account by using the information that you specify here. When users activate their device, a user account is created as

© 1997–2025 Citrix Systems, Inc. All rights reserved.

the primary account. The **Create primary account as a standard user** option determines whether the primary account has administrator privileges.

> **Important:**
>
> You can select **Create primary account as a standard user** only after you set **Wait for configuration to complete setup** to **On** on the **macOS settings** page.

- **Create primary account as a standard user:** When selected, Citrix Endpoint Management creates the user with standard permissions rather than granting the user administrator privileges on the device. Skip this option if you want to grant the user administrator privileges on the device. By default, this option isn't selected.
- **Admin full name:** Type the name that the system displays for the administrator account.
- **Admin short name:** Type the name that the device displays for the home folder and in the shell.
- **Admin password:** Type a secure password for the administrator account.
- **Show administrator account in Users and Groups:** If cleared, the administrator account doesn't appear in **Users and Groups** in the macOS settings. If you create the primary account as a standard user, enable this setting to hide the administrator account that Citrix Endpoint Management first creates.

To enhance security, Citrix Endpoint Management checks whether to rotate the password of the administrator account daily. By default, Citrix Endpoint Management rotates the password every 7 days. To change the default, update the `mac.dep.admin.passwd.rotate` server property. For more information, see Server properties.

To increase password strength and security, Citrix Endpoint Management generates passwords as follows:

- 12 characters long
- 3 upper-case letters
- 3 lower-case letters
- 3 numbers
- 3 special characters: `! \@ \\# \$ % \\^ \* ? + = -`

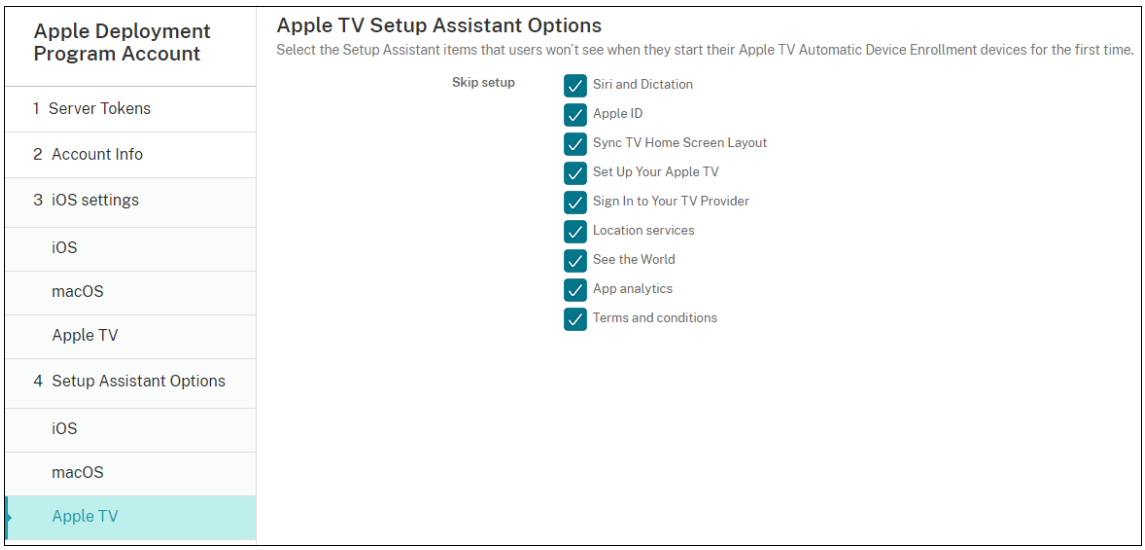
To view the previous password, the current password, and password change status for a device, go to **Manage > Devices**. Click that device, click **Show more**, and then view the **Device details > General** page. The **Security** section displays the following:

- **Previous administrator password:** Lets you view the previous password. Citrix Endpoint Management displays only the last password. Click **Show password** to view the password.
- **Current administrator password:** Lets you view the current password.
- **Change administrator password:** Lets you view password change status. The following information might appear, depending on actual status:

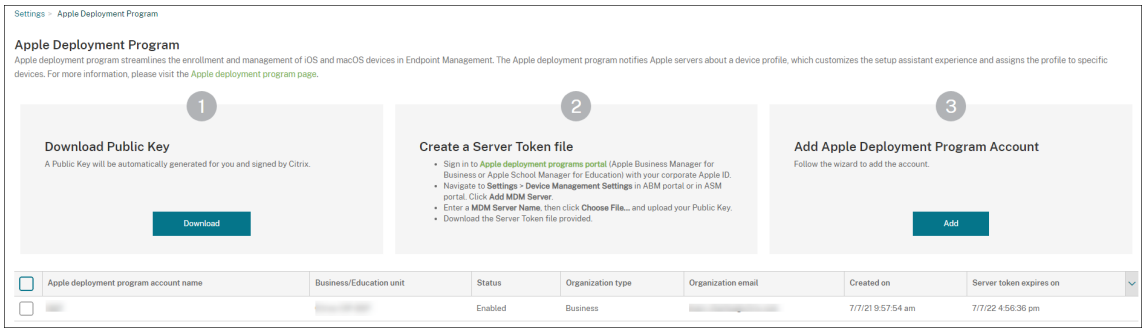
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Password change was requested at <specific time value>.
- The password was changed at <specific time value>.
- Attempts to change the password failed at <specific time value>.
- The password has not yet been changed.

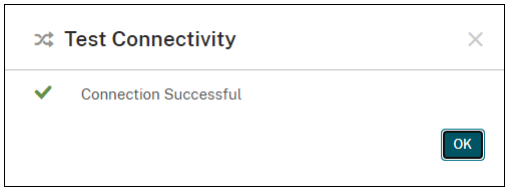
9. In **Apple TV Setup Assistant Options**, select the Apple TV Setup Assistant steps that your users skip when they start their devices the first time. The default for all items is cleared. Save the changes.



10. The account appears on **Settings > Apple Deployment Program**. To test connectivity between Citrix Endpoint Management and Apple, select the account and click **Test Connectivity**.



A status message appears.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Order devices

You can order devices directly from the following channels:

- Apple. Provide your Apple customer numbers to the seller.
- Participating Apple Authorized Reseller or carriers. Provide your Organization ID to the seller and get its Reseller ID.

For more information about managing device suppliers, see Apple Business Manager User Guide or Apple School Manager User Guide.

After your order ships, the Apple devices that you bought are added to your ABM or ASM account.

Assign devices to Citrix Endpoint Management

In the ABM or ASM portal, search for an order number and use it to assign devices in this order to your Citrix Endpoint Management. You can also add iPhone, iPad, iPod touch, and Apple TV devices to ABM or ASM by using Apple Configurator 2, regardless of where the devices were bought.

For more information, see the Apple Business Manager User Guide or Apple School Manager User Guide.

Buy content in volume and synchronize it to Citrix Endpoint Management

ABM and ASM let you buy, distribute, and manage licenses of apps and books in volume from a single organization account. To enable your Citrix Endpoint Management to communicate with ABM or ASM to get the license information for distribution, complete the following steps:

1. In the ABM or ASM portal, buy public apps and books from the **Apps and Books** and buy custom apps that are developed for your Citrix Endpoint Management from **Custom Apps**.
2. In the ABM or ASM portal, download the content token assigned to your Citrix Endpoint Management.

   For more information about Steps 1 and 2, see the Apple Business Manager User Guide or Apple School Manager User Guide.
3. In the Citrix Endpoint Management console, create a Volume Purchase account based on the content token you downloaded.

   For more information, see Adding apps through Apple Volume Purchase.

   After the Volume Purchase account is created, the apps and books that you bought appear in **Manage** > **Apps**, and the devices that you assigned to the Citrix Endpoint Management server appear in **Manage > Devices**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

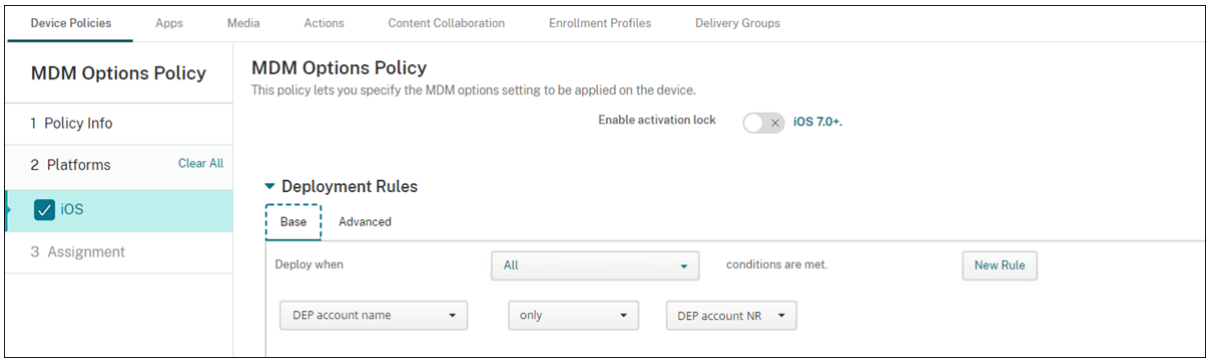
Configure deployment rules for device policies and apps

You can associate ABM or ASM accounts with different device policies and apps when configuring device policies and apps.

1. On the **Configure > Device Policies** and **Configure > Apps** pages, expand **Deployment Rules**.
2. Specify that a policy or app deploys for a particular ABM account or for all ABM accounts except the one selected.

The list of ABM accounts includes only those accounts with a status of enabled or disabled. If the ABM account is disabled, the ABM device doesn't belong to this account. So, Citrix Endpoint Management doesn't deploy the app or policy to the device.

In the following example, a device policy deploys only for devices with the ABM account name "ABM Account NR."



Enroll Apple devices in bulk

March 4, 2024

You can enroll large numbers of iOS, iPadOS, and macOS devices in Citrix Endpoint Management in two ways:

- Use the Apple Deployment Programs (ADP) to enroll Apple devices that you buy directly from Apple or from a participating Apple Authorized Reseller or a carrier.

  For more information about deploying ADP-enabled devices, see Deploy devices through the Apple Deployment Programs. This article describes how users enroll ADP-enabled devices and how to reenroll the devices.

- Use Apple Configurator 2 to enroll iOS devices regardless of whether you buy them directly from Apple.

This article describes how to deploy devices in bulk using Apple Configurator 2.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

About bulk enrollment

The ADPs include Apple Business Manager (ABM) for business and Apple School Manager (ASM) for Education. Bulk enrollment through the ADPs features the following:

- You don't have to touch or prepare the devices.
- After you complete the deployment settings in Citrix Endpoint Management, you can give the devices to users who can start using them right away.
- You can simplify the setup process for users by eliminating some of the Setup Assistant steps.
- For more information about setting up ABM and ASM, see the documentation available from Apple Business Manager and Apple School Manager.

Bulk enrollment through Apple Configurator 2 features the following:

- You attach iOS devices to a Mac running macOS 10.7.2 or later and the Apple Configurator 2 app. You prepare the iOS devices and configure policies through Apple Configurator 2.
- Devices automatically enroll in Citrix Endpoint Management during the setup process. Once setup is completed, Citrix Endpoint Management pushes policies, apps, and other resources to devices. You can then start managing the devices.
- For more information about using Apple Configurator 2, see the Apple Configurator Help.

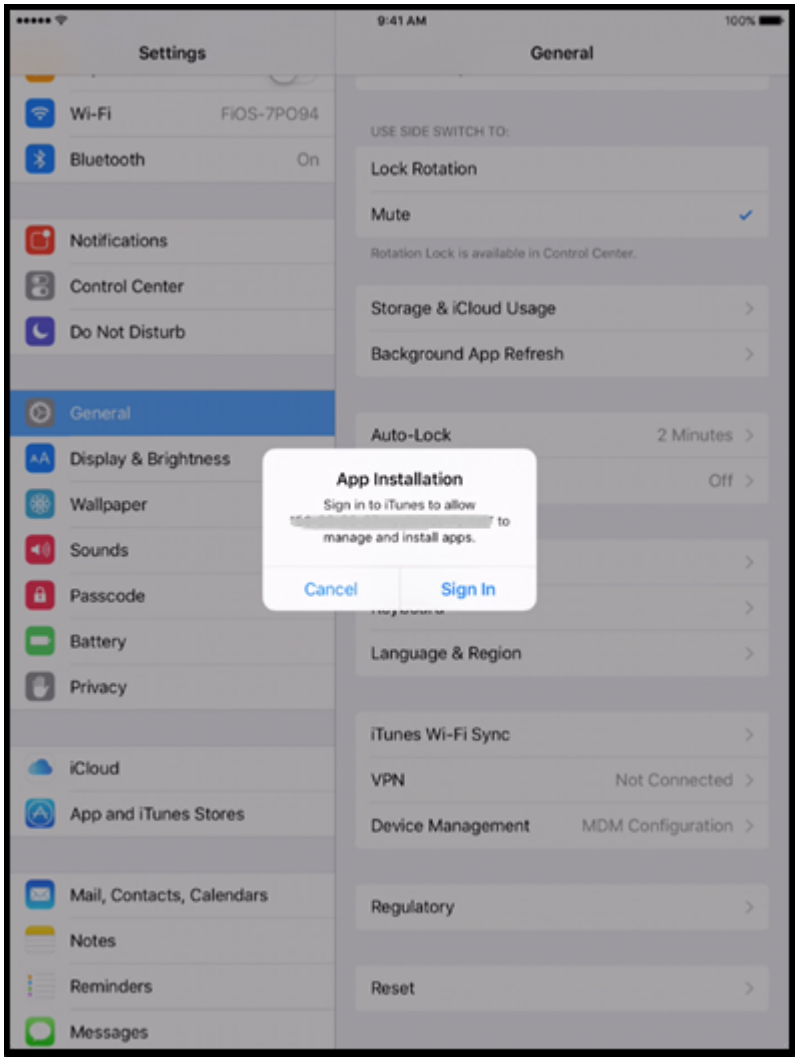
How users enroll ADP-enabled devices

Users enroll their devices in Citrix Endpoint Management as follows:

1. Users start their device.
2. Citrix Endpoint Management delivers the ADP settings that you configured on the **Settings > Apple Deployment Programs** page to the device.
3. Users configure the initial settings on their device.
4. The device automatically starts the Citrix Endpoint Management device enrollment process.
5. Users continue to configure the other initial settings on their device.
6. In the home screen, users might be prompted to sign in to the Apple App Store so that they can download Citrix Secure Hub.

   > **Note:**
   >
   > This step is optional if you configure Citrix Endpoint Management to deploy the Citrix Secure Hub app using the device-based Volume Purchase app assignment. In this case, you don't need to create an Apple App Store account or use an existing account.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



7. Users open Citrix Secure Hub and type their credentials. If required by the policy, users might be prompted to create and verify a Citrix PIN.

   Citrix Endpoint Management deploys any remaining required apps to the device.

Reenroll the ADP-enabled devices

ADP-enabled devices enroll from a factory reset condition. To reenroll an ADP-enabled device, you must first complete a full wipe to unenroll the device. Detailed steps are as follows:

1. On the **Manage > Devices** page, select the device.
2. Click **Security**.
3. Click **Full Wipe** to unenroll the device to the factory reset condition.
4. Start the device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

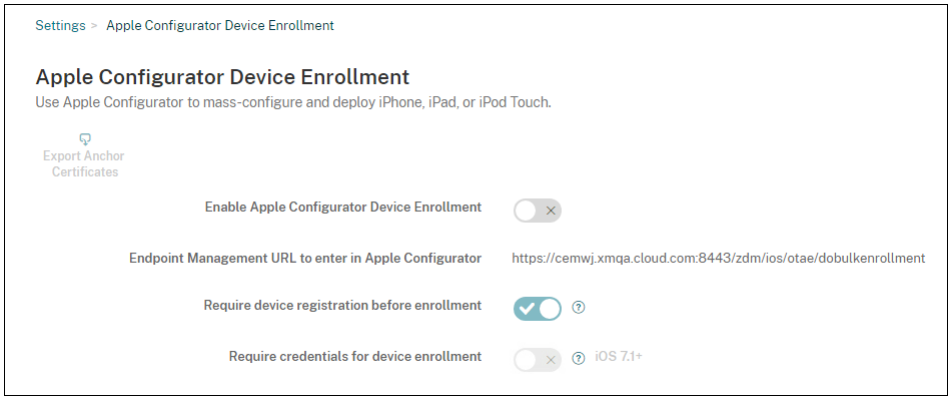
> **Important:**
>
> Do not use **Selective Wipe** to unenroll an ADP-enabled device because ADP enrollment requires the device in the factory reset condition.

Deploy devices using Apple Configurator 2

You can use Apple Configurator 2 to deploy large numbers of devices with settings, apps, and data and enroll these devices in Citrix Endpoint Management.

Step 1: Configure settings in Citrix Endpoint Management

1. In the Citrix Endpoint Management console, go to **Settings > Apple Configurator Device Enrollment**.

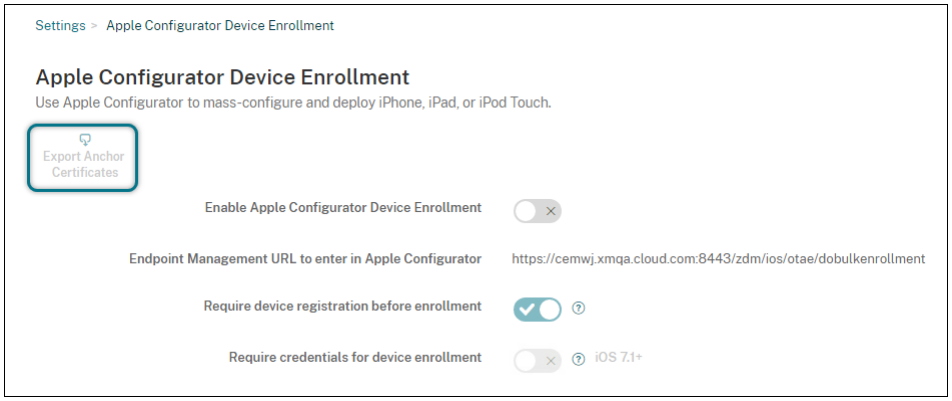


2. Set **Enable Apple Configurator device enrollment** to **Yes**.
3. Copy the **Enrollment URL to enter in Apple Configurator** setting and paste this URL when you configure settings in Apple Configurator 2. This setting provides the URL for the Citrix Endpoint Management server that communicates with Apple. The enrollment URL is the Citrix Endpoint Management server fully qualified domain name (FQDN), such as `mdm.server.url.com`, or the IP address.
4. To prevent unknown devices from enrolling, set **Require device registration before enrollment** to **Yes**. Note: If this setting is set as **Yes**, you must add the configured devices to **Manage > Devices** in Citrix Endpoint Management manually or through a CSV file before enrollment.
5. To require users of iOS devices to enter their credentials when enrolling, set **Require credentials for device enrollment** to **Yes**. The default is **No**.

   > **Note:**
   >
   > If the Citrix Endpoint Management server is using a trusted SSL certificate, skip this step.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> Click **Export anchor certs** and save the certchain.pem file to the macOS keychain (login or System).



Step 2: Configure settings in Apple Configurator 2

1. Prepare a Mac that runs macOS 10.7.2 or later and has Apple Configurator 2 installed.
2. Use a Dock Connector-to-USB cable to connect Apple devices to the Mac. You can configure up to 30 connected devices simultaneously. If you do not have a Dock Connector, use one or more powered USB 2.0 high-speed hubs to connect the devices.
3. Start Apple Configurator 2. The configurator shows any devices that you can prepare for supervision.
4. To prepare a device for supervision:
   - Select **Supervise devices** if you intend to maintain control of the device by reapplying a configuration regularly. Click **Next**.

     > **Important:**
     >
     > Placing a device into Supervised mode installs the selected version of iOS on the device, completely wiping the device of any previously stored user data or apps.

   - In iOS, click **Latest** for the latest version of iOS that you want to install.
5. In **Enroll in MDM Server**, choose an MDM server. To add a server, click **Next**.
6. In **Define an MDM server**, provide a name for the server and paste the MDM server URL from the Citrix Endpoint Management console.
7. In **Assign to organization**, choose an organization to supervise the device.

   For more information on preparing devices with Apple Configurator 2, see the Apple Configurator help page, Prepare devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

8. As each device is prepared, turn it on to start the iOS Setup Assistant, which prepares the device for first-time use.

Add devices to ABM or ASM using Apple Configurator 2

You can add iPhone, iPad, and Apple TV devices to your ABM or ASM account using Apple Configurator 2 regardless of where the devices were bought.
After you add devices, they appear in the **Devices** section. These devices no longer include enrollment settings assigned through Apple Configurator 2. For more information, see the Apple Business Manager User Guide or Apple School Manager User Guide.

Renew the ADP token

Citrix Endpoint Management displays a license expiration warning when your ADP token expires. Replace the token from ASM or ABM.

Step 1: Download a public key from your Citrix Endpoint Management server

1. In the Citrix Endpoint Management console, go to **Settings > Apple Deployment Program** to download a new public key.

Step 2: Create and download a server token file from your Apple account

1. Sign in to ABM to download the token.
2. Open **Settings** and select the server from which you need a token. Click **Edit**.
3. Under **MDM Server Settings**, upload the new public key you downloaded from Citrix Endpoint Management and save the changes.
4. Click **Download Token** to download the new token.

Step 3: Upload a server token file in Citrix Endpoint Management

1. In Citrix Endpoint Management, go to **Settings > Apple Deployment Program**.
2. Select the Deployment Program account, click **Edit**, and upload your server token file.
3. Click **Next** and save the changes.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Integrate with Apple Education features

March 4, 2024

You can use Citrix Endpoint Management as your Mobile Device Management (MDM) solution in an environment that uses Apple Education. Citrix Endpoint Management support includes Apple School Manager (ASM) and Classroom app for the iPad. The Citrix Endpoint Management Education Configuration device policy configures instructor and student devices for use with Apple Education.

You provide preconfigured and supervised iPads to instructors and students. That configuration includes ASM enrollment in Citrix Endpoint Management, a Managed Apple ID account configured with a new password, and required Volume Purchase apps and iBooks.

For more information about Apple Education features, see the Apple Education site and the Apple Education Deployment Guide from the same site.

Apple School Manager

Follow these general steps to integrate Citrix Endpoint Management with ASM.

1. Create an account for your institution in ASM to enroll your institution in ASM.
2. Configure an Education Volume Purchase account for the Apple School Manager.
3. Add passwords for Apple School Manager users.
4. Plan and add resources and delivery groups to Citrix Endpoint Management.
5. Test instructor and student device enrollments.
6. Provide the preconfigured devices to instructors and students.
7. Manage instructor, student, and class data
8. If a device is lost or stolen, you can lock and locate the device.

For information on enrolling in ASM and connecting your account to Citrix Endpoint Management, see Deploy devices through the Apple Deployment Program.

Prerequisites

- NetScaler Gateway
- Enrollment profile configured for MDM+MAM.
- Apple iPad third generation (minimum version) or iPad Mini, with iOS 9.3 (minimum version)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Citrix Endpoint Management doesn't validate ASM user accounts against LDAP or Active Directory. However, you can connect Citrix Endpoint Management to the LDAP or Active Directory for management of users and devices not related to ASM instructors or students. For example, you can use Active Directory to provide Citrix Secure Mail and Citrix Secure Web to other ASM members, such as IT administrators and managers.
>
> Because ASM instructors and students are local users, there is no need to deploy Citrix Secure Hub to their devices.
>
> MAM enrollment that includes NetScaler Gateway authentication doesn't support local users (only Active Directory users). So, Citrix Endpoint Management deploys only required Volume Purchase apps and iBooks to instructor and student devices.

Classroom app for iPad

The Classroom app for iPad enables instructors to connect to and manage student devices. You can view device screens, open apps on iPads, share, and open web links, and present a student screen on Apple TV.

Classroom is free in the App Store. You upload the app to the Citrix Endpoint Management console. You then use the Education Configuration device policy to configure the Classroom app, which you deploy to instructor devices.

For more information on how to deploy the Classroom app, see Distribute Apple apps.

For more information on Classroom app requirements, setup, and features, see the Classroom user guide on the Apple support site.

Add passwords for Apple School Manager users

After you add an ASM account, Citrix Endpoint Management imports classes and users from ASM. Citrix Endpoint Management treats classes as local groups and uses the term "group"in the console. If a class has a group name in ASM, Citrix Endpoint Management assigns the group name to the class. Otherwise, Citrix Endpoint Management uses the source system ID for the group name. Citrix Endpoint Management doesn't use the course name for the class name because course names in ASM aren't unique.

Citrix Endpoint Management uses the Managed Apple IDs to create local users with the user type **ASM**. The users are local because ASM creates the credentials independently of all external data sources. As a result, Citrix Endpoint Management doesn't use a directory server to authenticate these new users.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

ASM doesn't send temporary user passwords to Citrix Endpoint Management. You can import them from a CSV file or add them manually. To import temporary user passwords:

1. Get the CSV file generated by ASM when creating the Managed Apple ID temporary passwords.
2. Edit the CSV file, replacing the temporary passwords with new passwords that users provide to enroll to Citrix Endpoint Management. There's no constraint on the password type for this purpose.

   The format of an entry in the CSV file is as follows: `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`

   Where:

   User: `user@appleid.citrix.com`

   First name: `Firstname`

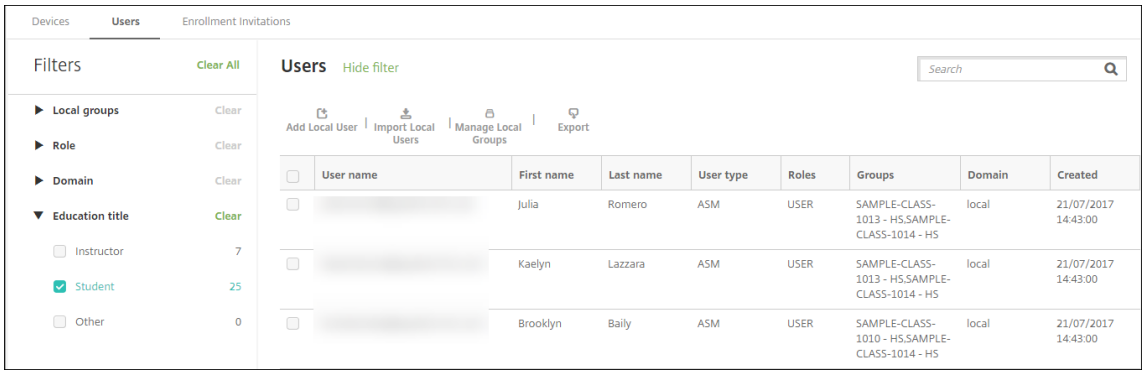
   Middle name: `Middle`

   Last name: `Lastname`

   Password: `Password123!`
3. In the Citrix Endpoint Management console, click **Manage > Users**. The **Users** page appears.

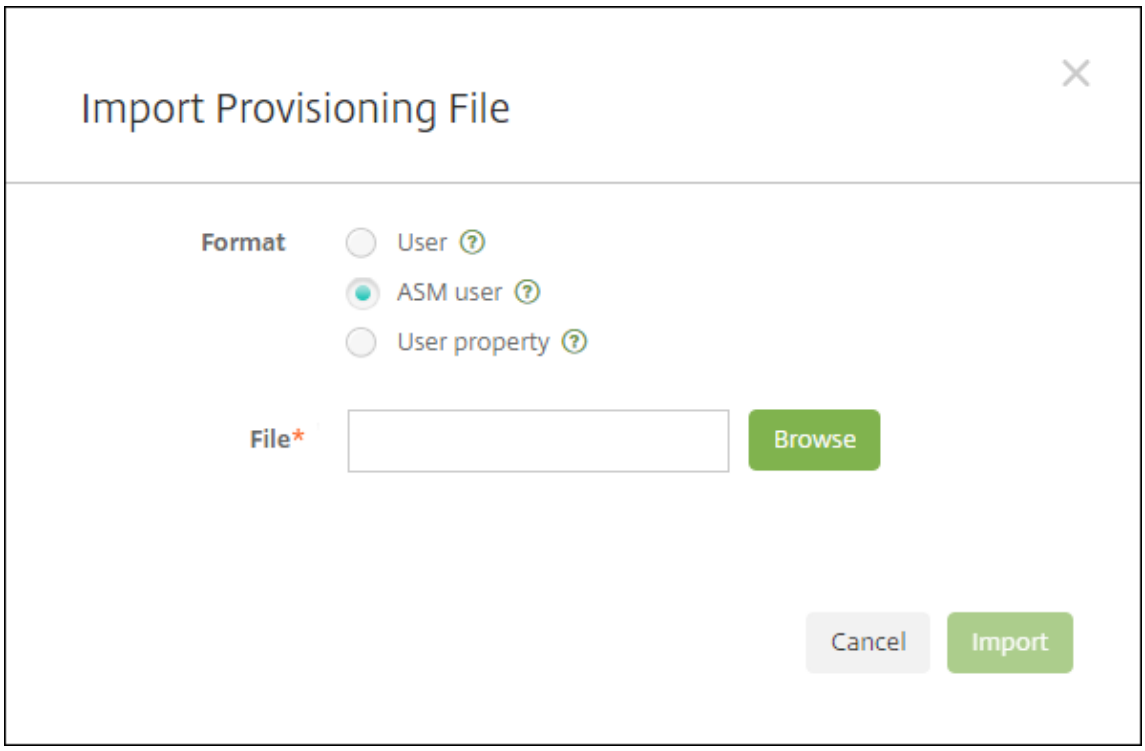
   The following **Manage > Users** screen sample shows a list of users imported from ASM. In the **Users** list:

   - **User name** shows the managed Apple ID.
   - User type is **ASM**, to indicate the account originated from ASM.
   - **Groups** show the classes.

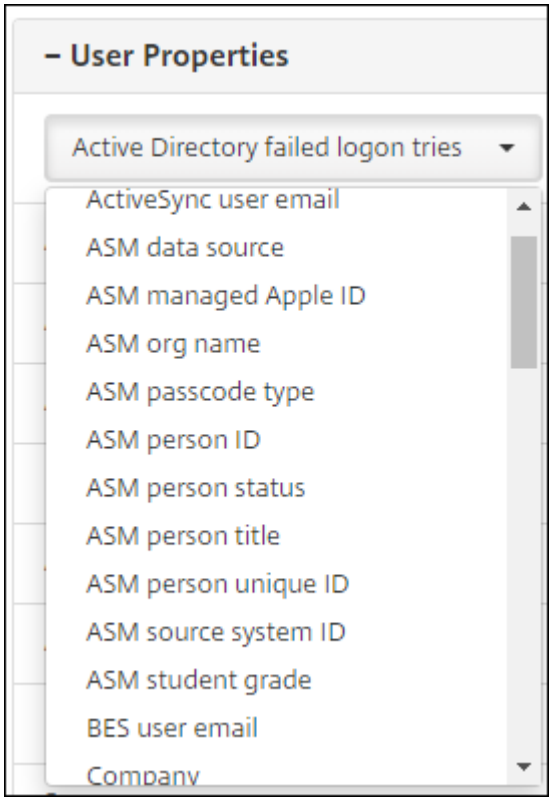


4. Click **Import Local Users**. The **Import Provisioning File** dialog box appears.
5. For Format, choose **ASM user**, navigate to the CSV file you prepared in step 2, and then click **Import**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. To view the properties for a local user, select the user and then click **Edit**.



In addition to the name properties, these ASM properties are available:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **ASM data source:** The data source of the class, such as **CSV** or **SFTP**.
- **ASM managed Apple ID:** A Managed Apple ID might include your institution name and `appleid`. For example, the ID might resemble johnappleseed@appleid.myschool.edu. Citrix Endpoint Management requires a Managed Apple ID for authentication.
- **ASM org name:** The name you gave the account in Citrix Endpoint Management.
- **ASM passcode type:** Password policy of the person: **complex** (a non-student password of eight or more numbers and letters), **four** (digits), or **six** (digits).
- **ASM person unique ID:** Identifier for the user.
- **ASM person status:** Specifies whether the Managed Apple ID is **Active** or **Inactive**. This status becomes active after the user provides their new password for the Managed Apple ID account.
- **ASM person title:** Either Instructor, Student or Other.
- **ASM person unique ID:** Unique identifier for the user.
- **ASM source system ID:** Identifier for the system source.
- **ASM student grade:** Student grade information (not used by instructors).

Plan and add resources and delivery groups to Citrix Endpoint Management

A delivery group specifies the resources to deploy to categories of users. For example, you might create one delivery group for instructors and students. Alternatively, you might create multiple delivery groups so you can customize the apps, media, and policies sent to various instructors or students. You might create one or more delivery groups per class. You can also create one or more delivery groups for managers (other staff in your educational institution).

Resources that you deploy to user devices include device policies, Volume Purchase apps, and iBooks.

- Device policies:

  If instructors use the Classroom app, the Education Configuration device policy is required. Be sure to review other device policies to determine how you want to configure and restrict instructor and student iPads.

- Volume Purchase apps:

  Citrix Endpoint Management requires that you deploy Volume Purchase apps as required apps for education users. Citrix Endpoint Management doesn't support deploying such Volume Purchase apps as optional.

  If you use the Apple Classroom app, deploy it only to instructor devices.

  Deploy any other apps that you want to provide to instructors or students. This solution doesn't use the Citrix Secure Hub app, so there's no need to deploy it to instructors or students.

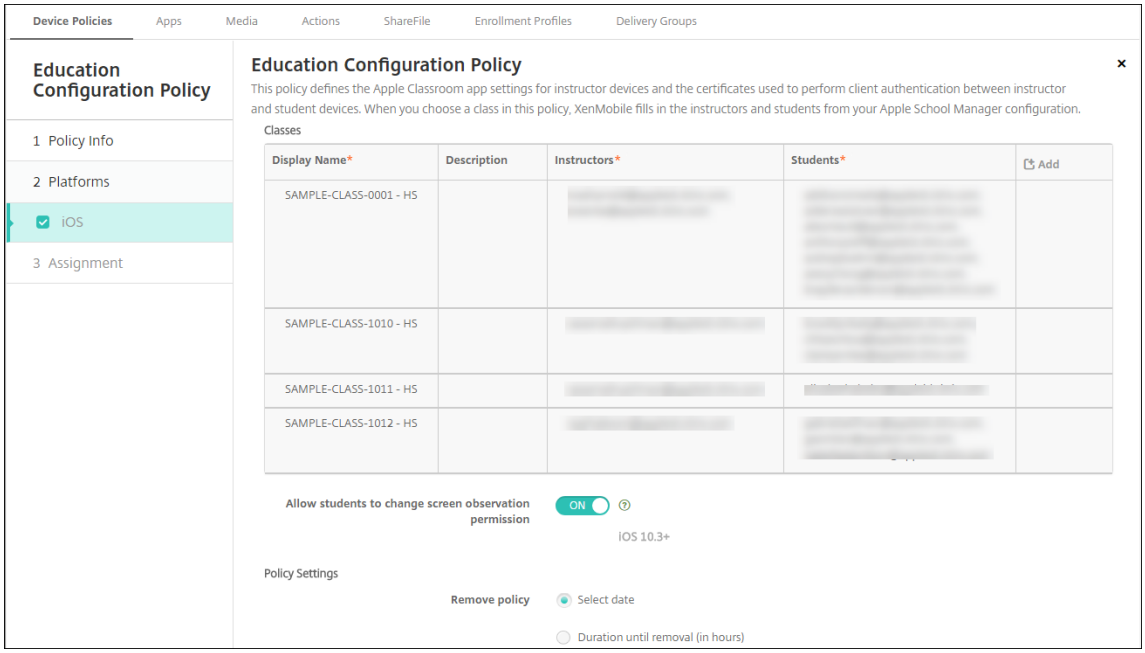
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Volume Purchase iBooks:

  After Citrix Endpoint Management connects to your ASM account, your bought iBooks appear in the Citrix Endpoint Management console, in **Configure > Media**. The iBooks listed on that page are available to add to delivery groups. Citrix Endpoint Management supports adding iBooks as required media only.

After you plan the resources and delivery groups for instructors and students, you can create those items in the Citrix Endpoint Management console.

1. Create any device policies that you want to deploy to instructor or student devices. For information about the Education Configuration device policy, see Education Configuration device policy.



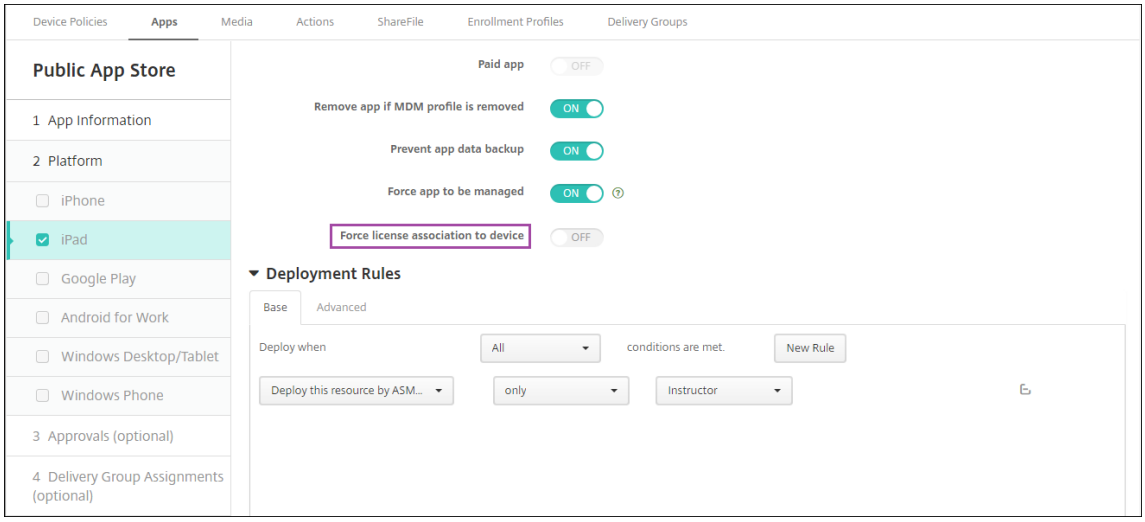
   For information about device policies, see Device policies and the individual policy articles.

2. Configure apps (**Configure > Apps**) and iBooks (**Configure > Media**):

   - By default, Citrix Endpoint Management assigns apps and iBooks at the user level. During first-time deployment, instructors and students receive a prompt to register to ASM. After accepting the invitation, users receive their ASM apps and iBooks at the next deployment (within six hours). Citrix recommends that you force the deployment of apps and iBooks to new ASM users. To do that, select the delivery group and click **Deploy**.

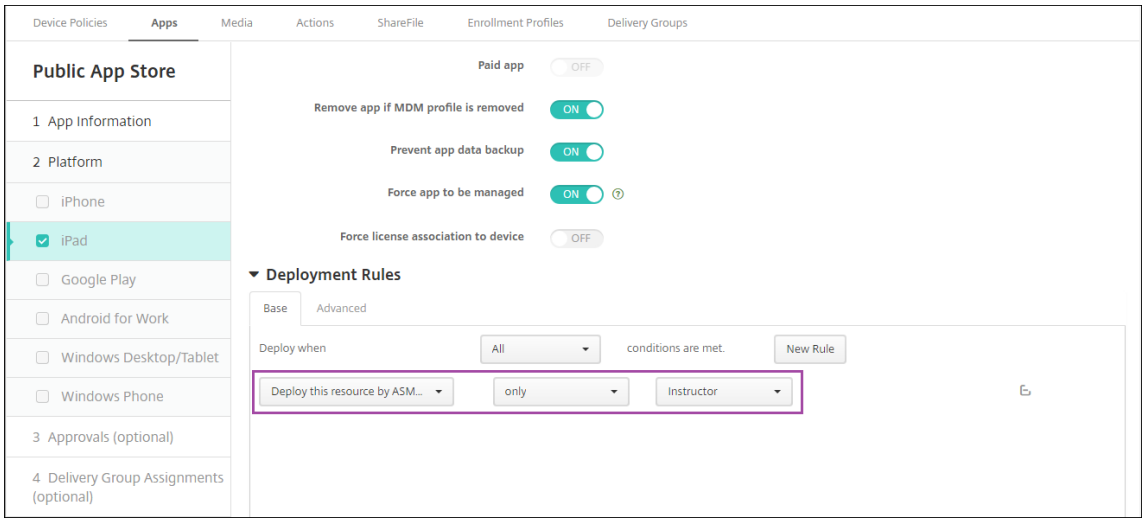
     You can choose to assign apps (but not iBooks) at the device level. To do that, change the setting **Force license association to device** to **On**. When you assign apps at the device level, users don't receive an invitation to join the Volume Purchase program.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- To deploy an app only to instructors, select a delivery group that includes only instructors or use the following deployment rule:

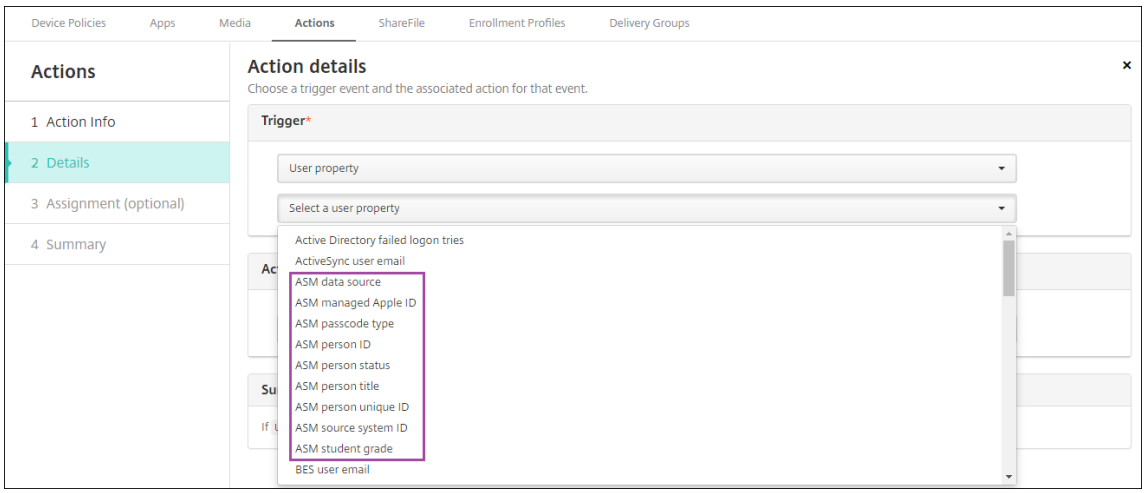
```
Deploy this resource by ASM device type
only
Instructor
```



- For help with adding Volume Purchase apps, see Add a Public App Store app.

3. Optional. Create actions based on ASM user properties. For example, you might create an action to send a notification to student devices when a new app installs. Alternatively, you can create an action that a user property triggers, as shown in the following example.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



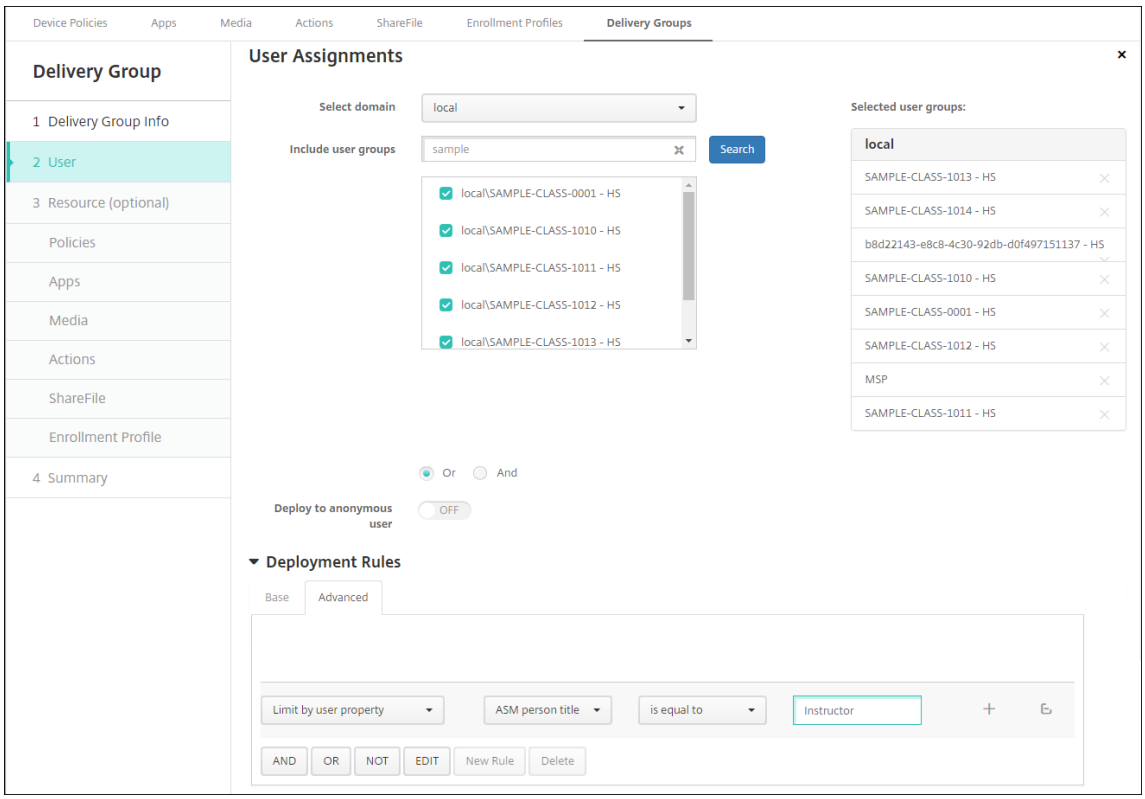
To create an action, go to **Configure > Actions**. For information about configuring actions, see Automated actions.

4. In **Configure > Delivery Groups**, create delivery groups for instructors and for students. Choose the classes that were imported from ASM. Also, create a deployment rule for instructors and students.

   For example, the following user assignments are for instructors. The deployment rule is:

```
Limit by user property
ASM person title
is equal to
Instructor
```

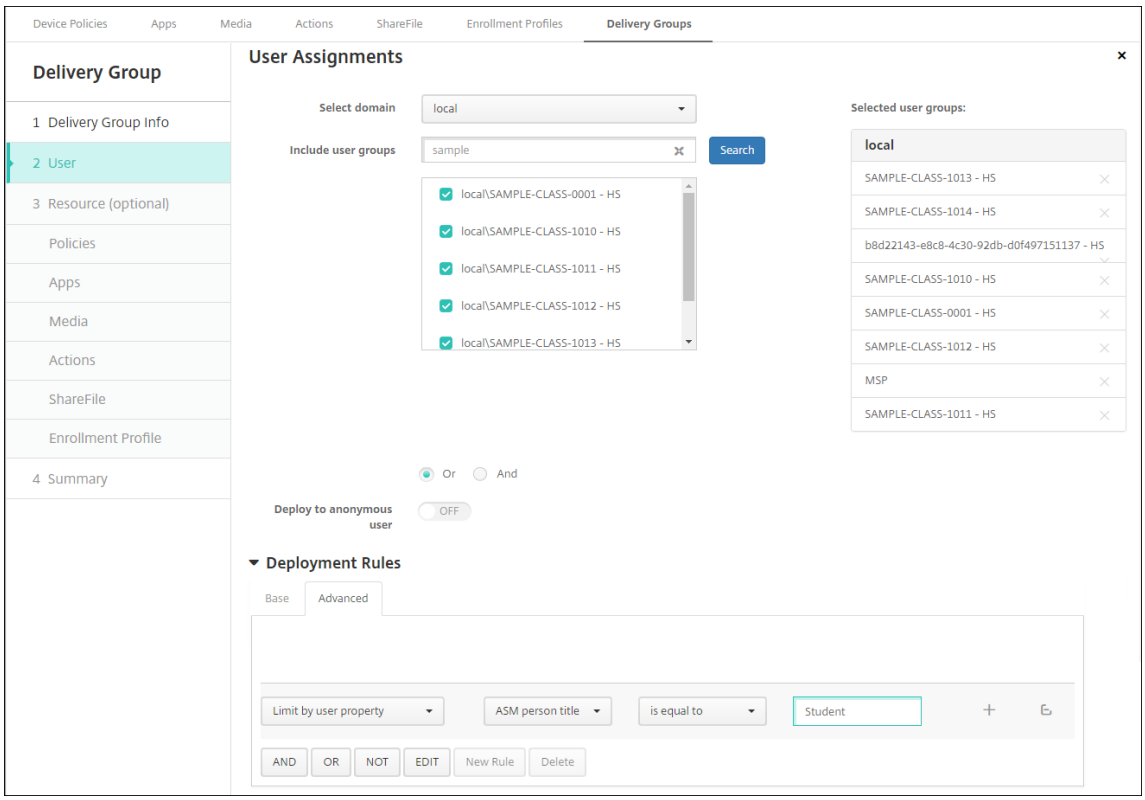
© 1997–2025 Citrix Systems, Inc. All rights reserved.



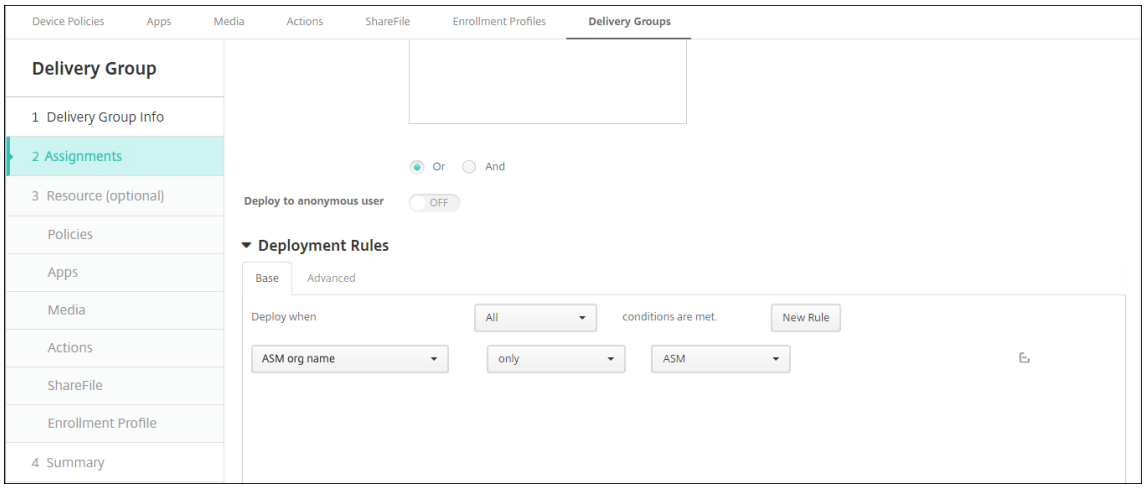
The following user assignments are for students. The deployment rule is:

```
Limit by user property
ASM person title
is equal to
Student
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

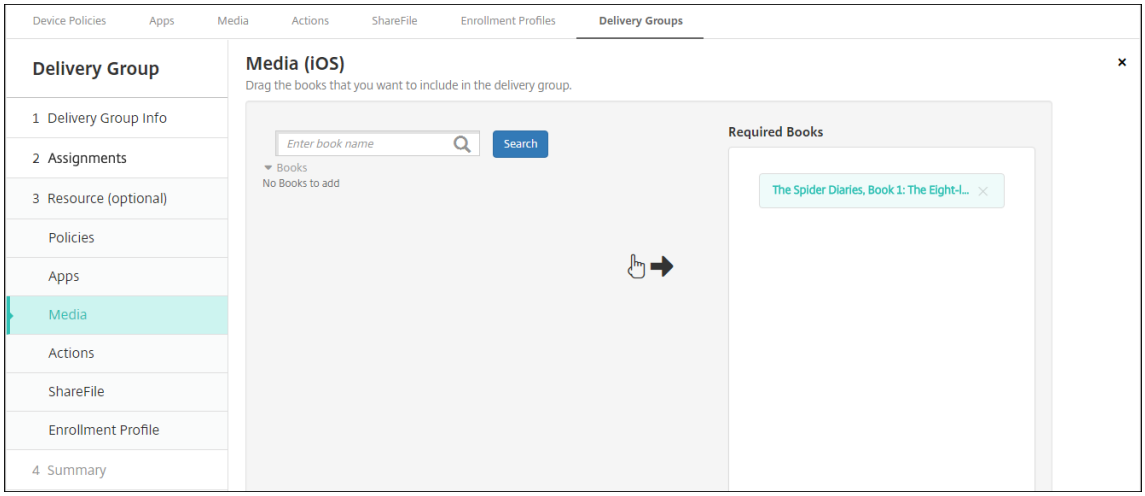


You can also filter a delivery group by using a deployment rule based on the ASM org name.

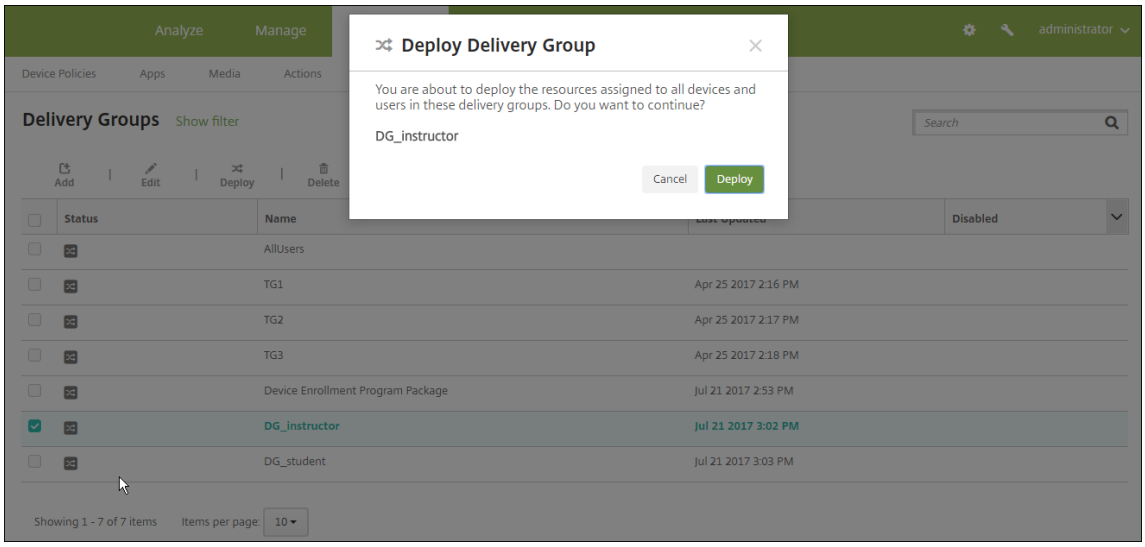


5. Assign the resources to delivery groups. The following example shows an iBook in a delivery group.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The following example shows the confirmation dialog that appears when you select a delivery group and click **Deploy**.



For more information, see “To edit a delivery group”and “To deploy to delivery groups”in Deploy resources.

Test instructor and student device enrollments

You can enroll devices through either of the following methods:

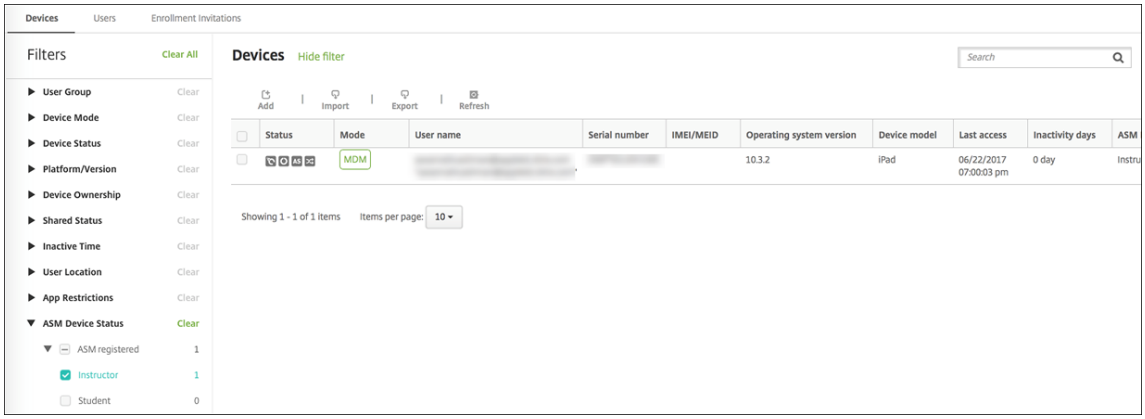
- A school administrator can enroll instructor and student devices by using the user password you can set in the Citrix Endpoint Management console. As a result, you can provide users with devices that are already set up with apps and media.
- When users receive the devices, they enroll using the user password that you provide to them. After enrollment completes, Citrix Endpoint Management sends device policies, apps, and media to the devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

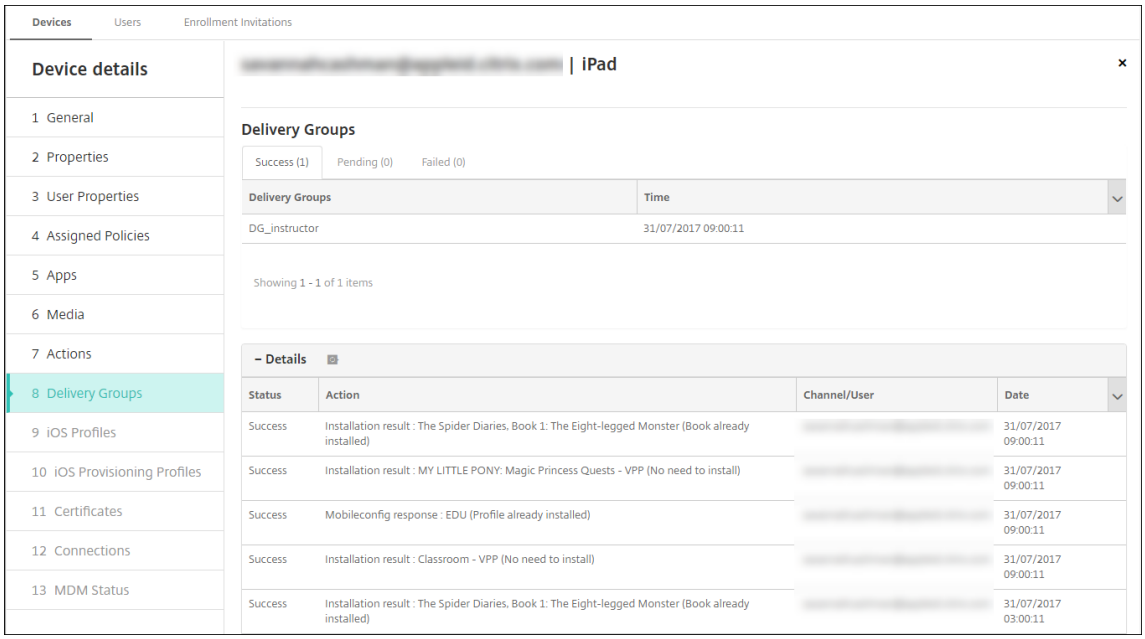
To test enrollment, use Apple Deployment Program devices that are linked to ASM.

1. If the devices aren't linked to ASM, erase the device contents and settings by doing a hard reset.
2. Enroll an ASM device with an instructor. Then, enroll an ASM device with a student.
3. In the **Manage > Devices** page, check that both ASM devices are enrolled in MDM only.

   You can filter the **Devices** page by the ASM device status: **ASM registered**, **ASM shared**, **Instructor**, and **Student**.



4. To verify that MDM resources deployed correctly for each device: Select the device, click **Edit**, and check the various pages.



Distribute devices

Apple recommends that you host an event so you can distribute the devices to instructors and students.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

If you don't distribute pre-enrolled devices, also provide the following to these users:

- Citrix Endpoint Management passwords for enrollment
- ASM temporary passwords for Managed Apple IDs.

The first-time user experience is as follows.

1. The first time that a user starts their device after a hard-reset, Citrix Endpoint Management prompts them in the enrollment screen to enroll their device.
2. The user provides their Managed Apple ID and Citrix Endpoint Management password used to authenticate to Citrix Endpoint Management.
3. In the Apple ID setup step, the device prompts the user to provide their Managed Apple ID and ASM temporary password. Those items authenticate the user to Apple services.
4. The device prompts the user to create a password for their Managed Apple ID, used to protect their data in iCloud.
5. At the end of the Setup Assistant, Citrix Endpoint Management starts installing the policies, apps, and media to the device. For apps and iBooks assigned at the user level, the assistant prompts instructors and students to register to Volume Purchase. After accepting the invitation, users receive their Volume Purchase apps and iBooks at the next deployment (within six hours).

Manage instructor, student, and class data

When managing instructor, student, and class data, note the following:

- Don't change Managed Apple IDs after you import ASM information into Citrix Endpoint Management. Citrix Endpoint Management also uses ASM user identifiers to identify users.
- If you add or change class data in the ASM after you create one or more Education Configuration device policies: Edit the policies and then redeploy them.
- If the instructor for a class changes after you deploy the Education Configuration device policy: Review the policy to make sure it updates in the Citrix Endpoint Management console and then redeploy the policy.
- If you update user properties in the ASM portal, Citrix Endpoint Management also updates those properties in the console. However, Citrix Endpoint Management doesn't receive the ASM person title property (Instructor, Student, or Other) in the same way it receives other properties. Thus, if you change the ASM person title in the ASM, complete the following steps to reflect that change in Citrix Endpoint Management.

To manage the data:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. In the ASM portal, update the student grade and clear the instructor grade.
2. If you changed a student account to an instructor account, remove the user from the list of students in the class. Then, add the user to the list of instructors in the same or another class.

   If you changed an instructor account to a student account, remove the user from the class. Then, add the user to the list of students in the same or another class. Your updates appear in the Citrix Endpoint Management console during the next sync (every five minutes by default) or fetch (every 24 hours by default).
3. Edit the Education Configuration device policy to apply the change and redeploy it.

   - If you delete a user from the ASM portal, Citrix Endpoint Management also deletes that user from the Citrix Endpoint Management console after a fetch.

     You can reduce the interval between the two baselines by changing this server property value: **bulk.enrollment.fetchRosterInfoDelay** (default is **1440** minutes).
   - After you deploy resources: If a student joins a class, create a delivery group with just that student and deploy the resources to the student.
   - If a student or instructor loses their temporary password, have them contact the ASM administrator. The administrator can provide the temporary password or generate a new one.

Manage a lost or stolen device

The Apple Find My iPhone/iPad service includes an Activation Lock feature. Activation Lock prevents non-authorized users from using or reselling a lost or stolen device that's enrolled in the Apple Deployment Program.

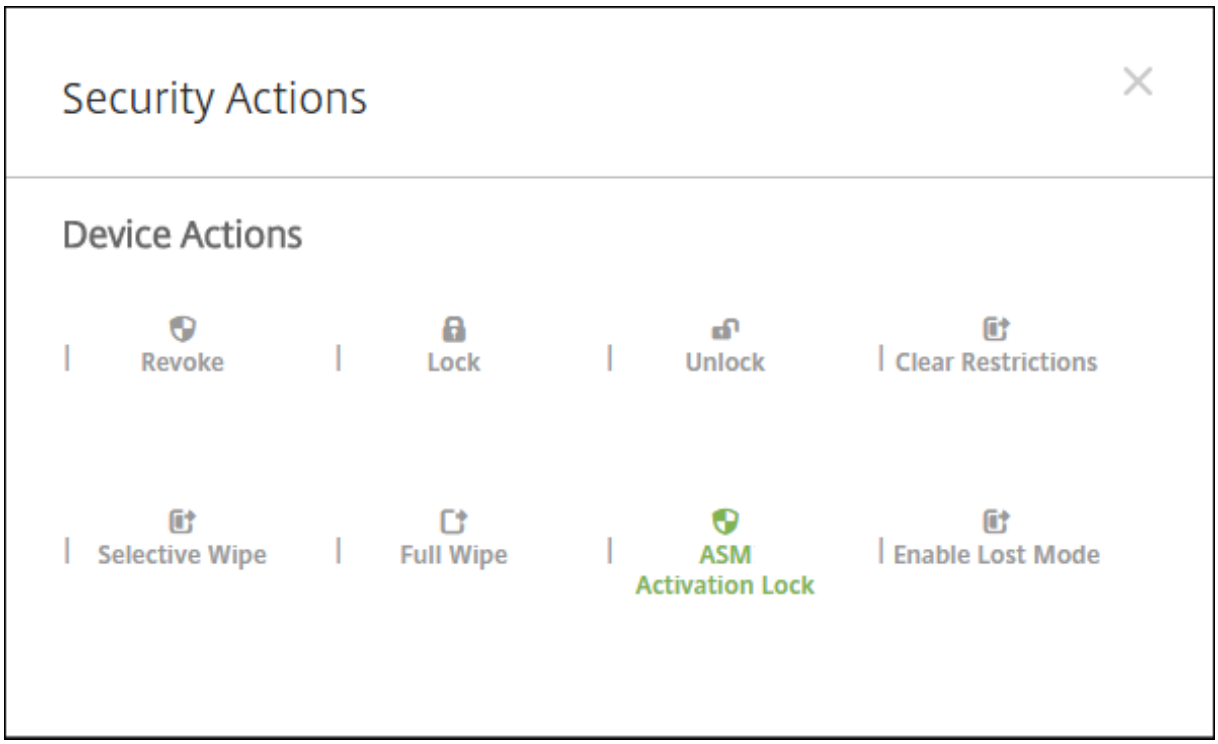
Citrix Endpoint Management includes an **ASM Activation Lock** security action that enables you to send a lock code to an ASM Apple Deployment Program enrolled device.

When you use the **ASM Activation Lock** security action, Citrix Endpoint Management can locate devices without requiring users to enable the Find My iPhone/iPad service. When an ASM device is hard-reset or fully wiped, the user provides their Managed Apple ID and password to unlock the device.

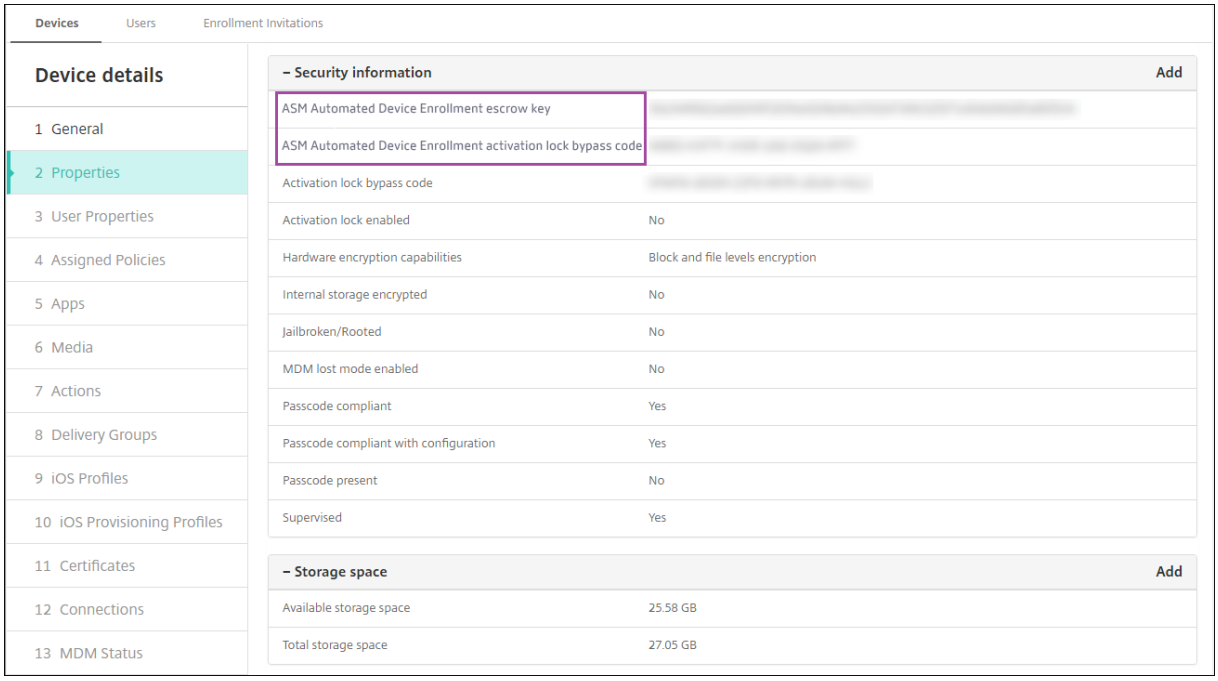
To release the lock from the console, click the security action **Activation Lock Bypass**. For information about bypassing an activation lock, see Bypass an iOS activation lock. The user can also leave the login blank and type the **ASM activation lock bypass code** as the password. That information is available in **Device Details**, on the **Properties** tab.

To set the activation lock, go to **Manage > Devices**, select the device, click **Security**, and then click **ASM Activation Lock**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

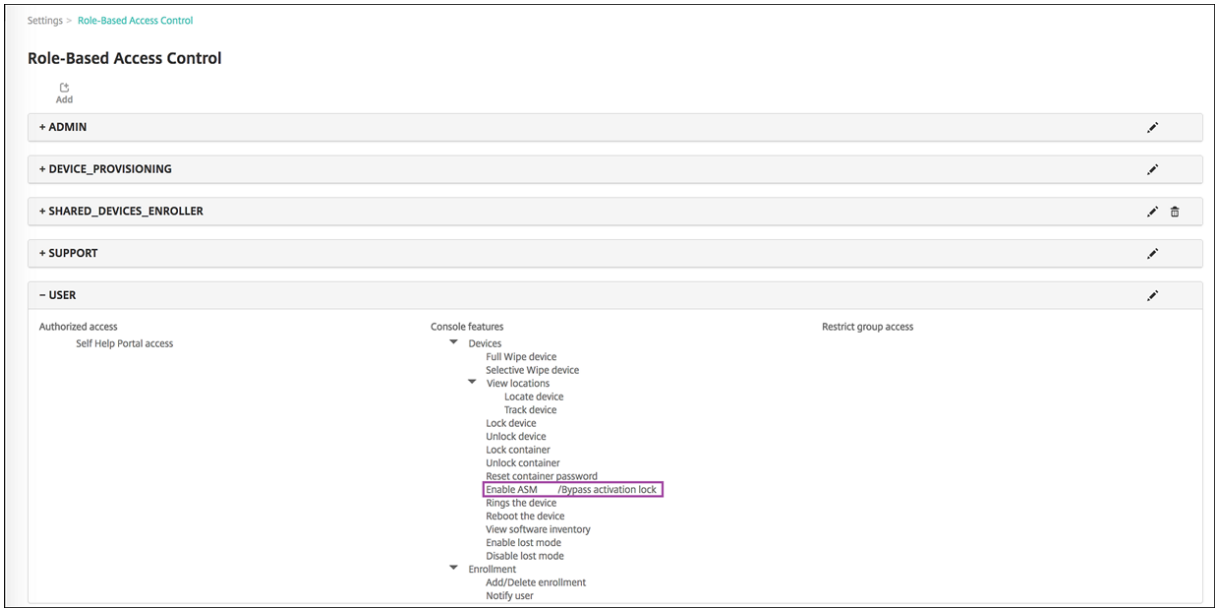


The properties **ASM escrow key** and **ASM activation lock bypass code** appear in **Device details**.



The RBAC permission for an ASM Activation Lock is **Devices > Enable ASM Bypass activation lock**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Shared iPads

March 4, 2024

The shared iPad feature allows multiple users to use an iPad. The user experience can be personalized even though the devices are shared. You can use shared iPads for education or business. Apple School Manager (ASM) supports the instructor and student roles in addition to the roles Apple Business Manager (ABM) supports.

Prerequisites for Shared iPads

- Apple School Manager or Apple Business Manager
- Citrix Endpoint Management
- Any iPad Pro, iPad fifth generation, iPad Air 2 or later, and iPad mini 4 or later
- At least 32 GB of storage
- Supervised devices

Configure Shared iPads

Multiple students or employees can share an iPad for different purposes.

Either you or device owners enroll Shared iPads and then deploy device policies, apps, and media to the devices. After that, users provide their managed Apple ID credentials to sign in to a Shared iPad. If

© 1997–2025 Citrix Systems, Inc. All rights reserved.

you previously deployed an Education Configuration policy to students, they no longer sign-in as an "Other User"to share devices.

Citrix Endpoint Management uses two communications channels for Shared iPads: The system channel for the device owner (instructor or supervisor) and the user channel for the current resident user (student or employee). Citrix Endpoint Management uses those channels to send the appropriate MDM commands for the resources supported by Apple.

Resources that deploy over the system channel are:

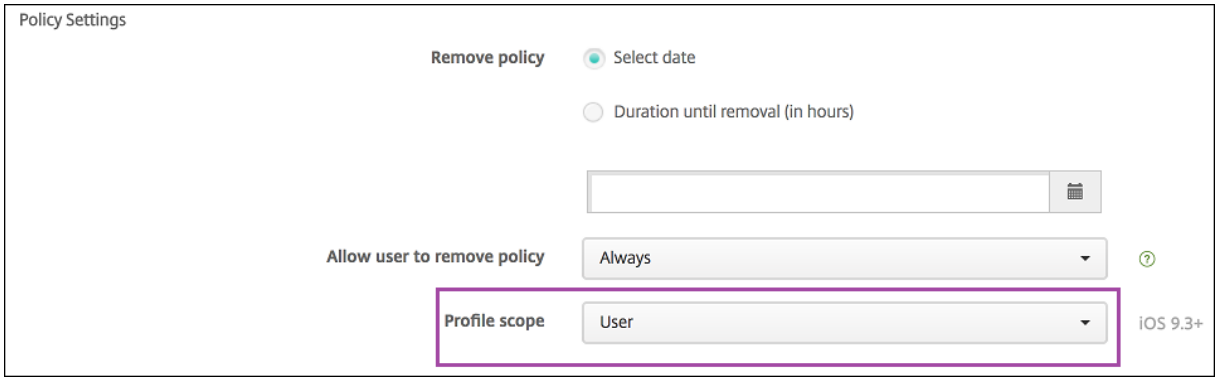
- Device policies, such as Education Configuration, Lock Screen Message, Maximum Resident Users, and Passcode Lock Grace Period
- Device-based Volume Purchase apps
  Apple doesn't support Enterprise apps or user-based Volume Purchase apps on Shared iPads. Apps installed on a Shared iPad are global to the device and not per user.
- User-based Volume Purchase iBooks
  Apple supports assignment of user-based Volume Purchase iBooks on Shared iPads.

Resources that deploy over the user channel are:

- Device policies: Apps Notifications, Home Screen Layout, Restrictions, and Webclip.

  Citrix Endpoint Management supports only these device policies over the user channel.

When configuring device policies, you specify the deployment channel in the policy setting **Profile scope**.



To remove device policies that you deployed over the user channel, be sure to choose a **Deployment scope** of **User** for the Profile Removal policy.

General workflow

Typically, you provide preconfigured and supervised Shared iPads to device owners. Those individuals then distribute the devices to students or employees. If you don't distribute pre-enrolled Shared

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iPads: Be sure to provide the device owners with their Citrix Endpoint Management server passwords so they can enroll their devices.

The general workflow for configuring and enrolling Shared iPads is as follows.

1. Use the Citrix Endpoint Management server console to add ASM or ABM accounts (**Settings > Apple Deployment Program**) with **Shared mode** enabled. For more information, see "Manage accounts for Shared iPads"next.
2. As described in this section, add the required device policies, apps, and media to Citrix Endpoint Management. Assign those resources to delivery groups.
3. Have the device owners do a hard reset on the Shared iPads. The Remote Management screen for enrollment appears.
4. The device owners enroll the Shared iPads.
   Citrix Endpoint Management deploys configured resources to each enrolled Shared iPad. After an automatic restart, device owners can share the devices with users. A sign-in page appears on the iPad.
5. A device user enters their Managed Apple ID and temporary ASM password.
   The Shared iPad authenticates to ASM and prompts the user to create an ASM password. For the next sign into the Shared iPad, the device user provides the new ASM password.
6. Another device user who shares the iPad can then sign in by repeating the previous step.

Manage accounts for Shared iPads

If you already use Citrix Endpoint Management with Apple Education or Apple Business: You have an existing ASM/ABM account configured in Citrix Endpoint Management for devices that aren't shared, such as the devices used by device owners. You can use the same ASM/ABM account and the same Citrix Endpoint Management server for both shared and non-shared devices.

Organize Shared iPads into device groups

ASM/ABM lets you organize devices into groups by creating multiple MDM servers. When you assign the Shared iPads to an MDM server, create a device group for each group of Shared iPads:

- Group 1 of Shared iPads > Device Group 1 MDM Server
- Group 2 of Shared iPads > Device Group 2 MDM Server
- Group N of Shared iPads > Device Group N MDM Server

Add ASM accounts for each device group

When you create multiple ASM/ABM accounts from the Citrix Endpoint Management server console, you automatically import groups of Shared iPads:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Device Group 1 MDM Server > Device Group 1 account
- Device Group 2 MDM Server > Device Group 2 account
- Device Group N MDM Server > Device Group N account

Requirements specific to Shared iPads are as follows:

- One ASM/ABM account for each device group with these settings enabled:
  - **Require device enrollment**
  - **Supervised mode**
  - **Shared mode**
- For a given educational organization, be sure to use the same **Education suffix** for all ASM accounts.

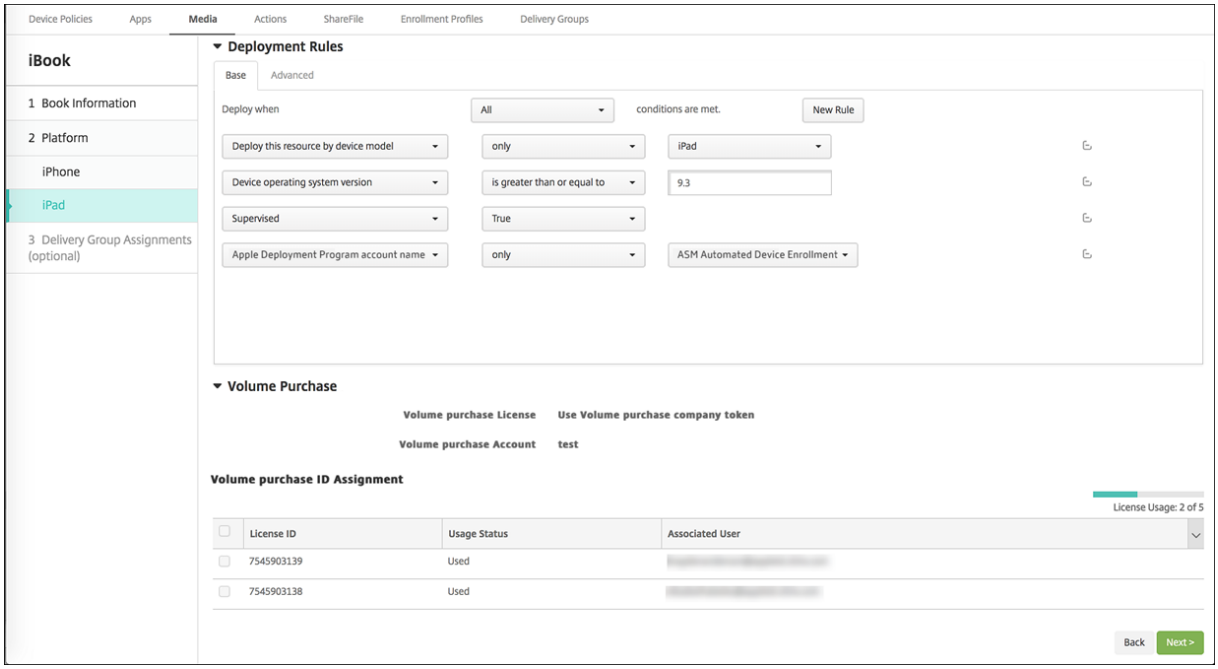
Apps for Shared iPads

Shared iPads support assignment of device-based Volume Purchase apps. Before deploying an app on a Shared iPad, Citrix Endpoint Management sends a request to the Apple Volume Purchase server to assign Volume Purchase licenses to the devices. To check the Volume Purchase assignments, go to **Configure > Apps > iPad** and expand **Volume Purchase**.

Media for Shared iPads

Shared iPads support assignment of user-based Volume Purchase iBooks. Before deploying iBooks on a Shared iPad, Citrix Endpoint Management sends a request to the Apple Volume Purchase server to assign Volume Purchase licenses to users. To check the Volume Purchase assignments, go to **Configure > Media > iPad** and expand **Volume Purchase**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Deployment rules for Shared iPads

For Shared iPad deployment, the rules at the delivery group level don't apply because they relate to user properties. To filter the policies, apps, and media for each group of devices: Add a deployment rule for the resources based on the account name. For example:

- For the Device Group 1 account, set this deployment rule:

```
Apple Deployment Program account name
Only
Device Group 1 account
```

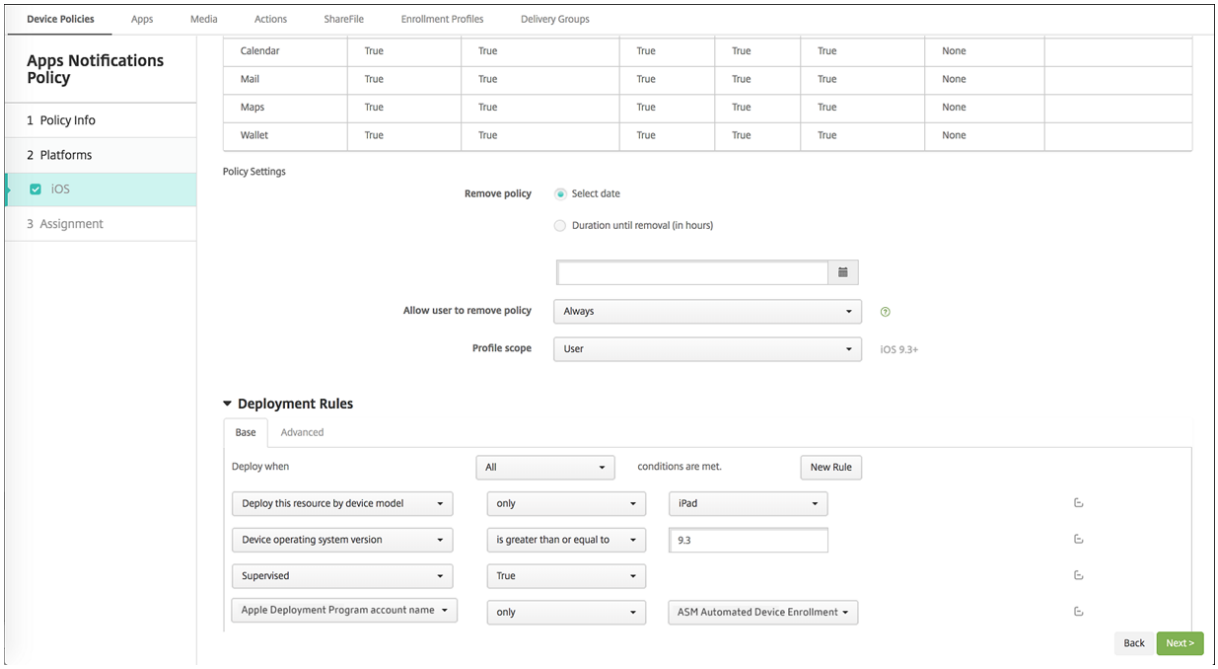
- For the Device Group 2 account, set this deployment rule:

```
Apple Deployment Program account name
Only
Device Group 2 account
```

- For the Device Group N account, set this deployment rule:

```
Apple Deployment Program account name
Only
Device Group N account
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.



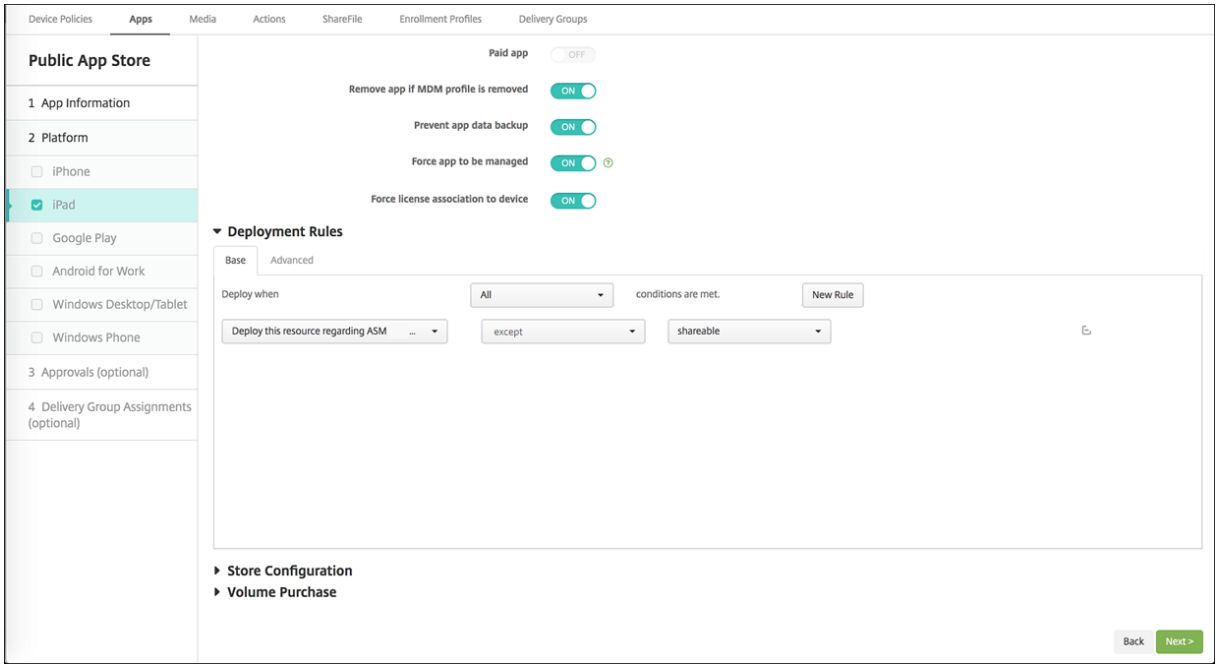
To deploy the Apple Classroom app only to device owners (using unshared iPads), filter the resources by ASM shared status with these deployment rules:

```
Deploy this resource regarding ASM/ABM shared mode
only
unshared
```

Or:

```
Deploy this resource regarding ASM/ABM shared mode
except
shareable
```

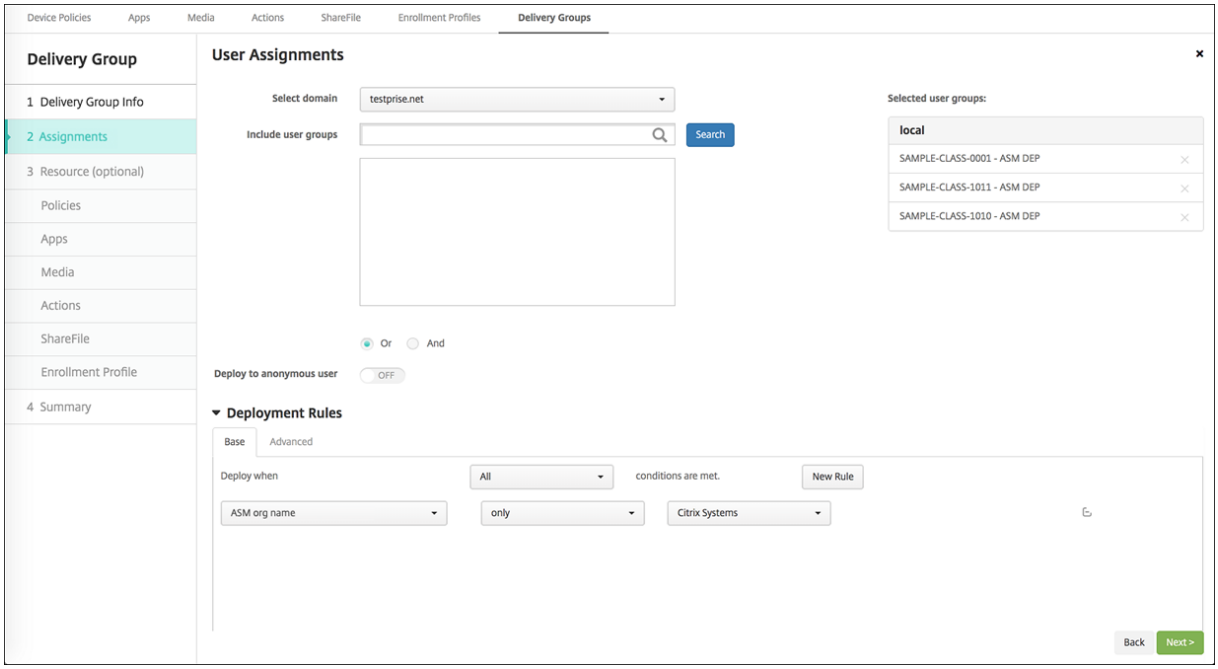
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Delivery groups for Shared iPads

For the device group:

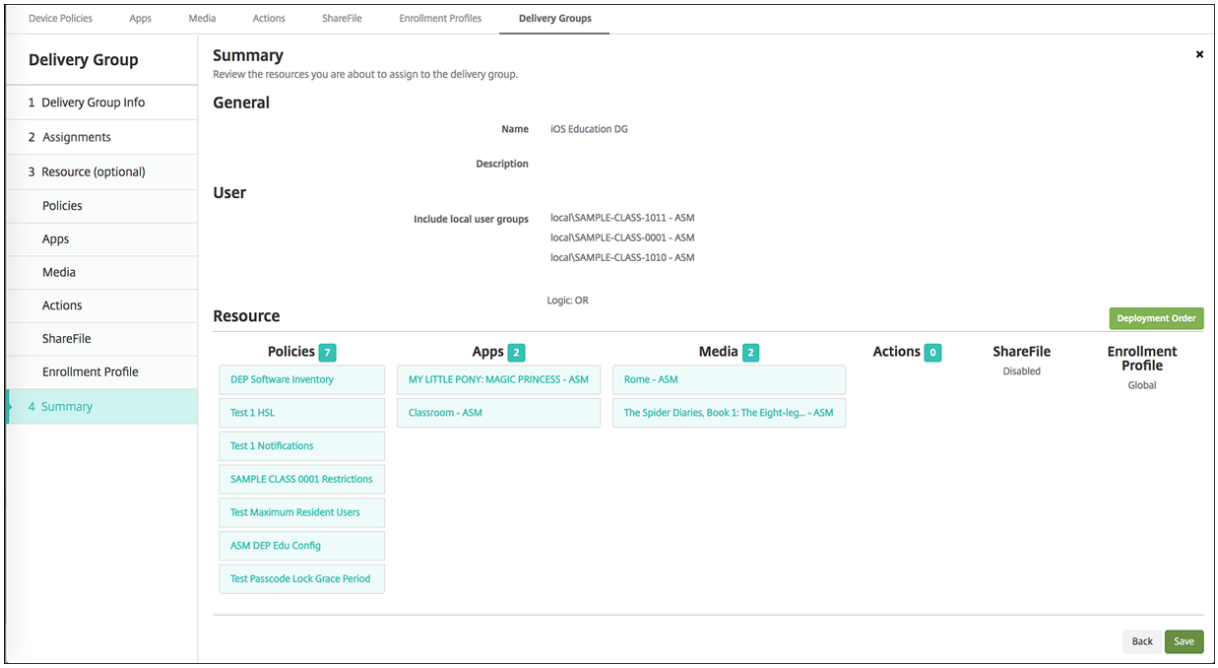
- Configure one delivery group. For instructors, assign all the classes that the Education Configuration policy defines.



- That delivery group must include these MDM resources:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Device policies:
  - Education Configuration (for ASM)
  - Lock Screen Message
  - Apps Notifications
  - Home Screen Layout
  - Restrictions
  - Maximum Resident Users
  - Passcode Lock Grace Period
- Required Volume Purchase apps
- Required Volume Purchase iBooks

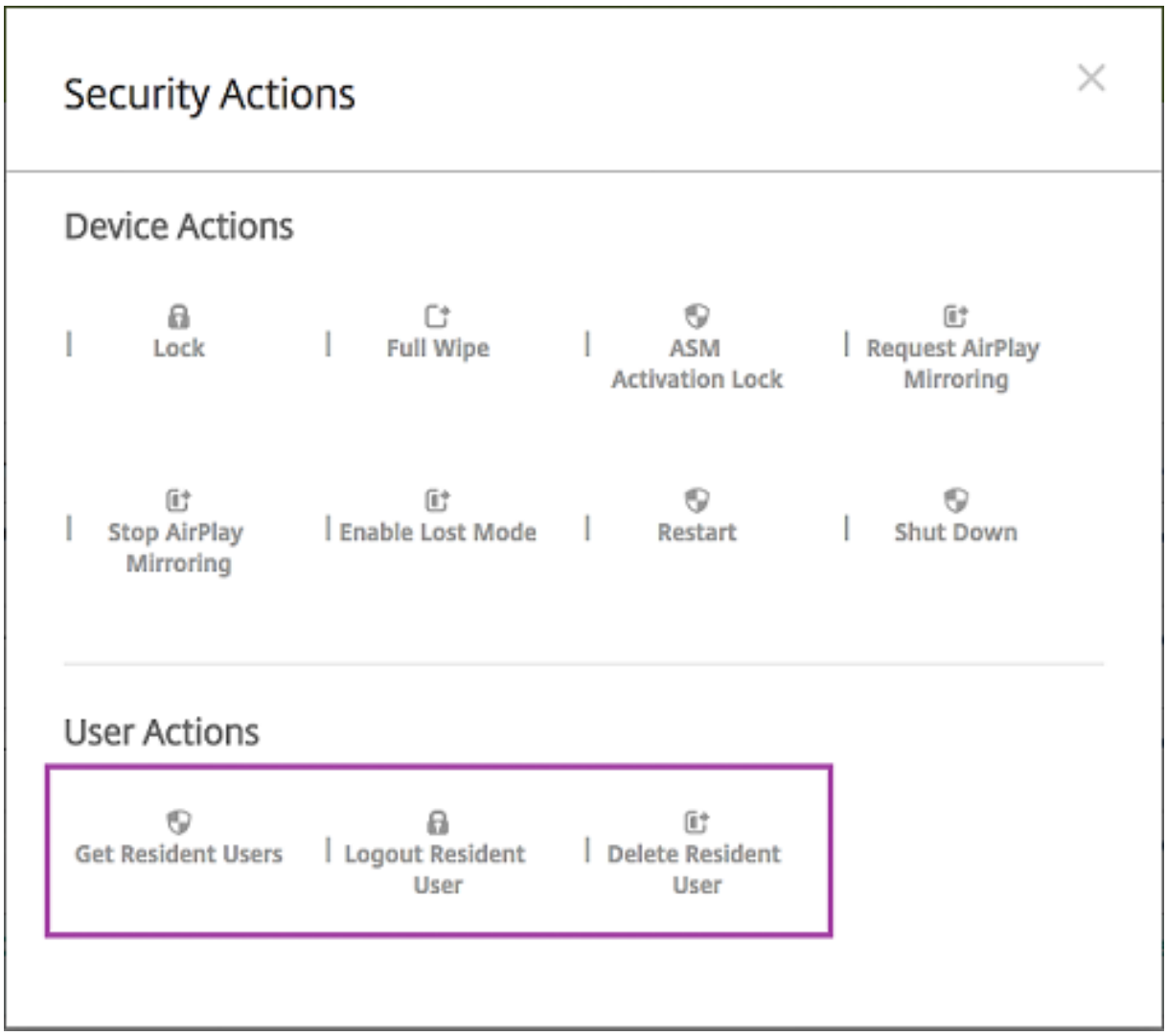


Security actions for Shared iPads

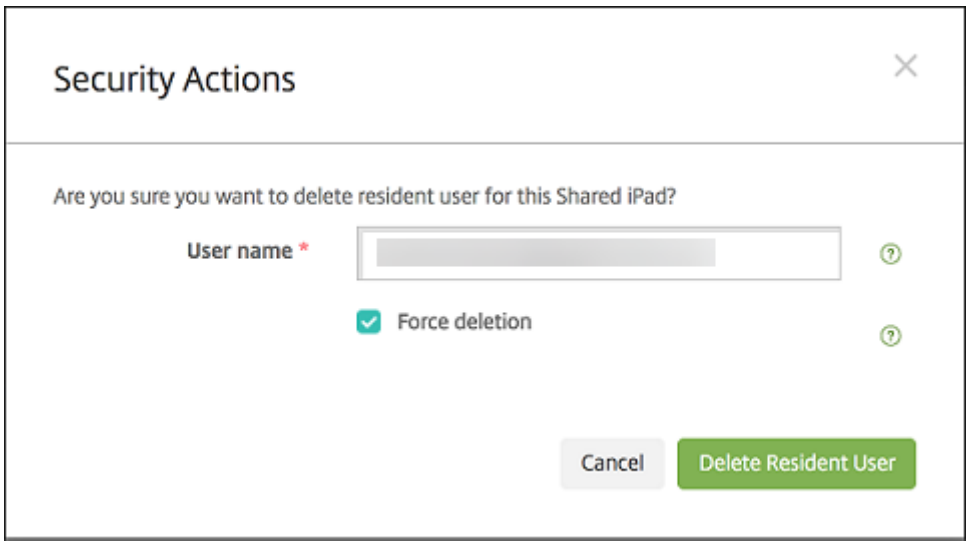
In addition to existing security actions, you can use these security actions for Shared iPads:

- **Get Resident Users:** Lists the users that have active accounts on the current device. This action forces a sync between the device and the Citrix Endpoint Management console.
- **Logout Resident User:** Forces a log out of the current user.
- **Delete Resident User:** Deletes the current session for a specific user. The user can sign in again.
- **Delete All Users:** Deletes all users on the device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



After you click **Delete Resident User**, you can specify the user name.



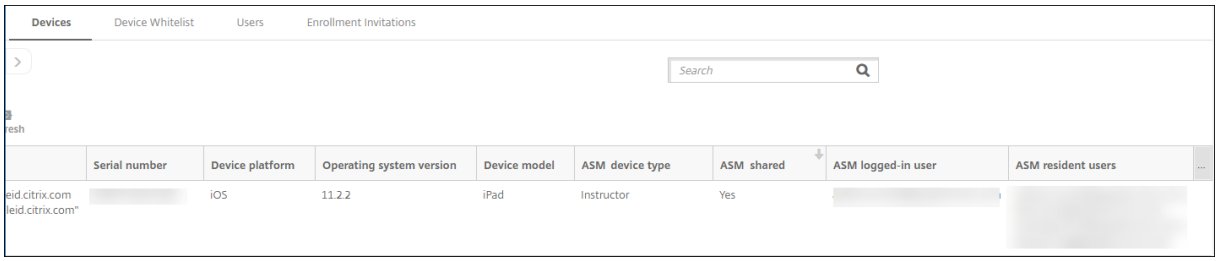
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Results of security actions appear on the **Manage > Devices > General** and **Manage > Devices > Delivery Groups** pages.

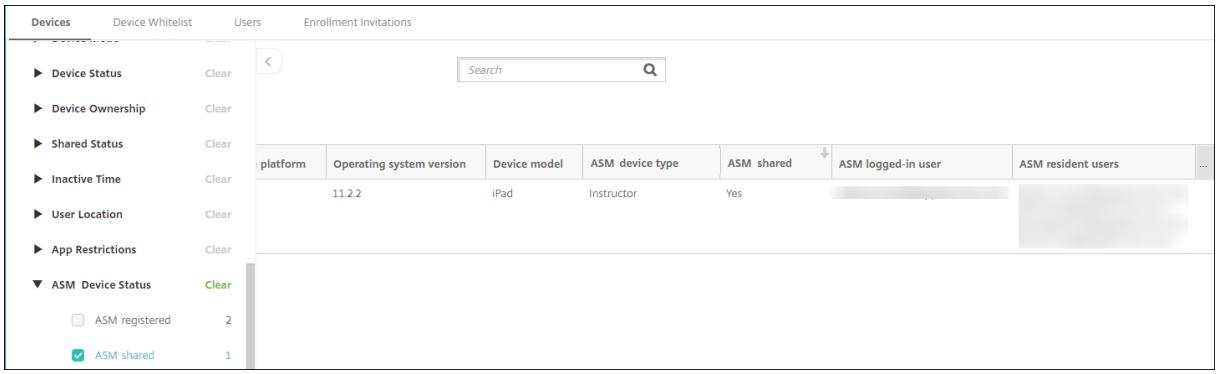
Get information about Shared iPads

Find information specific to Shared iPads on the **Manage > Devices** page:

- Look up:
  - Whether a device is shared (**ASM/ABM shared**)
  - Who is logged in to the shared device (**ASM/ABM logged-in user**)
  - All users assigned to the shared device (**ASM/ABM resident users**)

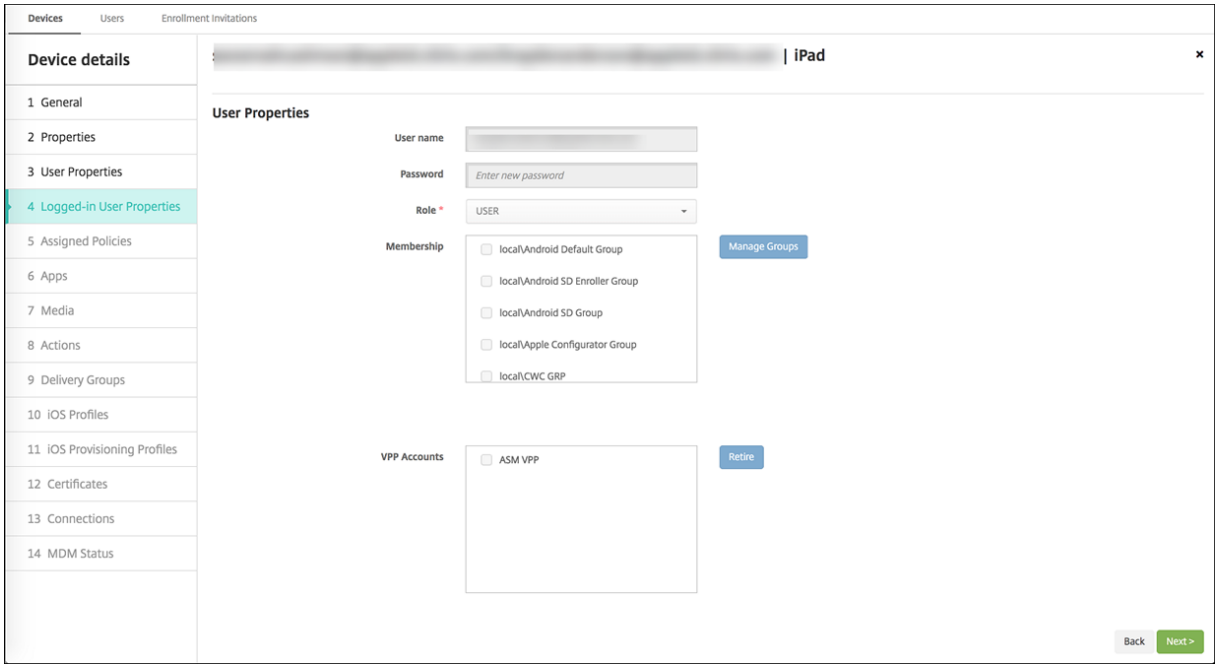


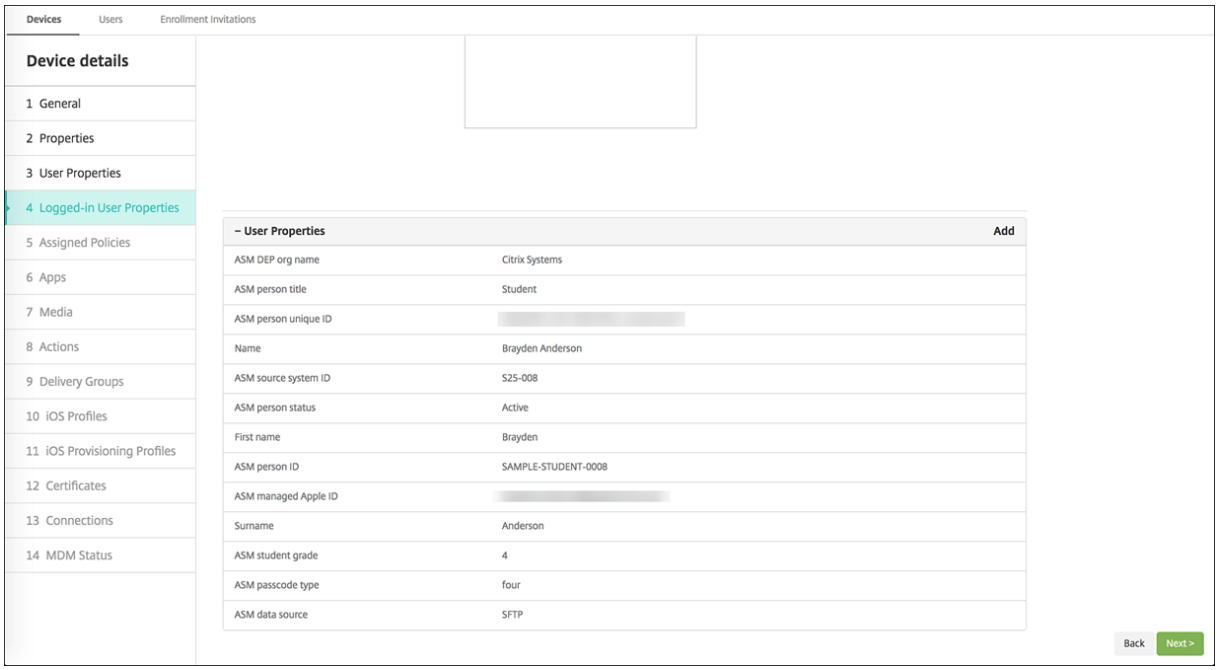
- Filter the device list by its **ASM/ABM Device Status:**



- View details about the user logged in to a Shared iPad, on the **Manage > Devices > Logged-in User Properties** page.

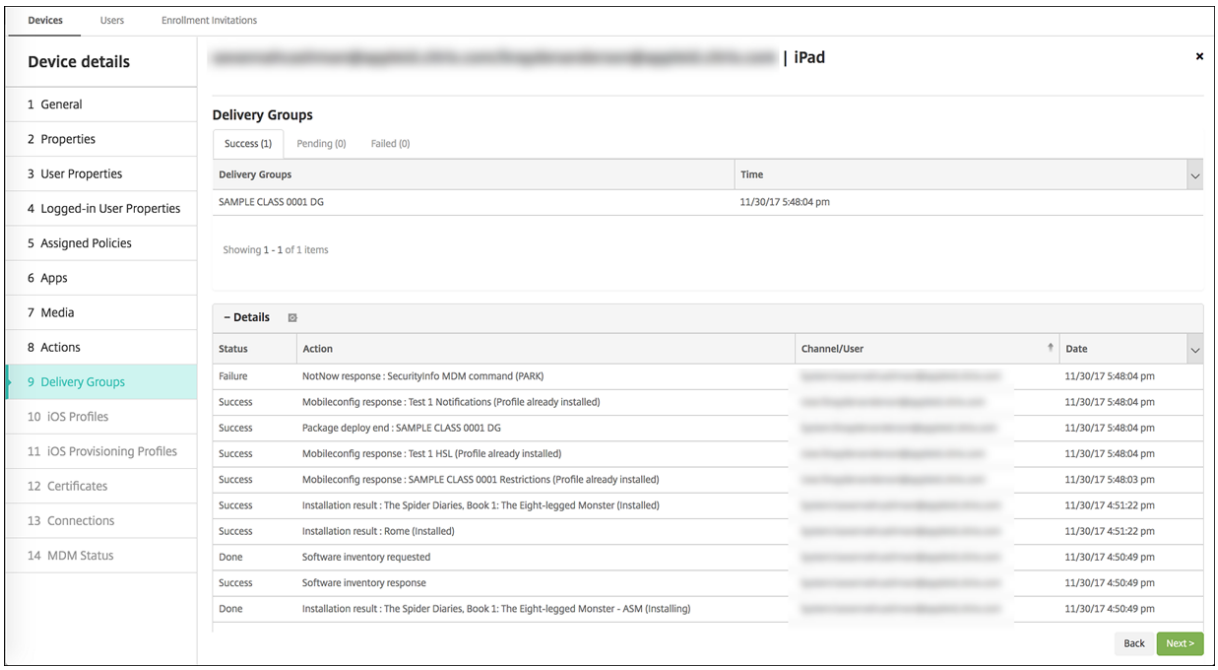
© 1997–2025 Citrix Systems, Inc. All rights reserved.



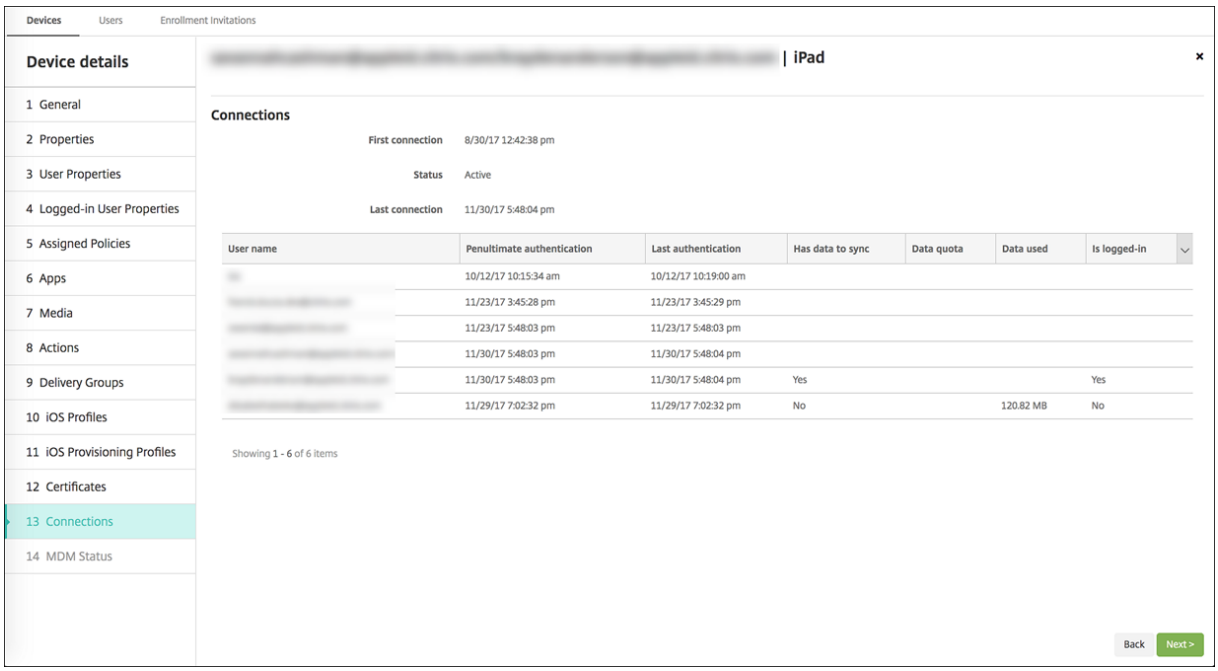


- See the channel used to deploy resources to device owners and users in a delivery group on the **Manage > Devices > Delivery Groups** page. The **Channel/User** column shows the type (**System** or **User**) and the recipient.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

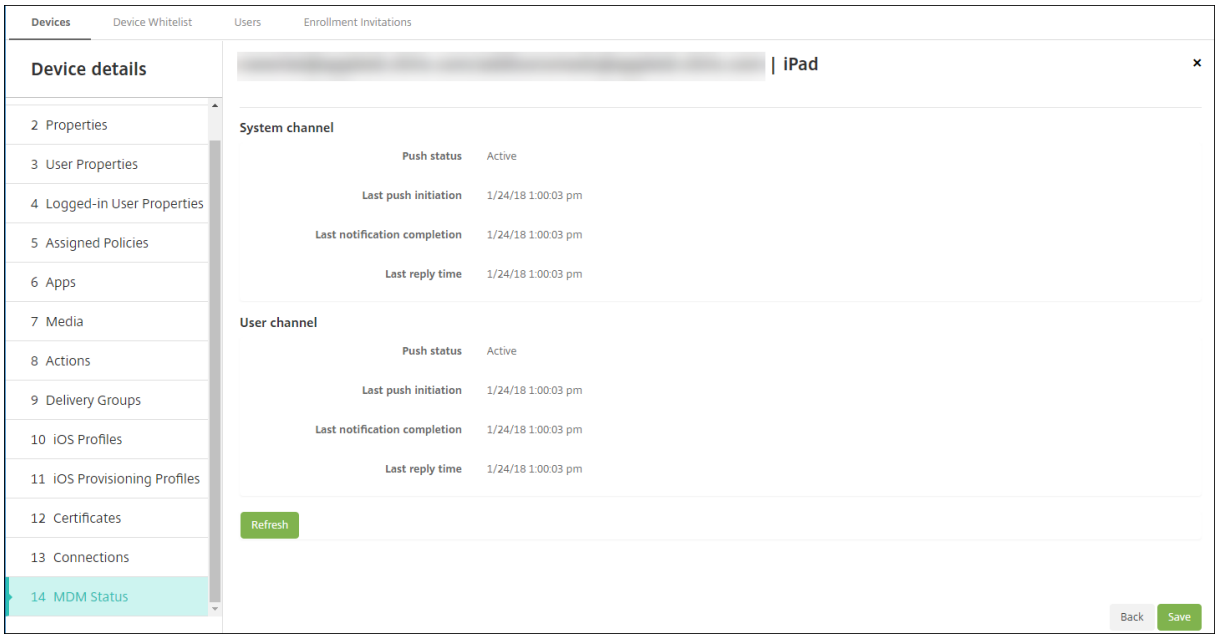


- Get information about resident users:
  - **Has data to sync:** Whether the user has data to be synchronized to the cloud.
  - **Data quotas:** The data quota set for the user in bytes. A quota might not appear if user quotas are temporarily off or aren't enforced for the user.
  - **Data used:** The amount of data used by the user in bytes. A value might not appear if an error occurs as the system gathers the information.
  - **Is logged in:** Whether the user is logged on to the device.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

- View the push status for both channels.



Distribute Apple apps

September 6, 2025

Citrix Endpoint Management manages apps deployed to devices. You can organize and deploy the following types of iOS/iPadOS and macOS apps.

- **Public App Store (iOS/iPadOS only):** These apps include free or paid apps available in a public app store, such as the Apple App Store or Google Play. For example, GoToMeeting.
- **Enterprise (iOS/iPadOS/macOS):** Native apps that aren't MDX-enabled and don't have the policies associated with MDX apps.
- **MDX (iOS/iPadOS only):** Apps prepared with the MAM SDK or wrapped with the MDX Toolkit. These apps include MDX policies. You get MDX apps from internal sources and public stores.
- **Volume Purchase (iOS/iPadOS/macOS):** Apps with licenses managed through the Apple Volume Purchase program.
- **iOS custom apps (iOS/iPadOS only):** Proprietary business-to-business apps developed in-house or by a third-party.

For more information about different types of apps, see Add apps.

Some deployments require an Apple Business Management (ABM) or Apple School Management (ASM) account. See the following sections for more information.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For each type of app and distribution method, Citrix recommends a set of configuration practices. For information about distributing apps for other platforms, see Add Apps. The following sections provide more in-depth information for iOS app configuration.

General steps for app distribution

Scenario	Step 1: Link accounts	Step 2: Add and configure apps	Step 3: Configure delivery groups and deploy apps
Public app store apps, including Citrix mobility apps	Not applicable	**In Citrix Endpoint Management: Configure > Apps**, add **Public App Store** apps for iPhone or iPad. Configure the apps and assign them to delivery groups.	**In Citrix Endpoint Management:** Configure and deploy apps using delivery groups.
Public app store apps delivered with Apple Volume Purchase, including Citrix mobility apps	Enroll in an Apple deployment program. **In Citrix Endpoint Management:** Go to **Settings > Volume Purchase** to add your Volume Purchase account.	**In ABM or ASM:** Purchase and add apps from Apps and Books. **In Citrix Endpoint Management:** Go to **Configure > Apps**, configure the apps, and assign them to delivery groups.	**In Citrix Endpoint Management:** Configure and deploy apps using delivery groups.
Enterprise apps	Not applicable	**In Citrix Endpoint Management:** Go to **Configure > Apps**. Click **Add** then click **Enterprise**. Upload the IPA file. Configure the apps and assign them to delivery groups.	**In Citrix Endpoint Management:** Configure and deploy apps using delivery groups.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Scenario	Step 1: Link accounts	Step 2: Add and configure apps	Step 3: Configure delivery groups and deploy apps
MDX apps	Not applicable	**In Citrix Endpoint Management:** Go to **Configure > Apps**. Click **Add** then click **MDX**. Make sure that you select **iPad**/**iPhone** for the platform. Upload the MDX file. Configure the apps and assign them to delivery groups.	**In Citrix Endpoint Management:** Configure and deploy apps using delivery groups.
MDX apps distributed using Apple Volume Purchase	Enroll in an Apple deployment program. **In Citrix Endpoint Management:** Go to **Settings > Volume Purchase** to add your Volume Purchase account.	**In ABM:** Purchase and add MDX apps from Apps and Books. Link the app to your ABM account. **In Citrix Endpoint Management:** Go to **Configure > Apps**, configure the apps, and assign them to delivery groups.	**In Citrix Endpoint Management:** Configure and deploy apps using delivery groups.
Custom apps	Enroll in an Apple deployment program. **In Citrix Endpoint Management:** Go to **Settings > Volume Purchase** to add your Volume Purchase account.	**In ABM:** Add your app to the App Store as a private app. Link the app to your ABM account. **In Citrix Endpoint Management:** Go to **Configure > Apps**, configure the apps, and assign them to delivery groups.	**In Citrix Endpoint Management:** Configure and deploy apps using delivery groups.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Scenario	Step 1: Link accounts	Step 2: Add and configure apps	Step 3: Configure delivery groups and deploy apps
MDX-enabled custom apps	Enroll in an Apple deployment program. **In Citrix Endpoint Management:** Go to **Settings > Volume Purchase** to add your Volume Purchase account.	**In ABM:** Add your app to the app store as a private app. Link the app to your ABM account. **In Citrix Endpoint Management:** Go to **Configure > Apps** and upload the MDX file. Configure the apps and assign them to delivery groups.	**In Citrix Endpoint Management:** Configure and deploy apps using delivery groups.

Public app store apps

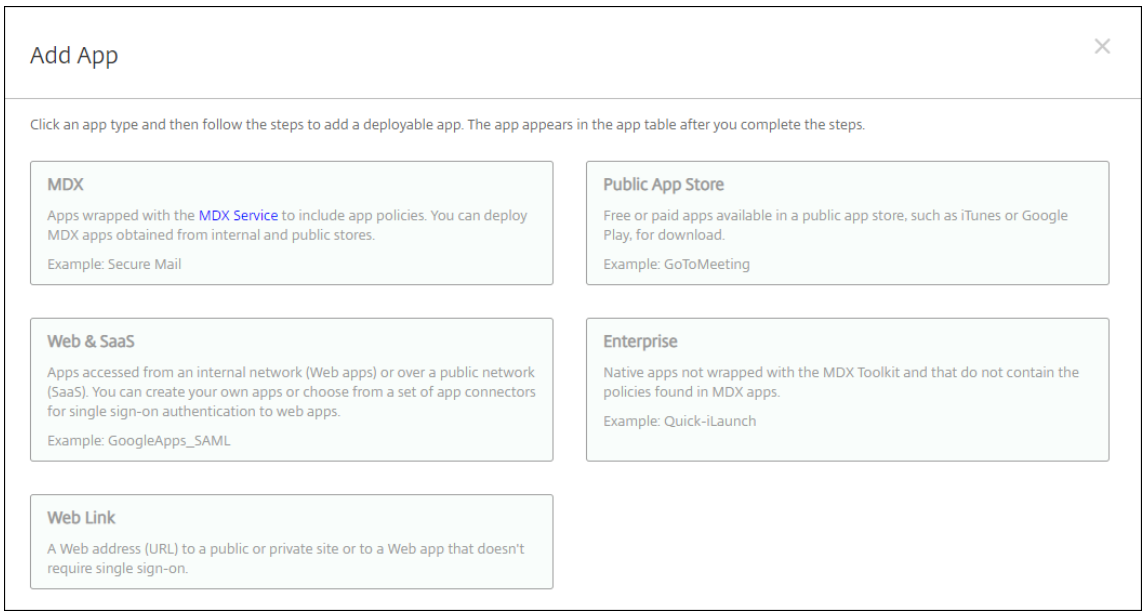
You can add free and paid apps available on the App Store to Citrix Endpoint Management.

Feature availability	
Requires device supervision	No
Available for user enrollment mode	No
Available on	iOS/iPadOS

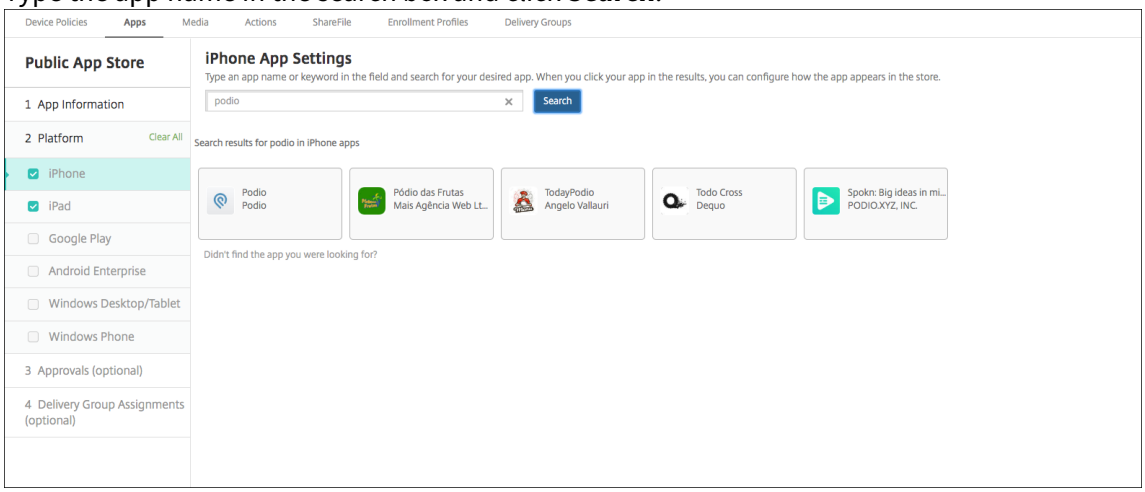
Step 1: Add and configure apps

1. In the Citrix Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.
2. Click **Public App Store**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Select **iPhone** or **iPad** for platforms
4. Type the app name in the search box and click **Search**.

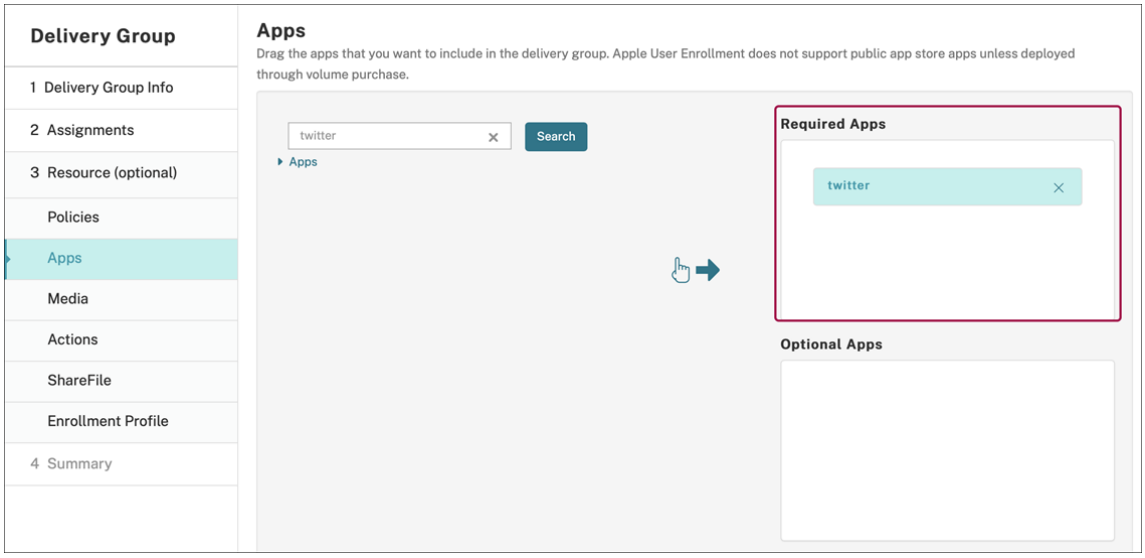


5. Apps matching the search criteria appear. Click the desired app.
6. Assign a delivery group to the app and click **Save**.

Step 2: Configure app deployment

1. In the Citrix Endpoint Management console, navigate to **Configure > Apps**.
2. Select the app that you want to configure and click **Edit**.
3. Citrix® recommends enabling the **Force app to be managed** feature.
4. Assign any delivery groups and click **Save**.
5. Navigate to **Configure > Delivery Groups** and click **Add**.
6. In the **Apps** section, drag the desired apps to the **Required Apps** box.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



7. Navigate back up to **Configure > Delivery Groups**.
8. Select the delivery group and click **Deploy**.
9. Users receive a request to install the app and the app installs in the background after they accept.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Public app store apps delivered with Apple Volume Purchase

You can manage iOS/iPadOS app licenses through the Apple Volume Purchase program. Follow these steps to add Volume Purchase apps to Citrix Endpoint Management.

Feature availability	
Requires device supervision	No
Available for user enrollment mode	Yes
Available on	iOS/iPadOS/macOS

Step 1: Link accounts

1. Set up and enroll in Apple Business Manager (ABM) or Apple School Manager (ASM). For more information about these programs, see the Apple documentation.
2. Link your ABM/ASM account with Citrix Endpoint Management. For more information on linking Volume Purchase accounts, see Apple Volume Purchase.
3. When you add your Volume Purchase account, enable **App Auto Update**. This setting makes sure that apps on user devices automatically update when an update appears in the Apple store. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens regardless of whether the app is required or optional.

   To use the **Force app to be managed** and **App Auto Update** settings, enable the `apple.app.force.managed` server property. See Server properties.

Step 2: Get apps and licenses from Apple

Purchase the apps on your ABM/ASM account. You can make purchases in Apple Books (for iOS/iPadOS only) and the Apple App Store. Keep in mind that you must buy all apps, even if they are free. Once you buy licenses on ABM/ASM, Citrix Endpoint Management shows the app automatically.

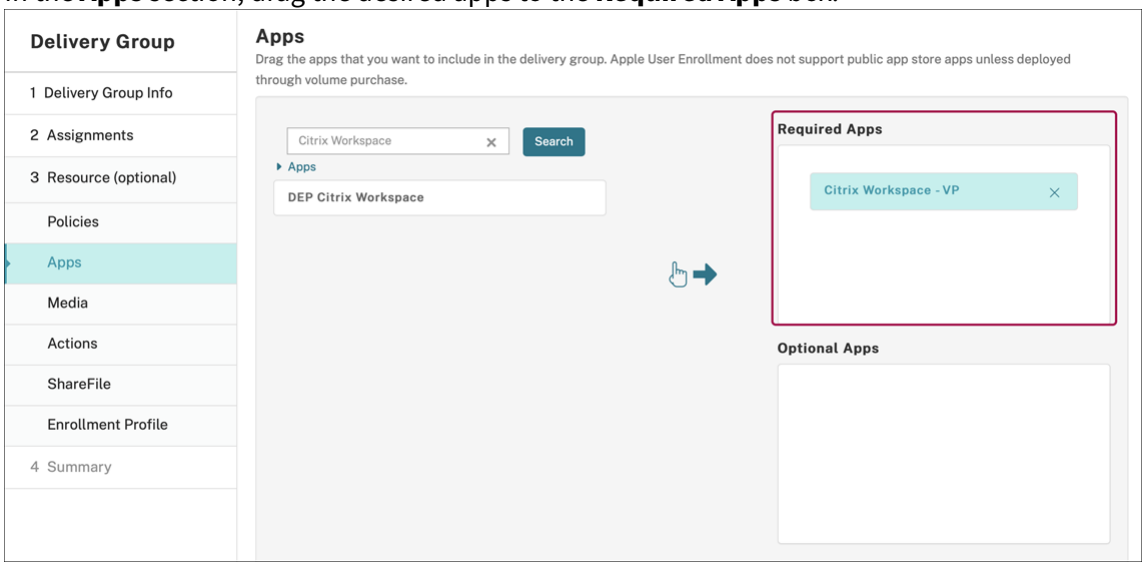
For information about how to make apps available to your business, see the Apple documentation.

Step 3: Configure app deployment

1. In the Citrix Endpoint Management console, navigate to **Configure > Apps**.
2. Select the Volume Purchase app that you want to configure and click **Edit**.
3. Select the platforms: **iPhone**, **iPad**, or **macOS**.
4. Citrix recommends enabling the **Force app to be managed** feature (iOS/iPadOS only).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. Assign any delivery groups and click **Save**.
6. Navigate to **Configure > Delivery Groups** and click **Add**.
7. In the **Apps** section, drag the desired apps to the **Required Apps** box.



8. Navigate back to **Configure > Delivery Groups**.
9. Select the delivery group and click **Deploy**.
10. Users receive a request to install the app and the app installs in the background after they accept.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

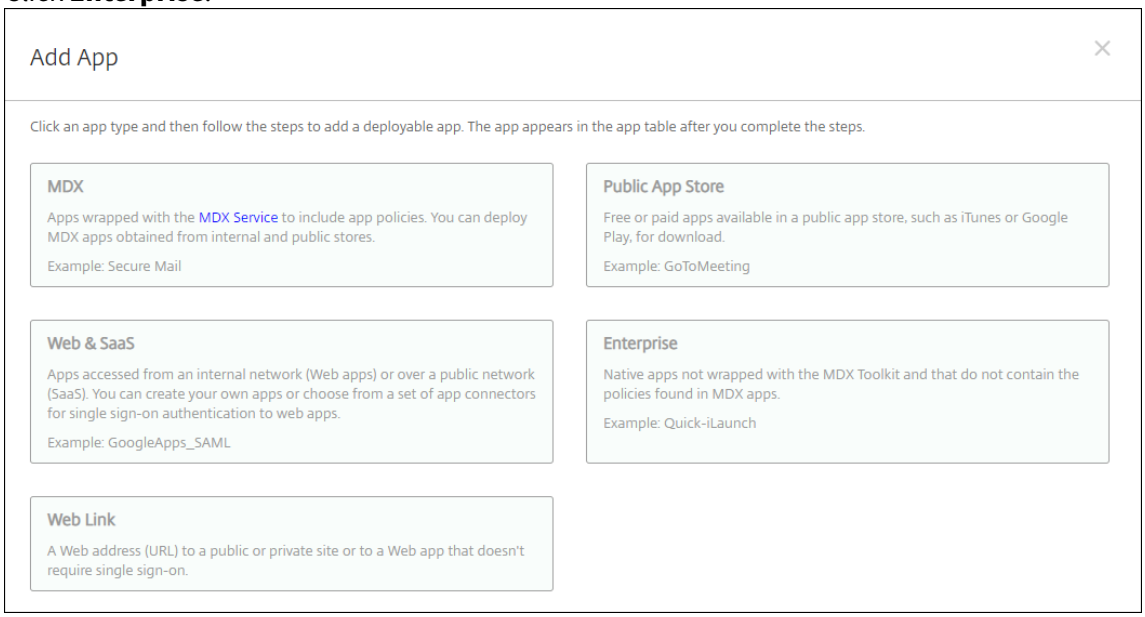
Enterprise apps

You can also add native apps that don't have any MDX policies associated with them. Follow these steps to add apps that don't exist on the App Store.

Feature availability	
Requires device supervision	No
Available for user enrollment mode	Yes
OS	iOS/iPadOS/macOS

Step 1: Add and configure apps

1. In the Citrix Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.
2. Click **Enterprise**.



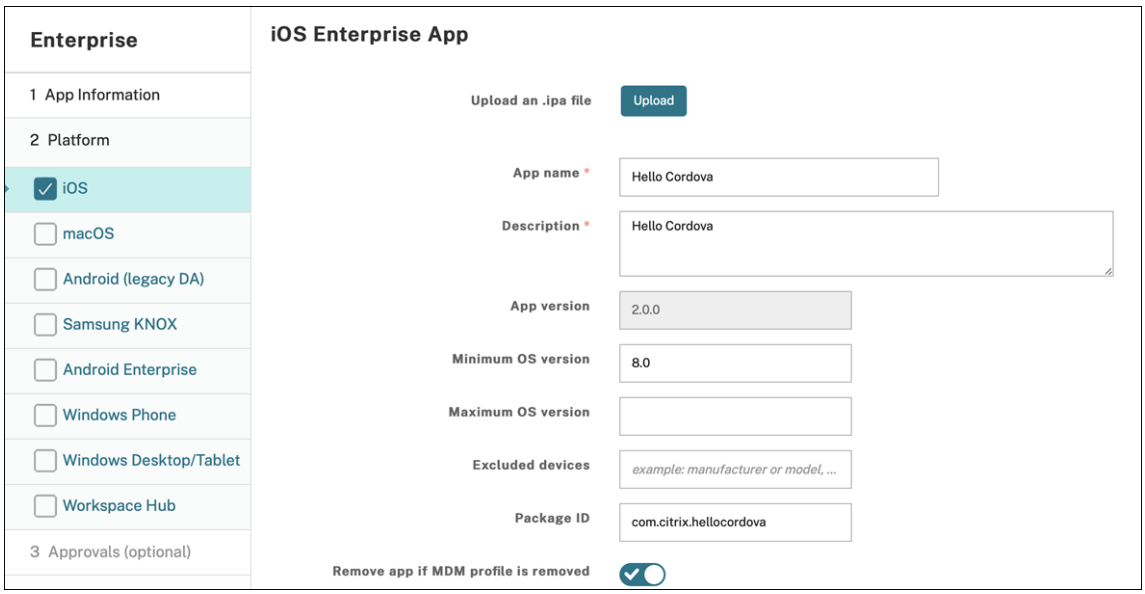
3. On the **App information** page, configure the following:
   - **Name:** Type a descriptive name for the app. The name appears under App Name on the Apps table.
   - **Description:** Type an optional description of the app.
   - **App category:** Optionally, in the list, click the category to which you want to add the app.
4. Click **Next**. The **App Platforms** page appears.
5. Select the platforms: **iPhone**, **iPad**, or **macOS**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

6. Upload the IPA file (iOS/iPadOS) or upload the PKG file (macOS)
7. Click **Next**. The **App details** page appears.
8. Configure these settings:

    - **File name:** Optionally, type a new name for the app.
    - **App description:** Optionally, type a new description for the app.
    - **App version:** You can't change this field.
    - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
    - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
    - **Excluded devices:** Optionally, type the manufacturer or models of devices that can't run the app.
    - **Remove app if MDM profile is removed:** Select whether to remove the app from a device when the MDM profile is removed. The default is On. (iOS/iPadOS only)
    - **Prevent app data backup:** Select whether to prevent the app from backing up data. The default is On. (iOS/iPadOS only)
    - **Force app to be managed:** If you install an unmanaged app, select **On** if you want users on unsupervised devices see a prompt to allow management of the app. If they accept the prompt, the app is managed. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens regardless of whether the app is required or optional. (iOS/iPadOS only)

    To use the **Force app to be managed** and **App Auto Update** settings, enable the `apple.app.force.managed` server property. See Server properties.

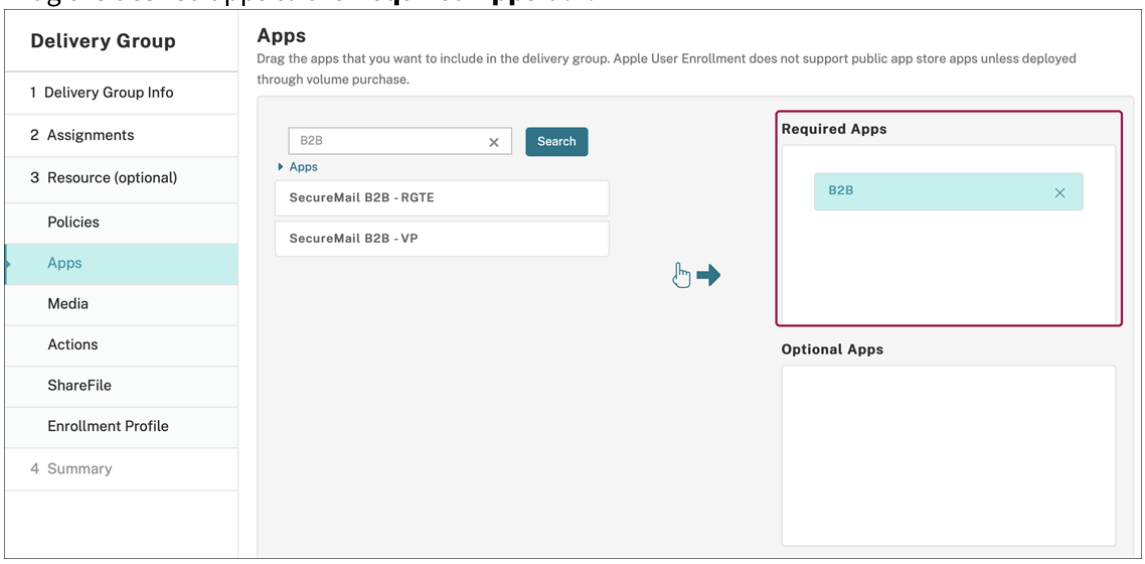


9. Assign a delivery group to the app and click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Step 2: Configure app deployment

1. In the Citrix Endpoint Management console, navigate to **Configure > Delivery Groups**. Select the delivery group to configure and click the **Apps** page.
2. Drag the desired apps to the **Required Apps** box.



3. Navigate to **Configure > Delivery Groups**.
4. Select the delivery group and click **Deploy**.
5. Users receive a request to install the app and the app installs in the background after they accept.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

MDX apps

To use MDX policies and security features, add apps that are MAM SDK enabled or MDX-wrapped. You can deploy MDX apps using Volume Purchase or without it.

Feature availability	
Requires device supervision	No
Available for user enrollment mode	Yes
Available On	iOS/iPadOS

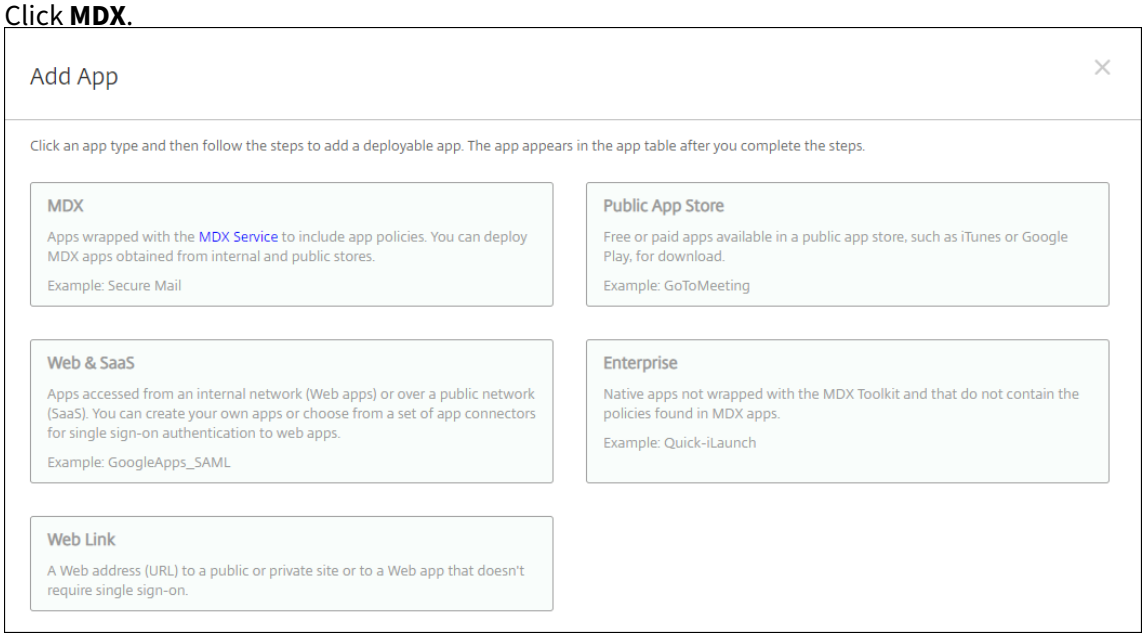
To add the MDX version of a public app store app, follow the steps under Public app store apps, and then follow the steps in this section.

Step 1: Add and configure apps

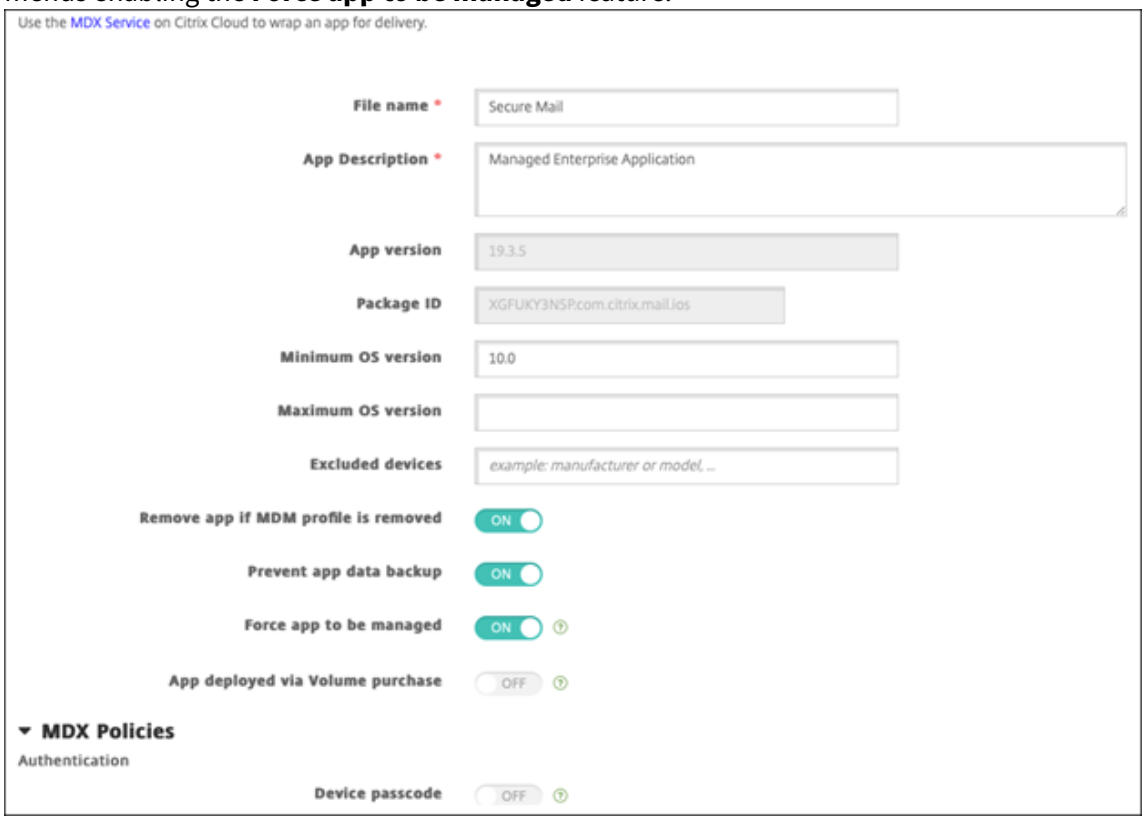
1. In the Citrix Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Click **MDX**.

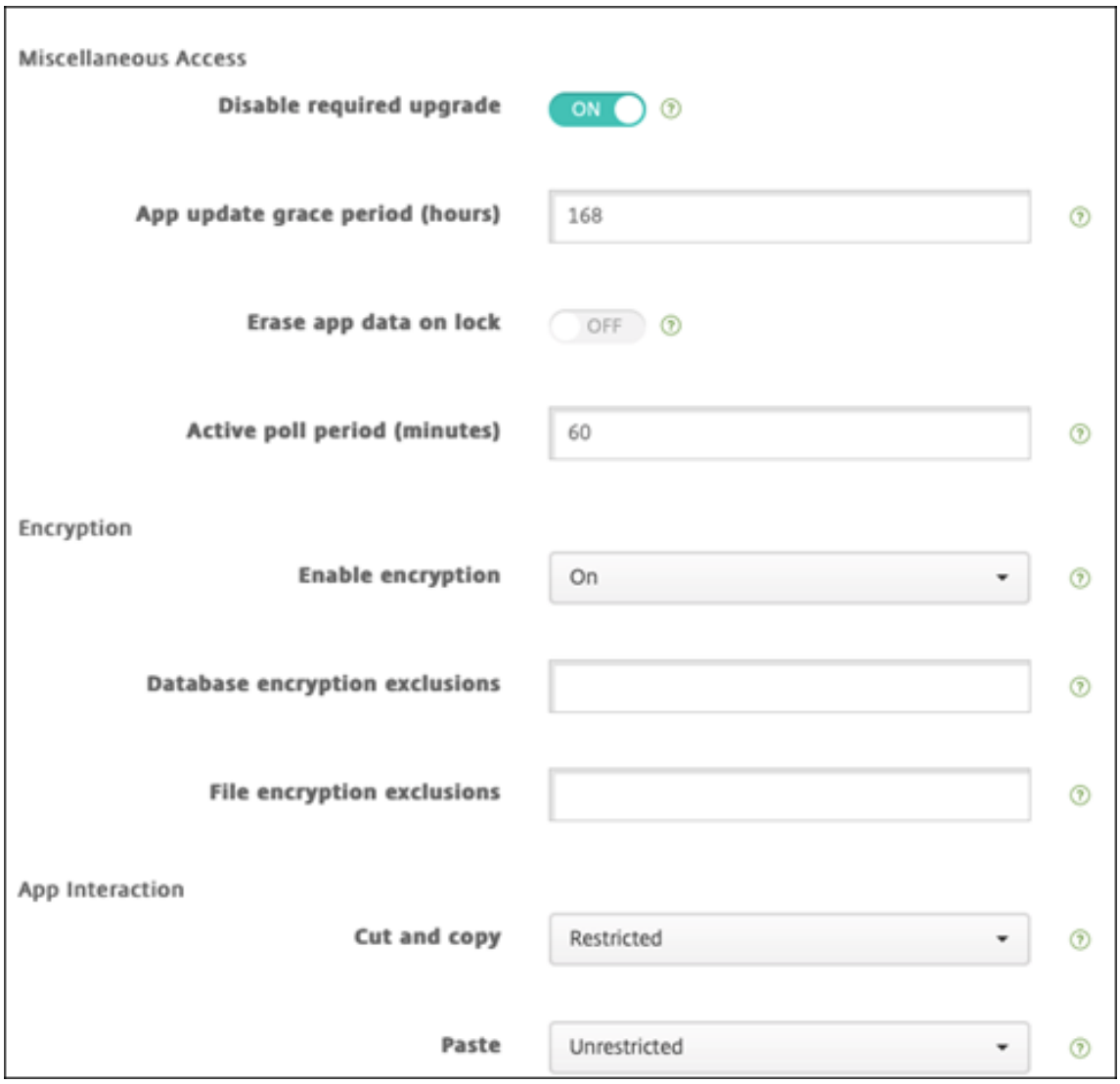


3. Select **iPhone** or **iPad** for platforms.
4. Upload the MDX file.
5. Configure the app details. Set **App deployed via Volume Purchase** to **Off**. Citrix also recommends enabling the **Force app to be managed** feature.



6. Configure the MDX policies. Set **Disable required upgrade** to **On**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

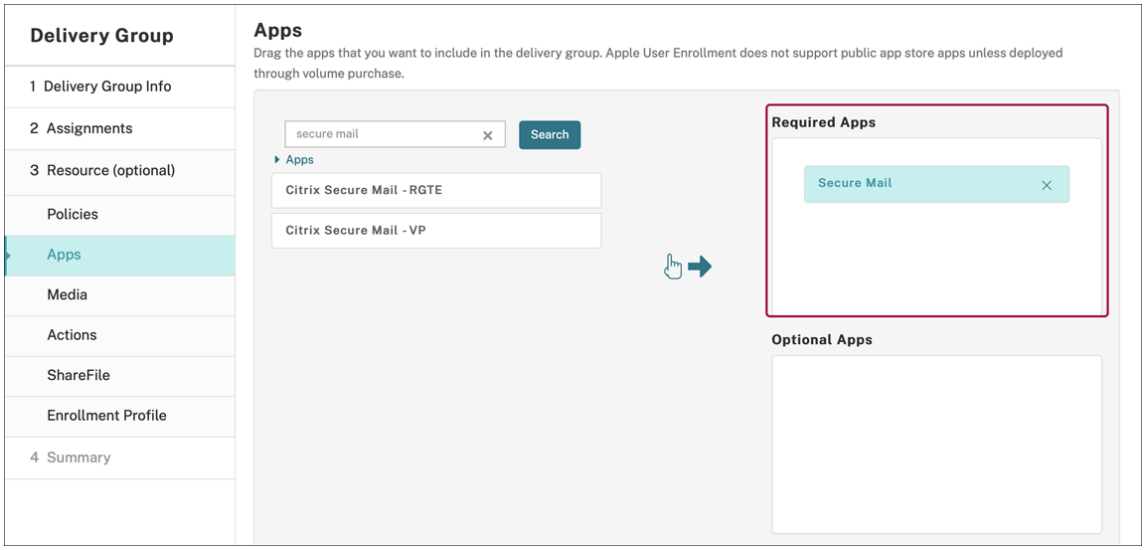


7. Assign a delivery group to the app and click **Save**.

Step 2: Configure app deployment

1. In the Citrix Endpoint Management console, navigate to **Configure > Delivery Groups** and click **Add**.
2. In the **Apps** section, drag the desired apps to the **Required Apps** box.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Navigate to **Configure > Delivery Groups**.
4. Select the delivery group and click **Deploy**.
5. Users receive a request to install the app and the app installs in the background after they accept.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

MDX apps distributed using Apple Volume Purchase

To use MDX policies and security features, add apps that are MAM SDK enabled or MDX-wrapped. To deploy apps using Volume Purchase, the apps must exist on the app store.

Feature availability	
Requires device supervision	No
Available for user enrollment mode	Yes
Available on	iOS/iPadOS

Step 1: Link accounts

1. Set up and enroll in Apple Business Manager (ABM) or Apple School Manager (ASM). For more information about these programs, see the Apple documentation.
2. Link your ABM/ASM account with Citrix Endpoint Management. For more information on linking Volume Purchase accounts, see Apple Volume Purchase.
3. When you add your Volume Purchase account, enable **App Auto Update**. This setting makes sure that the apps on user devices automatically update when an update appears in the Apple store. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens regardless of whether the app is required or optional.

   To use the **Force app to be managed** and **App Auto Update** settings, enable the `apple.app.force.managed` server property. See Server properties.

Step 2: Get apps and licenses from Apple

Purchase the apps on your ABM/ASM account. You can make purchases in Apple Books (for iOS/iPadOS only) and the Apple App Store. Keep in mind that you must buy all apps, even if they are free. Once you buy licenses on ABM/ASM, Citrix Endpoint Management shows the app automatically.

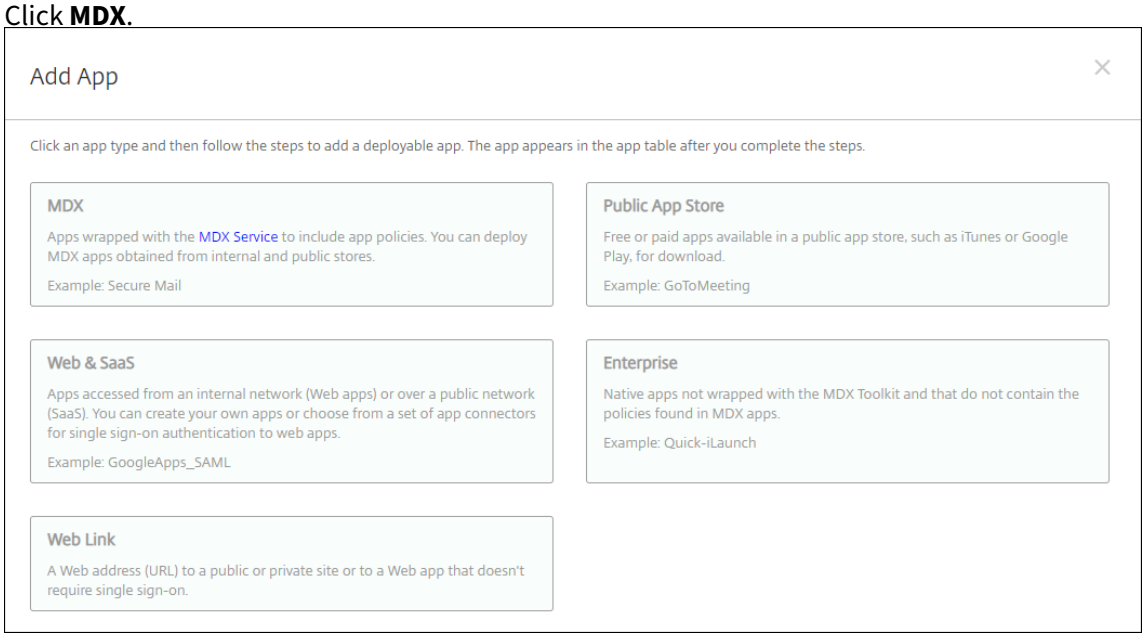
For information about how to make apps available to your business, see the Apple documentation.

Step 3: Add and configure apps

1. In the Citrix Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.

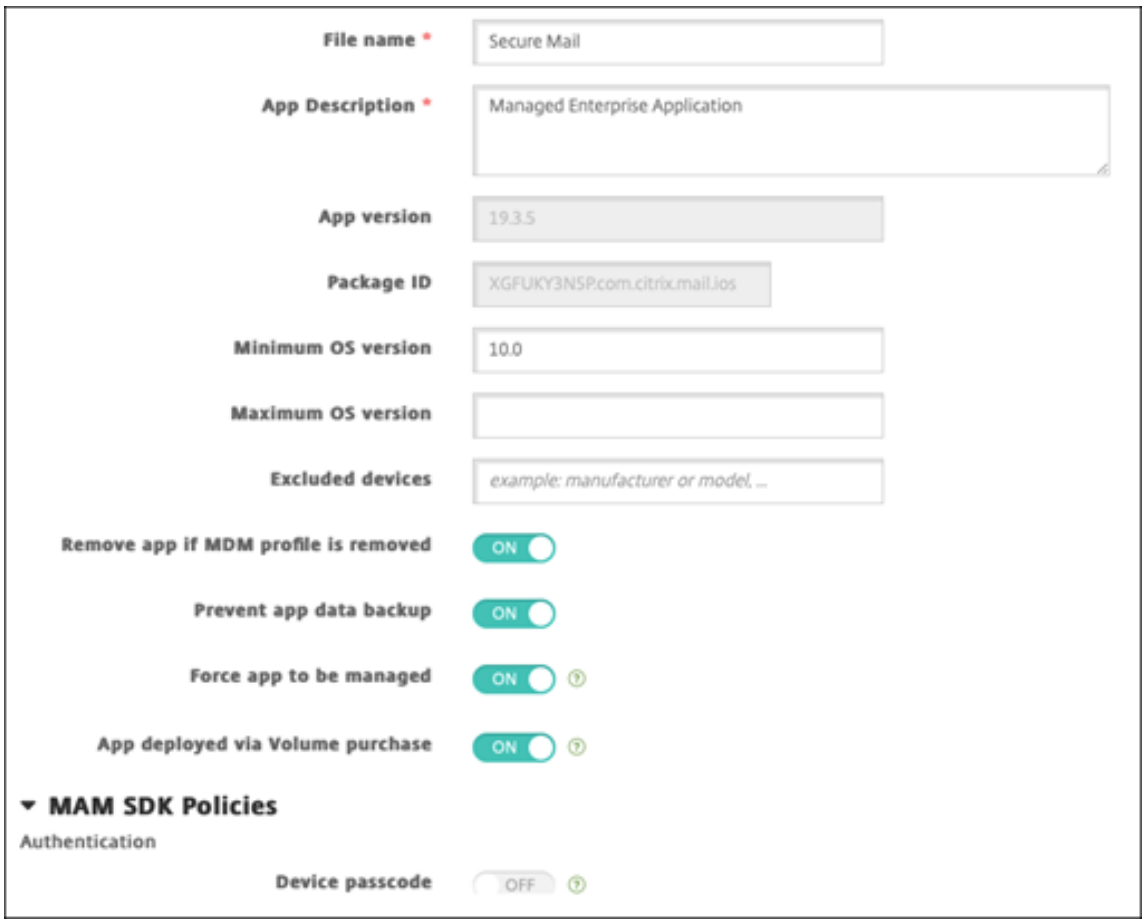
© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Click **MDX**.



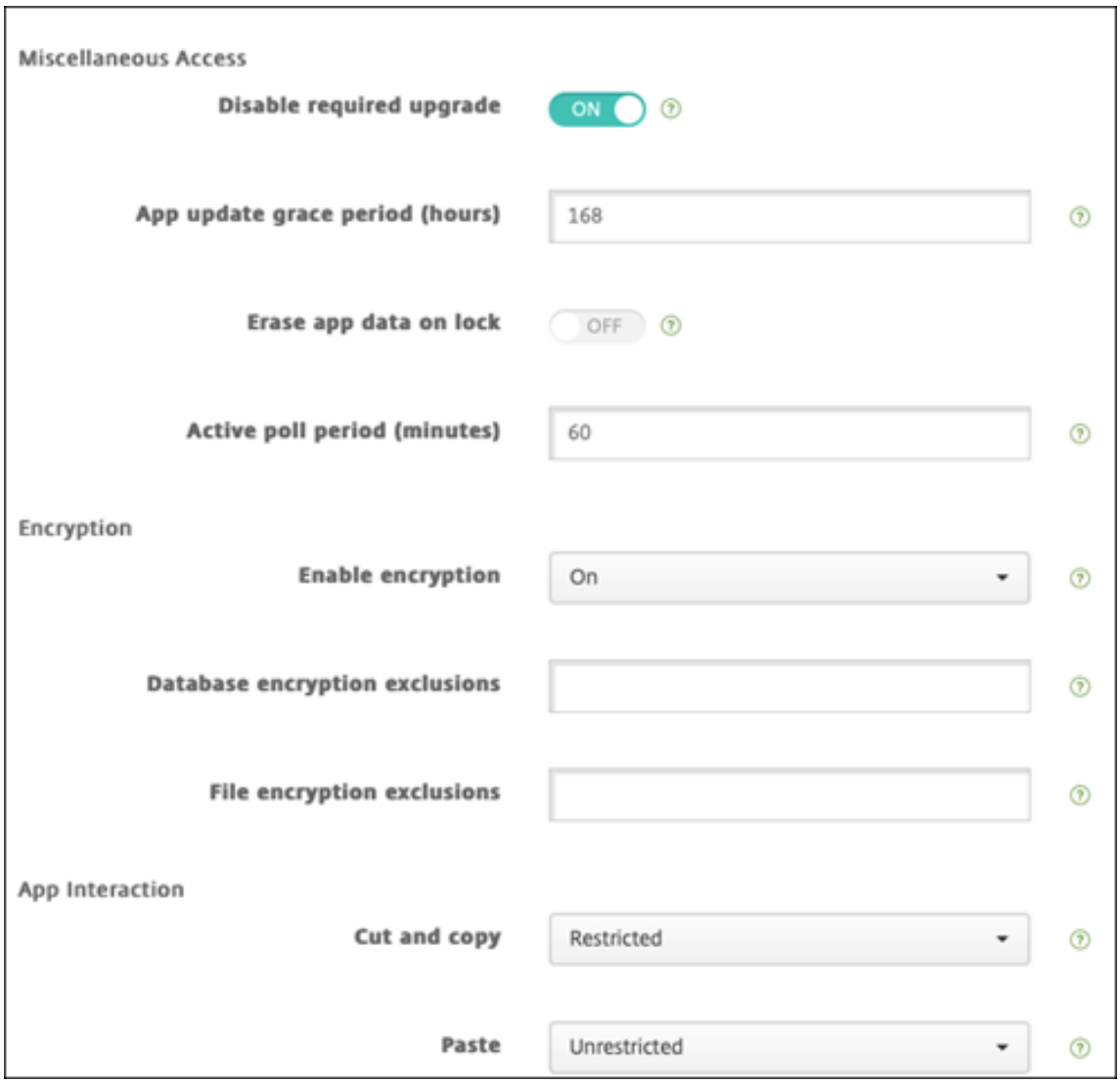
3. Select **iPhone** or **iPad** for platforms.
4. Upload the MDX file.
5. Configure the app details. Set **App deployed via Volume Purchase** to **On**. Citrix also recommends enabling the **Force app to be managed** feature.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. Configure the MDX policies. Set **Disable required upgrade** to **On**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



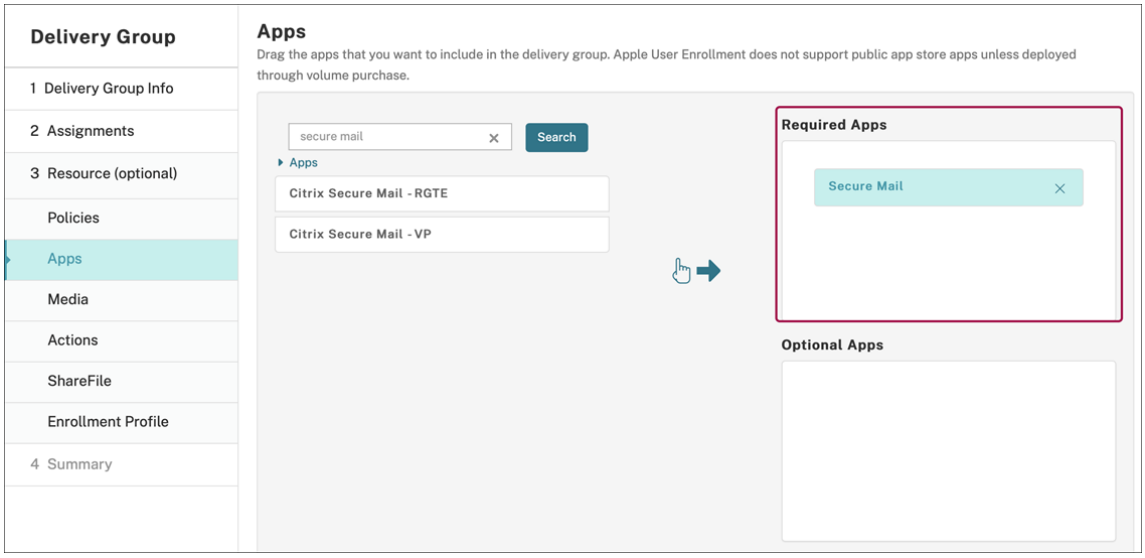
7. Assign a delivery group to the app for each platform and click **Save**.

This configuration results in two entries listed for this app in the apps list. When you select an app to configure, select the app with **Type MDX**.

Step 4: Configure app deployment

1. In the Citrix Endpoint Management console, navigate to **Configure > Delivery Groups** and click **Add**.
2. In the **Apps** section, drag the desired MDX apps to the **Required Apps** box.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Navigate to **Configure > Delivery Groups**.
4. Select the delivery group and click **Deploy**.
5. Users receive a request to install the app and the app installs in the background after they accept.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Custom apps

Custom apps are proprietary business-to-business apps. You can use Citrix Endpoint Management and Apple Volume Purchase to distribute proprietary apps privately and securely. You can distribute the apps to specific partners, clients, franchisees, and internal employees.

Feature availability	
Requires device supervision	No
Available for user enrollment mode	Yes
Available on	iOS/iPadOS

Requirements for custom apps

- Apple Business Manager or Apple School Manager account
- Apple Volume Purchase account (requires devices with iOS 7 or later)
- Enroll devices in Citrix Endpoint Management, using one of the following Apple enrollment modes:
  - Automated Device Enrollment
  - Device enrollment
  - User enrollment

Step 1: Link accounts

To deploy custom apps using Volume Purchase, link your Volume Purchase account to Citrix Endpoint Management.

1. Set up and enroll in Apple Business Manager (ABM). For more information about these programs, see the Apple documentation.
2. Link your ABM account with Citrix Endpoint Management. For more information on linking Volume Purchase accounts, see Apple Volume Purchase.
3. When you add your Volume Purchase account, enable **App Auto Update**. This setting makes sure that apps on user devices automatically update when an update appears in the Apple store. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens regardless of whether the app is required or optional.

   To use the **Force app to be managed** and **App Auto Update** settings, enable the `apple.app.force.managed` server property. See Server properties.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Step 2: Configure apps on ABM

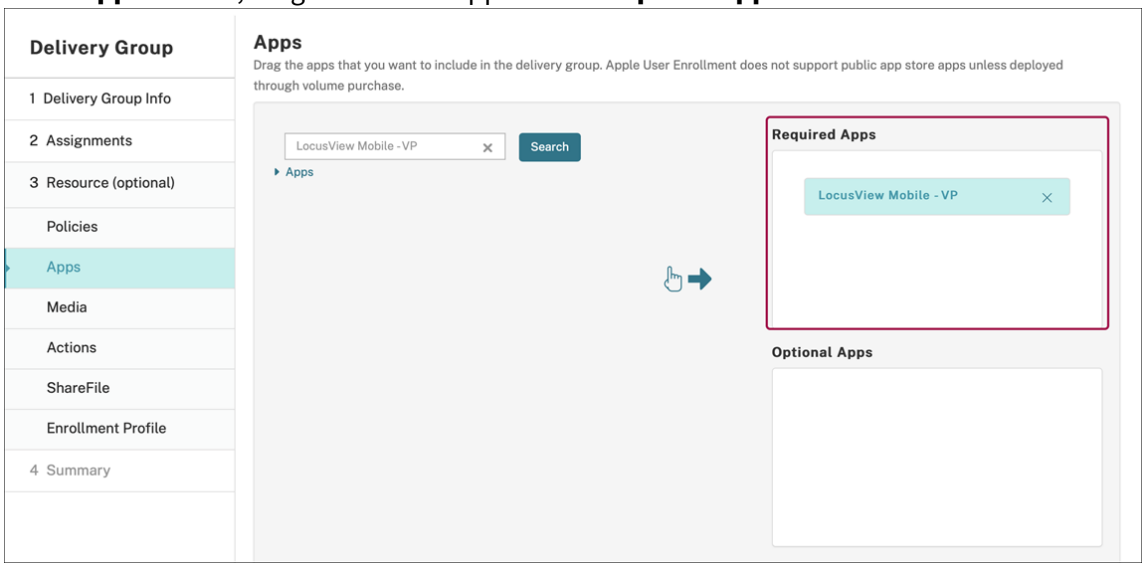
Add apps on your ABM account. You can upload and distribute your own custom apps or buy licenses for custom apps from other organizations. For more information on adding and enabling custom apps on ABM, see the Apple documentation.

Step 3: Add and configure apps in Citrix Endpoint Management

1. In the Citrix Endpoint Management console, navigate to **Configure > Apps**. Volume Purchase apps appear in the list of apps.
2. Select the app that you want to configure. Click **Edit**.
3. Select the platforms: **iPhone**, **iPad**, or **macOS**.
4. Choose the delivery groups to which you want the app distributed. Click **Save**.

Step 4: Configure app deployment

1. In the Citrix Endpoint Management console, navigate to **Configure > Delivery Groups** and click **Add**.
2. In the **Apps** section, drag the desired apps to the **Required Apps** box.



3. Navigate back to **Configure > Delivery Groups**.
4. Select the delivery group that you want deployed and click **Deploy**.
5. Users receive a request to deploy apps. Apps install in the background after users accept them.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

MDX enabled custom apps

To use MDX policies and security features, add custom apps that are MAM SDK enabled or MDX-wrapped.

Feature availability	
Requires device supervision	No
Available for user enrollment mode	Yes
Available on	iOS/iPadOS

Step 1: Link accounts

To deploy custom apps using Volume Purchase, link your Volume Purchase account to Citrix Endpoint Management.

1. Set up and enroll in Apple Business Manager (ABM). For more information about these programs, see the Apple documentation.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Link your ABM account with Citrix Endpoint Management. For more information on linking Volume Purchase accounts, see Apple Volume Purchase.
3. When you add your Volume Purchase account, enable **App Auto Update**. This setting makes sure that the apps on user devices automatically update when an update appears in the Apple store. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens regardless of whether the app is required or optional.

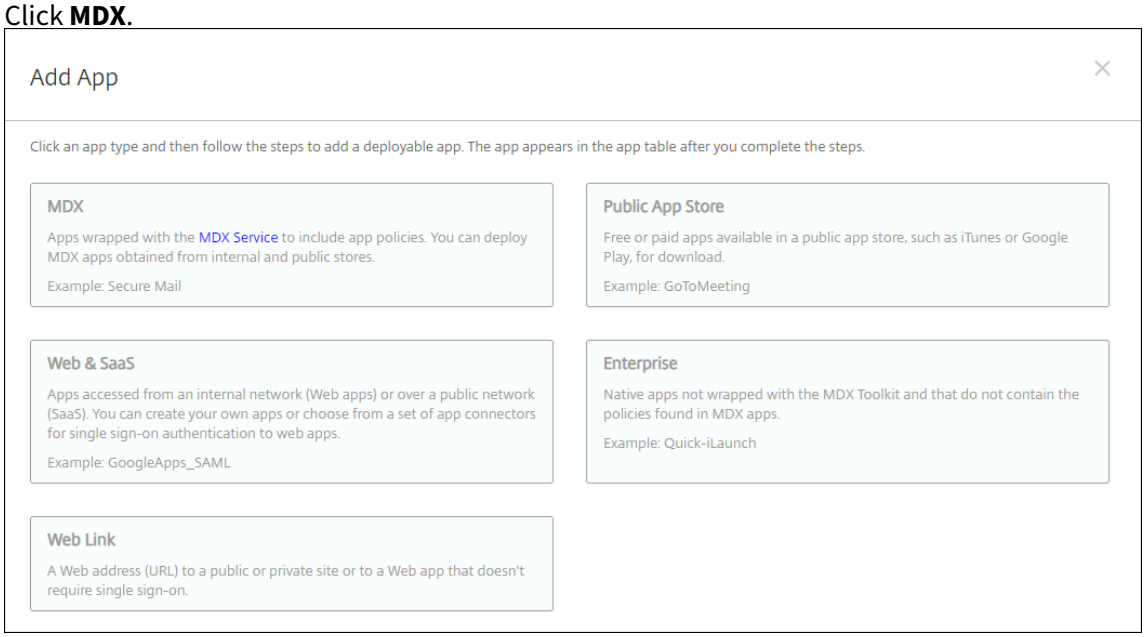
   To use the **Force app to be managed** and **App Auto Update** settings, enable the `apple.app.force.managed` server property. See Server properties.

Step 2: Configure apps on ABM

Add apps on your ABM account. You can upload and distribute your own custom apps or buy licenses for custom apps from other organizations. For more information on adding and enabling custom apps on ABM, see the Apple documentation.

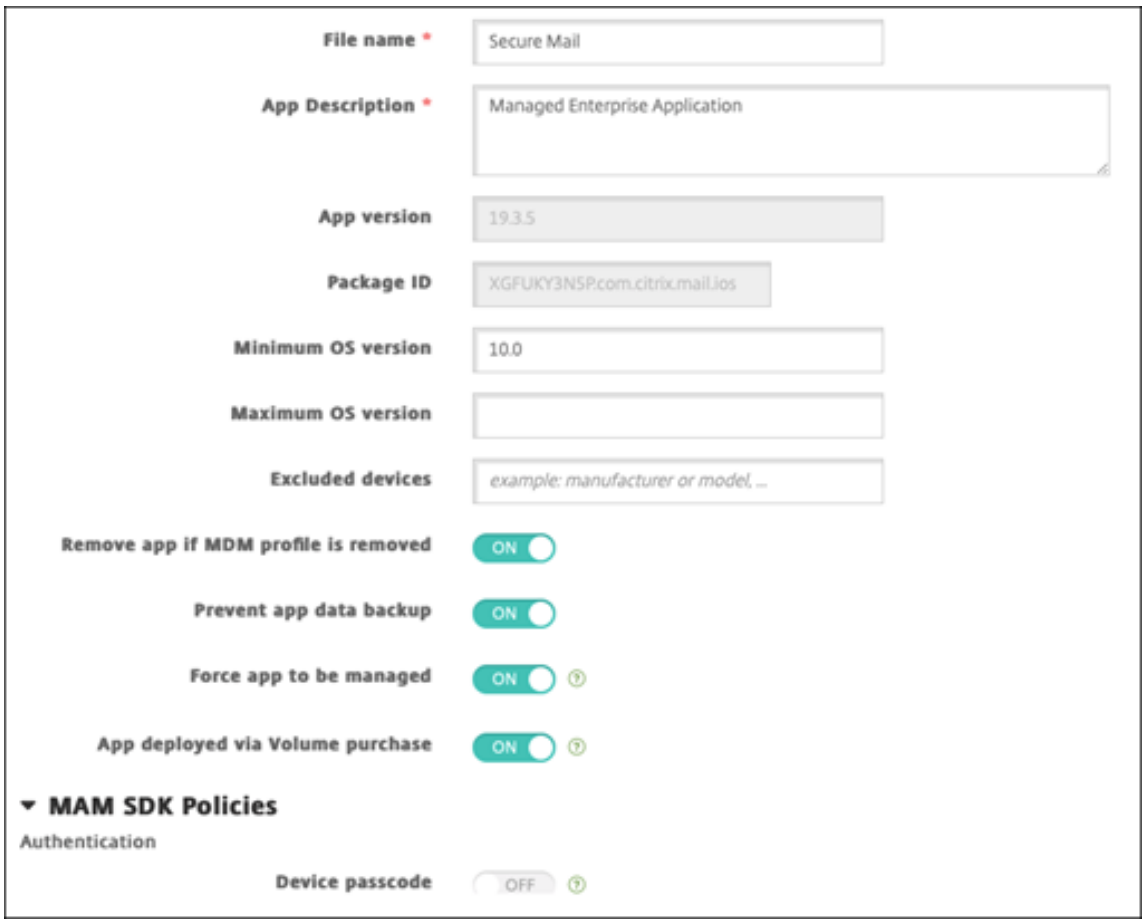
Step 3: Add and configure apps in Citrix Endpoint Management

1. In the Citrix Endpoint Management console, navigate to **Configure > Apps**. Click **Add**.
2. Click **MDX**.



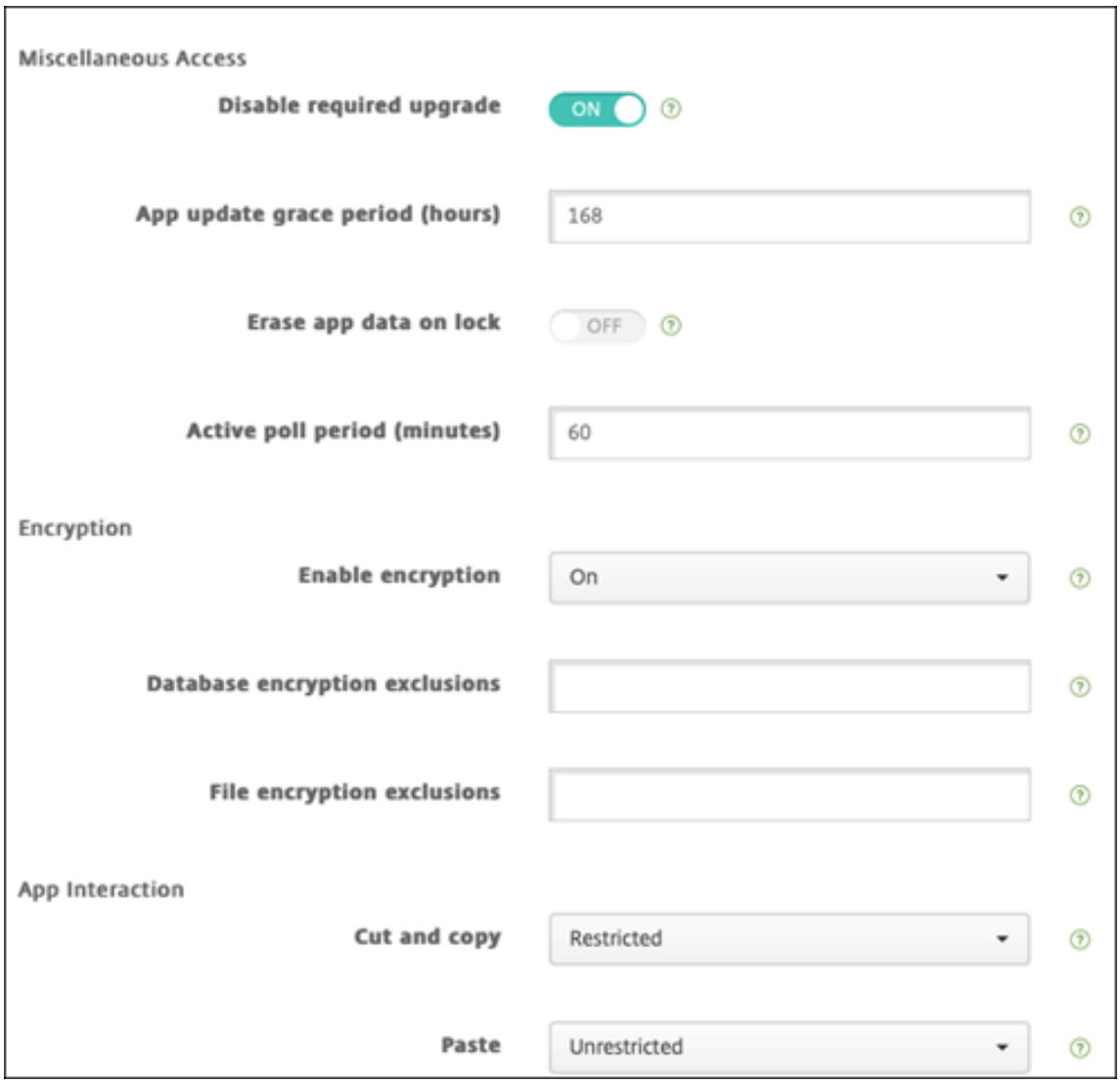
3. Select the **iPhone** or **iPad** platforms.
4. Upload the MDX file for the app that you want to add.
5. Configure the app details. Set **App deployed via Volume Purchase** to **On**. Citrix also recommends enabling the **Force app to be managed** feature.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. Configure the MDX policies. Set **Disable required upgrade** to **On**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



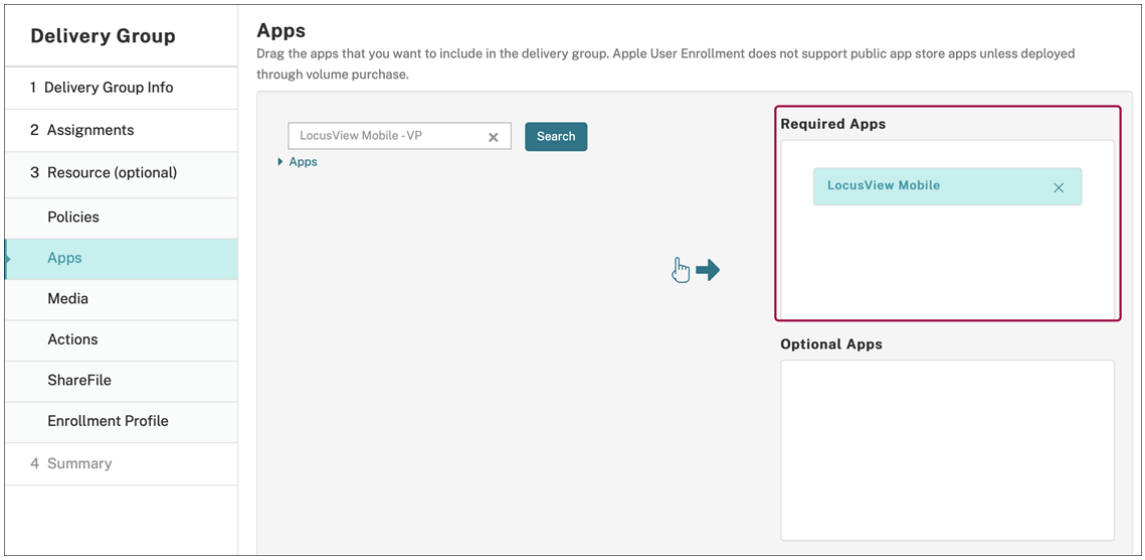
7. Assign a delivery group to the app and click **Save**.

This configuration results in two entries listed for this app in the apps list. When you select an app to configure, select the app with **Type MDX**.

Step 4: Configure app deployment

1. In the Citrix Endpoint Management console, navigate to **Configure > Apps**. Volume Purchase apps appear in the list of apps.
2. Select the app that you want to configure. Click **Edit**.
3. Choose the delivery groups to which you want the app distributed on each platform. Click **Save**.
4. Navigate to **Configure > Delivery Groups** and click **Add**.
5. In the **Apps** section, drag the desired MDX apps to the **Required Apps** box.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. Navigate back to **Configure > Delivery Groups**.
7. Select the delivery group that you want deployed and click **Deploy**.
8. Users receive a request to deploy apps. Apps install in the background after they accept.

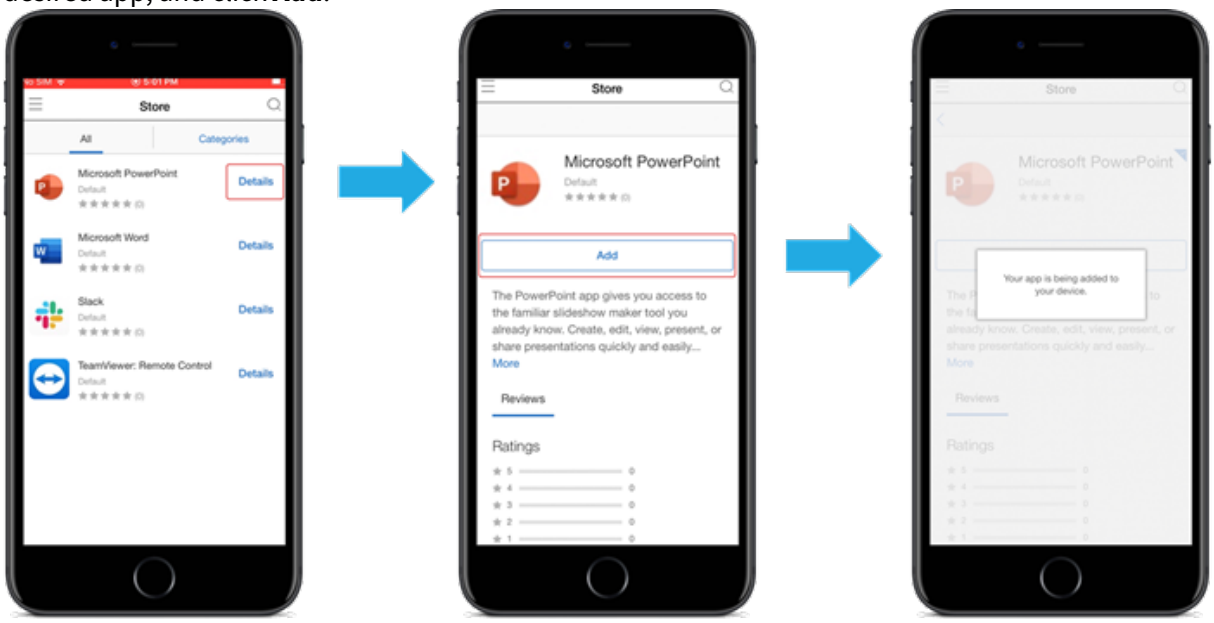
Optional apps (iOS/iPadOS only)

Citrix recommends deploying apps as **Required**. Required apps install silently on user devices, minimizing interaction. Having this feature enabled also allows apps to update automatically.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Optional apps allow users to choose what apps to install, but users must start the installation manually through Citrix Secure Hub.

To install optional apps, users must launch Citrix Secure Hub, go to **Store**, select **Details** for the desired app, and click **Add**.



Network Access Control

September 6, 2025

You can use your Network Access Control (NAC) solution to extend the Citrix Endpoint Management device security assessment for Android and Apple devices. Your NAC solution uses the Citrix Endpoint Management security assessment to facilitate and handle authentication decisions. After you configure your NAC appliance, the device policies and NAC filters that you configure in Citrix Endpoint Management get enforced.

Using Citrix Endpoint Management with a NAC solution adds QoS and more granular control over devices that are internal to your network. For a summary of the advantages of integrating NAC with Citrix Endpoint Management, see Access control.

Citrix supports these solutions for integration with Citrix Endpoint Management:

- NetScaler Gateway
- ForeScout

Citrix® doesn't guarantee integration for other NAC solutions.

With a NAC appliance in your network:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Management supports NAC as an endpoint security feature for iOS, Android Enterprise, and Android devices.
- You can enable filters in Citrix Endpoint Management to set devices as compliant or non-compliant for NAC, based on rules or properties. For example:
  - If a managed device in Citrix Endpoint Management doesn't meet the specified criteria, Citrix Endpoint Management marks the device as non-compliant. A NAC appliance blocks non-compliant devices on your network.
  - If a managed device in Citrix Endpoint Management has non-compliant apps installed, a NAC filter can block the VPN connection. As a result, a non-compliant user device cannot access apps or websites through the VPN.
  - If you use NetScaler Gateway for NAC, you can enable split tunneling to prevent the NetScaler Gateway plug-in from sending unnecessary network traffic to NetScaler Gateway. For more information on split tunneling, see Configuring Split Tunneling.

Supported NAC compliance filters

Citrix Endpoint Management supports the following NAC compliance filters:

Anonymous Devices: Checks if a device is in anonymous mode. This check is available if Citrix Endpoint Management can't reauthenticate the user when a device tries to reconnect.

Forbidden Apps: Checks if a device has forbidden apps, as defined in an App Access policy. For more information about that policy, see App access device policies.

Inactive Devices: Checks if a device is inactive as defined by the **Device Inactivity Days Threshold** setting in **Server Properties**. For details, see Server properties.

Missing Required Apps: Checks if a device is missing any required apps, as defined in an App Access policy.

Non-suggested Apps: Checks if a device has non-suggested apps, as defined in an App Access policy.

Noncompliant Password: Checks if the user password is compliant. On iOS and Android devices, Citrix Endpoint Management can determine whether the password currently on the device is compliant with the passcode policy sent to the device. For instance, on iOS, the user has 60 minutes to set a password if Citrix Endpoint Management sends a passcode policy to the device. Before the user sets the password, the passcode might be non-compliant.

Out of Compliance Devices: Checks whether a device is out of compliance, based on the Out of Compliance device property. Typically, automated actions or third parties using Citrix Endpoint Management APIs change that property.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Revoked Status: Checks whether the device certificate is revoked. A revoked device cannot re-enroll until it is authorized again.

Rooted Android and Jailbroken iOS Devices: Checks whether an Android or iOS device is jailbroken.

Unmanaged Devices: Check whether Citrix Endpoint Management is managing a device. For example, a device enrolled in MAM or an unenrolled device is not managed.

> **Note:**
>
> The Implicit Compliant/Not Compliant filter sets the default value only on devices that Citrix Endpoint Management is managing. For example, any devices that have a blocked app installed or are not enrolled, get marked as Not Compliant. The NAC appliance blocks those devices from your network.

Configuration overview

We recommend that you configure the NAC components in the order listed.

1. Configure device policies to support NAC:

   For iOS devices: See Configure the VPN device policy to support NAC.

   For Android Enterprise devices: See Create an Android Enterprise managed configuration for Citrix SSO.

   For Android devices: See Configure the Citrix SSO protocol for Android.

2. Enable NAC filters in Citrix Endpoint Management.
3. Configure a NAC solution:

   - NetScaler Gateway, detailed in Update NetScaler Gateway policies to support NAC.

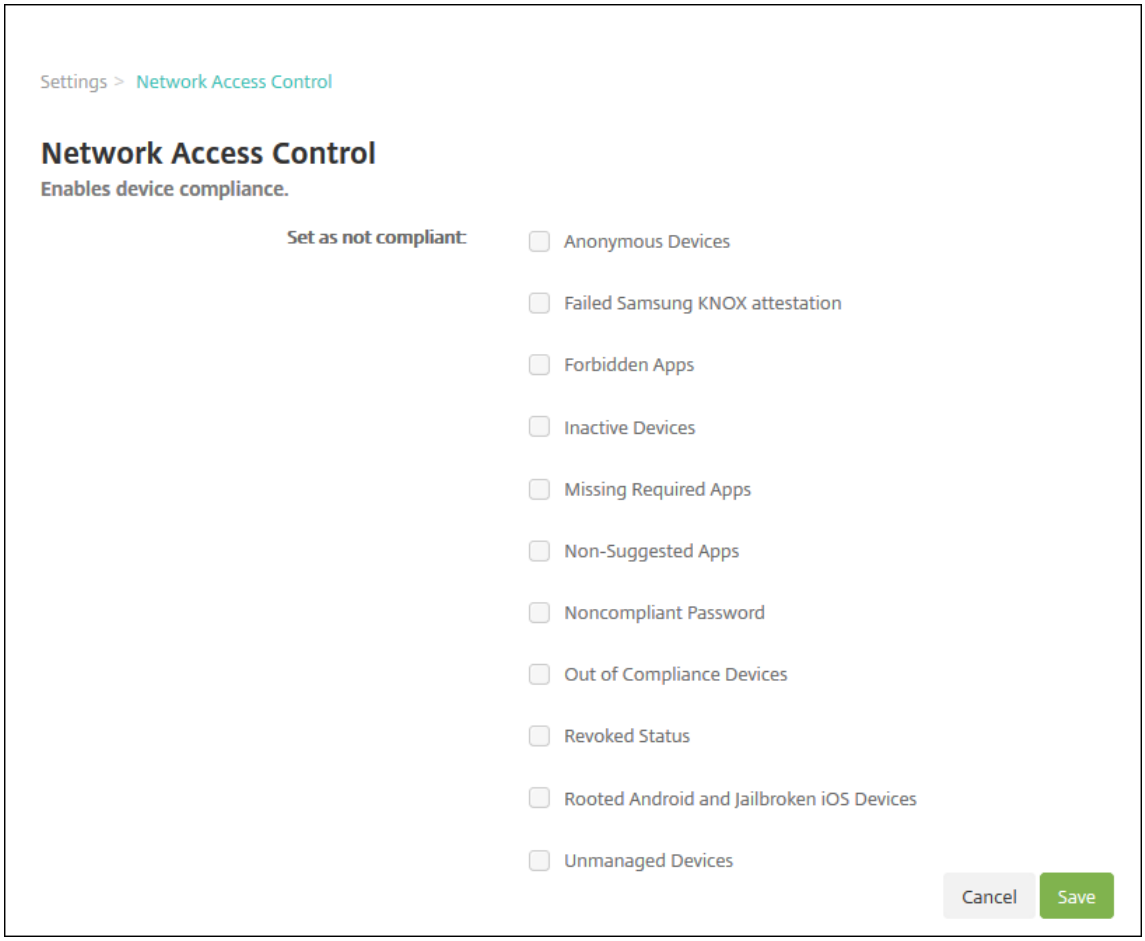
     Requires that you install Citrix SSO on devices. See NetScaler Gateway Clients.

   - ForeScout: See the ForeScout documentation.

Enable NAC filters in Citrix Endpoint Management

1. In the Citrix Endpoint Management console, go to **Settings > Network Access Control**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. Select the checkboxes for the **Set as not compliant** filters you want to enable.
3. Click **Save**.

Update NetScaler Gateway policies to support NAC

You must configure advanced (not classic) authentication and VPN sessions policies on your VPN virtual server.

These steps update a NetScaler Gateway with either of these characteristics:

- Is integrated with Citrix Endpoint Management.
- Or, is set up for VPN, not part of the Citrix Endpoint Management environment, and can reach Citrix Endpoint Management.

On your virtual VPN server from a console window, do the following. The FQDNs and IP addresses in the commands and examples are fictitious.

1. If you are using classic policies on your VPN virtual server, remove and unbind all classic policies. To check, type:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
show vpn vserver <VPN_VServer>
```

Remove any result that has the word **Classic**. For example: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

To remove the policy, type:

```
unbind vpn vserver <VPN_VServer> -policy <policy_name>
```

2. Create the corresponding advanced session policy by typing the following.

```
add vpn sessionPolicy <policy_name> <rule> <session action>
```

For example: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. Bind the policy to your VPN virtual server by typing the following.

```
bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100
```

4. Create an authentication virtual server by typing the following.

```
add authentication vserver <authentication vserver name> <service type> <ip address>
```

For example: `add authentication vserver authvs SSL 0.0.0.0`
In the example, `0.0.0.0` means that the authentication virtual server is not public facing.

5. Bind an SSL certificate with the virtual server by typing the following.

```
bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>
```

For example: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Associate an authentication profile to the authentication virtual server from the VPN virtual server. First, create the authentication profile by typing the following.

```
add authentication authnProfile <profile name> -authnVsName <authentication vserver name>
```

For example:

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. Associate the authentication profile with the VPN virtual server by typing the following.

```
set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
```

For example:

```
set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

8. Check the connection from NetScaler Gateway to a device by typing the following.

   ```
   curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
   ```

   For example, this query verifies connectivity by getting the compliance status for the first device (`deviceid_1`) enrolled in the environment:

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"
   ```

   A successful result is similar to the following example.

   ```
   1 HTTP/1.1 200 OK
   2 < Server: Apache-Coyote/1.1
   3 < X-Citrix-Device-State: Non Compliant
   4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   ```

9. When the preceding step is successful, create the web authentication action to Citrix Endpoint Management. First, create a policy expression to extract the device ID from the iOS VPN plug-in. Type the following.

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. Send the request to Citrix Endpoint Management by typing the following. In this example, the Citrix Endpoint Management IP is `10.207.87.82` and the FQDN is `example.em.cloud.com:4443`.

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort 4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n"+ "Host: example.em.cloud.com:4443\r\n"+ "X-Citrix-VPN-Device-ID: "+ xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ(\"Compliant\")"
    ```

    The successful output for the Citrix Endpoint Management NAC is `HTTP status 200 OK`. The `X-Citrix-Device-State` header must have the value of `Compliant`.

11. Create an authentication policy with which to associate the action by typing the following.

    ```
    add authentication Policy <policy name> -rule <rule> -action <web authentication action>
    ```

    For example: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. Convert the existing LDAP policy to an advanced policy by typing the following.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
add authentication Policy <policy_name> -rule <rule> -action <
LDAP action name>
```

For example: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Add a policy label with which to associate the LDAP policy by typing the following.

```
add authentication policylabel <policy_label_name>
```

For example: `add authentication policylabel ldap_pol_label`

14. Associate the LDAP policy to the policy label by typing the following.

```
bind authentication policylabel ldap_pol_label -policyName
ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
```

15. Connect a compliant device to do a NAC test to confirm successful LDAP authentication. Type the following.

```
bind authentication vserver <authentication vserver> -policy <web
 authentication policy> -priority 100 -nextFactor <ldap policy
label> -gotoPriorityExpression END
```

16. Add the UI to associate with the authentication virtual server. Type the following command to retrieve the device ID.

```
add authentication loginSchemaPolicy <schema policy>-rule <rule>
-action lschema_single_factor_deviceid
```

17. Bind the authentication virtual server by typing the following.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -
priority 100 -gotoPriorityExpression END
```

18. Create an LDAP advanced authentication policy enable the Citrix Secure Hub connection. Type the following.

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER
(\"User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
```

```
bind authentication vserver authvs -policy ldap_xm_test_pol -
priority 110 -gotoPriorityExpression NEXT
```

Windows Desktop and Tablet

September 6, 2025

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management enrolls Windows 10 and Windows 11 devices in MDM. Citrix Endpoint Management supports the following authentication types for Windows 10 and Windows 11 devices enrolled in MDM:

- Domain-based authentication
  - Active Directory
  - Azure Active Directory
- Identity providers:
  - Azure Active Directory
  - Citrix® identity provider

For more information about the supported authentication types, see Certificates and authentication.

A general workflow for starting Windows 10 or Windows 11 device management is as follows:

1. Complete the onboarding process. See Onboarding and resource setup and Prepare to enroll devices and deliver resources.

   If you plan to enroll Windows devices using the AutoDiscovery service, you must configure the Citrix AutoDiscovery service. Request Citrix Technical Support for assistance. For more information, see Request AutoDiscovery for Windows devices.
2. Choose and configure an enrollment method. See Supported enrollment methods.
3. Configure Windows Desktop and Tablet device policies.
4. Users enroll Windows 10 and Windows 11 devices.
5. Set up device and app security actions. See Security actions.

For supported operating systems, see Supported device operating systems.

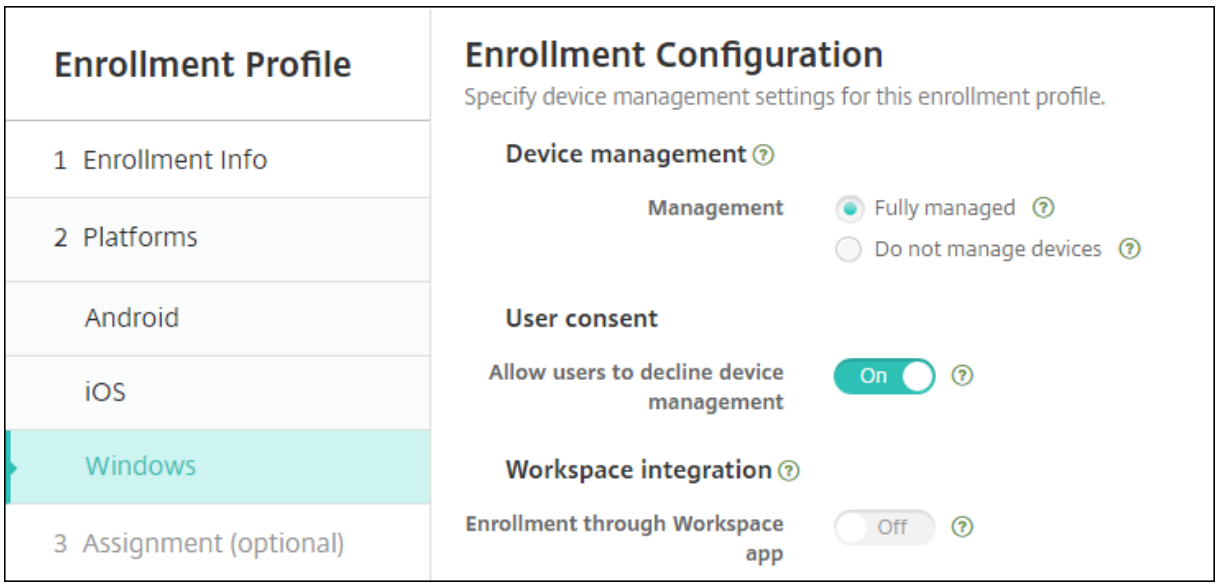
Supported enrollment methods

You specify how to manage Windows 10 and Windows 11 devices in the enrollment profiles. Two options are available:

- Fully managed (MDM enrollment)
- Do not manage devices (no MDM enrollment)

To configure enrollment settings for Windows 10 and Windows 11 devices, go to **Configure > Enrollment Profiles > Windows**. For more information about enrollment profiles, see Enrollment profiles.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The following table lists the enrollment methods that Citrix Endpoint Management supports for Windows 10 and Windows 11 devices:

Method	Supported
Azure Active Directory enrollment	Yes
AutoDiscovery service enrollment	Yes
Windows bulk enrollment	Yes
Manual enrollment	Yes
Enrollment invitations	No

> **Note:**
>
> - Manual enrollment requires users to enter a fully qualified domain name (FQDN) of the Citrix Endpoint Management server. We do not recommend using manual enrollment. Instead, use other methods to simplify the enrollment process for users.
> - You cannot send enrollment invitations to Windows devices. Windows users enroll directly through their devices.

Configure Windows Desktop and Tablet device policies

Use these policies to configure how Citrix Endpoint Management interacts with desktop and tablet devices running Windows 10 or Windows 11. This table lists all device policies available for Windows desktop and tablet devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App configuration	App inventory	App lock
App uninstall	Application Guard	BitLocker
Credentials	Custom XML	Defender
Device Guard	Device Health Attestation	Exchange
Firewall	Kiosk	Network
Office	OS update	Passcode
Restrictions	Store	Terms and Conditions
VPN	Web clip	Windows Agent
Windows GPO configuration	Windows Hello for Business	

Enroll Windows 10 and Windows 11 devices through Azure Active Directory

> **Important:**
>
> Before users can enroll, you must configure Azure Active Directory (AD) settings in Azure and then configure Citrix Endpoint Management. For details, see Connect Citrix Endpoint Management to Azure AD.

Windows 10 and Windows 11 devices can enroll with Azure as a federated means of AD authentication. This enrollment requires an Azure AD Premium subscription.

You can join Windows 10 and Windows 11 devices to Microsoft Azure AD by using any of the following methods:

- For company-owned devices:
  - Enroll in MDM when joining the device to Azure AD the first time the device is powered on. In this scenario, users complete the enrollment as described in this article: https://docs.microsoft.com/en-us/azure/active-directory/devices/azuread-joined-devices-frx.

    For Windows devices that you enroll with this method, you can use Windows AutoPilot to set up and pre-configure the devices. For more information, see Use Windows AutoPilot to set up and configure devices.
  - Enroll in MDM when joining the device to Azure AD from the Windows **Settings** page after configuring the device. In this scenario, users complete the enrollment as described in Enroll in MDM when joining Azure AD after configuring devices.
- For personal devices (BYOD or mobile devices):

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Enroll in MDM when registering to Azure AD while adding the Microsoft work account to Windows. In this scenario, users complete the enrollment as described in Enroll in MDM when registering to Azure AD.

Enroll in MDM when joining Azure AD after configuring devices

1. On a device, from the Start menu, navigate to **Settings > Accounts > Access work or school** and click **Connect**.
2. In the **Set up a work or school account** dialog box, under **Alternate actions**, click **Join this device to Azure Active Directory**.
3. Enter Azure AD credentials and click **Sign in**.
4. Accept the terms and conditions that the organization requires.
   - If users click **Decline**, the device neither joins Azure AD nor enrolls in Citrix Endpoint Management.
5. Click **Join** to continue with the enrollment process.
6. Click **Done** to complete the enrollment process.

Enroll in MDM when registering to Azure AD

1. On a device, from the Start menu, navigate to **Settings > Accounts > Access work or school** and click **Connect**.
2. In the **Set up a work or school account** dialog box, enter Azure AD credentials and click **Sign in**.
3. Accept the terms and conditions that the organization requires. The device is registered to Azure AD and enrolled in Citrix Endpoint Management.
   - If users click **Decline**, the device is registered to Azure AD but not enrolled into Citrix Endpoint Management. There is no **Info** button on the account.
4. Click **Join** to proceed with the enrollment process.
5. Click **Done** to complete the enrollment process.

Enroll Windows devices by using the AutoDiscovery service

To configure the AutoDiscovery service for Windows devices, request Citrix Technical Support for assistance. For more information, see Request AutoDiscovery for Windows devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> For Windows devices to enroll, the SSL listener certificate must be a public certificate. Enrollment fails for self-signed SSL certificates.

Users do the following steps to complete the enrollment:

1. On a device, from the Start menu, navigate to **Settings > Accounts > Access work or school** and click **Enroll only in device management**.
2. In the **Set up a work or school account** dialog box, enter a corporate email address and click **Next**.

   To enroll as a local user, enter a nonexistent email address with the correct domain name (for example, `foo\@mydomain.com`). That step lets a user bypass a known Microsoft limitation where the built-in Device Management on Windows does enrollment. In the **Connecting to a service** dialog box, enter the user name and password associated with the local user. The device then finds an Citrix Endpoint Management server and starts the enrollment process.
3. Enter the credential and click **Continue**.
4. In the **Terms of use** dialog box, agree to have the device managed and then click **Accept**.

Enrolling domain-joined Windows devices through the AutoDiscovery service fails if the domain policy disables MDM enrollment. Users can use either of the following methods instead:

- Remove the devices from the domain, enroll, and then rejoin them.
- Enter the FQDN of the Citrix Endpoint Management server to continue.

Windows bulk enrollment

With Windows bulk enrollment, you can set up many devices for an MDM server to manage without the need to reimage devices. You use a provisioning package for bulk enrollment for Windows 10 and Windows 11 Desktop and Laptop devices. For information, see Enroll Windows devices in bulk.

Security actions

Windows 10 and Windows 11 devices support the following security actions. For a description of each security action, see Security actions.

Locate	Lock	Reboot

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Revoke	Selective Wipe	Wipe

Connect Citrix Endpoint Management to Azure AD

Windows 10 and Windows 11 devices can enroll with Azure. Users created in Azure AD can have access to the devices. Citrix Endpoint Management is deployed in Microsoft Azure as an MDM service. Connecting Citrix Endpoint Management to Azure AD enables users to automatically enroll their devices into Citrix Endpoint Management when they enroll the devices into Azure AD.

To connect Citrix Endpoint Management to Azure AD, do the following steps:

1. In the Azure portal, navigate to **Azure Active Directory > Mobility (MDM and MAM) > Add application** and click **On-premises MDM application**.
2. Provide a name for the application and click **Add**.
3. (Optional) Azure doesn't allow unverified domains, such as cloud.com, to be used for IdP configuration. If your Citrix Endpoint Management Enrollment FQDN includes cloud.com, reach out to Citrix Support and provide them with the TXT record from Azure. Citrix Support verifies the subdomain, allowing you to continue your configuration. If your FQDN is under your own domain, you can verify it normally within Azure.
4. Select the application that you created, configure the following, and then click **Save**.
   - **MDM user scope**. Select **All**.
   - **MDM terms of use URL**. Enter in the format, `https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe/tou`.
   - **MDM discovery URL**. Enter in the format, `https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe`.
5. Click **On-premises MDM application settings**.
   - In the **Properties** pane, set **APP ID URI** in the format, `https://< Citrix Endpoint Management Enrollment FQDN>:8443`. This App ID URI is a unique ID that you cannot use again in any other app.
   - In the **Required permissions** pane, select **Microsoft Graph** and **Windows Azure Active Directory**.
   - In the **Keys** pane, create the authentication key. Click **Save** to view the key value. The key value appears only once. Save the key for later use. You need the key in step 7.
6. In the Citrix Endpoint Management console, go to **Settings > Identity Provider (IDP)** and then click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

7. On the **Discovery URL** page, configure the following and click **Next**.
    - **IDP Name**. Enter a unique name to identify the IdP connection that you are creating.
    - **IDP Type**. Select **Azure Active Directory**.
    - **Tenant ID**. The **Directory ID** in Azure. You see it when you navigate to **Azure Active Directory > Properties** in Azure.
8. On the **Windows MDM Info** page, configure the following and click **Next**.
    - **App ID URI**. The APP ID URI value you typed in Azure.
    - **Client ID**. The Application ID that you see in the **Properties** pane in Azure.
    - **Key**. The key value you created and saved in the preceding step 4.
9. On the **IDP Claims Usage** page, configure the following and click Next.
    - **User Identifier type**. Select **userPrincipalName**.
    - **User Identifier string**. Enter `${ id_token } .upn`.
10. Click **Save**.
11. Add an Azure AD user as a local user and assign it to a local user group.
12. Create a terms and conditions device policy and a delivery group that includes that local user group.

Device management when integrated with Workspace Environment Management™

With Workspace Environment Management (WEM) alone, MDM deployments aren't possible. With Citrix Endpoint Management alone, you're limited to managing Windows 10 and Windows 11 devices. By integrating the two, WEM can access MDM features and you can manage a wider spectrum of Windows operating systems through Citrix Endpoint Management. That management takes the form of configuring Windows GPOs. Currently, administrators import an ADMX file to Citrix Endpoint Management and push it to Windows 10 and Windows 11 desktops and tablets to configure specific applications. Using the Windows GPO Configuration device policy, you can configure GPOs and push changes to the WEM service. The WEM Agent then applies the GPOs to devices and their apps.

MDM management isn't a requirement for WEM integration. Any device that WEM supports can have GPO configurations pushed to it, even if Citrix Endpoint Management doesn't support that device natively.

For a list of the devices supported, see Operating System requirements.

Devices which receive the Windows GPO Configuration device policy run in a new Citrix Endpoint Management mode called WEM. In the **Manage > Devices** list of enrolled devices, the **Mode** column for WEM-managed devices lists **WEM**.

For more information, see Windows GPO Configuration device policy.

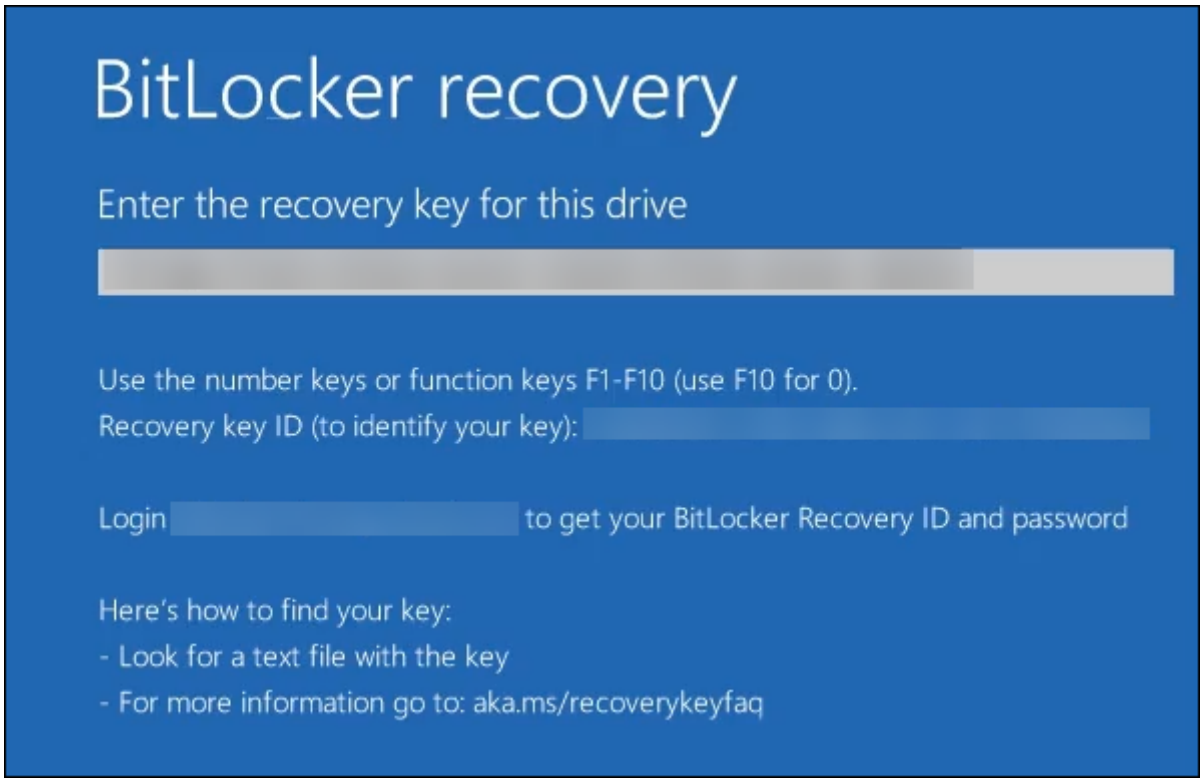
© 1997–2025 Citrix Systems, Inc. All rights reserved.

BitLocker recovery key

Encrypting disks using BitLocker is a useful security feature. However, unlocking devices can be a challenge if the user loses their BitLocker recovery key. Citrix Endpoint Management can now automatically, securely save BitLocker recovery keys for users. Users can find their BitLocker recovery key on the Self-Help Portal. To enable and find the BitLocker recovery key:

1. In the Citrix Endpoint Management console, navigate to **Settings > Server Properties**.
2. Search for `shp` and enable the `shp.console.enable` feature. Make sure that `enable.new.shp` stays disabled. For more information on enabling the Self-Help Portal, see Configure enrollment security modes.
3. Navigate to **Configure > Device policies**. Find your BitLocker policy or create one and enable the **BitLocker Recovery backup to Citrix Endpoint Management** setting.

When unlocking their device, end users see a message asking them to enter their key. The message displays the Recovery key ID as well.

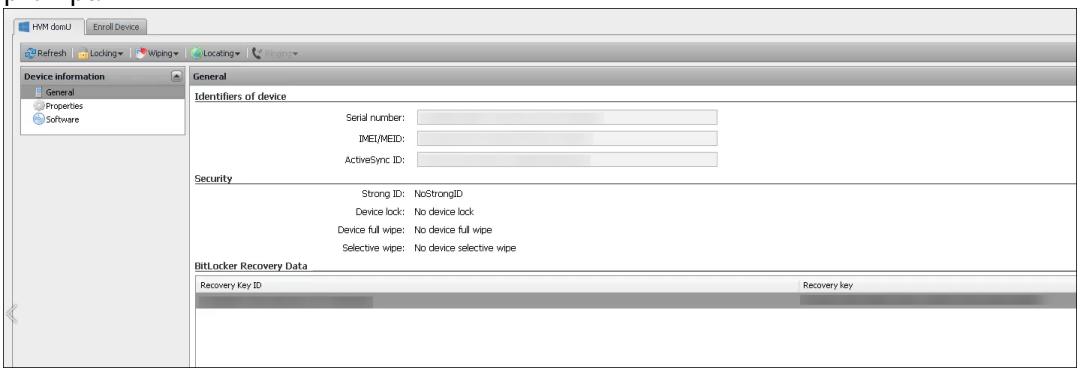


To find their BitLocker recovery key, users navigate to the Self-Help Portal.

1. Under the **General** details, see the **BitLocker Recovery Data**.
    - **Recovery key ID:** The identifier for the BitLocker recovery key used to encrypt the disk. This ID must match the key ID given in the previous message.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Recovery key:** The key user must enter to unlock their disk. Enter this key at the unlock prompt.



For more information about the BitLocker device policy, see BitLocker device policy.

Enroll Windows devices in bulk

September 6, 2025

Citrix Endpoint Management supports bulk enrollment of Windows 10 and Windows 11 desktop and tablet devices. With bulk enrollment, you can set up many devices for Citrix Endpoint Management to manage without reimaging devices. You use the provisioning package for bulk enrollment.

A general workflow to bulk enroll Windows 10 and Windows 11 devices is as follows:

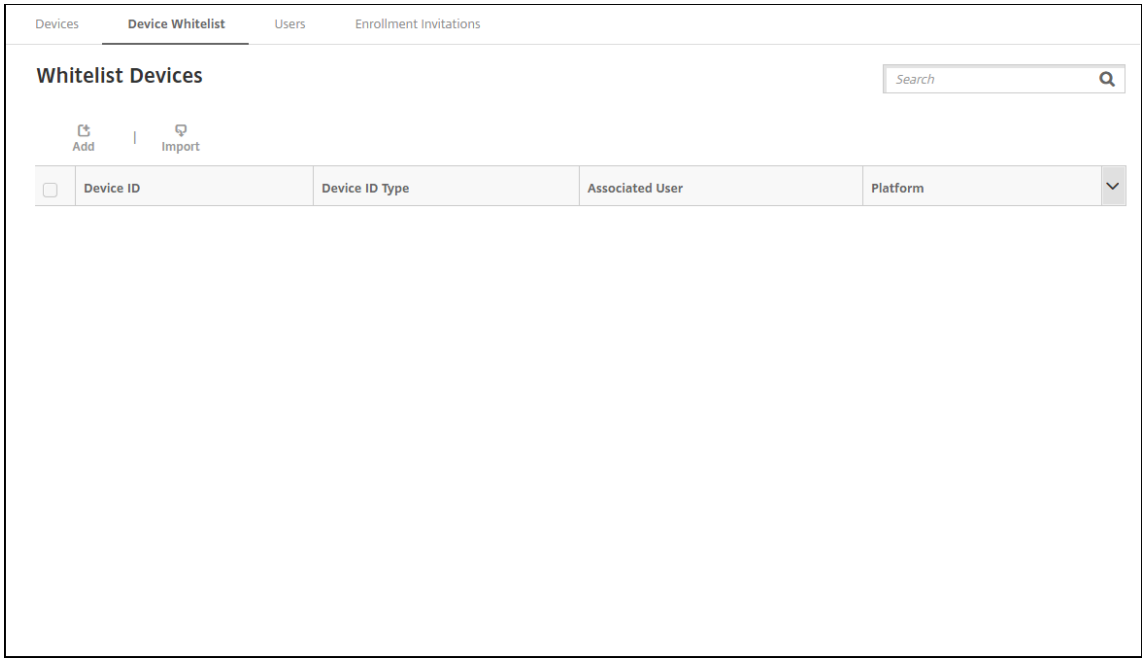
1. Assign devices. You can assign devices either on a per-device basis or in bulk.
2. Configure bulk enrollment.
3. Create a provisioning package and apply that package per device.

Before running bulk enrollment, make sure that you assign all devices to the correct users. Do this assignment by adding the devices on a per-device basis or in bulk.

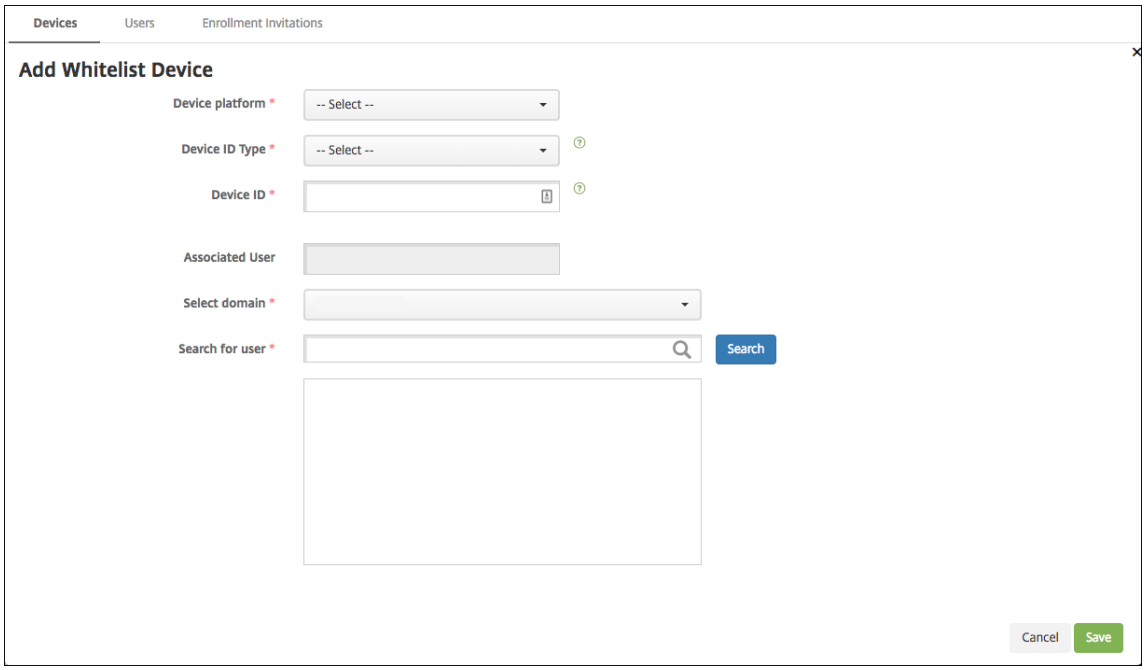
Assign devices on a per-device basis

1. In the Citrix Endpoint Management console, navigate to **Manage** > **Devices** > **Device Allow List**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. To add each device, click **Add**.



3. Type the following information:

   - **Device platform:** Select **Windows**.
   - **Device ID Type:** Select an ID that identifies the device. Citrix Endpoint Management supports **Hardware ID** and **Device Name** for Windows devices.
   - **Device ID:** Type the ID corresponding to the type that you selected previously for the device.

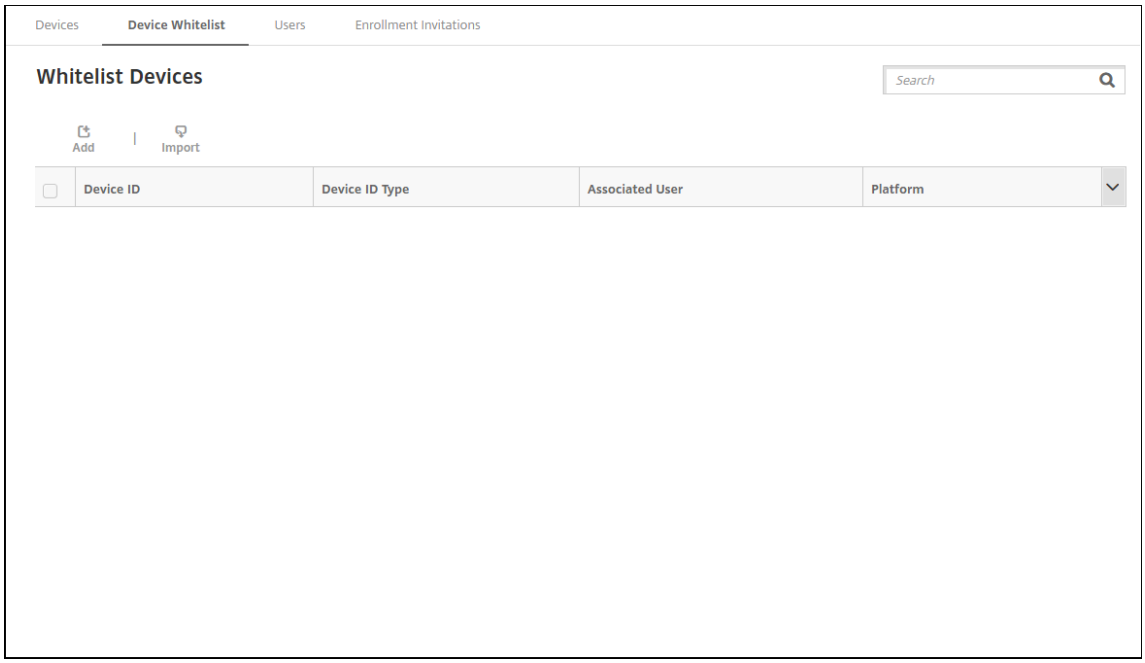
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Associated User:** Displays the associated user for this device. This field automatically populates with the user that you select.
- **Select domain:** Select the domain from which you want to search for an associated user.
- **Search for user** Type a full or partial user name in this field and click **Search** to find a user to associate with this device.

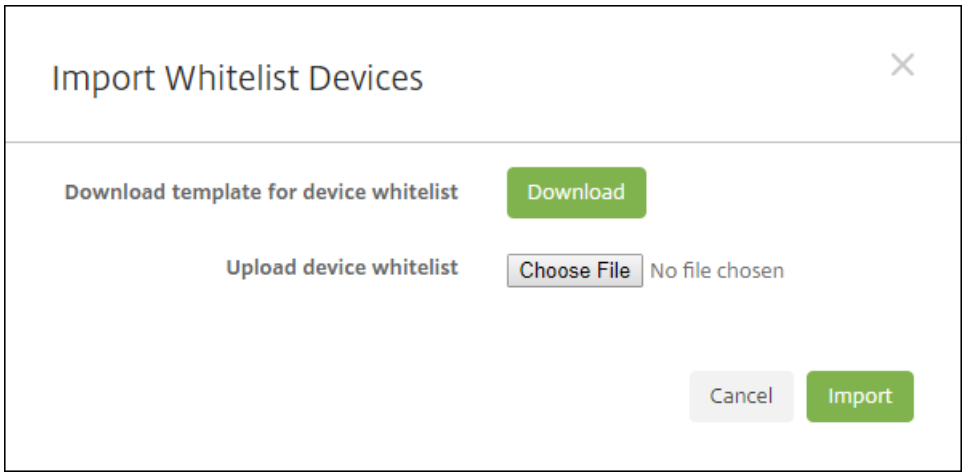
4. Click **Save**.

Add devices in bulk

1. In the Citrix Endpoint Management console, navigate to **Manage > Devices > Device Allow List**.



2. Click **Import**.

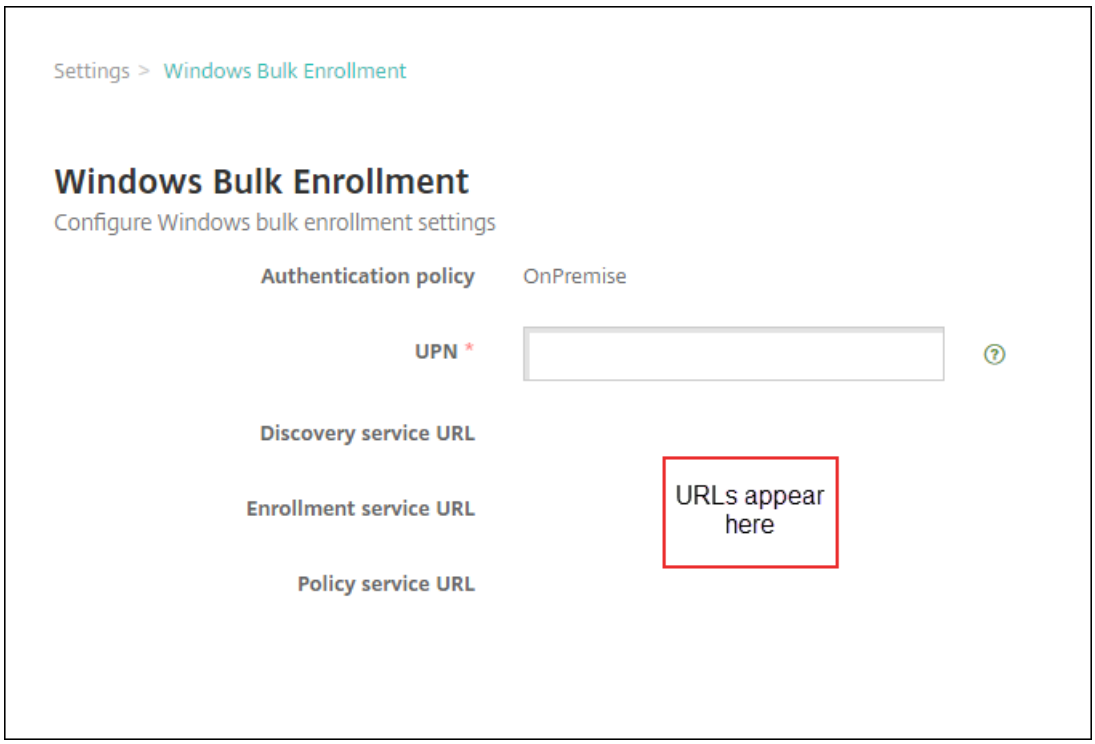


© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. Click **Download** to download a template (spreadsheet) for the device allow list. Fill out that spreadsheet and then upload the spreadsheet using **Choose File** and **Import**.

Configure bulk enrollment

1. In the Citrix Endpoint Management console, navigate to **Settings > Windows Bulk Enrollment**.
2. In the **UPN** field, type a user name through which to deploy all devices. The UPN must be a valid user in Citrix Endpoint Management that has the enrollment permissions. You can provide a UPN that is different from the associated user you selected previously.



   You need the URLs when creating a provisioning package in the Windows Configuration Designer.

3. Click **Save**.

Create and apply a provisioning package

To bulk provision devices, download the Windows Configuration Designer from the Microsoft Store. The Windows Configuration Designer creates provisioning packages used to image devices. As part of these packages, you can include Citrix Endpoint Management bulk enrollment configuration settings so that provisioned devices automatically enroll into Citrix Endpoint Management.

For information about using a provisioning package, see https://docs.microsoft.com/en-us/windows/client-management/mdm/bulk-enrollment-using-windows-provisioning-tool. Follow the

© 1997–2025 Citrix Systems, Inc. All rights reserved.

steps described in the *Create and apply a provisioning package for on-premises authentication* section in that document. You follow those steps to include the following Citrix Endpoint Management bulk enrollment configuration settings and to apply the package to each device.

- **Discovery service URL**.
- **Enrollment service URL**.
- **Policy service URL**.
- **Secret**. Password of the UPN. You previously typed the user name in the UPN field.

Bulk enroll devices out of the box

Citrix Endpoint Management supports bulk enrollment of Windows devices out of the box. Follow these steps to set up and do bulk enrollment:

1. Use the Citrix Endpoint Management console to add devices (on a per-device basis or in bulk) and to configure bulk enrollment. For more information, see Add devices in bulk and Configure bulk enrollment.
2. Create a provisioning package, as described in Create, and apply a provisioning package.

   > **Note:**
   >
   > You must configure the device name for each device when creating a provisioning package. To do so, in Windows Configuration Designer, navigate to **Runtime settings > Accounts > ComputerAccount > ComputerName** and specify the name of the device. The device name that you specify for each device must align with the name you used when importing allow list devices.

3. Place that provisioning package into a USB stick.
4. Insert the USB stick into the target device the first time that the user turns on the device.

   Windows device automatically finds the provisioning package (.ppkg) on the USB stick. For detailed instructions, see the Microsoft documentation on how to apply a provisioning package during initial setup.

The device automatically enrolls into Citrix Endpoint Management.

For devices running Windows 10(version 2004 or later) or Windows 11, you can simplify the enrollment process by creating only one provisioning package. The package can then be applied to all devices. As a result, you no longer need to create a provisioning package on a per-device basis.

To simplify the enrollment process, do these steps when creating a provisioning package:

1. In Windows Configuration Designer, navigate to **Runtime settings > Accounts > ComputerAccount > ComputerName**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. In the **ComputerName** field, include the following string as part of the device name: `%SERIAL%`. For example: `Surface-%SERIAL%`. The string expands to the BIOS serial number of each device.

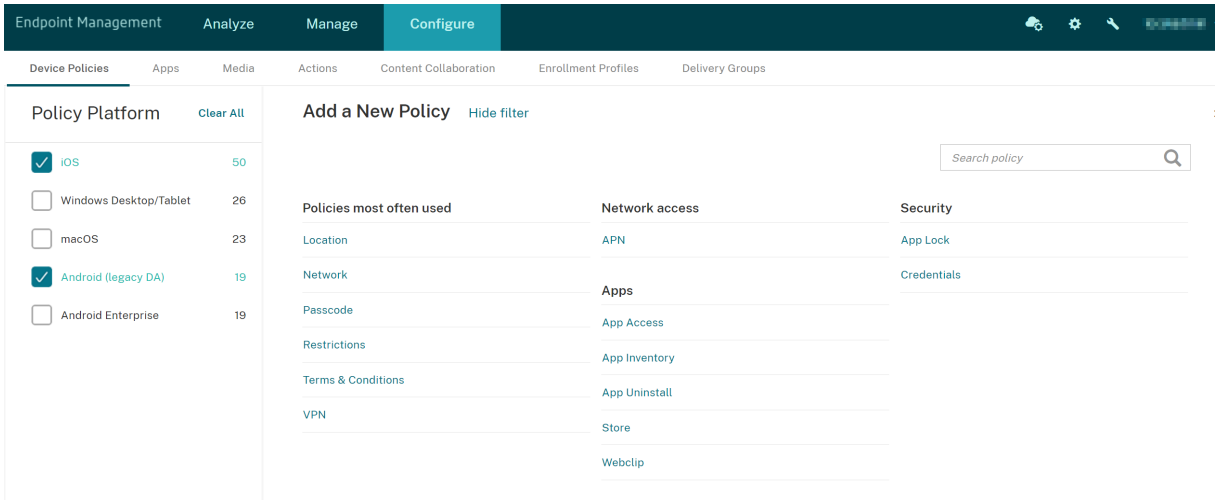
Device policies

April 16, 2024

You can configure how Citrix Endpoint Management interacts with your devices by creating policies. Although many policies are common to all devices, each device has a set of policies specific to its operating system. As a result, you might find differences between platforms, and even between different manufacturers of Android devices.

To view the policies that are available per platform:

1. In the Citrix Endpoint Management console, go to **Configure > Device Policies**.
2. Click **Add**.
3. Each device platform appears in a list in the **Policy Platform** pane. If that pane isn't open, click **Show filter**.
4. To see a list of all policies available for a platform, select that platform. To see a list of the policies that are available for multiple platforms, select each of those platforms. A policy appears in the list only if it applies to each platform selected.



For a summary description of each device policy, see Device policy summaries in this article.

> **Note:**
>
> If your environment is configured with Group Policy Objects (GPOs):

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> When you configure Citrix Endpoint Management device policies for Windows 10 and Windows 11, keep the following rules in mind. If a policy on one or more enrolled devices conflicts, the policy aligned with the GPO takes precedence.

To see which policies the Android Enterprise container supports, see Android Enterprise.

Prerequisites

- Create any delivery groups that you plan to use.
- Install any necessary CA certificates.

Add a device policy

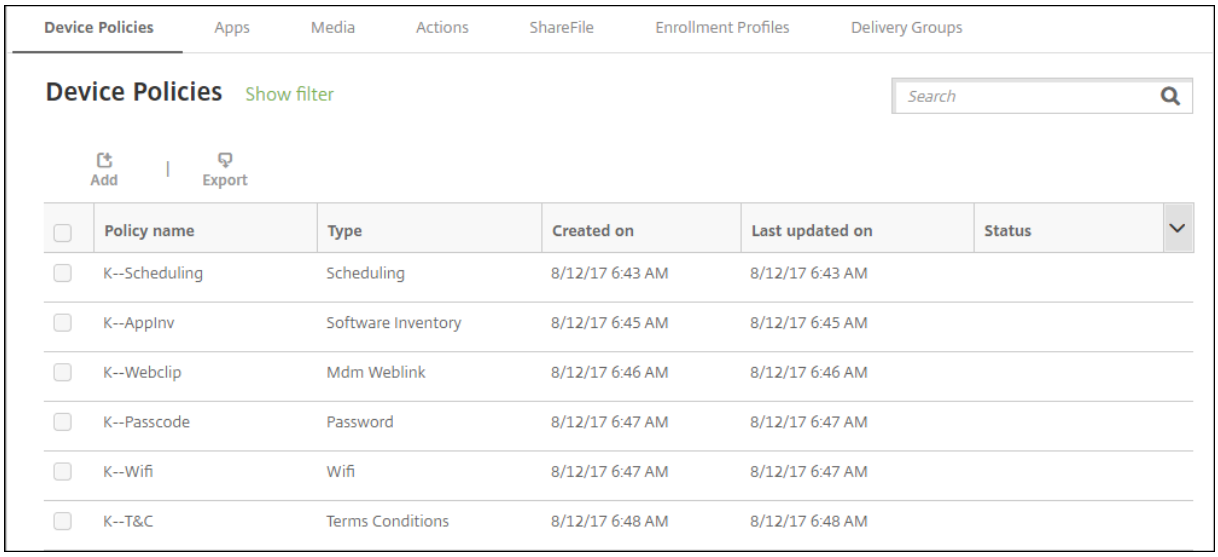
The basic steps to create a device policy are as follows:

1. Name and describe the policy.

   > **Important:**
   >
   > Do not use a forward slash (/) in a policy name. If you do, an error might occur when you edit the policy later.

2. Configure the policy for one or more platforms.
3. Create deployment rules (optional).
4. Assign the policy to delivery groups.
5. Configure the deployment schedule (optional).

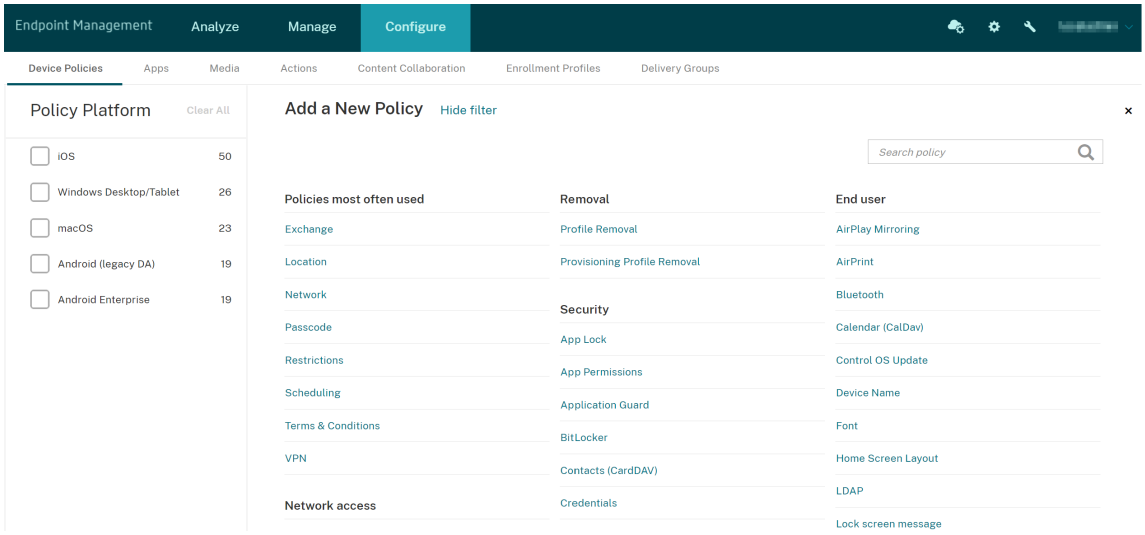
To create and manage device policies, go to **Configure > Device Policies**.



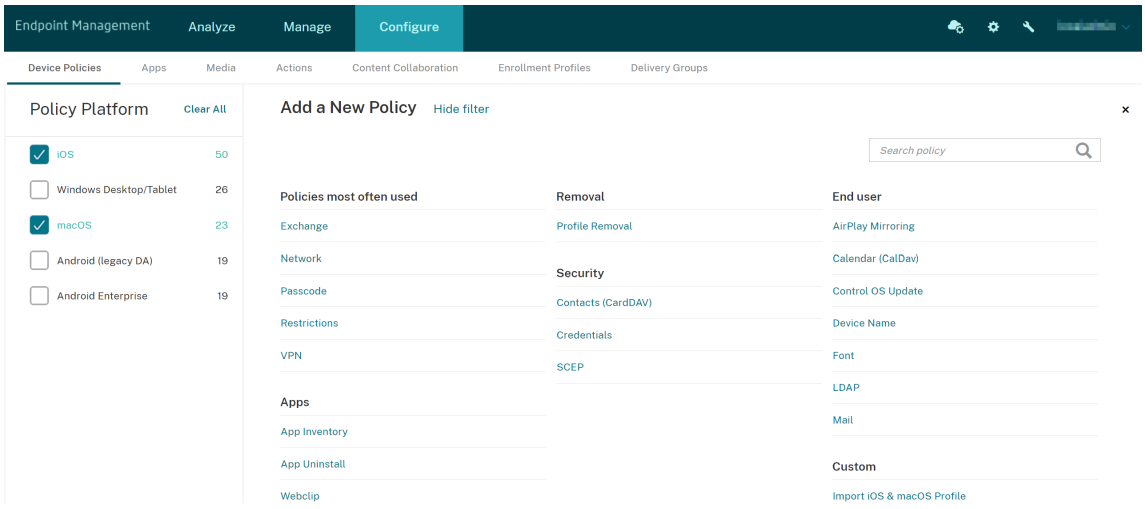
© 1997–2025 Citrix Systems, Inc. All rights reserved.

To add a policy:

1. On the **Device Policies** page, click **Add**. The **Add a New Policy** page appears.



2. Click one or more platforms to view a list of the device policies for the selected platforms. Click a policy name to continue with adding the policy.



   You can also type the name of the policy in the search box. As you type, potential matches appear. If your policy is in the list, click it. Only your selected policy stays in the results. Click it to open the **Policy Information** page for that policy.

3. Select the platforms that you want to include in the policy. Configuration pages for the selected platforms appear in Step 5.

4. Complete the **Policy Information** page and then click **Next**. The **Policy Information** page collects information, such as the policy name, to help you identify and track your policies. This page is similar for all policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. Complete the platform pages. Platform pages appear for each platform you selected in Step 3. These pages are different for each policy. A policy might differ among platforms. Not all policies apply to all platforms.

   Some pages include tables of items. To delete an existing item, hover over the line that has the listing and click the trash can icon on the right side. In the confirmation dialog, click **Delete**.

   To edit an existing item, hover over the line that has the listing and click the pen icon on the right side.

To configure deployment rules, assignments, and schedule

For more information about configuring deployment rules, see Deploy resources.

1. On a platform page, expand **Deployment Rules** and then configure the following settings. The **Base** tab appears by default.

   - In the lists, click options to specify the deployment conditions. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is set as **All**.
   - Click **New Rule** to define the conditions.
   - In the lists, click the conditions, such as **Device ownership** and **BYOD**.
   - Click **New Rule** again if you want to add more conditions. You can add as many conditions as you want.

2. Click the **Advanced** tab to combine the rules with Boolean options. The conditions you chose on the **Base** tab appear.
3. You can use more advanced Boolean logic to combine, edit, or add rules.

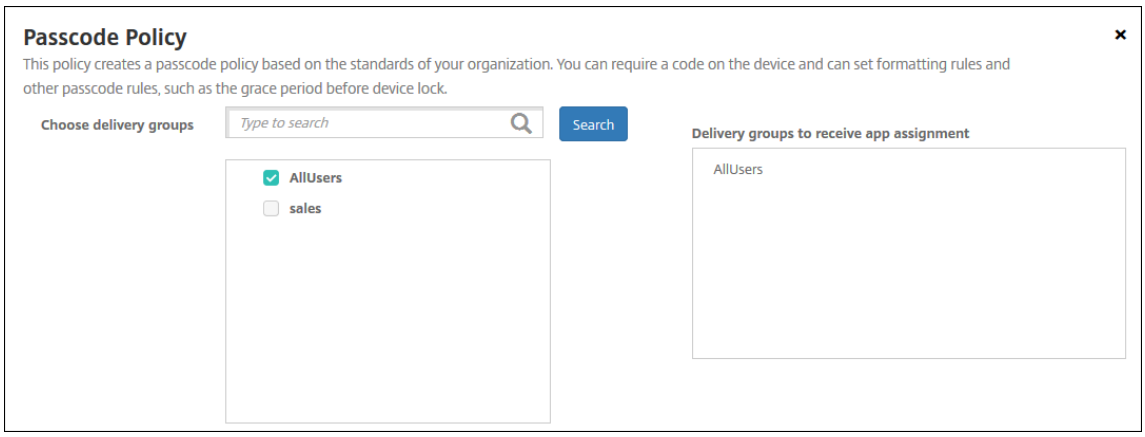
   - Click **AND**, **OR**, or **NOT**.
   - In the lists, choose the conditions that you want to add to the rule. Then, click the Plus sign (**+**) on the right side to add the condition to the rule.

     At any time, you can click to select a condition and then click **EDIT** or **Delete**.
   - Click **New Rule** to add another condition.

4. Click **Next** to move to the next platform page or, when all the platform pages are complete, to the **Assignments** page.
5. On the **Assignments** page, select the delivery groups to which you want to apply the policy. If you click a delivery group, the group appears in the **Delivery groups to receive app assignment** box.

   Delivery groups to receive app assignment doesn't appear until you select a delivery group.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

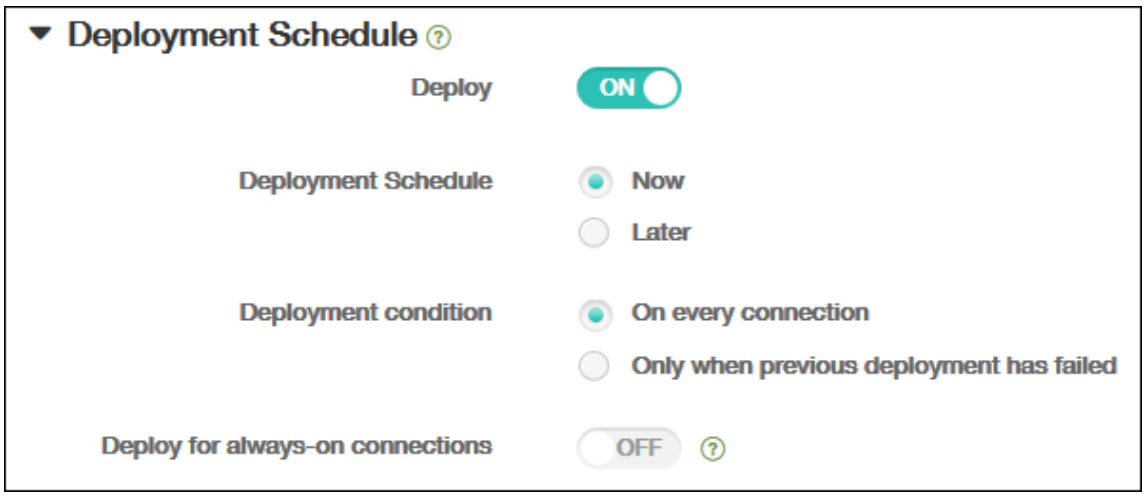


6. On the **Assignments** page, expand **Deployment Schedule** and then configure the following settings:

   - Next to **Deploy**, click **On** to schedule deployment or click **Off** to prevent deployment. The default option is set as **On**.
   - Next to **Deployment schedule**, click **Now**, or **Later**. The default option is set as **Now**.
   - If you click **Later**, click the calendar icon and then select the date and time for deployment.
   - Next to **Deployment condition**, click **On every connection**, or **Only when previous deployment has failed**. The default option is set as **On every connection**.
   - Next to **Deploy for always-on connection**, click **On**, or **Off**. The default option is set as **Off**.

     > **Note:**
     >
     > This option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.
     >
     > The always-on option:
     >
     > - Is not available for iOS devices
     > - Is not available for Android and Android Enterprise customers who began using Citrix Endpoint Management with version 10.18.19 or later
     > - Is not recommended for Android and Android Enterprise customers who began using Citrix Endpoint Management with before version 10.18.19
     >
     > The deployment schedule that you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



7. Click **Save**.

   The policy appears in the **Device Policies** table.

Remove a device policy from a device

The steps to remove a device policy from a device depends on the platform.

- Android

  To remove a device policy from an Android device, use the Citrix Endpoint Management Uninstall device policy. For information, see Citrix Endpoint Management uninstall device policy.

- iOS and macOS

  To remove a device policy from an iOS or macOS device, use the Profile Removal device policy. On iOS and macOS devices, all policies are part of the MDM profile. So, you can create a Profile Removal device policy for just the policy that you want to remove. The rest of the policies and the profile stay on the device. For more information, see Profile Removal device policy.

- Windows 10 and Windows 11

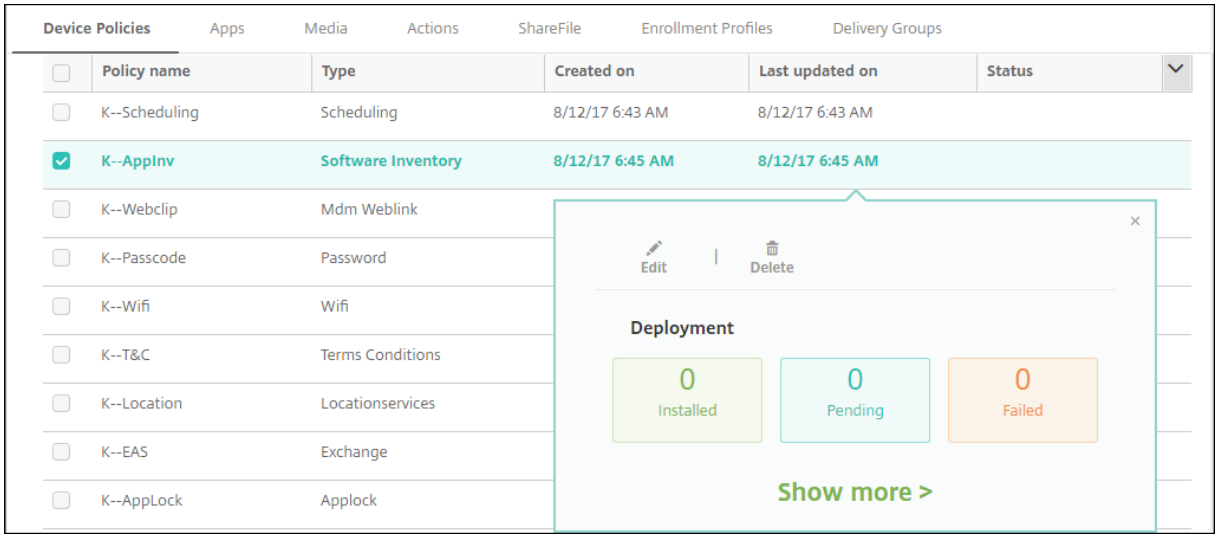
  You can't directly remove a device policy from a Windows Desktop or Tablet device. However, you can use either of the following methods:

  - Unenroll the device and then push a new set of policies to the device. Users then re-enroll to continue.
  - Push a security action to selectively wipe the specific device. That action removes all corporate apps and data from the device. You then remove the device policy from a delivery group that has just that device and push the delivery group to the device. Users then re-enroll to continue.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Edit a device policy

To edit a policy, select the checkbox next to a policy. The options menu appears above the policy list. Or, click a policy in the list to show more controls.



To view policy details, click **Show more**.

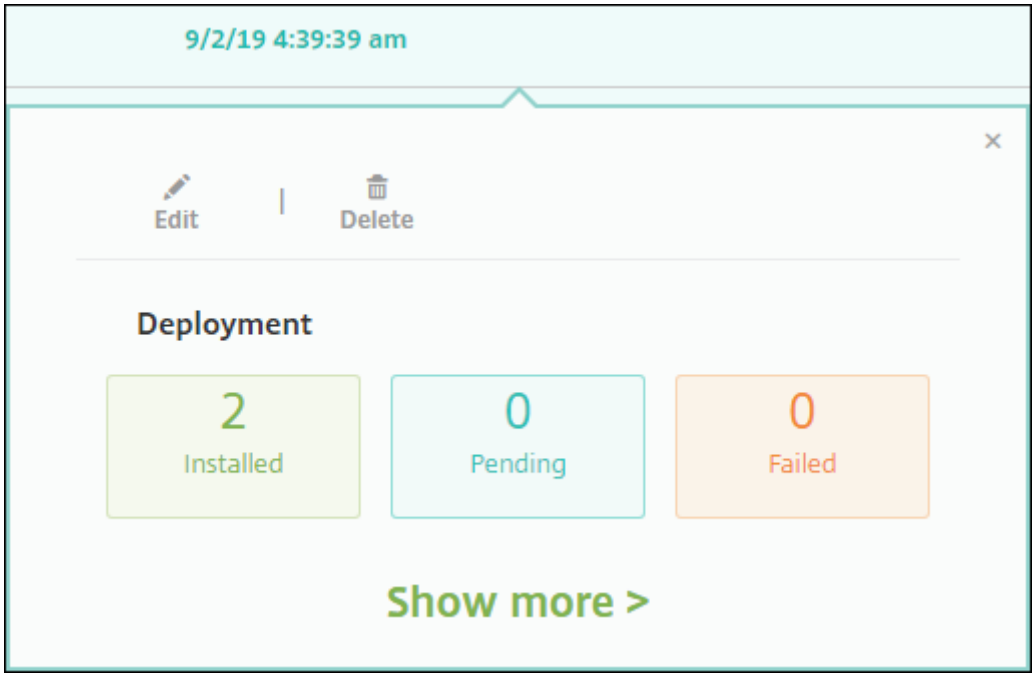
To edit all settings for a device policy, click **Edit**.

If you click **Delete**, a confirmation dialog box appears. Click **Delete** again to delete the policy.

Check policy deployment status

Click a policy row on the **Configure > Device Policies** page to check its deployment status.

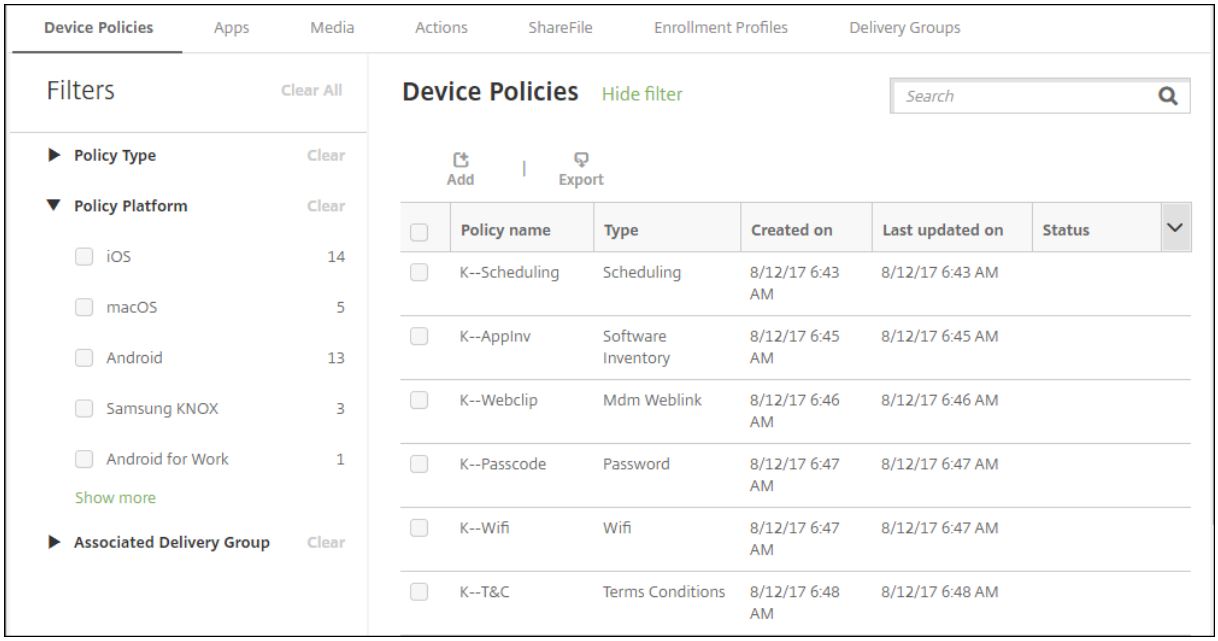
© 1997–2025 Citrix Systems, Inc. All rights reserved.



When a policy deployment is pending, users can refresh the policy from Citrix Secure Hub by tapping **Preferences > Device Information > Refresh policy**.

Filter the list of added device policies

You can filter the list of added policies by policy types, platforms, and associated delivery groups. On the **Configure > Device Policies** page, click **Show filter**. In the list, select the checkboxes for the items you want to see.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Click **SAVE THIS VIEW** to save a filter. The name of the filter then appears in a button below the **SAVE THIS VIEW** button.

Device policy summaries

Device Policy Name	Device Policy Description
AirPlay Mirroring	Adds specific AirPlay devices (such as Apple TV or another Mac computer) to iOS devices. You can also add devices to an allow list for supervised devices. That option limits users to only the AirPlay devices on the allow list.
AirPrint	Adds AirPrint printers to the AirPrint printer list on iOS devices. This policy makes it easier to support environments where the printers and the devices are on different subnets.
APN	Determines the settings used to connect your devices to the General Packet Radio Service (GPRS) of a specific phone carrier. This setting is already defined in most new phones. Use this policy if your organization doesn't use a consumer APN to connect to the internet from a mobile device.
App Access	Defines a list of the apps that are required, optional, or prevented on the device. You can then create an automated action to react to the device compliance with that list of apps.
App Attributes	Specifies attributes, such as a managed app bundle ID or per-app VPN identifier, for iOS devices.
App Configuration	Remotely configures various settings and behaviors of apps that support managed configuration. To do that, you deploy an XML configuration file (called a property list, or `plist`) to iOS devices. Or, you deploy key/value pairs to Windows 10 desktop or tablet devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device Policy Name	Device Policy Description
App Inventory	Collects an inventory of the apps on managed devices. Citrix Endpoint Management then compares the inventory to any app access policies deployed to those devices. In this way, you can detect apps that are on an allow list or block list for app access and then act correctly.
App Lock	Defines a list of apps that users either can or can't run on iOS or certain Android devices. Can turn an iPad into a kiosk.
App Permissions	Configures how requests to Android Enterprise apps within work profiles handle what Google calls "dangerous"permissions.
App Uninstall	Remove apps from user devices.
App Uninstall Restrictions	Specifies the apps that users can or can't uninstall.
Application Guard	For the Microsoft Edge browser only, this policy specifies Windows Defender Application Guard settings. The settings include whether to block external content on enterprise sites.
Apps Notifications	Controls how iOS users receive notifications from specified apps.
Automatically update managed apps	Controls how installed managed apps are updated on Android Enterprise devices.
BitLocker	Configures the settings available in the BitLocker interface on Windows 10 and Windows 11 devices.
Bluetooth	Enables or disables Bluetooth on iOS devices.
Browser	Defines whether user devices can use the browser or which browser functions the devices can use.
Calendar (CalDAV)	Adds a calendar (CalDAV) account to iOS or macOS devices. The CalDAV account enables users to synchronize scheduling data with any server that supports CalDAV.
Cellular	Configures cellular network settings.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device Policy Name	Device Policy Description
Connection scheduling	Required for Android devices to connect back in to Citrix Endpoint Management for MDM management, app push, and policy deployment. If you don't send this policy to devices and don't enable Google FCM, a device can't connect back to the server.
Contacts (CardDAV)	Adds an iOS contact (CardDAV) account to iOS or macOS devices. The CardDAV account enables users to synchronize contact data with any server that supports CardDAV.
Credentials	Enables integrated authentication with your PKI configuration in Citrix Endpoint Management. For example, with a PKI entity, a keystore, a credential provider, or a server certificate.
Custom XML	Customizes features such as provisioning devices, enabling device features, configuring devices, and managing faults.
Defender	Configures Windows Defender settings for Windows 10 and Windows 11 for desktop and tablet.
Device Guard	Enable security features such as secure boot, UEFI lock, and virtualization.
Device Health Attestation	Requires that Windows 10 and Windows 11 devices report the state of their health. To do that they send specific data and runtime information to the Health Attestation Service (HAS) for analysis. The HAS creates and returns a Health Attestation Certificate that the device then sends to Citrix Endpoint Management. When Citrix Endpoint Management receives the Health Attestation Certificate, based on the contents of that certificate, it can deploy the automatic actions that you configured.
Device Name	Sets the names on iOS and macOS devices so that you can identify the devices. You can use macros, text, or a combination of both to define a device name.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device Policy Name	Device Policy Description
Education Configuration	Configures instructor and student devices for use with Apple Education. If instructors use the Classroom app, the Education Configuration device policy is required. Supported for iOS (iPadOS) devices.
Citrix Endpoint Management Options	Configures the Citrix Secure Hub behavior when connecting to Citrix Endpoint Management from Android devices.
Citrix Endpoint Management Uninstall	Uninstalls Citrix Endpoint Management from Android devices. When deployed, this policy removes Citrix Endpoint Management from all devices in the deployment group.
Exchange	Enables ActiveSync email for the native email client on the device.
Files	Adds script files to Citrix Endpoint Management that do certain functions for users. Or, you can add document files that you want Android device users to access on their devices. When you add the file, you can also specify the directory in which you want the file to be stored on the device.
FileVault	This policy lets you enable FileVault device encryption on enrolled macOS devices. You can also control how many times a user can skip FileVault setup during login. Available for macOS 10.7 or later.
Firewall	Configures the firewall settings. You provide the IP addresses, ports, and host names that you want to allow or block on devices. You can also configure the proxy and proxy reroute settings.
Font	Adds fonts to iOS and macOS devices. Fonts must be TrueType (.TTF) or OpenType (.OFT) fonts. Citrix Endpoint Management doesn't support font collections (.TTC, .OTC).
Home screen layout	Specifies the layout of apps and folders for the iOS Home screen on supervised iOS devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device Policy Name	Device Policy Description
Import iOS & macOS Profile	Imports device configuration XML files for iOS and macOS devices into Citrix Endpoint Management. The file contains device security policies and restrictions that you prepare by using the Apple Configurator.
Keyguard Management	Controls the features available to users before they unlock the device keyguard and the work challenge keyguard. You can also control device keyguard features for fully managed and dedicated devices. For example, you can disable lock screen features such as fingerprint unlock, trust agents, and notifications.
Knox Platform for Enterprise Key	Allows you to provide the required Samsung Knox Platform for Enterprise (KPE) license information.
Launcher Configuration	Specifies settings for Citrix Launcher on Android devices, such as the apps allowed and a custom logo image for the Launcher icon.
LDAP	Provides information about an LDAP server to use for iOS devices, including any necessary account information such as the LDAP server host name. The policy also provides a set of LDAP search policies to use when querying the LDAP server.
Location	Lets you geo-locate devices on a map, assuming that the device has GPS enabled for Citrix Secure Hub. After deploying this policy to the device, you can send a locate command from Citrix Endpoint Management. The device then responds with its location coordinates. Citrix Endpoint Management also supports geofencing and tracking policies.
Lock screen message	Sets messages to appear on the following devices when they are lost: The login window of shared iPads and the lock screen of supervised iOS devices.
Mail	Configures an email account on iOS or macOS devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device Policy Name	Device Policy Description
Managed Configurations	Controls various app configuration options and app restrictions for Android Enterprise devices.
Managed Domains	Defines managed domains that apply to email and the Safari browser. Managed domains help you protect corporate data by controlling which apps can open documents downloaded from domains using Safari. For iOS supervised devices, you can specify URLs or subdomains to control how users can open documents, attachments, and downloads from the browser.
Maximum resident users	Specifies the maximum number of users for a Shared iPad. Supported for iOS and iPadOS devices.
MDM Options	Manages Find My Phone and iPad Activation Lock on supervised iOS devices.
Network	Allows administrators to deploy Wi-Fi router details to managed devices. The router details include SSID, authentication data, and configuration data.
Network Usage	Sets network usage rules to specify how managed apps use networks, such as cellular data networks, on iOS devices. The rules only apply to managed apps. Managed apps are apps that you deploy to user devices through Citrix Endpoint Management.
Office	Deploy Microsoft Office apps to any devices running Windows 10 (version 1709 or later) or Windows 11.
Organization Info	Specifies organization information for alert messages that Citrix Endpoint Management deploys to iOS devices.
OS Update	Deploys the latest OS updates to devices that are supported and supervised.
Passcode	Enforces a PIN code or password on a managed device. You can set the complexity and timeouts for the passcode on the device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device Policy Name	Device Policy Description
Passcode lock grace period	Specifies the number of minutes that a Shared iPad screen stays locked before the user must enter a passcode to unlock the screen. Supported for iOS and iPadOS devices.
Personal Hotspot	Allows users to connect to the internet when they are not in range of a Wi-Fi network. Users connect through the cellular data connection on their iOS device, using personal hotspot functionality.
Profile Removal	Removes the app profile from macOS devices.
Provisioning Profile	Specifies an enterprise distribution provisioning profile to send to devices. When you develop and code sign an iOS enterprise app, you usually include a provisioning profile. Apple requires the profile for the app to run on an iOS device. If a provisioning profile is missing or has expired, the app crashes when a user taps to open it.
Provisioning Profile Removal	Removes iOS provisioning profiles.
Proxy	Specifies global HTTP proxy settings for devices running iOS. You can deploy only one global HTTP proxy policy per device.
Restrictions	Provides hundreds of options to lock down and control features and functionality on managed devices. Examples of restriction options: Disable the camera or microphone, enforce roaming rules, and enforce access to third-party services, such as app stores.
Roaming	Configures whether to allow voice and data roaming on iOS devices. If voice roaming is disabled, data roaming is automatically disabled.
Samsung MDM License Key	Specifies the built-in Samsung Enterprise License Management (ELM) key that you must deploy to a device. Citrix Endpoint Management also supports the Samsung Enterprise Firmware-Over-The-Air (E-FOTA) service.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device Policy Name	Device Policy Description
SCEP	Configures iOS and macOS devices to retrieve a certificate from an external SCEP server. You can also deliver a certificate to the device using SCEP from a PKI that is connected to Citrix Endpoint Management. To do that, create a PKI entity and a PKI provider in distributed mode.
Single sign-on (SSO) Account	Creates SSO accounts so users sign on one-time only to access Citrix Endpoint Management and your internal company resources. Users do not need to store any credentials on the device. Citrix Endpoint Management uses the enterprise user credentials for an SSO account across apps, including apps from the App Store. This policy is compatible with Kerberos authentication. Available for iOS.
Storage Encryption	Encrypts internal and external storage. For some devices, this policy prevents users from using a storage card on their devices.
Store	Specifies whether an app store web clip appears on the home screen of user devices.
Subscribed Calendars	Adds a subscribed calendar to the calendar list on iOS devices. Make sure that you subscribe to a calendar before you add it to the subscribed calendars list on user devices.
Terms and Conditions	Requires that users accept the specific policies of your company that govern connections to the corporate network. When users enroll their devices with Citrix Endpoint Management, they must accept the terms and conditions to enroll their devices. Declining the terms and conditions cancels the enrollment process.
Tunnel	Define proxy parameters between the client component of any mobile device app and the app server component.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device Policy Name	Device Policy Description
VPN	Provides access to back end systems that use legacy VPN gateway technology. This policy provides VPN gateway connection details that you can deploy to devices. Citrix Endpoint Management supports several VPN providers, including Cisco AnyConnect, Juniper, and Citrix VPN. If your VPN gateway supports this option, you can link this policy to a CA and enable VPN on-demand.
Wallpaper	Adds a .png or .jpg file to set the wallpaper on an iOS device lock screen, home screen, or both. To use a different wallpaper on iPads and iPhones, create different wallpaper policies and deploy them to the appropriate users.
Web clip	Places shortcuts, or web clips, to websites so that they appear alongside apps on user devices. You can specify your own icons to represent the web clips for iOS, macOS, and Android devices. Windows tablet only requires a label and a URL.
Web Content Filter	Filters web content on iOS devices. Citrix Endpoint Management uses the Apple auto-filter function and the sites that you add to allow lists and block lists. Available only for iOS supervised devices.
Windows Agent	Enable this policy to run uploaded PowerShell scripts on Windows desktops and tablets.
Windows GPO configuration	Configure Group Policy Objects (GPOs) for any Windows device supported by Citrix Workspace Environment Management.
Windows Hello for Business	Enable the Windows feature so users can provision Windows Hello for Business on their device. The policy also lets you configure passcode limitations and other security features.

Device policies by platform

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Windows Desk-top/Tablet	Other
AirPlay mirroring device policy	X	X				
AirPrint device policy	X					
APN device policy	X			X		
App access device policy	X			X		
App attributes device policy	X					
App config-uration device policy	X				X	
App inventory device policy	X	X	X	X	X	
App lock device policy	X			X	X	
App permis-sions device policy			X			
App uninstall device policy	X	X	X	X		

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Windows Desk-top/Tablet	Other
App uninstall restrictions device policy						X
Application Guard device policy					X	
Apps notifi-cations device policy	X					
Automatically update managed apps			X			
BitLocker device policy					X	
Bluetooth device policy	X					
Browser device policy						X
Calendar (CalDav) device policy	X	X				
Cellular device policy	X					

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Windows Desk-top/Tablet	Other
Connection scheduling device policy			X	X		
Contacts (CardDAV) device policy	X	X				
Copy Apps to Samsung Container device policy						X
Credentials device policy	X	X	X	X	X	
Custom XML device policy			X		X	
Defender device policy					X	
Device Guard device policy					X	
Device Health Attestation device policy					X	
Device name device policy	X	X				

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Windows Desktop/Tablet	Other
Education Configuration device policy	X					
Citrix Endpoint Management options device policy			X	X		
Citrix Endpoint Management uninstall device policy				X		
Exchange device policy	X	X	X	X	X	
Files device policy			X	X		
FileVault device policy		X				
Firewall device policy		X			X	
Font device policy	X	X				

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Windows Desk-top/Tablet	Other
Home screen layout device policy	X					
Import Device Con-figuration device policy						X
Import iOS & macOS Profile device policy	X	X				
Keyguard Manage-ment device policy			X			
Kiosk device policy			X		X	
Launcher configura-tion device policy			X	X		
LDAP device policy	X	X				
Location device policy	X		X	X		

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Windows Desk-top/Tablet	Other
Lock screen message device policy	X					
Mail device policy	X	X				
Managed configura-tions device policy			X			
Managed domains device policy	X					
Maximum resident users device policy	X					
MDM options device policy	X					
Network device policy	X		X	X		
Network usage device policy	X					
Office device policy					X	

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Windows Desk-top/Tablet	Other
Organization information device policy	X					
OS Update device policy	X	X	X		X	
Passcode device policy	X	X	X	X	X	
Passcode lock grace period device policy	X					
Personal hotspot device policy	X					
Profile Removal device policy	X	X				
Provisioning profile device policy	X					
Provisioning profile removal device policy	X					
Proxy device policy	X					

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Windows Desk-top/Tablet	Other
Restrictions device policy	X	X		X	X	
Roaming device policy	X					
Samsung MDM license key device policy			X			
SCEP device policy	X	X				
Siri and dictation policies	X					
SSO account device policy	X					
Storage encryption device policy						
Store device policy	X			X	X	
Subscribed calendars device policy	X					

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Policy	iOS	macOS	Android Enterprise	Android (Legacy DA)	Windows Desk-top/Tablet	Other
Terms and conditions device policy	X			X	X	
Tunnel device policy				X		
VPN device policy	X	X		X	X	
Wallpaper device policy	X					
Web clip device policy	X	X		X	X	
Web content filter device policy	X					
Windows Agent device policy					X	
Windows GPO config-uration device policy					X	
Windows Hello for Business device policy					X	

© 1997–2025 Citrix Systems, Inc. All rights reserved.

AirPlay mirroring device policy

September 6, 2025

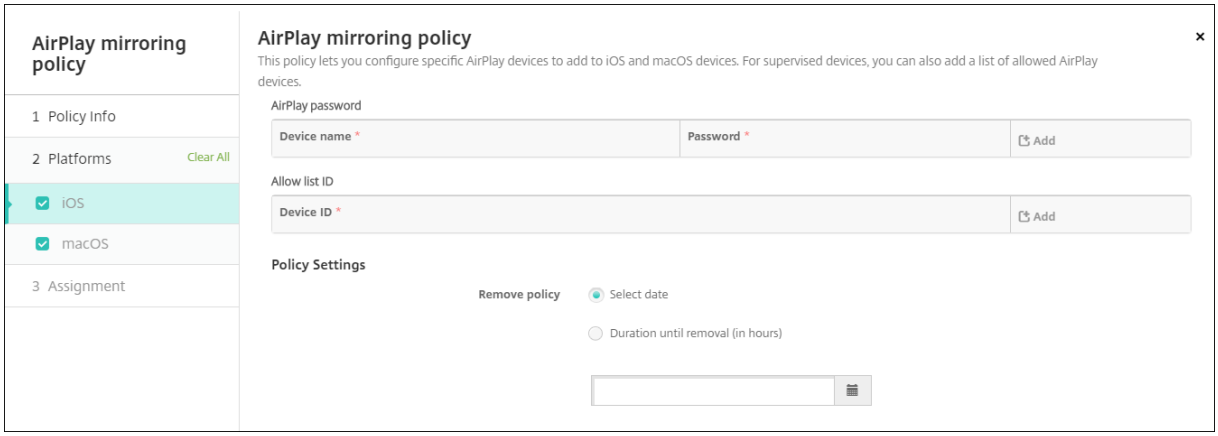
The Apple AirPlay feature allows users to stream content wirelessly from an iOS device to a TV screen through Apple TV, or to mirror exactly what's on a device display to a TV screen or another Mac computer.

You can add a device policy in Citrix Endpoint Management to add specific AirPlay devices (such as Apple TV or another Mac computer) to iOS devices. You also have the option of adding devices to an allow list for supervised devices, which limits users to only those AirPlay devices. For information about placing a device into Supervised mode, see Deploy devices using Apple Configurator 2.

> **Note:**
>
> Before proceeding, be sure to have the device IDs and any passwords for all the devices you want to add.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

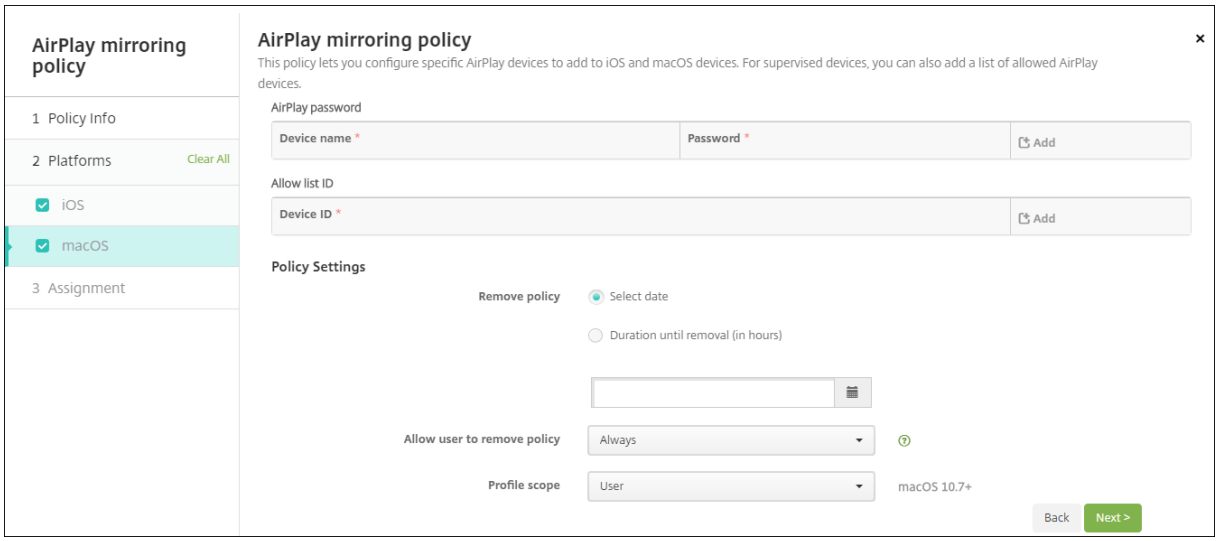


- **AirPlay Password:** For each device you want to add, click **Add** and then do the following:
  - **Device name:** Enter the hardware address (MAC address) in xx:xx:xx:xx:xx:xx format. This field isn't case-sensitive.
  - **Password:** Enter an optional password for the device.
  - Click **Add** to add the device or click **Cancel** to cancel adding the device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Allow list ID:** This list is ignored for unsupervised devices. The device IDs in this list are the only AirPlay devices available to users devices. For each AirPlay device you want to add to the list, click **Add** and then do the following:
  - **Device ID:** Type the device ID in the xx:xx:xx:xx:xx:xx format. This field isn't case-sensitive.
  - Click **Add** to add the device or click **Cancel** to cancel adding the device.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

macOS settings



- **AirPlay Password:** For each device you want to add, click **Add** and then do the following:
  - **Device name:** Enter the hardware address (MAC address) in xx:xx:xx:xx:xx:xx format. This field isn't case-sensitive.
  - **Password:** Enter an optional password for the device.
  - Click **Add** to add the device or click **Cancel** to cancel adding the device.
- **Allow list ID:** This list is ignored for unsupervised devices. The device IDs in this list are the only AirPlay devices available to users devices. For each AirPlay device you want to add to the list, click **Add** and then do the following:
  - **Device ID:** Type the device ID in the xx:xx:xx:xx:xx:xx format. This field isn't case-sensitive.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - Click **Add** to add the device or click **Cancel** to cancel adding the device.

- **Policy settings**

  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    * **Select date:** Click the calendar to select the specific date for removal.
    * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

AirPrint device policy

September 6, 2025

The AirPrint device policy adds AirPrint printers to the AirPrint printer list on iOS devices. This policy makes it easier to support environments where the printers and the devices are on different subnets.

> **Note:**
>
> To configure the AirPrint device policy, you need the IP address and resource path for each printer.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **AirPrint Destination:** For each AirPrint destination you want to add, click **Add** and then do the following:

  - **IP Address:** Enter the AirPrint printer IP address.
  - **Resource Path:** Enter the Resource Path associated with the printer. This value corresponds to the parameter of the `_ipps.tcp` Bonjour record. For example, `printers/Canon_MG5300_series` or `printers/Xerox_Phaser_7600`.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 or later.

App permissions device policy

September 6, 2025

For Android Enterprise apps that are within work profiles: You can configure how requests to those apps handle what Google calls "dangerous"permissions. You control whether the user is prompted to grant or deny the permission request from the app. This feature applies to devices running Android 7.0 and later.

Google defines dangerous permissions as permissions that:

- Give the app access to data or resources that involve the user's private information.
- Or, can potentially affect the user's stored data or the operation of other apps. For example, the ability to read user contacts is a dangerous permission.

You can configure a global status to control the behavior of all dangerous permission requests. The scope of this configuration is Android Enterprise apps that are within work profiles. You can also control the behavior of a dangerous permission request for individual permission groups, as defined by Google, for each app. These individual settings override the global status.

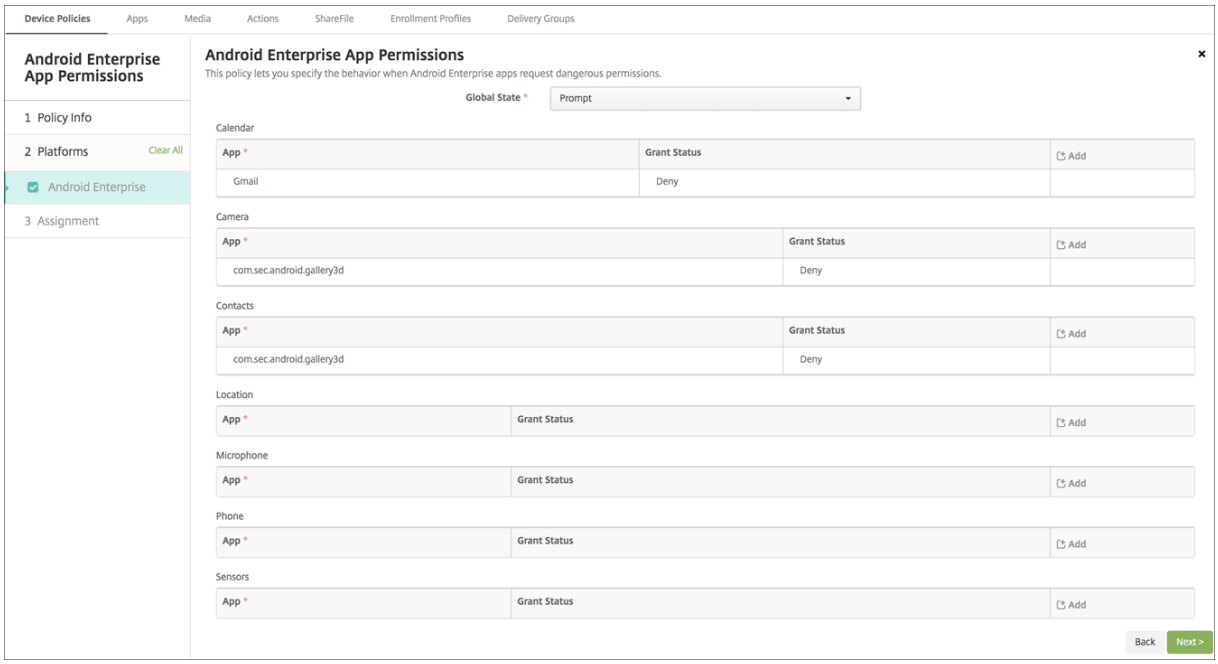
For information on how Google defines permission groups, see the Android developers guide.

By default, users are prompted to grant of deny dangerous permission requests.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Android Enterprise settings



- **Global State:** Controls the behavior of all dangerous permission requests. In the list, click **Prompt**, **Grant**, or **Deny**.
  - **Prompt:** Users are prompted to grant or deny dangerous permission requests.
  - **Grant:** All dangerous permission requests are granted. The user isn't prompted.
  - **Deny:** All dangerous permission requests are denied. The user isn't prompted.

  Default is **Prompt**.

- Set an individual behavior for each permission group, for each app. To configure the behavior for a permission group: Click **Add**. Then under **App**, choose an app from the list. If you configure Android Enterprise system apps, click **Add new** and enter the application package name you enabled in the Restrictions device policy. Under Grant Status, choose **Prompt**, **Grant**, or **Deny**. This grant status overrides the global status.
  - **Prompt:** Users are prompted to grant or deny dangerous permission requests from this permission group for this app.
  - **Grant:** Dangerous permission requests from this permission group for this app are granted. The user isn't prompted.

    > **Note:**
    >
    > For the devices enrolled in the **Profile Owner** mode, **Grant** permission isn't applica-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> ble for Camera, Location, Microphone, and Sensor if the device is running on Android 12 or later.

- **Deny:** Dangerous permission requests from this permission group for this app are denied. The user isn't prompted.

Default is **Prompt**.

- Click **Save** next to the app and grant status.
- To add more apps for the permission group, click **Add** again and repeat these steps.
- When you have finished setting the **Grant Status** for permission groups, click **Next**.

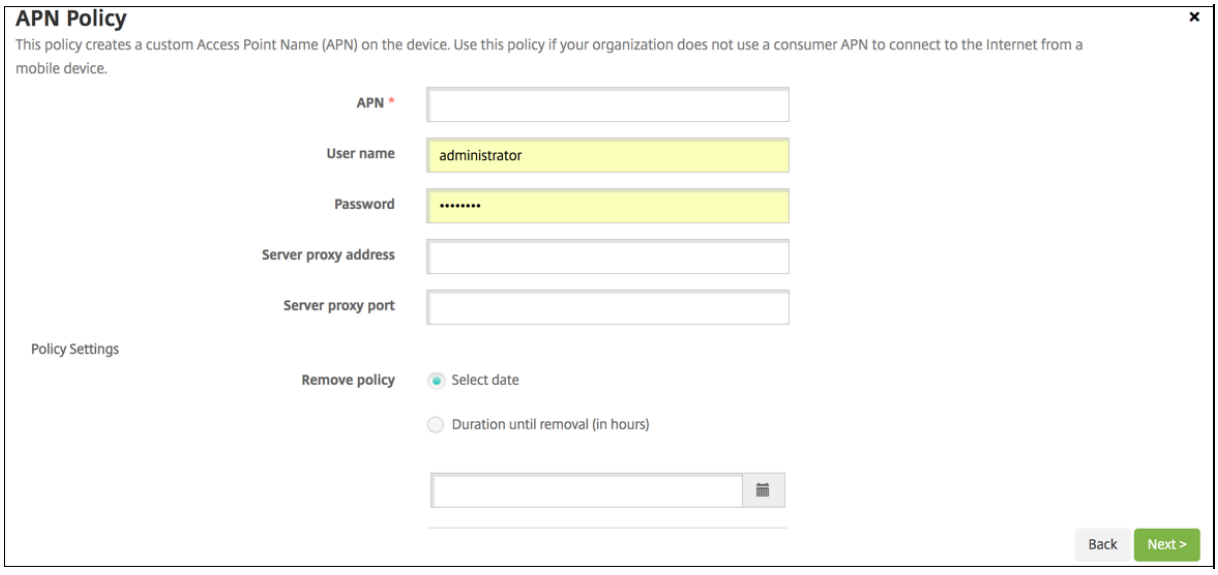
APN device policy

September 6, 2025

You can add a custom Access Point Name (APN) device policy for iOS and Android devices. You use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device. An APN policy determines the settings used to connect your devices to a specific phone carrier's General Packet Radio Service (GPRS). This setting is already defined in most newer phones.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

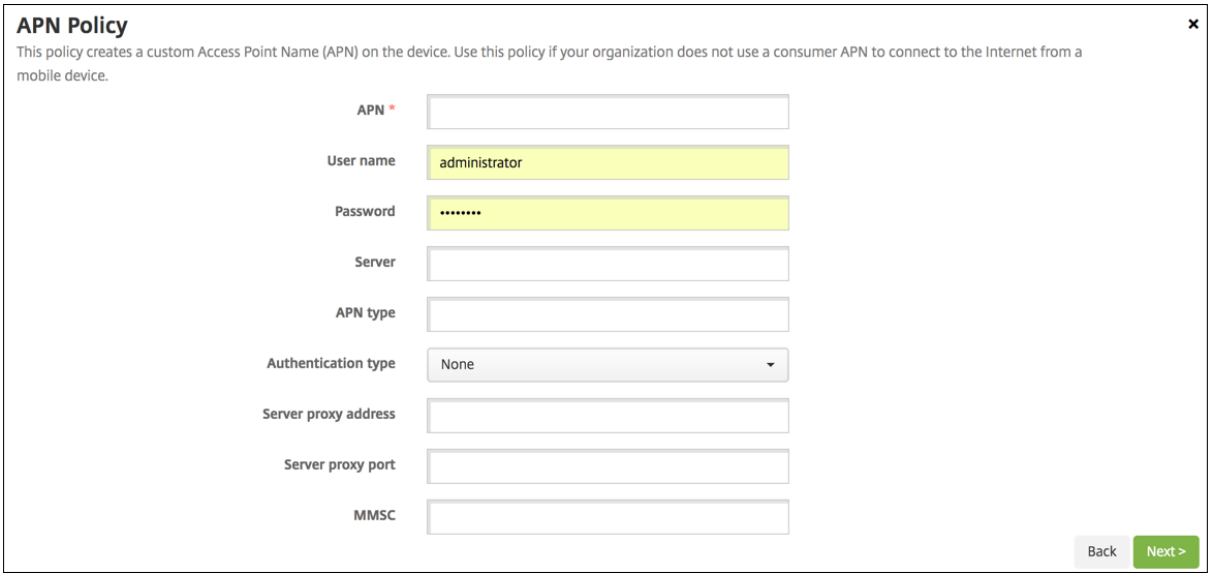
iOS settings



© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **APN:** Type the name of the access point. The name must match an accepted iOS APN or the policy doesn't work.
- **User name:** This string specifies the user name for this APN. If the user name is missing, the device prompts for the string during profile installation.
- **Password:** The password for the user for this APN. For obfuscation purposes, the password is encoded. If it is missing from the payload, the device prompts for the password during profile installation.
- **Server proxy address:** The IP address or URL of the APN proxy.
- **Server proxy port:** The port number for the APN proxy. The port number is required if you entered a server proxy address.
- Under **Policy Settings**, next to **Remove policy**, click either **Select date** or **Duration until removal (in hours)**.
  - For the option **Select date**, click the calendar to select the specific date for removal.
  - For the option **Password required**, type the password.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 or later.

Android settings



© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **APN:** Type the name of the access point. The name must match an accepted Android APN or the policy doesn't work.
- **User name:** This string specifies the user name for this APN. If the user name is missing, the device prompts for the string during profile installation.
- **Password:** The password for the user for this APN. For obfuscation purposes, the password is encoded. If it is missing from the payload, the device prompts for the password during profile installation.
- **Server:** This setting, which predates smart phones, is usually empty. It references a Wireless Application Protocol (WAP) gateway server for phones that can't access or render standard websites.
- **APN type:** This setting must match the carrier's intended use for the access point. It is a comma-separated string of APN service specifiers and must match the wireless carrier's published definitions. Examples include:
  - `\*`: All traffic goes through this access point.
  - `mms`: Multimedia traffic goes through this access point.
  - **`default`**: All traffic, including multimedia, goes through this access point.
  - `supl`: Secure User Plane Location is associated with assisted GPS.
  - `dun`: Dial Up Networking is outdated and rarely used.
  - `hipri.`: High priority networking.
  - `fota`: Firmware over the air is used for receiving firmware updates.
- **Authentication type:** Click the type of authentication to be used in the drop-down list. Defaults to None.
- **Server proxy address:** The IP address or URL of the carrier's APN HTTP proxy.
- **Server proxy port:** The port number for the APN proxy. The port is required if you entered a server proxy address.
- **MMSC:** The MMS Gateway Server address provided by the carrier.
- **Multimedia Messaging Server (MMS) proxy address:** The address for the multimedia messaging service server for MMS traffic. MMS succeeded SMS for sending larger messages with multimedia content, such as pictures or videos. These servers require specific protocols (such as MM1, …MM11).
- **MMS port:** The port used for the MMS proxy.

App access device policy

March 6, 2024

The app access device policy allows you to define a list of apps that must be installed, can be installed, or must not be installed. If the apps on a device contradict this policy, Citrix Endpoint Management

© 1997–2025 Citrix Systems, Inc. All rights reserved.

marks the device as out of compliance. You can then create an automated action to react to that device compliance.

> **Important:**
>
> The app access device policy doesn't prevent a user from installing a forbidden app or uninstalling a required app.

You can only configure one type of access policy at a time. Each policy has a list of required apps, suggested apps, or forbidden apps, but not a mix within the same app access policy. If you create a policy for each type of list, name each policy carefully, so you know which policy applies to which list of apps.

To add or configure this policy, go to **Configure** > **Device Policies**. For more information, see Device policies.

iOS and Android (legacy DA) settings

- **Access policy:** Select the type of list to configure for this policy.
  - **Required:** The app must exist on the device. If the app doesn't exist, the device is marked as out of compliance. **Required** is the default option.
  - **Forbidden:** The app must not exist on the device. If the app does exist, the device is marked as out of compliance.
- To add one or more apps to the list:
  1. Click **Add** and then configure the following:
     - **App name:** Enter an app name.
     - **App Identifier:** Enter an optional app identifier.
  2. Click **Save**.
  3. Repeat these steps for each app that you want to add.

Configure automated actions based on app access compliance

1. Add an app access policy to require or forbid apps.
2. Configure two automated actions based on whether the apps in question are required or forbidden:
   - Required
     - Mark a device as out of compliance if a required app doesn't exist on the device.
     - Mark a device as compliant once that required app is installed.
   - Forbidden

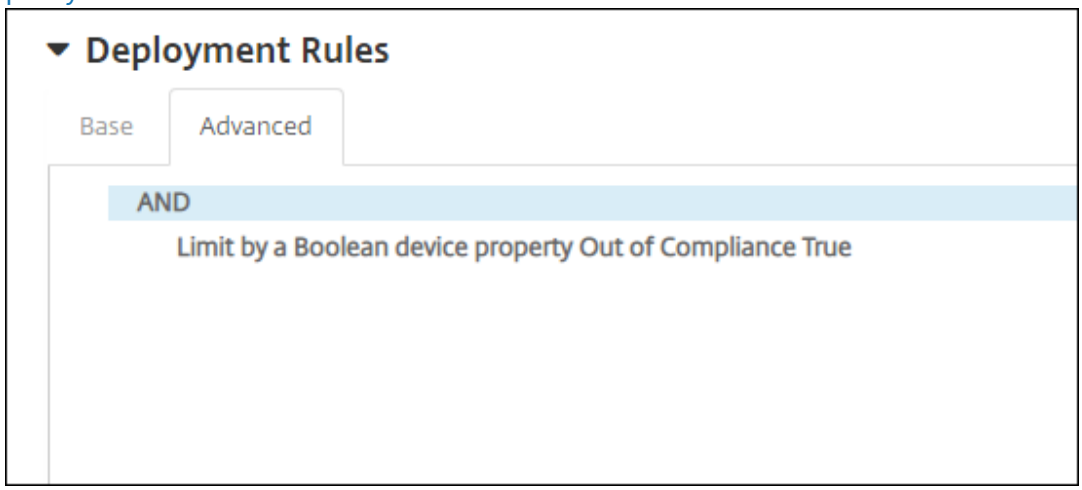
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Mark a device as out of compliance if a forbidden app exists on the device.
- Mark a device as compliant once that forbidden app is no longer installed.

  For information on setting up automated actions, see Automated actions.

3. Create a restriction policy with the settings that you want to implement on out of compliance devices.

   a) As part of the restriction policy, add an advanced deployment rule with the options **Limit by a Boolean device property**, **Out of Compliance**, and **True**. See Restrictions device policy.



4. Create a profile removal policy to remove the restriction policy once the device is back in compliance.
5. Add an advanced deployment rule with the options **Limit by a Boolean device property**, **Out of Compliance**, and **False**. See Profile removal device policy.

App attributes device policy

March 6, 2024

The **App attributes** device policy lets you specify attributes for apps on iOS devices. By configuring this type of policy, you can accomplish the following:

- Assign per app VPNs to apps.
- Prevent users from uninstalling mission-critical apps. Applies to iOS 14 and later.
- If the Associated Domains feature is enabled, specify associated domains to add to apps. Applies to iOS 13 and later.

  For more information, see About Associated Domains.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

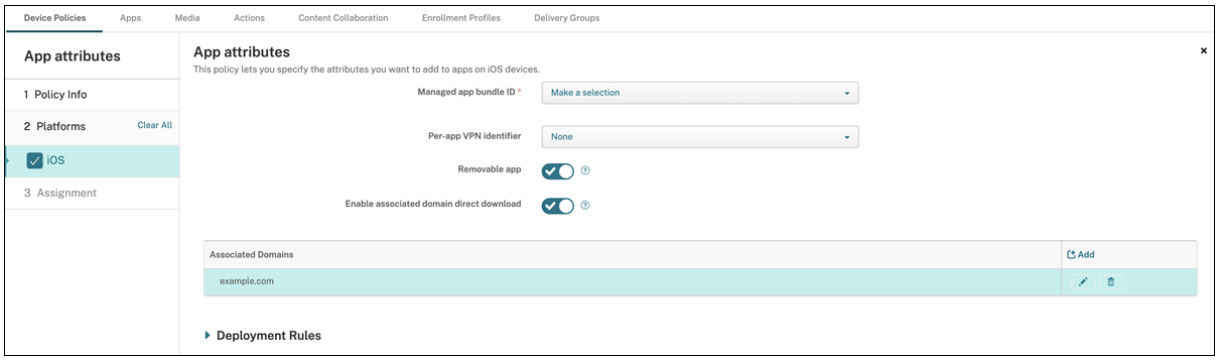
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

About Associated Domains

Associated Domains let you establish a secure association between domains and your app so you can share credentials or provide features in your app from your websites. For example, with this feature enabled, you can share data and sign-in credentials between apps and websites in your organization.

For more information about how to enable this feature, see Supporting Associated Domains on Apple's website.

iOS settings



- **Managed app bundle ID:** Specify an app in the following ways:
  - Select the app bundle ID. Options are available only after you enable the **App Inventory** device policy, which collects an inventory of apps on managed devices.
  - Select **Add new**, and then type the app bundle ID.
    To find an app bundle ID, see Find the bundle ID for an app in the App Store.
- **Per-app VPN identifier:** (Optional) Select a per app VPN for this app. Options include the per app VPN connections that you configured on the **Device Policies > VPN Policy** page.
  For more information, see Configure a per app VPN.
- **Removable app:** (Optional) Specify whether this app is removable by users when it's a managed app. To prevent users from uninstalling this app, set this option to **Off**. The default is **On**.
- **Enable associated domain direct download:** (Optional) The default is **On**, indicating this app does claimed site association verification directly at the domain instead of on Apple's servers. Set this option to **On** only for domains that can't access the Internet.
- **Associated Domains:** (Optional) To add an Associated Domain for this app, click **Add**, and then type its fully qualified domain name (FQDN).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Find the bundle ID for an app in the App Store

1. Locate the app in the App Store and copy the number at the end of the URL. For example, 363501921 is the app ID for Citrix Workspace app.
2. Go to `https://itunes.apple.com/lookup?id=` and paste the number after that URL. A TXT file is downloaded to your computer automatically.
3. In the TXT file, search for `bundleId` and get the bundle ID of the app. Example: the bundle ID for Citrix Workspace app is `com.citrix.ReceiveriPad`.

App configuration device policy

March 6, 2024

You can remotely configure apps that support managed configuration by deploying:

- An XML configuration file (`.plist`, also called a property list) to iOS devices
- Key/value pairs for Phone, Desktop, or Tablet devices running Windows 10 or Windows 11

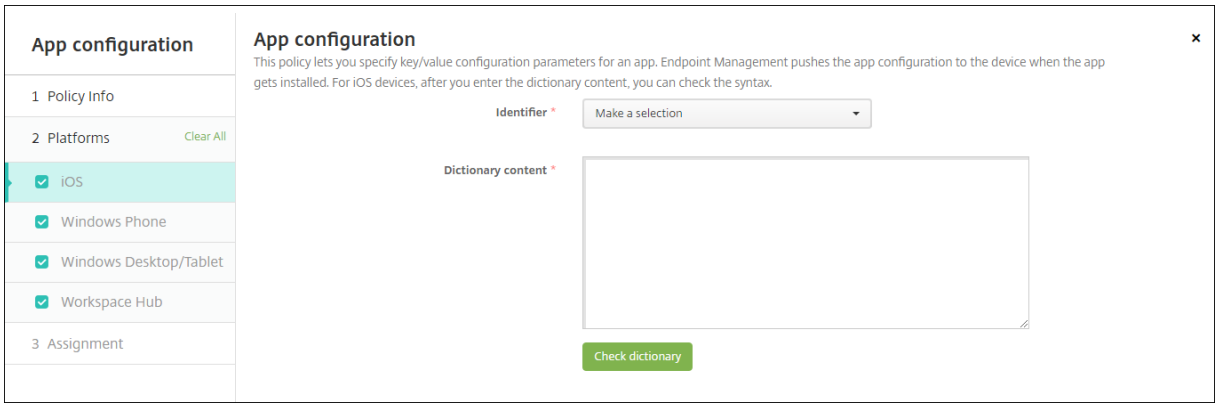
The configuration specifies various settings and behaviors in the app. Citrix Endpoint Management pushes the configuration to devices when the user installs the app. The actual settings and behaviors that you can configure depend on the app and are beyond the scope of this article.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

> **Note:**
>
> The respective application owners define the app configuration variables.
> For example, Chrome manages and maintains the app configuration variables for Chrome. For more information, see Chrome app configuration variables.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS settings



- **Identifier:** Click the app that you want to configure in the drop-down list, or click **Add new** to add an app to the list.
  - If you click **Add new**, type the app identifier in the field that appears.
- **Dictionary content:** Type, or copy and paste, the XML property list (`.plist`) configuration information.
- Click **Check dictionary**. Citrix Endpoint Management verifies the XML. If there are no errors, you see **Valid XML** below the content box. If any syntax errors appear below the content box, you must correct them before you can continue.

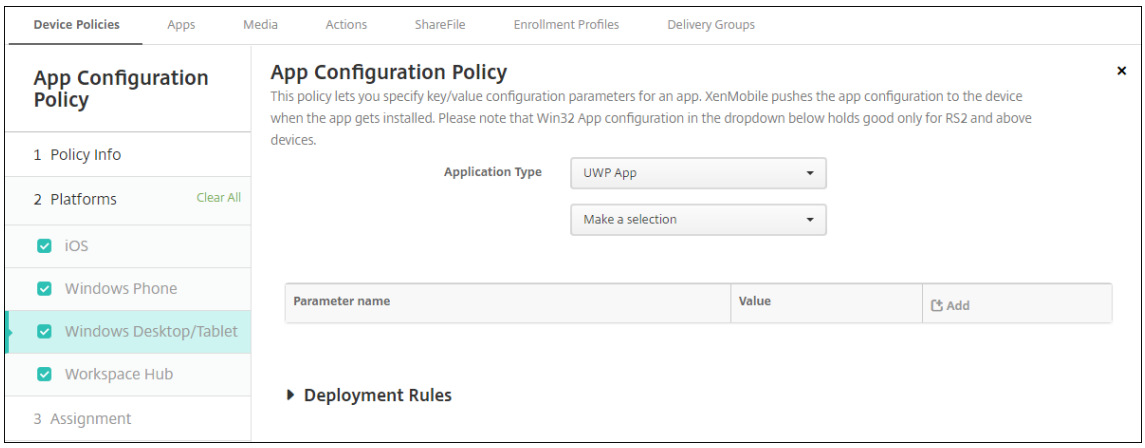
Windows Desktop/Tablet settings

You can configure either Universal Windows Platform (UWP) apps or Win 32 apps. To import Microsoft Administrative Template (ADMX) policy settings, configure Win 32 apps.

> **Note:**
>
> The App Configuration device policy supports third-party ADMX files for third-party applications such as Office. Not supported are Microsoft ADMX templates for Windows that are provided as operating system Group Policies available under `%SystemRoot%\PolicyDefinitions`.

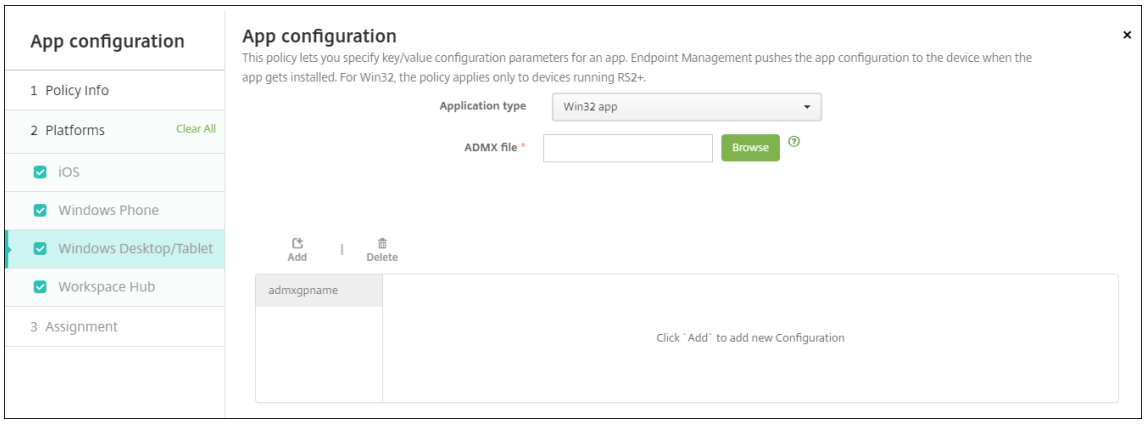
- If you choose **UWP App:** In the **Make a selection** list, click the app you want to configure or click **Add new** to add an app to the list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



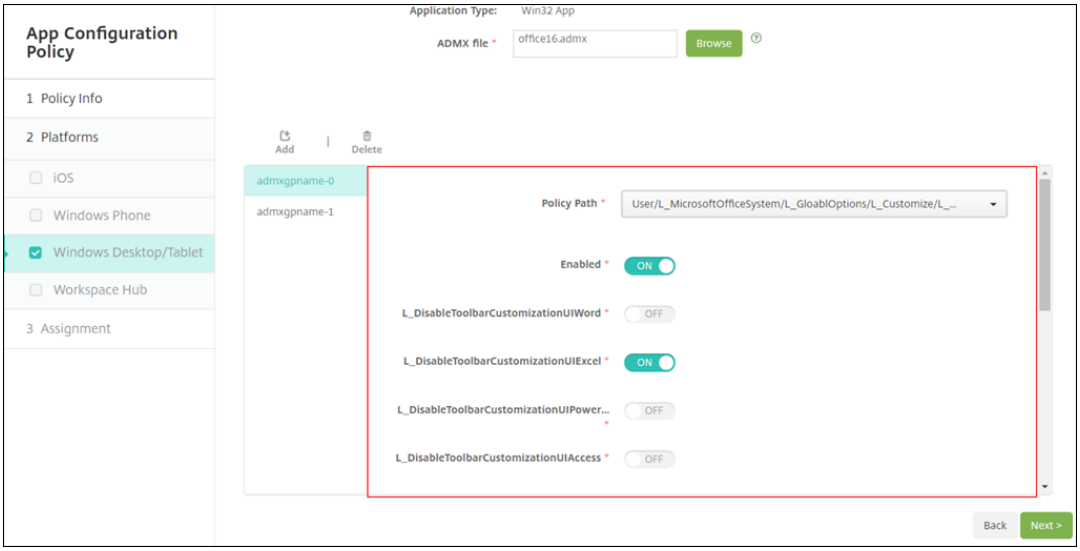
- If you click **Add new**, type the package family name in the field that appears.
- For each configuration parameter you want to add, click **Add** and then do the following:
  - **Parameter name:** Enter the key name of an application setting for the Windows device. For information about Windows app settings, refer to the Microsoft documentation.
  - **Value:** Enter the value for the specified parameter.
  - Click **Add** to add the parameter or click **Cancel** to cancel adding the parameter.

- If you choose **Win32 App:** Click **Browse** and navigate to the ADMX file you want to use to configure the policy.



- Click **Add**. Configuration options from the ADMX file appear on the right side of the page.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- Choose a policy path. If you choose the same path more than once, the configuration associated with the most recent version is enforced.
- Set **Enable** to **On**.
- Input any required list element values as key-value pairs. Use the text string **&#xF000** to separate each key-value pair and the value and key within the pair.
- Element values that include a decimal might require values within a specific range.

App inventory device policy

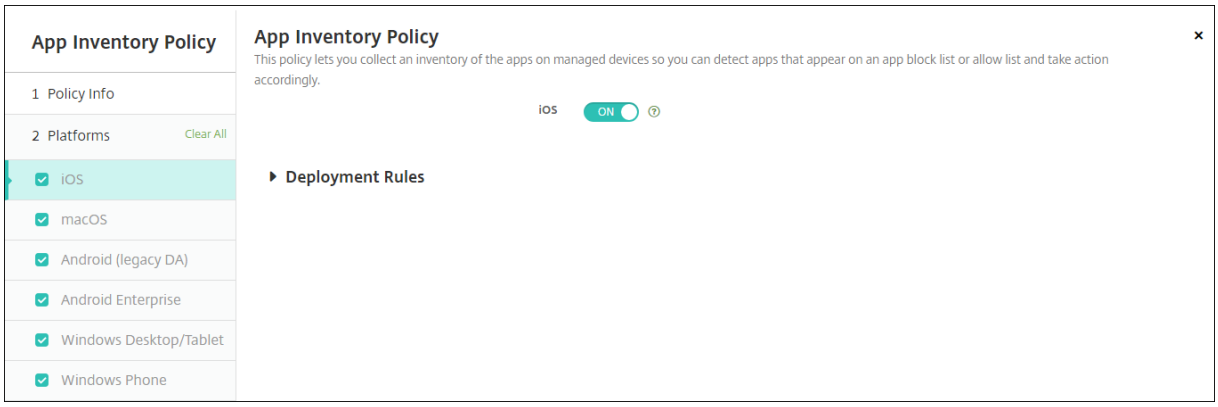
September 6, 2025

The App inventory policy lets you collect an inventory of the apps on managed devices. Citrix Endpoint Management can then compare the inventory to any app access policies deployed to those devices. In this way, you can detect apps that appear on an app allow list or block list and act correctly. Use an App access policy to define the allow list or block list.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS, macOS, Android (legacy DA), Android Enterprise, and Windows Desktop/Tablet



- For each platform you select, leave the default setting or change the setting to **Off**. The default is **On**.

Inventory and delete `Win32` apps

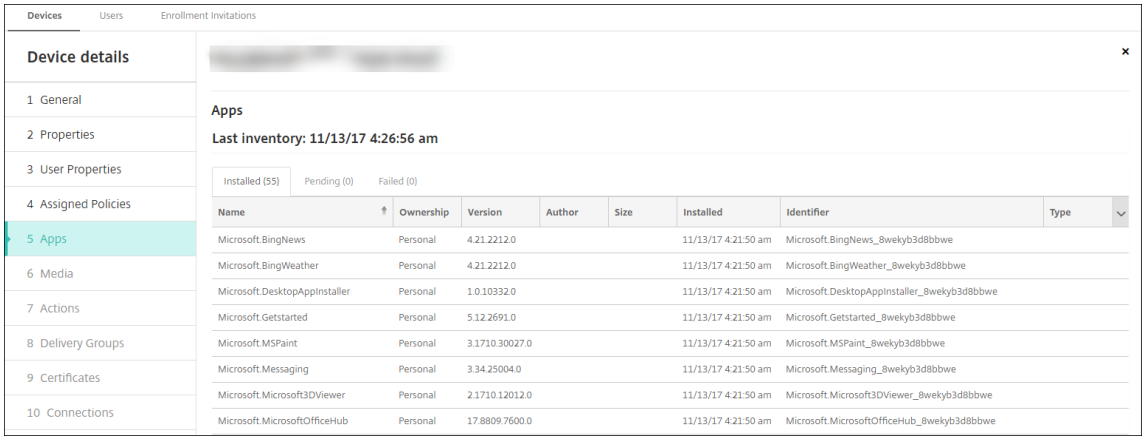
You can determine whether the `Win32` apps on user devices follow your App access device policy. To view an inventory of `Win32` apps on managed Windows 10 and Windows 11 Desktop and Tablet devices:

1. Go to **Configure > Device Policies** and add an App Inventory policy for the **Windows Desktop/Tablet** platform. Deploy the policy.
2. Go to **Manage > Devices**, select the Windows 10 and Windows 11 device that you want to view, click **Edit**, and then click the **Apps** tab.

   The results of the inventory appear.

   > **Note:**
   >
   > If you're configuring a Windows 11 device, you must wait up to 24 hours for correct inventory results, as designed by Microsoft.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Compare the app inventory to your App access device policy. If the device has apps installed that are on the block list, you can delete them from the device.

App install and uninstall issues caused by an incorrect Product Code

If a `Win32` app is configured with the incorrect Product Code, the app initially installs, however Microsoft doesn't return the app status to Citrix Endpoint Management. As a result:

- The App Uninstall device policy doesn't uninstall the app.
- Citrix Endpoint Management continues to deploy the app because it doesn't have confirmation that the app installed. With each deployment, the device generates an error code because the app is already installed. The error shown in **Manage > Device > Delivery Group Details** is: `Msi Application received: Reporting:AppPush id:7z1701-x64.msi: Command execution failed -2147023293`

To correct the Product Code:

1. Manually remove the app from the device.
2. In the Citrix Endpoint Management console, go to **Configure > Apps** and correct the Product Code for the `Win32` app.
3. Deploy the `Win32` app.

Application Guard device policy

March 6, 2024

The Application Guard policy specifies Windows Defender Application Guard settings. The settings include whether to enable Application Guard and controls for clipboard behavior.

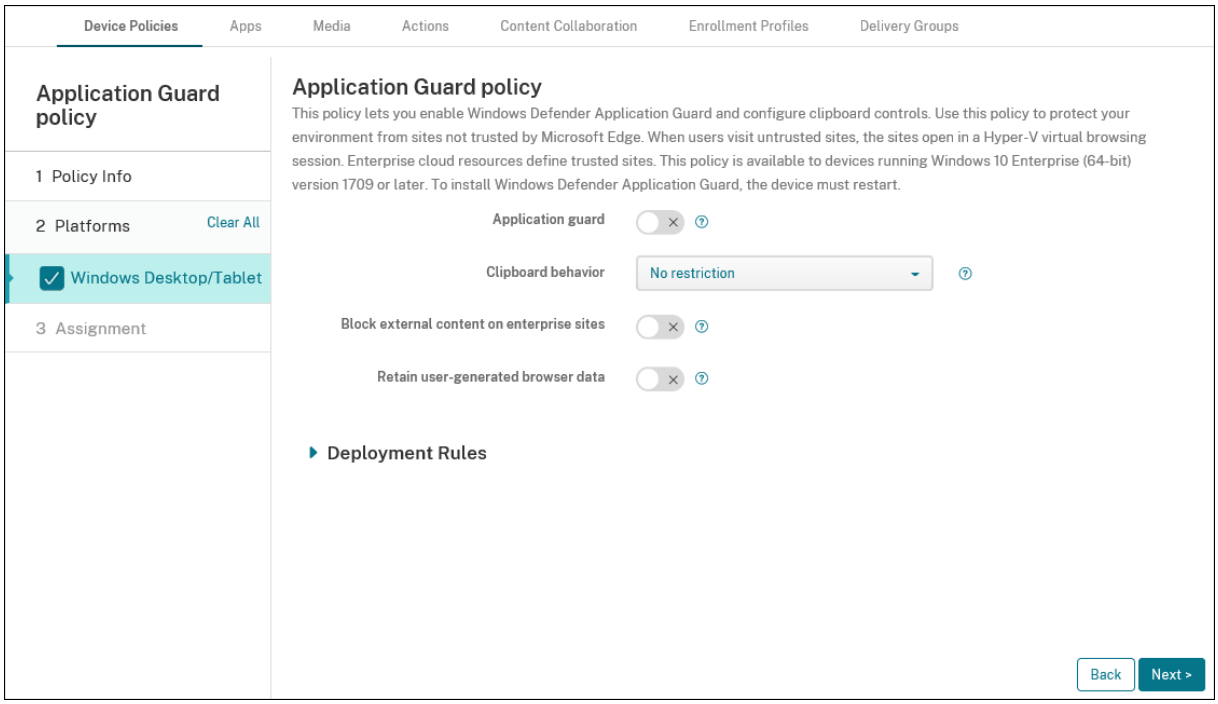
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Windows Defender Application Guard protects your environment from sites that haven't been defined as trusted by your organization. When users visit sites that aren't listed in your isolated network boundary: The sites open in a virtual browsing session in Hyper-V. Enterprise cloud resources define trusted sites.

Requirements

- Devices running Windows 10 Enterprise (64-bit) or Windows 11 Enterprise (64-bit). A device restart is required to install the Windows Defender Application Guard.
- Microsoft Edge browser

Windows Desktop and Tablet settings



- **Application guard:** Enables Application Guard. Default is **Off**.
  - **Enterprise cloud resources:** A comma-separated list of enterprise cloud domains.
- **Clipboard behavior:** Controls which directions content can be copied and pasted. The options are as follows:
  - **Not configured**
  - **Allow copy and paste only from browser to PC:** Allows users to copy and paste content only from their browser to their PC.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Allow copy and paste only from PC to browser:** Allows users to copy and paste content only from their PC to their browser.
  - **Allow copy and paste between PC and browser:** Allows users to copy and paste content freely between their PC and browser.
  - **Block copy and paste between PC and browser:** Does not allow users to copy and paste content between their PC and browser.

- **Clipboard content:** Controls which content users can copy and paste. The options are as follows:

  - **No restriction**
  - **Allow text copying:** Allows users to copy text only.
  - **Allow image copying:** Allows users to copy images only.
  - **Allow both text and image copying:** Allows users to copy both text and images.

- **Block external content on enterprise sites:** If **On** then the Windows Defender Application Guard prevents content from unapproved sites from loading on enterprise sites. Default is **Off**.
- **Retain user-generated browser data:** If **On** then allows saving user data created during an Application Guard virtual browsing session. This data includes things like passwords, favorites, and cookies. Default is **Off**.

App lock device policy

September 6, 2025

The App lock device policy defines a list of apps that are either:

- Allowed to run on a device.
- Blocked from running on a device.

The exact way that the policy works differs for each supported platform. For example, you can't block multiple apps on an iOS device.

Likewise, for iOS devices, you can select only one iOS app per policy. Users are only able to use their device to run a single app. They can't do any other activities on the device except for the options you specifically allow when the App lock device policy is enforced.

Also, the iOS devices must be supervised to push app lock policies.

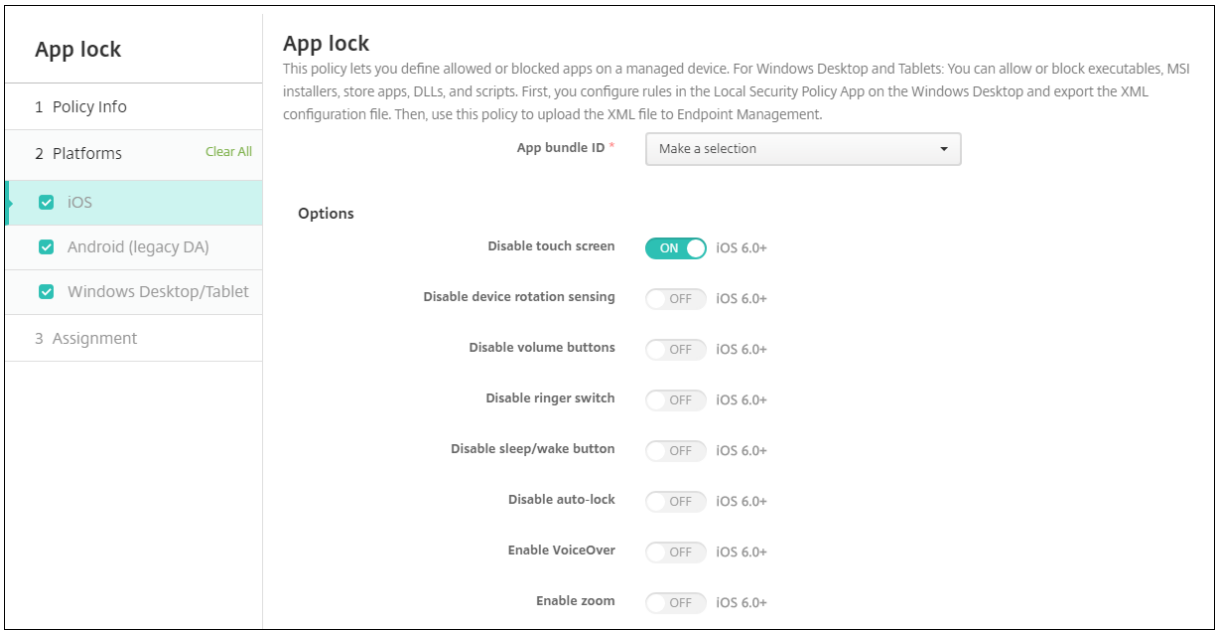
Although the device policy works on most Android L and M devices, app lock doesn't function on Android N or later devices. It doesn't work because Google deprecated the required API.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For managed Windows Desktops and Tablets, you can create an App lock device policy that defines the list of apps on the allow and block lists. You can allow or block executables, MSI installers, store apps, DLLs, and scripts.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **App bundle ID:** Click the app in the drop-down list to which this policy applies, or click **Add new** to add an app to the list. If you select **Add new**, type the app name in the field that appears.
- **Options:** For each option, the default is **Off** except for **Disable touch screen**, which defaults to **On**.
  - Disable touch screen
  - Disable device rotation sensing
  - Disable volume buttons
  - Disable ringer switch

    When **Disable ringer switch** is **On**, the ringer behavior depends on what position the switch was in when it was first disabled.
  - Disable sleep/wake button
  - Disable auto lock
  - Disable VoiceOver
  - Enable zoom

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - Enable invert colors
  - Enable AssistiveTouch
  - Enable speak selection
  - Enable mono audio
  - Enable voice control

- **User Enabled Options:** For each option, the default is **Off**.
  - Allow VoiceOver adjustment
  - Allow zoom adjustment
  - Allow invert colors adjustment
  - Allow AssitiveTouch adjustment
  - Allow voice control adjustment

- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    * **Select date:** Click the calendar to select the specific date for removal.
    * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 or later.

Configure an iPad as a kiosk

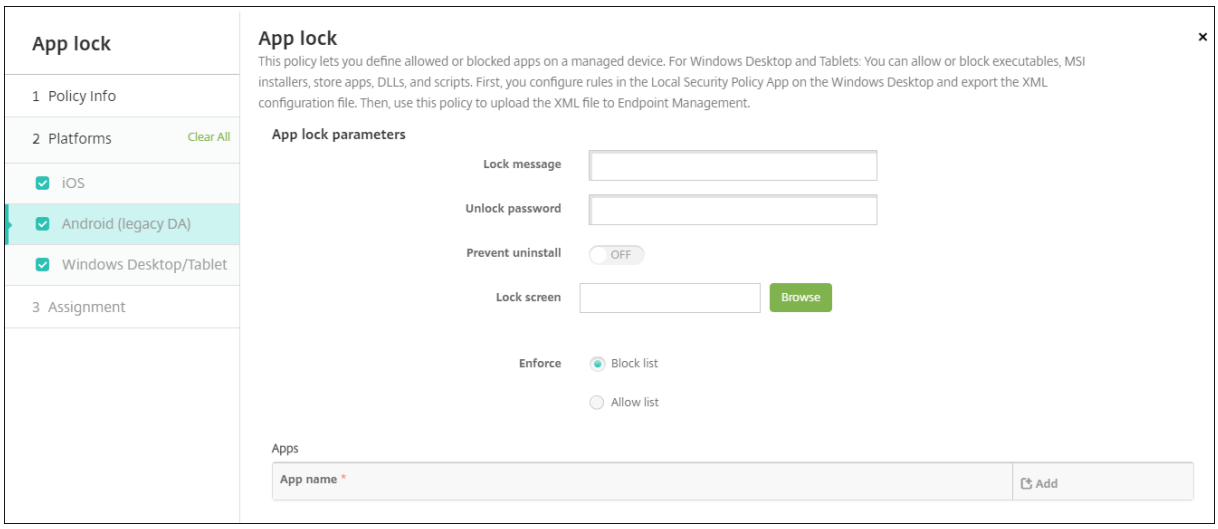
You can use the App lock device policy to run a supervised iPad as a kiosk. Apple refers to this feature as Single App Mode. For more information about this feature, see the Apple documentation. Make sure that you deploy the app you want to run before deploying this policy.

1. Navigate to **Configure > Device policies** and click **Add**.
2. Select the **App Lock** policy.
3. Type a **Policy Name** and optional **Description**.
4. Select only the **iOS** platform.
5. For **App bundle ID**, select the app you want to run on the iPad.
6. Configure any options that you want, as described previously, and save the policy.
7. Add the policy to the same delivery group as your iPad and deploy the policy.

Android (legacy DA) settings

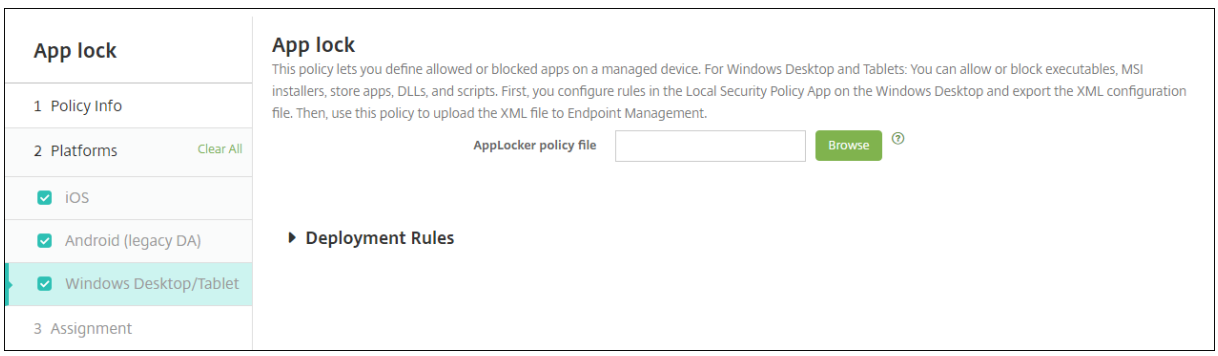
> **Note:**
>
> You can't block the Android Settings app by using the App Lock device policy.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **App Lock parameters**
  - **Lock message:** Type a message that users see when they try to open a locked app.
  - **Unlock password:** Type the password to unlock the app.
  - **Prevent uninstall:** Select whether users are allowed to uninstall apps. The default is **Off**.
  - **Lock screen:** Select the image that appears on the device's lock screen by clicking **Browse** and navigating to the file's location.
  - **Enforce:** Click **Block list** to create a list of apps that aren't allowed to run on devices. Click **Allow list** to create a list of apps that are allowed to run on devices.
- **Apps:** Click **Add** and then do the following:
  - **App name:** Click the name of the app in the drop-down list that you want to add to the allow or block list. Alternatively, click **Add new** to add an app to the list of available apps.
  - If you select **Add new**, type the app name in the field that appears.
  - Click **Save** or **Cancel**.
  - Repeat these steps each app that you want to add to the allow or block list.

Windows Desktop and Tablet settings



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Prerequisites for App lock

- In Windows, configure the rules in the Local Security Policy editor on a Windows 10 or Windows 11 desktop.
- Export the policy XML file. Citrix® recommends that you create default rules in Windows to avoid locking the default configuration or causing issues on devices.
- Then, upload the XML file to Citrix Endpoint Management by using the App Lock device policy. For more information about creating rules, see this Microsoft article: https://docs.microsoft.com/en-us/windows/security/threat-protection/applocker/applocker-overview

To configure and export the policy XML file from Windows

> **Important:**
>
> When configuring the policy XML file through the Windows policy editor, use Audit Only mode.

1. On the Windows computer, start the **Local Security Policy** editor. Click **Start**, type **local security policy** and then click **Local Security Policy**.
2. In the console tree, expand **Application Control Policies**.
3. Click **AppLocker** and then in the center pane, click **Configure rule enforcement**.
4. Select **Configured** and then **Enforce rules**. When you enable a rule, **Enforce rules** is the default.
5. Right-click **AppLocker**, click **Export Policy**, and then save the XML file.

> **Note:**
>
> You can create **Executable Rules**, **Windows Installer Rules**, **Script Rules**, and **Packaged App Rules**. To do so, right-click the folder and then click **Create New Rule**.

To import the policy XML file into Citrix Endpoint Management

Create an App Lock policy. Across from the **App Lock policy file** setting, click **Browse** and navigate to the XML file.

To stop applying an App Lock policy

After you deploy an App Lock policy in Citrix Endpoint Management: To stop applying that App Lock policy, create an empty XML file. Then, create another App Lock policy, upload the file, and deploy the policy. Devices that have an App Lock enabled aren't affected. Devices receiving the policy for the first time do not have the App Lock policy in place.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

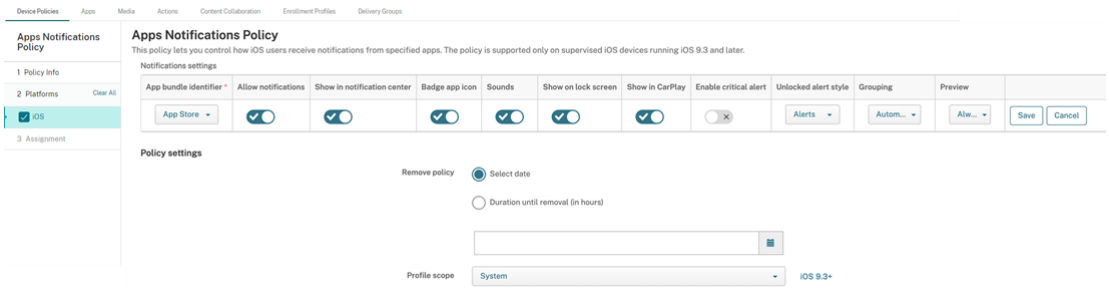
Apps notifications device policy

September 6, 2025

The Apps notifications policy lets you control how iOS users receive notifications from specified apps. The policy is supported only on supervised iOS devices running iOS 9.3 or later.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **App bundle identifier:** Specify the app where you want to manage notification settings:
  - Select the app bundle ID. Options are available only after you enable the **App Inventory** device policy, which collects an inventory of apps on managed devices.
  - Select **Add new**, and then type the app bundle ID.
    To find an app bundle ID, see Find the bundle ID for an app in the App Store.
- **Allow notifications:** Select **On** to allow notifications.
- **Show in notification center:** Select **On** to show notifications in the notification center of the user device.
- **Badge app icon:** Select **On** to show a badge app icon with notifications.
- **Sounds:** Select **On** to include sounds with notifications.
- **Show on lock screen:** Select **On** to show notifications on the lock screen of the user devices.
- **Show in CarPlay:** Select **On** to show notifications in Apple CarPlay. Applies to iOS 12 and later. Default is **On**.
- **Enable Critical Alert:** Select **On** to enable the app to mark a notification as a critical notification that ignores Do Not Disturb and ringer settings. Applies to iOS 12 and later. Default is **Off**.
- **Unlocked Alert Style:** Select **None**, **Banner**, or **Alerts** to configure the appearance of unlocked alerts.
- **Preview:** Select how devices display notification previews for the app. Applies to iOS 14 and later.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Always:** To show notification previews when the device is locked or unlocked.
  - **When Unlocked:** To show notification previews only when the device is unlocked.
  - **Never:** To clear notification previews on the device.

- **Grouping:** Select how devices group notifications from the app. Applies to devices iOS 12 and later.

  - **Automatic:** To group notifications into groups specified by the app.
  - **By app:** To group notifications from the app into one group.
  - **Off:** To clear notification groupings for the app. Devices display all notifications in sequence.

- **Policy settings**

  - **Remove policy:** Select a method for scheduling policy removal. Options include the following:
    * **Select date:** Click the calendar to select the specific date for removal.
    * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Applies to iOS 6.0 or later.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. Applies to iOS 9.3 and later.

App uninstall device policy

September 6, 2025

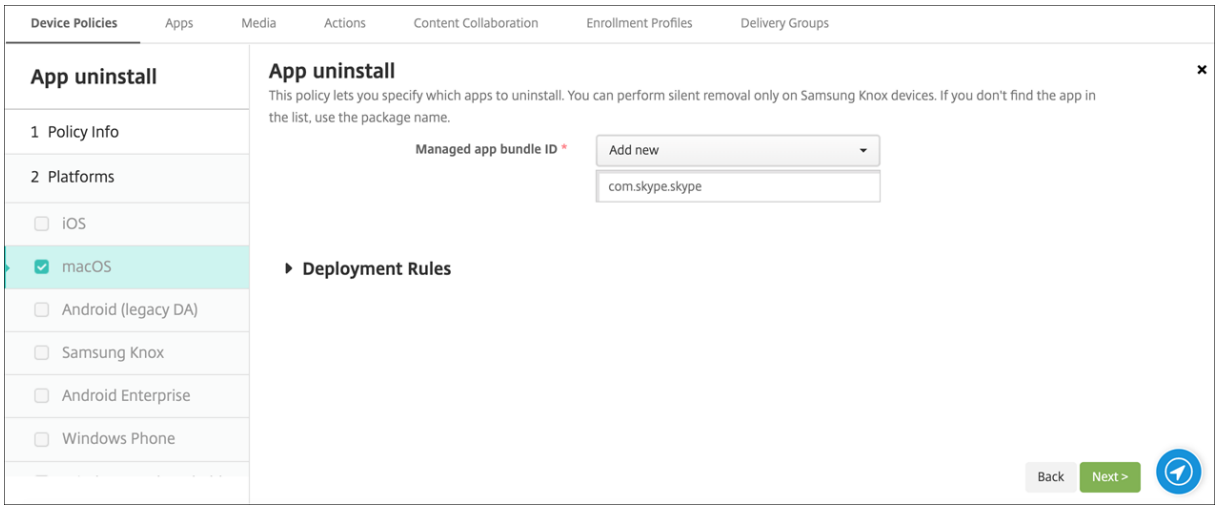
The App uninstall policy lets you remove apps from user devices. You might remove an app if you no longer want to support it or if you want to replace it with a similar app from a different vendor.

When this policy is deployed to user devices, users receive a prompt to uninstall the app, then the app is removed.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS and macOS settings



- **Managed app bundle ID:** In the list, select an existing managed app or **Add new**. If there are no apps configured for this platform, the list is empty, and you must add a new managed app. When you select **Add new**, a field appears where you can type a managed app name. Available for iOS 5.0 and later and macOS 11.0 and later.

Android (legacy DA), Android Enterprise, and Windows Desktop/Tablet settings

- **Apps to uninstall:** For each app you want to add, click **Add** and then do the following:
  - **App name:** Click an existing app in the drop-down list, or click **Add new** to enter a new app name. If there are no apps configured for this platform, the list is empty and you must add new apps.
  - Click **Add** to add the app or click **Cancel** to cancel adding the app.

For Android Enterprise apps, also enable the App inventory device policy. See App inventory device policy.

Automatically uninstall an Enterprise app after the corresponding public app store app installs

You can configure Citrix Endpoint Management to remove the Enterprise version of Citrix apps upon installation of the public app store version. This feature prevents user devices from having two similar app icons after the public app store version installs.

A deployment condition for the App Uninstall device policy triggers Citrix Endpoint Management to remove older apps from user devices upon installation of the new version. This feature is available

© 1997–2025 Citrix Systems, Inc. All rights reserved.

only for managed iOS devices connected to an Citrix Endpoint Management server in enterprise mode (XME).

To configure a deployment rule with the Installed app name condition:

- Specify the **Managed app bundle ID** for the Enterprise app.
- Add a rule: Click **New Rule** and then, as shown in the sample, choose **Installed app name**, and **is equal to**. Type the app bundle ID for the public app store app.

In the example, when the public app store app (com.citrix.mail.ios) installs on a device in the delivery groups specified, Citrix Endpoint Management removes the Enterprise version (com.citrix.mail).

App uninstall restrictions device policy

September 6, 2025

You can specify the apps users can or can't uninstall on an Amazon device.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Amazon settings

- **App Uninstall Restrictions Settings:** For each app rule that you want to add, click **Add** and then do the following:
  - **App Name:** Click an app in the drop-down list or **Add new** to add an app.
  - **Rule:** Select whether users can uninstall the app. The default is to allow uninstallation.
  - Click **Save** or **Cancel**.

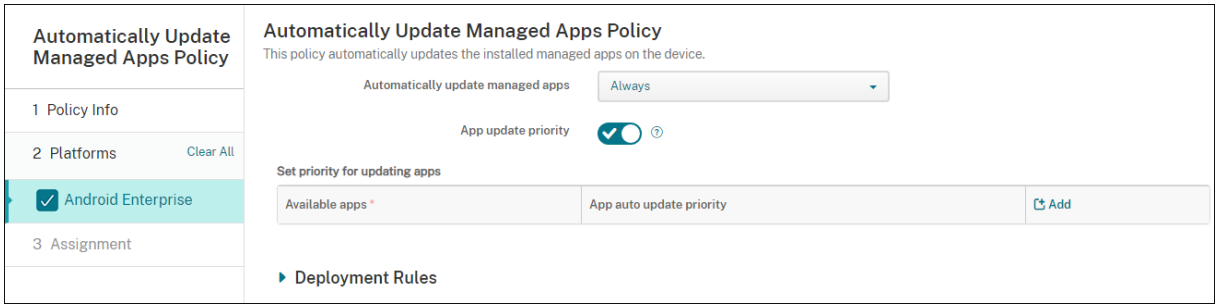
Automatically update managed apps device policy

September 6, 2025

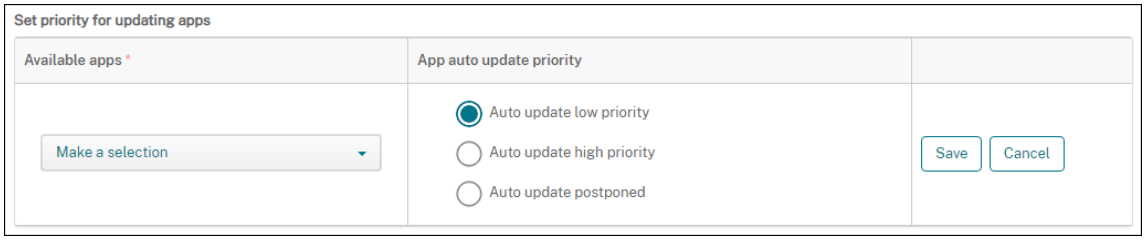
This policy controls how installed managed apps are updated on Android Enterprise devices. You can restrict the ability of users to allow automatic updates of apps on their devices. If you allow users to control automatic updates for apps on their devices, they set automatic app update policies in the managed Google Play store.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.



- **Automatically Update Managed Apps**
  - **Always:** Enables automatic app updates. **Always** is the default.
  - **Allow user to configure policy:** Allows the user to configure the automatic app update policy for the device in the managed Google Play store.
  - **Never:** Disables automatic app updates.
  - **Only when device is connected to Wi-Fi:** Allows automatic app updates only when the device is connected to Wi-Fi.
- **App update priority:** If **On**, you can configure an update priority level for each managed app.
- **Set priority for updating apps:** Click **Add** to configure update priority for an app.



  - **Available apps:** Select an app from the menu to configure the update priority.
  - **App auto-update priority:** Select an update priority from the following:
    - **Auto update low priority:** The app updates when the device is charging, not actively being used, and connected to an unmetered network.
    - **Auto update high priority:** The app updates as soon as possible, without constraints.
    - **Auto update postponed:** The app isn't updated automatically for a maximum of 90 days after a new version is available. After 90 days, the app updates automatically with low priority. After the app updates, the app doesn't update automatically for another 90 days. The user can update the app manually at any time.
  - Click **Save** when you're done. You can edit a configuration by clicking the pencil icon. Delete the configuration by clicking the trash can.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

BitLocker device policy

September 6, 2025

Windows 10 and Windows 11 include a disk encryption feature called BitLocker, which provides extra file and system protections against unauthorized access of a lost or stolen Windows device. For more protection, you can use BitLocker with Trusted Platform Module (TPM) chips, version 1.2 or later. A TPM chip handles cryptographic operations and generates, stores, and limits the use of cryptographic keys.

Starting with Windows 10, build 1703, MDM policies can control BitLocker. You use the BitLocker device policy in Citrix Endpoint Management to configure the settings available in the BitLocker wizard on Windows 10 and Windows 11 devices. For example, on a device with BitLocker enabled, BitLocker prompt users with several options:

- How they want to unlock their drive at startup
- How to back up their recovery key
- How to unlock a fixed drive.

BitLocker device policy settings also configure whether to:

- Enable BitLocker on devices without a TPM chip.
- Show recovery options in the BitLocker interface.
- Deny write access to a fixed or removable drive when BitLocker isn't enabled.
- Securely save an encrypted BitLocker recovery key for users to access in case they forget or misplace the key. This key can be found on the Self-Help Portal.

> Note
>
> After BitLocker encryption starts on a device, you can't change the BitLocker settings on the device by deploying an updated BitLocker device policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

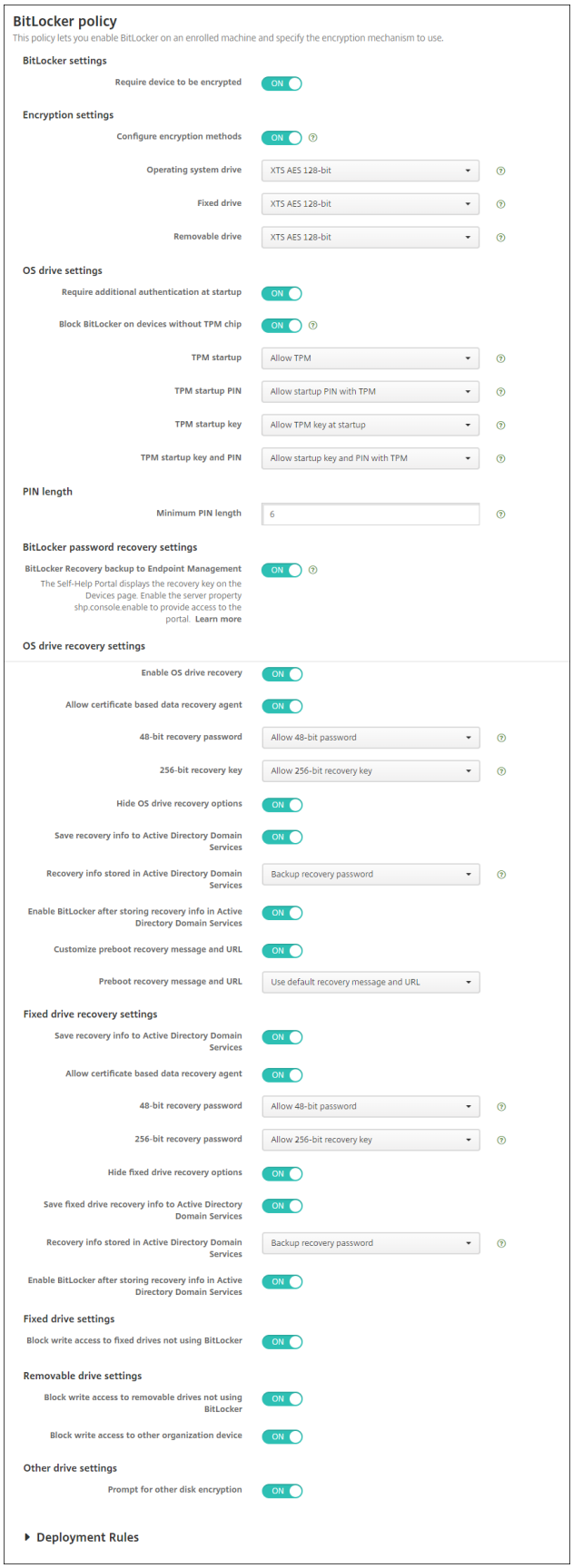
Requirements

- The BitLocker device policy requires Windows 10 Enterprise or Windows 11 Enterprise edition.
- Before deploying the BitLocker device policy, prepare your environment for BitLocker use. For detailed information from Microsoft, including BitLocker system requirements, and setup, see the articles in BitLocker.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Windows Desktop and Tablet settings



© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Bitlocker settings**
  - **Require device to be encrypted:** Determines whether to prompt users to enable BitLocker encryption on the Windows Desktop or Tablet. If **On**, the devices show a message after enrollment completes indicating that the enterprise requires device encryption. If **Off**, the user isn't prompted and BitLocker uses the policy settings. Defaults to **Off**.
- **Encryption settings**
  - **Configure encryption methods:** Determines the encryption methods to use for specific drive types. If **Off**, the BitLocker wizard prompts the device user for the encryption method to use for a drive type. The encryption method for all drives defaults to XTS-AES 128 bit. The encryption method for removable drives defaults to AES-CBC 128-bit. If **On**, BitLocker uses the encryption method specified in the policy. If **On**, these extra settings appear: **Operating system drive**, **Fixed drive**, and **Removable drive**. Choose the default encryption method for each drive type. Defaults to **Off**.
- **OS drive settings**
  - **Require additional authentication at startup:** Specifies the additional authentication required during device startup. Also specifies whether to allow BitLocker on devices that don't have a TPM chip. If **Off**, devices without TPM can't use BitLocker encryption. For information about TPM, see the Microsoft article, Trusted Platform Module Technology Overview. If **On**, the following extra settings appear. Defaults to **Off**.
  - **Block BitLocker on devices without a TPM chip:** On a device with no TPM chip, BitLocker requires users to create an unlock password or startup key. The startup key is stored in a USB drive, which the user must connect to the device before startup. The unlock password is a minimum of eight characters. Defaults to **Off**.
  - **TPM startup:** On a device with TPM, there are four unlock modes: TPM-only, TPM + PIN, TPM + Key, and TPM + PIN + Key. TPM startup is for the TPM-only mode, in which encryption keys are stored in the TPM chip. This mode doesn't require a user to provide extra unlock data. The user device automatically unlocks during restart, using the encryption key from the TPM chip. Defaults to **Allow TPM**.
  - **TPM startup PIN:** This setting is the TPM + PIN unlock mode. A PIN can have up to 20 digits. Use the **Minimum PIN length** setting to specify the minimum PIN length. A user configures a PIN during BitLocker setup and provides the PIN during device startup.
  - **TPM startup key:** This setting is the TPM + Key unlock mode. The startup key is stored in a USB or other removable drive, which the user must connect to the device before startup.
  - **TPM startup key and PIN:** This setting is the TPM + PIN + Key unlock mode.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

If the unlock succeeds, the operating system starts loading. Otherwise, the device enters recovery mode.

- **PIN length**
  - **Minimum PIN length:** The minimum length of the TPM startup PIN. Defaults to **6**.
- **BitLocker password recovery settings**
  - **BitLocker Recovery backup to Citrix Endpoint Management:** If this option is enabled, users who must unlock their devices can find their BitLocker recovery key on the Self-Help Portal. The Citrix Endpoint Management administrator can't see a user's BitLocker recovery key. For more information on seeing your BitLocker recovery key, see BitLocker recovery key.
- **OS drive recovery settings:** Configures the recovery options to users for a BitLocker-encrypted OS drive.
  - **Enable OS drive recovery:** If the unlock step fails, BitLocker prompts the user for the configured recovery key. This setting configures the operating system drive recovery options available to users if they don't have the unlock password or USB startup key. Default is **Off**.
  - **Allow certificate based data recovery agent:** Specifies whether to allow a certificate-based data recovery agent. Add a data recovery agent from Public Key Policies, which is in the Group Policy Management Console (GPMC) or in the Local Group Policy Editor. For more information about data recovery agents, see the Microsoft article, BitLocker Group Policy settings. Default is **Off**.
  - **48-bit recovery password:** Specifies whether to allow or require users to use a recovery password. BitLocker generates the password and stores it in a file or Microsoft Cloud account. Default is **Allow 48 bit password**.
  - **256-bit recovery key:** Specifies whether to allow or require users to use a recovery key. A recovery key is a BEK file, which is stored on a USB drive. Default is **Allow 256-bit recovery key**.
  - **Hide OS drive recovery options:** Specifies whether to show or hide recovery options in the BitLocker interface. If **On**, no recovery options appear in the BitLocker interface. In that case, register the device to Active Directory, save the recovery options to Active Directory, and set **Save recovery info to AD DS** to **On**. Default is **Off**.
  - **Save recovery info to Active Directory Domain Services:** Specifies whether to save the recovery options to Active Directory Domain Services. Default is **Off**.
  - **Recovery info stored in Active Directory Domain Services:** Specifies whether to store the BitLocker recovery password or the recovery password and the key package in Active

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Directory Domain Services. Storing the key package supports recovering data from a drive that is physically corrupted. Default is **Backup recovery password**.

  - **Enable BitLocker after storing recovery info in Active Directory Domain Services:** Specifies whether to prevent users from enabling BitLocker unless the device is domain-connected and the backup of BitLocker recovery information to the Active Directory succeeds. If **On**, a device must be domain-joined before starting BitLocker. Default is **Off**.
  - **Preboot recovery message and URL:** Specifies whether BitLocker shows a customized message and URL on the recovery screen. If **On**, the following extra settings appear: **Use default recovery message and URL**, **Use empty recovery message and URL**, **Use custom recovery message**, **Use custom recovery URL**, and **Use Citrix Endpoint Management recovery message and URL**. If **Off**, the default recovery message and URL display. Default is **Off**.

- **Fixed drive recovery settings:** Configures the recovery options for users for a BitLocker-encrypted fixed drive. BitLocker doesn't display a message to users about fixed drive encryption. To unlock a drive during startup, a user provides a password or smart card. The startup unlock settings, which aren't in this policy, appear in the BitLocker interface when a user enables BitLocker encryption on a fixed drive. For information about the related settings, see **Configure OS drive recovery**, earlier in this list. Default is **Off**.
- **Fixed drive settings**
  - **Block write access to fixed drives not using BitLocker:** If **On**, users can write to fixed drives only when those drives are encrypted with BitLocker. Default is **Off**.
- **Removable drive settings**
- **Block write access to removable drives not using BitLocker:** If **On**, users can write to removable drives only when those drives are encrypted with BitLocker. Configure this setting according to whether your organization allows the write access on other organization removable drives. Default is **Off**.
- **Block write access to other organization device:** If **On**, users can't write to other devices within their organization, such as a network drive.
- **Other drive settings**
- **Prompt for other disk encryption:** Allows you to disable the warning prompt for other disk encryption on devices. Defaults to **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Bluetooth device policy

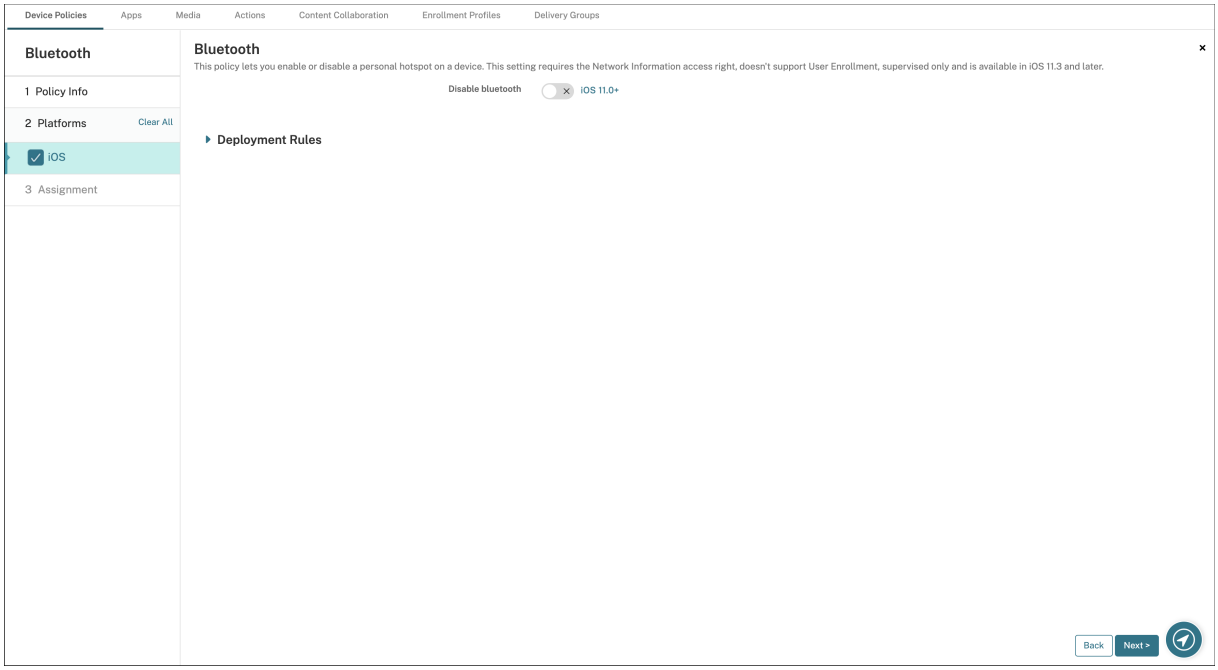
October 26, 2021

You can configure a Bluetooth policy on supervised iOS devices to enable or disable Bluetooth.

This setting requires the Network Information access right, does not support user enrollment, and is available on iOS 11.3 and later.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **Disable Bluetooth:** Allows you to disable or enable Bluetooth on the supervised device.

Calendar (CalDav) device policy

September 6, 2025

You can add a device policy in Citrix Endpoint Management to add a calendar (CalDAV) account to users'iOS or macOS devices to enable them to synchronize scheduling data with any server that supports CalDAV.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Account description:** Type an account description. This field is required.
- **Host name:** Type the address of the CalDAV server. This field is required.
- **Port:** Type the port on which to connect to the CalDAV server. This field is required. The default is **8443**.
- **Principal URL:** Type the base URL to the user's calendar.
- **User name:** Type the user's logon name. This field is required.
- **Password:** Type an optional user password.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the CalDAV server. The default is **On**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 or later.

macOS settings

- **Account description:** Type an account description. This field is required.
- **Host name:** Type the address of the CalDAV server. This field is required.
- **Port:** Type the port on which to connect to the CalDAV server. This field is required. The default is **8443**.
- **Principal URL:** Type the base URL to the user's calendar.
- **User name:** Type the user's logon name. This field is required.
- **Password:** Type an optional user password.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the CalDAV server. The default is **On**.
- **Policy settings**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    * **Select date:** Click the calendar to select the specific date for removal.
    * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

Cellular device policy

September 6, 2025

This policy allows you to configure cellular network settings on an iOS device.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

You can use macros in non-string fields, such as **Proxy server port**.

For example, you can use a macro such as `${ device.xyz }` or `${ setting.xyz }`, which expands into an integer. You can also use the macros in a device configuration XML file that you import into Citrix Endpoint Management by using the **Import iOS & macOS Profile** device policy.

- **Attach APN**
  - **Name:** A name for this configuration.
  - **Authentication type:** Click Challenge Handshake Authentication Protocol (**CHAP**) or Password Authentication Protocol (**PAP**) in the drop-down list. The default is **PAP**.
  - **User name** and **Password:** The user name and password to use for authentication.
- **APN**
  - **Name:** A name for the Access Point Name (APN) configuration.
  - **Authentication type:** Click **CHAP** or **PAP** in the drop-down list. The default is **PAP**.
  - **User name** and **Password:** The user name and password to use for authentication.
  - **Proxy server:** The proxy server network address.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Proxy server port:** The proxy server port.

- **Policy settings**

  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**

    * **Select date:** Click the calendar to select the specific date for removal.
    * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

Connection scheduling device policy

September 6, 2025

> **Important:**
>
> Citrix recommends that you use Firebase Cloud Messaging (FCM) to control connections from Android and Android Enterprise devices to Citrix Endpoint Management. For information on using FCM, see Firebase Cloud Messaging.

If you choose to not use FCM, you can create connection scheduling policies to control how and when user devices connect to Citrix Endpoint Management. If you choose to use FCM, you must also create a connection scheduling policy.

You can specify that users connect their devices manually or that devices connect within a defined time frame.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Android and Android Enterprise settings

- **Require devices to connect:** Click the option that you want to set for this schedule.

  - **Never:** Connect manually. Users must start the connection from Citrix Endpoint Management on their devices. Citrix doesn't recommend this option for production deployments because it prevents you from deploying security policies to devices, which means users never receive any new apps or policies. The **Never** option is enabled by default.
  - **Every:** Connect at the designated interval. When this option is in effect and you send a security policy such as a lock or a wipe, Citrix Endpoint Management processes the action on the device the next time the device connects. When you select this option, the **Connect**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

every N minutes field appears where you must enter the number of minutes after which the device must reconnect. The default, and minimum value, is **120**.

- **Define schedule:** Citrix Endpoint Management on the user device tries to reconnect to the Citrix Endpoint Management server after a network connection loss. Citrix Endpoint Management and monitors the connection by transmitting control packets at regular intervals within the time frame that you define. See Defining a connection time frame, next, for how to define a connection time frame.
  - **Require a connection within each of these ranges:** Users' devices must be connected at least once in any of the defined time frames.
  - **Use local device time rather than UTC:** Synchronize the defined time frames to local device time rather than Coordinated Universal Time (UTC).

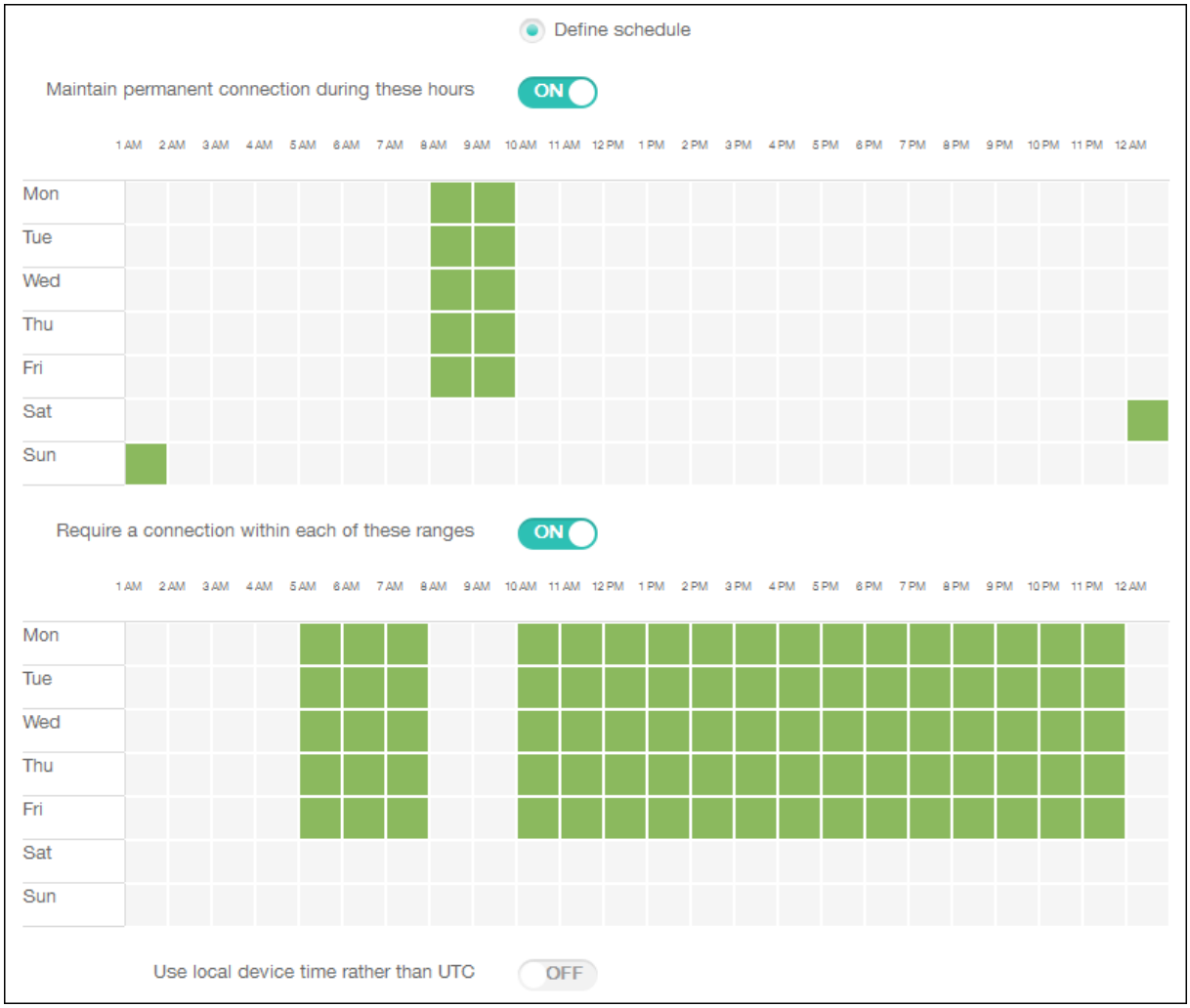
Defining a connection time frame

When you enable the following options, a timeline appears where you can define the time frames you want. You can enable either or both options to require a permanent connection during specific hours or to require a connection within certain time frames. Each square in the timeline is 1 hour. To specify a connection between 8:00 AM and 9:00 AM every weekday, you click the square on the timeline between 8 AM and 9 AM every weekday.

For example, the two timelines in the following figure require:

- A permanent connection between 8:00 AM and 10:00 AM every weekday
- A permanent connection between 1:00 AM Saturday and 2:00 AM Sunday
- At least one connection every weekday between 5:00 AM and 8:00 AM or between 10:00 AM and 12:00 AM

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Contacts (CardDAV) device policy

September 6, 2025

You can add a device policy in Citrix Endpoint Management to add an iOS contacts (CardDAV) account to users'iOS or macOS devices to enable them to synchronize contact data with any server that supports CardDAV.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Account description:** Type an account description. This field is required.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Host name:** Type the address of the CardDAV server. This field is required.
- **Port:** Type the port on which to connect to the CardDAV server. This field is required. The default is **8443**.
- **Principal URL:** Type the base URL to the user's calendar.
- **User name:** Type the user's logon name. This field is required.
- **Password:** Type an optional user password.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the CardDAV server. The default is **On**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

macOS settings

- **Account description:** Type an account description. This field is required.
- **Host name:** Type the address of the CardDAV server. This field is required.
- **Port:** Type the port on which to connect to the CardDAV server. This field is required. The default is **8443**.
- **Principal URL:** Type the base URL to the user's calendar.
- **User name:** Type the user's logon name. This field is required.
- **Password:** Type an optional user password.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the CardDAV server. The default is **On**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
- **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

Custom XML device policy

March 6, 2024

You can create custom XML policies in Citrix Endpoint Management to customize the following features on supported Windows devices:

- Provisioning, which includes configuring the device, and enabling or disabling features
- Device configuration, which includes allowing users to change settings and device parameters
- Software upgrades, which include providing new software or bug fixes to be loaded onto the device, including apps and system software
- Fault management, which includes receiving error and status reports from the device

> **Note:**
>
> When creating your XML content, use the \% character with caution. The \% character is an XML reserved character, used only to escape XML special characters. To use \% in a name, encode it as \%25.

For Windows devices: You create your custom XML configuration by using the Open Mobile Alliance Device Management (OMA DM) API in Windows. Creating custom XML with the OMA DM API is beyond the scope of this topic. For more information about using the OMA DM API, see OMA DM protocol support on the Microsoft Developer Network site.

For Android Enterprise devices: You create your custom XML configuration by using the MX Management System (MXMS). Creating custom XML with the MXMS API is beyond the scope of this article.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows Desktop/Tablet settings

XML content: Type, or cut and paste, the custom XML code you want to add to the policy.

After you click **Next**, Citrix Endpoint Management checks the XML content syntax. Any syntax errors appear below the content box. Fix any errors before you continue.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

If there are no syntax errors, the **Custom XML Policy** assignment page appears.

Use Windows AutoPilot to set up and configure devices

Windows AutoPilot is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use. You can use Windows AutoPilot to reset, repurpose, and recover devices. AutoPilot helps to remove some of the complexity of your current operating system deployment. Using AutoPilot reduces the task to a set of simple settings and operations that can get your devices ready to use quickly and efficiently.

For a brief overview of using Windows AutoPilot with Citrix Endpoint Management, watch this video.

This is an embedded video. Click the link to watch the video

Prerequisites

- Company branding configured in the Azure Active Directory portal.
- Company has an Azure Active Directory Premium P1 or P2 subscription.
- Configure Azure Active Directory as the IdP type for Citrix Endpoint Management. In the Citrix Endpoint Management console, go to **Settings > Identity Provider (IDP)**.
- Network connectivity to cloud services used by Windows AutoPilot.
- Devices pre-installed with Windows 10 Professional, Enterprise, or Education (version 1703 or later) or Windows 11 Professional, Enterprise, or Education.
- Devices have access to the internet.

For more information about configuring prerequisites, see the Microsoft Windows documentation on AutoPilot: https://docs.microsoft.com.

To configure Windows Automatic Redeployment in Citrix Endpoint Management for AutoPilot devices

1. Follow the steps to add a custom XML policy at the Custom XML Device Policy. Add the following in **XML Content:**

```
<Add>
<CmdID>_cmdid_</CmdID>
<Item>
<Target>
<LocURI>./Vendor/MSFT/Policy/Config/CredentialProviders/
   DisableAutomaticReDeploymentCredentials</LocURI>
</Target>
<Meta>
<Format xmlns="syncml:metinf">int</Format>
</Meta>
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
<Data>0</Data>
</Item>
</Add>
```

2. On the Windows lock screen, type the keystroke **CTRL + Windows key + R**.
3. Log in with an Azure Active Directory account.
4. The device verifies that the user has the right to redeploy the device. The device then redeploys.
5. After the device updates with the AutoPilot configuration, the user can then log into the freshly configured device.

Deploy a single-app kiosk on Windows 11 devices

> **Note:**
>
> Windows 11 devices support only the single-app Kiosk mode.

In the **XML content** text box, copy and paste the following XML script, and then replace the following strings with your settings:

- `your_username_here`(two instances): user name you want to create on the device. Keep the same settings for both instances.
- `your password_here`: password for the user.
- `your_UWP_app_id_here`: AUMID for the UMP app you want to deploy on the device.

XML script:

```
<Add>
    <CmdID>_cmdid_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/Accounts/Users/
               your_username_here/Password</LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data>your_password_here</Data>
    </Item>
</Add>
<Replace>
    <CmdID>_cmdid_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/AssignedAccess/Configuration</
               LocURI>
        </Target>
        <Meta>
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data><![CDATA[<AssignedAccessConfiguration
        xmlns="http://schemas.microsoft.com/AssignedAccess/2017/config"
        xmlns:rs5="http://schemas.microsoft.com/AssignedAccess/201810/
            config">
            <Profiles>
                <Profile Id="{
AFF9DA33-AE89-4039-B646-3A5706E92957 }
">
                    <KioskModeApp AppUserModelId="your_UWP_app_id_here"
                        />
                </Profile>
            </Profiles>
            <Configs>
                <Config>
                    <Account>your_username_here</Account>
                    <DefaultProfile Id="{
AFF9DA33-AE89-4039-B646-3A5706E92957 }
"/>
                </Config>
            </Configs>
        </AssignedAccessConfiguration>]]></Data>
    </Item>
</Replace>
```

Declarative Device Management policies (Technical Preview)

September 6, 2025

> **Note:**
>
> Features in the Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. You can provide feedback on this feature by clicking **Send us your feedback**. Citrix might act on feedback based on its severity, criticality, and importance.

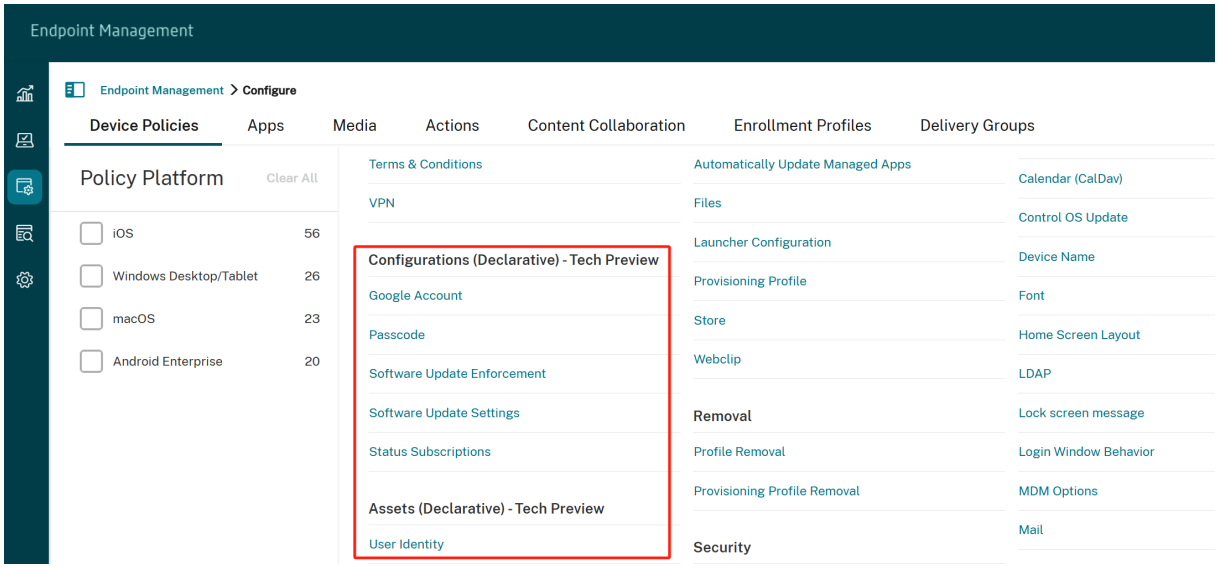
Apple has announced Declarative Device Management (DDM) in iOS 15, using a declarative data model paradigm. This paradigm allows servers to avoid the common performance and scalability issues typically associated with serializing commands and polling devices over MDM. For more information, see Leveraging the declarative management data model to scale devices.

Citrix Endpoint Management™ now supports DDM to adopt the latest capabilities that Apple provides. Contact your admin to enable this feature if needed.

The following declarative device policies are supported when you enable the DDM feature:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Google Account
- Passcode
- Software Update Enforcement
- Software Update Settings
- Status Subscriptions
- User Identity



Google Account device policy (Technical Preview)

September 6, 2025

> **Note:**
>
> Features in the Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. You can provide feedback on this feature by clicking **Send us your feedback**. Citrix might act on feedback based on its severity, criticality, and importance.

The Google Account device policy lets you configure Google account settings for iOS devices. The settings include the account name and user identity asset which configures the email address and the user's full name.

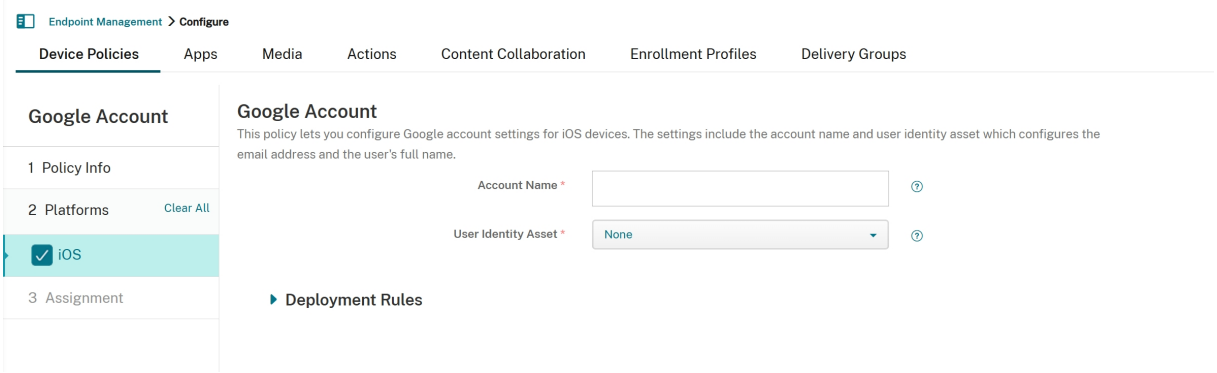
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Prerequisites

- CEM version is equal to or greater than **25.5.0**.
- The feature flag `ios.mdm.declarative.management` is activated. Contact your admin to enable this feature if needed.
- The User Identity policy is configured. Refer to User Identity device policy.

iOS settings



- **Account Name:** Type the name for the Google account.
- **User Identity Asset:** In the list, select the user identity asset created by User Identity policy, which contains the user's email address and full name. The default is **None**.

Passcode device policy (Technical Preview)

September 6, 2025

> **Note:**
>
> Features in the Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. You can provide feedback on this feature by clicking **Send us your feedback**. Citrix might act on feedback based on its severity, criticality, and importance.

The Passcode device policy creates passcode requirements based on the standards of your organization. You can require a code on devices and can set formatting rules and other passcode rules, such as the grace period before device lock.

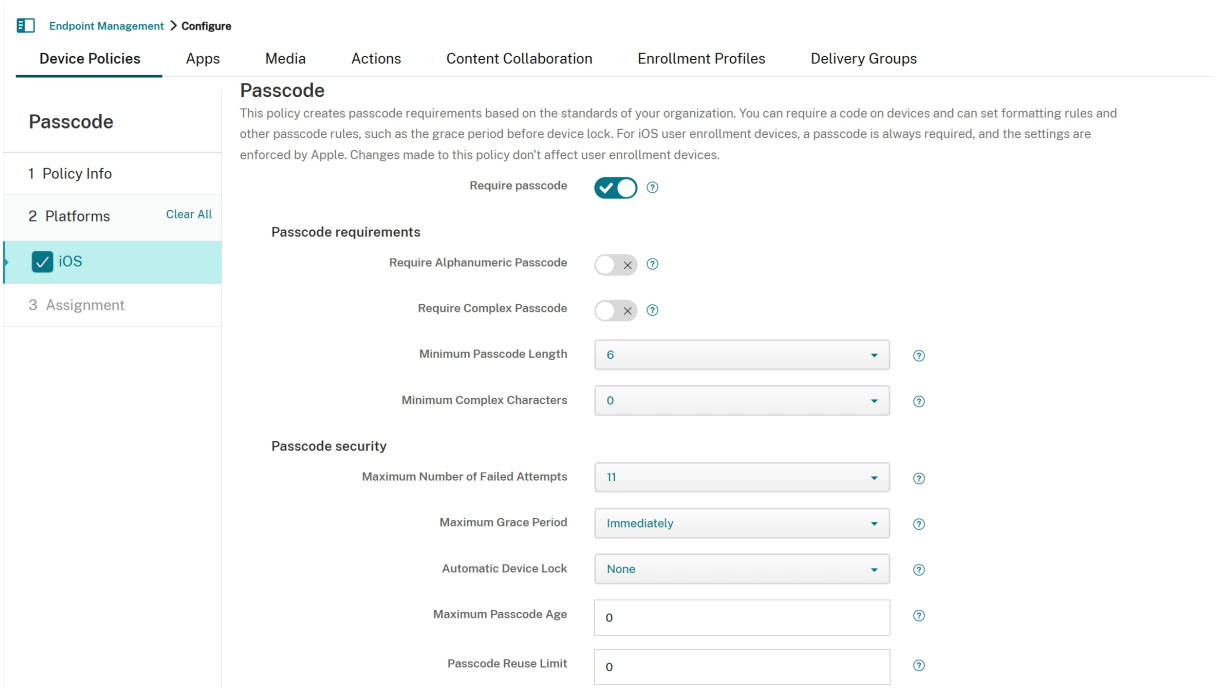
© 1997–2025 Citrix Systems, Inc. All rights reserved.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Prerequisites

- CEM version is equal to or greater than **25.5.0**.
- The feature flag `ios.mdm.declarative.management` is activated. Contact your admin to enable this feature if needed.

iOS settings



- **Require passcode:** Select this option to require a passcode and to display the configuration options for an iOS passcode device policy. If **On**, requires the user to set a passcode without any requirements about the length or quality of the passcode and the page expands to let you configure settings for passcode requirements and passcode security. The default is **On**.
- **Passcode requirements**
  - **Require Alphanumeric Passcode:** Select whether to require the passcode to consist of at least one alphabetic character and at least one number. The default is **Off**.
  - **Require Complex Passcode:** Select whether to require a complex passcode. A complex passcode is one that doesn't contain repeated characters or increasing or decreasing characters (such as 123 or CBA), and must contain at least one nonnumeric and nonalphabetic character. The default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Minimum Passcode Length:** Select the minimum number of characters a passcode can contain. The default is **6**.
  - **Minimum Complex Characters:** Select the minimum number of complex characters in the password. A complex character is a character other than a number or a letter, such as &, %, $, and #. The default is **0**.

- **Passcode security**

  - **Maximum Number of Failed Attempts:** Select the number of failed passcode attempts that the system allows the user before iOS erases the device. If you don't change this setting, after six failed attempts, the device imposes a time delay before the user can enter a passcode again. The time delay increases with each failed attempt. After the final failed attempt, the system securely erases all data and settings from the iOS device. The passcode time delay begins after the sixth attempt, so if this value is six or lower, the system has no time delay and triggers the erase or lock as soon as the user exceeds the limit. The default is **11**.
  - **Maximum Grace Period:** Select the maximum period during which the user can unlock the device without a passcode. A value of 0 means no grace period, and the device requires a passcode immediately. In the absence of this key, the user can select any period. The default is **immediately**.
  - **Automatic Device Lock:** Select the maximum period during which the device can be idle before the system automatically locks it. When the device reaches this limit, the device locks and the user must enter the passcode to unlock it. In the absence of this key, the user can select any period. Set the value to **None** to disable the policy. The default is **None**.
  - **Maximum Passcode Age:** Select the maximum number of days that the passcode can remain unchanged. After this number of days, the system forces the user to change the passcode before it unlocks the device. Valid values are 0–730. The default is **0**, which means the passcode never expires.
  - **Passcode Reuse Limit:** Select the number of historical passcode entries the system checks when validating a new passcode. The device refuses a new passcode if it matches a previously used passcode within the specified passcode history range. Valid values are 0–50. The default is **0**, which means users can reuse passwords.

> **Note:**
>
> If the same setting is sent as an MDM profile and a declarative configuration to a device, the same rules apply as if the setting was delivered by multiple profiles. For example, if passcode policies are configured by a profile (via Passcode policy) and a configuration (via declarative Passcode policy), the policies are merged and the strictest settings are enforced.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Software Update Enforcement device policy (Technical Preview)

September 6, 2025

> **Note:**
>
> Features in the Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. You can provide feedback on this feature by clicking **Send us your feedback**. Citrix might act on feedback based on its severity, criticality, and importance.

The software update enforcement device policy for a specific OS release enables IT administrators to manage iOS device updates, allowing them to control which updates are applied and set deadlines for completing all updates. These settings configure the declarations used by Apple's declarative device management feature. These settings are separate from older MDM settings and only apply to a device enabled for declarative management. It takes precedence over the Control OS Update policy for the same setting.

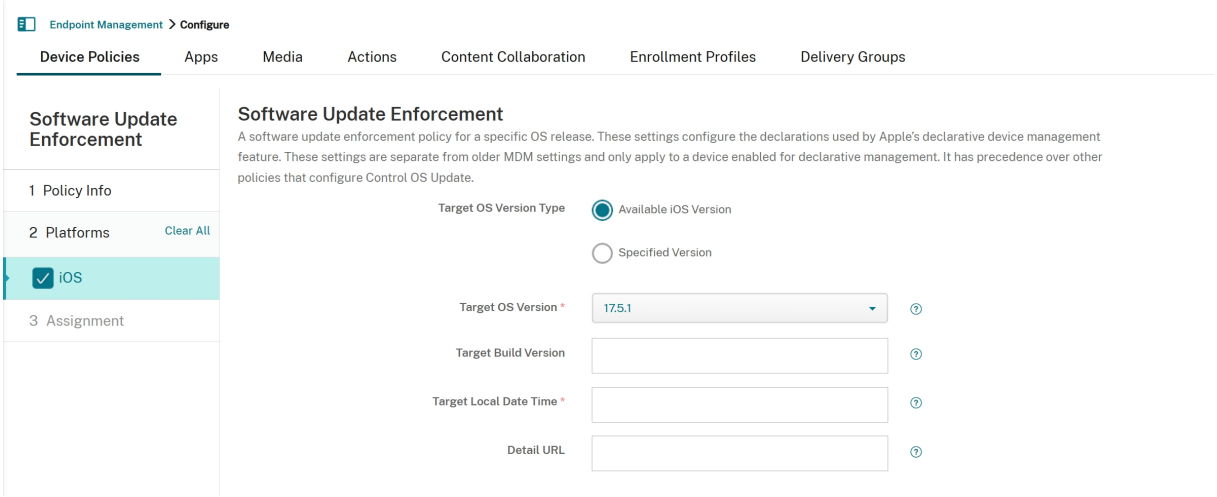
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Prerequisites

- CEM version is equal to or greater than **25.5.0**.
- The feature flag `ios.mdm.declarative.management` is activated. Contact your admin to enable this feature if needed.
- Available for **iOS 17.0** or later and **iPadOS 17.0** or later.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS settings



- **Target OS Version Type:** Specify how to configure the target OS version. The default is **Available iOS Version**.
  - **Available iOS Version:** If **On**, list the available target OS versions in **Target OS Version**.
  - **Specified Version:** If **On**, manually input the OS version with suggested format.
- **Target OS Version: (Required)** Select or type the target OS version to update the device to by the appropriate time. This is the OS version number, for example, 17.7. It may also include a supplemental version identifier, for example, 17.7.2.
- **Target Build Version:** Type the target build version to update the device to by the appropriate time, for example, 20A242. The system uses the build version for testing during seeding periods. The build version can include a supplemental version identifier, for example, 20A242a. If the build version isn't consistent with the target OS version specified in the TargetOSVersion key, the target OS version takes precedence.
- **Target Local Date Time: (Required)** Type the local date time value that specifies when to force install the software update. Use the format yyyy-mm-ddThh:mm:ss, which is derived from RFC3339 but doesn't include a time zone offset. If the user doesn't trigger the software update before this time, the device force installs it.
- **Detail URL:** Type the URL of a web page that shows details that the organization provides about the enforced update.

> **Note:**
>
> Both Software Update Enforcement policy and Control OS Update policy can manage the OS updates on devices. However, the Software Update Enforcement policy takes precedence over the Control OS Update policy. If both policies are deployed with the same setting, the configuration

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> in the Control OS Update policy will be overridden and will not take effect. For more information, see the Transition to declarative device management.

Besides, there are some differences between Software Update Enforcement policy and Control OS Update policy.

Policy Type	Software Update Enforcement	Control OS Update
Device Type	Supervised or Unsupervised device	Supervised device
Enforce an update deadline	☒	☒
Enter a help URL	☒	☒
Specify the build version number	☒	☒
Auto deploy latest update	☒	☒
Minimum supported version	iOS 17.0	iOS 10.3 (supervised)

Software Update Settings device policy (Technical Preview)

September 6, 2025

> **Note:**
>
> Features in the Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. You can provide feedback on this feature by clicking **Send us your feedback**. Citrix might act on feedback based on its severity, criticality, and importance.

The Software Update Settings device policy can be used to defer OS updates and control how users can manually interact with software updates in System Settings. The policy only supports supervised devices.

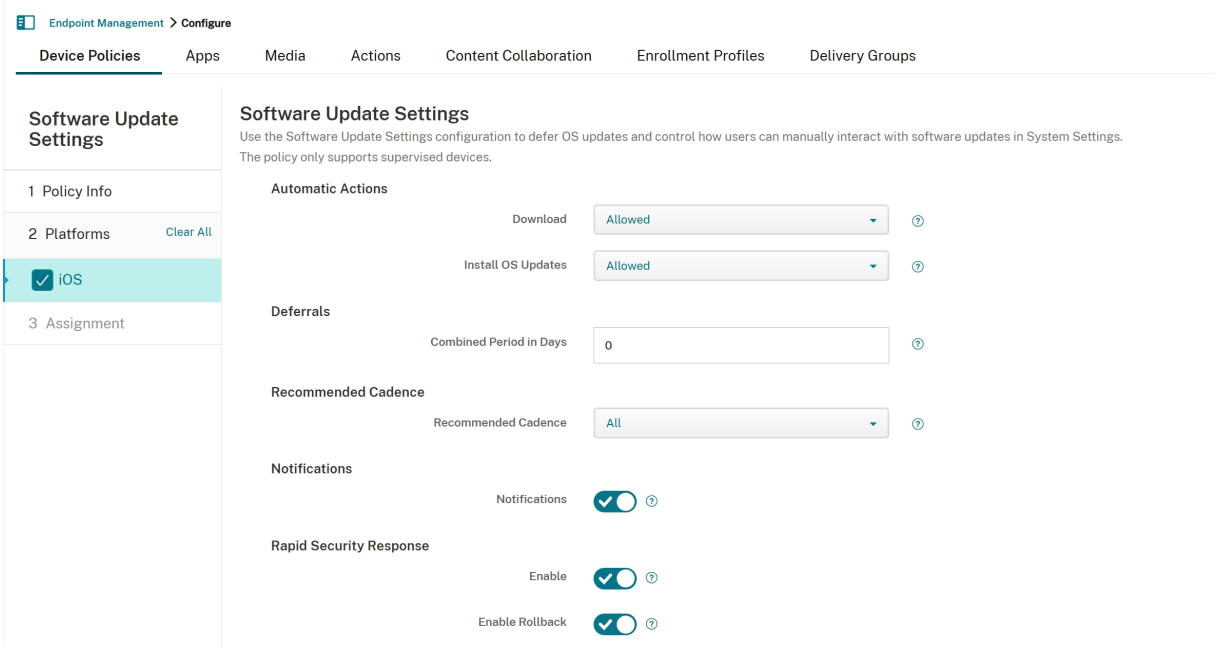
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Prerequisites

- CEM version is equal to or greater than **25.5.0**.
- The feature flags `ios.mdm.declarative.management` and `ios.mdm.software.update.setting` are activated. Contact your admin to enable this feature if needed.
- Available for **iOS 18.0** or later and **iPadOS 18.0** or later, only support supervised devices.

iOS settings



- **Automatic Actions**
  - **Download:** Specify whether the user can control automatic downloads of available updates. The default is **Allowed**.
    - **Allowed** - the user can enable or disable automatic downloads.
    - **AlwaysOn** - automatic downloads are always enabled.
    - **AlwaysOff** - automatic downloads are always disabled.
  - **Install OS Updates:** Specify whether the user can control automatic installation of available updates. The default is **Allowed**.
    - **Allowed** - the user can enable or disable automatic installation.
    - **AlwaysOn** - automatic installations are always enabled.
    - **AlwaysOff** - automatic installations are always disabled.
- **Deferrals**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Combined Period in Days:** Specify the number of days to defer a major or minor OS software update on the device. When set, software updates only appear after the specified delay, following the release of the software update. Available in iOS 18 and later. Valid values are 0–90. The default is **0**, which means no delay is expected.

- **Recommended Cadence**

  - **Recommended Cadence:** Specify how the device shows software updates to the user. When more than one update is available, the device behaves as follows. The default is **All**.

    * **All** - Shows all software update versions.
    * **Oldest** - Shows only the oldest (lower numbered) software update version.
    * **Newest** - Shows only the newest (highest numbered) software update version.

- **Notifications**

  - **Notifications:** If **On**, the device shows all software update enforcement notifications. If **Off**, the device only shows notifications triggered one hour before the enforcement deadline, and the restart countdown notification.The default is **On**.

- **Rapid Security Response**

  - **Enable:** If **Off**, Rapid Security Responses aren't offered for user installation. The system can still install Rapid Security Responses with `com.apple.configuration.softwareupdate.enforcement.specific` configurations. If **On**, the system offers Rapid Security Responses to the user. The default is **On**.
  - **Enable Rollback:** If **Off**, the system doesn't offer Rapid Security Response rollbacks to the user. If **On**, the system offers Rapid Security Response rollbacks to the user. The default is **On**.

Status Subscriptions device policy (Technical Preview)

September 6, 2025

> **Note:**
>
> Features in the Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. You

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> can provide feedback on this feature by clicking **Send us your feedback**. Citrix might act on feedback based on its severity, criticality, and importance.

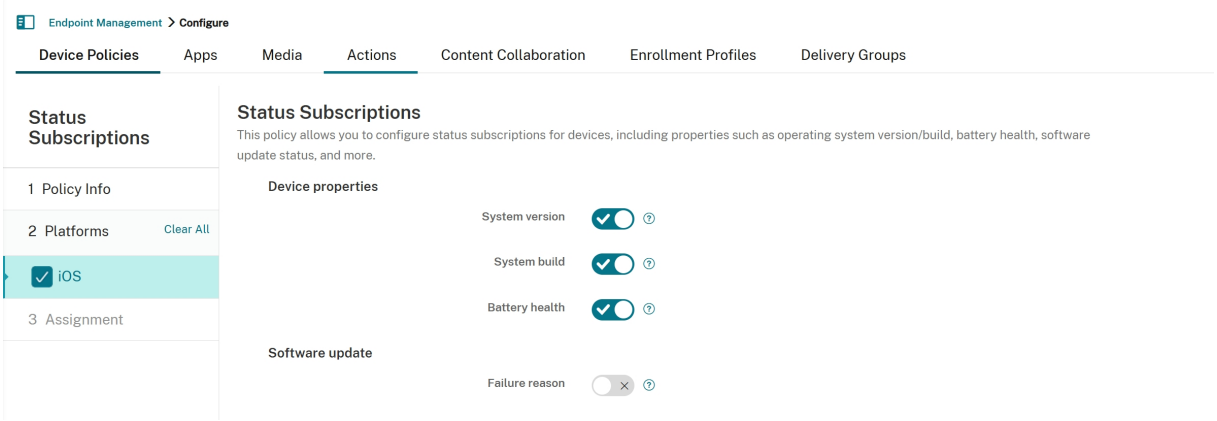
The Status Subscriptions device policy allows you to configure status subscriptions for devices, including properties such as operating system version/build, battery health, software update status, and more.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Prerequisites

- CEM version is equal to or greater than **25.5.0**.
- The feature flag `ios.mdm.declarative.management` is activated. Contact your admin to enable this feature if needed.

iOS settings



- **Device properties**
  - **System version:** If **On**, the device will report the operating system's version (e.g., 18.0), which will be displayed in the System Information section of Device Properties. This is useful because the device will automatically report it when a version upgrade occurs. The default is **On**. Available for iOS 15 and later.
  - **System build:** If **On**, the device will report the operating system's build version (e.g., 18F132), which will be displayed in the System Information section of Device Properties. This is useful because the device will automatically report it when a version upgrade occurs. The default in **On**. Available for iOS 15 and later.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Battery health:** If **On**, a new setting **Battery Health** is added to the Device Properties. This setting allows the administrators to view the battery health status of the enrolled iOS devices by navigating to **Manage > Devices > Properties > Battery > Battery health**. The default is **On**. Available for iOS 17 and later.

- **Software update**

  - **Failure reason:** If **On**, the device will report the reason for a failed OS Update, which will be displayed in the Software Updates information section of Device Properties. The default is **Off**. Available for iOS 17 and later.

User Identity device policy (Technical Preview)

September 6, 2025

> **Note:**
>
> Features in the Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. You can provide feedback on this feature by clicking **Send us your feedback**. Citrix might act on feedback based on its severity, criticality, and importance.

The User Identity device policy lets you configure user identity assets for iOS devices. The settings include the user's email address and full name.

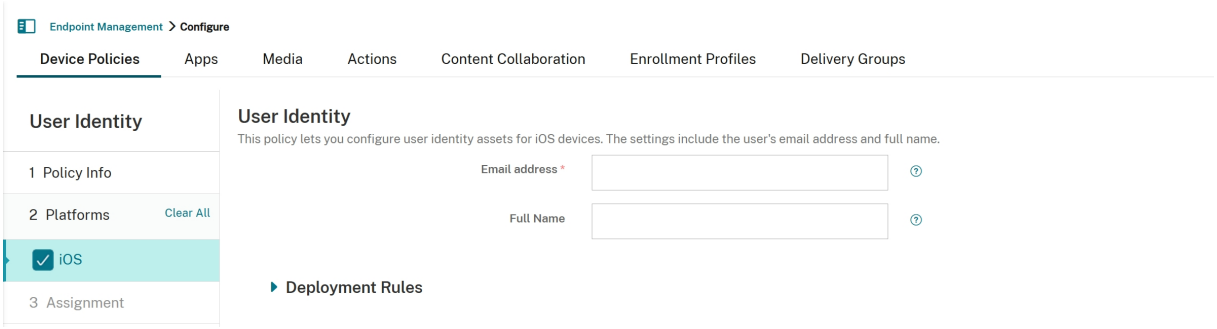
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Prerequisites

- CEM version is equal to or greater than **25.5.0**.
- The feature flag `ios.mdm.declarative.management` is activated. Contact your admin to enable this feature if needed.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS settings



- **Email address:** Type the email address for the user. This field is required.
- **Full Name:** Type the full name for the user.

Defender device policy

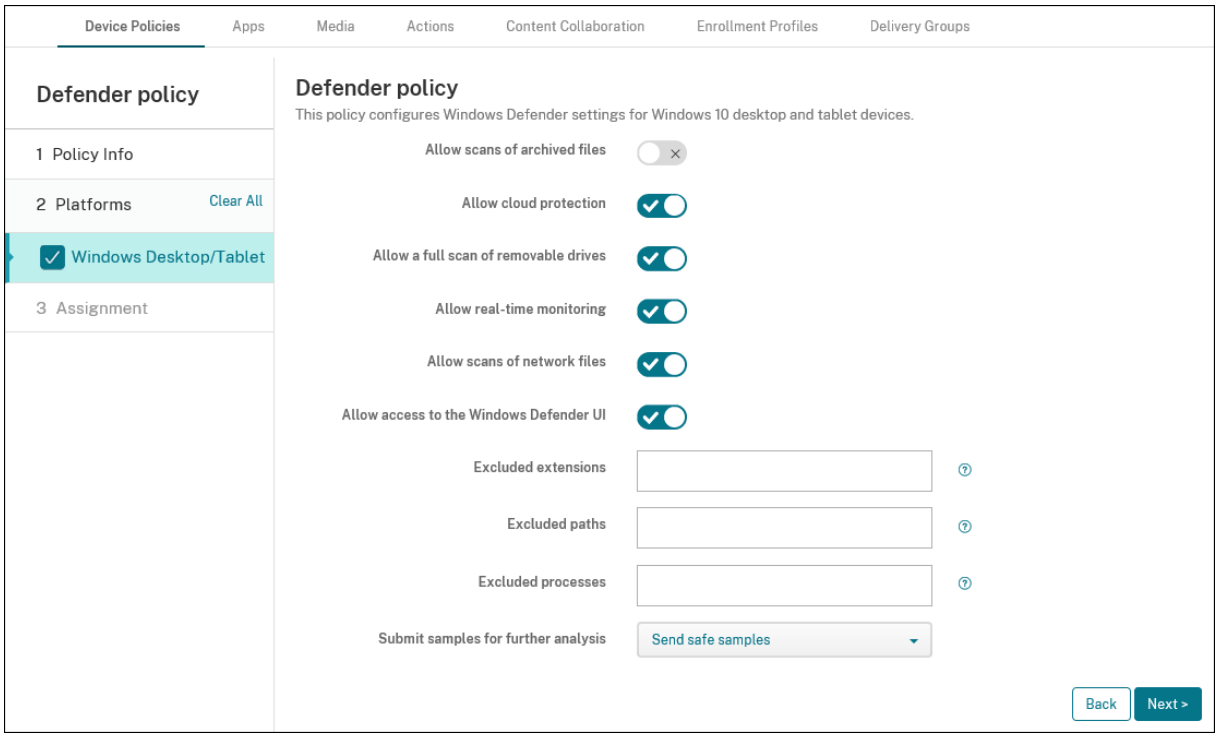
September 6, 2025

Windows Defender is a malware protection included with Windows 10 and Windows 11. You can use the Citrix Endpoint Management device policy, Defender, to configure the Microsoft Defender policy for Windows 10 and Windows 11 desktop and tablet devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Windows Desktop and Tablet settings



- **Allow scanning of archived files:** Allows or blocks Defender to scan archived files. Defaults to **Off**.
- **Allow cloud protection:** Allows or blocks Defender to send information to Microsoft about malware activity. Defaults to **On**.
- **Allow a full scan of removable drives:** Allows or blocks Defender to scan removable drives such as USB sticks. Defaults to **On**.
- **Allow real-time monitoring:** Defaults to **On**.
- **Allow scans of network files:** Allows or blocks Defender to scan network files. Defaults to **On**.
- **Allow access to the Windows Defender UI:** Specifies whether users can access the Windows Defender user interface. This setting takes effect the next time the user device starts. If this setting is set as **Off**, users don't receive any Windows Defender notifications. Defaults to **On**.
- **Excluded extensions:** The extensions to exclude from real-time or scheduled scans. To separate extensions, use the | character. For example, `lib\|obj`.
- **Excluded paths:** The paths to exclude from real-time or scheduled scans. To separate paths, use the | character. For example, `C:\Example|C:\Example1`.
- **Excluded processes:** The processes to exclude from real-time or scheduled scans. To separate processes, use the | character. For example, `C:\Example.exe|C:\Example1.exe`.
- **Submit samples for further analysis:** Controls whether to send to Microsoft files that might require further analysis to determine if they're malicious. Options: **Always prompt**, **Send safe samples**, **Never send**, **Send all samples**. Defaults to **Send safe samples**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device Guard device policy

March 6, 2024

Device Guard is a security feature available with Windows 10 and Windows 11. This feature enables virtualization-based security by using the **Windows Hypervisor** to support security services on the device. The Device Guard policy enables security features such as secure boot, UEFI lock, and virtualization.

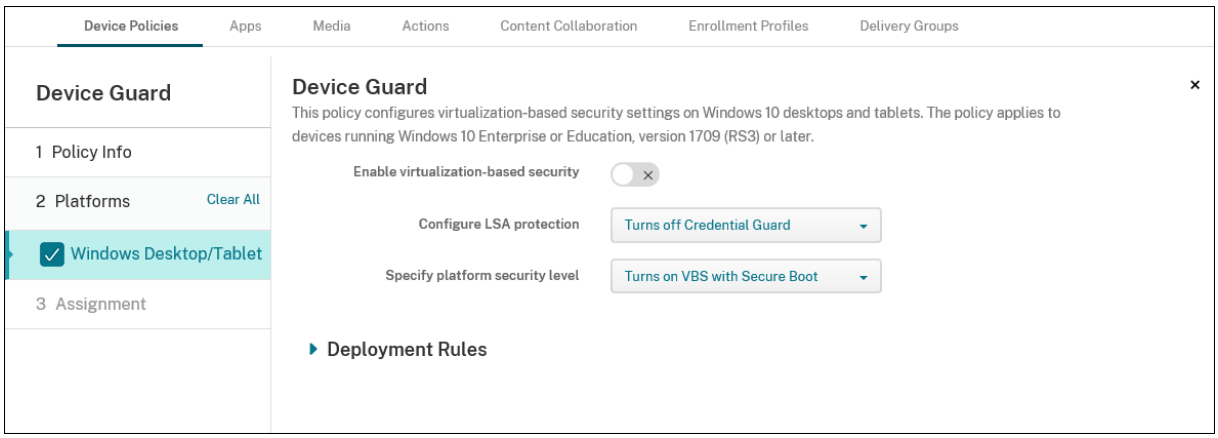
Prerequisites

- Windows 10 and Windows 11 Desktops and Tablets with an Enterprise or Education license
- Device Guard enabled in Windows

  For more information on Device Guard, see https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-manage.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows Desktop and Tablet settings



- **Enable virtualization-based security:** Disable or enable virtualization-based security features. Virtualization-based security uses the Windows Hypervisor to support security services.
- **Configure LSA protection:** Lets you configure Credential Guard. This setting lets users turn on Credential Guard with virtualization-based security to help protect credentials on the next restart. Options are **Turns off Credential Guard**, **Turns on Credential Guard with UEFI lock**, and **Turns on Credential Guard without UEFI lock**. Default is **Turns off Credential Guard**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Specify platform security level:** Lets you specify the platform security level on the next restart. Options are **Turns on VBS with Secure Boot** and **Turns on VBS with Secure Boot and direct memory access**. Default is **Turns on VBS with Secure Boot**.

Citrix Endpoint Management queries a device to determine whether the virtualization-based security settings match the settings on the server. If the security settings match, Citrix Endpoint Management doesn't deploy this policy to the device. If the security settings don't match, Citrix Endpoint Management deploys the policy.

Device Health Attestation device policy

September 6, 2025

In Citrix Endpoint Management, you can require Windows 10 and Windows 11 devices to report the state of their health. To report their health state, devices send specific data and runtime information to the Health Attestation Service (HAS) for analysis. The HAS creates and returns a Health Attestation Certificate that the device then sends to Citrix Endpoint Management. Citrix Endpoint Management uses the contents of the Health Attestation Certificate to deploy automatic actions that you have set up.

The data verified by the HAS are:

- AIK Present
- BitLocker Status
- Boot Debugging Enabled
- Boot Manager Rev List Version
- Code Integrity Enabled
- Code Integrity Rev List Version
- Apple Deployment Program Policy
- ELAM Driver Loaded
- Issued At
- Kernel Debugging Enabled
- PCR
- Reset Count
- Restart Count
- Safe Mode Enabled
- SBCP Hash
- Secure Boot Enabled
- Test Signing Enabled
- VSM Enabled

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- WinPE Enabled

For more information, refer to the Microsoft Device HealthAttestation CSP page.

You can configure DHA by using Microsoft Cloud or an on-premises Windows DHA server, as follows:

- To configure DHA by using Microsoft Cloud: Add a Device Health Attestation policy and configure it as described in this article.
- To configure DHA by using an on-premises Windows DHA server: Configure a DHA server. Then, add a Device Health Attestation policy and configure it as described in this article.

  To configure a DHA server, you install the DHA server role on a machine running Windows Server 2016 Technical Preview 5 or later. For instructions, see Configure an on-premises Device Heath Attestation server.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows Desktop/Tablet settings

If you configure DHA by using Microsoft Cloud

- **Enable Device Health Attestation:** Select whether to require Device Health Attestation. The default is **Off**.

If you configure DHA by using an on-premises Windows DHA server

- **Enable Device Health Attestation:** Set to **On**.
- **Configure On-prem Health Attestation Service:** Set to **On**.
- **On-prem DHA Service FQDN:** Type the fully qualified domain name of the DHA server that you set up.
- **On-prem DHA API version:** Select the version of the DHA service installed on the DHA server.

Device name device policy

September 6, 2025

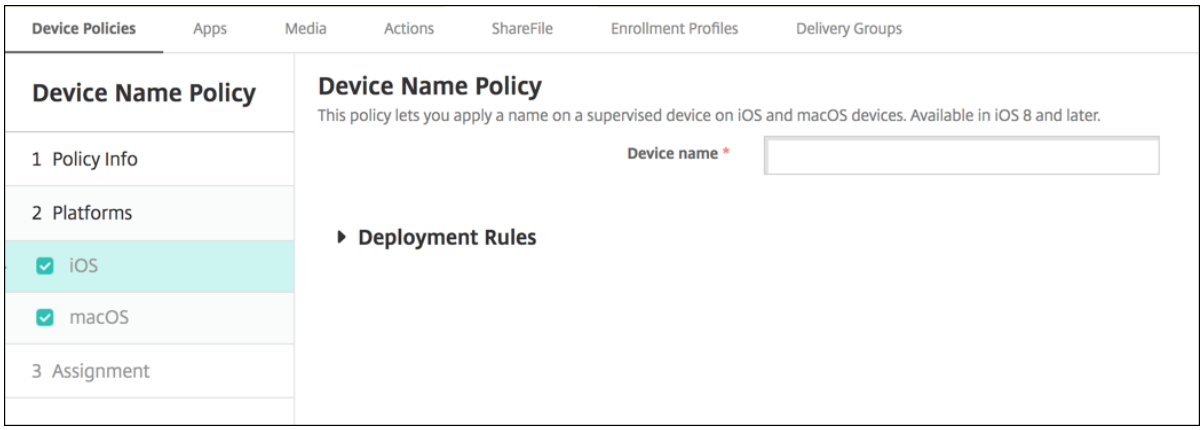
You can set the names on supervised iOS and macOS devices so that you can easily identify the devices. You can use macros, text, or a combination of both to define the device's name. For example,

© 1997–2025 Citrix Systems, Inc. All rights reserved.

to set the device name as the serial number of the device, you can use ${device.serialnumber}. To set the device name as a combination of the user's name and your domain, you can use ${user.username}@example.com. For more information about macros, see Macros in Citrix Endpoint Management.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS and macOS settings



- **Device name:** Type the macro, a combination of macros, or a combination of macros and text to name each device uniquely. For example, use ${device.serialnumber} to set the device names to each device's serial number, or use ${device.serialnumber} ${ user.username } to include the user's Apple ID in the device name.

Education Configuration device policy

September 6, 2025

The Education Configuration device policy defines:

- The Apple Classroom app settings for instructor devices.
- The certificates used to do client authentication between instructor and student devices.

The Education Configuration device policy is supported for iOS (iPadOS) devices.

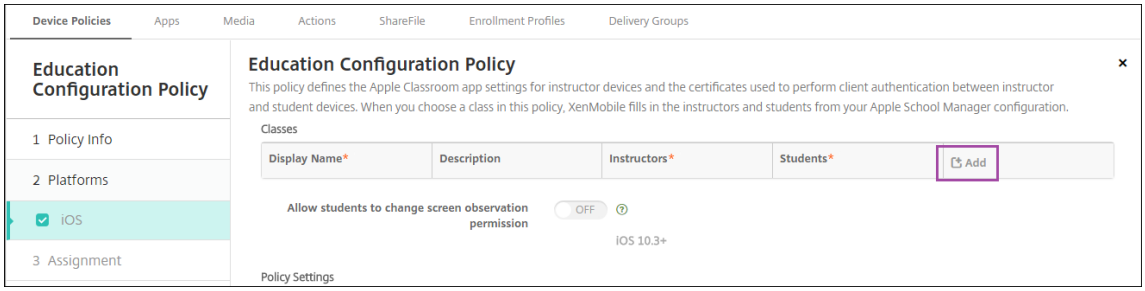
When you choose a class in this policy, the Citrix Endpoint Management console fills in the instructors and students from your Apple School Manager configuration. Create one policy if the Apple Classroom app settings in this policy are the same for all classes.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

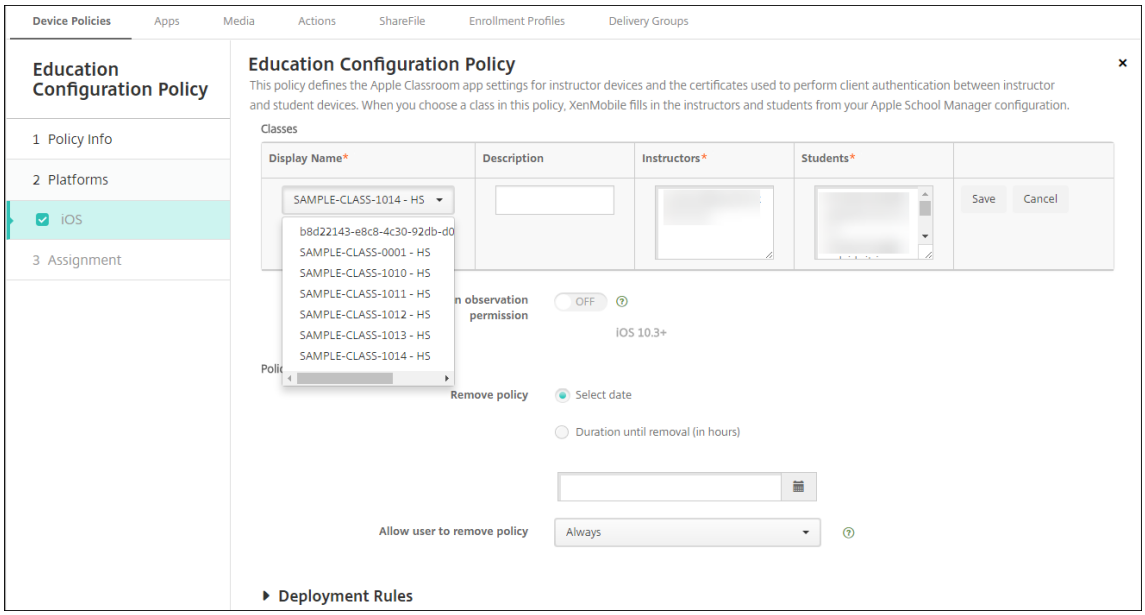
To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Classes:** To add a class, click **Add**.

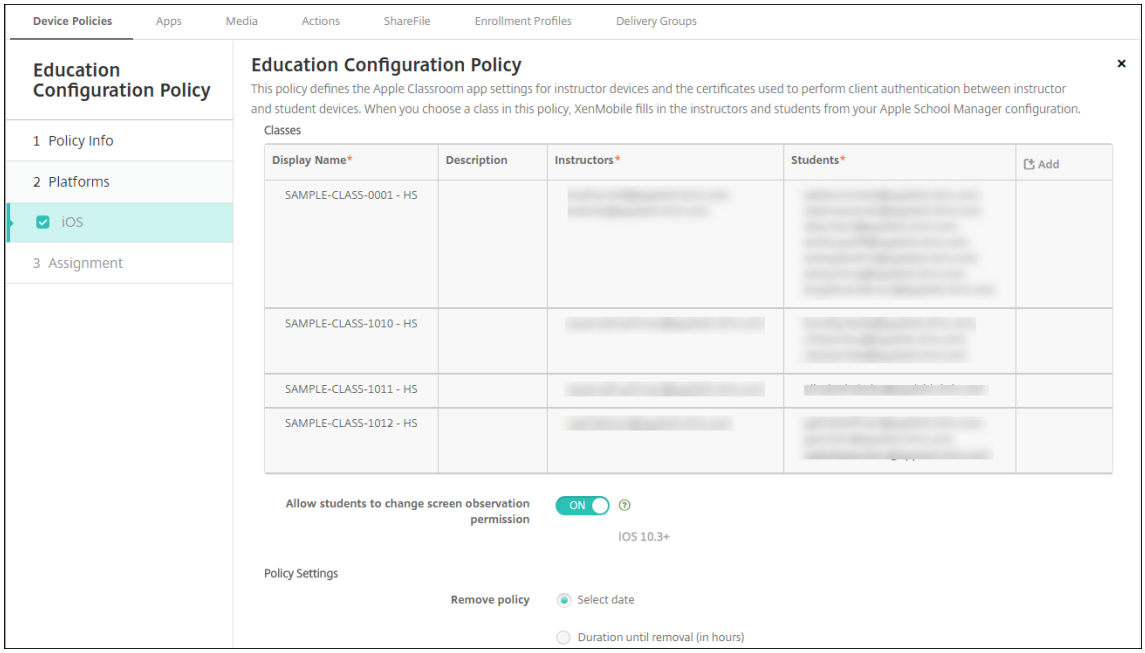


Then, Click the **Display Name** list. A list of classes got from your connected Apple School Manager account appears.



When you choose a class from **Display Name**, Citrix Endpoint Management fills in the instructors and students. Continue adding classes.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



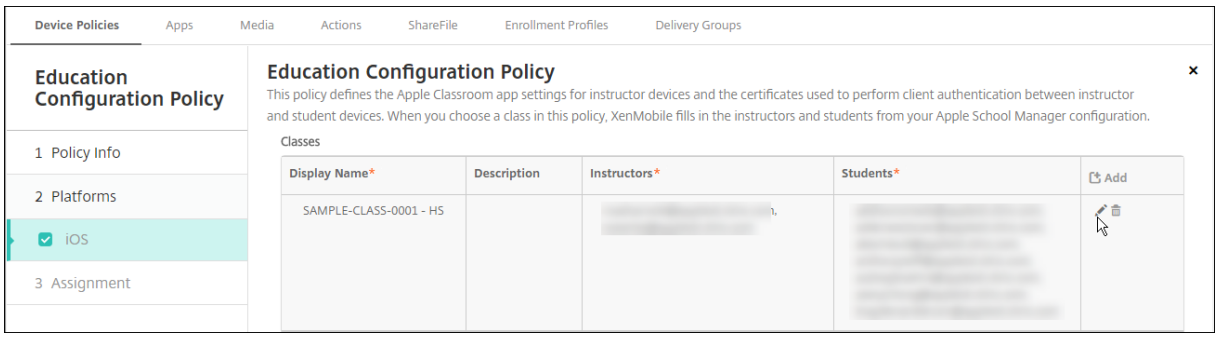
- **Allow students to change screen observation permission:** If **On**, students enrolled in managed classes can choose whether to allow their teacher to observe their device screens. Default is **Off**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    * **Select date:** Click the calendar to select the specific date for removal.
    * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

To edit class information in the policy

You can add a description to a class (the "Display name"in the Classroom app). You can also add or remove instructors and students. Citrix Endpoint Management doesn't save such changes to your Apple School Manager account. For more information, see "Manage instructor, student, and class data"in Integrate with Apple Education features.

Mouse over the **Add** column for the class you want to edit and then click the pencil icon.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



To delete a class from the policy, mouse over the **Add** column for the class you want to delete and then click the trash icon.

Endpoint Management options device policy

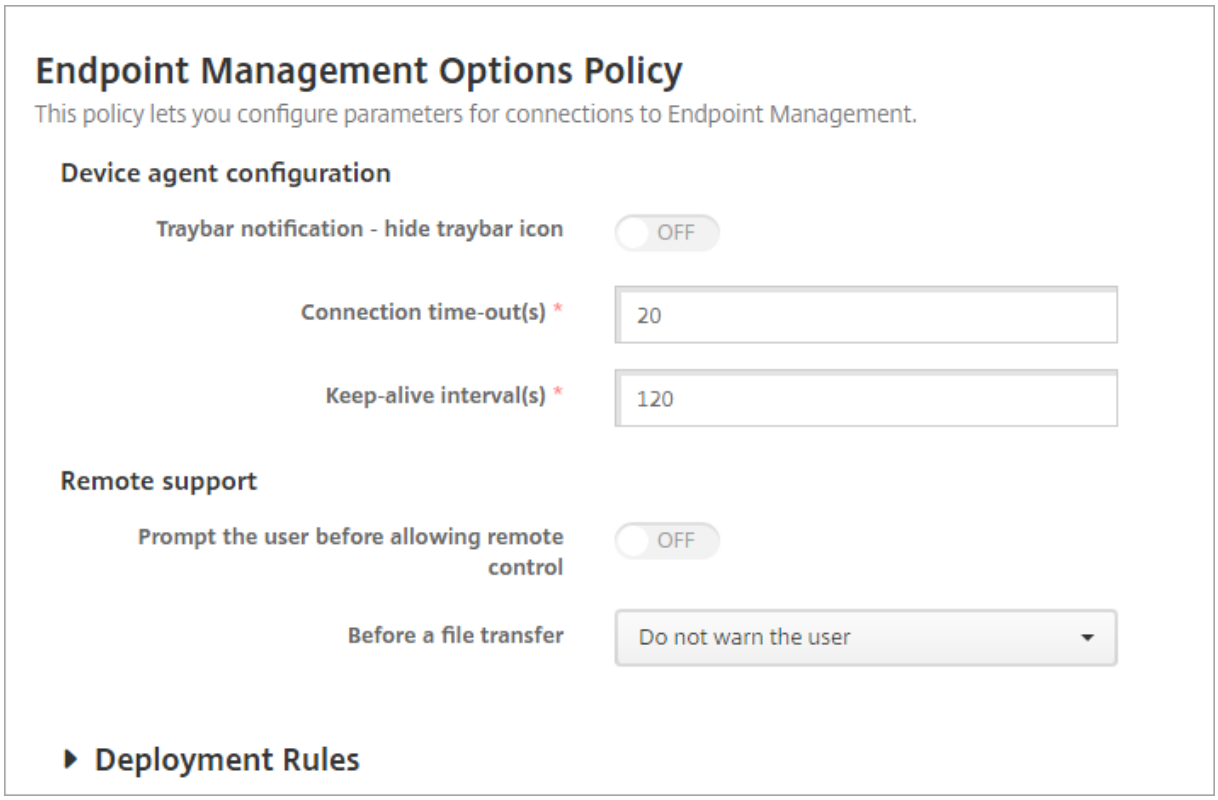
March 7, 2024

You add an Endpoint Management options policy to configure Citrix Secure Hub behavior when connecting to Citrix Endpoint Management from Android devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

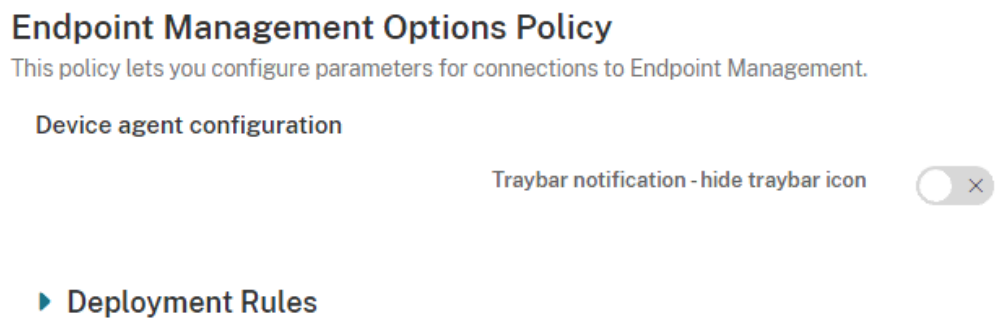
Android settings



- **Tray bar notification - hide tray bar icon:** Select whether the tray bar icon is hidden or visible. The default is **Off**.
- **Connection: time-outs:** Type the length of time in seconds that a connection can be idle before the connection times out. The default is 20 seconds.
- **Keep-alive intervals:** Type the length of time in seconds to keep a connection open. The default is 120 seconds.
- **Prompt the user before allowing remote control:** Select whether to prompt the user before allowing remote support control. The default is **Off**.
- **Before a file transfer:** Click whether to warn the user about a file transfer or whether to ask the user for permission in the drop-down list. Available values: **Do not warn the user**, **Warn the user**, and **Ask for user permission**. The default is **Do not warn the user**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Android Enterprise settings



Supported starting with Android version 7.

Tray bar notification - hide tray bar icon: Select whether the tray bar icon is hidden or visible. The default is **Off**.

> **Note:**
>
> If you want to enable VPN service for devices running on Android Enterprise, then you can enable the **Enable Always-On VPN** option in the **VPN device policy**. If you have already enabled the **Enable Always-On VPN** option in the **Endpoint Management Options device policy** in a previous version, then make sure that you enable the same in the **VPN device policy** again.

Citrix Endpoint Management uninstall device policy

September 6, 2025

You can add a device policy in Citrix Endpoint Management to uninstall Citrix Endpoint Management from Android devices. When deployed, this policy removes Citrix Endpoint Management from all devices in the deployment group.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Android settings

- **Uninstall Citrix Endpoint Management from devices:** Select whether to uninstall Citrix Endpoint Management from every device to which you deploy this policy. The default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Exchange device policy

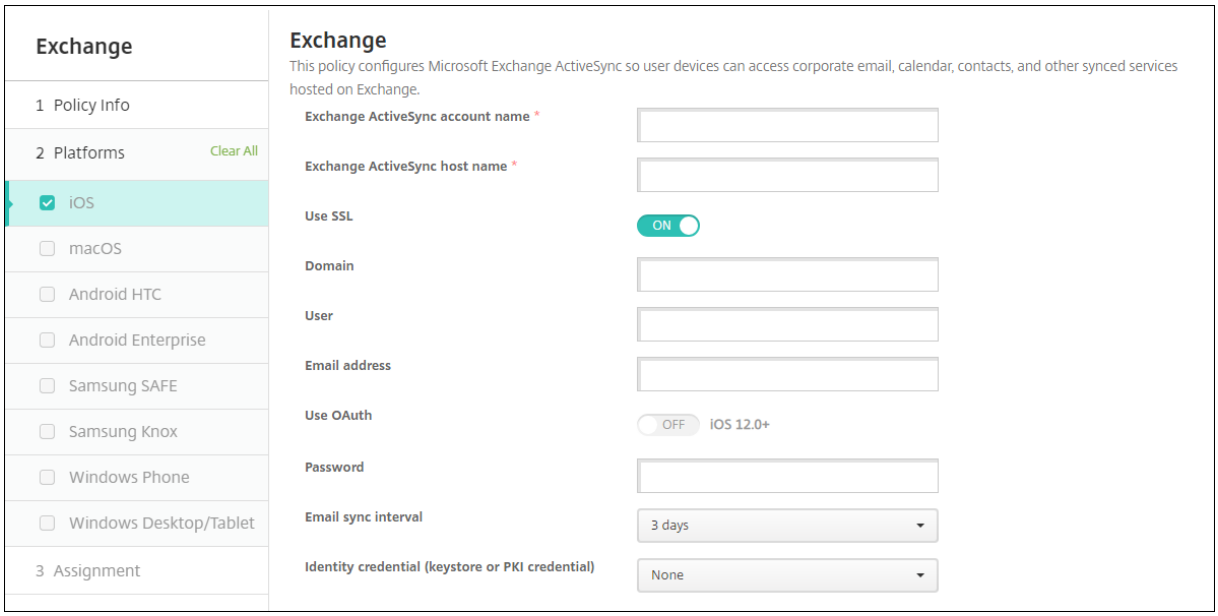
September 6, 2025

You can use the Exchange ActiveSync device policy to configure an email client on user devices to let them access their corporate email hosted on Exchange. Each platform requires a different set of values, which are described in detail in the following sections.

To create this policy, you need the host name or IP address of the Exchange Server. For information about ActiveSync settings, see the Microsoft article, ActiveSync CSP.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **Exchange ActiveSync account name:** Type the description of the email account that is displayed on user devices.
- **Exchange ActiveSync host name:** Type the address of the email server.
- **Use SSL:** Select whether to secure connections between user devices and the Exchange Server. The default is **On**.
- **Domain:** Enter the domain in which the Exchange Server is. You can use the system macro `$user.domainname` in this field to automatically lookup user domain names.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **User:** Specify the user name for the Exchange user account. You can use the system macro `$user.username` in this field to automatically lookup user names.
- **Email address:** Specify the full email address. You can use the system macro `$user.mail` in this field to automatically lookup user email accounts.
- **Use OAuth:** If set to **On**, the connection uses OAuth for authentication. The default is **Off**. This option applies to iOS 12.0 and later.
- **Password:** Enter an optional password for the Exchange user account. This setting doesn't appear when **Use OAuth** is **On**.
- **Email sync interval:** In the list, choose how often the email is synced with the Exchange Server. The default is **3 days**.
- **Identity credential (keystore or PKI):** Click an optional identity credential in the drop-down list if you've configured an identity provider for Citrix Endpoint Management. This field is only required when Exchange requires a client certificate authentication. The default is **None**.
- **Authorize moving email between accounts:** Select whether to allow users to:
  - move email out of this account into another account
  - forward email from a different account
  - reply from a different account.

  The default is **Off**.
- **Send email only from the email app:** Select whether to restrict users to the iOS mail app for sending email. The default is **Off**.
- **Prevent users from syncing recent addresses:** Select whether to prevent users from syncing recent addresses. The default is **Off**.
- **Allow Mail Drop:** Select whether to allow the account to use Mail Drop. The default is **Off**.
- **Enable S/MIME signing:** Select whether this account supports S/MIME signing. The default is **On**. When set to **On**, the following fields appear.
  - **Signing identity credential:** Choose the signing credential to use.
  - **User can override S/MIME signing:** If set to **On**, users can turn S/MIME signing on and off in the settings of their devices. The default is **Off**. This option applies to iOS 12.0 and later.
  - **User can override S/MIME signing certificate UUID:** If set to **On**, users can select, in the settings of their devices, the signing credential to use. The default is **Off**. This option applies to iOS 12.0 and later.
- **Enable S/MIME encryption:** Select whether this account supports S/MIME encryption. The default is **Off**. When set to **On**, the following fields appear.
  - **Encryption identity credential:** Choose the encryption credential to use.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Enable per message S/MIME switch:** When set to **On**, shows users an option to switch S/MIME encryption on or off for each message they compose. The default is **Off**.
  - **User can override S/MIME encryption:** If set to **On**, users can, in the settings of their devices, select whether S/MIME is on by default. The default is **Off**. This option applies to iOS 12.0 and later.
  - **User can override S/MIME encryption certificate UUID:** If set to **On**, users can turn S/MIME encryption identity and encryption on and off in the settings of their devices. The default is **Off**. This option applies to iOS 12.0 and later.

- **Policy settings**

  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

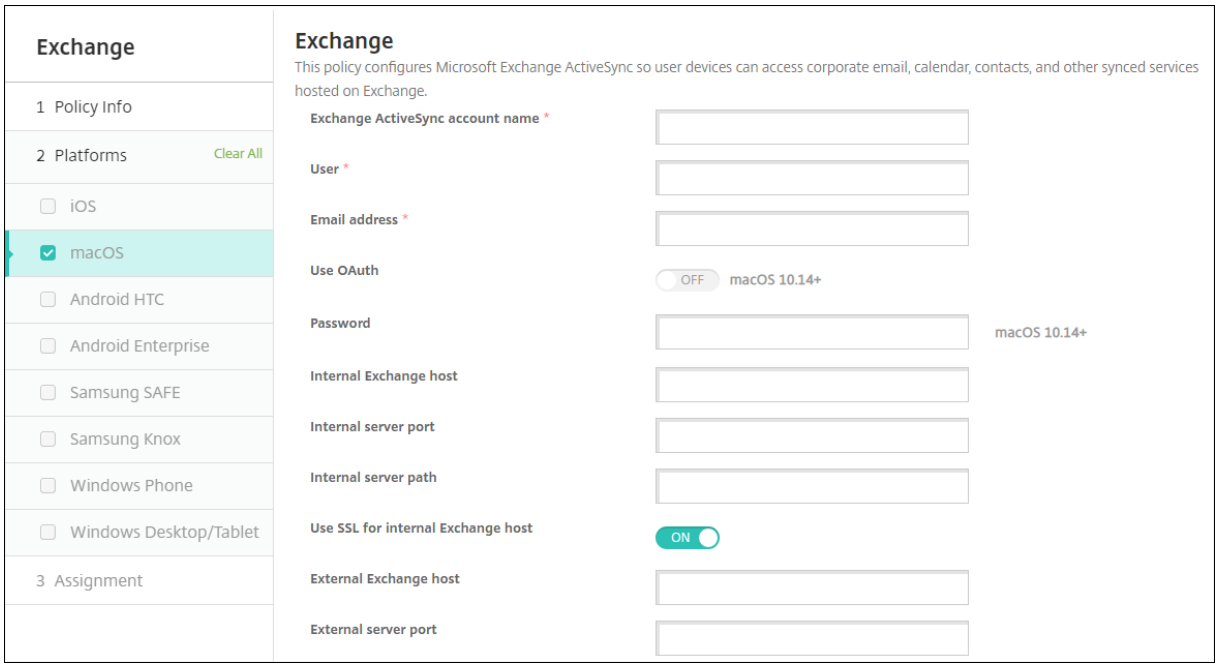
Synced Exchange Services

The synced Exchange Services settings allow you to choose whether to sync the following features:

- Calendars
- Contacts
- Mail
- Notes
- Reminders

© 1997–2025 Citrix Systems, Inc. All rights reserved.

macOS settings



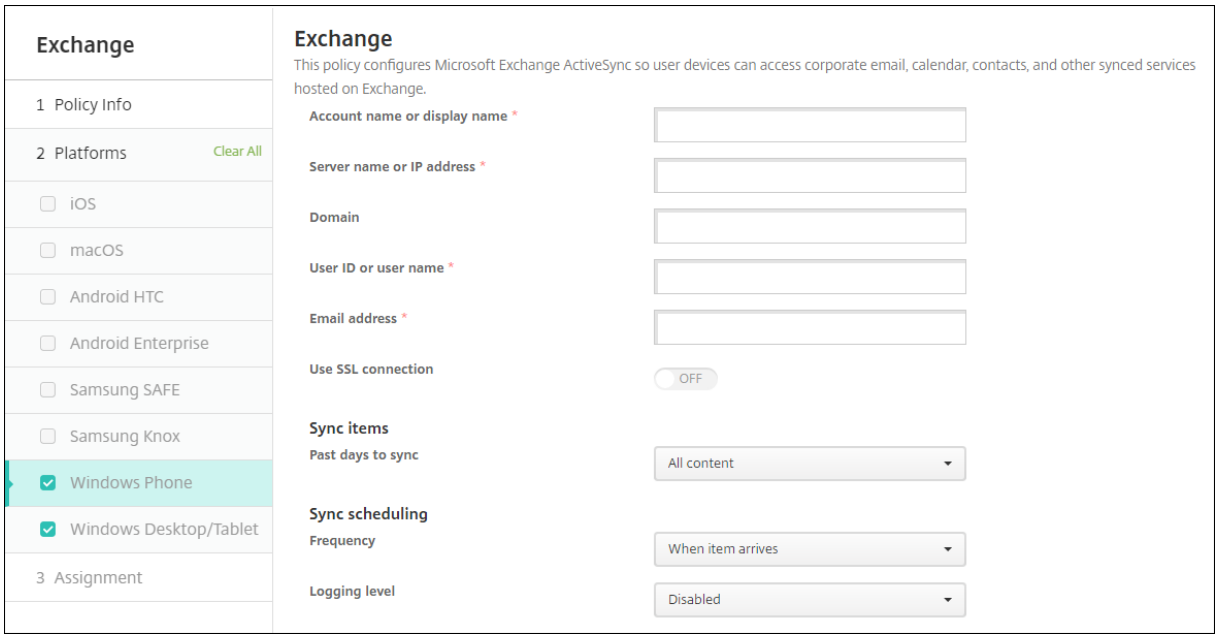
- **Exchange ActiveSync account name:** Type the description of the email account that is displayed on user devices.
- **User:** Specify the user name for the Exchange user account. You can use the system macro `$user.username` in this field to automatically lookup user names.
- **Email address:** Specify the full email address. You can use the system macro `$user.mail` in this field to automatically lookup user email accounts.
- **Use OAuth:** If set to **On**, the connection uses OAuth for authentication. The default is **Off**. This option applies to macOS 10.14 and later.
- **OAuth sign-in URL:** Specifies the URL to load into a webview to authenticate using OAuth when you don't use the AutoDiscovery service. This field appears when **Use OAuth** is set to **On**.
- **Password:** Enter an optional password for the Exchange user account. This setting doesn't appear when **Use OAuth** is **On**.
- **Internal Exchange host:** If you want your internal and external Exchange host names to be different, type an optional internal Exchange host name.
- **Internal server port:** If you want your internal and external Exchange server ports to be different, type an optional internal Exchange server port number.
- **Internal server path:** If you want your internal and external Exchange server paths to be different, type an optional internal Exchange server path.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Use SSL for internal Exchange host:** Select whether to secure connections between user devices and the internal Exchange host. The default is **On**.
- **External Exchange host:** If you want your internal and external Exchange host names to be different, type an optional external Exchange host name.
- **External server port:** If you want your internal and external Exchange server ports to be different, type an optional external Exchange server port number.
- **External server path:** If you want your internal and external Exchange server paths to be different, type an optional external Exchange server path.
- **Use SSL for external Exchange host:** Select whether to secure connections between user devices and the internal Exchange host. The default is **On**.
- **Allow Mail Drop:** Select whether to allow users to share files wirelessly between two Macs, without having to connect to an existing network. The default is **Off**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Windows Desktop/Tablet settings



> **Note:**
>
> This policy does not allow you to set the user password. Users must set that parameter from their devices after you push the policy.

- **Account name or display name:** Type the Exchange ActiveSync account name.
- **Server name or IP address:** Type the Exchange Server host name or IP address.
- **Domain:** Enter the domain in which the Exchange Server is. You can use the system macro `$user.domainname` in this field to automatically lookup user domain names.
- **User ID or user name:** Specify the user name for the Exchange user account. You can use the system macro `$user.username` in this field to automatically lookup user names.
- **Email address:** Specify the full email address. You can use the system macro `$user.mail` in this field to automatically lookup user email accounts.
- **Use SSL connection:** Select whether to secure connections between user devices and the Exchange Server. The default is **Off**.
- **Past days to sync:** In the list, click how many days into the past to sync all content on the device with the Exchange Server. The default is **All content**.
- **Frequency:** Click the schedule in the drop-down list that you want to use when syncing data that is sent to the device from the Exchange Server. The default is **When item arrives**.
- **Logging level:** Click **Disabled**, **Basic**, or **Advanced** in the drop-down list to specify the level of detail when logging Exchange activity. The **default is Disabled**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Files device policy

September 6, 2025

You can add and deploy files for users to access on their Android and Android Enterprise devices. You specify the directory where you want to store the file on the device. For example, you want users to receive a company document or .pdf file. Deploy the file to devices and let users know where the file is located.

Android devices don't support running scripts natively. Users need third-party software to run scripts.

You can add the following file types with this policy:

- Text-based files (.xml, .html, .py, and so on)
- Other files, such as documents, pictures, spreadsheets, or presentations

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Android Enterprise settings

- **File to be imported:** To select the file to import, click **Browse** and navigate to the file location.
- **Destination folder:** In the list, select the location where you want to store the uploaded file, or select **Add new** to specify a file location. Select the `%Flash Storage%\` or the `%XenMobile Storage%\` macro to indicate where to store the uploaded file. The macro expands to the applicable location on each device.
  - `%XenMobile Storage%\` expands to `Android/data/com.zenprise/` in the internal storage directory.
  - For Android 9.0 and earlier, `%Flash Storage%\` saves the file to the external storage directory.
  - For Android 10.0 and later, `%Flash Storage%\` saves the file to the **Downloads** folder of the internal storage directory.
  - For Android 11.0 and later, `%XenMobile Storage%\` no longer applies because of restrictions imposed by Google on access to the target location.
- **Destination file name:** Optional. If you must change a file name before deploying it to a device, type the file name.
- **If file exists:** In the list, select whether to copy an existing file. The default is **Copy file only if different**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> The Files device policy no longer supports adding scripts on the Android Enterprise. If an existing policy has a script, an error message displays when selecting the policy and you can re-add the policy to resolve the issue.

Android settings

- **File to be imported:** To select the file to import, click **Browse** and navigate to the file location.
- **File type:** Select either **File** or **Script**.
- **Execute immediately:** When you select **Script**, the **Execute immediately** option appears. Nothing happens when you enable this setting. Users must run the script manually.
- **Replace macro expressions:** Select whether to replace macro token names in a script with a device or user property. For macro syntax, see Macros. The default is **Off**.
- **Destination folder:** In the list, select the location where you want to store the uploaded file, or select **Add new** to specify a file location. Select the `%Flash Storage%\` or the `%XenMobile Storage%\` macro to indicate where to store the uploaded file. The macro expands to the applicable location on each device.
  - `%XenMobile Storage%\` expands to `Android/data/com.zenprise/` in the internal storage directory.
  - For Android 9.0 and earlier, `%Flash Storage%\` saves the file to the external storage directory.
  - For Android 10.0 and later, `%Flash Storage%\` saves the file to the **Downloads** folder of the internal storage directory.
  - For Android 11.0 and later, `%XenMobile Storage%\` no longer applies because of restrictions imposed by Google on access to the target location.
- **Destination file name:** Optional. If you must change a file name before deploying it to a device, type the file name.
- **If file exists:** In the list, select whether to copy an existing file. The default is **Copy file only if different**.

FileVault device policy

March 6, 2024

The macOS FileVault full-disk encryption (FileVault 2) feature protects the system volume by encrypting its contents. A user logs in to a FileVault-enabled macOS device with their account password each

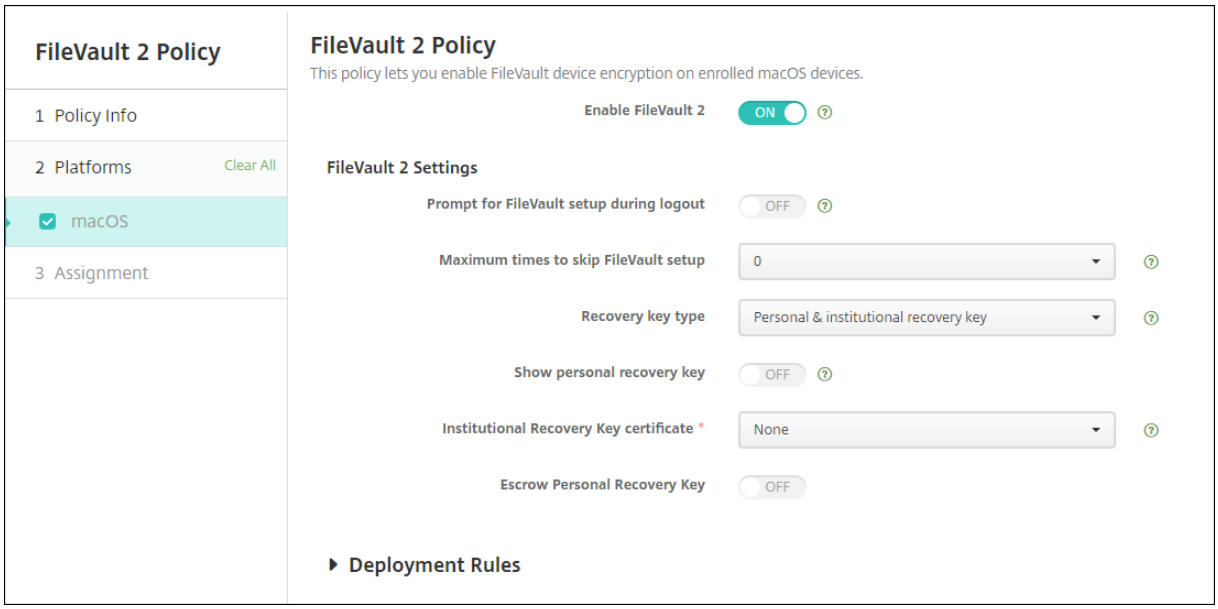
© 1997–2025 Citrix Systems, Inc. All rights reserved.

time that the device starts. If the user loses their password, a recovery key enables them to unlock the disk and reset their password.

This device policy enables FileVault user setup screens and configures settings such as recovery keys. For more information about FileVault, see the Apple support site.

To add the FileVault policy, go to **Configure > Device Policies**.

macOS settings



- **Enable FileVault:** If this setting is set as **On**, then it prompts the user to enable FileVault during the next N logouts as specified by the option **Maximum times to skip FileVault setup**. If **Off**, users don't receive a prompt to enable FileVault, but they can still enable FileVault on their own.
- **Prompt for FileVault setup during logout:** If **On**, users see a prompt asking them to enable FileVault when they log out.
- **Maximum times to skip FileVault setup:** The maximum number of times that the user can skip FileVault setup. When the user reaches the maximum, the user must set up FileVault to log in. If **0**, the user must enable FileVault during the first login attempt. Default is **0**.
- **Recovery key type:** A user who forgets their password can type a recovery key to unlock the disk and reset their password. Recovery key options:
  - **Personal recovery key:** A personal recovery key is unique to a user. During FileVault setup, a user chooses whether to create a recovery key or to allow their iCloud account to unlock their disk. To show the recovery key to the user after FileVault setup completes, enable **Show personal recovery key**. Showing the key enables the user to record the key for

© 1997–2025 Citrix Systems, Inc. All rights reserved.

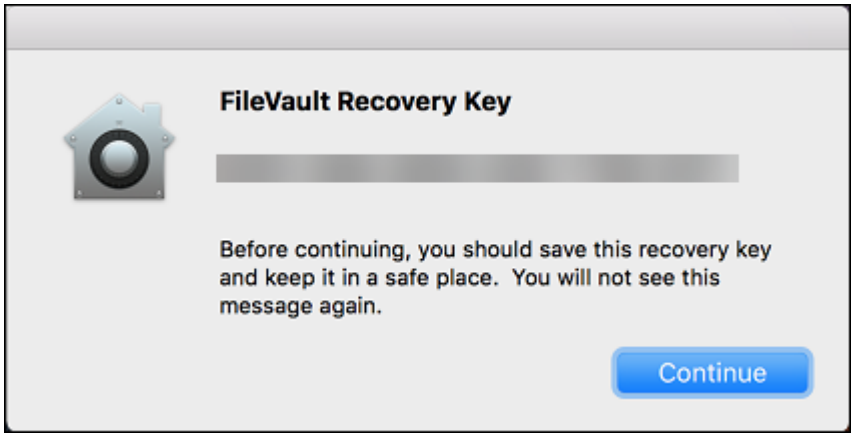
future use. To allow users to look up their key if they lose it, enable **Escrow personal recovery key**.

You can rotate personal recovery keys through security actions. For more information on rotating personal recovery keys, see Security actions.

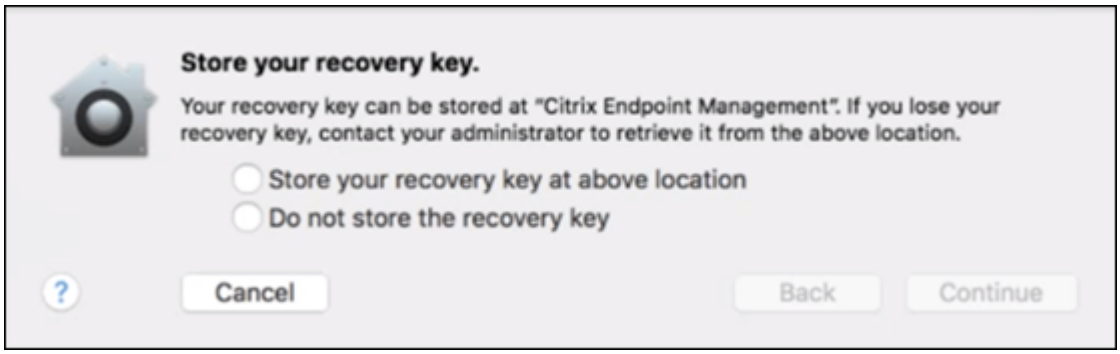
For information about recovery key management, see the Apple support site.

- **Institutional recovery key:** You can create an institutional (or main) recovery key and FileVault certificate, which you then use to unlock user devices. For information, see the Apple support site. Use Citrix Endpoint Management to deploy the FileVault certificate to devices. For information, see Certificates and authentication.
- **Personal & institutional recovery key:** By enabling both types of recovery keys, you must unlock a user device only if the user loses their personal recovery key.

- **Institutional recovery key certificate:** If you select **Institutional recovery key** or **Personal & Institutional recovery key** as the **Recovery key type**, select the recovery key certificate for that key.
- **Show personal recovery key:** If **On**, the user device shows the personal recovery key to the user after setting up FileVault. Defaults to **Off**.



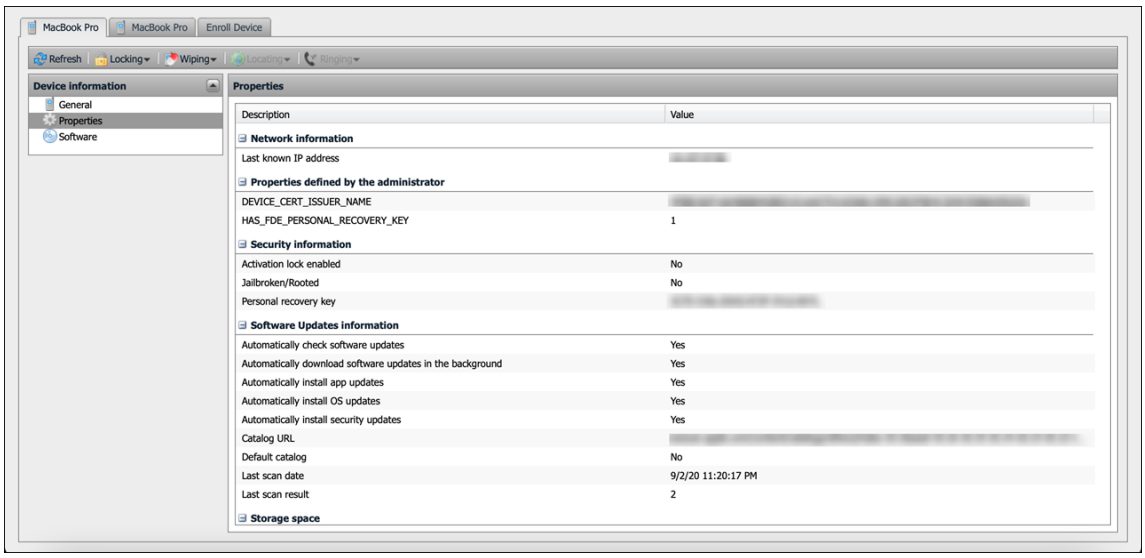
- **Escrow personal recovery key:** When enabled, users can store a copy of the personal recovery key for each device with Citrix Endpoint Management.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

To access the key from Citrix Endpoint Management, go to **Manage > Devices**, select the macOS device, and click **Edit**. Then, go to **Device details > General** and locate the **Personal recovery Key**.

To allow users to view their recovery key from the Self-Help Portal, enable **Escrow personal recovery key** and **Display personal recovery key to user**. The key appears in the Self-Help Portal on the **Properties** page under **Security information**. For more information about the Self-Help Portal, see Self-Help Portal.



You can enable the **Escrow personal recovery key** setting even if you don't enable the **Enable FileVault** setting. If you disable the **Enable FileVault** setting, users can still enable FileVault on their own. In this situation, enable **Escrow personal recovery key** to allow users to store a copy of their key with Citrix Endpoint Management.

If a user enables FileVault before enrolling the device in Citrix Endpoint Management, Citrix Endpoint Management doesn't store their recovery key. The device shows up as FileVault-enabled in the console.

Firewall device policy

September 6, 2025

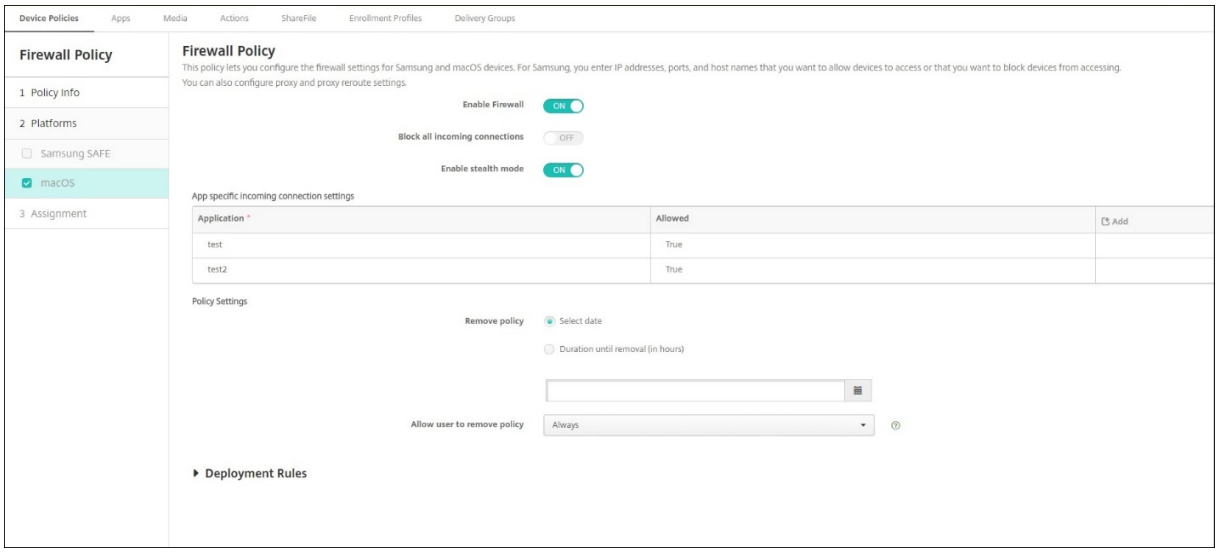
This policy lets you configure firewall settings for Samsung, macOS, and Windows devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

macOS settings

Requires macOS 10.12 and later.

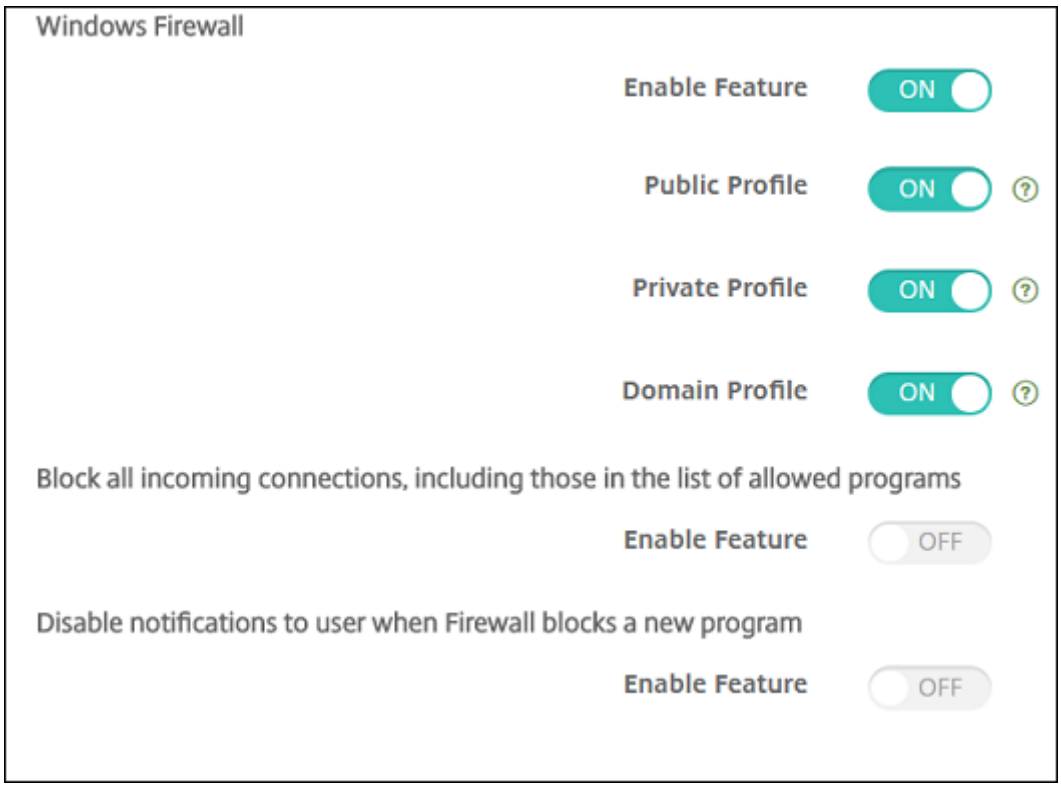


- **Enable Firewall**. To enable the firewall, set this option to **On**.
- **Block all incoming connections**. When this option is set to **On**, it blocks all incoming connections except the connections required for basic services.
- **Enable stealth mode**. In stealth mode, the device doesn't respond to or acknowledge attempts to access it from the network by test applications using ICMP, such as Ping. To enable stealth mode, set this option to **On**.
- **App specific incoming connection settings**. To allow specific apps to receive connections, add the apps and set **Allowed** to **True**.

Windows Desktop and Tablet settings

Requires Windows Desktop and Tablet devices running Windows 10 (version 1709 or later) or Windows 11.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Enable Feature:** Controls incoming and outgoing traffic on computers to which this policy is deployed. Default is **On**.
- **Public Profile:** Controls Windows Firewall while computers are connected to untrusted networks at public places, such as at an airport or coffee shop. Default is **On**.
- **Private Profile:** Controls Windows Firewall while computers are connected to trusted networks, such as their home network. Default is **On**.
- **Domain Profile:** Controls Windows Firewall while the computers are connected to the domain networks, such as at their workplace. Default is **On**.
- **Block all incoming connections, including those in the list of allowed programs:** Default is **Off**.
- **Disable notifications to user when Firewall blocks a new program:** Default is **Off**.

Font device policy

September 6, 2025

You can add a device policy in Citrix Endpoint Management to add more fonts to iOS and macOS devices. Fonts must be TrueType (`.ttf`) or OpenType (`.oft`) fonts. Font collections (`.ttc` or `.otc`) aren't supported.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **User-visible name:** Type the name that users see in their font lists.
- **Font file:** To select the font file to add to user devices, click **Browse** and then navigate to the file location.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

macOS settings

- **User-visible name:** Type the name that users see in their font lists.
- **Font file:** To select the font file to add to user devices, click **Browse** and then navigate to the file location.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

Home screen layout device policy

September 6, 2025

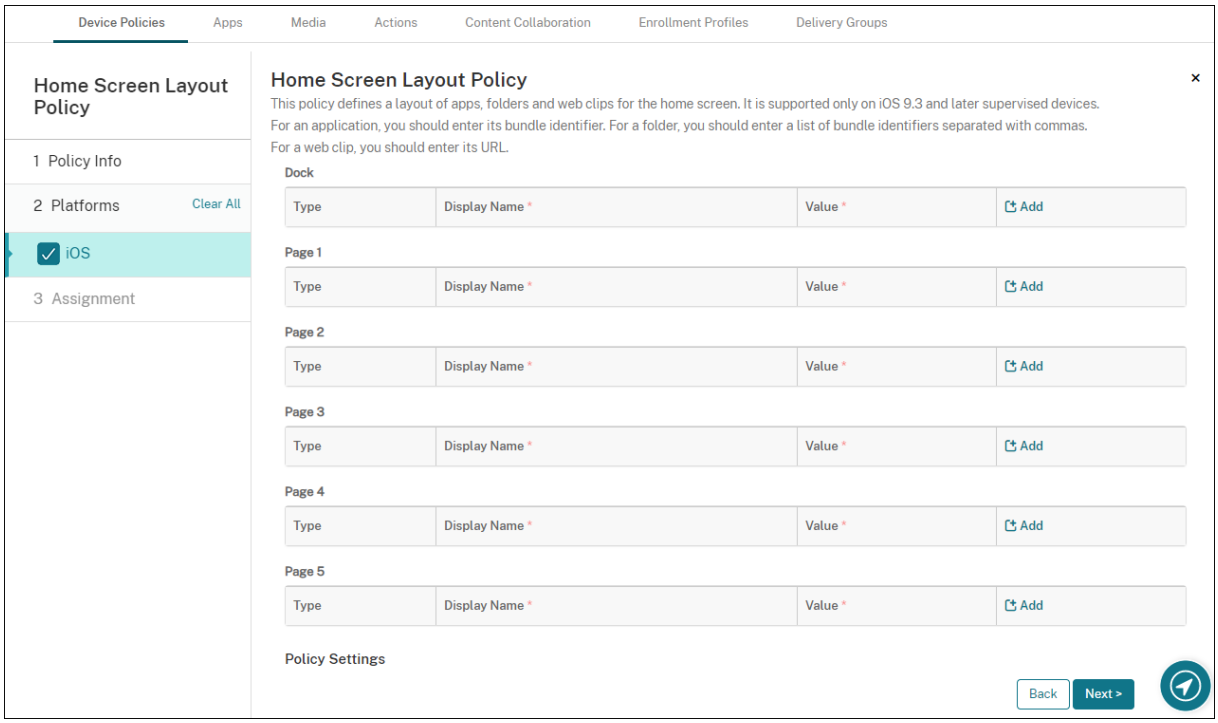
© 1997–2025 Citrix Systems, Inc. All rights reserved.

The **Home screen layout** device policy lets you specify the layout of apps and folders for the iOS Home screen of supervised iOS devices.

> **Important:**
>
> Deploying multiple Home Screen Layout policies to a device results in an iOS error on the device. This limitation applies whether you define the home screen through this Citrix Endpoint Management policy or through the Apple Configurator.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

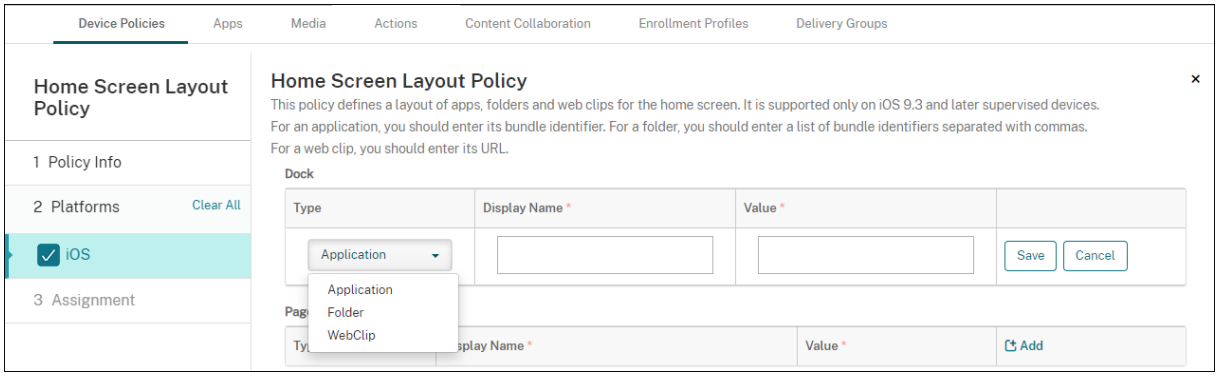


- For each of the screen areas you want to configure (such as **Dock** or **Page 1**), click **Add**.
- **Type:** Choose **Application**, **Folder**, or **Web Clip**.

  The **Restricted app usage > Allow only some apps** setting in the Restrictions device policy can prevent web clips from appearing properly on the home screen. For web clips to appear properly, do either of the following:

  - Set **Restricted app usage** to **Allow all apps** or **Do not allow some apps**.
  - With **Restricted app usage** set to **Allow only some apps**, add an app with the bundle ID `com.apple.webapp` to allow web clips.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Display Name:** The name to appear on the home screen for the app or folder.
- **Value:** For apps, type the bundle identifier. For folders, type a list of bundle identifiers, separated by commas. For web clips, type the bundle ID `com.apple.webClip.managed` and configure the URL of the web clip in the web clip policy. If more than one Web Clip value exists with the same URL, the behavior is undefined on iOS 11.3 and later devices.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on iOS 9.3 and later.

Import iOS & macOS Profile device policy

September 6, 2025

You can import device configuration XML files for iOS and macOS devices into Citrix Endpoint Management. The file has device security policies and restrictions that you prepare with the Apple Configurator 2 or Profile Creator. The configuration XML file can have macros. For more information, see Macros.

Use cases

Import the following configurations created outside of Citrix Endpoint Management for macOS devices using Profile Creator:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **System Policy Control:** The policy identifies apps signed by the certified Apple developers and lets users download verified apps from the Mac App Store.

  When configuring the policy:

  - Select **Enable Gatekeeper** to make sure that users run only verified and trusted software.
  - Select **Allow Identified Developers** to make sure that users install apps only signed by certified Apple developers.

- **Privacy Preferences Policy Control:** The policy lets you grant or restrict cross-application access to certain files or features, such as location services, camera, and screen capture.

  Configure the settings that you plan to deploy. For more information, see Privacy Preferences Policy Control payload settings.

- **Kernel Extensions Policy:** The policy lets the users install app extensions that extend the native capabilities of the operating system. Kernel extensions run at the kernel level.

  Configure the settings that you plan to deploy. For more information, see Kernel Extension Policy payload settings.

- **Ethernet Settings Policy:** The policy lets you manage the Ethernet network connection.

  Configure the settings that you plan to deploy. For more information, see Ethernet settings.

Use either the Apple Configurator 2 or Profile Creator to configure the following policies for macOS and iOS devices:

- **Wi-Fi Policy:** The policy lets you manage how users connect their devices to a Wi-Fi network.

  When configuring the policy:

  - Add the target SSID to the top of the priority list.
  - Choose the connection mode to use when the user joins a network. If you select **System**, the device uses the system credentials to authenticate the user. If you select **Login window**, the device uses the same credentials entered at the login window to authenticate the user.

  For more information, see Wi-Fi settings.

- **Restrictions Policy:** The policy allows or restricts the use of certain features on user devices.

  Configure the settings that you plan to deploy. For more information, see Restrictions overview.

- **VPN Policy:** The policy provides a device-level encrypted connection to private networks.

  Configure the settings that you plan to deploy. For more information, see the VPN overview.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Create a configuration profile using the Apple Configurator 2

1. Install the Apple Configurator 2 from the Apple App Store.
2. Start the Apple Configurator 2 and go to **File > New Profile**. A new configuration window appears.
3. In the **General** settings pane, type a name and an identifier for your profile, then add any additional payload options.
4. On the left pane, select a payload, click **Configure**, and enter the settings. Don't sign your profile, as signed profiles aren't supported.

   To add multiple payloads within a single profile, select a payload and click the **Add Payload** button in the upper-right corner.
5. Go to **File > Save**, choose a name and location to save the XML file, and click **Save**.

Create a configuration profile using Profile Creator

1. Install the Profile Creator from GitHub.
2. Start the Profile Creator and go to **File > New**. A new configuration window appears.
3. In the **General** settings pane, type a name and description for your profile, then add any additional payload options.

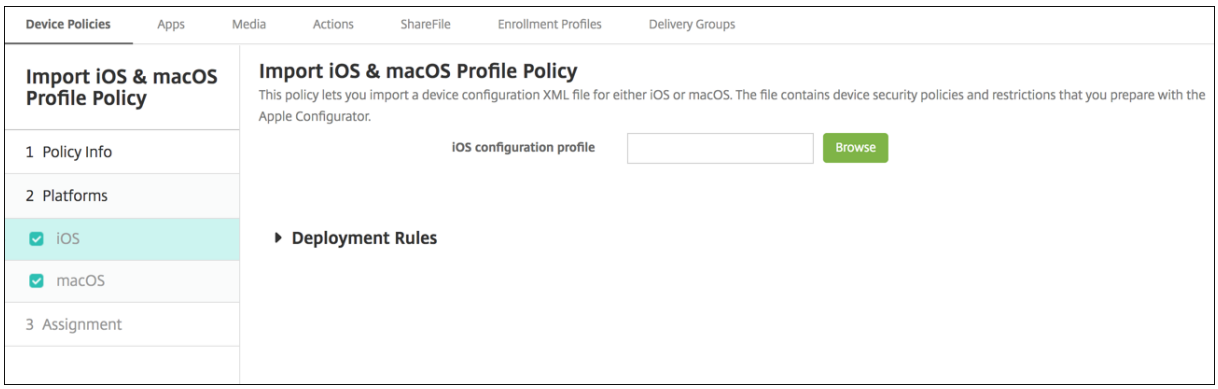
   - Recommendation: Select **Prevent users from removing this profile**.
   - Set **Payload Scope** to **System** or **User**.
4. On the left pane, choose the policy, configure the settings, and click **Add** in the upper-right corner.

   To configure multiple policies within a single profile, select a policy and click the **Add** button.
5. Go to **File > Export**, choose a name and location to save the XML file, and click **Save**.

To import a configuration file for the iOS and macOS Profile device policy in the Citrix Endpoint Management console, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS and macOS settings



- **iOS configuration profile** or **macOS configuration profile:** To select the configuration file to import, click **Browse** and then navigate to the file location.

Compliance Enforcement for Android device (Technical Preview)

September 6, 2025

> **Note:**
>
> Features in the Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. You can provide feedback on this feature by clicking **Send us your feedback**. Citrix might act on feedback based on its severity, criticality, and importance.

For Android devices enrolled in *Device Owner* mode, customer admin can manage the device compliance. They can define custom rules to assess compliance, including:

- Ensuring device password strength meets specified standards.
- Verifying installation of all required apps.
- Confirming removal of any forbidden apps.

In cases where devices are found non-compliant, customers can prompt users to rectify the issues. Additionally, more stringent measures are available, such as freezing apps on the device to restrict user access until compliance is achieved.
To enable this functionality, two prerequisites are necessary, as changes are required on both server and client sides:

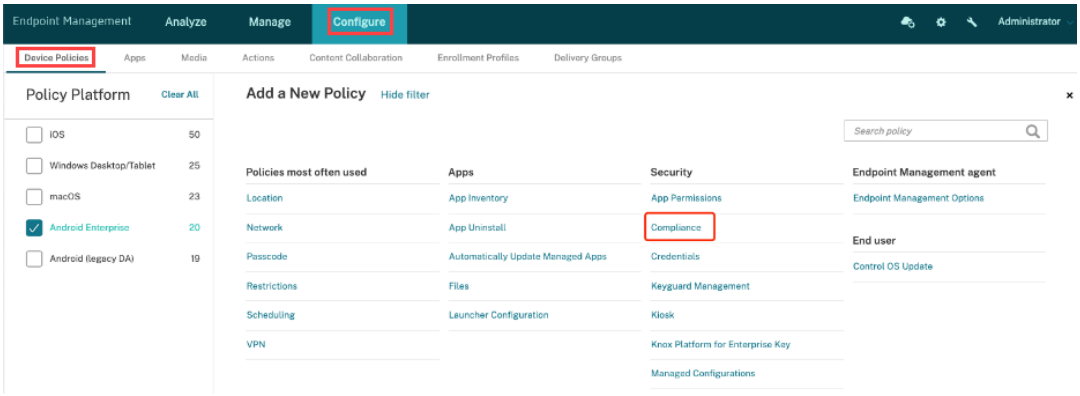
- Upgrade CEM Server to version 24.8.0.
- Upgrade Secure Hub to version 24.8.0.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Android Device Compliance Management Procedure

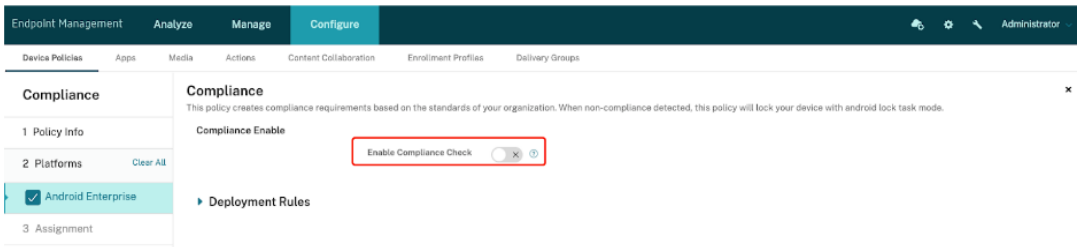
1. Activate the feature flag `afw.policy.compliance` specifically for the CEM server.
2. Add and deploy Compliance policy.

   a) From the **Configure** tab, select **Device Policies**, and click **Compliance**.



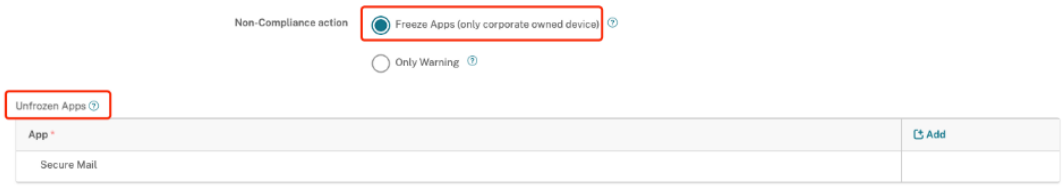
   b) Configure the policy with the following settings:

   - Enable **Compliance Check**: This setting controls whether devices undergo compliance checks. To revoke a deployed compliance policy, disable this option and redeploy the policy. Just by removing the policy from the delivery group will not be effective.



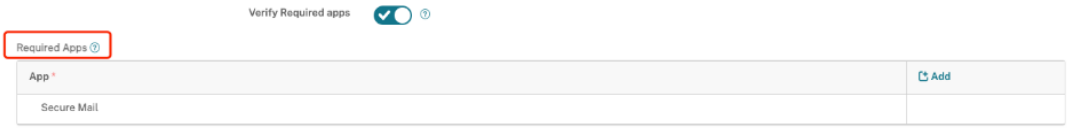
   - Non-Compliance Action: Choose between **Only Warning** and **Freeze Apps (only corporate owned device)**. Selecting **Only Warning** will notify users in Secure Hub about non-compliant items and request them to address these issues. Choosing **Freeze Apps (only corporate owned device)** locks all apps on the device, but admins can customize an Unfrozen Apps list to exempt specific apps, such as Secure Hub (for displaying and resolving non-compliant items), Google Play Store (for installing necessary apps), Settings (for factory resets), and SMS (for emergency communication). The **Freeze Apps (only corporate owned device)** is applicable only to corporate owned devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- Verify Passcode Compliance: Checks if device passcodes meet the specified standards. Typically used with passcode policies.
- Verify Required apps: Displays a list of mandatory apps. Ensures these apps are installed on the device.

> **Note:**
>
> - Apps listed under **Required Apps** must also be included in the required apps section of the delivery group to ensure their functionality. Otherwise, they will not be effective.
> - As required apps might be unavailable in managed Google Play, end users will remain in locked mode.



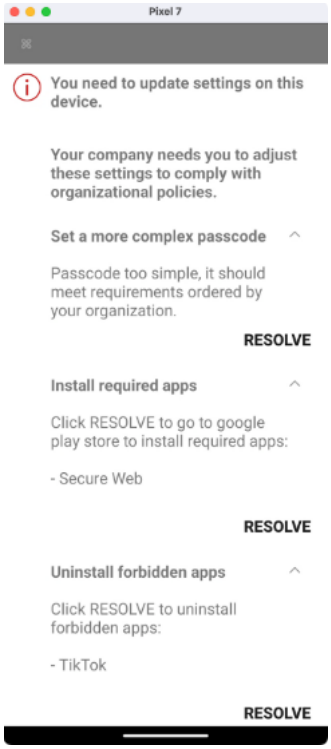
- Verify Forbidden Apps: Displays a list of prohibited apps. Ensures none of these apps are installed.

> **Note:**
>
> Admins should refrain from adding system pre-installed apps to the **Forbidden Apps** list, as end users do not have permission to remove them.

3. Deploy Policy.

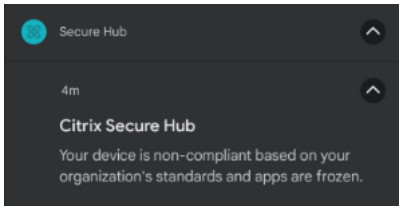
   a) In Secure Hub, click Refresh Policy or wait for the 6-hour periodic sync to deploy the policy to devices.
   b) Upon deployment, a compliance check is immediately triggered. Non-compliant devices in Freeze Apps mode restrict both the device and its apps until compliance is met.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



If the admin configures the Non-compliance Action to Freeze Apps, both Secure Hub and the device itself will restrict app usage. Specifically:

- A persistent notification will appear in the notification bar, reminding the user that apps have been frozen.

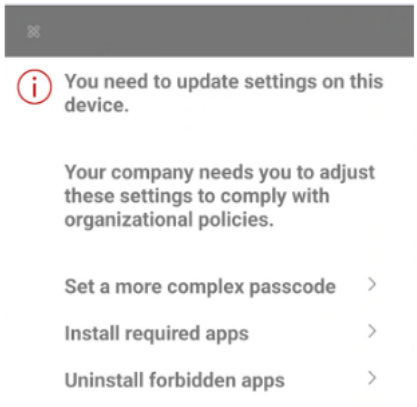


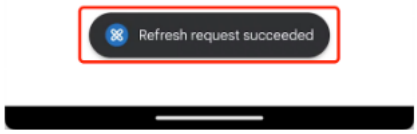
- Apps, excluding those listed as default allowed or in the **Unfrozen Apps** list, will be frozen and unresponsive when clicked.
- This state persists until the device achieves compliance. Even after restarting or undergoing a system upgrade, the device will immediately return to this frozen state (except during Secure Hub upgrades, which require manual launching by the user).

4. Non-Compliance Resolution:

   - When a device is non-compliant, Secure Hub is blocked from refreshing the policy through the usual method (clicking the **Refresh policy** button in **Device information** page).
   - Instead, an alternative solution is provided by pulling down the page that displays the non-compliant items, and the refresh result is conveyed through a toast notification.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

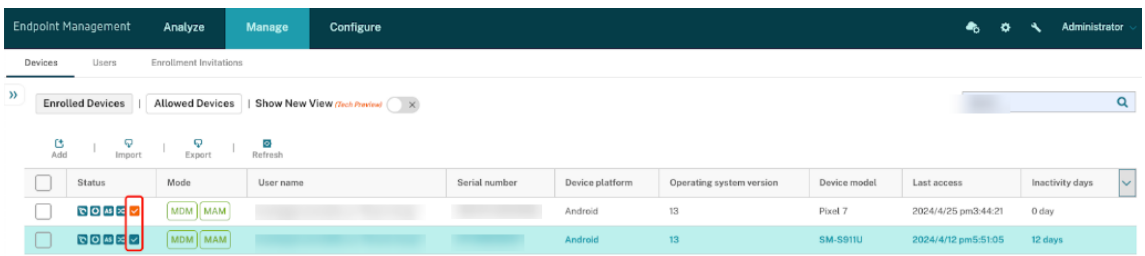




- Specific actions for users:
  - Set a more complex passcode to meet standards.
  - Install required apps from the Google Play Store.
  - Uninstall forbidden apps.

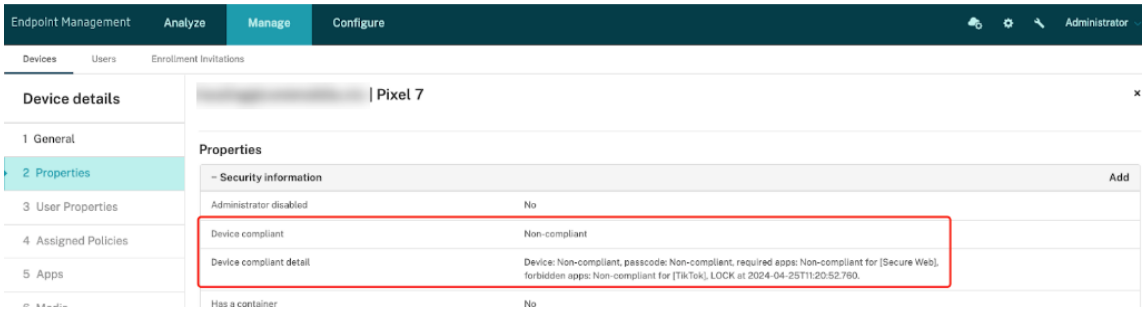
5. Monitoring compliance

   - View compliance status: A new compliance status icon in **Manage** -> **Devices** -> **Status**. Green indicates compliance, while orange indicates non-compliance.



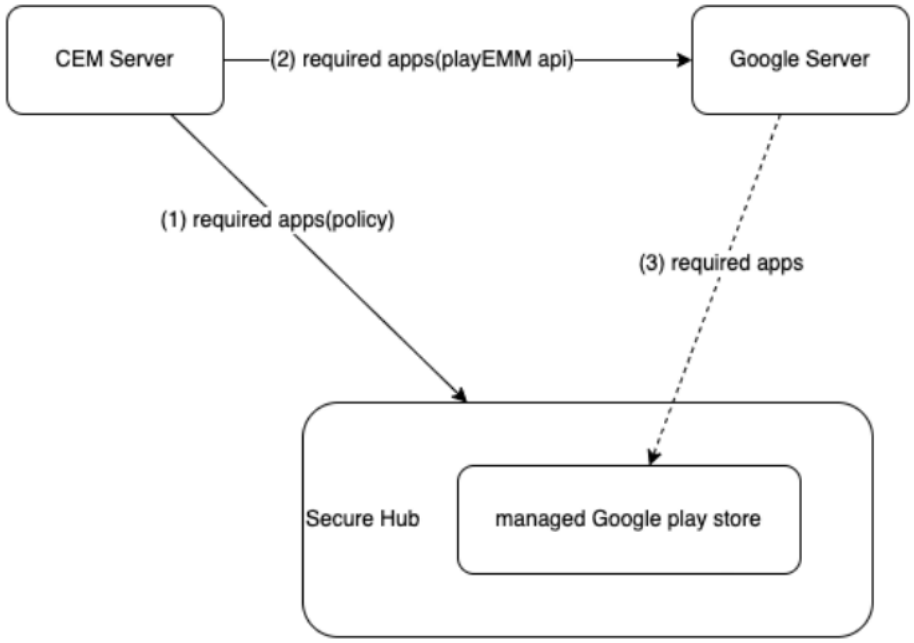
   - Detailed compliance status available in **Manage** -> **Devices** -> **Device details** -> **Properties** -> **Security Information**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Troubleshooting

1. The configured required app cannot be found on the Google Play Store, resulting in the device becoming non-compliant and unable to resolve the issue. This is a design flaw.



   The CEM Server pushes required apps to Secure Hub and Google Servers through links 1 and 2, but link 3 is beyond our control. When Secure Hub checks for required apps using link 1, we cannot guarantee that the managed Google Play Store has these apps available. This discrepancy means that while the compliance policy requires Secure Hub to install these apps, they might not not be found in the store immediately. Typically, Google Servers push the required apps to the device within 24 hours using link 3.

2. Before upgrading Secure Hub, the device was non-compliant, and the apps were frozen. However, after upgrading Secure Hub, all apps were unfrozen. This occurred because during the upgrade process, Secure Hub's operation was terminated, preventing it from maintaining the app freeze.

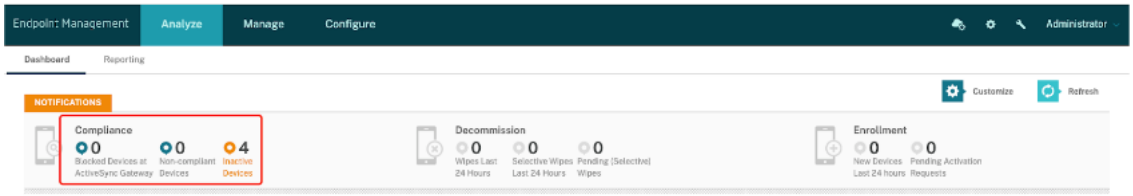
© 1997–2025 Citrix Systems, Inc. All rights reserved.

This issue is known and currently has no solution. We are actively working with Google to address this and expect improvements in future versions. After completing the upgrade, users can manually launch Secure Hub to initiate the process and restore the apps to their frozen state.

3. How to unfreeze apps?
   The most common method is for users to resolve all non-compliant issues, thereby bringing the device into compliance and automatically unfreezing all apps. If it's not feasible to achieve compliance quickly, the following steps can be taken:

   - Add related apps to the Unfrozen Apps list and perform a pull-down refresh.
   - Change the Non-Compliance Action to Warning and perform a pull-down refresh.
   - Disable the check switch corresponding to non-compliant items or the master switch, then perform a pull-down refresh.
   - If none of the above methods work, enable the feature flag `afw.locktaskmode.disable` for the specific CEM server and perform a pull-down refresh. This action forcibly unfreezes all apps, but Secure Hub remains blocked similar to when Non-Compliance Action is set to **Warning**.
   - Disable the feature flag `afw.policy.compliance` for the specific CEM server and perform a pull-down refresh.
   - In the worst-case scenario where Secure Hub cannot connect to the CEM Server, perform a factory reset from Settings.

4. The Compliance status displayed under Analyze -> Dashboard is a different type of compliance in Citrix Endpoint Management™ than the one referenced in this policy. This feature is not yet developed and will be enhanced in future versions.



5. This feature does not apply to devices enrolled through COSU/WPCOD/BYOD modes. Currently, it only supports devices enrolled in Device Owner (DO) mode.

Keyguard Management device policy

March 7, 2024

The Android keyguard manages the device and work challenge lock screens. This policy lets you manage features for Android Enterprise work profile keyguard and advanced device keyguard. You can control:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

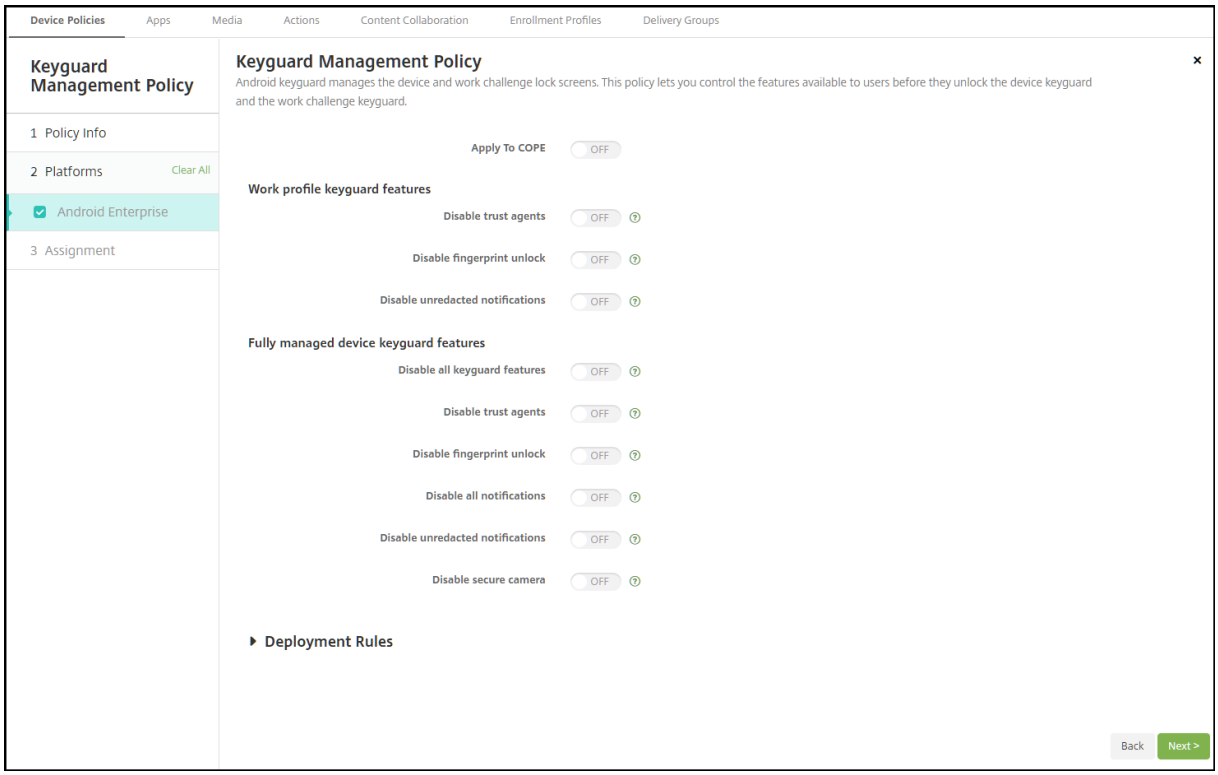
- Keyguard management on work profile devices. You can specify the features available to users before they unlock the device keyguard and the work challenge keyguard. For example, by default users can use fingerprint unlock and view unredacted notifications on the lock screen.
- Keyguard management on fully managed and dedicated devices. You can specify the features available, such as trust agents and secure camera, before they unlock the keyguard screen. Or, you can choose to disable all keyguard features.
- Keyguard management on fully managed devices with work profiles. These devices were formerly known as COPE (corporate owned personally enabled) devices. You can use one Keyguard Management policy to apply separate settings to the device and the work profile.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Watch this video to learn more:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Android Enterprise settings



- **Apply to COPE:** Allows you to configure Keyguard Management device policy settings for fully managed devices with work profiles.

  When this setting is **On**, you can apply separate settings to the device and to the work profile on fully managed devices with work profiles.

  When this setting is **Off**, you can apply settings to work profile devices or fully managed devices. Settings you configure for work profiles only apply to work profile devices. Settings you configure for fully managed devices apply only to fully managed devices.

  Default is **Off**.

- **Work profile keyguard features:** Controls whether the following features are available before a user unlocks the work profile keyguard (lock screen).

  - **Disable trust agents:** If **Off**, trust agents can operate on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable all trust agents on the work profile. Default is **Off**.
  - **Disable biometric authentication:** If **Off**, biometric authentication is available on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable biometric authentication on the work profile. This setting disables fingerprint unlock, face authentication, and iris authentication. Default is **Off**. For Android 9.0 and later.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Disable fingerprint unlock:** If **Off**, fingerprint unlock is available on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable fingerprint unlock on the work profile. Default is **Off**.
  - **Disable face authentication:** If **Off**, face authentication is available on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable face authentication on the work profile. Default is **Off**. For Android 9.0 and later.
  - **Disable iris authentication:** If **Off**, iris authentication is available on secure keyguard screens when a challenge is set on the work profile. Set to **On** to disable iris authentication on the work profile. Default is **Off**. For Android 9.0 and later.
  - **Disable unredacted notifications:** If **Off**, both redacted and unredacted notifications appear on secure keyguard screens. Set to **On** to disable unredacted notifications and only show redacted notifications. Default is **Off**.

- **Fully managed device keyguard features:** Controls whether the following features are available before a user unlocks the device keyguard (lock screen). These features apply to fully managed or dedicated devices.

  - **Disable all keyguard features:** If **Off**, all current and future keyguard customizations are available on the secure keyguard screens. Set to **On** to disable all keyguard customizations. Default is **Off**.
  - **Disable trust agents:** If **Off**, trust agents can operate on secure keyguard screens. Set to **On** to disable trust agents. Default is **Off**.
  - **Disable biometric authentication:** If **Off**, biometric authentication is available on secure keyguard screens when a challenge is set on the device. Set to **On** to disable biometric authentication on the device. The biometric authentication features disabled are fingerprint unlock, face authentication, and iris authentication. Default is **Off**. For Android 9.0 and later.
  - **Disable fingerprint unlock:** If **Off**, fingerprint unlock is available on secure keyguard screens when a challenge is set on the device. Set to **On** to disable fingerprint unlock on the device. Default is **Off**.
  - **Disable face authentication:** If **Off**, face authentication is available on secure keyguard screens when a challenge is set on the device. Set to **On** to disable face authentication on the device. Default is **Off**. For Android 9.0 and later.
  - **Disable iris authentication:** If **Off**, iris authentication is available on secure keyguard screens when a challenge is set on the device. Set to **On** to disable iris authentication on the device. Default is **Off**. For Android 9.0 and later.
  - **Disable all notifications:** If **Off**, all notifications appear on secure keyguard screens. Set to **On** to show all notifications. Default is **Off**.
  - **Disable unredacted notifications:** If **Off**, both redacted and unredacted notifications appear on secure keyguard screens. Set to **On** to disable unredacted notifications and only show redacted notifications. Default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Disable secure camera:** If **Off**, secure camera is available on secure keyguard screens. Set to **On** to disable the secure camera. Default is **Off**.

Kiosk device policy

September 6, 2025

The Kiosk policy lets you restrict devices to Kiosk mode by limiting the apps that can run. Citrix Endpoint Management does not control which part of the device locks in Kiosk mode. The device manages the kiosk mode settings after you deploy the policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

To set up iPads to run in Kiosk mode, use the App lock device policy. For information about setting up iPads as kiosks, see Configure an iPad as a kiosk. You can also configure an iPad to open only a single website. For information, see the Webclip policy.

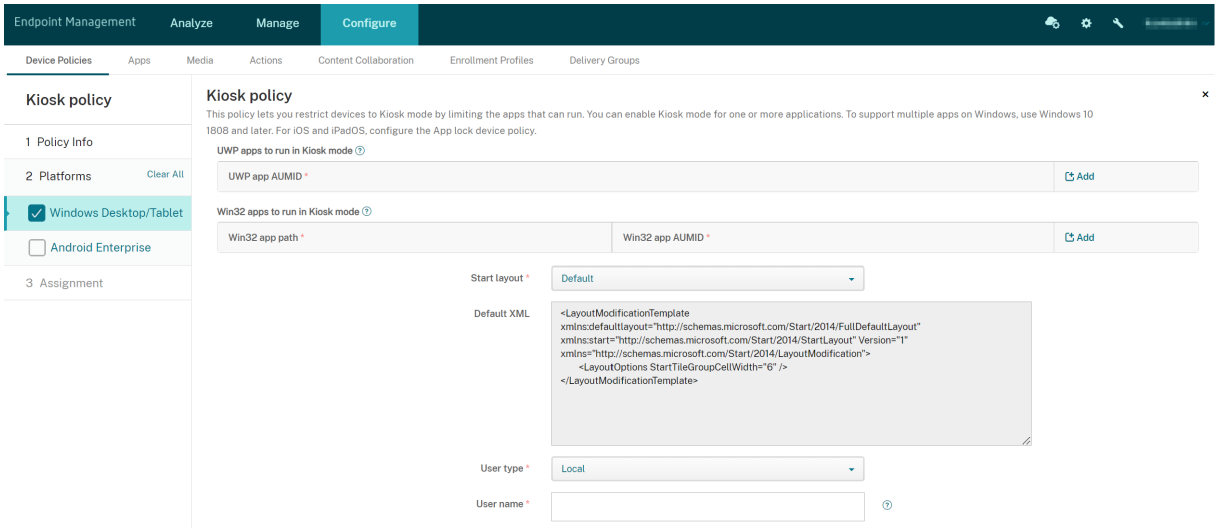
Windows Desktop and Tablet settings

For Windows Desktop and Tablet devices, the Kiosk policy applies only to local users and users enrolled in Azure AD.

A single app or multiple apps can run in Kiosk mode on Windows Desktop and Tablet devices.

> **Note:**
>
> The Kiosk device policy applies only to Windows 10 devices.
> To deploy a single-app kiosk on Windows 11 devices, you can use the Custom XML device policy to deploy the XML script we provide to the devices. For more information, see Deploy a single-app kiosk on Windows 11 devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **UWP app AUMID:** Click **Add**, select Universal Windows Platform (UWP) app, and enter the application user model ID (AUMID) for each UWP app. For example, enter the following AUMID:
  - `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`
- **Win32 app path** and **Win32 app AUMID**: Click **Add**, select the Windows desktop (`Win32`) app, and enter the path and the AUMID for each `Win32` app. For example, enter the following path and AUMID:
  - `%windir%\system32\mspaint.exe` or `C:\Windows\System32\mspaint.exe`
  - `{ 1AC14E77-02E7-4E5D-B744-2EB1AE5198B7 } \mspaint.exe`
- **Start layout:** Only the default start screen for apps is available.
- **Default XML:** Only the default XML script is available.
- **Select user type:** Specify the user type to receive the Kiosk policy. Your options:
  - **Local:** Citrix Endpoint Management creates a user for the target device or adds an existing user.
  - **Azure AD:** Citrix Endpoint Management adds users enrolled in Azure AD.
- **User name:** Enter the user name to receive the Kiosk policy.
  - To create a local user name on the target device, enter the name. Make sure that your local user name doesn't have the domain. If you enter an existing name, Citrix Endpoint Management doesn't create a user or change the current password.
  - To add an Azure AD user, enter the name in the format `azuread\user`. The `user` portion can be either the **Name** entered when creating a user in Azure AD, or the **User name** entered when creating a user in Azure AD. The assigned user can't be an Azure AD administrator.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Password:** There is no password configuration for the Azure AD users. Type the password only for the local user name.
- **Show task bar:** Enable the taskbar to provide users with an easy way to view and manage applications. The default is **Off**.
- Click **Next** and save the changes.

For a UWP app that you want to allow in Kiosk mode, you need to provide the AUMID. To get a list of the AUMIDs for all Microsoft Store apps installed for the current device user, run the following PowerShell command:

```
$installedapps = get-AppxPackage

$aumidList = @()
foreach ($app in $installedapps)
{

    foreach ($id in (Get-AppxPackageManifest $app).package.applications
        .application.id)
    {

        $aumidList += $app.packagefamilyname + "!"+ $id
     }

 }


$aumidList
```

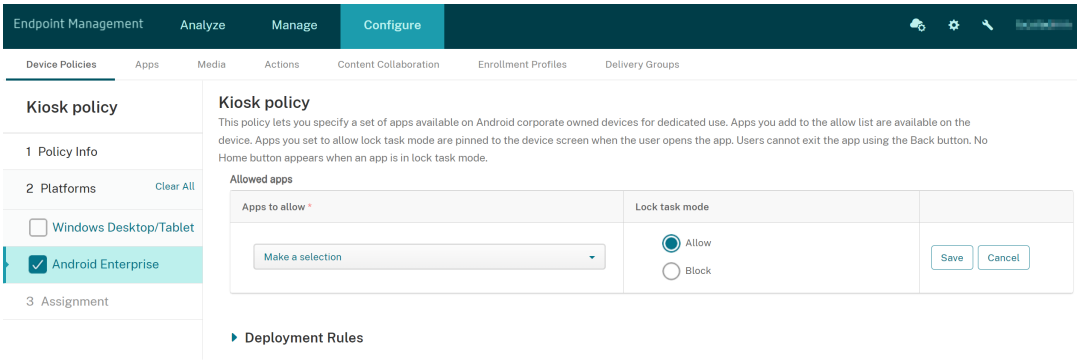
Android Enterprise settings

You can allow apps and set lock task mode for dedicated Android Enterprise devices, which are also known as corporate owned single use (COSU) devices.

To allow an app, click **Add**. You can add multiple apps to the allow list. For more information, see Android Enterprise.

- **Apps to allow:** Enter the package name of the app that you want to allow or select the app from the list.
  - Click **Add new** to enter the package name of the allowed app in the list.
  - Select the existing app from the list. The list shows apps that are uploaded in Citrix Endpoint Management. By default, Citrix Secure Hub and Google Play services are on the allow list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Lock task mode:** Choose **Allow** to set the app to be pinned to the device screen when the user starts the app. Choose **Block** to set the app not to be pinned. Default is **Allow**.

When an app is in lock task mode, the app is pinned to the device screen when the user opens it. No Home button appears and the **Back** button is disabled. The user exits the app using an action programmed into the app, such as signing out.

Knox Platform for Enterprise Key device policy

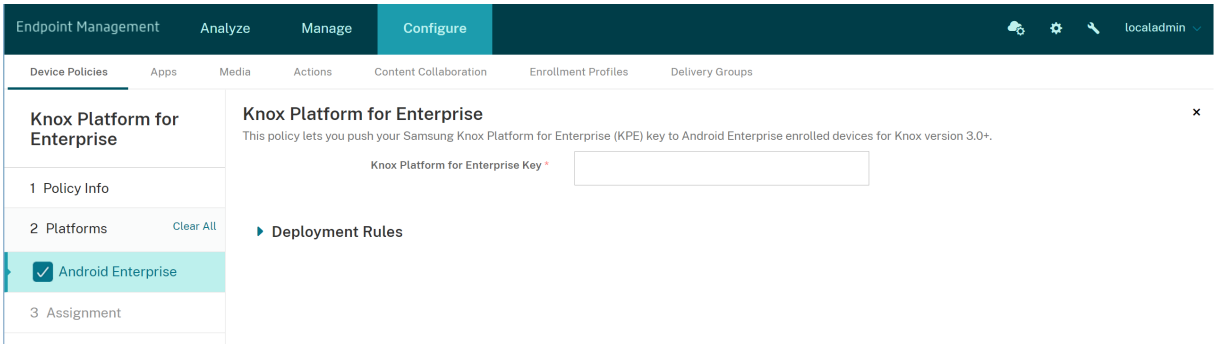
April 16, 2024

This policy allows you to provide the required Samsung Knox Platform for Enterprise (KPE) license information.

To add or configure this policy, navigate to **Configure** > **Device Policies**. For more information, see Device policies.

Android Enterprise settings

This policy provides the required Samsung Knox Platform for Enterprise (KPE) license information. For Android 12 or earlier, you must request a KPE premium license to use Knox premium features. For Android 13 or later, KPE premium license is provided by default.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Knox Platform for Enterprise Key: Enter the Samsung Knox Platform for Enterprise (KPE) key that you want to push to the Android Enterprise device. Apply for a KPE license key at Samsung Knox Platform for Enterprise (KPE) key.

Launcher configuration device policy

September 6, 2025

Citrix Launcher lets you customize the user experience for Android Enterprise devices and legacy Android devices deployed by Citrix Endpoint Management.

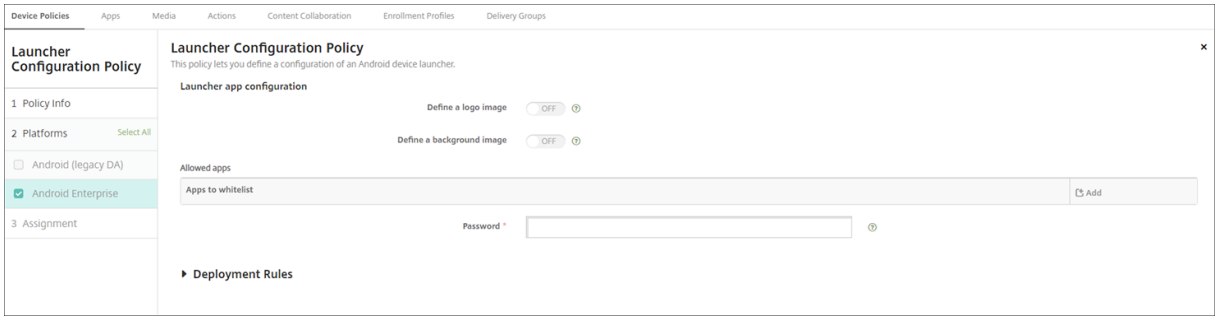
Use a Launcher configuration policy to control these Citrix Launcher features:

- Manage Android Enterprise devices and legacy Android devices so that users can access only the apps that you specify.
- Optionally specify a custom logo image for the Citrix Launcher icon and a custom background image for Citrix Launcher.
- Specify a password that users must type to exit the launcher.

Citrix Launcher isn't intended to be an extra layer of security over what the device platform already provides.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Android Enterprise and Android settings



- **Define a logo image:** Select whether to use a custom logo image for the Citrix Launcher icon. The default is **Off**.
- **Logo image:** When you enable **Define a logo image**, select the image file by clicking **Browse** and navigating to the file's location. Supported file types are PNG, JPG, JPEG, and GIF.
- **Define a background image:** Select whether to use a custom image for the Citrix Launcher background. The default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Background image:** When you enable **Define a background image**, select the image file by clicking **Browse** and navigating to the file's location. Supported file types are PNG, JPG, JPEG, and GIF.
- **Allowed apps:** For each app that you want to allow in Citrix Launcher, click **Add** and then do the following:
  - **New app to add:** Enter the full name of the app to add. For example, com.android.calendar for the Android calendar app.
  - Click **Save** to add the app or click **Cancel** to cancel adding the app.
- **Password:** The password a user must enter to exit Citrix Launcher.

LDAP device policy

September 6, 2025

You create an LDAP policy for iOS devices in Citrix Endpoint Management to provide information about an LDAP server to use, including any necessary account information. The policy also provides a set of LDAP search policies to use when querying the LDAP server.

You need the LDAP host name before configuring this policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Account description:** Enter an optional account description.
- **Account user name:** Enter an optional user name.
- **Account password:** Enter an optional password. Use this field only with encrypted profiles.
- **LDAP host name:** Enter the LDAP server host name. This field is required.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the LDAP server. The default is **On**.
- **Search Settings:** Add search settings to use when querying the LDAP server. You can enter as many search settings as you want, but you must add at least one search setting to make the account useful. Click **Add** and then do the following:
  - **Description:** Enter a description of the search setting. This field is required.
  - **Scope:** Choose **Base**, **One level**, or **Subtree** to define how deeply into the LDAP tree to search. The default is **Base**.
    - **Base** searches the node pointed to by Search base.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    - **One level** searches the Base node and one level below it.
    - **Subtree** searches the Base node, plus all its children, regardless of depth.
  - **Search base:** Enter the path to the node at which to start searching. For example, ou=people or 0=example corp. This field is required.
  - Click **Save** to add the search setting or click **Cancel** to cancel adding the search setting.
  - Repeat these steps for each search setting that you want to add.

- **Policy settings**

  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.

macOS settings

- **Account description:** Enter an optional account description.
- **Account user name:** Enter an optional user name.
- **Account password:** Enter an optional password. Use this field only with encrypted profiles.
- **LDAP host name:** Enter the LDAP server host name. This field is required.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the LDAP server. The default is **On**.
- **Search Settings:** Add search settings to use when querying the LDAP server. You can enter as many search settings as you want, but you must add at least one search setting to make the account useful. Click **Add** and then do the following:

  - **Description:** Enter a description of the search setting. This field is required.
  - **Scope:** Choose **Base**, **One leve**l, or **Subtree** to define how deeply into the LDAP tree to search. The default is **Base**.
    - **Base** searches the node pointed to by the Search base.
    - **One level** searches the Base node and one level below it.
    - **Subtree** searches the Base node, plus all its children, regardless of depth.
  - **Search base:** Enter the path to the node at which to start searching. For example, ou=people or 0=example corp. This field is required.
  - Click **Save** to add the search setting or click **Cancel** to cancel adding the search setting.
  - Repeat these steps for each search setting that you want to add.

- **Policy settings**

  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
- **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
- **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

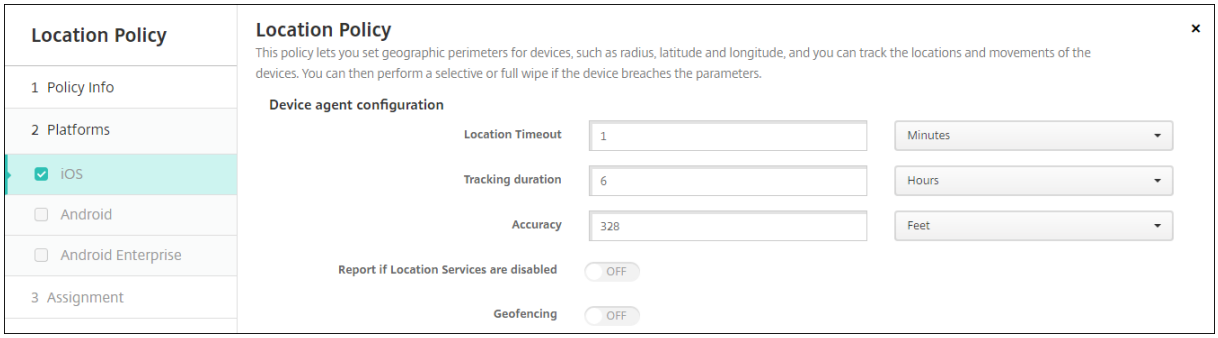
Location device policy

September 6, 2025

You create location device policies in Citrix Endpoint Management to enforce geographic boundaries. When users breach the defined boundary, also called a *geofence*, Citrix Endpoint Management can do certain actions. For example, you can configure the policy to issue a warning message to users when they breach the defined perimeter. You can also configure the policy to wipe users' corporate data when they breach a perimeter, right away or after a delay. For information about security actions, such as enabling tracking and locating a device, see Security actions.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

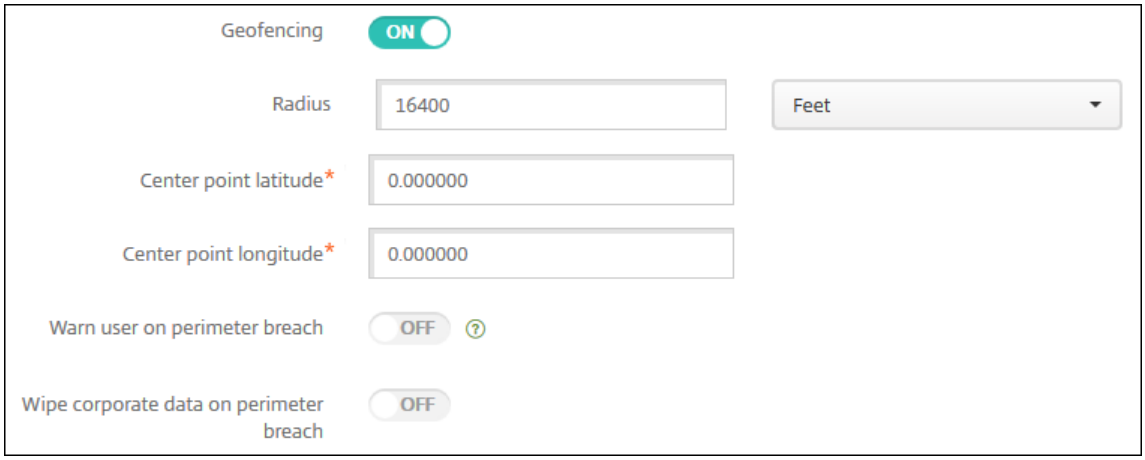
iOS settings



- **Location timeout:** Type a numeral and then click **Seconds** or **Minutes** to set how often Citrix Endpoint Management attempts to fix the device's location. Valid values are 60–900 seconds or 1–15 minutes. The default is **1 minute**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Tracking duration:** Type a numeral and then click **Hours** or **Minutes** to set how long Citrix Endpoint Management tracks the device. Valid values are 1–10 hours or 10–600 minutes. The default is **6 hours**.
- **Accuracy:** Type a numeral and then click **Meters**, **Feet**, or **Yards** to set how close to a device Citrix Endpoint Management tracks the device. Valid values are 10–5000 yards, 30–15000 feet, or 10–5000 meters. The default is **328 feet** (**100 meters**).
- **Report if Location Services are disabled:** Select whether the device sends a report to Citrix Endpoint Management when the user turns off the GPS. The default is **Off**.
- **Geofencing**



When you enable Geofencing, configure these settings:

- **Radius:** Type a numeral and then click the units to be used to measure the radius. The default is **16400 feet** (**5000 meters**). Valid values for radius are:
  - 164–16400 feet
  - 50–50000 meters
  - 54–54680 yards
  - 1–31 miles
- **Center point latitude:** Type a latitude, such as 37.787454, to define the geofence center point's latitude.
- **Center point longitude:** Type a longitude, such as 122.402952, to define the geofence center point's longitude.
- **Warn user on perimeter breach:** Select whether to issue a warning message when users breach the defined perimeter. The default is **Off**. No connection to Citrix Endpoint Management is required to display the warning message.
- **Wipe corporate data on perimeter breach:** Select whether to wipe users'devices when they breach the perimeter. The default is **Off**. When you enable this option, the **Delay on local wipe**

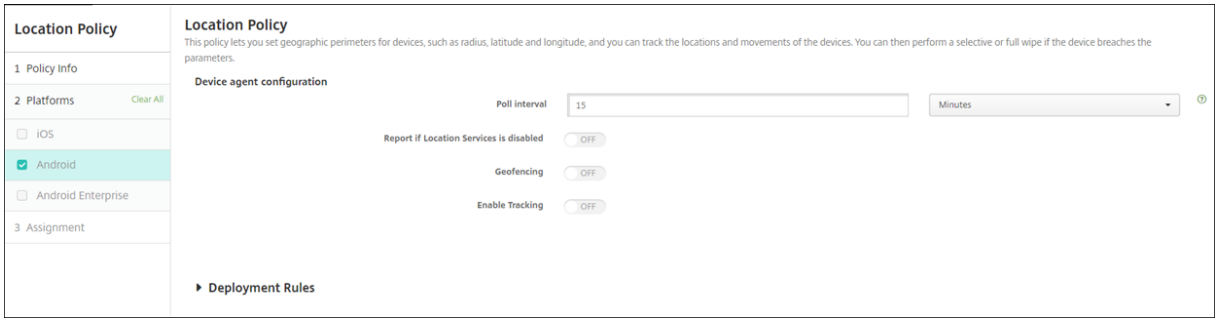
© 1997–2025 Citrix Systems, Inc. All rights reserved.

field appears.

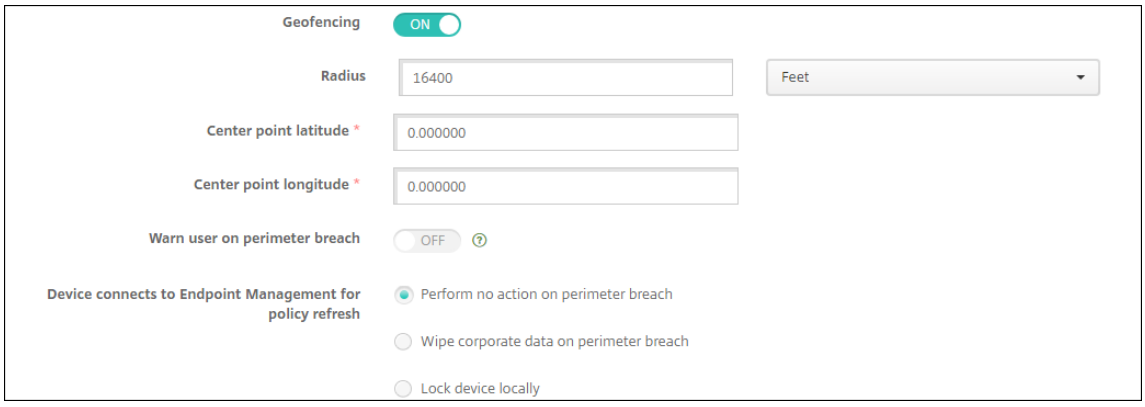
- Type a numeral and then click **Seconds** or **Minutes** to set the length of time to delay before wiping corporate data from user devices. The delay gives users an opportunity to return to the allowed location before Citrix Endpoint Management selectively wipes their devices. The default is **0 seconds**.

Android (legacy DA) settings

Android location tracking requires Android 9 or later.



- **Poll interval:** Type a numeral and then click **Minutes** or **Hours**, or **Days** to set how often Citrix Endpoint Management attempts to fix the device's location. Valid values are 15–1440 minutes, 1–24 hours, or any number of days. The default is **15 minutes**.
- **Report if Location Services are disabled:** Select whether the device sends a report to Citrix Endpoint Management when the user turns off the GPS. The default is **Off**.
- **Geofencing**



When you enable Geofencing, configure these settings:

- **Radius:** Type a numeral and then click the units to be used to measure the radius. The default is **16400 feet** (**5000 meters**). Valid values for radius are:
  - 164–164000 feet

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - 1–50 kilometers
  - 50–50000 meters
  - 54–54680 yards
  - 1–31 miles

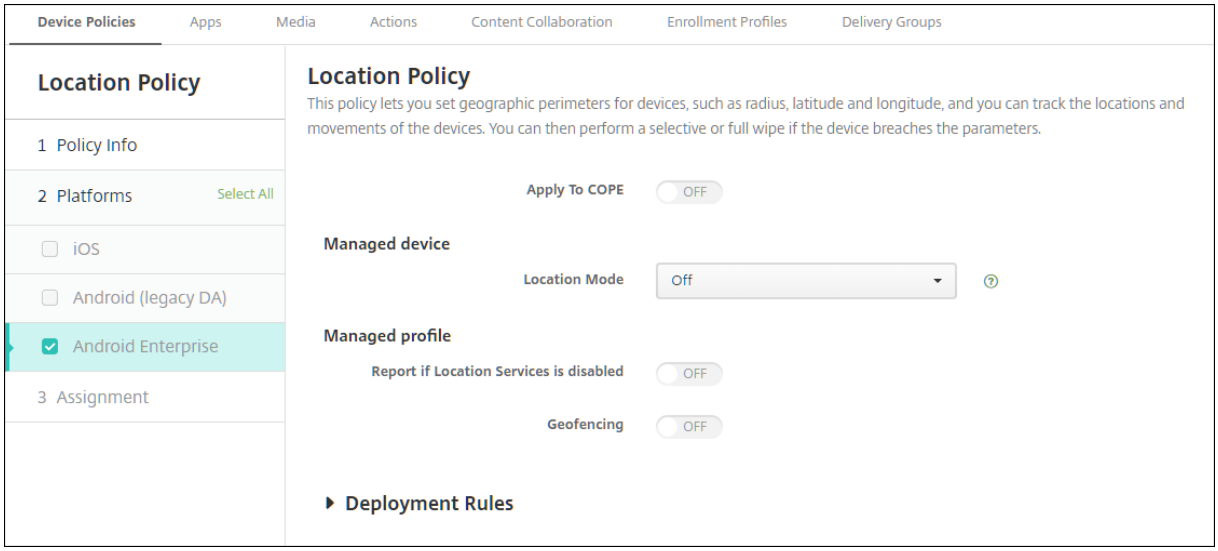
- **Center point latitude:** Type a latitude, such as 37.787454, to define the geofence center point's latitude.
- **Center point longitude:** Type a longitude, such as 122.402952, to define the geofence center point's longitude.
- **Warn user on perimeter breach:** Select whether to issue a warning message when users breach the defined perimeter. The default is **Off**. No connection to Citrix Endpoint Management is required to display the warning message.
- **Device connects to Citrix Endpoint Management for policy refresh:** Select one of the following options for when users breach the perimeter:
  - **Perform no action on perimeter breach:** Do nothing. This is the default.
  - **Wipe corporate data on perimeter breach:** Wipe corporate data after a specified length of time. When you enable this option, the **Delay on local wipe** field appears.
    * Type a numeral and then click **Seconds** or **Minutes** to set the length of time to delay before wiping corporate data from user devices. The delay gives users an opportunity to return to the allowed location before Citrix Endpoint Management selectively wipes their devices. The default is **0 seconds**.
  - **Lock device locally:** Lock users' devices after a specified length of time. When you enable this option, the **Delay on lock** field appears.
    * Type a numeral and then click **Seconds** or **Minutes** to set the length of time to delay before locking user devices. The delay gives users an opportunity to return to the allowed location before Citrix Endpoint Management locks their devices. The default is **0 seconds**.
- **Enable tracking:** Select whether the device tracks user location. The default is **Off**.

Android Enterprise settings

For Android location tracking to work, make sure that the following requirements are met:

- Android 9 or later
- The Allow location sharing setting enabled in the Restrictions device policy for Android Enterprise
- Connection scheduling (Firebase Cloud Messaging recommended)

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Apply to fully managed devices with a work profile

For fully managed devices with work profiles (formerly known as COPE devices), only the location mode setting is available.

- **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices:** Allows you to configure the location mode for fully managed devices with work profiles. When this setting is on, configure the settings for the work profile:
  - **Report if Location Services are disabled:** Select whether the device sends a report to Citrix Endpoint Management when the user turns off the GPS. The default is **Off**.
  - **Geofencing:** See the settings in this article under Managed device.

When **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices** is off, settings apply to the managed device and work profile as shown in the following sections. Default is **Off**.

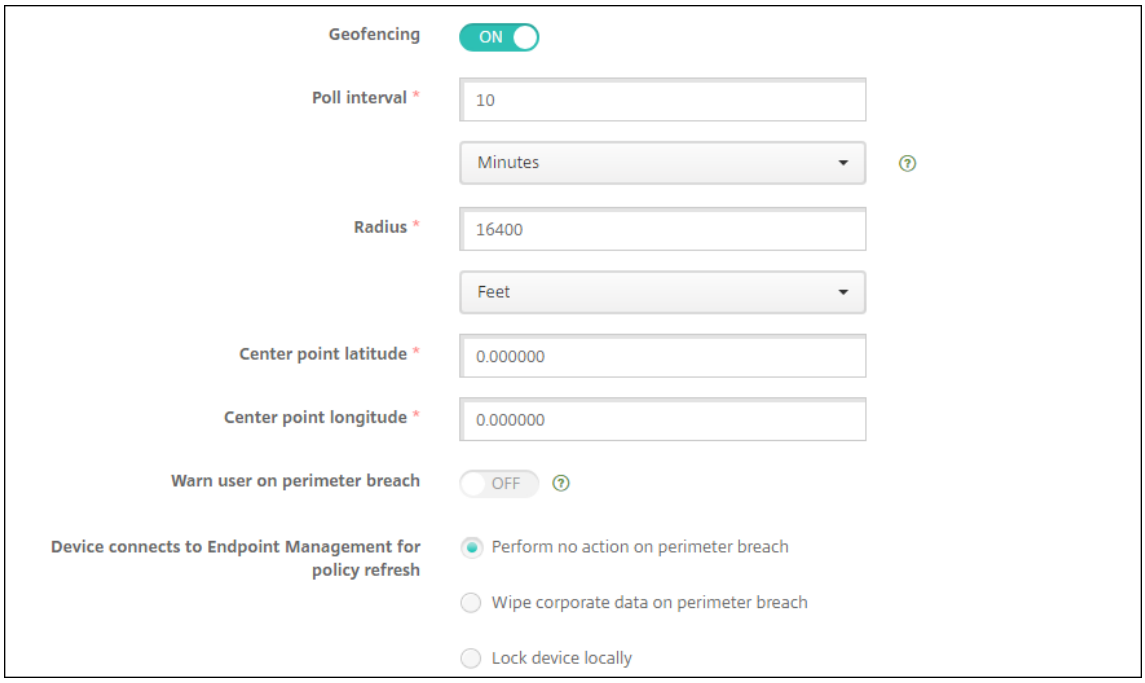
Managed device

- **Location Mode:** Specify the degree of location detection to enable. You can use the Locate security action only when the location mode is set to **High Accuracy** or **Battery Saving**. The default is **High Accuracy**.
  - **High Accuracy:** Enables all location detection methods, including GPS, networks, and other sensors.
  - **Sensors Only:** Enables only GPS and other sensors.
  - **Battery Saving:** Enables only the network location provider.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Off:** Disables location detection.

- **Geofencing:**



When you enable **Geofencing**, configure these settings:

- **Poll interval:** Type a numeral and then click **Minutes** or **Hours**, or **Days** to set how often Citrix Endpoint Management attempts to fix the device's location. Valid values are 1–1440 minutes, 1–24 hours, or any number of days. The default is **10 minutes**. Setting this value to less than 10 minutes might adversely affect the device's battery life.
- **Radius:** Type a numeral and then click the units to be used to measure the radius. The default is **16400 feet** (**5000 meters**). Valid values for radius are:
  - 164–164000 feet
  - 1–50 kilometers
  - 50–50000 meters
  - 54–54680 yards
  - 1–31 miles
- **Center point latitude:** Type a latitude, such as 37.787454, to define the geofence center point's latitude. To look up the value, go to **Manage > Devices**, select the device, click **Secure**, and then click **Locate**. After locating the device, Citrix Endpoint Management reports the device location in the **Device Details > General** page under **Security**.
- **Center point longitude:** Type a longitude, such as 122.402952, to define the geofence center point's longitude.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Warn user on perimeter breach:** Select whether to issue a warning message when users breach the defined perimeter. The default is **Off**. No connection to Citrix Endpoint Management is required to display the warning message.
- **Device connects to Citrix Endpoint Management for policy refresh:** Select one of the following options for when users breach the perimeter:
  - **Perform no action on perimeter breach:** Do nothing. This setting is the default.
  - **Wipe corporate data on perimeter breach:** Wipe corporate data after a specified length of time. When you enable this option, the **Delay on local wipe** field appears.
    * Type a numeral and then click **Seconds** or **Minutes** to set the length of time to delay before wiping corporate data from user devices. The delay gives users an opportunity to return to the allowed location before Citrix Endpoint Management selectively wipes their devices. The default is **0 seconds**.
  - **Lock device locally:** Lock users' devices after a specified length of time. When you enable this option, the **Delay on lock field** appears.
    * Type a numeral and then click **Seconds** or **Minutes** to set the length of time to delay before locking user devices. The delay gives users an opportunity to return to the allowed location before Citrix Endpoint Management locks their devices. The default is **0 seconds**.

Work profile

- **Report if Location Services are disabled:** Select whether the device sends a report to Citrix Endpoint Management when the user turns off the GPS. The default is **Off**.
- **Geofencing:** See the settings in this article under Managed device.

Lock screen message device policy

September 6, 2025

The **Lock screen message** policy lets you set messages to appear on the following iOS devices when they're lost:

- The login window of shared iPads
- The lock screen of supervised iOS devices

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS settings

- **Asset tag information for the device:** The asset tag for the device. Apple devices truncate long strings, so be sure to test a string before deploying the policy to production. The string length depends on the Apple device model and Apple settings, which can change.
- **Login window and lock screen footnote:** Information to help in returning the device, such as an address or other contact information. For example, your message might be in the form "If Lost, return to". Apple devices truncate long strings, so be sure to test a string before deploying the policy to production. The string length depends on the Apple device model and Apple settings, which can change.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

Mail device policy

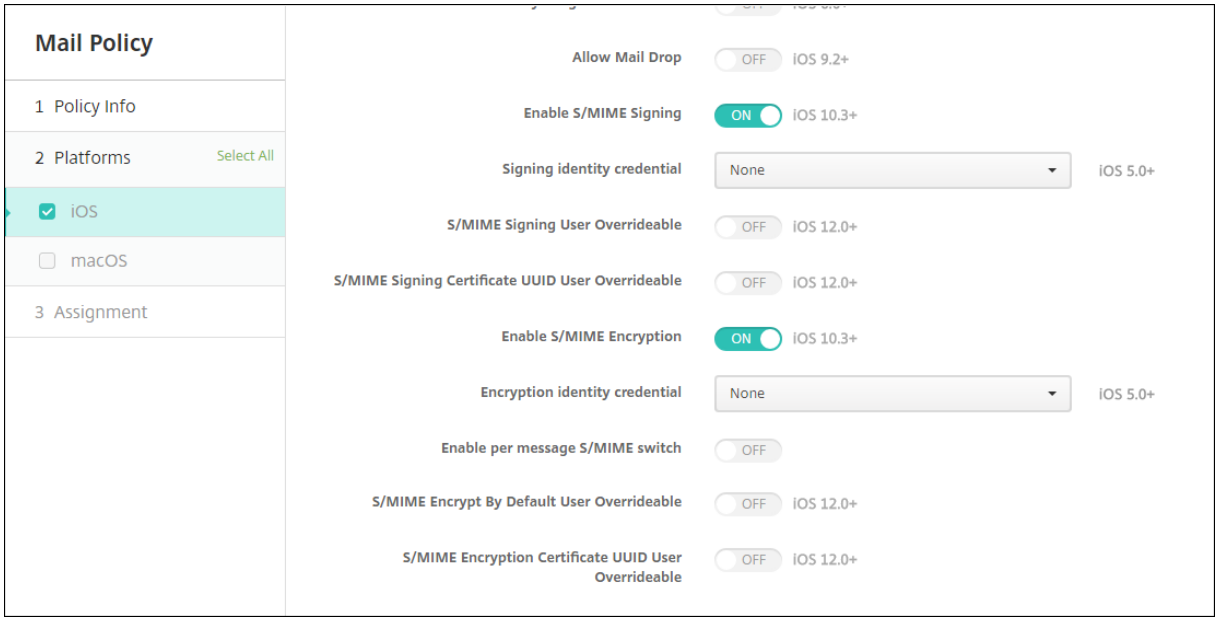
March 7, 2024

You can add a mail device policy in Citrix Endpoint Management to configure an email account on iOS or macOS devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS and macOS settings



- **Account description:** Type an account description that appears in the Mail and Settings apps. This field is required.
- **Account type:** Choose either **IMAP** or **POP** to select the protocol to be used for user accounts. The default is **IMAP**. When you select **POP**, the following **Path** prefix option disappears.
- **Path prefix:** Type **INBOX** or your IMAP mail account path prefix. This field is required.
- **User display name:** Type the full user name to be used for messages and other purposes. This field is required.
- **Email address:** Type the full email address for the account. This field is required.
- **Incoming email settings**
  - **Email server host name:** Type the incoming mail server host name or IP address. This field is required.
  - **Email server port:** Type the incoming mail server port number. The default is **143**. This field is required.
  - **User name:** Type the user name for the email account. This name is generally the same as the email address up to the @ character. This field is required.
  - **Authentication type:** Choose the authentication type to be used. The default is **Password**. When **None** is selected, the following **Password** field disappears.
  - **Password:** Type an optional password for the incoming mail server.
  - **Use SSL:** Select whether the incoming mail server uses Secure Socket Layer authentication. The default is **Off**.
- **Outgoing email settings**
  - **Email server host name:** Type the outgoing mail server host name or IP address. This

© 1997–2025 Citrix Systems, Inc. All rights reserved.

field is required.

- **Email server port:** Type the outgoing mail server port number. If no port, you do not enter a port number, the default port for the given protocol is used.
- **User name:** Type the user name for the email account. This name is generally the same as the email address up to the @ character. This field is required.
- **Authentication type:** Choose the authentication type to use. The default is **Password**.
- **Password:** Type an optional password for the outgoing mail server.
- **Outgoing password same as incoming:** Select whether the incoming and outgoing passwords are the same. The default is **Off**, which means the passwords are different.
- **Use SSL:** Select whether the outgoing mail server uses Secure Socket Layer authentication. The default is **Off**.

- **Policy**
  - **Authorize email move between accounts:** Select whether to allow users to:
    - move email out of this account into another account
    - forward email from a different account
    - reply from a different account.

    The default is **Off**.
  - **Sending email only from mail app:** Select whether to restrict users to the iOS mail app for sending email.
  - **Disable mail recents syncing:** Select whether to prevent users from syncing recent addresses. The default is **Off**. This option applies only to iOS 6.0 and later.
  - **Allow Mail Drop:** Select whether to allow use of Apple Mail Drop for devices running iOS 9.2 and later. The default is **Off**.
  - **Enable S/MIME Signing:** Select whether this account supports S/MIME signing. The default is **On**. When set to **On**, the following fields appear.
    - **Signing identity credential:** Choose the signing credential to use.
    - **S/MIME Signing User Overridable:** If set to **On**, users can turn S/MIME signing on and off in the settings of their devices. The default is **Off**. This option applies to iOS 12.0 and later.
    - **S/MIME Signing Certificate UUID User Overridable:** If set to **On**, users can select, in the settings of their devices, the signing credential to use. The default is **Off**. This option applies to iOS 12.0 and later.
  - **Enable S/MIME Encryption:** Select whether this account supports S/MIME encryption. The default is **Off**. When set to **On**, the following fields appear.
    - **Encryption identity credential:** Choose the encryption credential to use.
    - **Enable per message S/MIME switch:** When set to **On**, shows users an option to switch S/MIME encryption on or off for each message they compose. The default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    - **S/MIME Encrypt By Default User Overridable:** If set to **On**, users can, in the settings of their devices, select whether S/MIME is on by default. The default is **Off**. This option applies to iOS 12.0 and later.
    - **S/MIME Encryption Certificate UUID User Overridable:** If set to **On**, users can turn S/MIME encryption identity and encryption on and off in the settings of their devices. The default is **Off**. This option applies to iOS 12.0 and later.

- **Policy Settings**
  - **Remove policy:** To remove the policy later, configure this setting to remove the policy on a **Select date** or for a **Duration until removal (in hours)**.
  - **Allow user to remove policy:** Allow users to remove the mail policy **Always**, only with a **Passcode required**, or **Never**. Only available for macOS.
  - **Profile scope:** For macOS only, choose whether the policy applies on a per **User** level or across the whole **System**.

Managed configurations policy

January 15, 2025

The Managed configurations device policy controls various app configuration options and app restrictions. You create this policy for each Android Enterprise app that you want to control.

The app developer defines the options and tooltips available for an app. If a tooltip mentions using a "templated value,"use the corresponding Citrix Endpoint Management macro instead. For more information, see Remote configuration overview (on the Android developer site) and Macros.

The app configuration settings can include items such as:

- Email app settings
- Allow or block URLs for a web browser
- Option to control app content sync through a cellular connection or only by a Wi-Fi connection

For information about the settings that appear for your apps, contact the app developer.

> **Note:**
>
> Citrix SSO for Android is now called Citrix Secure Access. We are updating our documentation to reflect this name change.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Prerequisites

- Complete Android Enterprise setup tasks on Google and connect Android Enterprise to managed Google Play. For more information, see Android Enterprise.
- Add Android Enterprise apps to Citrix Endpoint Management. For more information, see Adding Apps to Citrix Endpoint Management.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Requirements for per-app VPNs

To create a per-app VPN for AE, you need to do extra steps in addition to configuring the Managed configurations device policy. Also, you must verify that the following prerequisites are met:

- On-premises NetScaler Gateway
- The following applications are installed on the device:
  - Citrix SSO
  - Citrix Secure Hub

A general workflow to configure a per-app VPN for AE devices is as follows:

1. Configure a VPN profile as described in this article.
2. Configure Citrix ADC to accept traffic from the per-app VPN. For details, see Full VPN setup on NetScaler Gateway.

Limitations

The following are the limitations for per-app VPN in the Android Enterprise environment on Android 11+ devices because of package visibility restrictions introduced in Android 11:

- If an app that is part of the allowed/denied list is deployed to a device after the VPN session has started, the end user must restart the VPN session for the app to route its traffic through the VPN session.
- If a per-app VPN is used via an Always On VPN session, then after installing a new app on the device, the end user must restart the work profile or reboot the device for the app's traffic to be routed via the VPN session.

> **Note:**

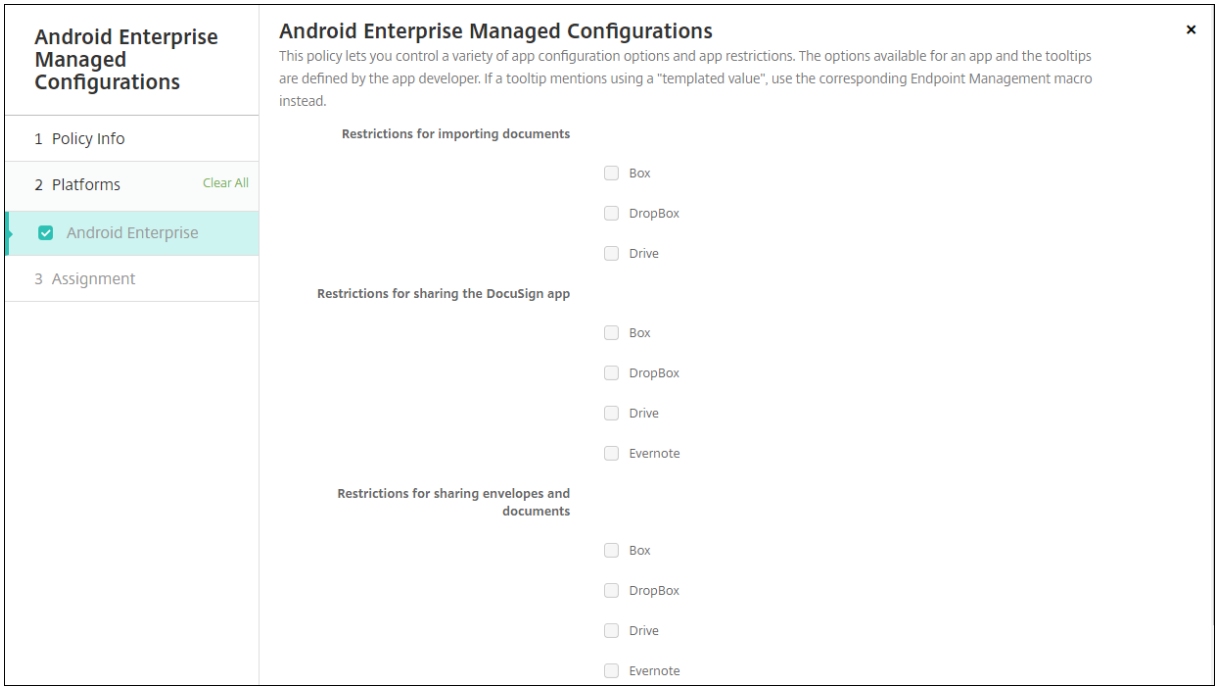
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> These limitations aren't applicable if you're using Citrix SSO for Android 23.8.1 or later versions. For more information, see Automatic restart of Always On VPN.

Android Enterprise settings

After you choose to add a Managed configurations device policy, a prompt to select an app appears. If there are no Android Enterprise apps added to Citrix Endpoint Management, you can't continue.

After you select an app, then configure the policy settings. The settings are specific to each app.

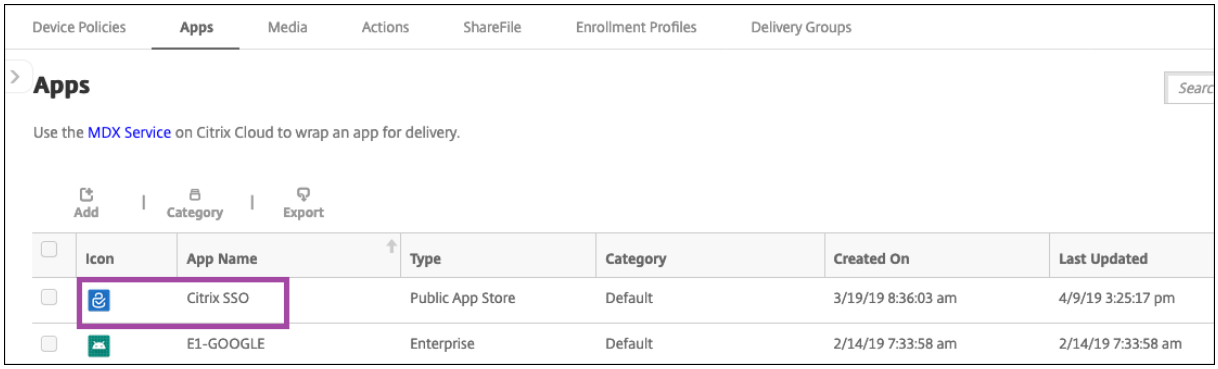


Configure VPN profiles for Android Enterprise

Make VPN profiles available to Android Enterprise devices using the Citrix SSO app with the Managed configurations device policy.

Start by adding Citrix SSO to the Citrix Endpoint Management console as a Google Play store app. See Add a public app store app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Watch this video to learn more:

Create an Android Enterprise managed configuration for Citrix SSO

Configure the Managed configurations device policy for Citrix SSO to create VPN profiles. Devices that have the Citrix SSO app installed and the policy deployed can access the VPN profiles you create.

Citrix Endpoint Management uses the user certificate in the device keystore if:

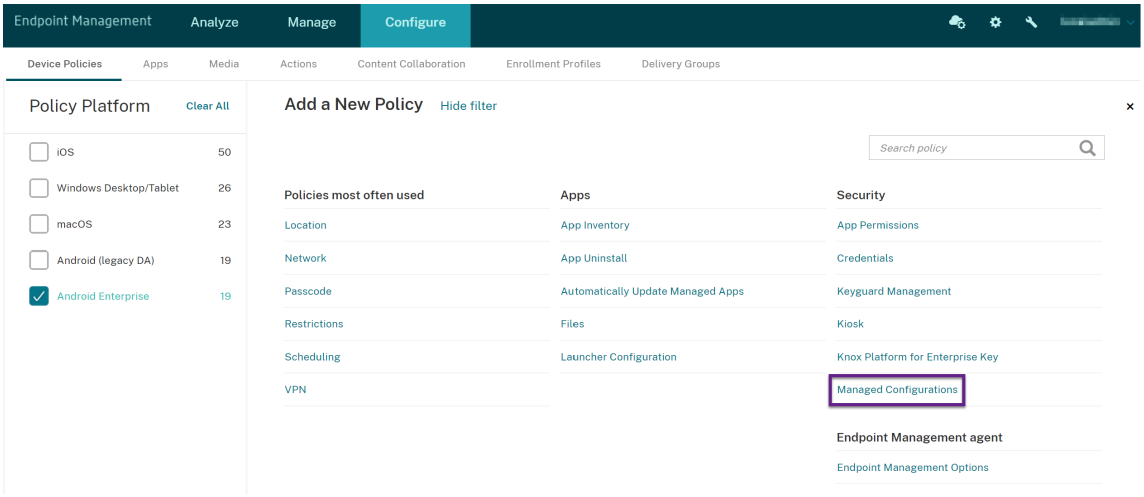
- NetScaler Gateway is configured for certificate-based authentication.
- **Deliver user certificate for authentication** is enabled in the Citrix Endpoint Management page **Settings > NetScaler Gateway**.

You need your NetScaler Gateway FQDN and port.

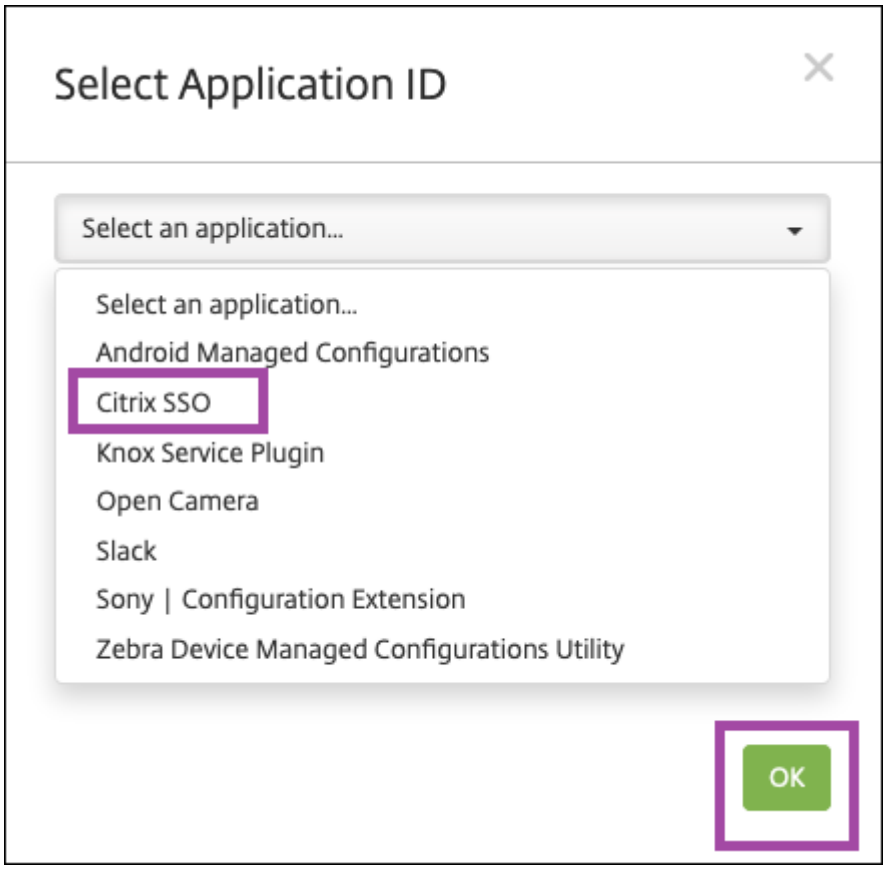
1. In the Citrix Endpoint Management console, click **Configure > Device Policies**. Click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Select **Android Enterprise**. Click **Managed configurations**.

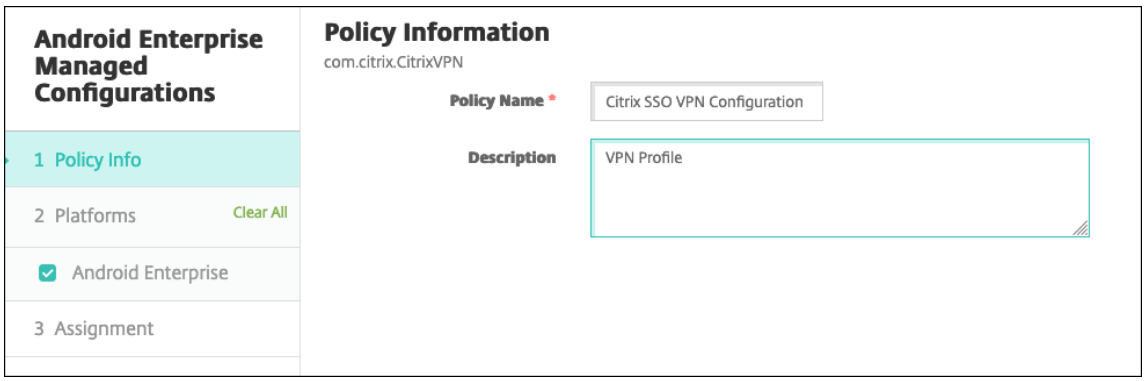


3. When the **Select Application ID** window appears, choose **Citrix SSO** from the list and click **OK**.



4. Type a name and description for your Citrix SSO VPN configuration. Click **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. Configure VPN profile parameters.

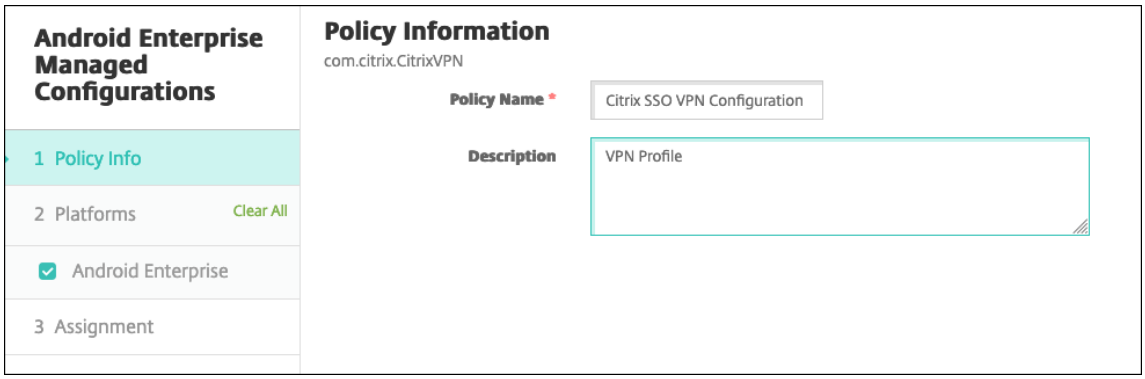
   - **VPN Profile Name:** Type a name for the VPN profile. If you're creating more than one VPN profile, use a unique name for each. If you don't provide a name, the address you put in the **Server Address** field is used as the VPN profile name.
   - **Server Address(*):** Type your NetScaler Gateway FQDN. If your NetScaler Gateway port isn't 443, also type your port. Use URL format. For example,`https://gateway.mycompany.com:8443`.
   - **Username (optional):** Provide the user name that end users use to authenticate to the NetScaler Gateway. You can use the Citrix Endpoint Management macro {user.username} for this field. (See Macros.) If you don't provide a user name, users are prompted to provide a user name when the connect to NetScaler Gateway.
   - **Password (optional):** Provide the password that end users use to authenticate to the NetScaler Gateway. If you don't provide a password, users are prompted to provide a password when the connect to NetScaler Gateway.
   - **Certificate Alias (optional):** Type a certificate alias. The certificate alias makes it easier for the app to access the certificate. When the same certificate alias is used with the Credentials device policy, the app retrieves the certificate and authenticates the VPN without any action by users.
   - **Gateway Certificate Pins (optional):** JSON object describing certificate pins used for NetScaler Gateway. Example value: `{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`. For more information, see NetScaler Gateway certificate pinning with Android Citrix SSO.
   - **Per-App VPN Type (optional):** If you're using a per-app VPN to restrict which apps use this VPN, you can configure this setting. If you select **Allow**, network traffic for the app package names listed in the **PerAppVPN app list** are routed through the VPN. The network traffic of all other apps is routed outside the VPN. If you select **Disallow**, network traffic for the app

© 1997–2025 Citrix Systems, Inc. All rights reserved.

package names listed in the **PerAppVPN app list** are routed outside the VPN. The network traffic of all other apps is routed through the VPN. Default is **Allow**.

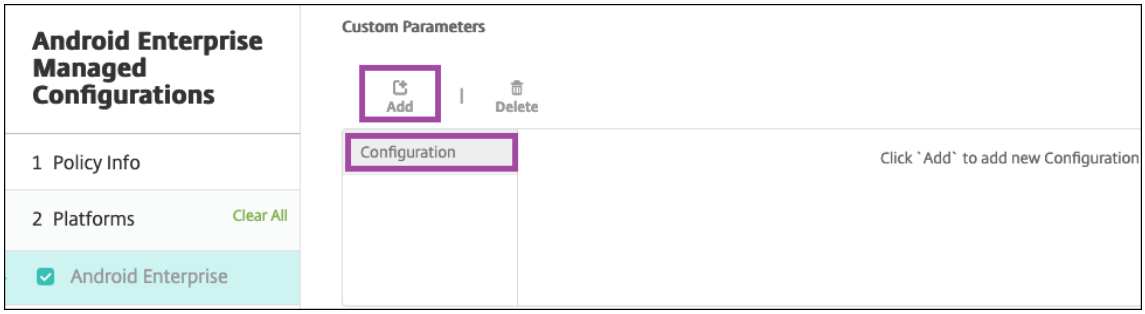
- **PerAppVPN app list:** A list of apps whose traffic is allowed or blocked on the VPN, depending on the value of **Per-App VPN Type**. List the app package names separated by commas or semicolons. App package names are case sensitive and must appear on this list exactly as they appear in the Google Play store. This list is optional. Keep this list empty for provisioning device-wide VPN.
- **Default VPN profile:** Type the name of the VPN profile to use when users tap the connect switch in the Citrix SSO app instead of a specific profile. If this field is left empty, the main profile is used for the connection. If only one profile is configured, it is marked as the default profile. For always-on VPN, this field must be set to the name of the VPN profile to be used for establishing an always-on VPN.
- **Always On VPN (optional):** This attribute indicates whether the VPN profile is configured as an Always On VPN profile. When set to **true**, it signifies that the VPN profile is an Always On VPN profile. The default value is **false**. This property can only be assigned to the main VPN profile. Enabling this property is essential for ensuring the reliable functioning of Always On VPN.
- **Disable User Profiles:** If this setting is On, users can't create their own VPNs on their devices. If this setting is Off, users can create their own VPNs on their devices. Default is Off.
- **Block Untrusted Servers:** This setting is Off during either of the following scenarios:
  - When you use a self-signed certificate for NetScaler Gateway
  - When the root certificate for the CA issuing the NetScaler Gateway certificate isn't in the system CA list.

  If this setting is On, the Android operating system validates the NetScaler Gateway certificate. If the validation fails, the connection isn't allowed. The default value is On.



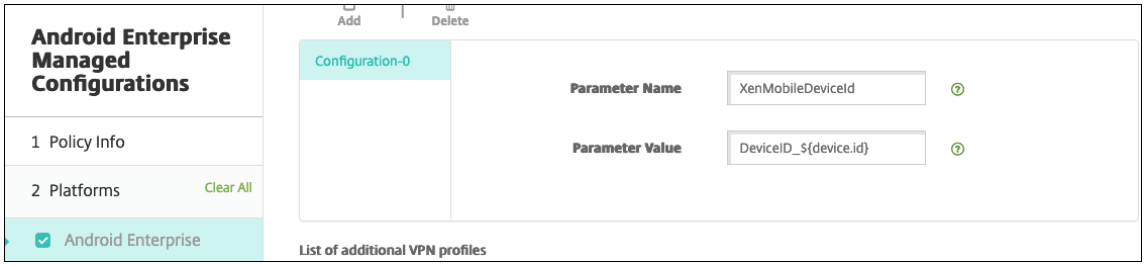
6. Optionally, create custom parameters. The custom parameters **XenMobileDeviceId** and **User-Agent** are supported. Select the current VPN configuration and click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



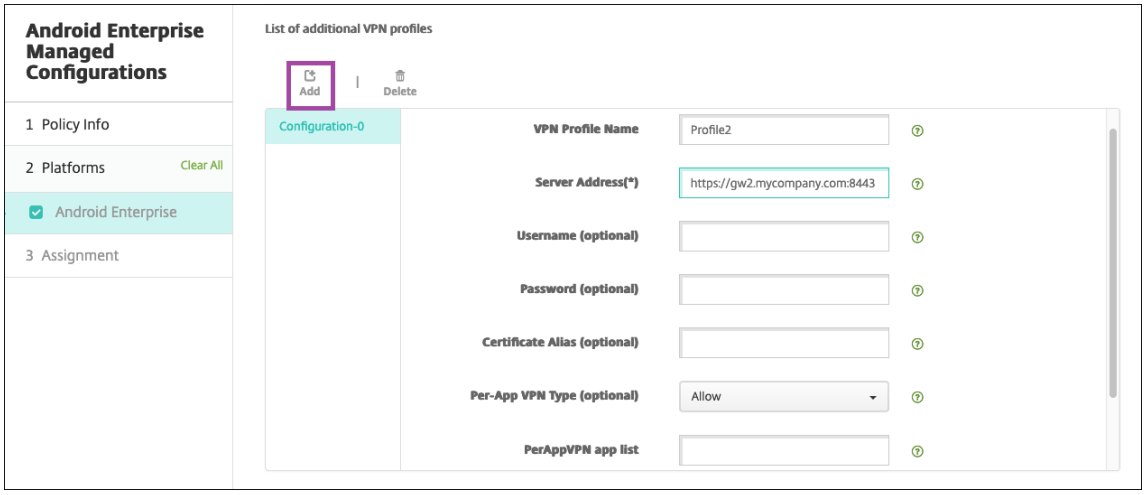
Parameter name	Description	Value
XenMobileDeviceId	This field is the device ID to use for Network Access Check based on device enrollment in Citrix Endpoint Management. If Citrix Endpoint Management enrolls and manages the device, the VPN connection is allowed. Otherwise, authentication is denied at the time of VPN establishment.	For Citrix Endpoint Management to determine the enrollment and management state of the devices, the value of XenMobileDeviceID set to `DeviceID_${ device.id }`.
UserAgent	This text appended to the User-Agent HTTP header for doing an extra check on NetScaler Gateway. The value of this text is appended to the User-Agent HTTP header by the Citrix SSO app while communicating with the NetScaler Gateway.	Type the text that you want to append to the User-Agent HTTP header. This text must conform to the HTTP User-Agent specifications.
EnableDebugLogging	Enable debug logging on the Citrix SSO app to help troubleshoot VPN connectivity issues in case of Always On VPN. You can enable it in any one of the managed VPN configurations. The debug logging takes effect when the managed configurations are processed.	**True**: Enables debug logging. Default value: **False**

© 1997–2025 Citrix Systems, Inc. All rights reserved.



To create another custom parameter, click **Add** again.

7. Optionally, create more VPN profile configurations. Click **Add** under the list of configurations. A new configuration appears in the list. Select the new configuration and repeat step 5 and, optionally, step 6.



8. When you've created all the VPN profiles you want, click **Next**.
9. Configure deployment rules for this managed configuration for Citrix SSO.
10. Click **Save**.

This managed configuration for Citrix SSO now appears in your list of configured device policies.

To enable always-on for the VPN profiles you configured, set the Citrix Endpoint Management options device policy.

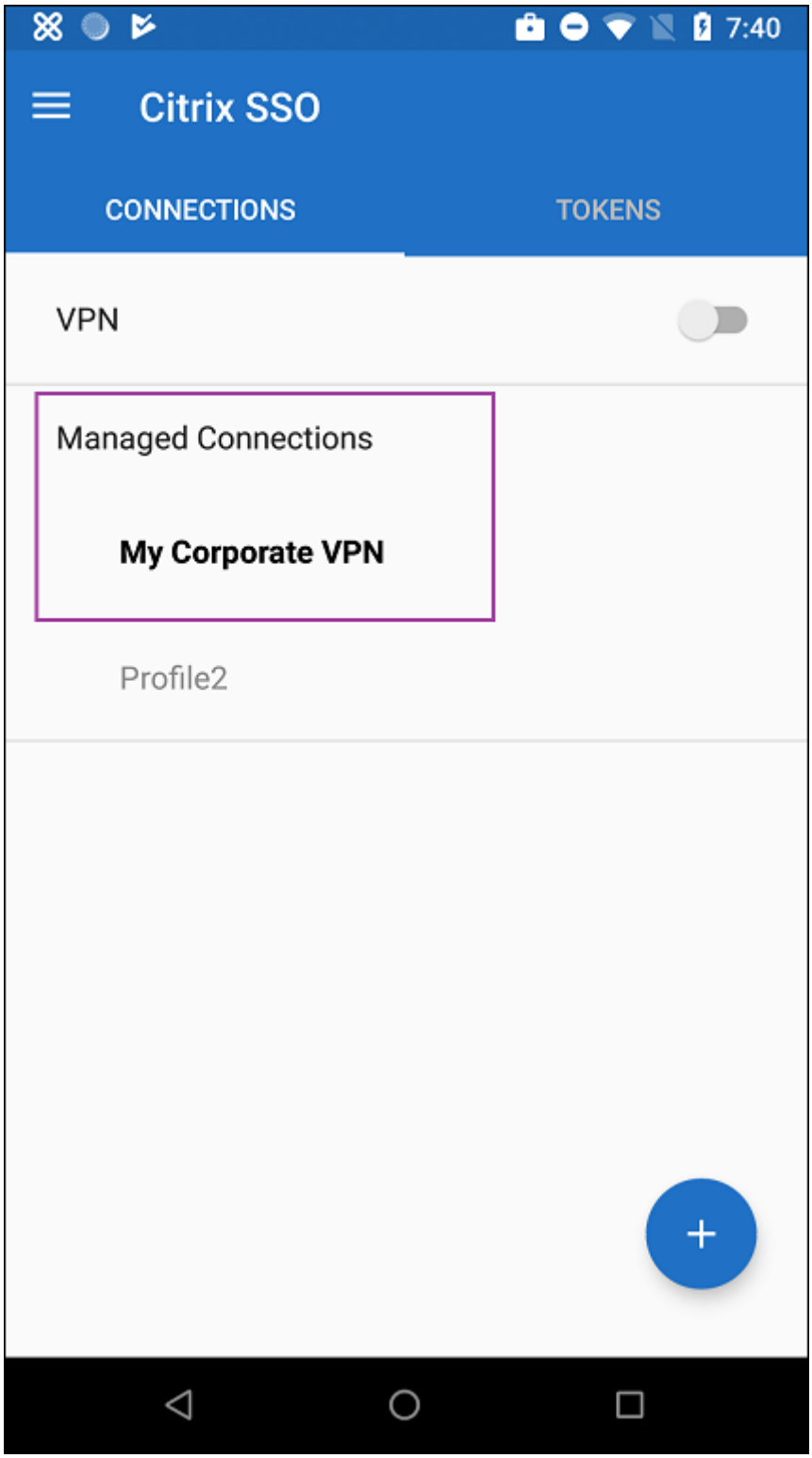
> **Note:**
>
> Citrix Secure Hub 19.5.5 or higher is required for always-on VPN for Android Enterprise.

Accessing VPN profiles from the device

To access the VPN profiles you created, Android Enterprise users install Citrix SSO from the managed Google Play store.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The VPN profile or profiles you configured appear in the **Managed Connections** area of the app. Users tap the VPN profile to connect using that VPN profile.



After users have authenticated and connected, a check mark appears next to the VPN profile. The key

© 1997–2025 Citrix Systems, Inc. All rights reserved.

icon indicates that the VPN is connected.

Manage Zebra Android devices using Zebra OEMConfig

Manage Zebra Android devices using the Zebra Technologies OEMConfig administrative tool. For information about the Zebra OEMConfig app, see the Zebra Technologies website.

Citrix Endpoint Management supports Zebra OEMConfig version 9.2 and higher. For information about system requirements for installing Zebra OEMConfig on devices, see OEMConfig Setup on the Zebra Technologies website.

We currently support the following Zebra devices:

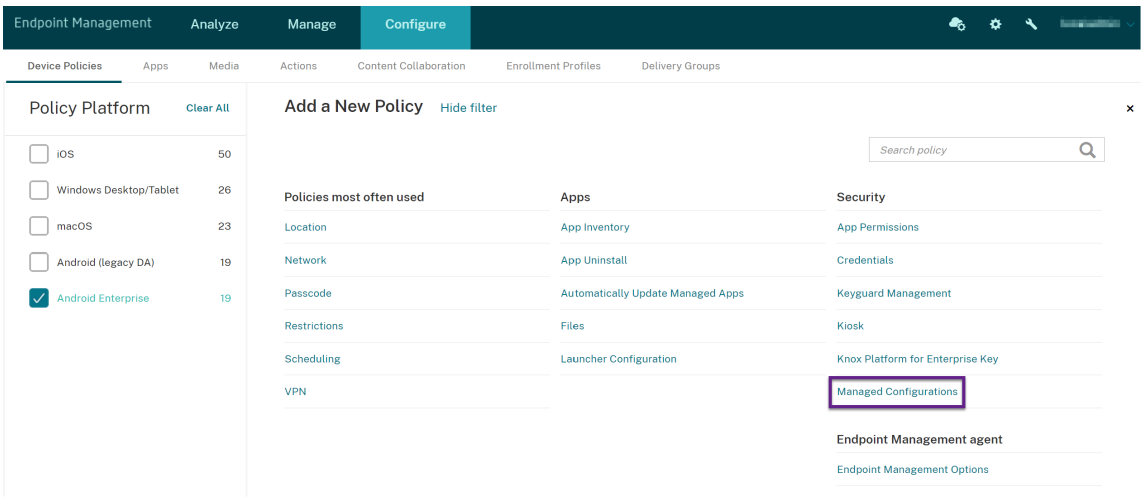
- EC50, EC55, ET56
- TC52x, TC52x-HC
- TC52ax, TC52ax-HC
- TC57x

To start: In the Citrix Endpoint Management console, add the Zebra OEMConfig app as a Google Play store app. See Add a public app store app.

Create an Android Enterprise managed configuration for the Zebra OEMConfig app

Configure the Managed configurations device policy for the Zebra OEMConfig app. The policy applies to Zebra devices that have the Zebra OEMConfig app installed and the policy deployed.

1. In the Citrix Endpoint Management console, click **Configure > Device Policies**. Click **Add**.
2. Select **Android Enterprise**. Click **Managed configurations**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. When the **Select Application ID** window appears, choose **ZebraOEMConfig powered by MX** from the list and click **OK**.
4. Type a name and description for your Zebra OEMConfig configuration. Click **Next**.
5. Type a name for the Zebra OEMConfig configuration.
6. Configure the available parameters. For example:
    - To disable the camera on the front of the device, select **Camera Configuration** and set **Use of Front Camera** to **Off**.
    - To change the devices time format, select **Clock Configuration** and set **Time Format** to **12** (12-hour) or **24** (24-hour).

For a list and descriptions of all available configurations, see Zebra Managed Configurations on the Zebra Technologies website.

1. Optionally, create more Zebra OEMConfig configurations. Click **Add** under the list of configurations. A new configuration appears in the list. Select the new configuration and configure the parameters.
2. When you've created all the Zebra OEMConfig configurations you want, click **Next**.
3. Configure deployment rules for this managed configuration for Zebra OEMConfig.
4. Click **Save**.

Manage Chrome Browser with predefined bookmarks

Here is an example of how to manage Chrome Browser with predefined bookmarks:

```
[

{
  "toplevel_name": "My managed bookmarks folder"  }

,

{
  "name": "Google", "url": "[google.com|http://google.com/]"  }

,

{
  "name": "Youtube", "url": "[youtube.com|http://youtube.com/]"  }

,
{

"nested_links": [
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
20
21 {
22   "name": "Chromium", "url": "[chromium.org|http://chromium.org/]"  }
23
24 ,
25
26 {
27   "name": "Chromium Developers", "url": "[dev.chromium.org|http://dev.
       chromium.org/]"  }
28
29 ],
30 "name": "Chrome links"
31  }
32
33 ]
```

Support managed configurations feedback (Technical Preview)

For more information on Support managed configurations feedback feature, see Support managed configurations feedback.

Managed domains device policy

September 6, 2025

You can define managed domains that apply to email and the Safari browser. Managed domains help you protect corporate data by controlling which apps can open documents downloaded from domains using Safari.

For iOS supervised devices, you specify:

- URLs or subdomains to control how users can open documents, attachments, and downloads from the browser.
- URLs from which users can save passwords in Safari.

For the steps on setting an iOS device to supervised mode, see Deploy devices using Apple Configurator 2.

When a user sends an email to a recipient whose domain isn't on the managed email domains list, the message is flagged on the user's device to warn them that they're sending a message to someone outside your corporate domain.

For items such as documents, attachments, or downloads: When a user opens an item by using Safari from a web domain that is on the managed web domains list, the appropriate corporate app opens

© 1997–2025 Citrix Systems, Inc. All rights reserved.

the item. If the item isn't from a web domain on the managed web domains list, the user can't open the item with a corporate app. They must use a personal, unmanaged app.

For supervised devices, even if you don't specify Safari password autofill domains: If the device is configured as an ephemeral multi-user, users can't save passwords. However, if the device isn't configured as an ephemeral multi-user, users can save all passwords.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

To specify domains:

Format	Description
`example.com`	Treat any path under `example.com` as managed, but not `site.example.com/`.
`foo.example.com`	Treat any path under `foo.example.com` as managed, but not `example.com/` or `bar.example.com/`.
`\*.example.com`	Treat any path under `foo.example.com` or `bar.example.com` as managed, but not `example.com/`.
`example.com/sub`	Treat `example.com/sub` and any path under it as managed, but not `example.com/`.
`foo.example.com/sub`	Treat any path under `foo.example.com/sub` as managed, but not `example.com`, `example.com/sub`, `foo.example.com/`, or `bar.example.com/sub`.
`\*.example.com/sub`	Treat any path under `foo.example.com/sub` or `bar.example.com/sub` as managed, but not `example.com` or `foo.example.com/`.

Rules:

- Leading "www."and trailing slashes in URLs are ignored when domains are compared.
- If an entry has a port number, only addresses that specify that port number are considered managed. Otherwise, only the standard ports are considered managed (port 80 for http and port 443 for https). For example, the pattern `*.example.com:8080` matches

© 1997–2025 Citrix Systems, Inc. All rights reserved.

`https://site.example.com:8080/page.html`, but not `https://site.example.com/page.html`, but the pattern `*.example.com` matches `https://site.example.com/page.html` and `https://site.example.com/page.html`, but not `https://site.example.com:8080/page.html`.

- Managed Safari web domain definitions are cumulative. Patterns defined by all managed Safari web domain payloads are used to match a URL request.

Settings:

- **Managed Domains**
  - **Unmarked Email Domains:** For each email domain you want to include in the list, click **Add** and then do the following:
    - **Managed Email Domain:** Type the email domain.
    - Click **Save** to save the email domain or click **Cancel** to not save the email domain.
  - **Managed Safari Web Domains:** For each web domain you want to include in the list, click **Add** and then do the following:
    - **Managed Web Domain:** Type the web domain.
    - Click **Save** to save the web domain or click **Cancel** to not save the web domain.
  - **Safari Password AutoFill Domains:** For each autofill domain you want to include in the list, click **Add** and then do the following:
    - **Safari Password AutoFill Domain:** Type the autofill domain.
    - Click **Save** to save the autofill domain or click **Cancel** to not save the autofill domain.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

Maximum resident users device policy

March 7, 2024

The Maximum resident users device policy is for shared devices running iOS (iPadOS). For more information about Shared iPads, see Integrate with Apple Education features.

This policy must deploy when the iPad is in the "awaiting configuration"phase during the Setup Assistant. Apple doesn't allow this policy to deploy after Shared iPads enroll.

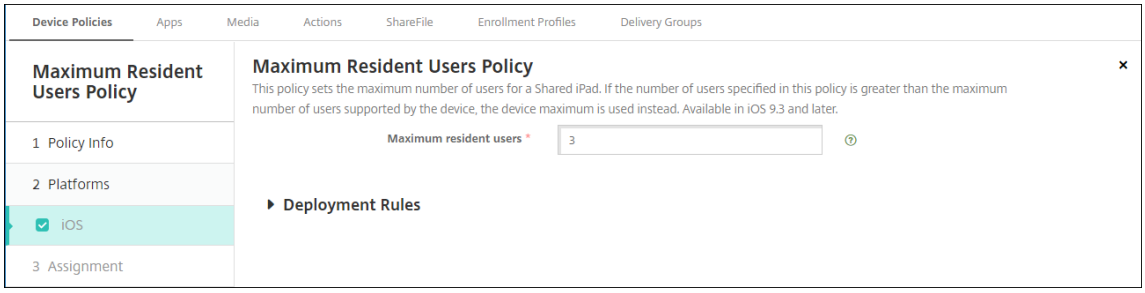
© 1997–2025 Citrix Systems, Inc. All rights reserved.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Maximum Resident Users:** The maximum number of users for a Shared iPad. If the number of users specified in this policy is greater than the maximum number of users supported by the device: Citrix Endpoint Management uses the device maximum instead. Default is **5** users.

  Apple recommends that you keep the Maximum resident users value as low as possible. A low value maximizes the amount of iPad storage for each user. Also, a low value minimizes communication with iCloud and provides a faster sign-in experience. For information about how Apple handles shared storage on an iPad, see https://developer.apple.com/education/shared-ipad/.



MDM options device policy

September 6, 2025

The MDM options device policy manages Find My Phone/iPad Activation Lock on supervised iOS devices. For the steps on setting an iOS device to supervised mode, see Deploy devices using Apple Configurator 2.

Activation Lock is a feature of Find My iPhone/iPad that prevents reactivation of a lost or stolen supervised device. Activation Lock requires the user Apple ID and password before anyone can turn off Find My iPhone/iPad, erase the device, or reactivate the device. For the devices that your organization owns, bypassing an Activation Lock is necessary to, for example, reset or reallocate devices.

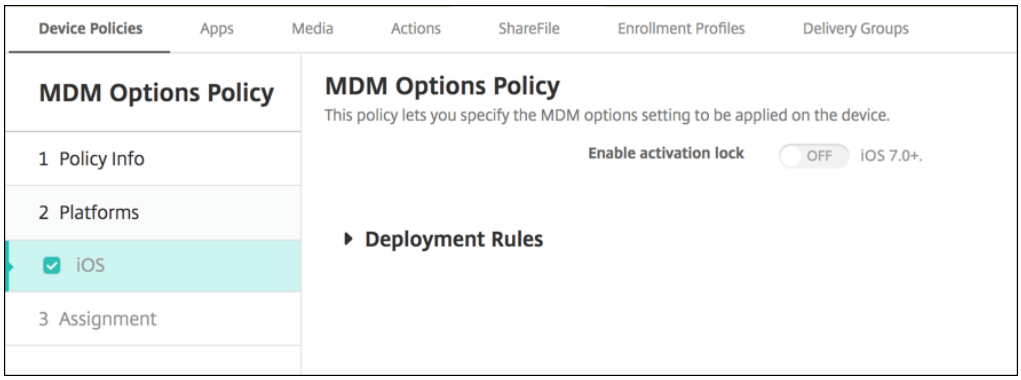
To enable Activation Lock, you configure and deploy the Citrix Endpoint Management MDM Options device policy. You can then manage a device from the Citrix Endpoint Management console without the Apple credentials of the user. To bypass the Apple credential requirement of an Activation Lock, issue the Activation Lock Bypass security action from the Citrix Endpoint Management console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For example, if the user returns a lost phone or to set up the device before or after a Full Wipe: When the phone prompts for the Apple App Store account credential, you can bypass that step by issuing the Activation Lock Bypass security action from the Citrix Endpoint Management console.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **Enable Activation Lock:** Select whether to enable Activation Lock on the devices to which you deploy this policy. The default is **Off**.

After you enable Activation Lock by deploying the MDM options device policy: The Security action **Activation Lock Bypass** appears when you select those devices on the **Manage > Devices** page and click **Security**. An Activation Lock Bypass allows you to remove the Activation Lock from supervised devices before device activation without knowing the Apple ID and password of the device users. You can send an Activation Lock Bypass to a device before or after a Full Wipe. For more information, see Bypass an iOS activation lock.

Network device policy

September 6, 2025

The network device policy lets you manage how users connect their devices to Wi-Fi networks by defining the following items:

- Network names and types
- Authentication and security policies
- Proxy server use
- Other Wi-Fi related details

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Prerequisites

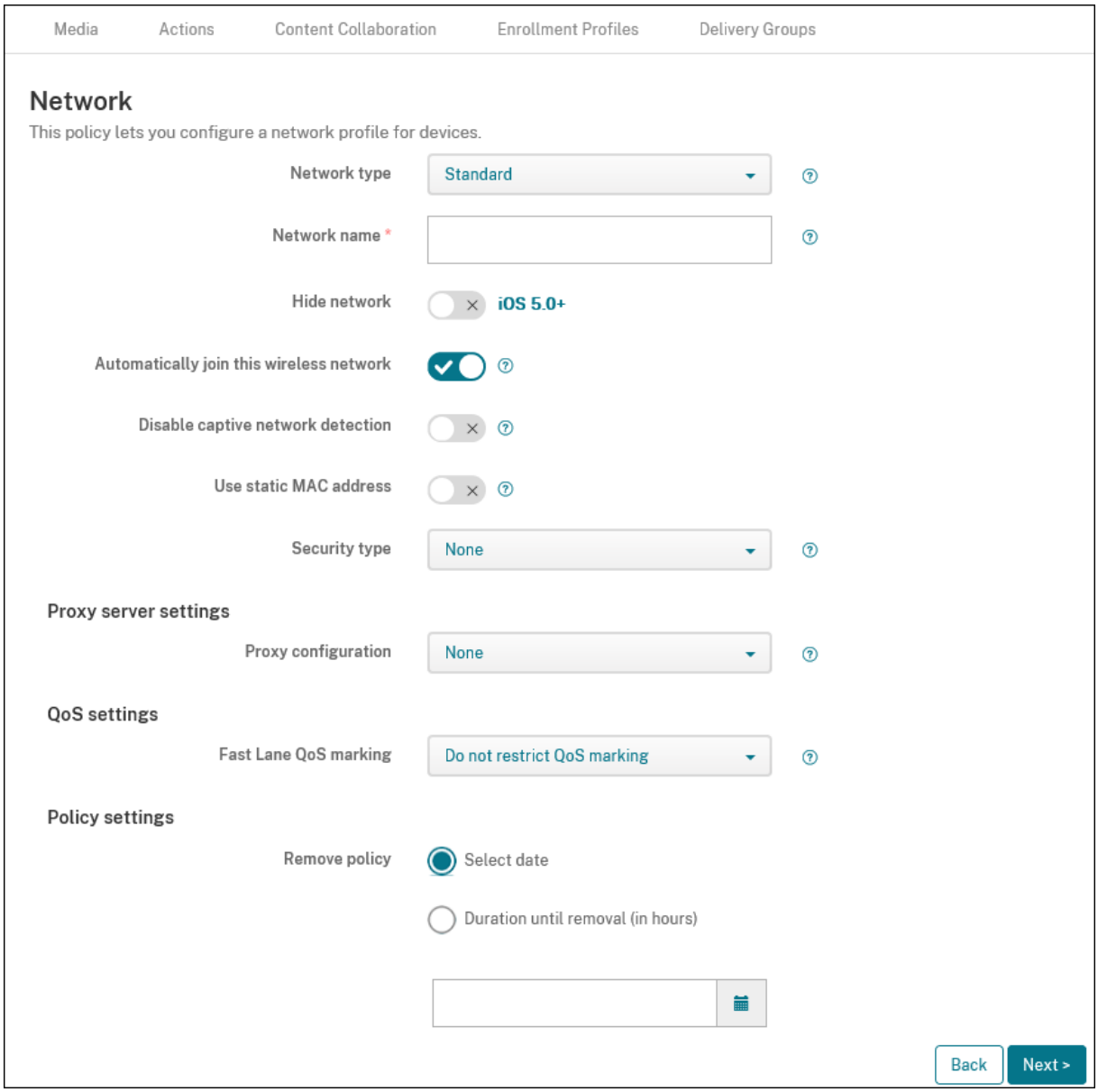
Before you create a policy, complete the following:

- Create any delivery groups that you plan to use.
- Know the network name and type.
- Know any authentication or security types that you plan to use.
- Know any proxy server information that you might need.
- Install any necessary CA certificates.
- Have any necessary shared keys.
- Create the PKI entity for certificate-based authentication.
- Configure credential providers.

For more information, see Authentication and its subarticles.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS settings



- **Network type:** In the list, choose **Standard**, **Legacy Hotspot**, or **Hotspot 2.0** to set the network type you plan to use.
- **Network name:** Type the SSID that is seen in the list of available networks for the device. Does not apply to **Hotspot 2.0**.
- **Hide network:** Choose whether the network is hidden.
- **Automatically join this wireless network:** Choose whether a device joins the network automatically. If a device is connected to another network, it doesn't join this network. The user must disconnect from the previous network before the device automatically connects. The de-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

fault is **On**.

- **Disable captive network detection:** The captive network assistant helps users access subscription or Wi-Fi Hotspot networks. You typically find these networks in coffee shops, hotels, and other public locations. If **On**, devices can still connect to captive networks, but the user must open a browser and log in manually. The default is **Off**.
- **Use static MAC address:** MAC addresses are unique identifiers that a device transmits within a network. To increase privacy, iOS and iPadOS devices can use a different MAC address each time they connect to a network. If **On**, the device always uses the same MAC address when connecting to this network. If **Off**, the device uses a different MAC address every time it connects to this network. The default is **Off**.
- **Security type:** In the list, choose the security type you plan to use. Does not apply to **Hotspot 2.0**.
  - None - Requires no further configuration.
  - WEP
  - WPA/WPA2/WPA3 Personal
  - Any (Personal)
  - WEP Enterprise
  - WPA/WPA2/WPA3 Enterprise: For the latest release of Windows 10, configure the Simple Certificate Enrollment Protocol (SCEP) to use WPA-2 Enterprise. Citrix Endpoint Management can then send the certificate to the devices to authenticate to the Wi-Fi server. To configure SCEP, go to the Distribution page of **Settings > Credential Providers**. For more information, see Credential providers.
  - Any (Enterprise)

The following sections list the options that you configure for each of the preceding connection types.

- **Proxy server settings**
  - **Proxy configuration:** In the list, choose **None**, **Manual**, or **Automatic** to set how the VPN connection routes through a proxy server and then configure any additional options. The default is **None**, which requires no further configuration.
  - If you choose **Manual**, configure these settings:
    - **Host name or IP address:** Type the host name or IP address of the proxy server.
    - **Port:** Type the proxy server port number.
    - **User name:** Type an optional user name to authenticate to the proxy server.
    - **Password:** Type an optional password to authenticate to the proxy server.
  - If you choose **Automatic**, configure these settings:
    - **Server URL:** Type the URL of the PAC file that defines the proxy configuration.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

        * **Allow direct connection if PAC is unreachable:** Choose whether to allow users to connect directly to the destination if the PAC file is unreachable. The default is **On**.

- **Fast Lane QoS marking:** If you don't restrict QoS marking for a Wi-Fi network that supports Cisco Fast Lane QoS, all apps are allowed to use L2 and L3 marking. If you restrict QoS marking, specify the apps that can use L2 and L3 marking.
  - **Enable QoS marking:** If you restrict QoS marking, use this setting to disable it completely or only mark certain apps. If **Off**, you disable QoS marking entirely. If **On**, configure a list of apps that can use QoS marking. The default is **On**.
  - **Allow Apple audio/video calling:** Choose whether audio and video calling apps can use QoS marking. If **Off**, the quality of video and audio calls can suffer.
  - **Allow specific apps:** Add an app package ID to this list to allow the app to use QoS marking.
- **Hotspot 2.0 settings**
  - **Displayed operator name:** The friendly name broadcast by the Hotspot device. Users see this name in their list of available Wi-Fi networks.
  - **Domain name:** The domain name used for Hotspot 2.0 negotiation.
  - **Allow connecting to roaming partner networks:** If **On**, devices roaming off their home network can connect to partner networks.
  - **Roaming Consortium Organization Identifiers (OI):** Add a list of organization identifiers that the device can access. A Roaming Consortium OI belongs to an organization with shared authentication methods. If the Hotspot you configure isn't available, the device connects to a Roaming Consortium OI listed here.
  - **Network Access Identifier (NAI) realm names:** Configure a list of realm names used to identify users to a roaming network. A NAI transmits in the form `user@realm`.
  - **Mobile Country Codes (MCCs) and Mobile Network Configurations (MNCs):** A Mobile Country Code consists of three digits that identify the country of a network. The Mobile Network Code consists of 2 or 3 unique digits. When used together, the MCC/MNC uniquely identifies a mobile network operator or carrier.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    * **Select date:** Click the calendar to select the specific date for removal.
    * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field. Not available for iOS.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

WPA, WPA Personal, Any (Personal) settings for iOS

Password: Type an optional password. If you leave this field blank, users might be prompted for their passwords when they log on.

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, WPA3 Enterprise, Any (Enterprise) settings for iOS

When you choose any of these security types, **EAP** settings appear after **QoS settings**.

> **Important:**
>
> If you select the **WPA2 Enterprise** security type, you must allow at least one EAP protocol.

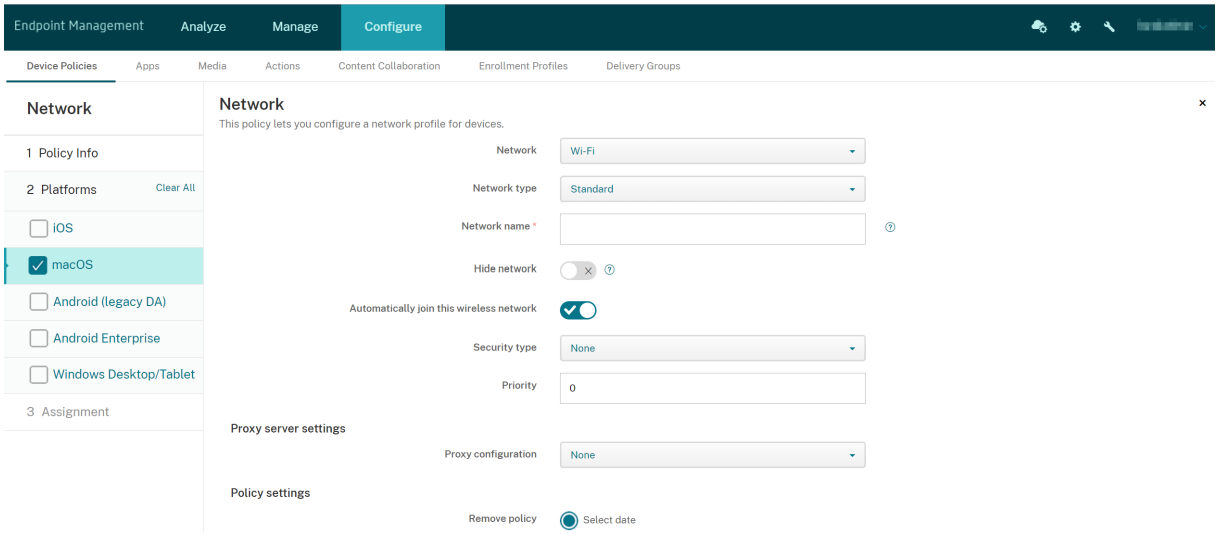
- **Allowed EAP protocols:** Enable the EAP types that you want to support and then configure the associated settings. The default is **Off** for each of the available EAP types.
- **Inner authentication (TTLS):** *Required only when you enable TTLS*. In the list, choose the inner authentication method to use. Options are: **PAP**, **CHAP**, **MSCHAP**, or **MSCHAPv2**. The default is **MSCHAPv2**.
- **EAP-FAST with PAC:** Choose whether to use protected access credentials (PACs).
  - If you choose **Use PAC**, choose whether to use a provisioning PAC.
    - If you choose **Provisioning PAC**, choose whether to allow an anonymous TLS handshake between the end-user client and Citrix Endpoint Management.
      - **Provisioning PAC anonymously**
- **Authentication:**
  - **User name:** Type a user name.
  - **Per-connection password:** Choose whether to require a password each time that users log on.
  - **Password:** Type an optional password. If you leave this field blank, users might be prompted for their passwords when they log on.
  - **Identity credential (keystore or PKI credential):** In the list, choose the type of identity credential. The default is **None**.
  - **Outer identity:** *Required only when you enable* **PEAP**, **TTLS**, *or* **EAP-FAST**. Type the externally visible user name. You can increase security by typing a generic term such as "anonymous"so that the user name isn't visible.
  - **Require a TLS certificate:** Choose whether to require a TLS certificate.
- **Trust**
  - **Trusted certificates:** To add a trusted certificate, click **Add** and, for each certificate you want to add, do the following:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    - **Application:** In the list, choose the application you want to add.
    - Click **Save** to save the certificate or click **Cancel**.
  - **Trusted server certificate names:** To add trusted server certificate common names, click **Add** and, for each name you want to add, do the following:
    - **Certificate:** Type the name of the server certificate. You can use wildcards to specify the name, such as wpa.*.example.com.
    - Click **Save** to save the certificate name or click **Cancel**.

- **Allow trust exceptions:** Choose whether the certificate trust dialog appears on users devices when a certificate is untrusted. The default is **On**.

macOS settings



- **Network:** In the list, choose the network option you plan to use. The default is **Wi-Fi**.
  - Wi-Fi
  - Global Ethernet
  - First Active Ethernet
  - Second Active Ethernet
  - Third Active Ethernet
  - First Ethernet
  - Second Ethernet
  - Third Ethernet
- **Network type:** In the list, choose **Standard**, **Legacy Hotspot**, or **Hotspot 2.0** to set the network type you plan to use.
- **Network name:** Type the SSID that is seen in the list of available networks for the device. Does not apply to **Hotspot 2.0**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Hide network:** Choose whether the network is hidden.
- **Automatically join this wireless network:** Choose whether the network is joined automatically. If a device is already connected to another network, it doesn't join this network. The user must disconnect from the previous network before the device automatically connects. The default is **On**.
- **Security type:** In the list, choose the security type you plan to use. Does not apply to **Hotspot 2.0**.
  - None - Requires no further configuration.
  - WEP
  - WPA/WPA2 Personal
  - Any (Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Any (Enterprise)

  The following sections list the options that you configure for each of the preceding connection types.
- **Priority:** For multiple networks, type a number to define the priority of the network connection. The device connects to the network with the lowest priority number first. Negative numbers are acceptable. The default is **0**.
- **Proxy server settings**
  - **Proxy configuration:** In the list, choose **None**, **Manual**, or **Automatic** to set how the VPN connection routes through a proxy server and then configure any additional options. The default is **None**, which requires no further configuration.
  - If you choose **Manual**, configure these settings:
    - **Host name or IP address:** Type the host name or IP address of the proxy server.
    - **Port:** Type the proxy server port number.
    - **User name:** Type an optional user name to authenticate to the proxy server.
    - **Password:** Type an optional password to authenticate to the proxy server.
  - If you choose **Automatic**, configure these settings:
    - **Server URL:** Type the URL of the PAC file that defines the proxy configuration.
    - **Allow direct connection if PAC is unreachable:** Choose whether to allow users to connect directly to the destination if the PAC file is unreachable. The default is **On**.
- **Hotspot 2.0 settings**
  - **Displayed operator name:** The friendly name broadcast by the Hotspot device. Users see this name in their list of available Wi-Fi networks.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Domain name:** The domain name used for Hotspot 2.0 negotiation.
  - **Allow connecting to roaming partner networks:** If **On**, devices roaming off their home network can connect to partner networks.
  - **Roaming Consortium Organization Identifiers (OI):** Add a list of organization identifiers that the device can access. A Roaming Consortium OI belongs to an organization with shared authentication methods. If the Hotspot you configure isn't available, the device connects to a Roaming Consortium OI listed here.
  - **Network Access Identifier (NAI) realm names:** Configure a list of realm names used to identify users to a roaming network. A NAI transmits in the form `user@realm`.
  - **Mobile Country Codes (MCCs) and Mobile Network Configurations (MNCs):** A Mobile Country Code consists of three digits that identify the country of a network. The Mobile Network Code consists of 2 or 3 unique digits. When used together, the MCC/MNC uniquely identifies a mobile network operator or carrier.

- **Policy settings**

  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

WPA, WPA Personal, WPA 2 Personal, Any (Personal) settings for macOS

- **Password:** Type an optional password. If you leave this field blank, users might be prompted for their passwords when they log on.

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise) settings for macOS

- **Connection mode:** If **On**, choose the connection mode to use when the user joins the network. The default is **Off**.

  - **System:** If marked, the device uses the system credentials to authenticate the user. The default is cleared.
  - **Login window:** If marked, the device uses the same credentials entered at the login window to authenticate the user. The default is cleared.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

When you choose any of these security types, **EAP** settings appear after **QoS settings**.

> **Important:**
>
> If you select the **WPA2 Enterprise** security type, you must allow at least one EAP protocol.

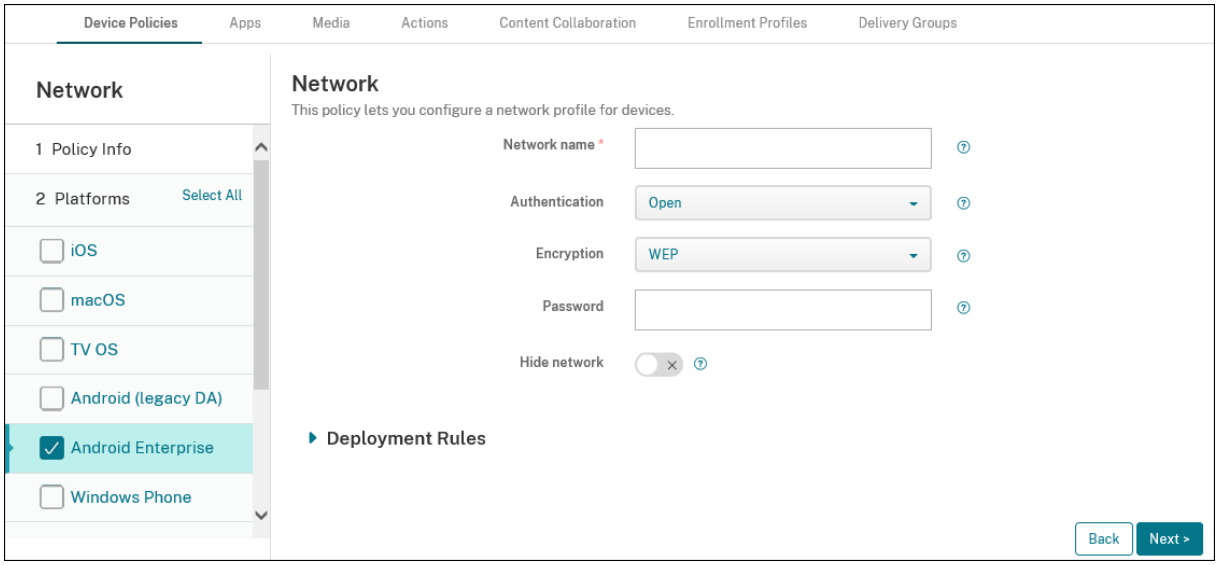
- **Allowed EAP protocols:** Enable the EAP types that you want to support and then configure the associated settings. The default is **Off** for each of the available EAP types.
- **Inner authentication (TTLS):** *Required only when you enable TTLS*. In the list, choose the inner authentication method to use. Options are: **PAP**, **CHAP**, **MSCHAP**, or **MSCHAPv2**. The default is **MSCHAPv2**.
- **EAP-FAST with PAC:** Choose whether to use protected access credentials (PACs).
  - If you select **Use PAC**, choose whether to use a provisioning PAC.
    - If you choose **Provisioning PAC**, choose whether to allow an anonymous TLS handshake between the end-user client and Citrix Endpoint Management.
      - **Provisioning PAC anonymously**
- **Authentication:**
  - **Use Active Directory authentication:** Choose whether to enable Active Directory authentication. Available for macOS 10.7 and later. To make this option available, complete the following:
    - Set **PEAP** as the EAP protocol.
    - Set the profile scope to **System**. You can use this setting option only when you apply the policy to the entire system.
  - **User name:** Type a user name.
  - **Per-connection password:** Choose whether to require a password each time users log on.
  - **Password:** Type an optional password. If you leave this field blank, users might be prompted for their passwords when they log on.
  - **Identity credential (keystore or PKI credential):** In the list, choose the type of identity credential. The default is **None**.
  - **Outer identity:** *Required only when you enable* **PEAP**, **TTLS**, *or* **EAP-FAST**. Type the externally visible user name. You can increase security by typing a generic term like "anonymous"so that the user name isn't visible.
  - **Require a TLS certificate:** Choose whether to require a TLS certificate.
- **Trust**
  - **Trusted certificates:** To add a trusted certificate, click **Add** and, for each certificate you want to add, do the following:
    - **Application:** In the list, choose the application you want to add.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    - Click **Save** to save the certificate or click **Cancel**.
  - **Trusted server certificate names:** To add trusted server certificate common names, click **Add** and, for each name you want to add, do the following:
    - **Certificate:** Type the name of the server certificate that you want to add. You can use wildcards to specify the name, such as wpa.*.example.com.
    - Click **Save** to save the certificate name or click **Cancel**.

- **Allow trust exceptions:** Choose whether the certificate trust dialog appears on user devices when a certificate is untrusted. The default is **On**.

Android Enterprise settings



- **Network name:** Type the SSID that is in the list of available networks on the user device.
- **Authentication:** In the list, choose the type of security to use with the Wi-Fi connection.
  - Open
  - Shared
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

The following sections list the options that you configure for each of the preceding connection types. The default is **Open**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Open, Shared settings for Android Enterprise

- **Encryption:** In the list, choose either **Disabled** or **WEP**. The default is **WEP**.
- **Password:** Type an optional password.
- **Hide network:** Choose whether the network is hidden.

WPA, WPA-PSK, WPA2, WPA2-PSK settings for Android Enterprise

- **Encryption:** In the list, choose either **TKIP** or **AES**. The default is **TKIP**.
- **Password:** Type an optional password.
- **Hide network:** Choose whether the network is hidden.

802.1x settings for Android Enterprise

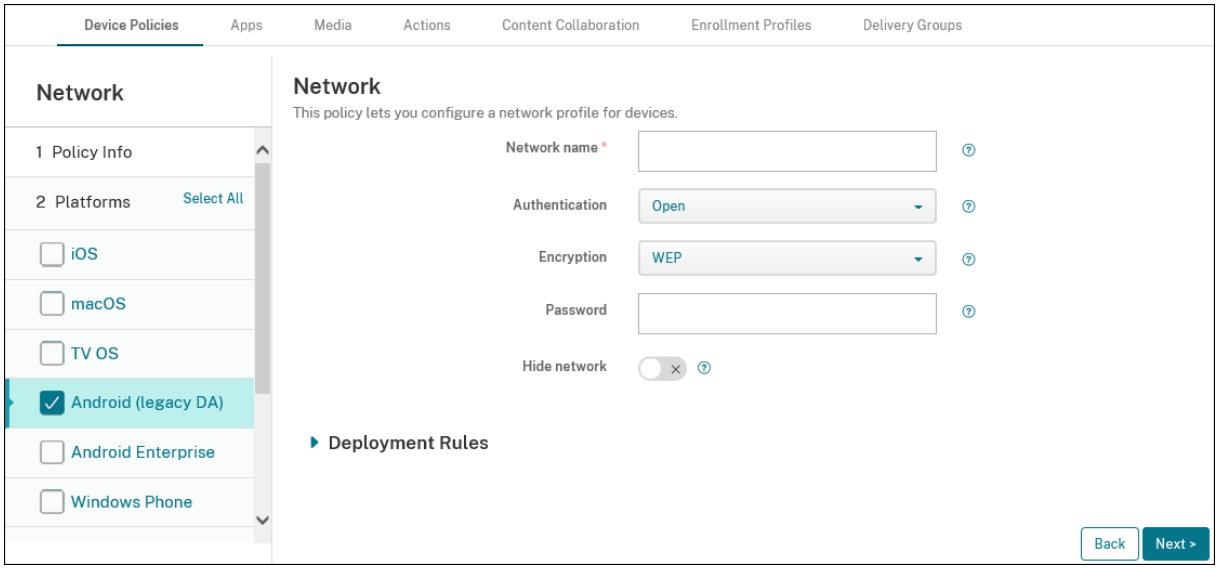
- **EAP Type:** In the list, choose **PEAP**, **TLS**, or **TTLS**. The default is **PEAP**.
- **Password:** Type an optional password.
- **Authentication phase 2:** In the list, choose **None**, **PAP**, **MSCHAP**, **MSCHAPPv2**, or **GTC**. The default is **PAP**.
- **Identity:** Type the optional user name and domain.
- **Anonymous:** Type the optional, externally visible user name. You can increase security by typing a generic term like "anonymous"so that the user name isn't visible.
- **CA certificate:** In the list, choose the certificate to use.
- **Domain:** Type the required domain name. For more information, see Domain.

  > **Note:**
  >
  > When you configure the Wi-Fi policy on devices running on Android 13 or later, the **CA certificate** and **Domain** fields must be mandatorily updated. If they aren't updated, then the configuration fails.

- **Identity credential:** In the list, choose the identity credential to use. The default is **None**.
- **Hide network:** Choose whether the network is hidden.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Android (legacy DA) settings



- **Network name:** Type the SSID that is in the list of available networks on the user device.
- **Authentication:** In the list, choose the type of security to use with the Wi-Fi connection.
  - Open
  - Shared (Android Enterprise only)
  - WPA (Android Enterprise only)
  - WPA-PSK (Android Enterprise only)
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

The following sections list the options that you configure for each of the preceding connection types.

Open, Shared settings for Android

- **Encryption:** In the list, choose either **Disabled** or **WEP**. The default is **WEP**.
- **Password:** Type an optional password.
- **Hide network:** Choose whether the network is hidden.

WPA, WPA-PSK, WPA2, WPA2-PSK settings for Android

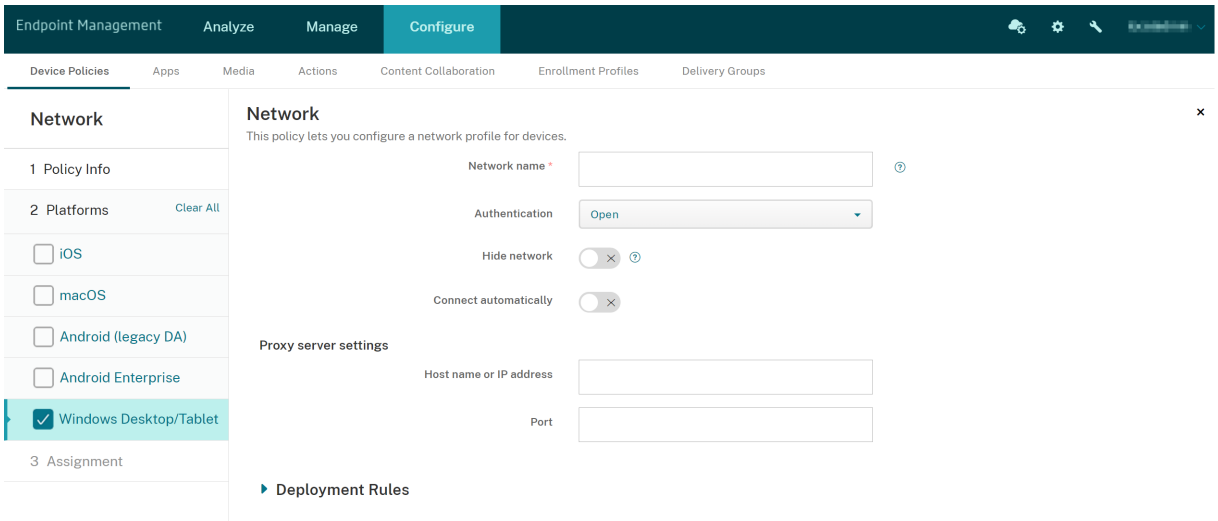
- **Encryption:** In the list, choose either **TKIP** or **AES**. The default is **TKIP**.
- **Password:** Type an optional password.
- **Hide network:** Choose whether the network is hidden.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

802.1x settings for Android

- **EAP type:** In the list, choose **PEAP**, **TLS**, or **TTLS**. The default is **PEAP**.
- **Password:** Type an optional password.
- **Authentication phase 2:** In the list, choose **None**, **PAP**, **MSCHAP**, **MSCHAPPv2**, or **GTC**. The default is **PAP**.
- **Identity:** Type the optional user name and domain.
- **Anonymous:** Type the optional, externally visible user name. You can increase security by typing a generic term like "anonymous"so that the user name isn't visible.
- **CA certificate:** In the list, choose the certificate to use.
- **Identity credential:** In the list, choose the identity credential to use. The default is **None**.
- **Hide network:** Choose whether the network is hidden.

Windows Desktop/Tablet settings



- **Network name:** The SSID seen in the list of available networks.
- **Authentication:** Click the type of security in the drop-down list that you want to use with the Wi-Fi connection.
  - Open
  - WPA Personal
  - WPA-2 Personal
  - WPA Enterprise
  - WPA-2 Enterprise: For the latest release of Windows 10, configure SCEP to use WPA-2 Enterprise. SCEP configuration enables Citrix Endpoint Management to send the certificate to devices to authenticate to the Wi-Fi server. To configure SCEP, go to **Distribution** page of **Settings > Credential Providers**. For more information, see Credential providers.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The following sections list the options that you configure for each of the preceding connection types.

Open settings for Windows 10 and Windows 11

- **Hide network:** Choose whether the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.

WPA Personal, WPA-2 Personal settings for Windows 10 and Windows 11

- **Encryption:** In the list, choose either **AES** or **TKIP** to set the type of encryption. The default is **AES**.
- **Shared key:** Provide the encryption key for the method that you selected.
- **Hide network:** Choose whether the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.

WPA-2 Enterprise settings for Windows 10 and Windows 11

- **Encryption:** In the list, choose either **AES** or **TKIP** to set the type of encryption. The default is **AES**.
- **EAP Type:** in the list, choose either **PEAP-MSCHAPv2** or **TLS** to set the EAP type. The default is **PEAP-MSCHAPv2**.
- **Hide network:** Choose whether the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.
- **Enable SCEP?:** Choose whether to push the certificate to user devices by using SCEP.
- **Credential provider for SCEP:** In the list, choose the SCEP credential provider. The default is **None**.

Network usage device policy

March 7, 2024

You can set network usage rules to specify how iOS devices use networks, such as cellular data networks. The rules apply to managed apps and specified SIMs. Managed apps are apps that you deploy to users'devices through Citrix Endpoint Management. They don't include apps that users have downloaded directly to their devices if they aren't being deployed through Citrix Endpoint Management. They also don't include apps already installed on the devices when the devices were enrolled

© 1997–2025 Citrix Systems, Inc. All rights reserved.

in Citrix Endpoint Management. This policy applies to SIMs for iOS 13 devices. You can configure app rules, SIM rules, or both. SIM rules apply to all managed apps on that device.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Application Rules**
  - **Allow roaming cellular data:** Select whether the specified apps can use a cellular data connection while roaming. The default is **Off**.
  - **Allow cellular data:** Select whether the specified apps can use a cellular data connection. The default is **Off**.
  - **App Identifier Matches:** For each app you want to add to the list, click **Add**, and then configure the following:
    - **App Identifier:** Type an app identifier.
  - Click **Save** to save the app to the list or **Cancel** to not save the app to the list.
- **SIM Rules**
  - **SIM Wi-Fi assist policy:** Enabling **Switch from poor Wi-Fi** makes the Wi-Fi assist policy switch from poor Wi-Fi to cellular connections more aggressively. This setting can increase cellular data use and impact battery life.
  - **SIM ICCIDs:** For each SIM you want to add to the list, click **Add**, and then configure the following:
    - **ICCID:** Type the 19- or 20-digit number for the SIM card to add.

Office device policy

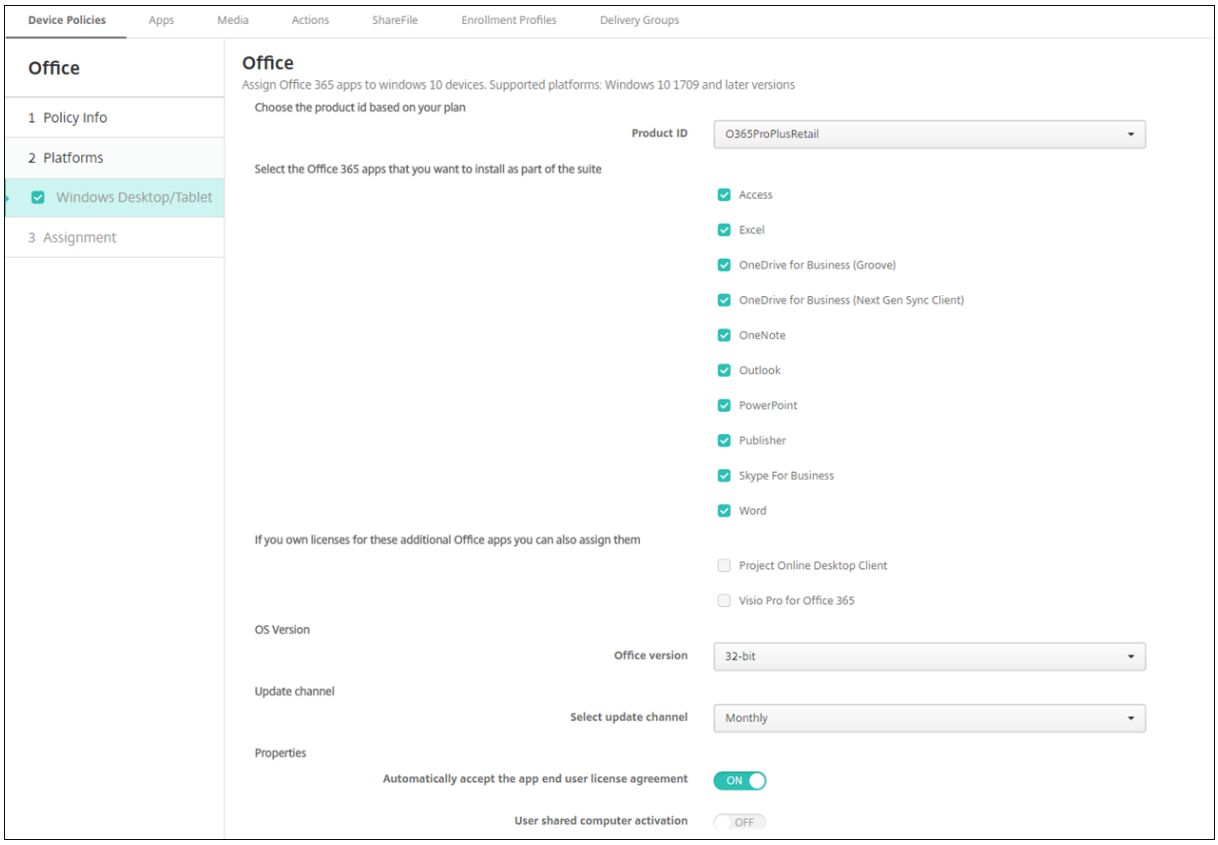
November 6, 2023

Citrix Endpoint Management lets you deploy Microsoft Office 365 products using the Office configuration service provider (CSP). By configuring the Office device policy, you can deploy Microsoft Office apps to any devices running Windows 10 (version 1709 or later) or Windows 11.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Windows Desktop/Tablet settings



- **Product ID:** Select a product ID based on your Office 365 plan. Options are **O365ProPlusRetail, O365BusinessRetail,** or **O365SmallBusPremRetail**.
- **Office 365 Apps:** Select the Office 365 apps that you want deployed. All apps are selected by default.
- **Additional Office apps:** If you own licenses for **Project Online Desktop Client** or **Visio Pro for Office 365**, you can select these apps to have them installed.
- **Office Version:** Select whether to install the **32-bit** or **64-bit** version of Office.
- **Update channel:** Choose how often you want updates to occur. Options are **Monthly**, **Monthly (Targeted)**, **Semi-Annual**, or **Semi-Annual (Targeted)**.
- **Properties:**
  - **Automatically accept the app end user license agreement:** Select **On** or **Off**. Defaults to **On**.
  - **User shared computer activation:** Select whether the computer is shared or not. Options are **On** or **Off**. Defaults to **Off**.
- **Office Language:** Office automatically installs in any languages that Windows already has installed. You can select extra languages to install.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Organization information device policy

September 6, 2025

The Organization information device policy specifies your organization information for alert messages that are pushed from Citrix Endpoint Management to iOS devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Name:** Type the name of the organization running Citrix Endpoint Management.
- **Address:** Type the organization's address.
- **Phone:** Type the organization's support phone number.
- **Email:** Type the support email address.
- **Magic:** Type a word or phrase that describes the services managed by the organization.

OS Update device policy

September 6, 2025

The OS Update device policy lets you deploy:

- The latest OS updates to supervised iOS devices.

  The OS Update device policy only works for supervised devices enrolled in the Apple Deployment Program.

- The latest OS and app updates to the Apple Deployment Program enrolled macOS devices running macOS 10.11.5 and later.

> **Note:**
>
> Apple currently limits OS updates to major versions only. Administrators aren't allowed to update minor versions. For more information, see this article in Apple's documentation.

- The latest OS updates to supervised Desktop and Tablet devices running Windows 10 or Windows 11.

  You can also use the OS Update policy to manage delivery optimization settings for desktops and tablets running Windows 10 (version 1607 or later) or Windows 11. Delivery optimization

© 1997–2025 Citrix Systems, Inc. All rights reserved.

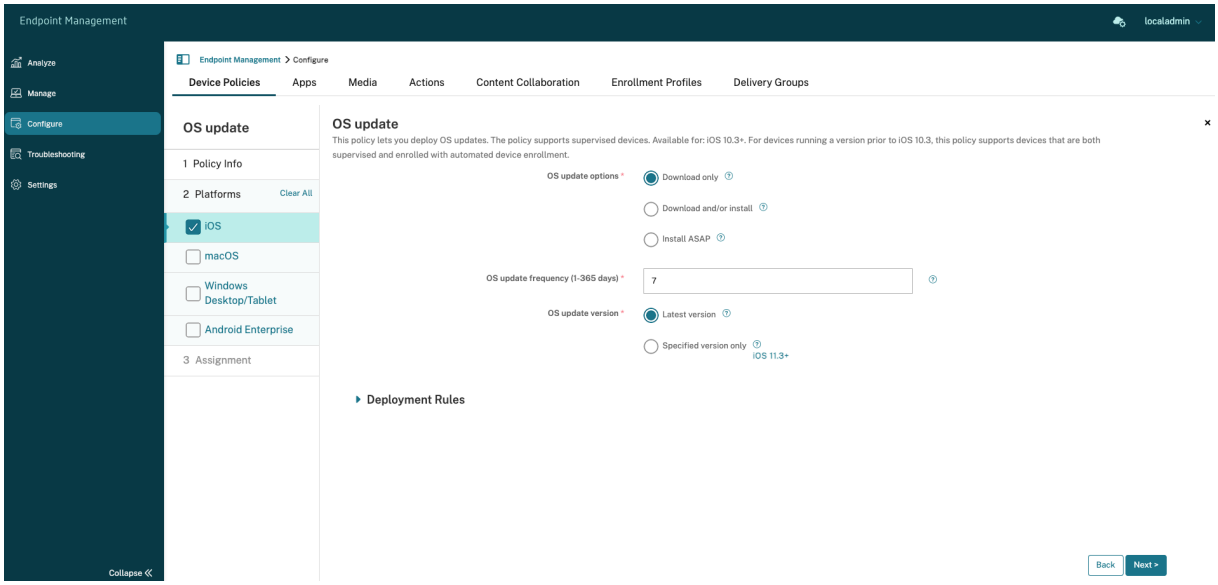
is a peer-to-peer client update service provided by Microsoft for Windows 10 and Windows 11 updates. The goal of delivery optimization is to reduce bandwidth issues during the update process. Bandwidth reduction is achieved by sharing the downloading task among multiple devices. For more information, see the Microsoft article, Configure Delivery Optimization for Windows 10 updates.

- The latest OS updates to managed Android Enterprise devices (Android 7.0 and later).

> **Important:**
>
> The OS update policy does not allow you to disable updates entirely. To delay updates up to 90 days, create a restriction policy. See Restriction device policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



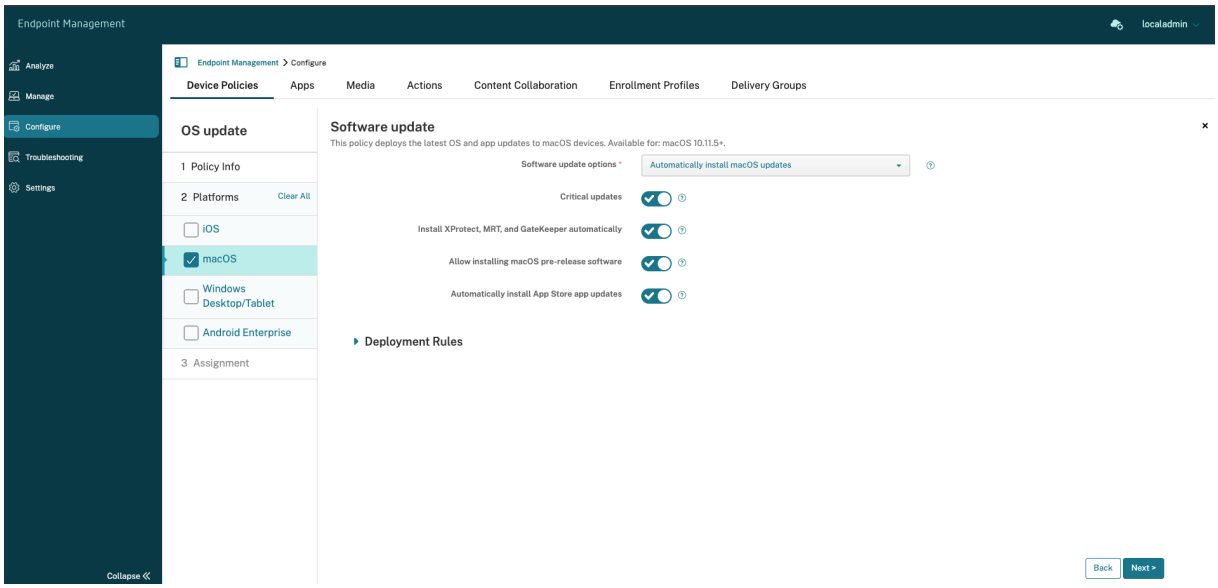
The following settings are for supervised iOS devices.

- **OS update options:** Both of the options download the latest OS updates to supervised devices according to the **OS update frequency**. The device prompts users to install updates. The prompt is visible after the user unlocks the device.
- **OS update frequency:** Determines how frequently Citrix Endpoint Management checks and updates the device OS. The default is **7** days.
- **OS updates version:** Specifies the version to use to update supervised iOS devices. The default is **Latest version**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Latest version:** Select to update to the latest OS version.
  - **Specific version only:** Select to update to a specific OS version and then type the version number.

macOS settings



- **Software updates options:** Controls how macOS devices check for and install updates. Select from the following options:
  - **Automatically install macOS updates:** Updates download and install automatically.
  - **Download new updates when available:** Updates download but require manual installation.
  - **Check for updates:** Checks to see if updates exist but doesn't download or install the updates automatically.
  - **Don't check for updates:** Don't check for new updates, download the updates, or install the updates automatically. Users can still install updates manually.
- **Critical updates:** Allow automatic installation of critical macOS updates.
- **Install xProtect, MRT, and GateKeeper updates automatically:** Allow macOS devices to install updates for security software automatically.
- **Allow installation of macOS pre-release software:** Allow users to install pre-release versions of macOS software.
- **Automatically install App Store app updates:** Allow App Store apps to update automatically.

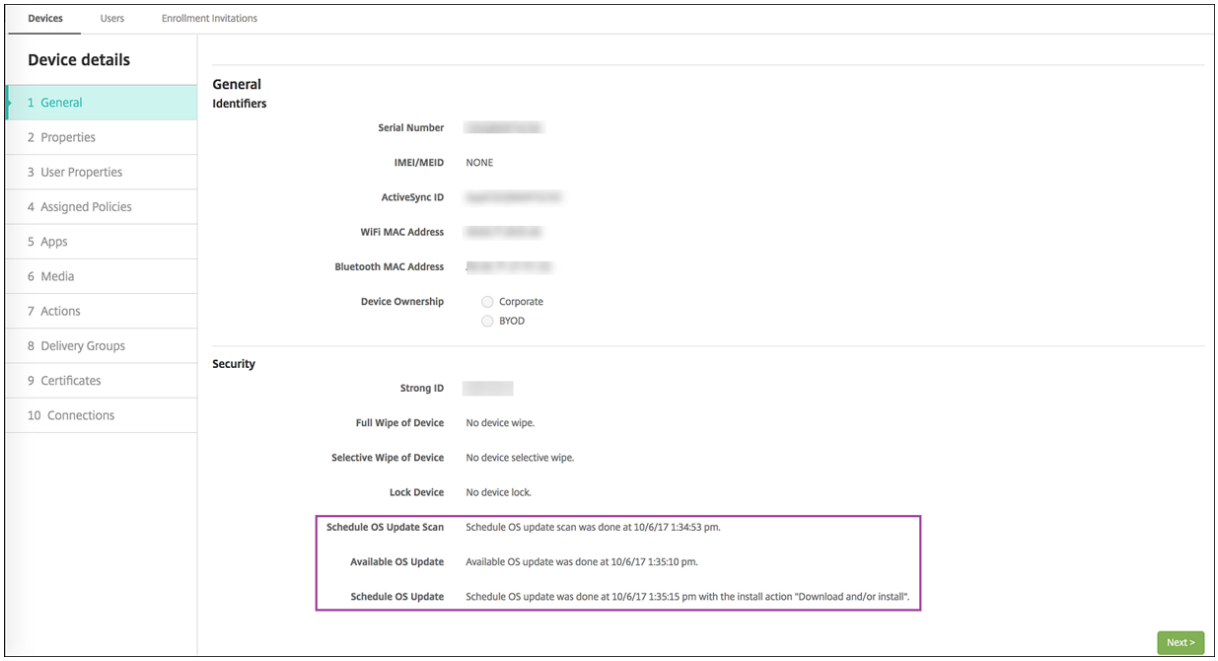
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Get status for iOS and macOS update actions

For iOS and macOS, Citrix Endpoint Management doesn't deploy the Control OS Update policy to devices. Instead, Citrix Endpoint Management uses the policy to send these MDM commands to devices:

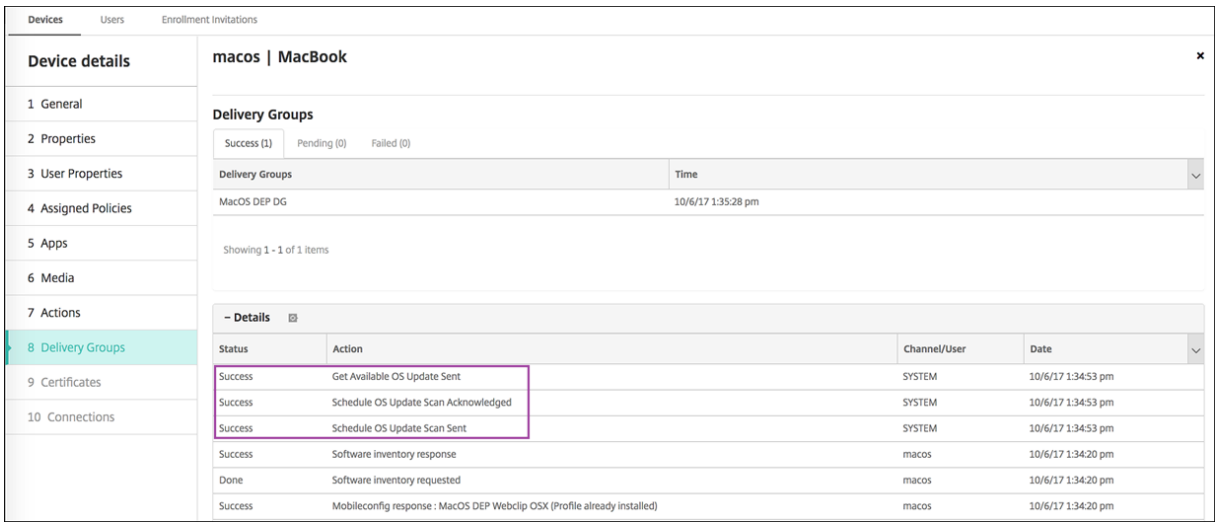
- Schedule OS Update Scan: Requests that the device does a background scan for OS updates. (Optional for iOS)
- Available OS Updates: Queries the device for a list of available OS updates.
- Schedule OS Update: Requests that the device does macOS updates, app updates, or both. Thus, the device OS determines when it downloads or installs the OS and app updates.

The **Manage > Devices > Device details (General)** page shows the status of scheduled and available OS update scans, and scheduled macOS and app updates.

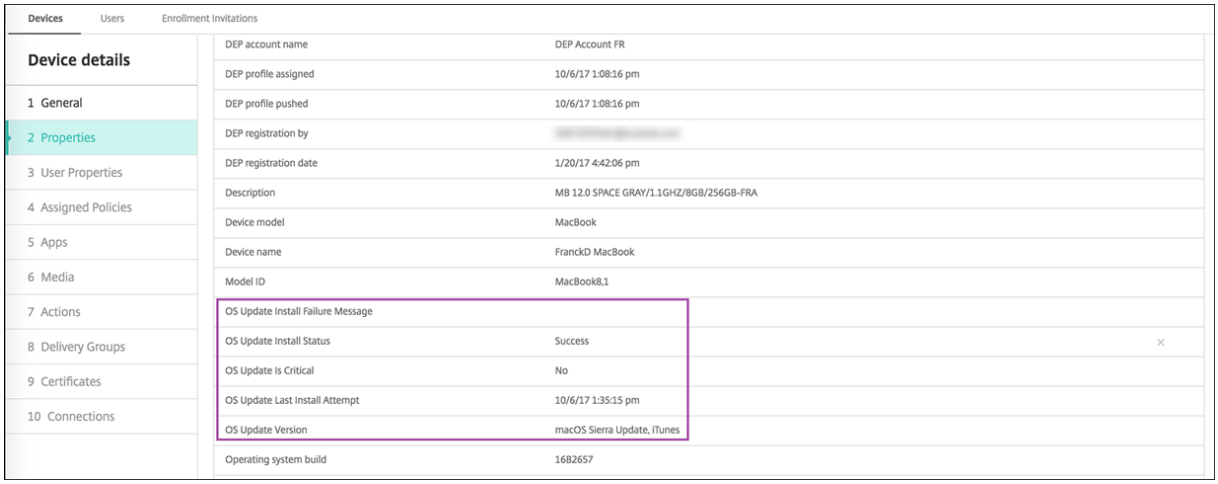


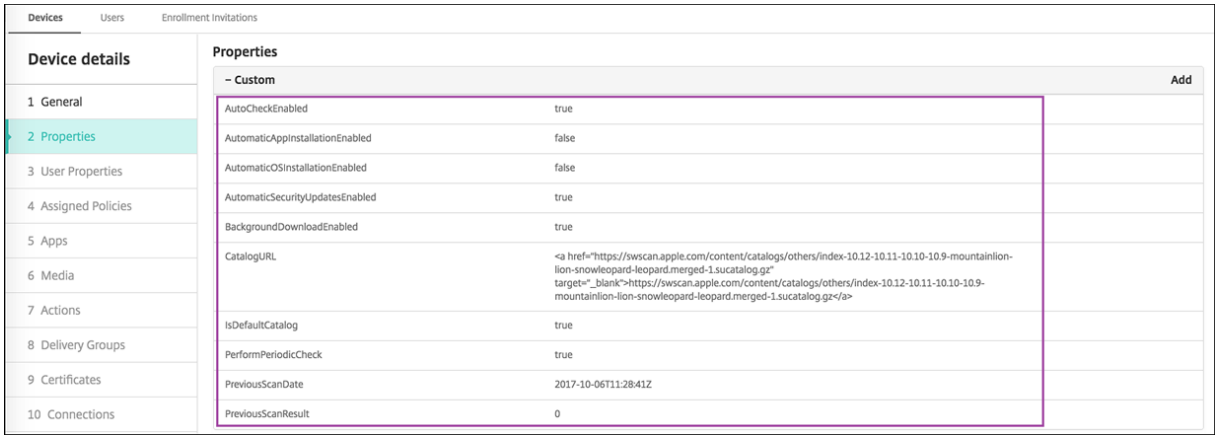
For more details about the status of update actions, go to the **Manage > Devices > Device details (Delivery Groups)** page.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



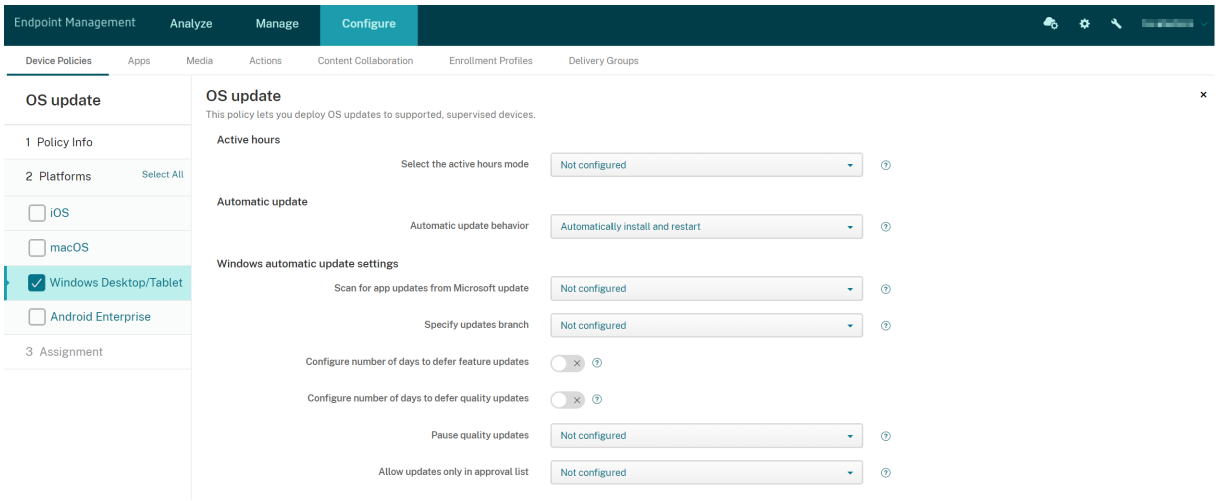
For details such as available OS updates and the last installation attempt, go to the **Manage > Devices > Device details (Properties)** page.





© 1997–2025 Citrix Systems, Inc. All rights reserved.

Windows Desktop and Tablet settings



- **Select active hours mode:** Select a mode to configure the active hours for doing OS updates. You can specify a range of hours or a start and end time. After you select a mode, more settings appear: **Specify max range for active hours** or **Active hours start** and **Active hours end**. **Not configured** allows Windows to do OS updates at any time. Defaults to **Not configured**.
- **Auto update behavior:** Configures the download, install, and restart behavior of the Windows update service on user devices. Defaults to **Auto install and restart**.
  - **Notify user before downloading the update:** Windows notifies users when updates are available. Windows doesn't automatically download and install updates. Users must start the download and install actions.
  - **Auto install and notify to schedule device restart:** Windows downloads updates automatically on non-metered networks. Windows installs updates during Automatic Maintenance when the device isn't in use and isn't running on battery power. If Automatic Maintenance can't install updates for two days, Windows Update installs the updates immediately. If the installation requires a restart, Windows prompts the user to schedule the restart time. The user has up to seven days to schedule the restart. After seven days, Windows forces the device to restart. Enabling the user to control the start time reduces the risk of accidental data loss caused by apps that don't shut down properly on restart.
  - **Auto install and restart:** Default setting. Windows downloads updates automatically on non-metered networks. Windows installs updates during Automatic Maintenance when the device isn't in use and isn't running on battery power. If Automatic Maintenance can't install updates for two days, Windows Update installs the updates immediately. If the installation requires a restart, Windows automatically restarts the device when the device is inactive.
  - **Auto install and restart at a specified time:** When you choose this option, more settings appear so you can specify the day and time. The default is 3 AM daily. Automatic installa-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

tion happens at the specified time and device restart occurs after a 15-minute countdown. When Windows is ready to restart, a logged-in user can interrupt the 15-minute countdown to delay the restart.
  - **Auto install and restart without end-user control:** Windows downloads updates automatically on non-metered networks. Windows installs updates during Automatic Maintenance when the device isn't in use and isn't running on battery power. If Automatic Maintenance can't install updates for two days, Windows Update installs updates immediately. If the installation requires a restart, Windows automatically restarts the device when the device is inactive. This option also sets the user control panel to read-only.
  - **Turn off automatic updates:** Disables Windows automatic updates on the device.

- **Scan for app updates from Microsoft update:** Specifies whether Windows accepts updates for other Microsoft apps from the Microsoft update service. Defaults to **Not configured**.
  - **Not configured:** Use this setting if you don't want to configure the behavior. Windows doesn't change the related UI on user devices. Users can accept or reject updates for other Microsoft apps.
  - **Yes:** Windows allows app updates to be installed from the Windows update service. The related setting on the user device is inactive, so the user can't modify the setting.
  - **No:** Windows doesn't allow app updates to be installed from the Windows update service. The related setting on the user device is inactive, so the user can't modify the setting.

- **Specify updates branch:** Specifies which Windows update service branch to use for updates. Defaults to **Not configured**.
  - **Not configured:** Use this setting if you don't want to configure the behavior. Windows doesn't change the related UI on user devices. Users can choose a Windows update service branch.
  - **Current Branch:** Windows receives updates from Current Branch. The related setting on the user device is inactive, so the user can't modify the setting.
  - **Current Branch for Business:** Windows receives updates from Current Branch for Business. The related setting on the user device is inactive, so the user can't modify the setting.

- **Configure number of days to defer feature updates:** If **On**, Windows defers feature updates by the specified number of days and the user can't change the setting. If **Off**, the user can change the number of days to defer feature updates. Defaults to **Off**.
- **Configure number of days to defer quality updates:** If **On**, Windows defers quality updates by the specified number of days and the user can't change the setting. If **Off**, the user can change the number of days to defer quality updates. Defaults to **Off**.
- **Pause quality updates:** Specifies whether to pause quality updates for 35 days. Defaults to **Not configured**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Not configured:** Use this setting if you don't want to configure the behavior. Windows doesn't change the related UI on user devices. Users can choose to pause quality updates for 35 days.
  - **Yes:** Windows pauses the installation of quality updates from the Windows Update Service for 35 days. The related setting on the user device is inactive, so the user can't modify the setting.
  - **No:** Windows doesn't pause the installation of quality updates from the Windows Update Service. The related setting on the user device is inactive, so the user can't modify the setting.

- **Allow updates only in approval list:** Specifies whether to install only the updates that an MDM server approves. Citrix Endpoint Management doesn't support configuring an approved list of updates. Defaults to **Not configured**.

  - **Not configured:** Use this setting if you don't want to configure the behavior. Windows doesn't change the related UI on user devices. Users can choose which updates to allow.
  - **Yes, install only approved updates:** Allows installation of approved updates only.
  - **No, install all applicable updates:** Allows installation of any applicable updates on the device.

- **Use internal update server:** Specifies whether to get updates from the Windows update service or an internal update server through Windows Server Update Services (WSUS). If **Off**, devices use the Windows update service. If **On**, devices connect to the specified WSUS server for updates. Defaults to **Off**.

  - **Accept updates signed by entities other than Microsoft:** Specifies whether to accept updates signed by third-party entities other than Microsoft. This feature requires that the device trusts the third-party vendor certificate. Defaults to **Off**.
  - **Allow connection to Microsoft update service:** Allows Windows update on the device to connect periodically to the Microsoft update service, even if the device is configured to get updates from a WSUS server. Defaults to **On**.
  - **WSUS server:** Specify the server URL for the WSUS server.
  - **Alternate intranet server to host updates:** Specify an alternate intranet server URL to host updates and receive reporting information.

- **Configure delivery optimization:** Whether to use delivery optimization for Windows 10 and Windows 11 Updates. Default is **Off**.
- **Cache size:** The maximum size of the delivery optimization cache. A value of **0** means an unlimited cache. The default is **10** GB.
- **Allow VPN peer caching:** Whether to allow devices to participate in peer caching when connected to the domain network through VPN. When **On**, the device can download from or upload to other domain network devices, either on VPN or on the corporate domain network. Default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Download method:** The download method that delivery optimization can use for downloads of Windows Updates, app, and app updates. Default is **HTTP blended with peering behind the same NAT**. Options are:
  - **HTTP only, no peering:** Disables peer-to-peer caching but allows delivery optimization to download content from Windows Update servers or Windows Server Update Services (WSUS) servers.
  - **HTTP blended with peering behind the same NAT:** Enables peer sharing on the same network. The Delivery Optimization cloud service finds other clients that connect to the Internet using the same public IP as the target client. These clients then try to connect to other peers on the same network by using their private subnet IP.
  - **HTTP blended with peering across a private group:** Automatically selects a group based on the device Active Directory Domain Services (AD DS) site or the domain that the device authenticates to. Peering occurs across internal subnets, between devices that belong to the same group, including devices in remote offices.
  - **HTTP blended with Internet peering:** Enable Internet peer sources for Delivery Optimization.
  - **Simple download mode with no peering:** Disable the use of Delivery Optimization cloud services. Delivery Optimization switches to this mode automatically during these conditions: When the Delivery Optimization cloud services are unavailable, unreachable, or when the content file size is less than 10 MB. In this mode, Delivery Optimization provides a reliable download experience, with no peer-to-peer caching.
  - **Do not use Delivery Optimization and use BITS instead:** Enables clients to use BranchCache. For more information, see the Microsoft article, BranchCache.
- **Max download bandwidth:** The maximum download bandwidth in KBs/second. Default is **0**, which means dynamic bandwidth adjustment.
- **Percentage of maximum download bandwidth:** The maximum download bandwidth that delivery optimization can use across all concurrent download activities. The value is a percentage of the available download bandwidth. Default is **0**, which means dynamic adjustment.
- **Max upload bandwidth:** The maximum upload bandwidth in KBs/second. Default is **0**. A value of **0** means unlimited bandwidth.
- **Monthly upload data cap:** The maximum size in GBs that delivery optimization can upload to Internet peers in each calendar month. The default is 20 GB. A value of **0** means unlimited monthly uploads.

How Citrix Endpoint Management handles approved updates to Windows Desktop and Tablet devices

You can specify whether to install only approved updates. Citrix Endpoint Management handles the updates as follows:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- For a security update, such as for Windows Defender definitions, Citrix Endpoint Management automatically approves the update and sends an install command to the device during the next sync.
- For all other update types, Citrix Endpoint Management waits for your approval before sending the install command to the device.

Prerequisites

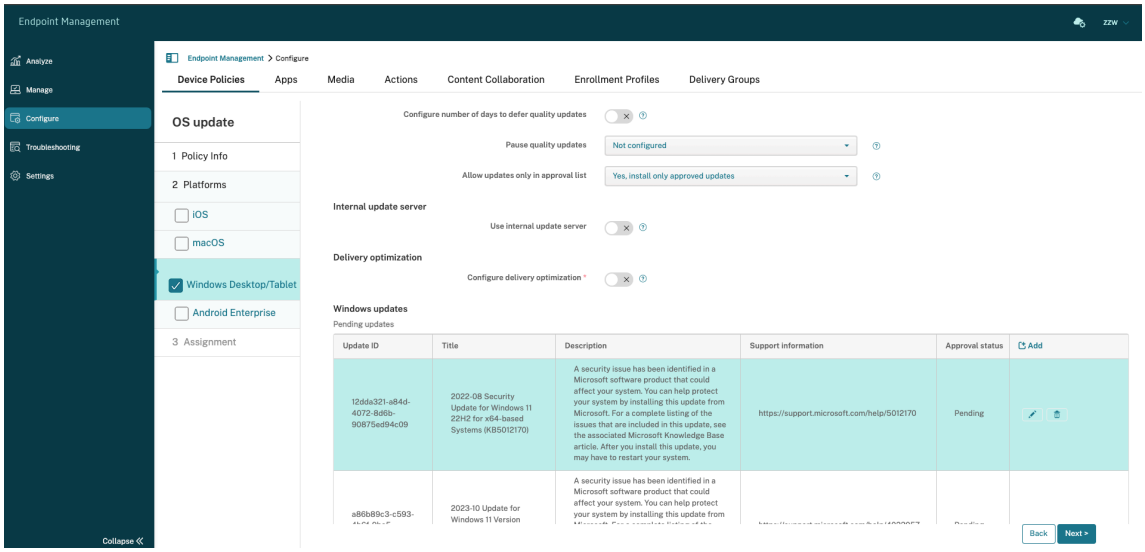
- You must upload the Microsoft root certificate to the Citrix Endpoint Management server as a server certificate.
- For information about importing a server certificate, see "To import a certificate"in Certificates and authentication.

To install only approved updates

1. Go to **Configure > Device Policies** and open the OS Update device policy.
2. Change the **Allow updates only in approval list** setting to **Yes, install only approved updates**.

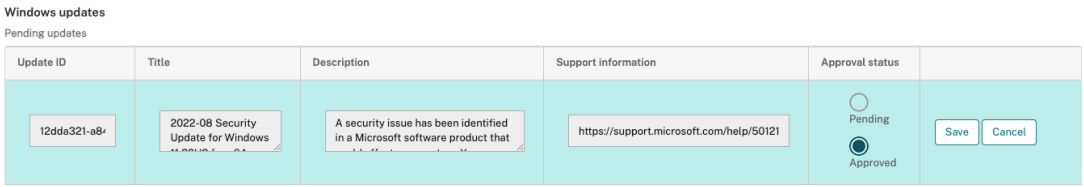
To approve an update

1. In the OS Update device policy, scroll down to the **Pending updates** table. Citrix Endpoint Management gets the updates listed in the table from the devices.
2. Search for updates with an **Approval status** of **Pending**.
3. Click the row for the update that you want to approve and then click the edit icon for that row (in the **Add** column).



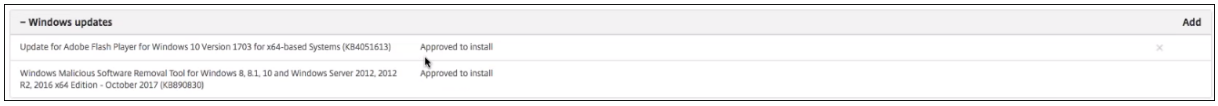
4. To approve the update, click **Approved** and then click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> Although the Pending updates table includes add and delete commands, those commands don't result in any changes to the Citrix Endpoint Management database. Editing approval status is the only action available for pending updates.

To view the Windows update status for a device, go to **Manage > Devices > Properties**.



When an update publishes, the **Update ID** appears in the first column with a status (Success or Failure). You can create a report or an automated action for devices with failed updates. The date and time of the publication also appears.

How updates work for first-time and subsequent deployments The effect of the OS Update device policy on devices differs for a first-time deployment versus a deployment after devices get updates.

- For Citrix Endpoint Management to query a device for updates, you must configure and assign to a delivery group at least one OS Update device policy.

  Citrix Endpoint Management queries a device for installable updates during a device MDM sync.
- After the first OS Update device policy deploys, the list of Windows updates is empty because no device has reported yet.
- When the devices in the assigned delivery group report updates, Citrix Endpoint Management saves those updates in its database. To approve any reported updates, edit the policy again.

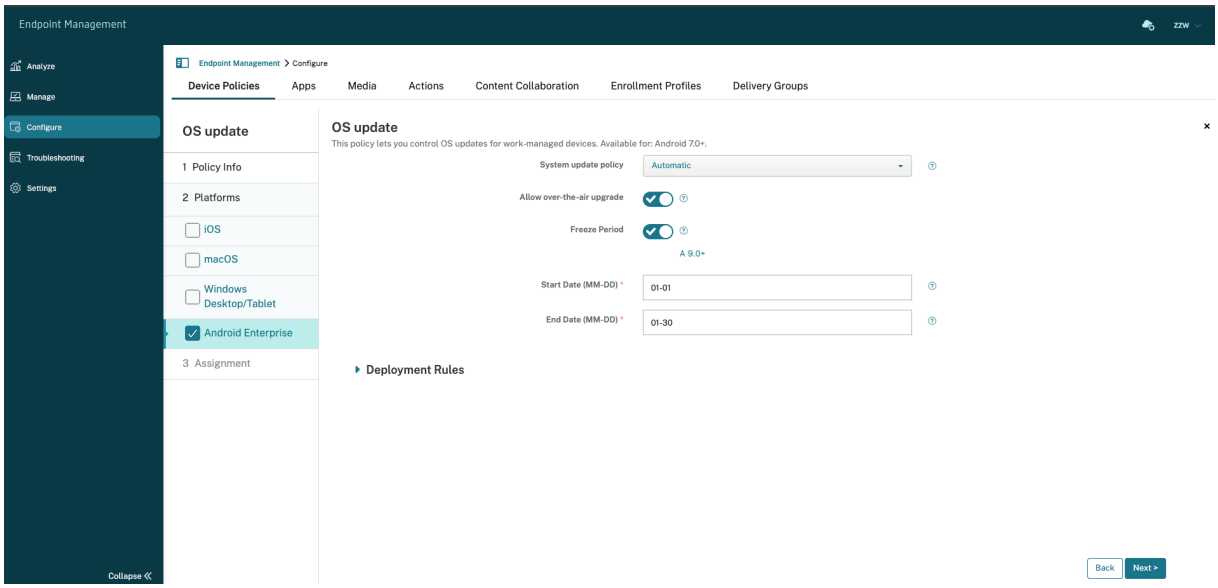
  Update approval applies only to the policy that you are editing. Updates approved in one policy don't show as approved in another policy. The next time that a device syncs, Citrix Endpoint Management sends a command to the device to indicate that the update is approved.
- For a second OS Update device policy, the update list has the updates stored in the Citrix Endpoint Management database. Approve updates for each policy.

  During each device sync, Citrix Endpoint Management queries the device for the approved update state until the device reports that an update installed. For updates that require a restart after an install, Citrix Endpoint Management queries the state of the update until the device reports that the update installed.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Management doesn't restrict the updates shown in the policy configuration page by delivery group or device. All updates reported by devices appear in the list.

Android Enterprise settings



- **System update policy:** Determines when system updates occur.
  - **Automatic:** Installs an update when it's available.
  - **Windowed:** Installs an update automatically within the daily maintenance window specified in the **Start time** and **End time**.
    - **Start time:** The start of the maintenance window, measured as the number of minutes (**0** - **1440**) from midnight in the device local time. Default is **0**.
    - **End time:** The end of the maintenance window, measured as the number of minutes (**0** - **1440**) from midnight in the device local time. Default is **120**.
  - **Postpone:** Allows a user to postpone an update for up to 30 days.
  - **Default:** Sets the update policy to the system default.
- **Allow over-the-air upgrade:** If disabled, user devices can't receive software updates wirelessly. The default is **On**.
- **Freeze Period:** If **On**, OS updates aren't installed on the device during the date range specified for the **Automatic**, **Postpone**, and **Windowed** update policies. Only one freeze period can be set for a device at a time. The length of the freeze period can't exceed 90 days.
  - **Start Date/End Date:** The date range in which OS updates aren't installed if **Freeze Period** is enabled.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Freeze Period:** If **On**, OS updates aren't installed on the device during the date range specified for the **Automatic**, **Postpone**, and **Windowed** update policies. Only one freeze period can be set for a device at a time. The length of the freeze period can't exceed 90 days.
  - **Start Date/End Date:** The date range in which OS updates aren't installed if **Freeze Period** is enabled.

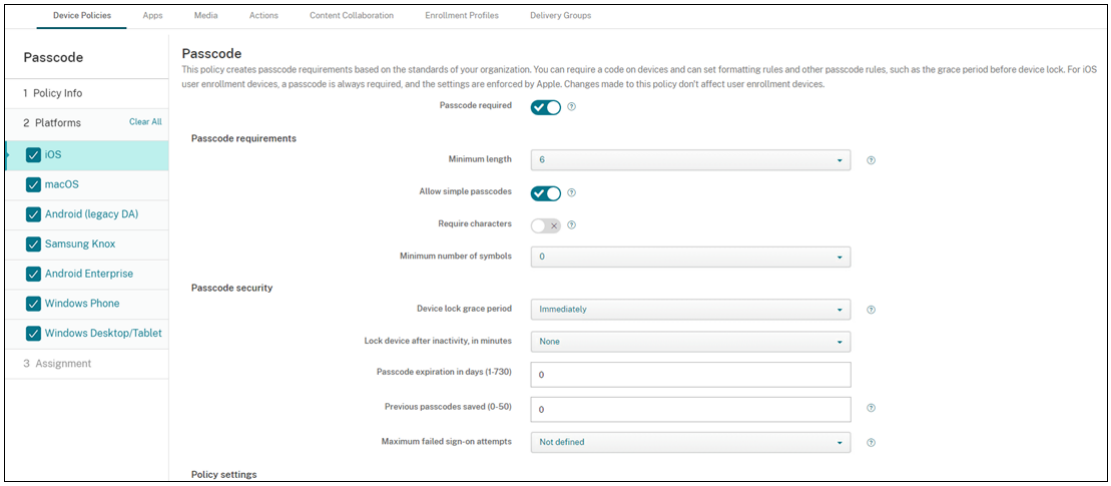
Passcode device policy

September 6, 2025

Create a passcode policy in Citrix Endpoint Management based on your organization's standards. You can require passcodes on users' devices and can set various formatting and passcode rules. Create policies for iOS, macOS, Android, Android Enterprise, and Windows desktop/tablet. Each platform requires a different set of values, which are described in this article.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **Passcode required:** Select this option to require a passcode and to display the configuration options for an iOS passcode device policy. The page expands to let you configure settings for passcode requirements, passcode security, and policy settings.
- **Passcode requirements**
  - **Minimum length:** Click the minimum passcode length in the drop-down list. The default is **6**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Allow simple passcodes:** Select whether to allow simple passcodes. Simple passcodes are a repeated or sequential set of characters. The default is **On**.
- **Required characters:** Select whether to require passcodes to have at least one letter. The default is **Off**.
- **Minimum number of symbols:** In the list, click the number of symbols the passcode must have. The default is **0**.

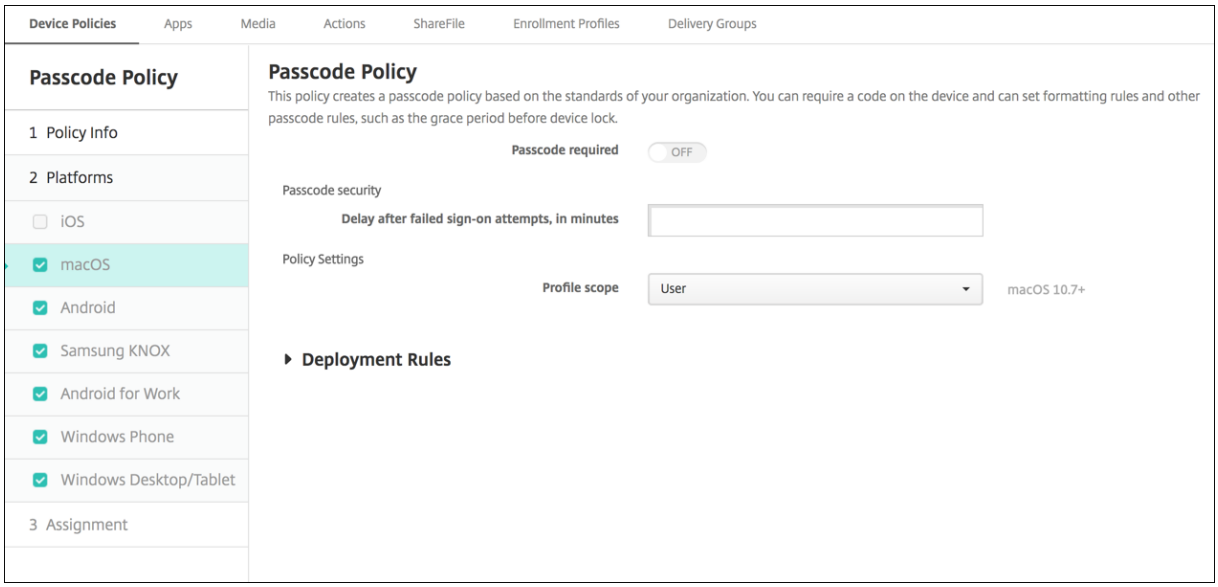
- **Passcode security**
  - **Device lock grace period:** In the list, click the length of time before users must enter a passcode to unlock a locked device. The default is **Immediately**.
  - **Lock device after inactivity:** In the box, enter the length of time a device can be inactive before it is locked. The value can be between 1 and 15 minutes. Set the value to **None** to disable the policy. The default is **None**.
  - **Passcode expiration in days (1-730):** Type the number of days after which the passcode expires. Valid values are 1–730. The default is **0**, which means the passcode never expires.
  - **Previous passwords saved (0-50):** Type the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is **0**, which means users can reuse passwords.
  - **Maximum failed sign-on attempts:** In the list, click the number of times a user can fail to sign in.
    - If you set this number higher than 6, after the sixth attempt, the device imposes a time delay between attempts. The time delay increases with each failed attempt. After the final attempt, all data and settings are securely erased.
    - If you set the number at 6 or lower, the device is erased without implementing a time delay.
    - If you select **Not defined**, after 6 attempts, the device imposes an increasing time limit between attempts but isn't wiped.

    The default is **Not defined**.

- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

macOS settings



- **Passcode required:** Select this option to require a passcode and to display the configuration options for an iOS passcode device policy. The page expands to let you configure settings for passcode requirements, passcode security, and policy settings.
- If **Passcode required** is disabled, next to **Delay after failed sign-on attempts, in minutes**, type the number of minutes to delay before allowing users to reenter their passcodes.
- If you enable **Passcode required**, configure the following settings:
- **Passcode requirements**
  - **Minimum length:** Click the minimum passcode length in the drop-down list. The default is **6**.
  - **Allow simple passcodes:** Select whether to allow simple passcodes. Simple passcodes are a repeated or sequential set of characters. The default is **On**.
  - **Required characters:** Select whether to require passcodes to have at least one letter. The default is **Off**.
  - **Minimum number of symbols:** In the list, click the number of symbols the passcode must have. The default is **0**.
- **Passcode security**
  - **Device lock grace period:** In the list, click the length of time before users must enter a passcode to unlock a locked device. The default is **None**.
  - **Lock device after inactivity:** In the list, click the length of time a device can be inactive before it is locked. The value can be between 1 and 5 minutes. Set the value to **None** to disable the policy. The default is **None**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

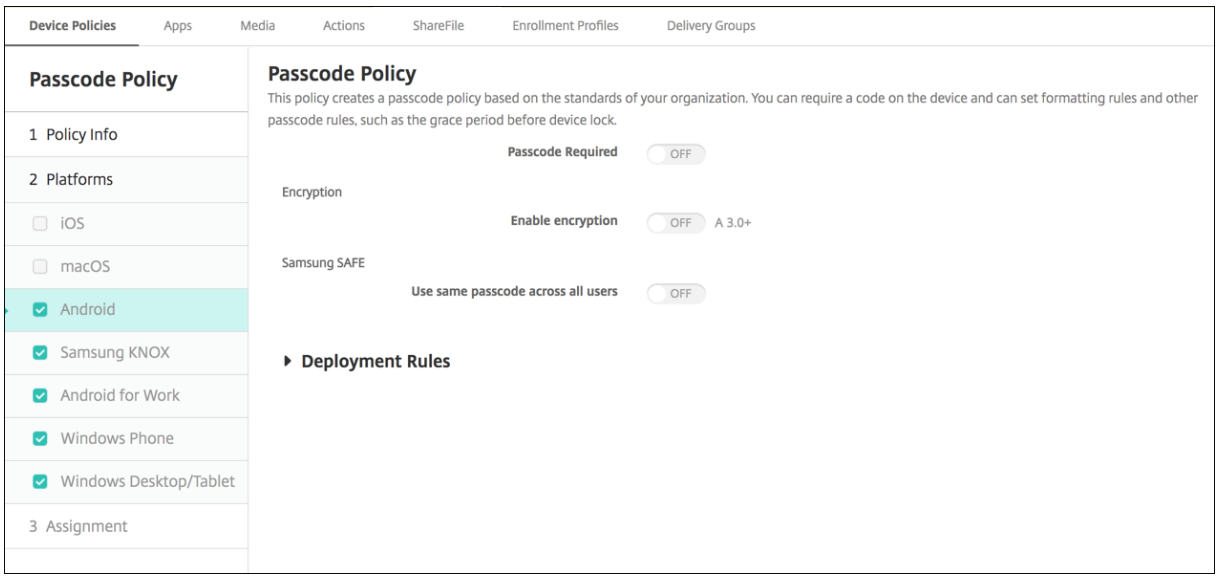
- **Passcode expiration in days (1-730):** Type the number of days after which the passcode expires. Valid values are 1–730. The default is **0**, which means the passcode never expires.
- **Previous passwords saved (0-50):** Type the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is **0**, which means users can reuse passwords.
- **Maximum failed sign-on attempts:** In the list, click the number of times a user can fail to sign in.
  - If you set this number higher than 6, after the sixth attempt, the device imposes a time delay between attempts. The time delay increases with each failed attempt. After the final attempt, the device locks.
  - If you set the number at 6 or lower, the device locks without implementing a time delay.
  - If you select **Not defined**, after 6 attempts, the device imposes an increasing time limit between attempts but does not lock.

  The default is **Not defined**.
- **Delay after failed sign-on attempts, in minutes:** Type the number of minutes before the login window appears after a user reaches the maximum number of failed attempts.
- **Force passcode reset:** If **Off**, users don't need to reset their passcode the next time they authenticate after their device receives this policy. The default is **On**.

- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Android (legacy DA) settings



> **Note:**
>
> The default setting for Android is **Off**.

- **Passcode required:** Select this option to require a passcode and to display the configuration options for an Android passcode device policy. The page expands to let you configure settings for passcode requirements, passcode security, and encryption.
- **Passcode requirements**
  - **Minimum length:** Click the minimum passcode length in the drop-down list. The default is 6.
  - **Biometric recognition:** Select whether to enable biometric recognition. If you enable this option, the Required characters field is hidden. The default is **Off**.
  - **Required characters:** In the list, click **No Restriction**, **Both numbers and letters**, **Numbers only**, or **Letters only** to configure how passcodes are composed. The default is **No restriction**.
  - **Advanced rules:** Select whether to apply advanced passcode rules. The default is **Off**.
  - When you enable **Advanced rules,** from each of the following lists, click the minimum number of each character type that a passcode must have:
    - **Symbols:** The minimum number of symbols.
    - **Letters:** The minimum number of letters.
    - **Lowercase letters:** The minimum number of lowercase letters.
    - **Uppercase letters:** The minimum number of uppercase letters.
    - **Numbers or symbols:** The minimum number of numbers or symbols.
    - **Numbers:** The minimum number of numbers.
- **Passcode security**

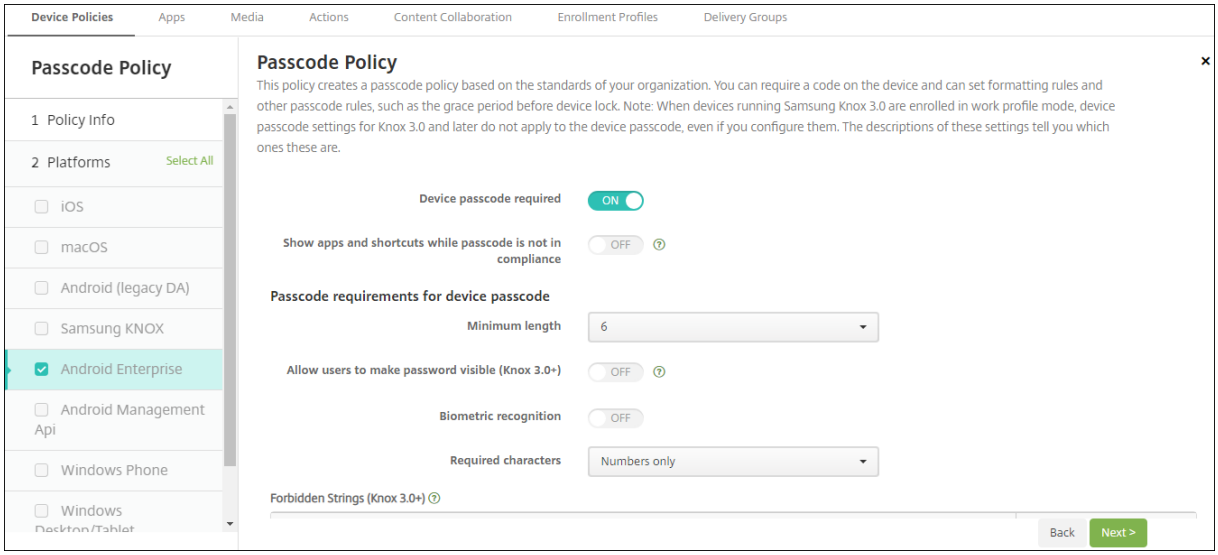
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Lock device after inactivity:** In the list, click the length of time a device can be inactive before it is locked. The default is **None**
- **Passcode expiration in days (1-730):** Type the number of days after which the passcode expires. Valid values are 1–730. The default is **0**, which means the passcode never expires.
- **Previous passwords saved (0-50):** Type the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is **0**, which means users can reuse passwords.
- **Maximum failed sign-on attempts:** In the list, click the number of times a user can fail to sign in successfully after which the device is wiped. The default is **Not defined**.

- **Encryption**
  - **Enable encryption:** Select whether to enable encryption. The option is available regardless of the **Passcode required** setting.

    To encrypt their devices, users must start with a charged battery and keep the device plugged in until encryption completes. The process can take an hour or more. If they interrupt the encryption process, they can lose some or all data on their devices. After a device is encrypted, the process can't be reversed except by doing a factory reset, which erases all the data on the device.

Android Enterprise settings



For Android Enterprise devices, you can require a passcode for the device or a security challenge for the Android Enterprise work profile or both.

- **Device passcode required:** Requires a passcode on the device. When this setting is **On**, configure the settings under **Passcode requirements for device passcode** and **Passcode security for device passcode**. Default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Show apps and shortcuts while passcode is not in compliance:** When this setting is **On**, apps and shortcuts on the device aren't hidden, even when the passcode isn't compliant. When this setting is **Off**, apps and shortcuts are hidden when the passcode isn't compliant. If you enable this setting, Citrix® recommends you create an automated action to mark the device as out of compliance when the passcode isn't in compliance. Default is **Off**.
- **Passcode requirements for device passcode:**
  - **Minimum length:** Specifies the minimum passcode length. The default is 6.
  - **Biometric recognition:** Enables biometric recognition. If this setting is **On**, the **Required characters** field is hidden. The default is **Off**.
  - **Required characters:** Specifies the types of characters required for passcodes. In the list, choose **No Restriction**, **Both numbers and letters**, **Numbers only**, or **Letters only**. Use **No restrictions** only for devices running Android 7.0. Android 7.1 and later don't honor the **No restrictions** setting. The default is **Both numbers and letters**.
  - **Advanced rules:** Applies advanced rules for the types of characters that can occur in passcodes. When this setting is **On**, configure the settings under **Minimum number of** and **Maximum number of**. This setting isn't available for Android devices earlier than Android 5.0. The default is **Off**.
  - **Minimum number of:**
    - **Symbols:** Specifies the minimum number of symbols. Default is **0**.
    - **Letters:** Specifies the minimum number of letters. Default is **0**.
    - **Lowercase letters:** Specifies the minimum number of lowercase letters. Default is **0**.
    - **Uppercase letters:** Specifies the minimum number of uppercase letters. Default is **0**.
    - **Numbers or symbols:** Specifies the minimum number of numbers or symbols. Default is **0**.
    - **Numbers:** Specifies the minimum number of numbers. Default is **0**.
    - **Changed characters:** For devices running Samsung Knox 3.0 and later that have a valid Knox license key configured. For fully managed devices only. This setting does not apply to devices enrolled as work profile devices. Specifies the number of characters users must change from their previous passcode. The default is **0**.
  - **Maximum number of:** For devices running Samsung Knox 3.0 and later that have a valid Knox license key configured. For fully managed devices only. This setting does not apply to devices enrolled as work profile devices.
    - **Times a character can occur:** Specifies the maximum number of times a character can occur in a passcode. The default is **0**, which means there is no maximum limit.
    - **Alphabetic sequence length:** Specifies the maximum length of an alphabetic sequence in a passcode. The default is **0**, which means there is no maximum limit.
    - **Numeric sequence length:** Specifies the maximum length of a numeric sequence in a passcode. The default is **0**, which means there is no maximum limit.
- **Passcode complexity for device passcode (Android 12+):**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **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 Citrix 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

      > **Note:**
      > For BYOD devices, passcode settings such as Minimum length, Required characters, Biometric recognition, and Advanced rules aren't applicable on Android 12+. Use passcode complexity instead.

- **Passcode security for device passcode:**
  - **Wipe the device after (failed sign-on attempts):** Specifies the number of times a user can fail to sign on after which the device is fully wiped. Default is **Not defined**.
  - **Lock device after inactivity:** Specifies the number of minutes a device can be inactive before it is locked. Set the value to 0 to disable the policy.
  - **Passcode expiration in days (1-730):** Specifies the number of days after which the passcode expires. Valid values are 1–730. The default is **0**, which means the passcode never expires.
  - **Previous passwords saved (0-50):** Specifies the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. Default is **0**, which means users can reuse passwords.
- **Work profile security challenge:** Require users to complete a security challenge for access to apps running in an Android Enterprise work profile. For devices running Android 7.0 and later. When this setting is **On**, configure the settings under **Passcode requirements for work profile security challenge** and **Passcode security for work profile security challenge**. Default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Passcode requirements for work profile security challenge:**
  - **Minimum length:** Specifies the minimum passcode length. The default is 6.
  - **Biometric recognition:** Enables biometric recognition. If this setting is **On**, the **Required characters** field is hidden. The default is **Off**.
  - **Required characters:** Specifies the types of characters required for passcodes. In the list, choose **No Restriction**, **Both numbers and letters**, **Numbers only**, or **Letters only**. Use **No restrictions** only for devices running Android 7.0. Android 7.1 and later don't honor the **No restrictions** setting. The default is **Both numbers and letters**.
  - **Advanced rules:** Applies advanced rules for the types of characters that can occur in passcodes. When this setting is **On**, configure the settings under **Minimum number of** and **Maximum number of**. This setting isn't available for Android devices earlier than Android 5.0. The default is **Off**.
  - **Minimum number of:**
    - **Symbols:** Specifies the minimum number of symbols. Default is **0**.
    - **Letters:** Specifies the minimum number of letters. Default is **0**.
    - **Lowercase letters:** Specifies the minimum number of lowercase letters. Default is **0**.
    - **Uppercase letters:** Specifies the minimum number of uppercase letters. Default is **0**.
    - **Numbers or symbols:** Specifies the minimum number of numbers or symbols. Default is **0**.
    - **Numbers:** Specifies the minimum number of numbers. Default is **0**.
    - **Changed characters:** For devices running Knox 3.0 and later that have a valid Knox license key configured. Specifies the number of characters users must change from their previous passcode. The default is **0**.
  - **Maximum number of:** For devices running Knox 3.0 and later that have a valid Knox license key configured.
    - **Times a character can occur:** Specifies the maximum number of times a character can occur in a passcode. The default is **0**, which means there is no maximum limit.
    - **Alphabetic sequence length:** Specifies the maximum length of an alphabetic sequence in a passcode. The default is **0**, which means there is no maximum limit.
    - **Numeric sequence length:** Specifies the maximum length of a numeric sequence in a passcode. The default is **0**, which means there is no maximum limit.
- **Passcode complexity for work profile security challenge (Android 12+):**
  - **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 Citrix Secure Hub 22.9 or later.
  - **Complexity level:** Predefined levels of password complexity.
    - **None:** No password required.
    - **Low:** Passwords can be:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

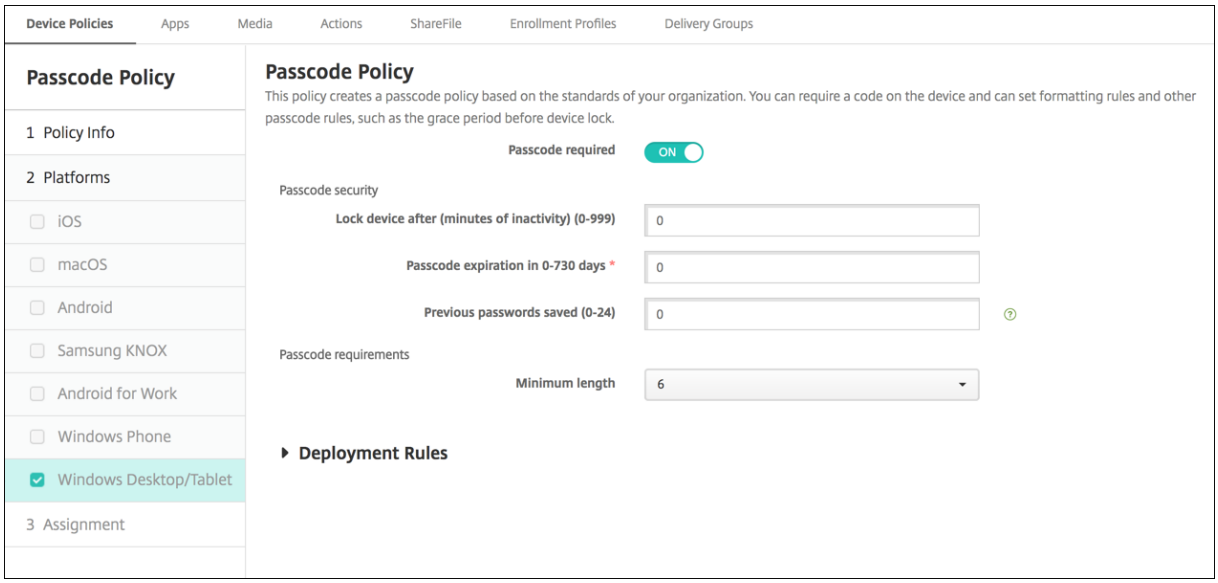
        - A pattern
        - A PIN with a minimum of four numbers
    - **Medium:** Passwords can be:
        - A PIN with no repeating sequences (4444) or ordered sequences (1234), and a minimum of four numbers
        - Alphabetic with a minimum of four characters
        - Alphanumeric with a minimum of 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

        > **Note:**
        > If you enable passcode complexity for a work profile, you must also enable it for the device.

- **Passcode security for work profile security challenge**
    - **Wipe the container after (failed sign-on attempts):** Specifies the number of times a user can fail to sign on, after which the work profile and its data are wiped from the device. Users must reinitialize the work profile after the wiping occurs. Default is **Not defined**.
    - **Lock container after inactivity:** Specifies the number of minutes a device can be inactive before the work profile is locked. The value can be between 0 and 999 minutes. Set the value to 0 to disable the policy.
    - **Passcode expiration in days (1-730):** Specifies the number of days after which the passcode expires. Valid values are 1–730. The default is **0**, which means the passcode never expires.
    - **Previous passwords saved (0-50):** Specifies the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is **0**, which means users can reuse passwords.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Windows Desktop/Tablet settings



- **Passcode required:** Select this option to not require a passcode for Windows Desktop/Tablet devices. The default setting is **On**, which requires a passcode. The page collapses and the following options disappear when you disable this setting.
- **Passcode security**
  - **Lock device after inactivity:** Type the number of minutes a device can be inactive before it is locked. The default is **0**.
  - **Passcode expiration in days (0-730):** Type the number of days after which the passcode expires. Valid values are 0–730. The default is **0**, which means the passcode never expires.
  - **Previous passwords saved (0-24):** Type the number of used passcodes to save. Users are unable to use any passcode found in this list. Valid values are 1–24. Enter a number between 1 and 24 in this field. The default is **0**.
- **Passcode requirements**
  - **Minimum length:** Click the minimum passcode length in the drop-down list. The default is **6**.

Passcode lock grace period device policy

April 15, 2020

The Passcode lock grace period device policy is for shared devices running iOS (iPadOS). For more information about Shared iPads, see Integrate with Apple Education features.

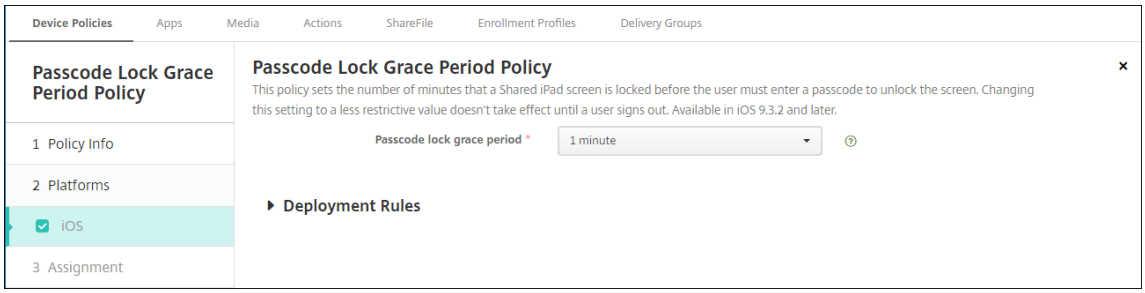
© 1997–2025 Citrix Systems, Inc. All rights reserved.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Passcode Lock Grace Period:** The number of minutes that a Shared iPad screen stays locked before the user must enter a passcode to unlock the screen. Changing this setting to a less restrictive value doesn't take effect until a user signs out. Default is **Immediately**.

  By default, the Shared iPad locks itself automatically after two minutes of inactivity.



Personal hotspot device policy

September 6, 2025

You can allow users to connect to the Internet when they aren't in range of a Wi-Fi network by using the cellular data connection through their iOS devices' personal hotspot functionality.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Disable personal hotspot:** Select whether to disable the personal hotspot functionality on user devices. The default is **Off**, which switches off the personal hotspot on users devices. This policy does not disable the functionality. Users can still use the personal hotspot on their devices, but when the policy is deployed, the personal hotspot is turned off so that it doesn't stay on by default.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

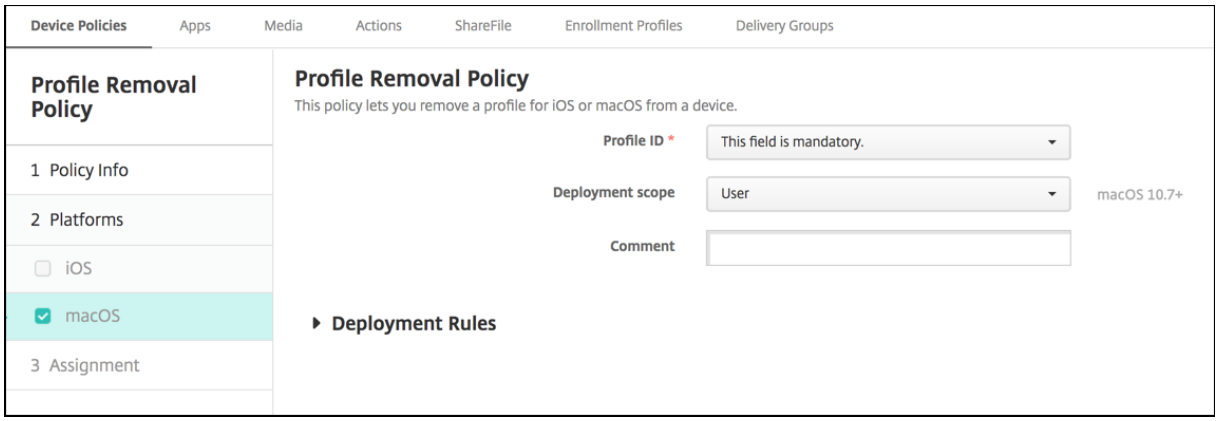
Profile Removal device policy

September 6, 2025

You can create an app profile removal device policy in Citrix Endpoint Management. The policy, when deployed, removes the app profile from users' iOS or macOS devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

macOS settings



- **Profile ID:** Click the app profile ID in the drop-down list. This field is required.
- **Deployment scope:** Click **User** or **System** in the drop-down list. The default is **User**. This option is available only on macOS 10.7 and later.
- **Comment:** Type an optional comment.

Provisioning profile device policy

September 6, 2025

When you develop and code sign an iOS enterprise app, you usually include an enterprise distribution provisioning profile, which Apple requires for the app to run on an iOS device. If a provisioning profile is missing or has expired, the app crashes when a user taps to open it.

The primary problem with provisioning profiles is that they expire one year after they are generated on the Apple Developer Portal and you must keep track of the expiration dates for all your provisioning profiles on all iOS devices enrolled by your users. Tracking the expiration dates not only involves

© 1997–2025 Citrix Systems, Inc. All rights reserved.

keeping track of the actual expiration dates, but also which users are using which version of the app. Two solutions are to email provisioning profiles to users or to put them on a web portal for download and installation. These solutions work, but they're prone to error because they require users to react to instructions in an email or to go to the web portal and download the correct profile and then install it.

To make this process transparent to users, in Citrix Endpoint Management you can install and remove provisioning profiles with device policies. Missing or expired profiles are removed as necessary and the up-to-date profiles are installed on users' devices, so that tapping an app simply opens it for use.

Before you can create a provisioning profile policy, you must create a provisioning profile file. For more information, see the Apple article about how to create a development provisioning profile on the Apple Developer site.

iOS settings

- **iOS provisioning profile:** Select the provisioning profile file to import by clicking **Browse** and then navigating to the file location.

Provisioning profile removal device policy

September 6, 2025

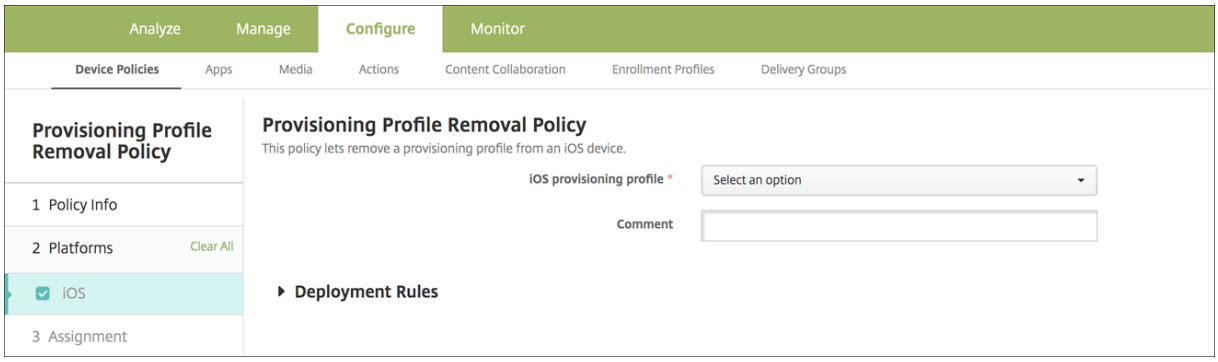
A provisioning profile lets you distribute iOS apps to user devices. Apple requires that you sign an app using a provisioning profile to authorize the app to run on iOS devices. For more information, see Provisioning profile device policy.

To remove or replace an older provisioning profile, use the Provisioning profile removal device policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS settings



- **iOS provisioning profile:** Click the provisioning profile in the drop-down list that you want to remove.
- **Comment:** Optionally, add a comment.

Proxy device policy

September 6, 2025

The Proxy device policy specifies global HTTP proxy settings for supported iOS devices. You can deploy only one global HTTP proxy policy per device.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Prerequisites

Before deploying this policy, be sure to set all iOS devices for which you want to set a global HTTP proxy into Supervised mode. For details, see Deploy devices using Apple Configurator 2 or Deploy devices through the Apple Deployment Program.

Set deployment rules to enroll devices before sending the Proxy policy to the devices.

iOS settings

- **Proxy configuration:** Click **Manual** or **Automatic** for how the proxy has to be configured on the users'devices.
  - If you click **Manual**, configure these settings:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

        * **Hostname or IP address for the proxy server:** Type the host name or IP address of the proxy server. This field is required.
        * **Port for the proxy server:** Type the proxy server port number. This field is required.
        * **User name:** Type an optional user name to authenticate to the proxy server.
        * **Password:** Type an optional password to authenticate to the proxy server.
    - If you click **Automatic**, configure these settings:
        * **Proxy PAC URL:** Type the URL of the PAC file that defines the proxy configuration.
        * **Allow direct connection if PAC is unreachable:** Select whether to allow users to connect directly to the destination if the PAC file is unreachable. The default is **On**.

- **Allow bypassing proxy to access captive networks:** Select whether to allow bypassing the proxy to access captive networks. The default is **Off**.
- **Policy settings**
    - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
        * **Select date:** Click the calendar to select the specific date for removal.
        * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

Restrictions device policy

September 5, 2025

> **Note:**
>
> When an upgrade includes new Restrictions device policy settings, you must edit and save the policy. Citrix Endpoint Management doesn't deploy the upgraded Restrictions device policy until you save it.

The Restrictions device policy allows or restricts certain features or functionality on user devices, such as the camera. You can set security restrictions and restrictions on media content. You can also set restrictions on the types of apps users can and can't install. Most of the restriction settings default to **On**, or *allows*. The main exceptions are the iOS Security - Force feature and all Windows Tablet features, which default to **Off**, or *restricts*.

Any option for which you select **On** means that the user can do the operation or use the feature. For example:

- **Camera:** If **On**, the user can use the camera on their device. If **Off**, the user can't use the camera on their device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Screenshots:** If **On**, the user can take screenshots on their device. If **Off**, the user can't take screenshots on their device.

If you have both the restrictions device policy and the kiosk device policy configured, the restrictions device policy takes precedence.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

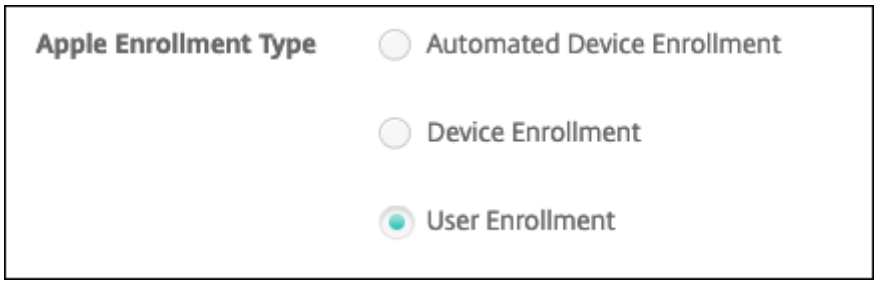
Some iOS restrictions policy settings apply only to specific versions of iOS, as noted here and in the Citrix Endpoint Management console Restrictions policy page.

These settings apply when the device is enrolled in user enrollment mode, unsupervised (full MDM) mode, or supervised mode. The following table shows the enrollment modes that are available for each setting for iOS 13 and later.

- **Automated Device Enrollment:** Supervised devices. These are the devices that are enrolled through bulk enrollment.
- **Device Enrollment:** Unsupervised devices. These devices are individually enrolled and the entire device is fully MDM.
- **User Enrollment:** Devices on which only specific users are managed. For more information about User Enrollment, see the Apple documentation.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS Restrictions policy settings might apply when the device is enrolled in user enrollment mode, unsupervised (full MDM) mode, or supervised mode. The following table shows the enrollment modes that are available for each Restrictions policy setting for iOS 13 and later.



As noted in the table, some settings that were previously available in unsupervised and supervised mode are available only in supervised mode starting with iOS 13. The following rules apply:

- If a supervised iOS 13+ device enrolls in Citrix Endpoint Management, the settings apply to the device.
- If an unsupervised iOS 13+ device enrolls in Citrix Endpoint Management, the settings don't apply to the device.
- If an iOS 12 (or lower) device already enrolled in Citrix Endpoint Management and then upgrades to iOS 13, there are no changes. The settings apply to the device as they did before the upgrade.

For information on setting an iOS device to supervised mode, see Deploy devices using Apple Configurator 2.

Setting	User Enrollment	Unsupervised	Supervised
Allow hardware controls			
Camera	No	Yes	Yes
FaceTime	No	No	Yes
Allow FaceTime Remote Control	No	No	Yes
Screen captures	Yes	No	Yes
Allow the Classroom app to remotely observe student screens	No	No	Yes
Allow the Classroom app to perform AirPlay and View Screen without prompting	No	No	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	User Enrollment	Unsupervised	Supervised
Photo streams	No	Yes	Yes
Shared photo streams	No	Yes	Yes
Allow shared iPad temporary session	No	No	Yes
Voice dialing	No	Yes	Yes
Siri	Yes	Yes	Yes
Allow while device is locked	Yes	Yes	Yes
Siri profanity filter	No	No	Yes
Installing apps	No	No	Yes
Alternative App Marketplace	No	No	Yes
Web Distribution apps	No	No	Yes
Allow global background fetch while roaming	No	Yes	Yes
Allow apps			
iTunes Store	No	No	Yes
In-app purchases	No	Yes	Yes
Require iTunes Store password for purchases	No	Yes	Yes
Safari	No	No	Yes
Autofill	No	No	Yes
Force fraud warning	Yes	Yes	Yes
Enable JavaScript	No	Yes	Yes
Block pop-ups	No	Yes	Yes
Accept cookies	No	Yes	Yes
Network - Allow iCloud actions			
iCloud documents and data	No	No	Yes
iCloud backup	No	Yes	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	User Enrollment	Unsupervised	Supervised
iCloud photo keychain	No	Yes	Yes
iCloud photo library	No	Yes	Yes
Security - Force			
Encrypted backups	Yes	Yes	Yes
Limited ad tracking	No	Yes	Yes
Passcode on first AirPlay pairing	Yes	Yes	Yes
Paired Apple Watch to use Wrist Detection	Yes	Yes	Yes
Sharing managed documents using AirDrop	Yes	Yes	Yes
Security - Allow			
Accepting untrusted SSL certificates	No	Yes	Yes
Automatic update to certificate trust settings	No	Yes	Yes
Require managed pasteboard	Yes	Yes	Yes
Documents from managed apps in unmanaged apps	Yes	Yes	Yes
Unmanaged apps read managed contacts	No	No	Yes
Managed apps write unmanaged contacts	No	No	Yes
Documents from unmanaged apps in managed apps	Yes	Yes	Yes
Diagnostic submission to Apple	Yes	Yes	Yes
Touch ID to unlock device	No	Yes	Yes
Auto unlock	No	Yes	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	User Enrollment	Unsupervised	Supervised
Wallet notifications when locked	No	Yes	Yes
Handoff	No	Yes	Yes
iCloud sync for managed apps	Yes	Yes	Yes
Backup for enterprise books	Yes	Yes	Yes
Notes and highlights sync for enterprise books	Yes	Yes	Yes
Internet results in Spotlight	No	Yes	Yes
Enterprise app trust	No	Yes	Yes
Allow Apple personalized advertising	No	Yes	Yes
Supervised only settings - Allow			
Allow eSIM modification	No	No	Yes
Preserve eSIM on erase	No	No	Yes
Erase all content and settings	No	No	Yes
Screen Time	No	No	Yes
Podcasts	No	No	Yes
Installing configuration profiles	No	No	Yes
Touch ID and Face ID modification	No	No	Yes
Installing apps from device	No	No	Yes
Keyboard shortcuts	No	No	Yes
Paired Apple watch	No	No	Yes
Passcode modification	No	No	Yes
Device name modification	No	No	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	User Enrollment	Unsupervised	Supervised
Wallpaper modification	No	No	Yes
Automatically downloading apps	No	No	Yes
AirDrop	No	No	Yes
iMessage	No	No	Yes
Siri user-generated content	No	No	Yes
iBooks	No	No	Yes
Removing apps	No	Yes	Yes
Game Center	No	No	Yes
Add friends	No	No	Yes
Multiplayer gaming	No	No	Yes
Modifying account settings	No	No	Yes
Modifying app cellular data settings	No	No	Yes
Modifying app cellular data settings	No	No	Yes
Allow network drive connections	No	No	Yes
Allow USB device connections	No	No	Yes
Allow Find My Device	No	No	Yes
Allow Find My Friends settings	No	No	Yes
Modifying Find My Friends settings	No	No	Yes
Pairing with non-Configurator hosts	No	No	Yes
Predictive keyboards	No	No	Yes
Keyboard auto-corrections	No	No	Yes
Keyboard spell-check	No	No	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	User Enrollment	Unsupervised	Supervised
Allow QuickPath Keyboard	No	No	Yes
Definition lookup	No	No	Yes
Single App bundle ID	No	No	Yes
News	No	No	Yes
Apple Music service	No	No	Yes
Apple Music Radio	No	No	Yes
Notifications modification	No	No	Yes
Restricted App usage	No	No	Yes
Diagnostic submission modification	No	No	Yes
Bluetooth modification	No	No	Yes
Allow dictation	No	No	Yes
Modify whether Wi-Fi is on or off	No	No	Yes
Join only Wi-Fi networks installed by a network policy	No	No	Yes
Allow the Classroom app to perform AirPlay and View Screen without prompting	No	No	Yes
Allow the Classroom app to lock to an app and lock the device without prompting	No	No	Yes
Automatically join the Classroom app classes without prompting	No	No	Yes
Allow AirPrint	No	No	Yes
Allow storage of AirPrint credentials in Keychain	No	No	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	User Enrollment	Unsupervised	Supervised
Allow discovery of AirPrint printers by using iBeacons	No	No	Yes
Allow AirPrint only to destinations with trusted certificates	No	No	Yes
Adding VPN configurations	No	No	Yes
Modifying cellular plan settings	No	No	Yes
Removing system apps	No	No	Yes
Setting up new nearby devices	No	No	Yes
Allow USB restricted mode	No	No	Yes
Force delayed software updates	No	No	Yes
Enforced software update delay	No	No	Yes
Force classroom request permission to leave classes	No	No	Yes
Force authentication before autofill	No	No	Yes
Force automatic date and time	No	No	Yes
Password AutoFill	No	No	Yes
Password proximity requests	No	No	Yes
Password Sharing	No	No	Yes
Allow personal hotspot modification	No	No	Yes
Allow boot to recovery by an unpaired device	No	No	Yes
Install rapid security response	No	No	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	User Enrollment	Unsupervised	Supervised
Remove rapid security response	No	No	Yes
Allow mail privacy protection	No	No	Yes
NFC	No	No	Yes
Allow App clips	No	No	Yes
Genmoji	No	No	Yes
Image Playground	No	No	Yes
Image Wand	No	No	Yes
iPhone Mirroring	No	No	Yes
Personalized Handwriting Results	No	No	Yes
Writing Tools	No	No	Yes
Call Recording	No	No	Yes
Apps To Be Hidden	No	No	Yes
Apps To Be Locked	No	No	Yes
Mail Summary	No	No	Yes
RCS Messaging	No	No	Yes
Allow external intelligence integrations	No	No	Yes
Allow signing in to external intelligence integrations	No	No	Yes
Allow Mail Smart Replies	No	No	Yes
Allow Notes Transcription	No	No	Yes
Allow Safari Summary	No	No	Yes
Allow visual intelligence summary	No	No	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	User Enrollment	Unsupervised	Supervised
Allow Notes Transcritpion Summary	No	No	Yes
Allow Apple Intelligence Report	No	No	Yes
Allow Default Calling App Modification	No	No	Yes
Allow Default Messaging App Modification	No	No	Yes
Allow External Intelligence Workspace IDs	No	No	Yes
Default Browser Modification	No	No	Yes
Allow Live Voicemail	No	No	Yes
Security - Show in lock screen			
Control Center	Yes	Yes	Yes
Notification	Yes	Yes	Yes
Today view	Yes	Yes	Yes
Media content - Allow			
Explicit music, podcasts, and iTunes U material	No	No	Yes
Explicit sexual content in iBooks	No	Yes	Yes
Ratings region	No	Yes	Yes
Movies	No	Yes	Yes
TV Shows	No	Yes	Yes
Apps	No	Yes	Yes

- **Allow hardware controls**
  - **Camera:** Allow users to use the camera on their devices.
    - **FaceTime:** Allow users to use FaceTime on their devices. For supervised iOS devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    - **Allow FaceTime Remote Control:** Allow a remote FaceTime session to request control of the device. For supervised iOS devices. Available for iOS 18.4 and later.
  - **Screen captures:** Allow users to take screenshots on their devices.
    - **Allow the Classroom app to remotely observe student screens:** If this restriction is unselected, an instructor can't use the Classroom app to remotely observe student screens. The default setting is selected, an instructor can use the Classroom app to observe student screens. The setting for **Allow the Classroom app to perform AirPlay and View Screen without prompting** determines whether students receive a prompt to give the instructor permission. For supervised iOS devices.
    - **Allow the Classroom app to perform AirPlay and View Screen without prompting:** If this restriction is selected, the instructor can do AirPlay and View Screen on a student device, without prompting for permission. The default setting is unselected. For supervised iOS devices.
  - **Photo streams:** Allow users to use MyPhotoStream to share photos through iCloud to all their iOS devices.
  - **Shared photo streams:** Allow users to use iCloud Photo Sharing to share photos with coworkers, friends, and family.
  - **Allow shared iPad temporary session:** Prevents access to temporary sessions on shared iPads.
  - **Voice dialing:** Enables voice dialing on user devices.
  - **Siri:** Allows users to use Siri.
    - **Allow while device is locked:** Allow users to use Siri while their devices are locked.
    - **Siri profanity filter:** Enable the Siri profanity filter. The default is to restrict this feature, which means no profanity filtering is done.
      For more information about Siri and security, see Siri and dictation policies.
  - **Installing apps:** Allow users to install apps. For supervised iOS devices.
  - **Alternative App Marketplace:** Prevents installation of alternative marketplace apps from the web and prevents any installed alternative marketplace apps from installing apps. This feature is available from iOS 17.4 and later versions. Default is **On**. For supervised iOS devices.
  - **Web Distribution apps:** Enable customer admins to block the web distributed third party apps on iOS devices. This is applicable for iOS versions 17.5 and later. For more information, see Restrictions.
  - **Allow global background fetch while roaming:** Allow devices to automatically sync mail accounts to iCloud while the device is roaming. When **Off**, disables global background fetch activity when an iOS phone is roaming. Defaults to **On**.

- **Allow apps**
  - **iTunes Store:** Allow users to access the iTunes Store. For supervised iOS devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **In-app purchases:** Allow users to make in-app purchases.
    - **Require iTunes Store password for purchases:** Require a password for in-app purchases. The default is to restrict this feature, which means no password is required for in-app purchases.
  - **Safari:** Allow users to access Safari. For supervised iOS devices.
    - **Autofill:** Allow users to set up autofill for user names and passwords on Safari.
    - **Force fraud warning:** If this setting is enabled and users visit a suspected phishing website, Safari alerts users. The default is to restrict this feature, which means no warnings are issued.
    - **Enable JavaScript:** Allow JavaScript to run on Safari.
    - **Block pop-ups:** Block pop-ups while viewing websites. The default is to restrict this feature, which means pop-ups aren't blocked.
  - **Accept cookies:** Set to what extent cookies are accepted. In the list, choose an option to allow or restrict cookies. The default option is **Always**, which allows all websites to save cookies in Safari. Other options are **Current website only**, **Never**, and **From visited sites only**.

- **Network - Allow iCloud actions**
  - **iCloud documents and data:** Allow users to sync documents and data to iCloud. For supervised iOS devices.
  - **iCloud backup:** Allow users to back up their devices to iCloud.
  - **iCloud keychain:** Allow users to store passwords, Wi-Fi network, credit card, and other information in the iCloud Keychain.
  - **Cloud photo library:** Allow users to access their iCloud photo library.

- **Security - Force**

  The default is to restrict the following features, which means no security features are enabled.
  - **Encrypted backups:** Force backups to iCloud to be encrypted.
  - **Limited ad tracking:** Block targeted ad tracking.
  - **Passcode on first Airplay pairing:** Require that AirPlay-enabled devices are verified with a one-time onscreen code before they can use AirPlay.
  - **Paired Apple Watch to use Wrist Detection:** Require a paired Apple Watch to use **Wrist Detection**.
  - **Sharing managed documents using AirDrop:** Setting this option to **On** makes AirDrop appear as an unmanaged drop target.

- **Security - Allow**
  - **Accepting untrusted SSL certificates:** Allow users to accept websites' untrusted SSL certificates.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Automatic update to certificate trust settings:** Allow trusted certificates to be updated automatically.
- **Require managed pasteboard:** Allow copy and paste functionality to follow the same restrictions that you apply to **Documents from managed apps in unmanaged apps** and **Documents from unmanaged apps in managed apps**.
  For example, you configure the following:
  * **Require managed pasteboard:** On
  * **Documents from managed apps in unmanaged apps:** Off
  * **Documents from unmanaged apps in managed apps:** On
    After you deploy the policy to iOS devices, users can't copy and paste data from managed apps to unmanaged apps, but they can copy and paste data from unmanaged apps to managed apps.
- **Documents from managed apps in unmanaged apps:** Allow users to move data from managed (corporate) apps to unmanaged (personal) apps.
- **Documents from unmanaged apps in managed apps:** Allow users to move data from unmanaged (personal) apps to managed (corporate) apps.
- **Diagnostic submission to Apple:** Allow anonymous diagnostic data about users' devices to be sent to Apple.
- **Touch ID or Face ID to unlock device:** Allow users to use Touch ID or Face ID to unlock their devices.
- **Auto unlock:** If **Off**, the user can't use the Apple watch to unlock a paired iPhone. Default is **On**. Available for iOS 14.5 and later.
- **Wallet notifications when locked:** Allow Wallet notifications to appear on the lock screen.
- **Handoff:** Allow users to transfer activities from one iOS device to another nearby iOS device.
- **iCloud sync for managed apps:** Allow users to sync managed apps to iCloud.
- **Backup for enterprise books:** Allow enterprise books to be backed up to iCloud.
- **Notes and highlights sync for enterprise books:** Allow notes and highlights users have added to enterprise books to be synced to iCloud.
- **Enterprise app trust:** Allow enterprise applications to be trusted. Enterprise apps are any apps that are custom-made for your organization. These apps can be made internally or they can be developed and bought from an external vendor. For additional information, see Install custom enterprise apps on iOS.
- **Internet results in Spotlight:** Allow Spotlight to show search results from the Internet in addition to the device.
- **Unmanaged apps read managed contacts:** Optional. Only available if **Documents from managed apps in unmanaged apps** is disabled. If this policy is enabled, unmanaged apps can read data from managed accounts' contacts. Default is **Off**. Available from iOS 12.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Managed apps write unmanaged contacts:** Optional. If enabled, allow managed apps to write contacts to unmanaged accounts' contacts. If **Documents from managed apps in unmanaged apps** is enabled, this restriction has no effect. Default is **Off**. Available from iOS 12.
- **Allow Apple personalized advertising:** If **Off**, the Apple advertising platform can't use the users' data to deliver personalized ads. Default is **On**. Available for iOS 14.0 and later.

- **Supervised only settings - Allow**

  These settings apply only to supervised devices. For the steps on setting an iOS device to supervised mode, see Deploy devices using Apple Configurator 2.

  - **Allow eSIM modification:** Allow users to change the eSIM settings on their device.
  - **Preserve eSIM on erase:** If **On**, the system preserves eSIM when it erases the device due to too many failed password attempts or the Erase All Content and Settings option in **Settings > General > Reset**. Default is **Off**.

  > **Note:**
  >
  > The system doesn't preserve eSIM if **Find My** initiates erasing the device.
  >
  > - **Erase all content and settings:** Allow users to erase all content and settings from their devices.
  > - **Screen Time:** Allow users to enable Screen Time.
  > - **Podcasts:** Allow users to download and sync podcasts.
  > - **Installing configuration profiles:** Allow users to install a configuration profile other than that the one deployed by you.
  > - **Touch ID and Face ID modification:** Allow users to change or delete their Touch ID or Face ID.
  > - **Installing apps from device:** Allow users to install apps. Disabling this setting stops end users from installing new apps. The App Store is disabled and its icon is removed from the Home Screen.
  > - **Keyboard shortcuts:** Allow users to create custom keyboard shortcuts for words or phrases that they use often.
  > - **Paired Apple watch:** Allow users to pair an Apple Watch to a supervised device.
  > - **Passcode modification:** Allow users to change the passcode on a supervised device.
  > - **Device name modification:** Allow users to change the name of their device.
  > - **Wallpaper modification:** Allow users to change the wallpaper on their devices.
  > - **Automatically downloading apps:** Allow apps to download.
  > - **AirDrop:** Allow users to share photos, videos, websites, locations, and more with nearby iOS devices.
  > - **iMessage:** Allow users to text over Wi-Fi with iMessage.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Siri user-generated content:** Allow Siri to query user-generated content from the web. Consumers, not traditional journalists; produce user-generated content. For example, content found on Twitter or Facebook is user-generated.
- **iBooks:** Allow users to use the iBooks app.
- **Removing apps:** Allow users to remove apps from their devices.
- **Game Center:** Allow users to play online games through Game Center on their devices.
  - **Add friends:** Allow users to send a notification to a friend to play a game.
  - **Multiplayer gaming:** Allow users to start multiplayer game play on their devices.
- **Modifying account settings:** Allow users to modify their device account settings.
- **Modifying app cellular data settings:** Allow users to modify how apps use cellular data.
- **Allow network drive connections:** Prevents connecting to network drives in the Files app.
- **Allow USB device connections:** Prevents connecting to any connected USB devices in the Files app.
- **Allow Find My Device:** Disables the **Find My Device** option in the Find My app.
- **Allow Find My Friends settings:** Disables the **Find My Friends** option in the Find My app.
- **Modifying Find My Friends settings:** Allow users to change their Find My Friends settings.
- **Pairing with non-Configurator hosts:** Allow the administrator to control to which devices a user device can pair. Disabling this setting prevents pairing except with the supervising host running the Apple Configurator. If no supervising host certificate is configured, all pairing is disabled.
- **Predictive keyboards:** Allow user devices to use the predictive keyboard for suggesting words as they type. Disable this option in situations such as administering standardized tests where you do not want users to have access to suggested words.
- **Keyboard auto-corrections:** Allow user devices to use keyboard autocorrect. Disable this option in situations such as administering standardized tests where you do not want users to have access to autocorrect.
- **Keyboard spell-check:** Allow user devices to use spell checking while typing. Disable this option in situations such as administering standardized tests where you do not want users to have access to the spell-checker.
- **Definition lookup:** Allow user devices to use definition look-up while typing. Disable this option in situations such as administering standardized tests where you don't want users to look up definitions as they type.
- **Single App bundle ID:** Create a list of apps allowed to keep control over the device and prevent interaction with other apps or functions.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> To add an app, click **Add**, type an **App name**, and click **Save**. Repeat that process for each app you want to add.
> - **News:** Allow users to use the News app.
> - **Apple Music service:** Allow users to use the Apple Music service. If you don't allow Apple Music service, the Music app runs in classic mode. Default is **On**. Available for iOS 9.3 or later.
> - **Apple Music Radio:** Allow users to use Apple Music Radio. Default is **On**. Available for iOS 9.3 or later.
> - **Notifications modification:** Allow users to modify notification settings.
> - **Restricted App usage:** Allow users to use all apps or to use or not use apps, based on the bundle IDs you provide. Applies only to supervised devices. If you select **Only allow some apps**, add an app with the bundle ID `com.apple.webapp` to allow web clips.

```
>**Note:**
>
>Beginning with iOS 11, Apple introduced changes to the policies
    that are available to app restrictions. Apple no longer lets
    you remove access to the Settings app and the Phone app by
    restricting the appropriate iOS application bundle.

After you configure the Restrictions device policy to block some
    apps and then deploy the policy: If you later want to allow
    some or all of those apps, changing and deploying the
    Restrictions device policy doesn't change the restrictions. In
     this case, iOS doesn't apply the changes to the iOS profile.
    To continue, use the Profile Removal policy to remove the iOS
    Profile and then deploy the updated Restrictions device policy
    .

If you change this setting to **Only allow some apps:** Before
    deploying this policy, advise users of devices enrolled using
    the Apple Deployment Program to sign in to their Apple
    accounts from the Setup Assistant. Otherwise, users might have
     to disable two-factor authentication on their devices to sign
     in to their Apple accounts and access-allowed apps.
```

- **Diagnostic submission modification:** Allow users to modify the diagnostic submission and app analytics settings in the **Settings > Diagnostics & Usage** pane.
- **Bluetooth modification:** Allow users to modify Bluetooth settings.
- **Allow dictation:** Supervised only. If this restriction is set to **Off**, dictation input isn't allowed, including speech-to-text. The default setting is **On**.
- **Modify whether Wi-Fi is on or off:** Prevents Wi-Fi from being turned on or off in the Settings or Control Center. Entering airplane mode has no effect also. This restriction does not prevent selecting which Wi-Fi network to use.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Join only Wi-Fi networks installed by a network policy:** Optional. Supervised only. If this restriction is set to **On**, the device can join Wi-Fi networks only when they were set up through a configuration profile. The default setting is **Off**.
- **Allow the Classroom app to perform AirPlay and View Screen without prompting:** If this restriction is selected, the instructor can perform AirPlay and View Screen on a student device, without prompting for permission. The default setting is unselected. For supervised iOS devices.
- **Allow the Classroom app to lock to an app and lock the device without prompting:** If this restriction is set to **On**, the Classroom app automatically locks user devices to an app and locks the device, without prompting the users. The default setting is **Off**. For supervised devices running iOS 11 (minimum version).
- **Automatically join the Classroom app classes without prompting:** If this restriction is set to **On**, the Classroom app automatically joins users to classes, without prompting the users. The default setting is **Off**. For supervised devices running iOS 11 (minimum version).
- **Allow AirPrint:** If this restriction is set to **Off**, users can't print with AirPrint. The default setting is **On**. When this restriction is **On**, these extra restrictions appear. For supervised devices running iOS 11 (minimum version).
  - **Allow storage of AirPrint credentials in Keychain:** If this restriction is unselected, the AirPrint user name and password aren't stored in the Keychain. The default setting is selected. For supervised devices running iOS 11 (minimum version).
  - **Allow discovery of AirPrint printers by using iBeacons:** If this restriction is unselected, iBeacon discovery of AirPrint printers is disabled. This setting prevents spurious AirPrint Bluetooth beacons from phishing for network traffic. The default setting is selected. For supervised devices running iOS 11 (minimum version).
  - **Allow AirPrint only to destinations with trusted certificates:** If this restriction is selected, users can use AirPrint to print only to destinations with trusted certificates. The default setting is unselected. For supervised devices running iOS 11 (minimum version).
- **Adding VPN configurations:** If this restriction is set to **Off**, users can't create VPN configurations. The default setting is **On**. For supervised devices running iOS 11 (minimum version).
- **Modifying cellular plan settings:** If this restriction is set to **Off**, users can't modify cellular plan settings. The default setting is **On**. For supervised devices running iOS 11 (minimum version).
- **Removing system apps:** If this restriction is set to **Off**, users can't remove system apps

© 1997–2025 Citrix Systems, Inc. All rights reserved.

from their device. The default setting is **On**. For supervised devices running iOS 11 (minimum version).

- **Setting up new nearby devices:** If this restriction is set to Off, users can't set up new nearby devices. The default setting is On. For supervised devices running iOS 11 (minimum version).
- **Allow USB restricted mode:** If **Off**, the device can always connect to USB accessories while locked. Default is **On**. Available only for supervised iOS 11.3 and later devices.
- **Force delayed software updates:** If **On**, delays user visibility of software updates. With this restriction in place, the user doesn't see a software update until the specified number of days after the software update release date. Default is **Off**. Available only for supervised iOS 11.3 and later devices. The OS update policy has more settings for controlling how often devices receive updates. See OS Update device policy.
- **Enforced software update delay (days):** Allows you to specify the number of days to delay a software update on the device. The maximum delay is **90** days. Default is **30** days. Available only for supervised iOS 11.3 and later devices.
- **Force classroom request permission to leave classes:** If **On**, a student enrolled in an unmanaged course with Classroom must request permission from the teacher when attempting to leave the course. Default is **Off**. Available only for supervised iOS 11.3 and later devices.
- **Force authentication before autofill:** Forces the user to authenticate before they can use the autofill feature.
- **Force automatic date and time:** Allows you to automatically set the date and time on supervised devices. If **On**, device users can't clear **Set Automatically** under **General > Date & Time**. The time zone on the device updates only when the device can determine its location. That is, when a device has a cellular connection or a Wi-Fi connection with location services enabled. Default is **Off**. Available only for supervised iOS 12 and later devices.
- **Password AutoFill:** Optional. If disabled, users can't use the AutoFill Passwords or Automatic Strong Passwords features. Default is **On**. Available from iOS 12.
- **Password proximity requests:** Optional. If disabled, users' devices don't request passwords from nearby devices. Default is **On**. Available from iOS 12.
- **Password Sharing:** Optional. If disabled, users can't share their passwords using the AirDrop Passwords feature. Default is **On**. Available from iOS 12.
- **Allow personal hotspot modification:** Prevents users from changing the personal hotspot settings.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Allow boot to recovery by an unpaired device:** If **On**, then allows the devices to be booted into recovery by an unpaired device. The default is **Off**. Available for iOS 14.5 and later.
- **Install rapid security response:** If **Off**, then prohibits the installation of rapid security responses. The default is **On**.
- **Remove rapid security response:** If **Off**, prohibits removal of rapid security responses. The default is **On**.
- **Allow mail privacy protection:** If **Off**, disables Mail Privacy Protection on the device. The default is **On**. Available for iOS 15.2 and later.
- **NFC:** If **Off**, disables NFC. The default is **On**. Available for iOS 14.2 and later.
- **Allow App clips**: If **Off**, prevents a user from adding any App Clips and removes any existing App Clips on the device. The default is **On**. Available for iOS 14.0 and later.
- **Genmoji:** If **Off**, prohibits creating new Genmoji. The default is **On**. Available for iOS 18 and later.
- **Image Playground:** If **Off**, prohibits the use of image generation. The default is **On**. Available for iOS 18 and later.
- **Image Wand:** If **Off**, prohibits the use of Image Wand. The default is **On**. Available for iOS 18 and later.
- **iPhone Mirroring:** If **Off**, prohibits the use of iPhone Mirroring and prevents the iPhone from mirroring to any Mac. The default is **On**. Available for iOS 18 and later.
- **Personalized Handwriting Results:** If **Off**, prevents the system from generating text in the user's handwriting. The default is **On**. Available for iOS 18 and later.
- **Writing Tools:** If **Off**, disables Apple Intelligence writing tools. The default is **On**. Available for iOS 18 and later.
- **Call Recording:** If **Off**, disables call recording. The default is **On**. Available for iOS 18 and later.
- **Apps To Be Hidden:** If **Off**, prevents the user from hiding apps. It does not affect the ability to leave apps in the App Library while removing them from the home screen. The default is **On**. Available for iOS 18 and later.
- **Apps To Be Locked:** If **Off**, disables the ability for the user to lock apps. Since hiding apps requires locking them, disabling locking also disables hiding. The default is **On**. Available for iOS 18 and later.
- **Mail Summary:** If **Off**, disables the ability to manually create summaries of email messages. This does not affect automatic summary generation. The default is **On**. Available for iOS 18.1 and later.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **RCS Messaging:** If **Off**, prevents the use of RCS messaging. The default is **On**. Available for iOS 18.1 and later.
- **Allow external intelligence integrations:** If **Off**, disables the use of external, cloud-based intelligence services with Siri. The default is **On**. Available for iOS 18.2 and later.
- **Allow signing in to external intelligence integrations:** If **Off**, forces external intelligence providers into anonymous mode. If a user is already signed in to an external intelligence provider, applying this restriction will cause them to be signed out when the next request is attempted. The default is **On**. Available for iOS 18.2 and later.
- **Allow Mail Smart Replies:** If **Off**, disables smart replies in Mail. The default is **On**. Available for iOS 18.2 and later.
- **Allow Notes Transcription:** If **Off**, disables transcription in Notes. The default is **On**. Available for iOS 18.2 and later.
- **Allow Safari Summary:** If **Off**, the system disables the ability to summarize content in Safari. The default is **On**. Available for iOS 18.4 and later.
- **Allow visual intelligence summary:** If **Off**, the system disables visual intelligence summarization. The default is **On**. Available for iOS 18.3 and later.
- **Allow Notes Transcritpion Summary:** If **Off**, disables transcription summarization in Notes. The default is **On**. Available for iOS 18.3 and later.
- **Allow Apple Intelligence Report:** If **Off**, the system disables Apple Intelligence reports. The default is **On**. Available for iOS 18.4 and later.
- **Allow Default Calling App Modification:** If **Off**, disables default calling app preference modification. The MDM Settings command to set the default calling app preference still works when this is applied. The default is **On**. Available for iOS 18.4 and later.
- **Allow Default Messaging App Modification:** If **Off**, disables default messaging app preference modification. The MDM Settings command to set the default messaging app preference still works when this is applied. The default is **On**. Available for iOS 18.4 and later.
- **Allow External Intelligence Workspace IDs:** An array of strings, but currently restricted to a single element. If present, Apple Intelligence only allows the given external integration workspace ID to be used, and requires a sign-in to make requests; the user will be required to sign in to integrations that support signing in. Multiple payloads combine using an intersect operation. This means the allowed set of workspace IDs can become the empty set if conflicting values are specified in multiple payloads. Available for iOS 18.3 and later.
  - **External Intelligence Workspace ID:** To add an external intelligence workspace ID, click **Add**, type an **External Intelligence Workspace ID**, and click **Save**. Repeat that process for each workspace ID you want to add.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Default Browser Modification:** If **Off**, disables default browser preference modification. The MDM Settings command to set the default browser preference will still work when this is applied. The default is **On**. Available for iOS 18.2 and later.
  - **Allow Live Voicemail:** If **Off**, the system disables live voicemail on the device. The default is **On**. Available for iOS 17.2 and later.

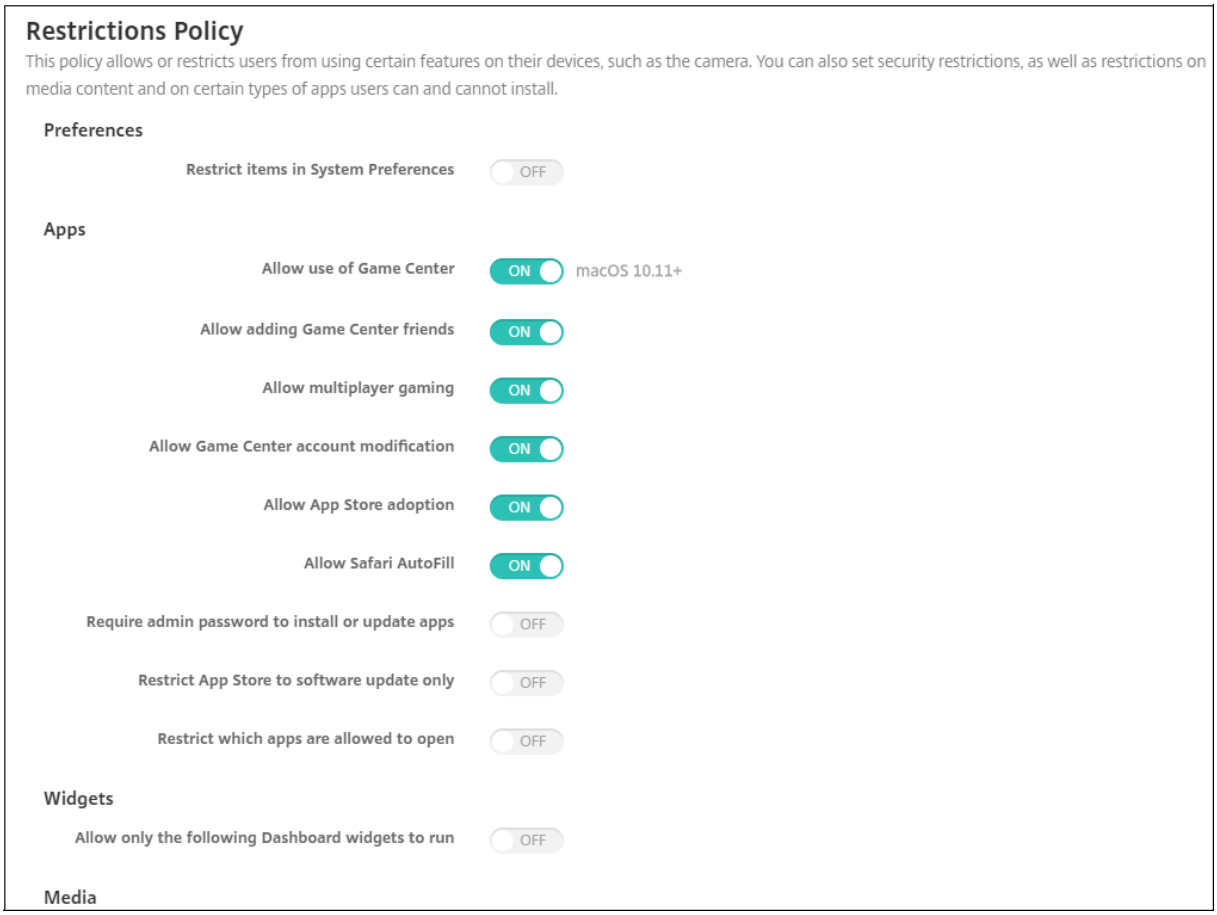
- **Security - Show in lock screen**
  - **Control Center:** Allow access to the Control Center on the lock screen. The Control Center lets users easily modify Airplane Mode, Wi-Fi, Bluetooth, Do Not Disturb Mode, and Lock Rotation settings.
  - **Notification:** Allow notifications on the lock screen.
  - **Today view:** Allow Today View, which aggregates information such as the weather and the current day's calendar items, on the lock screen.

- **Media content - Allow**
  - **Explicit music, podcasts, and iTunes U material:** Allow explicit material on users' devices.
  - **Explicit sexual content in iBooks:** Allow explicit material to be downloaded from iBooks.
  - **Ratings region:** Set the region from which parental control ratings are got. In the list, click a country to set the ratings region. The default is **United States**.
  - **Movies:** Set whether movies are allowed on users' devices. If movies are allowed, optionally set the ratings level for movies. In the list, click an option to allow or restrict movies on the device. The default is Allow all movies.
  - **TV Shows:** Set whether TV shows are allowed on users' devices. If TV shows are allowed, optionally set the ratings level for TV shows. In the list, click an option to allow or restrict TV shows on the device. The default is Allow all TV Shows.
  - **Apps:** Set whether apps are allowed on users' devices. If apps are allowed, optionally set the ratings level for apps. In the list, click an option to allow or restrict apps on the device. The default is Allow all apps.

- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on iOS 9.3 and later.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

macOS settings



Setting	Unsupervised	Supervised
Apps		
Allow use of Game Center	No	Yes
Allow adding Game Center friends	No	Yes
Allow multiplayer gaming	No	Yes
Allow Game Center account modification	Yes	Yes
Allow App Store adoption	Yes	Yes
Allow Safari Autofill	No	Yes
Require admin password to install or update apps	Yes	Yes
Restrict App Store to software update only	Yes	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	Unsupervised	Supervised
Restrict which apps are allowed to open	Yes	Yes
Media		
Allow AirDrop	No	Yes
Functionality		
Lock desktop picture	No	Yes
Allow use of camera	No	Yes
Allow Apple Music	No	Yes
Allow Spotlight Suggestions	Yes	Yes
Allow Look Up	Yes	Yes
Allow use of iCloud password for local accounts	Yes	Yes
Allow iCloud documents & data	Yes	Yes
Allow iCloud Desktop and Documents	No	Yes
Allow iCloud Keychain Sync	No	Yes
Allow iCloud Mail	Yes	Yes
Allow iCloud Contacts	Yes	Yes
Allow iCloud Calendars	Yes	Yes
Allow iCloud Reminders	Yes	Yes
Allow iCloud Bookmarks	Yes	Yes
Allow iCloud Notes	Yes	Yes
Allow iCloud Photos	Yes	Yes
Allow Auto Unlock	Yes	Yes
Allow Touch ID To Unlock Mac	Yes	Yes
Force delayed software updates	No	Yes
Password AutoFill	No	Yes
Password proximity requests	No	Yes
Password Sharing	Yes	Yes
Image Playground	No	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	Unsupervised	Supervised
iPhone Mirroring	No	Yes
Writing Tools	No	Yes
Allow Media Sharing Modification	Yes	Yes

- **Preferences**
  - **Restrict items in System Preferences:** Allow or restrict user access to System Preferences. The default is **Off**, which allows users full access to System Preferences. If enabled, configure the following settings.
    - **System Preference Pane:** Select whether the settings you select are enabled or disabled. The default is to enable all settings, which are **On** by default.
      - Users & Groups
      - General
      - Accessibility
      - App Store
      - Software Update
      - Bluetooth
      - CDs & DVDs
      - Date & Time
      - Desktop & Screen Saver
      - Displays
      - Dock
      - Energy Saver
      - Extensions
      - FibreChannel
      - iCloud
      - Ink
      - Internet Accounts
      - Keyboard
      - Language & Text
      - Mission Control
      - Mouse
      - Network
      - Notifications
      - Parental Controls
      - Printers & Scanners

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Profiles
- Security & Privacy
- Sharing
- Sound
- Dictation & Speech
- Spotlight
- Startup Disk
- Time Machine
- Trackpad
- Xsan

- **Apps**
  - **Allow use of Game Center:** Allow users to play online games through Game Center. The default is **On**.
  - **Allow adding Game Center friends:** Allow users to send a notification to a friend to play a game. The default is **On**.
  - **Allow multiplayer gaming:** Allow users to initiate multiplayer game play. The default is **On**.
  - **Allow Game Center account modification:** Allow users to modify their Game Center account settings. The default is **On**.
  - **Allow App Store adoption:** Allow or restrict the App Store to adopt apps that preexist in OS X. The default is **On**.
  - **Allow Safari Autofill:** Allow Safari to automatically populate fields on websites with passwords, addresses, and other basic information that it has stored. The default is **On**.
  - **Require admin password to install or update apps:** Require an administrator password to install or update apps. The default is **Off**, which means no administrator password is required.
  - **Restrict App Store to software update only:** Restrict the App Store to updates only, which disables all tabs in the App Store except Updates. The default is **Off**, which allows full App Store access.
  - **Restrict which apps are allowed to open:** Restrict or allow apps users can use. The default is Off, which allows all apps to be used. If enabled, configure the following settings:
    - **Allowed Apps:** Click **Add,** enter the name and bundle ID for an app allowed to launch, and then click **Save**. For Citrix mobile productivity apps, use the ID from the **Package ID** field when adding the app. Repeat this step for each app allowed to launch.
    - **Disallowed Folders:** Click **Add**, type the file path to a folder you want to restrict user access (for example, /Applications/Utilities), and then click **Save**. Repeat this step for all folders that you do not want users to be able to access.
    - **Allowed folders:** Click **Add**, type the file path to a folder to which you want to grant user access, and then click **Save**. Repeat this step for all folders that you want users

© 1997–2025 Citrix Systems, Inc. All rights reserved.

to be able to access.

- **Widgets**
  - **Allow only the following Dashboard widgets to run:** If **On**, users can only run the Dashboard widgets configured in this setting. The default is **Off**, which allows users to run all widgets. If enabled, configure the following setting:
    - **Allowed Widgets:** Click **Add**, type the name and ID of a widget that is allowed to run, and then click **Save**. Repeat this step for each widget that you want to run on the Dashboard.
- **Media**
  - **Allow AirDrop:** Allow users to share photos, videos, websites, locations, and more with nearby iOS devices.
- **Sharing**
  - **Automatically enable new sharing services:** Select whether to automatically enable sharing services.
  - **Mail:** Select whether to allow a shared mailbox.
  - **Facebook:** Select whether to allow a shared Facebook account.
  - **Video Services - Flickr, Vimeo, Tudou, and Youku:** Select whether to allow shared video services.
  - **Add to Aperture:** Select whether to allow shared ability to add to Aperture.
  - **Sina Weibo:** Select whether to allow a shared Sina Weibo account.
  - **Twitter:** Select whether to allow a shared Twitter account.
  - **Messages:** Select whether to allow shared access to messages.
  - **Add to iPhoto:** Select whether to allow shared ability to add to iPhoto.
  - **Add to Reading List:** Select whether to allow shared ability to add to Reading List.
  - **AirDrop:** Select whether to allow a shared AirDrop account.
- **Functionality**
  - **Lock desktop picture:** Select whether users can change the desktop picture. The default is **Off**, which means users can change the desktop picture.
  - **Allow use of camera:** Select whether users can use the camera on their Macs. The default is **Off**, which means users can't use the camera.
  - **Allow Apple Music:** Allow users to use the Apple Music service (macOS 10.12 and later). If you don't allow Apple Music service, the Music app runs in classic mode. Applies only to supervised devices. Defaults to **On**.
  - **Allow Spotlight Suggestions:** Select whether users can use Spotlight Suggestions to search their Mac and to provide Spotlight Suggestions from the Internet and the App Store. The default is **Off**, which prevents users from using Spotlight Suggestions.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Allow Look Up:** Select whether users can look up the definitions of words with the context menu or the Spotlight search menu. The default is Off, which prevents users from using Look Up on their Macs.
- **Allow use of iCloud password for local accounts:** Select whether users can use their Apple ID and iCloud password to sign on to their Macs. Enabling this policy means that users use only one ID and password for *all* login screens on their Macs. The default is **On**, which allows users to use their Apple ID and iCloud password to access their Macs.
- **Allow iCloud documents & data:** Select whether to allow users to access documents and data stored on iCloud on their Macs. The default is **On**, which prevents users from using iCloud documents and data on their Macs.
  * **Allow iCloud Desktop and Documents:** (macOS 10.12.4 and later) The default is selected.
- **Allow iCloud Keychain Sync:** Allow iCloud Keychain sync (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Mail:** Allow users to use iCloud Mail (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Contacts:** Allow users to use iCloud Contacts (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Calendars:** Allow users to use iCloud Calendars (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Reminders:** Allow users to use iCloud Reminders (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Bookmarks:** Allow users to sync with iCloud Bookmarks (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Notes:** Allow users to use Cloud Notes (macOS 10.12 and later). The default is **On**.
- **Allow iCloud Photos:** If you change this setting to **Off**, any photos not fully downloaded from the iCloud Photo Library are removed from local device storage (macOS 10.12 and later). The default is **On**.
- **Allow Auto Unlock:** For information about this option and Apple Watch, see https://www.imore.com/auto-unlock (macOS 10.12 and later). The default is **On**.
- **Allow Touch ID To Unlock Mac:** (macOS 10.12.4 and later). The default is **On**.
- **Force delayed software updates:** If **On**, this setting delays user visibility of software updates. Users don't see a software update until the specified number of days after the software update release date. Default is **Off**. Available only for supervised devices running macOS 10.13.4 and later. The OS update policy has more settings for controlling how often devices receive updates. See OS Update device policy.
- **Enforced software update delay (days):** Specifies how many days to delay a software update on the device. The maximum is 90 days. Default is **30**. Available only for supervised

© 1997–2025 Citrix Systems, Inc. All rights reserved.

devices running macOS 10.13.4 and later.

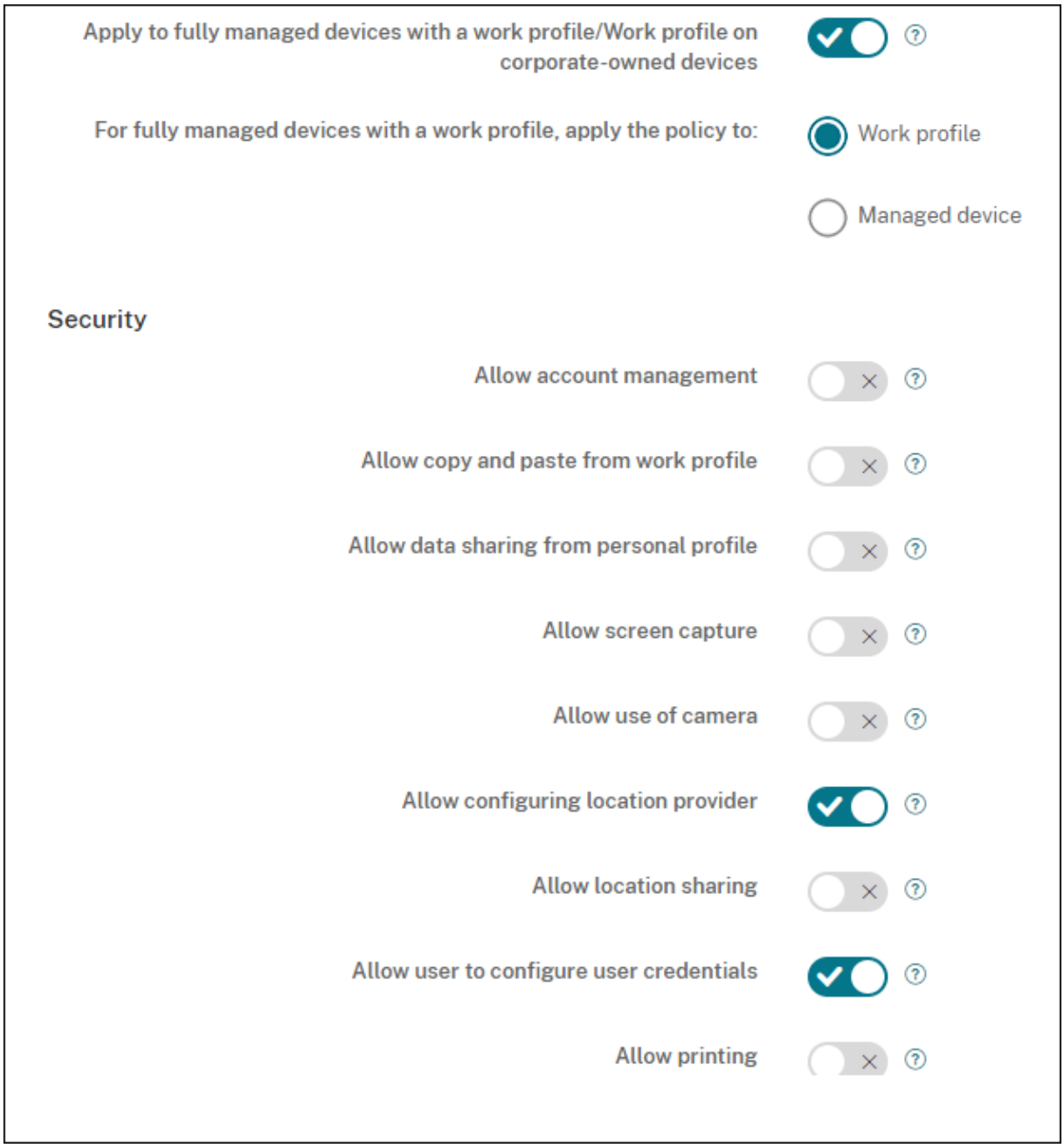
- **Password AutoFill:** Optional. If disabled, users cannot use the AutoFill Passwords or Automatic Strong Passwords features. Default is **On**. (macOS 10.14 and later)
- **Password proximity requests:** Optional. If disabled, users'devices don't request passwords from nearby devices. Default is **On**. (macOS 10.14 and later)
- **Password Sharing:** Optional. If disabled, users can't share their passwords using the AirDrop Passwords feature. Default is **On**. (macOS 10.14 and later)
- **Image Playground:** If **Off**, prohibits the use of image generation. Default is **On**. Available only for supervised devices running macOS 15 and later.
- **iPhone Mirroring:** If **Off**, prohibits the use of iPhone Mirroring. When used on macOS, this prevents the Mac from mirroring any iPhone. Default is **On**. Available only for supervised devices running macOS 15 and later.
- **Writing Tools:** If **Off**, disables Apple Intelligence writing tools. Default is **On**. Available only for supervised devices running macOS 15 and later.
- **Allow Media Sharing Modification:** If **Off**, prevents modification of Media Sharing settings. Default is **On**. Available for macOS 15.1 and later.

Android settings

- **Camera:** Allow users to use the camera on their devices. If **Off**, the camera is disabled. Defaults to **On**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Android Enterprise settings



When a new or factory reset Android device enrolls in work profile mode, devices running Android 9.0-10.x enroll as fully managed devices with a work profile. Devices running Android 11+ enroll as work profile on corporate-owned devices. The restriction policy can apply to either the work profile on the device or the managed device.

On devices enrolled in the work profile on corporate-owned devices mode, the following restrictions don't work:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Allow backup service
- Enable system apps
- Keep the keyguard from locking the device
- Allow use of the status bar
- Keep the device screen on
- Allow user control of application settings
- Allow user to configure user credentials
- Allow VPN configuration
- Allow USB mass storage
- Allow factory reset
- Allow app uninstall
- Allow non-Google Play apps
- Allow cross profile copy and paste
- Enable app verification
- Allow account management
- Allow printing
- Allow NFC
- Allow adding users

By default, the **USB Debugging and Unknown Sources** settings are disabled on a device when it is enrolled in Android Enterprise in work profile mode.

Watch this video to learn more:

- **Apply to fully managed devices with a work profile/Work profile on corporate-owned de-**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

vices: Allows Restrictions policy settings to be configured for fully managed devices with work profiles. These devices are also known as COPE (corporate owned personally enabled) devices. When this setting is **On**, select one of these settings:

- **Work profile:** The restrictions settings you configure apply only to the work profile on the device.
- **Managed device:** The restrictions settings you configure apply only to the device.

When this setting is **Off**, the credentials settings you configure apply to the device, except for settings that explicitly apply to the work profile. Default is **Off**.

When **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices** is off, configure the following settings:

- **Security**
  - **Allow account management:** Allows an account to be added to in work profile and managed devices. Default is **Off**.
  - **Allow copy and paste from work profile:** If **On**, users can copy and paste data from apps in the work profile to apps in the personal profile. Default is **Off**.
  - **Allow data sharing from personal profile:** If **On**, users can copy, paste, and share files and data from apps in the personal profile to apps in the work profile. Default is **Off**.
  - **Allow screen capture:** Allows users to record or take a screen capture of the device screen. Default is **Off**.
  - **Allow use of camera:** Allows users to take pictures and make videos with the device camera. Default is **Off**.
  - **Allow VPN configuration:** Allows users to create VPN configurations. For work profile devices running Android 6 and later and for fully managed devices. Default is **On**.
  - **Allow backup service:** Allows users to back up application and system data on their devices. Default is **On**.
  - **Allow NFC:** Allow users to send webpages, photos, videos, or other content from their devices to another device using Near Field Communication (NFC). For MDM 4.0 and later. Default is **On**.
  - **Allow configuring location provider:** Allows users to turn on GPS on their devices. For Android API 28 and later. Default is **On**.
  - **Allow location sharing:** For managed profiles, the device owner can override this setting. Default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Tip:**
>
> You can create Location device policies in Citrix Endpoint Management to enforce geographic boundaries. See Location device policy.

- **Allow user to configure user credentials:** Specify whether users can configure credentials in the managed keystore. Default is **On**.
- **Allow printing:** If **On**, the setting allows users to print to any printer accessible from the user device. The default is **Off**. Available for: Android 9 and later.
- **Allow USB debugging:** Default is **Off**.

- **Apps**
  - **Enable system apps:** Allows users to run pre-installed device apps. Default is **Off**. To enable specific apps, click **Add** in the **System apps list** table.
    - **System apps list:** A list of the system apps you want to enable on the device. Set **Enable system apps** to **On** and add the app package name. To look up the package name for a system app, you can use the Android Debug Bridge (adb) to call the Android package manager (pm) command. For example, `adb shell "pm list packages -f name"`, where "name"is part of the package name. For more information, see https://developer.android.com/studio/command-line/adb. For Android Enterprise devices, you can restrict app permissions using the Android Enterprise app permissions policy.
  - **Disable applications:** Blocks a specified list of apps from running on devices. Default is **Off**. To disable an installed app, change the setting to **On** and then click **Add** in the **Application list** table.
    - **Application list:** A list of the apps you want to block. Set **Disable applications** to **On** and add the app. Type the app package name. Changing and deploying an app list overwrites the prior app list. For example: If you disable com.example1 and com.example2, and then later change the list to com.example1 and com.example3, Citrix Endpoint Management enables com.example.2.
  - **Enable app verification:** Enables the OS to scan apps to detect malicious behavior. Default is **On**.
  - **Enable Google apps:** Allows users to download apps from Google Mobile Services onto the device. Default is **On**.
  - **Allow non-Google Play apps:** Allows the installation of apps from stores other than Google Play. Default is **Off**.
  - **Allow non-Google Play apps for all profiles:** If **On**, users can install apps from stores other than Google Play on all profiles on the device. Default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Allow user control of application settings:** Allows users to uninstall apps, disable apps, clear cache and data, force stop any app, and clear defaults. Users do these actions from the Settings app. Default is **Off**.
  - **Allow app uninstall:** Allows users to uninstall apps from within the Managed Google Play Store. Default is **Off**.

- **BYOD work profile**

  - **Enable connected apps:** If enabled, users can select apps that can communicate across work and personal profiles, using both work and personal data. After enabling, click **Add**, select the desired apps, then click **Save**. A work profile is required to enable this feature. Default is **Off**.
  - **Allow work profile app widgets on home screen:** If this setting is **On**, users can place work profile app widgets on the device home screen. If this setting is **Off**, users can't place work profile app widgets on the device home screen. Default is **Off**.
    * **Apps with allowed widgets:** A list of the apps you want to allow on the home screen. Set **Allow work profile app widgets on home screen** to **On** and add the app. Click **Add** and select an app whose widgets you want to allow on the home screen from the list. Click **Save**. Repeat that process to allow more app widgets.
  - **Allow work profile contacts in device contacts:** Shows contacts from the managed Android Enterprise profile in the parent profile, for incoming calls (Android 7.0 and later). Default is **Off**.

- **Fully managed device only**

  - **Allow adding users:** Allows users to add new users on a device. Default is **On**.
  - **Allow data roaming:** Allows users to use cellular data while roaming. The default is Off, which disables roaming on users' devices. Default is **Off**.
  - **Allow SMS:** Allows users to send and receive SMS messages. Default is **Off**.
  - **Allow use of the status bar:** If **On**, this setting enables the status bar on managed devices and dedicated devices (also known as COSU devices). This setting disables notifications, quick settings, and other screen overlays that allow escape from full-screen mode. Users can go to system settings and see notifications. For Android 6.0 and later. Default is **Off**.
  - **Allow Bluetooth:** Allows users to use Bluetooth. Default is **On**.
    * **Allow Bluetooth sharing:** If unselected, users can't establish outgoing Bluetooth sharing on their device. The default is selected.
  - **Allow configuring date and time:** Allows users to change the date and time on their devices. Default is **On**.
  - **Allow factory reset:** Allows users to do a factory reset on their devices. Default is **On**.
  - **Keep the device screen on:** If this setting is set to **On**, the device screen remains on when the device is plugged in. Default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Allow USB mass storage:** Allows transfer of large data files between users' devices and a computer over a USB connection. Default is **On**.
  - **Allow microphone:** Allows users to use the microphone on their devices. Default is **On**.
  - **Allow tethering:** Allows users to configure portable hotspots and tether data. Default is **Off**.
  - **Keep the keyguard from locking the device:** If **On**, this setting disables the keyguard on the lock screen on managed devices and dedicated devices (also known as COSU devices). Default is **Off**.
  - **Allow Wi-Fi changes:** If **On**, users can turn Wi-Fi on or off and connect to Wi-Fi networks. Default is **On**.
  - **Allow file transfer:** Allows file transfers over USB. Default is **Off**.

- **Samsung**

  - **Enable TIMA Keystore:** The TIMA Keystore provides TrustZone-based secure key storage for the symmetric keys. RSA key pairs and certificates are routed to the default key store provider for storage. Default is **Off**.
  - **Allow share list:** Allows users to share content between apps in the Share Via list. Default is **On**.
  - **Enable audit log:** Enables creation of event audit logs for forensic analysis of a device. Default is **Off**.

- **Samsung: Fully managed device only**

  - **Allow emergency calls only:** Allows users to enable Emergency Call Only mode on their devices. Default is **Off**.
  - **Allow firmware recovery:** Allows users to recover the firmware on their devices. Default is **On**.
  - **Allow fast encryption:** Allows encryption of only used memory space. This encryption contrasts full disk encryption, which encrypts all data. That data includes settings, application data, downloaded files and applications, media, and other files. Default is **On**.
  - **Enable Common Criteria mode:** Places the device into Common Criteria Mode. The Common Criteria configuration enforces stringent security processes. Default is **On**.
  - **Enable reboot banner:** Displays a DoD approved system use notification message or banner when users' devices are restarted. Default is **Off**.
  - **Allow settings changes:** Allows users to change settings on their fully managed devices. Default is **On**.
  - **Enable background data usage:** Allows apps to sync data in the background. for fully managed devices. Default is **On**.
  - **Allow clipboard:** Allow users to copy data to the clipboard on their devices.
    * **Allow clipboard share:** Allow users to share clipboard content between their devices and a computer (MDM 4.0 and later).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Allow home key:** Allows users to use the **Home** key on their fully managed devices. Default is **On**.
- **Allow mock location:** Allows users to fake their GPS location. For fully managed devices. Default is **Off**.
- **NFC:** Allows users to use NFC on their fully managed devices (MDM 3.0 and later). Default is **On**.
- **Allow power off:** Allows users to power off their fully managed devices (MDM 3.0 and later). Default is **On**.
- **Allow Wi-Fi direct:** Allows users to connect directly to another device through their Wi-Fi connection. Default is **On**. If **On**, you must enable the **Allow Wi-Fi changes** setting.
- **Allow SD card:** Allows users to use an SD card, if available, with their devices. Default is **On**.
- **Allow USB host storage:** Allows users'devices to act as the USB host when a USB device connects to their devices. Users'devices then supply power to the USB device. Default is **On**.
- **Allow voice dialer:** Allows users to use the voice dialer on their devices (MDM 4.0 and later). Default is **On**.
- **Allow S beam:** Allows users to share content with others using NFC and Wi-Fi Direct (MDM 4.0 and later). Default is **On**.
- **Allow S voice:** Allows users to use the intelligent personal assistant and knowledge navigator on their devices (MDM 4.0 and later). Default is **On**.
- **Allow USB tethering:** Allows users to share a mobile data connection with another device using their USB connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
- **Allow Bluetooth tethering:** Allows users to share a mobile data connection with another device using their Bluetooth connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
  - **Allow Bluetooth sharing:** If unselected, users can't establish outgoing Bluetooth sharing on their device. The default is selected.
- **Allow Wi-Fi tethering:** Allows users to share a mobile data connection with another device using their Wi-Fi connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
- **Allow incoming MMS:** Allows users to receive MMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Allow outgoing MMS:** Allows users to send MMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Allow incoming SMS:** Allows users to receive SMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Allow outgoing SMS:** Allows users to send SMS messages. Default is **Off**. If **On**, you must

© 1997–2025 Citrix Systems, Inc. All rights reserved.

turn on the **Allow SMS** setting.
- **Configure mobile networks:** Allows users to use their cellular data connection. Default is **Off**.
- **Limit by day (MB):** Enter the number of MB of mobile data users can use each day. The default is 0, which disables this feature (MDM 4.0 and later).
- **Limit by week (MB):** Enter the number of MB of mobile data users can use each week. The default is 0, which disables this feature (MDM 4.0 and later).
- **Limit by month (MB):** Enter the number of MB of mobile data users can use each month. The default is 0, which disables this feature (MDM 4.0 and later).
- **Allow only secure VPN connections:** Allows users to only use secure connections (MDM 4.0 and later). Default is **On**.
- **Allow audio recording:** Allows users to record audio with their devices (MDM 4.0 and later). Default is **On**. If **On** you must turn on the **Allow microphone** setting.
- **Allow video recording:** Allows users to record video with their devices (MDM 4.0 and later). Default is **Off**. If **On** you must turn on the **Allow use of camera** setting.
- **Allow push messages when roaming:** Allow users to use cellular data for pushing. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.
- **Allow automatic synchronization when roaming:** Allow users to use cellular data for syncing. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.
- **Allow voice calls when roaming:** Allow users to use cellular data for voice calls. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.

When **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices** is on and **For fully managed devices with a work profile, apply the policy to** is set to **Work profile**, configure these settings:

- **Security**
  - **Allow account management:** Allows an account to be added to in the work profile and managed devices. Default is **Off**.
  - **Allow cross profile copy and paste:** If **On**, users can copy and paste between apps in the Android Enterprise profile and apps in the personal area. Default is **Off**.
  - **Allow screen capture:** Allows users to record or take a screen capture of the device screen. Default is **Off**.
  - **Allow use of camera:** Allows users to take pictures and make videos with the device camera. Default is **Off**.
  - **Allow configuring location provider:** Allows users to turn on GPS on their devices. For Android API 28 and later. Default is **On**.
  - **Allow location sharing:** For managed profiles, the device owner can override this setting. Default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Tip:**
>
> You can create Location device policies in Citrix Endpoint Management to enforce geographic boundaries. See Location device policy.

- **Allow user to configure user credentials:** Specify whether users can configure credentials in the managed keystore. Default is **On**.
- **Allow printing:** If **On**, the setting allows users to print to any printer accessible from the user device. The default is **Off**. Available for: Android 9 and later.

- **Apps**
  - **Enable system apps:** Allows users to run pre-installed device apps. Default is **Off**. To enable specific apps, click **Add** in the **System apps list** table.
    - **System apps list:** A list of the system apps you want to enable on the device. Set **Enable system apps** to **On** and add the app package name. To look up the package name for a system app, you can use the Android Debug Bridge (adb) to call the Android package manager (pm) command. For example, `adb shell "pm list packages -f name"`, where "name"is part of the package name. For more information, see https://developer.android.com/studio/command-line/adb. For Android Enterprise devices, you can restrict app permissions using the Android Enterprise app permissions policy.
  - **Disable applications:** Blocks a specified list of apps from running on devices. Default is **Off**. To disable an installed app, change the setting to **On** and then click **Add** in the **Application list** table.
    - **Application list:** A list of the apps you want to block. Set **Disable applications** to **On** and add the app. Type the app package name. Changing and deploying an app list overwrites the prior app list. For example: If you disable com.example1 and com.example2, and then later change the list to com.example1 and com.example3, Citrix Endpoint Management enables com.example.2.
  - **Enable app verification:** Enables the OS to scan apps to detect malicious behavior. Default is **On**.
  - **Enable Google apps:** Allows users to download apps from Google Mobile Services onto the device. Default is **On**.
  - **Allow non-Google Play apps:** Allows the installation of apps from stores other than Google Play. Default is **Off**.
  - **Allow user control of application settings:** Allows users to uninstall apps, disable apps, clear cache and data, force stop any app, and clear defaults. Users perform these actions from the Settings app. Default is **Off**.
  - **Allow app uninstall:** Allows users to uninstall apps from within the Managed Google Play Store. Default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **BYOD work profile**
  - **Allow work profile app widgets on home screen:** If this setting is **On**, users can place work profile app widgets on the device home screen. If this setting is **Off**, users can't place work profile app widgets on the device home screen. Default is **Off**.
    - **Apps with allowed widgets:** A list of the apps you want to allow on the home screen. Set **Allow work profile app widgets on home screen** to **On** and add the app. Click **Add** and select an app whose widgets you want to allow on the home screen from the list. Click **Save**. Repeat that process to allow more app widgets.
  - **Allow work profile contacts in device contacts:** Shows contacts from the managed Android Enterprise profile in the parent profile, for incoming calls (Android 7.0 and later). Default is **Off**.
- **Samsung**
  - **Enable TIMA Keystore:** The TIMA Keystore provides TrustZone-based secure key storage for the symmetric keys. RSA key pairs and certificates are routed to the default key store provider for storage. Default is **Off**.
  - **Allow share list:** Allows users to share content between apps in the Share Via list. Default is **On**.
  - **Enable audit log:** Enables creation of event audit logs for forensic analysis of a device. Default is **Off**.

When **Apply to fully managed devices with a work profile/Work profile on corporate-owned devices** is on and **For fully managed devices with a work profile, apply the policy to** is set to **Managed device**, configure these settings:

- **Security**
  - **Allow account management:** Allows an account to be added to in the work profile and managed devices. Default is **Off**.
  - **Allow cross profile copy and paste:** If **On**, users can copy and paste between apps in the Android Enterprise profile and apps in the personal area. Default is **Off**.
  - **Allow screen capture:** Allows users to record or take a screen capture of the device screen. Default is **Off**.
  - **Allow use of camera:** Allows users to take pictures and make videos with the device camera. Default is **Off**.
  - **Allow VPN configuration:** Allows users to create VPN configurations. For work profile devices running Android 6 and later and for fully managed devices. Default is **On**.
  - **Allow backup service:** Allows users to back up application and system data on their devices. Default is **On**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Allow NFC:** Allow users to send webpages, photos, videos, or other content from their devices to another device using Near Field Communication (NFC). For MDM 4.0 and later. Default is **On**.
- **Allow configuring location provider:** Allows users to turn on GPS on their devices. For Android API 28 and later. Default is **On**.
- **Allow location sharing:** For managed profiles, the device owner can override this setting. Default is **Off**.

  > **Tip:**
  >
  > You can create Location device policies in Citrix Endpoint Management to enforce geographic boundaries. See Location device policy.

- **Allow user to configure user credentials:** Specify whether users can configure credentials in the managed keystore. Default is **On**.
- **Allow printing:** If **On**, the setting allows users to print to any printer accessible from the user device. The default is **Off**. Available for: Android 9 and later.
- **Allow USB debugging:** Default is **Off**.

- **Apps**
  - **Enable system apps:** Allows users to run pre-installed device apps. Default is **Off**. To enable specific apps, click **Add** in the **System apps list** table.
    - **System apps list:** A list of the system apps you want to enable on the device. Set **Enable system apps** to **On** and add the app package name. To look up the package name for a system app, you can use the Android Debug Bridge (`adb`) to call the Android package manager (`pm`) command. For example, `adb shell "pm list packages -f name"`, where "name"is part of the package name. For more information, see https://developer.android.com/studio/command-line/adb. For Android Enterprise devices, you can restrict app permissions using the Android Enterprise app permissions policy.
  - **Disable applications:** Blocks a specified list of apps from running on devices. Default is **Off**. To disable an installed app, change the setting to **On** and then click **Add** in the **Application list** table.
    - **Application list:** A list of the apps you want to block. Set **Disable applications** to **On** and add the app. Type the app package name. Changing and deploying an app list overwrites the prior app list. For example: If you disable com.example1 and com.example2, and then later change the list to com.example1 and com.example3, Citrix Endpoint Management enables com.example.2.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Enable app verification:** Enables the OS to scan apps to detect malicious behavior. Default is **On**.
- **Enable Google apps:** Allows users to download apps from Google Mobile Services onto the device. Default is **On**.
- **Allow non-Google Play apps:** Allows the installation of apps from stores other than Google Play. Default is **Off**.
- **Allow user control of application settings:** Allows users to uninstall apps, disable apps, clear cache and data, force stop any app, and clear defaults. Users perform these actions from the Settings app. Default is **Off**.
- **Allow app uninstall:** Allows users to uninstall apps from within the Managed Google Play Store. Default is **Off**.

- **Fully managed device only**
  - **Allow adding users:** Allows users to add new users on a device. Default is **On**.
  - **Allow data roaming:** Allows users to use cellular data while roaming. The default is Off, which disables roaming on users' devices. Default is **Off**.
  - **Allow SMS:** Allows users to send and receive SMS messages. Default is **Off**.
  - **Allow use of the status bar:** If **On**, this setting enables the status bar on managed devices and dedicated devices (also known as COSU devices). This setting disables notifications, quick settings, and other screen overlays that allow escape from full-screen mode. Users can go to system settings and see notifications. For Android 6.0 and later. Default is **Off**.
  - **Allow Bluetooth:** Allows users to use Bluetooth. Default is **On**.
    - **Allow Bluetooth sharing:** If unselected, users can't establish outgoing Bluetooth sharing on their device. The default is selected.
  - **Allow configuring date and time:** Allows users to change the date and time on their devices. Default is **On**.
  - **Allow factory reset:** Allows users to do a factory reset on their devices. Default is **On**.
  - **Allow factory reset protection:** If set to **On**, when the device is reset using recovery mode, the user must provide credentials for the account that was on the device before the reset. They can also provide the device lock if one was set before the reset. If set to **Off**, authentication isn't required after a reset. The default is **On**.
  - **Keep the device screen on:** If this setting is set to **On**, the device screen stays on when the device is plugged in. Default is **Off**.
  - **Allow USB mass storage:** Allows transfer of large data files between users' devices and a computer over a USB connection. Default is **On**.
  - **Allow microphone:** Allows users to use the microphone on their devices. Default is **On**.
  - **Allow tethering:** Allows users to configure portable hotspots and tether data. Default is **Off**. When this setting is on, these settings are available for Samsung devices:
  - **Keep the keyguard from locking the device:** If **On**, this setting disables the keyguard on

© 1997–2025 Citrix Systems, Inc. All rights reserved.

the lock screen on managed devices and dedicated devices (also known as COSU devices). Default is **Off**.
  - **Allow Wi-Fi changes:** If **On**, users can turn Wi-Fi on or off and connect to Wi-Fi networks. Default is **On**.
  - **Allow file transfer:** Allows file transfers over USB. Default is **Off**.

- **Samsung**
  - **Enable TIMA Keystore:** The TIMA Keystore provides TrustZone-based secure key storage for the symmetric keys. RSA key pairs and certificates are routed to the default key store provider for storage. Default is **Off**.
  - **Allow share list:** Allows users to share content between apps in the Share Via list. Default is **On**.
  - **Enable audit log:** Enables creation of event audit logs for forensic analysis of a device. Default is **Off**.

- **Samsung: Fully managed device only**
  - **Allow emergency calls only:** Allows users to enable Emergency Call Only mode on their devices. Default is **Off**.
  - **Allow firmware recovery:** Allows users to recover the firmware on their devices. Default is **On**.
  - **Allow fast encryption:** Allows encryption of only used memory space. This encryption contrasts full disk encryption, which encrypts all data. That data includes settings, application data, downloaded files and applications, media, and other files. Default is **On**.
  - **Enable Common Criteria mode:** Places the device into Common Criteria Mode. The Common Criteria configuration enforces stringent security processes. Default is **On**.
  - **Enable reboot banner:** Displays a DoD approved system use notification message or banner when users' devices are restarted. Default is **Off**.
  - **Allow settings changes:** Allows users to change settings on their fully managed devices. Default is **On**.
  - **Enable background data usage:** Allows apps to sync data in the background. for fully managed devices. Default is **On**.
  - **Allow clipboard:** Allow users to copy data to the clipboard on their devices. Default is **On**.
    - **Allow clipboard share:** Allow users to share clipboard content between their devices and a computer (MDM 4.0 and later).
  - **Allow home key:** Allows users to use the **Home** key on their fully managed devices. Default is **On**.
  - **Allow mock location:** Allows users to fake their GPS location. For fully managed devices. Default is **Off**.
  - **NFC:** Allows users to use NFC on their fully managed devices (MDM 3.0 and later). Default is **On**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

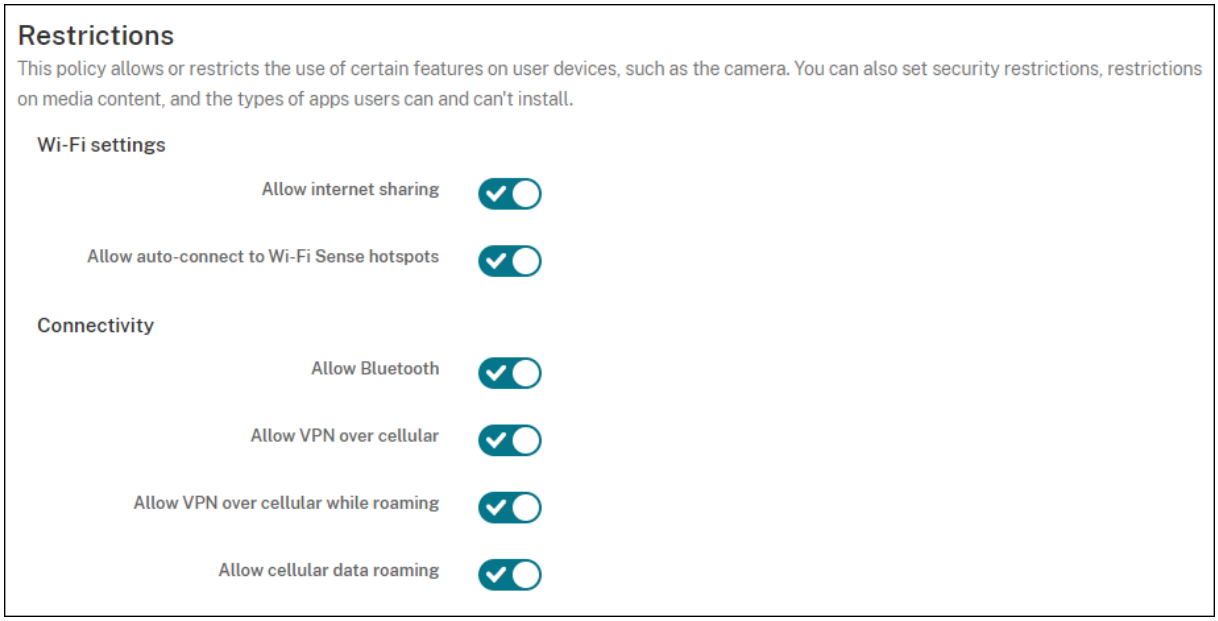
- **Allow power off:** Allows users to power off their fully managed devices (MDM 3.0 and later). Default is **On**.
- **Allow Wi-Fi direct:** Allows users to connect directly to another device through their Wi-Fi connection. Default is **On**. If **On**, you must enable the **Allow Wi-Fi changes** setting.
- **Allow SD card:** Allows users to use an SD card, if available, with their devices. Default is **On**.
- **Allow USB host storage:** Allows users' devices to act as the USB host when a USB device connects to their devices. Users' devices then supply power to the USB device. Default is **On**.
- **Allow voice dialer:** Allows users to use the voice dialer on their devices (MDM 4.0 and later). Default is **On**.
- **Allow S beam:** Allows users to share content with others using NFC and Wi-Fi Direct (MDM 4.0 and later). Default is **On**.
- **Allow S voice:** Allows users to use the intelligent personal assistant and knowledge navigator on their devices (MDM 4.0 and later). Default is **On**.
- **Allow USB tethering:** Allows users to share a mobile data connection with another device using their USB connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
- **Allow Bluetooth tethering:** Allows users to share a mobile data connection with another device using their Bluetooth connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
- **Allow Wi-Fi tethering:** Allows users to share a mobile data connection with another device using their Wi-Fi connection. The default is **Off**. If **On** the **Allow tethering** setting must be **On** as well.
- **Allow incoming MMS:** Allows users to receive MMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Allow outgoing MMS:** Allows users to send MMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Allow incoming SMS:** Allows users to receive SMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Allow outgoing SMS:** Allows users to send SMS messages. Default is **Off**. If **On**, you must turn on the **Allow SMS** setting.
- **Configure mobile networks:** Allows users to use their cellular data connection. Default is **Off**.
- **Limit by day (MB):** Enter the number of MB of mobile data users can use each day. The default is 0, which disables this feature (MDM 4.0 and later).
- **Limit by week (MB):** Enter the number of MB of mobile data users can use each week. The default is 0, which disables this feature (MDM 4.0 and later).
- **Limit by month (MB):** Enter the number of MB of mobile data users can use each month.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The default is 0, which disables this feature (MDM 4.0 and later).

- **Allow only secure VPN connections:** Allows users to only use secure connections (MDM 4.0 and later). Default is **On**.
- **Allow audio recording:** Allows users to record audio with their devices (MDM 4.0 and later). Default is **On**. If **On** you must turn on the **Allow microphone** setting.
- **Allow video recording:** Allows users to record video with their devices (MDM 4.0 and later). Default is **Off**. If **On** you must turn on the **Allow use of camera** setting.
- **Allow push messages when roaming:** Allow users to use cellular data for pushing. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.
- **Allow automatic synchronization when roaming:** Allow users to use cellular data for syncing. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.
- **Allow voice calls when roaming:** Allow users to use cellular data for voice calls. Default is **Off**. If **On**, you must enable the **Allow data roaming** setting.

Windows Desktop/Tablet settings



- **Wi-Fi Settings**
  - **Allow Internet sharing:** Allow a device to share its internet connection with other devices by turning it into a Wi-Fi hotspot.
- **Connectivity**
  - **Allow bluetooth:** Allow the device to connect through Bluetooth.
  - **Allow VPN over cellular:** Allow the device to connect over VPN to a cellular network.
  - **Allow VPN over cellular while roaming:** Allow the device to connect over VPN when the device roams over cellular networks.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Allow cellular data roaming:** Allow users to use cellular data while roaming.

- **Accounts**

  - **Allow Microsoft account connection:** Allow the device to use a Microsoft account for non-email related connection authentication and services.
  - **Allow non-Microsoft email:** Allow user to add non-Microsoft email accounts.

- **System**

  - **Allow storage card:** Allow the device to use a storage card.
  - **Telemetry:** Click an option in the drop-down list to allow or restrict the device from sending telemetry information. The default is **Allowed**. Other options are **Not allowed** and **Allowed, except for secondary data request**.
  - **Allow app access to Location service:** Allow app access to location services.
  - **Allow preview of internal builds:** Allow users to preview Microsoft internal builds.

- **Camera:** Windows Desktop/Tablet only

  - **Allow use of camera:** Allow users to use their device camera.

- **Bluetooth:** Windows Desktop/Tablet only

  - **Allow discoverable mode:** Allow Bluetooth devices to find the local device.
  - **Local device name:** A name for the local device.

- **Experience:** Windows Desktop/Tablet only

  - **Allow Cortana:** Allow users access to Cortana, the intelligent personal assistant and knowledge navigator.
  - **Allow device discovery:** Allow network discovery of the device.
  - **Allow manual MDM unenrollment:** Allow users to manually unenroll their device from the Citrix Endpoint Management MDM.
  - **Allow sync of device settings:** Allow users to sync settings between Windows 10 and Windows 11 devices when roaming.

- **Above Lock:** Windows Desktop/Tablet only

  - **Allow toast notifications on lock screen:** Allow toast notifications on the lock screen. Windows Desktop/Tablet only

- **Apps**

  - **Allow automatic updates from app store:** Allow apps from the app store to automatically update. Windows Desktop/Tablet only.

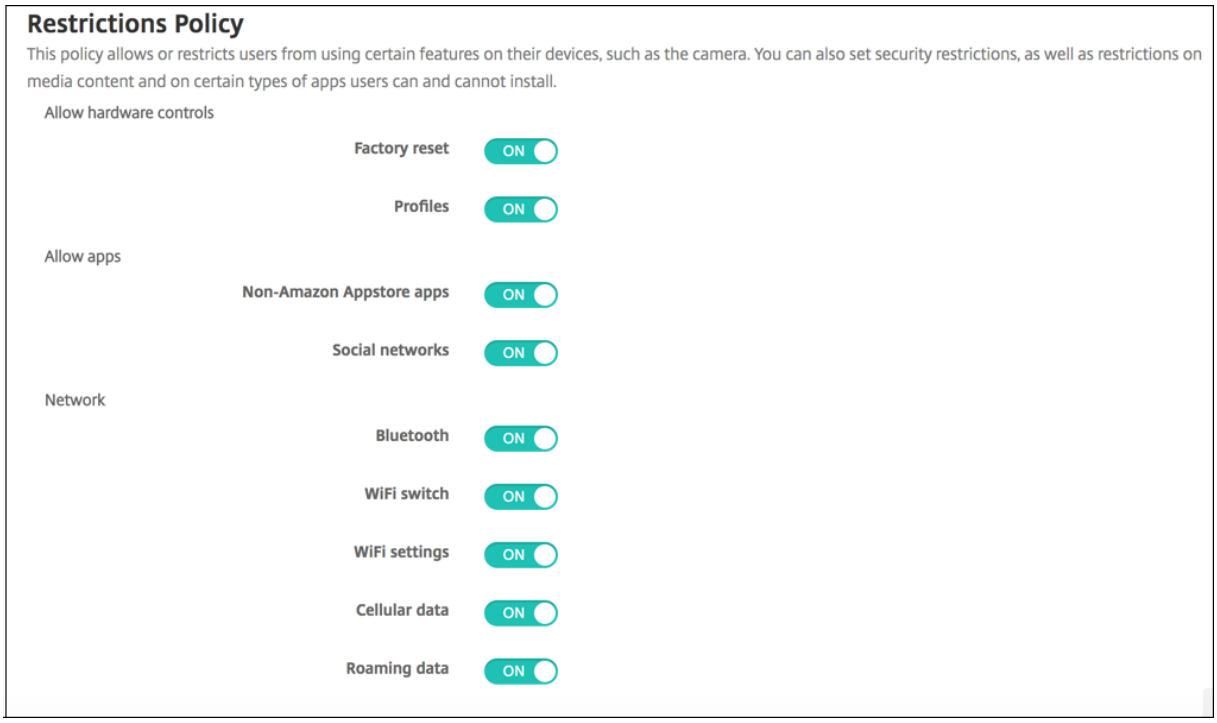
- **Privacy:** Windows Desktop/Tablet only

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Allow input personalization:** Allows the input personalization service to run. The input personalization service improves predictive inputs such as pen and touch keyboard based on what a user types.

- **Settings:** Windows Desktop/Tablet only.
  - **Allow auto play:** Allows users to change Auto Play settings.
  - **Allow data sense:** Allows users to change Data Sense settings.
  - **Allow date time:** Allows users to change date and time settings.
  - **Allow language:** Allows users to change language settings.
  - **Allow power sleep:** Allows users to change power and sleep settings.
  - **Allow region:** Allows users to change region settings.
  - **Allow sign-in options:** Allows users to change sign-in settings.
  - **Allow workplace:** Allows users to change workplace settings.
  - **Allow your account:** Allows users to change account settings.

Amazon settings



- **Allow hardware controls**
  - **Factory reset:** Allow users to do a factory reset on their devices
  - **Profiles:** Allow users to change the hardware profile on their devices.

- **Allow apps**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Non-Amazon Appstore apps:** Allow users to install non-Amazon app store apps on their devices.
  - **Social networks:** Allow users to access social networks from their devices.

- **Network**
  - **Bluetooth:** Allow users to use Bluetooth.
  - **Wi-Fi switch:** Allow apps to change Wi-Fi connectivity state.
  - **Wi-Fi settings:** Allow users to change Wi-Fi settings.
  - **Configure mobile networks:** Allow users to use their cellular data connection.
  - **Roaming data:** Allow users to use cellular data while roaming.
  - **Location services:** Allow users to use GPS.

- **USB actions:**
  - **Debugging:** Allow users'devices to connect through USB to a computer for debugging.

Roaming device policy

November 6, 2023

You can add a device policy in Citrix Endpoint Management to configure whether to allow voice and data roaming on supported iOS devices. When voice roaming is disabled, data roaming is automatically disabled.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Disable voice roaming:** Select whether to disable voice roaming. When this option is enabled, data roaming is automatically disabled. The default is **Off**, which allows voice roaming.
- **Disable data roaming:** Select whether to disable data roaming. This option is available only when voice roaming is enabled. The default is **Off**, which allows data roaming.

SCEP device policy

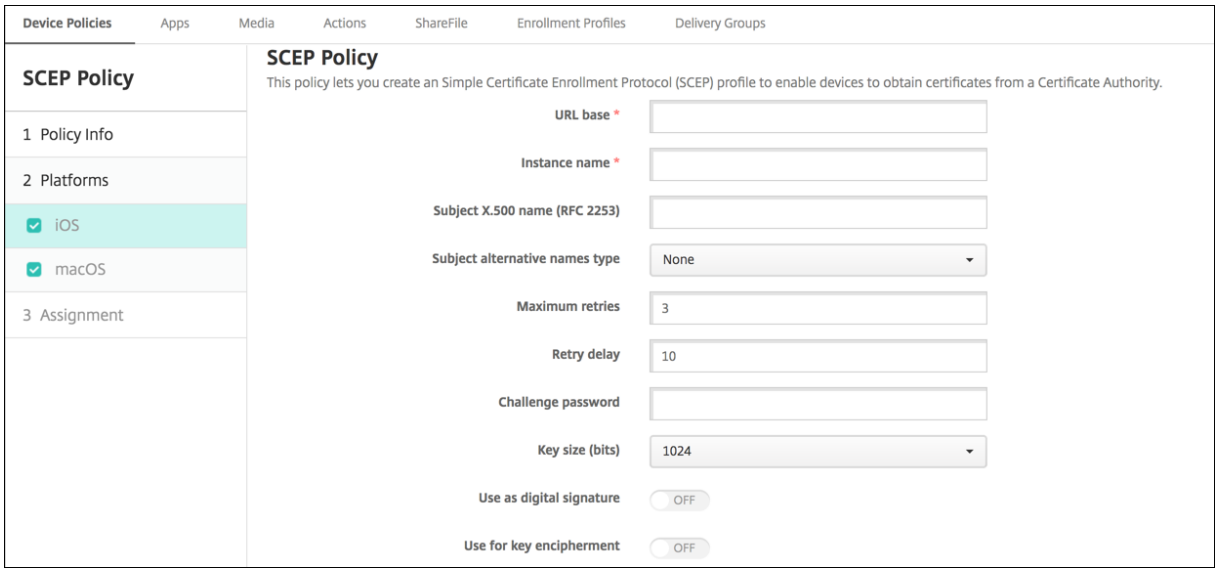
September 6, 2025

© 1997–2025 Citrix Systems, Inc. All rights reserved.

This policy lets you configure iOS and macOS devices to retrieve a certificate from an external SCEP server over the Simple Certificate Enrollment Protocol (SCEP). To deliver a certificate to devices using SCEP from a PKI that is connected to Citrix Endpoint Management, create a PKI entity and a PKI provider in distributed mode. For details, see PKI Entities.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings



- **URL base:** Type the address of the SCEP server to define where SCEP requests are sent, over HTTP or HTTPS. The private key isn't sent with the Certificate Signing Request (CSR), so it might be safe to send the request unencrypted. If the one-time password is configured for reuse, use HTTPS to protect the password. This step is required.
- **Instance name:** Type any string that the SCEP server recognizes. For example, it can be a domain name like example.org. If a CA has multiple CA certificates, you can use this field to distinguish the required domain. This step is required.
- **Subject X.500 name (RFC 2253):** Type the representation of an X.500 name as an array of Object Identifier (OID) and value. For example, `/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar`, which translates to: `[ [ ["C", "US"] ], [ ["O", "Apple Inc."] ], ..., [ ["1.2.5.3", "bar" ] ] ]`. You can represent OIDs as dotted numbers with shortcuts for country (C), locality (L), state (ST), organization (O), organizational unit (OU), and common name (CN).
- **Subject alternative names type:** Select an alternative name type. An optional alternative name type can provide the values required by the CA for issuing a certificate. You can specify

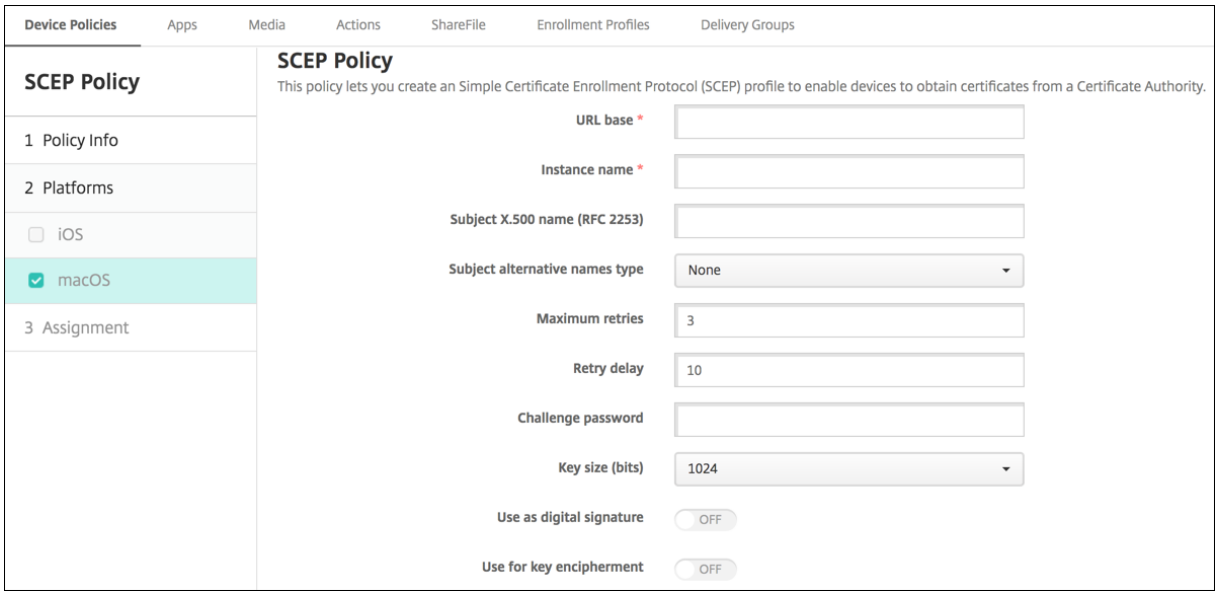
© 1997–2025 Citrix Systems, Inc. All rights reserved.

None, **RFC 822 name**, **DNS name**, or **URI**.

- **Maximum retries:** Type the number of times a device must retry when the SCEP server sends a PENDING response. The default is **3**.
- **Retry delay:** Type the number of seconds to wait between subsequent retries. The first retry is attempted without delay. The default is **10**.
- **Challenge password:** Enter a pre-shared secret.
- **Key size (bits):** Select **2048** or higher as the key size in bits.
- **Use as digital signature:** Choose whether to use the certificate as a digital signature. The SCEP server verifies the certificate use as a digital signature before using the public key to decrypt the hash.
- **Use for key encipherment:** Choose whether to use the certificate for key encipherment. A server first checks whether the certificate provided by a client is allowed for key encipherment. Then the server uses the public key in a certificate to verify that a piece of data was encrypted using the private key. If not, the operation fails.
- **SHA-256 fingerprint (hexadecimal string):** If your CA uses HTTP, use this field to provide the fingerprint of the CA certificate. The device uses the fingerprint to confirm the authenticity of the CA response during enrollment. You can provide an SHA-256 fingerprint, or you can select a certificate to import its signature.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

macOS settings



- **URL base:** Type the address of the SCEP server to define where SCEP requests are sent, over HTTP or HTTPS. The private key isn't sent with the Certificate Signing Request (CSR), so it might be safe to send the request unencrypted. If the one-time password is configured for reuse, use HTTPS to protect the password. This step is required.
- **Instance name:** Type any string that the SCEP server recognizes. For example, it can be a domain name like example.org. If a CA has multiple CA certificates, you can use this field to distinguish the required domain. This step is required.
- **Subject X.500 name (RFC 2253):** Type the representation of an X.500 name as an array of Object Identifier (OID) and value. For example, `/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar`, which translates to: `[ [ ["C", "US"] ], [ ["O", "Apple Inc."] ], ..., [ ["1.2.5.3", "bar" ] ] ]`. You can represent OIDs as dotted numbers with shortcuts for country (C), locality (L), state (ST), organization (O), organizational unit (OU), and common name (CN).
- **Subject alternative names type:** Select an alternative name type. An optional alternative name type can provide the values required by the CA for issuing a certificate. You can specify **None**, **RFC 822 name**, **DNS name**, or **URI**.
- **Maximum retries:** Type the number of times a device must retry when the SCEP server sends a PENDING response. The default is **3**.
- **Retry delay:** Type the number of seconds to wait between subsequent retries. The first retry is attempted without delay. The default is **10**.
- **Challenge password:** Type a pre-shared secret.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Key size (bits):** Select **2048** or higher as the key size in bits.
- **Use as digital signature:** Choose whether to use the certificate as a digital signature. The SCEP server verifies the certificate use as a digital signature before using the public key to decrypt the hash.
- **Use for key encipherment:** Choose whether to use the certificate for key encipherment. A server first checks whether the certificate provided by a client is allowed for key encipherment. Then the server uses the public key in a certificate to verify that a piece of data was encrypted using the private key. If not, the operation fails.
- **SHA-256 fingerprint (hexadecimal string):** If your CA uses HTTP, use this field to provide the fingerprint of the CA certificate. The device uses the fingerprint to confirm the authenticity of the CA response during enrollment. You can provide an SHA-256 fingerprint, or you can select a certificate to import its signature.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
  - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
  - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

Siri and dictation policies

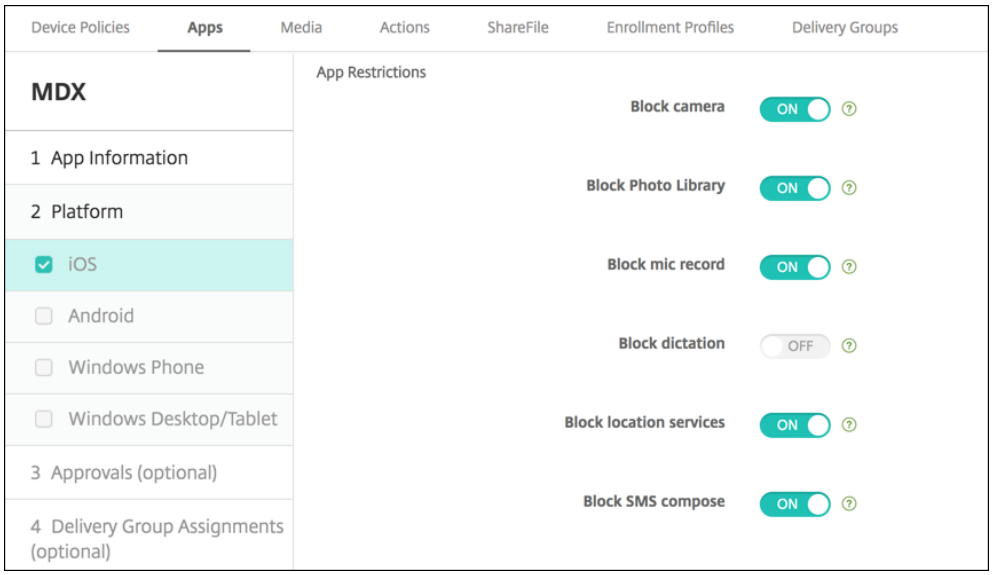
September 6, 2025

When users ask Siri something or dictate text on managed iOS devices, Apple collects the voice data for the purposes of improving Siri. The voice data passes through Apple's cloud-based services, and therefore exists outside the secure Citrix Endpoint Management container. The text that results from the dictation, however, remains within the container.

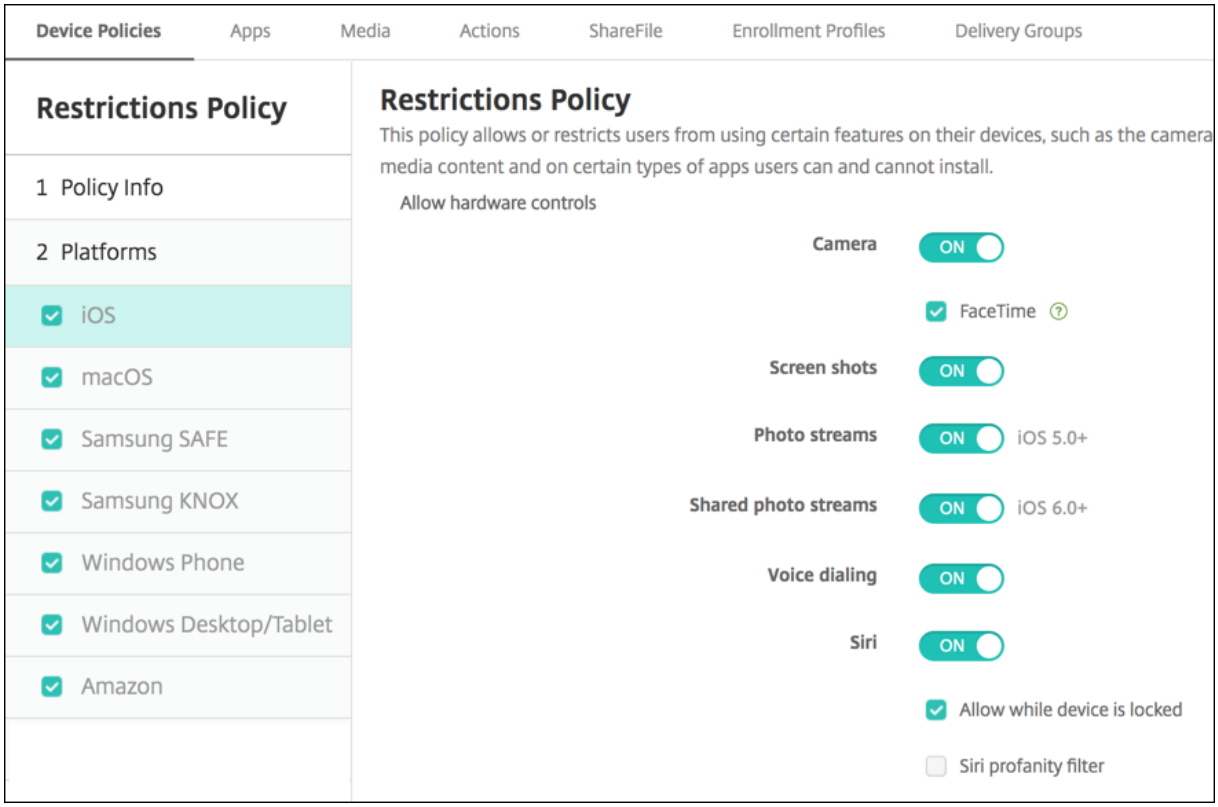
Citrix Endpoint Management allows you to block Siri and dictation services, as your security needs require.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

In MAM deployments, the **Block dictation** policy for each app is **On** by default, which disables the device's microphone. Set it to **Off** if you want to allow dictation. You can find the policy in the Citrix Endpoint Management console at **Configure > Apps**. Select the app, click **Edit**, then click **iOS**.



In MDM deployments, you can also disable Siri with the Siri policy at **Configure > Device Policies**. The use of Siri is allowed by default.



A few points to keep in mind when deciding whether to allow Siri and dictation:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- According to information that Apple has made public, Apple keeps Siri and dictation voice clip data for up to two years. The data is assigned a random number to represent the user, and voice files are associated with this random number.
- You can review the Apple privacy policy by going to **Settings > General > Keyboards** on any iOS device and tapping the link under **Enable Dictation**.

SSO account device policy

September 6, 2025

The SSO account device policy lets ou create single sign-on (SSO) accounts in Citrix Endpoint Management. Those accounts let users sign on one-time only to access Citrix Endpoint Management and your internal company resources from various apps. Users do not need to store any credentials on the device. The SSO account enterprise user credentials are used across apps, including apps from the App Store. This policy is designed to work with a Kerberos authentication back-end.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Account name:** Enter the Kerberos SSO account name that appears on users'devices. This field is required.
- **Kerberos principal name:** Enter the Kerberos principal name. This field is required.
- **Identity credential (Keystore or PKI credential):** Click an optional identity credential in the drop-down list that can be used to renew the Kerberos credential without user interaction.
- **Kerberos realm:** Enter the Kerberos realm for this policy. This value is typically your domain name in all capital letters (for example, EXAMPLE.COM). This field is required.
- **Permitted URLs:** For each URL for which you want to require SSO, click **Add** and then do the following:
  - **Permitted URL:** Enter a URL that you want to require SSO when a user visits the URL from the iOS device.

    For example, when a user tries to browse to a site and the website starts a Kerberos challenge: If that site isn't in the URL list, the iOS device doesn't attempt SSO by providing the Kerberos token that Kerberos might have cached on the device from a previous Kerberos logon. The match has to be exact on the host part of the URL. For example, `https://shopping.apple.com` is valid, but `https://*.apple.com` isn't.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Also, if Kerberos isn't activated based on host matching, the URL still falls back to a standard HTTP call. This can mean almost anything including a standard password challenge or an HTTP error if the URL is only configured for SSO using Kerberos.

  - Click **Add** to add the URL or click **Cancel** to cancel adding the URL.

- **App Identifiers:** For each app that is allowed to use this login, click **Add** and then do the following:
  - **App Identifier:** Enter an app identifier for an app that is allowed to use this login. If you do not add any app identifiers, this login matches **all** app identifiers.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

Store device policy

September 6, 2025

You can create a policy in Citrix Endpoint Management to specify whether devices display an app store web clip on the home screen.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS, Android, and Windows Desktop/Tablet settings

For each platform that you configure, select whether an app store web clip appears on user devices. The default is **On**.

Subscribed calendars device policy

September 6, 2025

© 1997–2025 Citrix Systems, Inc. All rights reserved.

You can add a device policy in Citrix Endpoint Management to add a subscribed calendar to the calendars list on iOS devices. The list of public calendars to which you can subscribe is available on the Apple Support site in Downloads.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Prerequisite

You must have subscribed to a calendar before you can add it to the subscribed calendars list on user devices.

iOS settings

- **Description:** Enter a description of the calendar. This field is required.
- **URL:** Enter the calendar URL. You can enter a `webcal://` URL or an `https://` link to an iCalendar file (.ics). This field is required.
- **User name:** Enter the user's logon name. This field is required.
- **Password:** Enter an optional user password.
- **Use SSL:** Select whether to use a Secure Socket Layer connection to the calendar. The default is **Off**.
- **Policy settings**
  - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
    - **Select date:** Click the calendar to select the specific date for removal.
    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

Terms and conditions device policy

September 6, 2025

You create terms and conditions device policies in Citrix Endpoint Management when you want users to accept your company's specific policies governing connections to the corporate network. When users enroll their devices with Citrix Endpoint Management, they're presented with the terms and

© 1997–2025 Citrix Systems, Inc. All rights reserved.

conditions and must accept them to enroll their devices. Declining the terms and conditions cancels the enrollment process.

You can create different policies for terms and conditions in different languages if your company has international users and you want them to accept terms and conditions in their native languages. You must provide a file for each platform and language combination you plan to deploy. For Android and iOS devices, you must supply PDF files. For Windows devices, you must supply text (.txt) files and accompanying image files.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS and Android settings

- **File to be imported:** Select the terms and conditions file to import by clicking **Browse** and then navigating to the file's location.
- **Default Terms & Conditions:** Select whether this file is the default document for users who are members of multiple groups with different terms and conditions. The default is **Off**.

> **Note:**
>
> Terms and Conditions aren't displayed if an iOS device is enrolled through the Device Enrollment Program (DEP).

Windows Tablet settings

- **File to be imported:** Select the terms and conditions file to import by clicking **Browse** and then navigating to the file's location.
- **Image:** Select the image file to import by clicking **Browse** and then navigating to the file's location.
- **Default Terms & Conditions:** Select whether this file is the default document for users who are members of multiple groups with different terms and conditions. The default is **Off**.

Tunnel device policy

September 6, 2025

Application tunnels (app tunnels) are designed to increase service continuity and data transfer reliability for your mobile apps. App tunnels define proxy parameters between the client component of any

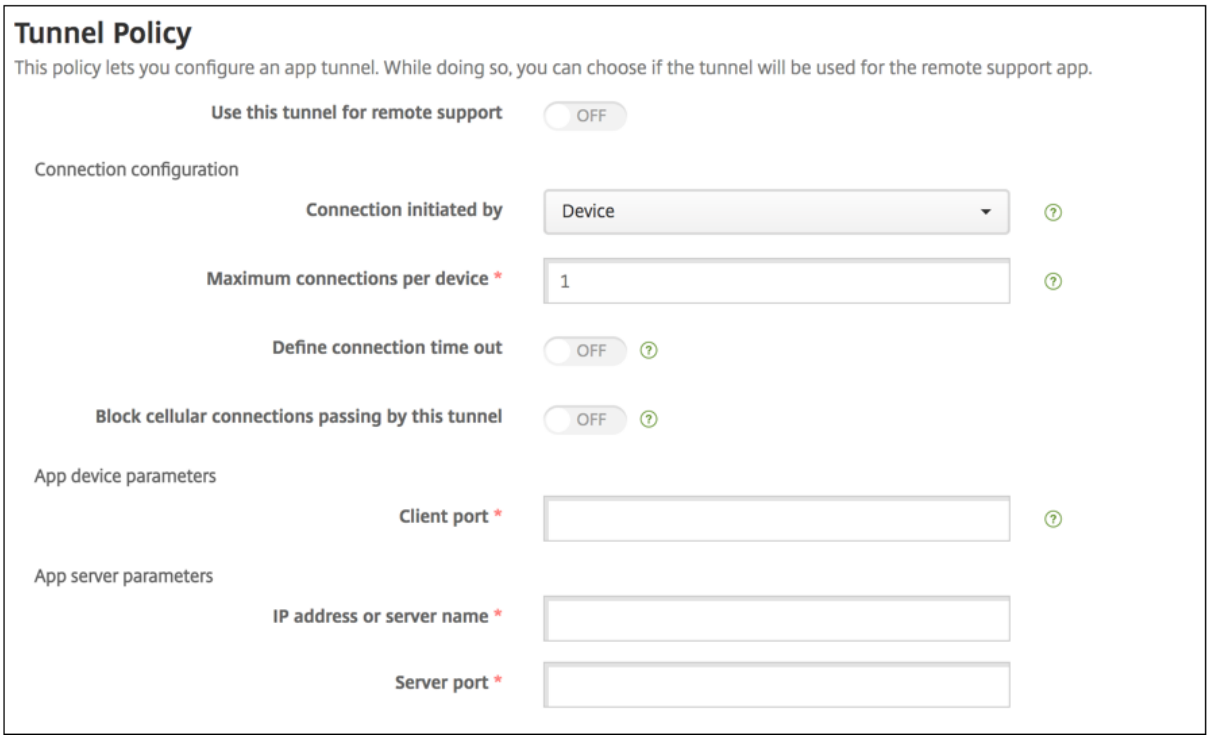
© 1997–2025 Citrix Systems, Inc. All rights reserved.

mobile device app and the app server component. You can configure the Tunnel policy for Android devices.

Any app traffic sent through a tunnel that you define in this policy goes through Citrix Endpoint Management before being redirected to the server running the app.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Android settings



- **Connection initiated by:** Click **Device** or **Server** to specify the source starting the connection.
- **Maximum connections per device:** Type a number to specify how many concurrent TCP connections the app can establish. This field applies only to device-initiated connections.
- **Define connection time out:** Select whether to set a length of time an app can be idle before the tunnel is closed.
  - **Connection time out:** If you set **Define connection time out** to **On**, type the length of time in seconds that an app can be idle before the tunnel is closed.
- **Block cellular connections passing by this tunnel:** Select whether this tunnel is blocked while roaming. Wi-Fi and USB connections aren't blocked.
- **Client port:** Type the client port number. Usually, this value is the same as for the server port.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **IP address or server name:** Type the IP address or name of the app server. This field applies only to device-initiated connections.
- **Server port:** Type the server port number.

VPN device policy

September 6, 2025

The VPN device policy configures virtual private network (VPN) settings that enable user devices to connect securely to corporate resources. You can configure the VPN device policy for the following platforms. Each platform requires a different set of values, which are described in detail in this article.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

> **Note:**
>
> Citrix SSO for Android and iOS are now called Citrix Secure Access. We are updating our documentation to reflect this name change.

Requirements for per-app VPNs

You configure the per-app VPN feature for the following platforms through VPN policies:

- iOS
- macOS
- Android (legacy DA)

For Android Enterprise, use the Managed configurations device policy to configure VPN profiles.

Per-app VPN options are available for certain connection types. The following table indicates when per-app VPN options are available.

Platform	Connection type	Remark
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO, or Custom SSL.	

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Platform	Connection type	Remark
macOS	Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, or Custom SSL.	
Android (legacy DA)	Citrix SSO	

To create a per-app VPN for iOS and Android (legacy DA) devices using the Citrix SSO app, you need to do extra steps, in addition to the VPN policy configuration. Also, you must verify that the following prerequisites are met:

- On-premises NetScaler Gateway
- The following applications are installed on the device:
  - Citrix SSO
  - Citrix Secure Hub

A general workflow to configure a per-app VPN for iOS and Android devices using the Citrix SSO app is as follows:

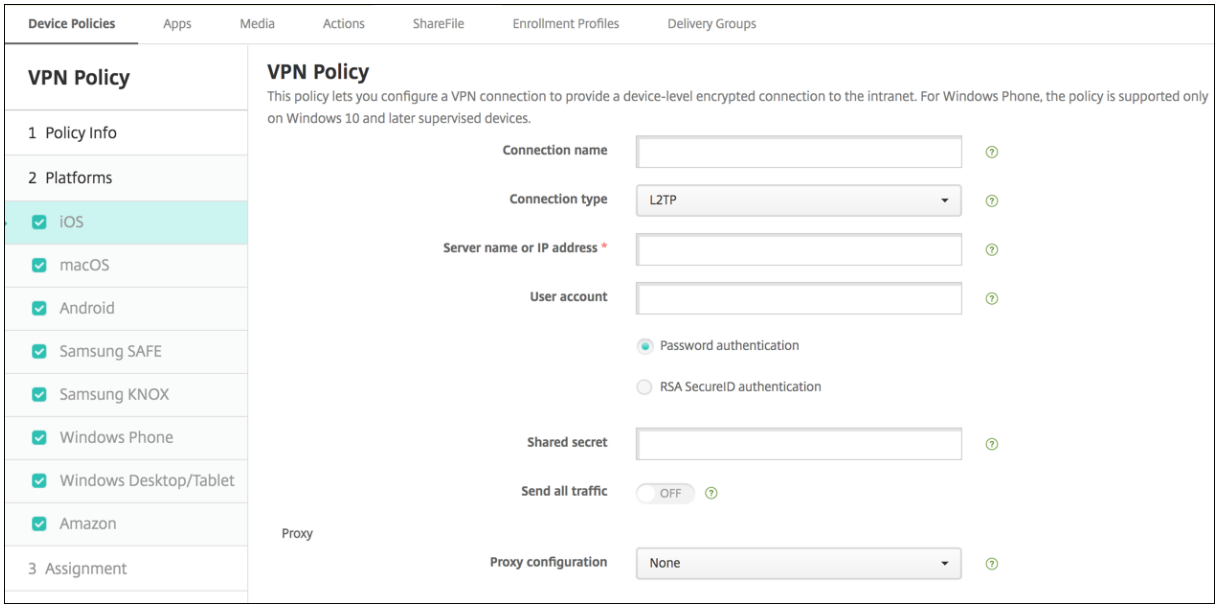
1. Configure a VPN device policy as described in this article.
   - For iOS, see Configure Citrix SSO protocol for iOS. After you configure the Citrix SSO protocol for iOS through a VPN device policy, you also must create an App Attributes policy to associate an app to the per-app VPN policy. For more information, see Configure a per-app VPN.
     - For the **Authentication type for the connection** field, if you select **Certificate**, you must first configure certificate-based authentication for Citrix Endpoint Management. See Client certificate or certificate plus domain authentication.
   - For Android (legacy DA), see Configure the Citrix SSO protocol for Android.
     - For the **Authentication type for the connection** field, if you select **Certificate** or **Password and Certificate**, you must first configure certificate-based authentication for Citrix Endpoint Management. See Client certificate or certificate plus domain authentication.
2. Configure Citrix ADC to accept traffic from the per-app VPN. For details, see Full VPN setup on NetScaler Gateway.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS settings

The Citrix VPN connection type in the VPN device policy for iOS doesn't support iOS 12. Do these steps to delete your existing VPN device policy and create a VPN device policy with the Citrix SSO connection type:

1. Delete your VPN device policy for iOS.
2. Add a VPN device policy for iOS with the following settings:
   - **Connection type: Citrix SSO**
   - **Enable per-app VPN: On**
   - **Provider type: Packet tunnel**
3. Add an App Attributes device policy for iOS. For **Per-app VPN identifier**, choose **iOS_VPN**.



- **Connection name:** Type a name for the connection.
- **Connection type:** In the list, select the protocol to be used for this connection. The default is **L2TP**.
  - **L2TP:** Layer 2 Tunneling Protocol with pre-shared key authentication.
  - **PPTP:** Point-to-Point Tunneling.
  - **IPSec:** Your corporate VPN connection.
  - **Cisco Legacy AnyConnect:** This connection type requires that the Cisco Legacy AnyConnect VPN client is installed on the user device. Cisco is phasing out the Cisco Legacy AnyConnect client that was based on a now deprecated VPN framework.

    To use the current Cisco AnyConnect client, use a **Connection type** of **Custom SSL**. For required settings, see "Configure Custom SSL protocol"in this section.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Juniper SSL:** Juniper Networks SSL VPN client.
  - **F5 SSL:** F5 Networks SSL VPN client.
  - **SonicWALL Mobile Connect:** Dell unified VPN client for iOS.
  - **Ariba VIA:** Ariba Networks Virtual Internet Access client.
  - **IKEv2 (iOS only):** Internet Key Exchange version 2 for iOS only.
  - **AlwaysOn IKEv2:** Always-on access using IKEv2.
  - **AlwaysOn IKEv2 Dual Configuration:** Always-on access using IKEv2 dual configuration.
  - **Citrix SSO:** Citrix SSO client for iOS 12 and later.
  - **Custom SSL:** Custom Secure Socket Layer. This connection type is required for the Cisco AnyConnect client that has a bundle ID of **com.cisco.anyconnect**. Specify a **Connection name** of **Cisco AnyConnect**. You can also deploy the VPN policy and enable a Network Access Control (NAC) filter for iOS devices. The filter blocks a VPN connection for devices that have non-compliant apps installed. The configuration requires specific settings for the iOS VPN policy as described in the following iOS section. For more information about other settings required to enable the NAC filter, see Network Access Control.

The following sections list the configuration options for each of the preceding connection types.

Configure L2TP Protocol for iOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- Select either **Password authentication** or **RSA SecurID authentication**.
- **Shared secret:** Type the IPsec shared secret key.
- **Send all traffic:** Select whether to send all traffic over the VPN. The default is **Off**.

Configure PPTP Protocol for iOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- Select either **Password authentication** or **RSA SecurID authentication**.
- **Encryption level:** In the list, select an encryption level. The default is **None**.
  - **None:** Use no encryption.
  - **Automatic:** Use the strongest encryption level supported by the server.
  - **Maximum (128-bit):** Always use 128-bit encryption.
- **Send all traffic:** Select whether to send all traffic over the VPN. The default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure IPsec Protocol for iOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Shared Secret** or **Certificate** for the type of authentication for this connection. The default is **Shared Secret**.
- If you enable **Shared Secret**, configure these settings:
  - **Group name:** Type an optional group name.
  - **Shared secret:** Type an optional shared secret key.
  - **Use hybrid authentication:** Select whether to use hybrid authentication. With hybrid authentication, the server first authenticates itself to the client, and then the client authenticates itself to the server. The default is **Off**.
  - **Prompt for password:** Select whether to prompt users for their passwords when they connect to the network. The default is **Off**.
- If you enable **Certificate**, configure these settings:
  - **Identity credential:** In the list, select the identity credential to use. The default is **None**.
  - **Prompt for PIN when connecting:** Select whether to require users to enter their PIN when connecting to the network. The default is **Off**.
  - **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.
- **Enable per-app VPN:** Select whether to enable per-app VPN. The default is **Off**.
- **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
- **Safari domains:** Click **Add** to add a Safari domain name.

Configure Cisco legacy AnyConnect Protocol for iOS

To transition from the Cisco legacy AnyConnect client to the new Cisco AnyConnect client, use the Custom SSL protocol.

- **Provider bundle identifier:** For the Legacy AnyConnect client, the bundle ID is com.cisco.anyconnect.gui.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Group:** Type an optional group name.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    * **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    * **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    * **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.

- **Include All Networks:** Select whether to allow all networks to use this connection. The default is **Off**.
- **Exclude Local Networks:** Select whether to exclude local networks from using the connection or to allow the networks. The default is **Off**.
- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service start network communication. The default is **Off**.
  - **Provider type:** Select whether the per-app VPN is provided as an **App proxy** or as a **Packet tunnel**. Default is **App proxy**.
  - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    * **Domain:** Type the domain to be added.
    * Click **Save** to save the domain or click **Cancel** to not save the domain.

Configure Juniper SSL Protocol for iOS

- **Provider bundle identifier:** If your per-app VPN profile has the bundle identifier of an app with multiple VPN providers of the same type, specify the provider to use here.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Realm:** Type an optional realm name.
- **Role:** Type an optional role name.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
- If you enable **Password**, type an optional authentication password in the **Authentication password** field.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- If you enable **Certificate**, configure these settings:
  - **Identity credential:** In the list, select the identity credential to use. The default is **None**.
  - **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
  - **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.
  - **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
  - **Provider type:** Select whether the per-app VPN is provided as an **App proxy** or as a **Packet tunnel**. Default is **App proxy**.
  - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
  - **Domain:** Type the domain to be added.
- Click **Save** to save the domain or click **Cancel** to not save the domain.

Configure F5 SSL Protocol for iOS

- **Provider bundle identifier:** If your per-app VPN profile has the bundle identifier of an app with multiple VPN providers of the same type, specify the provider to use here.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the

© 1997–2025 Citrix Systems, Inc. All rights reserved.

settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.

- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.
  - **Provider type:** Select whether the per-app VPN is provided as an **App proxy** or as a **Packet tunnel**. Default is **App proxy**.
  - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    * **Domain:** Type the domain to be added.
    * Click **Save** to save the domain or click **Cancel** to not save the domain.

Configure SonicWALL Protocol for iOS

- **Provider bundle identifier:** If your per-app VPN profile has the bundle identifier of an app with multiple VPN providers of the same type, specify the provider to use here.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Logon group or domain:** Type an optional logon group or domain.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    * **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    * **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    * **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.
- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you set this option to On, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Provider type:** Select whether the per-app VPN is provided as an **App proxy** or as a **Packet tunnel**. Default is **App proxy**.
  - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    * **Domain:** Type the domain to be added.
    * Click **Save** to save the domain or click **Cancel** to not save the domain.

Configure Ariba VIA protocol for iOS

- **Provider bundle identifier:** If your per-app VPN profile has the bundle identifier of an app with multiple VPN providers of the same type, specify the provider to use here.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    * **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    * **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    * **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.
- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.
  - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    * **Domain:** Type the domain to be added.
    * Click **Save** to save the domain or click **Cancel** to not save the domain.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure IKEv2 protocols for iOS

This section includes settings used for the IKEv2, Always On IKEv2, and Always On IKEv2 Dual Configuration protocols. For the Always On IKEv2 Dual Configuration protocol, configure all these settings for both Cellular and Wi-Fi networks.

- **Allow user to disable automatic connection:** For the Always On protocols. Select whether to allow users to disable automatic connection to the network on their devices. The default is **Off**.
- **Host name or IP address for server:** Type the server name or IP address for the VPN server.
- **Local Identifier:** The FQDN or IP address for the IKEv2 client. This field is required.
- **Remote Identifier:** The FQDN or IP address for the VPN server. This field is required.
- **Device Authentication:** Choose **Shared Secret**, **Certificate**, or **Device Certificate Based on Device Identifier** for the type of authentication for this connection. The default is **Shared Secret**.
  - If you choose **Shared Secret**, type an optional shared secret key.
  - If you choose **Certificate**, choose an **Identity credential** to use. The default is **None**.
  - If you choose **Device Certificate Based on Device Identifier**, choose the **Device identity type** to use. The default is **IMEI**. To use this option, bulk import certificates using the REST API. See Upload certificates in bulk using the REST API. Only available when you select **Always On IKEv2**.
- **Extended Authentication Enabled:** Select whether to enable Extended Authentication Protocol (EAP). If **On**, type the **User account** and **Authentication password**.
- **Dead Peer Detection Interval:** Choose how often a peer device is contacted to make sure that the peer device stays reachable. The default is **None**. Options are:
  - **None:** Disable dead peer detection.
  - **Low:** Contacts peer every 30 minutes.
  - **Medium:** Contacts peer every 10 minutes.
  - **High:** Contacts peer every 1 minute.
- **Disable Mobility and Multihoming:** Choose whether to disable this feature.
- **Use IPv4/IPv6 internal subnet attributes:** Choose whether to enable this feature.
- **Disable redirects:** Choose whether to disable redirects.
- **Enable Fallback:** If enabled, this setting allows a tunnel over cellular data to carry traffic that is eligible for Wi-Fi Assist and requires a VPN. Default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Enable NAT keepalive while the device is asleep:** For the Always On protocols. Keepalive packets maintain NAT mappings for IKEv2 connections. The chip sends these packets at regular intervals when the device is awake. If this setting is on, the chip sends keepalive packets even while the device is asleep. The default interval is 20 seconds over Wi-Fi and 110 seconds over cellular. You can change the interval by using the NAT keepalive interval parameter.
- **NAT keepalive Interval (seconds):** Defaults to 20 seconds.
- **Enable Perfect Forward Secrecy:** Choose whether to enable this feature.
- **DNS server IP addresses:** Optional. A list of DNS server IP address strings. These IP addresses can include a mixture of IPv4 and IPv6 addresses. Click **Add** to type an address.
- **Domain name:** Optional. The primary domain of the tunnel.
- **Search domains:** Optional. A list of domain strings used to qualify single-label host names fully.
- **Append supplemental match domains to resolver's list:** Optional. Determines whether to add the supplemental match domains list to the resolver's list of search domains. Default is **On**.
- **Supplemental match domains:** Optional. A list of domain strings used to determine which DNS queries are to use the DNS resolver settings that are in the DNS server addresses. This key creates a split DNS configuration where only hosts in certain domains get resolved by using the DNS resolver of the tunnel. Hosts not in one of the domains in this list get resolved by using the default resolver of the system.

If this parameter has an empty string, then that string is the default domain. As a result, a split tunnel configuration can direct all DNS queries to the VPN DNS servers before the primary DNS servers. If the VPN tunnel is the default route of the network, the listed DNS servers become the default resolver. In that case, the supplemental match domains list is ignored.

- **IKE SA Parameters** and **Child SA Parameters:** Configure these settings for each Security Association (SA) parameters option:
  - **Encryption Algorithm:** In the list, select the IKE encryption algorithm to use. The default is **3DES**.
  - **Integrity Algorithm:** In the list, select the integrity algorithm to use. The default is **SHA-256**.
  - **Diffie Hellman Group:** In the list, select the Diffie Hellman group number. The default is **2**.
  - **ike LifeTime in Minutes:** Type an integer between 10 and 1440 representing the SA lifetime (rekey interval). The default is **1440** minutes.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Service Exceptions:** For the Always On protocols. Service exceptions are system services that are exempt from Always On VPN. Configure these service exceptions settings:
  - **Voice Mail:** In the list, select how to handle the voice mail exception. The default is **Allow traffic via tunnel**.
  - **AirPrint:** In the list, select how to handle the AirPrint exception. The default is **Allow traffic via tunnel**.
  - **Allow traffic from captive web sheet outside the VPN tunnel:** Select whether to allow users to connect to public hotspots outside the VPN tunnel. The default is **Off**.
  - **Allow traffic from all captive networking apps outside the VPN tunnel:** Select whether to allow all hotspot networking apps outside the VPN tunnel. The default is **Off**.
  - **Captive networking app bundle identifiers:** For each hotspot networking app bundle identifier that users are allowed to access, click **Add** and type the hotspot networking app **Bundle Identifier**. Click **Save** to save the app bundle identifier.
- **Per-app VPN:** Configure these settings for IKEv2 connection types.
  - **Enable per-app VPN:** Select whether to enable per-app VPN. The default is **Off**.
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
  - **Safari domains:** Click **Add** to add a Safari domain name.
- **Proxy configuration:** Choose how the VPN connection routes through a proxy server. Default is **None**.

Configure Citrix SSO protocol for iOS

The Citrix SSO client is available in the Apple Store.

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - **Identity credential:** In the list, select the identity credential to use. The default is **None**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

        * **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
        * **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.

- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you set this option to On, configure the following settings:

    - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.
    - **Provider type:** Select whether the per-app VPN is provided as an **App proxy** or as a **Packet tunnel**. Default is **App proxy**.
    - **Provider type:** Set to **Packet tunnel**.
    - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
        * **Domain:** Type the domain to be added.
        * Click **Save** to save the domain or click **Cancel** to not save the domain.

- **Custom XML:** For each custom XML parameter you want to add, click **Add** and specify the key/-value pairs. Available parameters are:

    - **disableL3:** Disables system level VPN. Allows only per app VPN. No **Value** is needed.
    - **user agent:** Associates with this device policy any NetScaler Gateway policies that are targeted to VPN plug-in clients. For requests started by the plug-in, the **Value** for this key is automatically added to the VPN plug-in.

Configure Custom SSL protocol for iOS

To transition from the Cisco Legacy AnyConnect client to the Cisco AnyConnect client:

1. Configure the VPN device policy with the Custom SSL protocol. Deploy the policy to iOS devices.
2. Upload the Cisco AnyConnect client from https://apps.apple.com/us/app/cisco-secure-client/id1135064690, add the app to Citrix Endpoint Management, and then deploy the app to iOS devices.
3. Remove the old VPN device policy from iOS devices.

Settings:

- **Custom SSL identifier (reverse DNS format):** Set to the bundle identifier. For the Cisco AnyConnect client, use **com.cisco.anyconnect**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Provider Bundle Identifier:** If the app specified in **Custom SSL identifier** has multiple VPN providers of the same type (App proxy or Packet tunnel), then specify this bundle identifier. For the Cisco AnyConnect client, use **com.cisco.anyconnect**.
- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings for iOS.
- **Include All Networks:** Select whether to allow all networks to use this connection. The default is **Off**.
- **Exclude Local Networks:** Select whether to exclude local networks from using the connection or to allow the networks. The default is **Off**.
- **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you set this option to On, configure the following settings:
  - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.
  - **Provider Type:** A provider type indicates whether the provider is a VPN service or proxy service. For VPN service, choose **Packet tunnel**. For proxy service, choose **App proxy**. For the Cisco AnyConnect client, choose **Packet tunnel**.
  - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - **Domain:** Type the domain to be added.
    - Click **Save** to save the domain or click **Cancel** to not save the domain.
- **Custom XML:** For each custom XML parameter you want to add, click **Add** and do the following:
  - **Parameter name:** Type the name of the parameter to be added.
  - **Value:** Type the value associated with the **Parameter name**.
  - Click **Save** to save the parameter or click **Cancel** to not save the parameter.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure the VPN device policy to support NAC

1. The **Connection type** of **Custom SSL** is required for configuring the NAC filter.
2. Specify a **Connection name** of **VPN**.
3. For **Custom SSL identifier**, type **com.citrix.NetScalerGateway.ios.app**
4. For **Provider bundle identifier**, type **com.citrix.NetScalerGateway.ios.app.vpnplugin**

The values in steps 3 and 4 come from the required Citrix SSO installation for NAC filtering. You do not configure an authentication password. For more information on using the NAC function, see Network Access Control.

Configure enable VPN on demand options for iOS

- **On Demand Domain:** For each domain and associated action to take when users connect, click **Add** and do the following:
- **Domain:** Type the domain to be added.
- **Action:** In the list select one of the possible actions:
  - **Always establish:** The domain always triggers a VPN connection.
  - **Never establish:** The domain never triggers a VPN connection.
  - **Establish if necessary:** The domain triggers a VPN connection attempt if domain name resolution fails. Failure happens when the DNS server can't resolve the domain, redirects to a different server, or times out.
  - Click **Save** to save the domain or click **Cancel** to not save the domain.
- **On demand rules**
  - **Action:** In the list, select the action to be taken. The default is **EvaluateConnection**. Possible actions are:
    - **Allow:** Allow VPN on demand to connect when triggered.
    - **Connect:** Unconditionally start a VPN connection.
    - **Disconnect:** Remove the VPN connection and do not reconnect on demand as long as the rule matches.
    - **EvaluateConnection:** Evaluate the ActionParameters array for each connection.
    - **Ignore:** Leave any existing VPN connection up, but do not reconnect on demand as long as the rule matches.
  - **DNSDomainMatch:** For each domain against which a device's search domain list can match that you want to add, click **Add** and do the following:
    - **DNS Domain:** Type the domain name. You can use the wildcard "*"prefix for matching multiple domains. For example, *.example.com matches mydomain.example.com, yourdomain.example.com, and herdomain.example.com.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    - Click **Save** to save the domain or click **Cancel** to not save the domain.
- **DNSServerAddressMatch:** For each IP address to which any of the network's specified DNS servers can match that you want to add, click **Add** and do the following:
    - **DNS Server Address:** Type the DNS server address that you want to add. You can use the wildcard "*"suffix for matching DNS servers. For example, 17.* matches any DNS server in the class A subnet.
    - Click **Save** to save the DNS server address or click **Cancel** to not save the DNS server address.
- **InterfaceTypeMatch:** In the list, select the type of primary network interface hardware in use. The default is **Unspecified**. Possible values are:
    - **Unspecified:** Matches any network interface hardware. This option is the default.
    - **Ethernet:** Matches only Ethernet network interface hardware.
    - **WiFi:** Matches only Wi-Fi network interface hardware.
    - **Cellular:** Matches only Cellular network interface hardware.
- **SSIDMatch:** For each SSID to match against the current network that you want to add, click **Add** and so the following.
    - **SSID:** Type the SSID to add. If the network isn't a Wi-Fi network, or if the SSID does not appear, the match fails. Leave this list empty to match any SSID.
    - Click **Save** to save the SSID or click **Cancel** to not save the SSID.
- **URLStringProbe:** Type a URL to fetch. If this URL is successfully fetched without redirection, this rule matches.
- **ActionParameters : Domains:** For each domain that EvaluateConnection checks that you want to add, click **Add** and do the following:
    - **Domain:** Type the domain to be added.
    - Click **Save** to save the domain or click **Cancel** to not save the domain.
- **ActionParameters : DomainAction:** In the list, select the **VPN behavior** for the specified **ActionParameters : Domains** domains. The default is **ConnectIfNeeded**. Possible actions are:
    - **ConnectIfNeeded:** The domain triggers a VPN connection attempt if domain name resolution fails. Failure happens when the DNS server can't resolve the domain, redirects to a different server, or times out.
    - **NeverConnect:** The domain never triggers a VPN connection.
- **Action Parameters: RequiredDNSServers:** For each DNS server to use for resolving the specified domains, click **Add** and do the following:
    - **DNS Server:** Valid only when **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Type the DNS server IP address. This server can be outside of the device's current network configuration. If the DNS server isn't reachable, a VPN connection is established in response. Make sure that the DNS server is either an internal DNS server or a trusted external DNS server.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

        * Click **Save** to save the DNS server or click **Cancel** to not save the DNS server.
    - **ActionParameters : RequiredURLStringProbe:** Optionally, type an HTTP or HTTPS (preferred) URL to probe, using a GET request. If the URL's host name can't be resolved, the server is unreachable, or the server doesn't respond, a VPN connection is established. Valid only when **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
    - **OnDemandRules : XML content:** Type, or copy and paste, the XML configuration-on-demand rules.
        * Click **Check Dictionary** to validate the XML code. **Valid XML** appears below the **XML content** text box if the XML is valid. If it isn't valid, an error message describes the error.

- **Proxy**
    - **Proxy configuration:** In the list, select how the VPN connection routes through a proxy server. The default is **None**.
        * If you enable **Manual**, configure these settings:
            · **Host name or IP address for the proxy server:** Type the host name or IP address for the proxy server. This field is required.
            · **Port for the proxy server:** Type the proxy server port number. This field is required.
            · **User name:** Type an optional proxy server user name.
            · **Password:** Type an optional proxy server password.
        * If you configure **Automatic**, configure this setting:
            · **Proxy server URL:** Type the URL for the proxy server. This field is required.

- **Policy settings**
    - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
        * **Select date:** Click the calendar to select the specific date for removal.
        * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

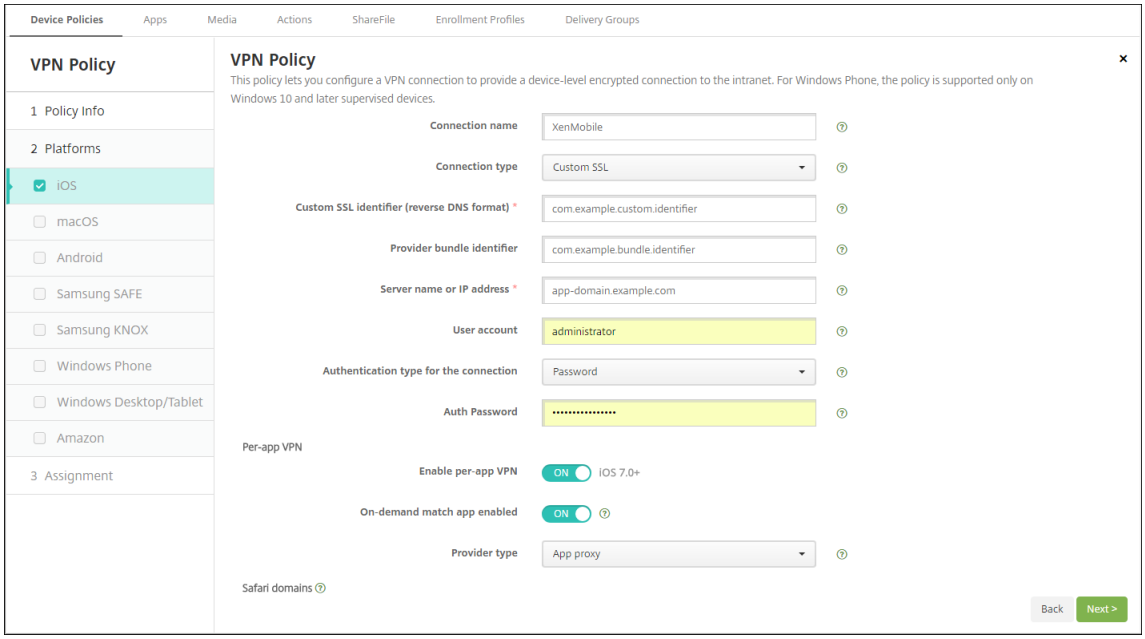
Configure a per-app VPN

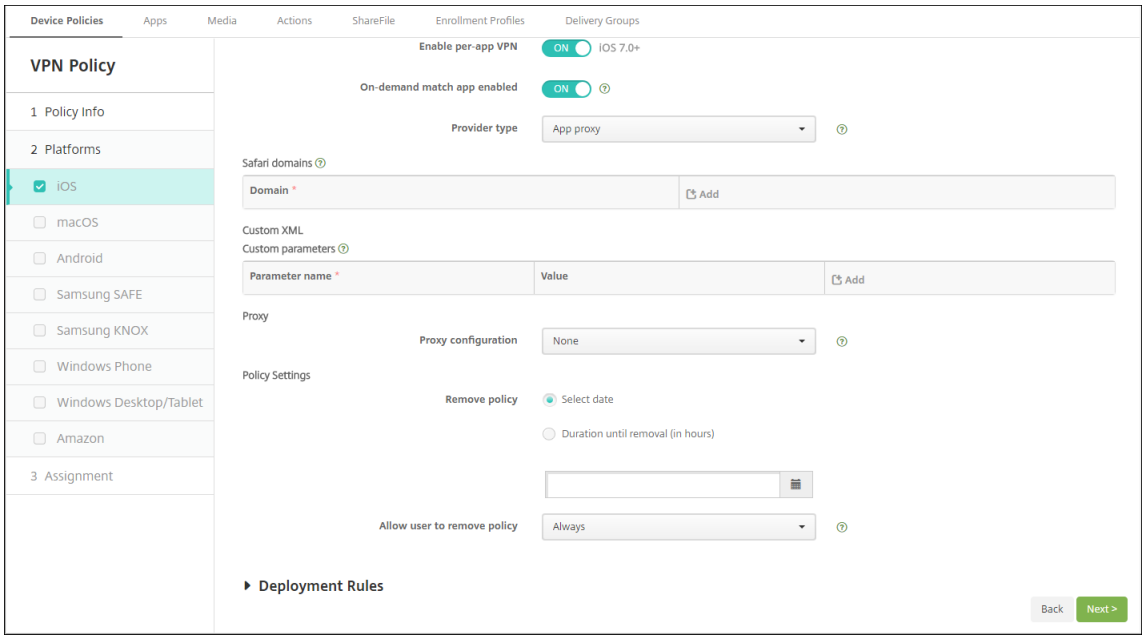
Per-app VPN options for iOS are available for these connection types: Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, Citrix SSO, and Custom SSL.

To configure a per-app VPN:

1. In **Configure > Device Policies**, create a VPN policy. For example:

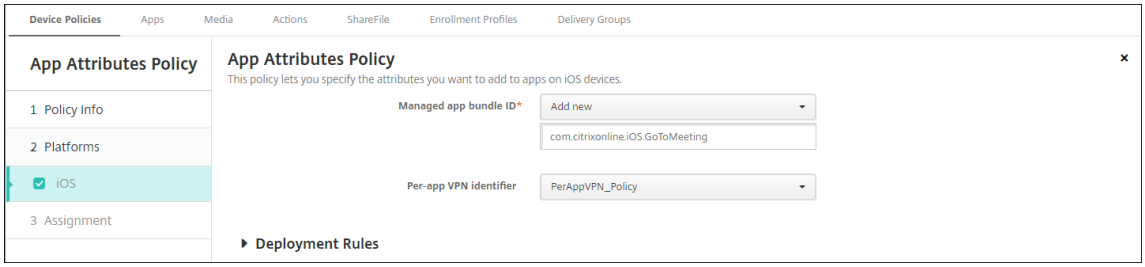
© 1997–2025 Citrix Systems, Inc. All rights reserved.



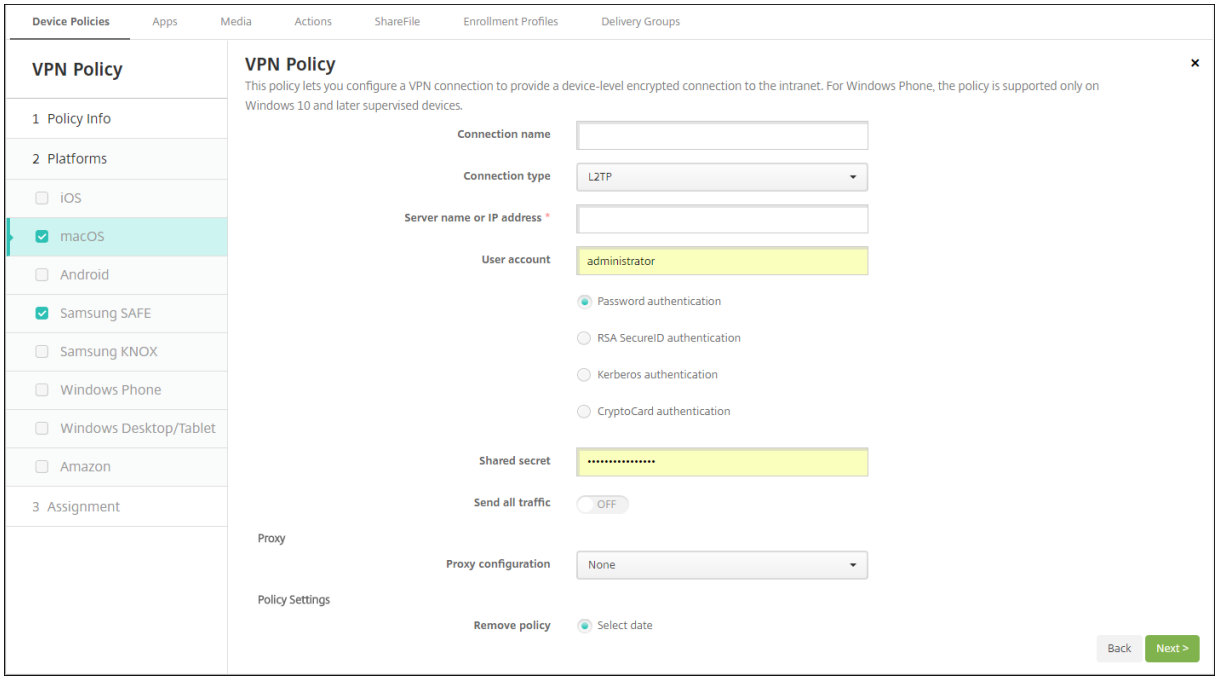


2. In **Configure > Device Policies**, create an App Attributes policy to associate an app to the per-app VPN policy. For **Per-app VPN identifier**, choose the name of the VPN policy created in Step 1. For **Managed app bundle ID**, choose from the app list or type the app bundle ID. (If you deploy an iOS App Inventory policy, the app list has apps.)

© 1997–2025 Citrix Systems, Inc. All rights reserved.



macOS settings



- **Connection name:** Type a name for the connection.
- **Connection type:** In the list, select the protocol to be used for this connection. The default is L2TP.
  - **L2TP:** Layer 2 Tunneling Protocol with pre-shared key authentication.
  - **PPTP:** Point-to-Point Tunneling.
  - **IPSec:** Your corporate VPN connection.
  - **Cisco AnyConnect:** Cisco AnyConnect VPN client.
  - **Juniper SSL:** Juniper Networks SSL VPN client.
  - **F5 SSL:** F5 Networks SSL VPN client.
  - **SonicWALL Mobile Connect:** Dell unified VPN client for iOS.
  - **Ariba VIA:** Ariba Networks Virtual Internet Access client.
  - **Citrix VPN:** Citrix VPN client.
  - **Custom SSL:** Custom Secure Socket Layer.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The following sections list the configuration options for each of the preceding connection types.

Configure L2TP Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- Select **Password authentication**, **RSA SecurID authentication**, **Kerberos authentication**, or **CryptoCard authentication**. The default is **Password authentication**.
- **Shared secret:** Type the IPsec shared secret key.
- **Send all traffic:** Select whether to send all traffic over the VPN. The default is **Off**.

Configure PPTP Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User Account:** Type an optional user account.
- Select **Password authentication**, **RSA SecurID authentication**, **Kerberos authentication**, or **CryptoCard authentication**. The default is **Password authentication**.
- **Encryption level:** Select the desired encryption level. The default is **None**.
  - **None:** Use no encryption.
  - **Automatic:** Use the strongest encryption level supported by the server.
  - **Maximum** (128-bit): Always use 128-bit encryption.
- **Send all traffic:** Select whether to send all traffic over the VPN. The default is **Off**.

Configure IPsec Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Shared Secret** or **Certificate** for the type of authentication for this connection. The default is **Shared Secret**.
  - If you enable **Shared Secret** authentication, configure these settings:
    - **Group name:** Type an optional group name.
    - **Shared secret:** Type an optional shared secret key.
    - **Use hybrid authentication:** Select whether to use hybrid authentication. With hybrid authentication, the server first authenticates itself to the client, and then the client authenticates itself to the server. The default is **Off**.
    - **Prompt for password:** Select whether to prompt users for their passwords when they connect to the network. The default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- If you enable **Certificate** authentication, configure these settings:
  - **Identity credential:** In the list, select the identity credential to use. The default is **None**.
  - **Prompt for PIN when connecting:** Select whether to require users to enter their PIN when connecting to the network. The default is **Off**.
  - **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand options.

Configure Cisco AnyConnect Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Group:** Type an optional group name.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand options.
  - **Enable Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
    - **On-demand match app enabled:** Select whether a per-app VPN connection triggers automatically when apps linked to the per-app VPN service start network communication. The default is **Off**.
    - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
      - **Domain:** Type the domain to be added.
      - Click **Save** to save the domain or click **Cancel** to not save the domain.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure Juniper SSL Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Realm:** Type an optional realm name.
- **Role:** Type an optional role name.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings.
- **Enable per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure the following settings:
  - **On-demand match app enabled:** Select whether a per-app VPN connection triggers automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
  - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    - **Domain:** Type the domain to be added.
    - Click **Save** to save the domain or click **Cancel** to not save the domain.

Configure F5 SSL Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - If you enable **Certificate**, configure these settings:
    * **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    * **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    * **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings.

- **Enable per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connection triggers automatically when apps linked to the per-app VPN service start network communication. The default is **Off**.
  - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    * **Domain:** Type the domain to be added.
    * Click **Save** to save the domain or click **Cancel** to not save the domain.

Configure SonicWALL Mobile Connect Protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Logon group or domain:** Type an optional logon group or domain.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    * **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    * **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    * **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Enable per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connection triggers automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
  - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    * **Domain:** Type the domain to be added.
    * Click **Save** to save the domain or click **Cancel** to not save the domain.

Configure Ariba VIA protocol for macOS

- **Server name or IP address:** Type the server name or IP address for the VPN server.
- **User account:** Type an optional user account.
- **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    * **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    * **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    * **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings.
- **Enable per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
  - **On-demand match app enabled:** Select whether per-app VPN connection triggers automatically when apps linked to the per-app VPN service initiate network communication. The default is **Off**.
  - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
    * **Domain:** Type the domain to be added.
    * Click **Save** to save the domain or click **Cancel** to not save the domain.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure Custom SSL protocol for macOS

- **Custom SSL identifier (reverse DNS format):** Type the SSL identifier in reverse DNS format. This field is required.
- **Server name or IP address:** Type the server name or IP address for the VPN server. This field is required.
- **User account:** Type an optional user account.
  - **Authentication type for the connection:** In the list, select either **Password** or **Certificate** for the type of authentication for this connection. The default is **Password**.
  - If you enable **Password**, type an optional authentication password in the **Authentication password** field.
  - If you enable **Certificate**, configure these settings:
    - **Identity credential:** In the list, select the identity credential to use. The default is **None**.
    - **Prompt for PIN when connecting:** Select whether to prompt users for their PIN when they connect to the network. The default is **Off**.
    - **Enable VPN on demand:** Select whether to enable triggering a VPN connection when users connect to the network. The default is **Off**. For information on configuring the settings when **Enable VPN on demand** is **On**, see Configure Enable VPN on demand settings.
  - **Per-app VPN:** Select whether to enable per-app VPN. The default is **Off**. If you enable this option, configure these settings:
    - **On-demand match app enabled:** Select whether per-app VPN connections trigger automatically when apps linked to the per-app VPN service initiate network communication.
    - **Safari domains:** For each Safari domain that can trigger a per-app VPN connection you want to include, click **Add** and do the following:
      - **Domain:** Type the domain to be added.
      - Click **Save** to save the domain or click **Cancel** to not save the domain.
- **Custom XML:** For each custom XML parameter you want to add, click **Add** and do the following:
  - **Parameter name:** Type the name of the parameter to be added.
  - **Value:** Type the value associated with **Parameter name**.
  - Click **Save** to save the domain or click **Cancel** to not save the domain.

Configure enable VPN on demand options

- **On Demand Domain:** For each domain and associated action to be taken when users connect to them that you want to add, click **Add** to and do the following:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **Domain:** Type the domain to be added.
  - **Action:** In the list select one of the possible actions:
    * **Always establish:** The domain always triggers a VPN connection.
    * **Never establish:** The domain never triggers a VPN connection.
    * **Establish if necessary:** The domain triggers a VPN connection attempt if domain name resolution fails. Failure happens when the DNS server can't resolve the domain, redirects to a different server, or times out.
  - Click **Save** to save the domain or click **Cancel** to not save the domain.

- **On demand rules**
  - **Action:** In the list, select the action to be taken. The default is **EvaluateConnection**. Possible actions are:
    * **Allow:** Allow VPN on demand to connect when triggered.
    * **Connect:** Unconditionally initiate a VPN connection.
    * **Disconnect:** Remove the VPN connection and do not reconnect on demand as long as the rule matches.
    * **EvaluateConnection:** Evaluate the **ActionParameters** array for each connection.
    * **Ignore:** Leave any existing VPN connection up, but do not reconnect on demand as long as the rule matches.
  - **DNSDomainMatch:** For the domains against which a device's search domain list can match, click **Add** to and do the following:
    * **DNS Domain:** Type the domain name. You can use the wildcard "*"prefix for matching multiple domains. For example, *.example.com matches mydomain.example.com, yourdomain.example.com, and herdomain.example.com.
    * Click **Save** to save the domain or click **Cancel** to not save the domain.
  - **DNSServerAddressMatch:** For each IP address to which any of the network's specified DNS servers can match that you want to add, click **Add** and do the following:
    * **DNS Server Address:** Type the DNS server address that you want to add. You can use the wildcard "*"suffix for matching DNS servers. For example, 17.* matches any DNS server in the class A subnet.
    * Click **Save** to save the DNS server address or click **Cancel** to not save the DNS server address.
  - **InterfaceTypeMatch:** In the list, click the type of primary network interface hardware in use. The default is **Unspecified**. Possible values are:
    * **Unspecified:** Matches any network interface hardware. This option is the default.
    * **Ethernet:** Matches only Ethernet network interface hardware.
    * **WiFi:** Matches only Wi-Fi network interface hardware.
    * **Cellular:** Matches only Cellular network interface hardware.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **SSIDMatch:** For each SSID to match against the current network that you want to add, click **Add** and so the following.
  - **SSID:** Type the SSID to add. If the network isn't a Wi-Fi network, or if the SSID does not appear, the match fails. Leave this list empty to match any SSID.
  - Click **Save** to save the SSID or click **Cancel** to not save the SSID.
- **URLStringProbe:** Type a URL to fetch. If this URL is successfully fetched without redirection, this rule matches.
- **ActionParameters : Domains:** For each domain that EvaluateConnection checks that you want to add, click **Add** and do the following:
  - **Domain:** Type the domain to be added.
  - Click **Save** to save the domain or click **Cancel** to not save the domain.
- **ActionParameters : DomainAction:** In the list, select the **VPN behavior** for the specified **ActionParameters : Domains** domains. The default is **ConnectIfNeeded**. Possible actions are:
  - **ConnectIfNeeded:** The domain triggers a VPN connection attempt if domain name resolution fails. Failure happens when the DNS server can't resolve the domain, redirects to a different server, or times out.
  - **NeverConnect:** The domain never triggers a VPN connection.
- **Action Parameters: RequiredDNSServers:** For each DNS server to use for resolving the specified domains, click **Add** and do the following:
  - **DNS Server:** Valid only when **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Type the DNS server IP address to add. This server can be outside of the device's current network configuration. If the DNS server isn't reachable, a VPN connection is established in response. This DNS server must be either an internal DNS server or a trusted external DNS server.
  - Click **Save** to save the DNS server or click **Cancel** to not save the DNS server.
- **ActionParameters : RequiredURLStringProbe:** Optionally, type an HTTP or HTTPS (preferred) URL to probe, using a GET request. If the URL's host name can't be resolved, the server is unreachable, or the server does not respond, a VPN connection is established. Valid only when **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
- **OnDemandRules : XML content:** Type, or copy and paste the XML configure-on-demand rules.
  - Click **Check Dictionary** to validate the XML code. **Valid XML** appears below the **XML content** text box if the XML is valid. If it isn't valid, an error message describes the error.

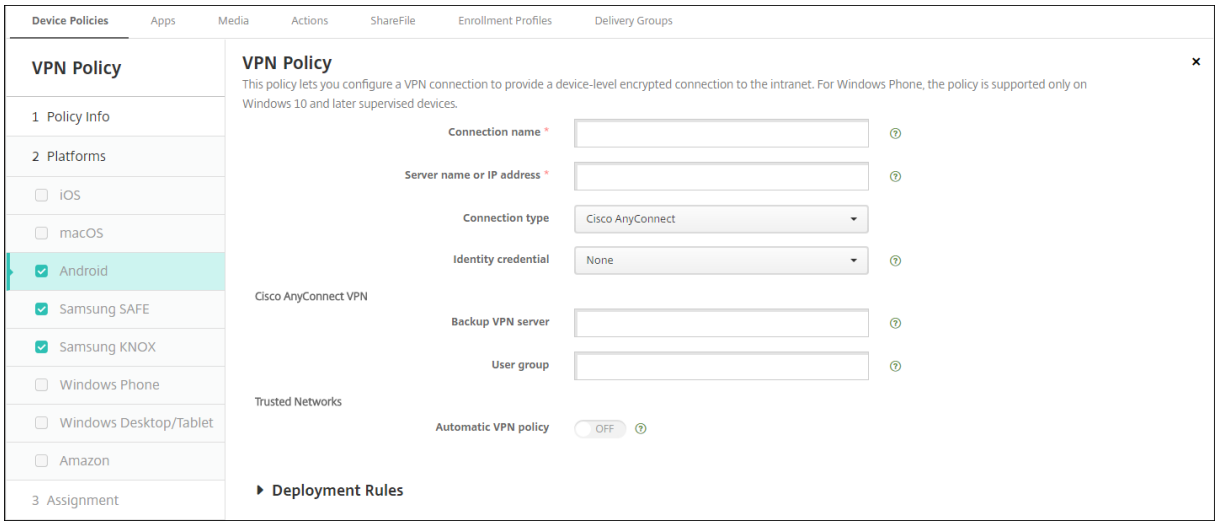
- **Proxy**
  - **Proxy configuration:** In the list, select how the VPN connection routes through a proxy server. The default is **None**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    * If you enable **Manual**, configure these settings:
        - **Host name or IP address for the proxy server:** Type the host name or IP address for the proxy server. This field is required.
        - **Port for the proxy server:** Type the proxy server port number. This field is required.
        - **User name:** Type an optional proxy server user name.
        - **Password:** Type an optional proxy server password.
    * If you configure **Automatic**, configure this setting:
        - **Proxy server URL:** Type the URL for the proxy server. This field is required.

- **Policy settings**
    - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
        * **Select date:** Click the calendar to select the specific date for removal.
        * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
    - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.
    - **Profile scope:** Select whether this policy applies to a **User** or an entire **System**. The default is **User**. This option is available only on macOS 10.7 and later.

Android (legacy DA) settings



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure Cisco AnyConnect VPN protocol for Android

- **Connection name:** Type a name for the Cisco AnyConnect VPN connection. This field is required.
- **Server name or IP address:** Type the name or IP address of the VPN server. This field is required.
- **Identity credential:** In the list, select an identity credential.
- **Backup VPN server:** Type the backup VPN server information.
- **User group:** Type the user group information.
- **Trusted Networks**
  - **Automatic VPN policy:** Enable or disable this option to set how the VPN reacts to trusted and untrusted networks. If enabled, configure these settings:
    - **Trusted network policy:** In the list, select the desired policy. The default is **Disconnect**. Possible options are:
      - **Disconnect:** The client terminates the VPN connection in the trusted network. This setting is the default.
      - **Connect:** The client starts a VPN connection in the trusted network.
      - **Do Nothing:** The client takes no action.
      - **Pause:** When a user establishes a VPN session outside the trusted network then enters a network configured as trusted, the VPN session gets suspended. When the user leaves the trusted network again, the session resumes. This setting eliminates the need to establish a new VPN session after leaving a trusted network.
    - **Untrusted network policy:** In the list, select the desired policy. The default is **Connect**. Possible options are:
      - **Connect:** The client starts a VPN connection in the untrusted network.
      - **Do Nothing:** The client starts a VPN connection in the untrusted network. This option disables the always-on VPN.
  - **Trusted domains:** For each domain suffix that the network interface has when the client is in the trusted network, click **Add** to do the following:
    - **Domain:** Type the domain to be added.
    - Click **Save** to save the domain or click **Cancel** to not save the domain.
  - **Trusted servers:** For each server address that a network interface has when the client is in the trusted network, click **Add** and do the following:
    - **Servers:** Type the server to be added.
    - Click **Save** to save the server or click **Cancel** to not save the server.

Configure the Citrix SSO protocol for Android

- **Connection name:** Type a name for the VPN connection. This field is required.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Server name or IP address:** Type the FQDN or IP address of the NetScaler Gateway.
- **Authentication type for the connection:** Choose an authentication type and complete any of these fields that appear for the type:
  - **User name** and **Password:** Type your VPN credentials for the **Authentication types** of **Password** or **Password and Certificate**. Optional. If you don't provide the VPN credentials, the Citrix VPN app prompts for a user name and password.
  - **Identity credential:** Appears for the **Authentication types** of **Certificate** or **Password and Certificate**. In the list, select an identity credential.
- **Enable per-app VPN:** Select whether to enable per-app VPN. If you don't enable a per-app VPN, all traffic goes through the Citrix VPN tunnel. If you enable a per-app VPN, specify the following settings. The default is **Off**.
  - **Allow list** or **Block list:** If **Allow list**, all apps in the allow list tunnel through this VPN. If **Block list**, all apps except those apps on the block list tunnel through this VPN.
  - **Application List:** The apps on an allow list or block list. Click **Add** and then type a comma-separated list of app package names.
- **Custom XML:** Click **Add** and then type the custom parameters. Citrix Endpoint Management supports these parameters for Citrix VPN:
  - **DisableUserProfiles:** Optional. To enable this parameter, type **Yes** for the **Value**. If enabled, Citrix Endpoint Management doesn't display user-added VPN connections and the user can't add a connection. This setting is a global restriction and applies to all VPN profiles.
  - **userAgent:** A string value. You can specify a custom User Agent string to send in each HTTP request. The specified user agent string gets appended to the existing Citrix VPN user agent.
  - **IsAlwaysOnVpn:** Optional. This property determines whether the VPN profile is an Always ON VPN profile or not. Set to **Yes** to indicate that VPN profile is an Always On VPN profile, default is **No**. Only one VPN profile can have this property set to **Yes** for Always On VPN to function reliably.

Configure VPNs to support NAC

1. Use the **Connection type** of **Custom SSL** to configure the NAC filter.
2. Specify a **Connection name** of **VPN**.
3. For **Custom XML**, click **Add** and do the following:
   - **Parameter name:** Type **XenMobileDeviceId**. This field is the device ID to use for the NAC check based on device enrollment in Citrix Endpoint Management. If Citrix Endpoint Man-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

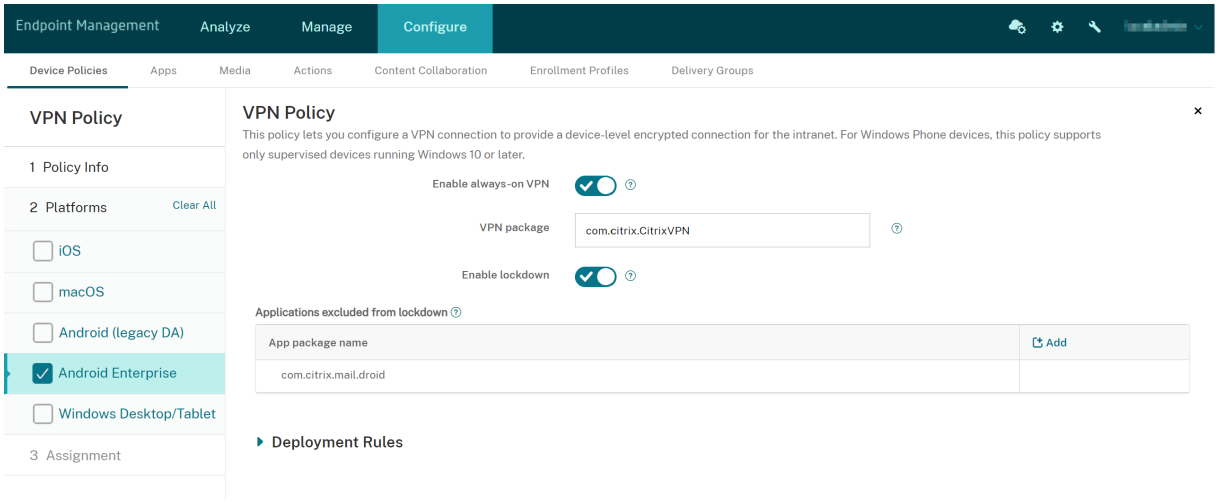
agement enrolls and manages the device, the VPN connection is allowed. Otherwise, authentication is denied at the time of VPN establishment.

- **Value:** Type **DeviceID_${device.id}**, which is the value for the parameter **XenMobileDeviceId**.
- Click **Save** to save the parameter.

Configure VPNs for Android Enterprise

To configure VPNs for Android Enterprise devices, create an Android Enterprise managed configuration device policy for the Citrix SSO app. See Configure VPN profiles for Android Enterprise.

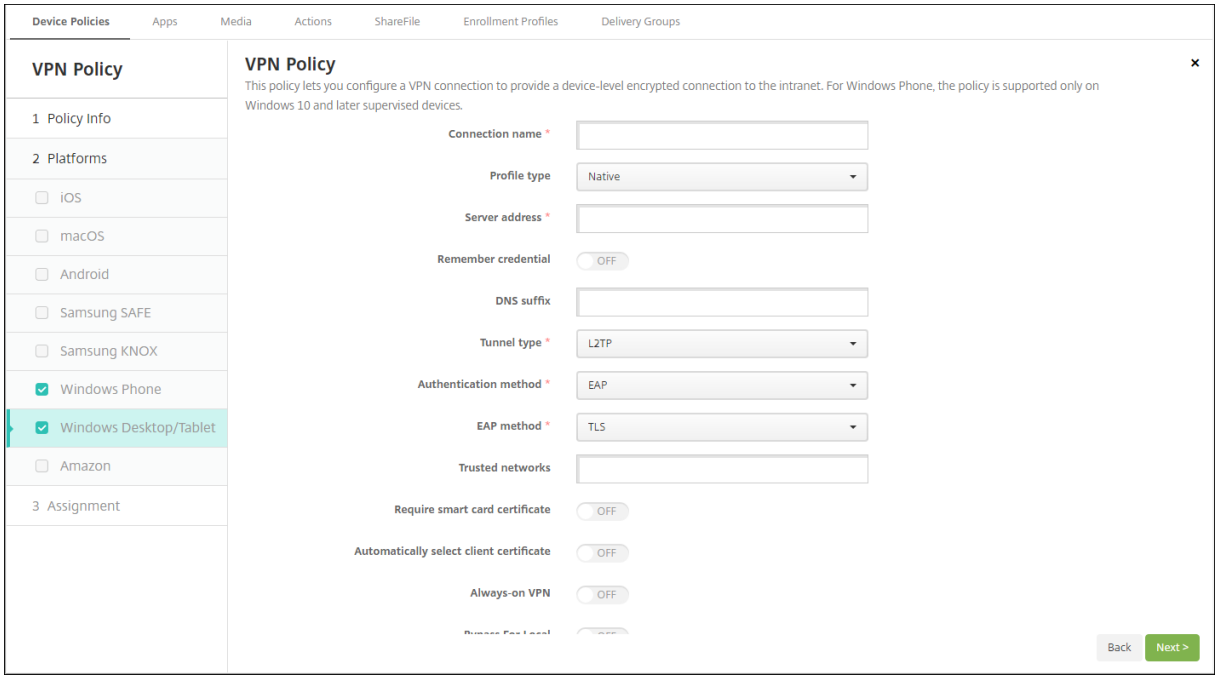
Android Enterprise settings



- **Enable always-on VPN:** Select whether the VPN is always on. The default is **Off**. When enabled, the VPN connection stays on until the user manually disconnects.
- **VPN package** Type the package name for the VPN app devices use.
- **Enable lockdown:** If disabled, no app can access the network if a VPN connection doesn't exist. If enabled, the apps you configure in the following settings can access the network, even if a VPN connection doesn't exist. Available for Android 10 and later devices.
- **Applications exluded from lockdown:** Click **Add** to type the package names of the apps that you want to bypass the lockdown setting.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Windows Desktop/Tablet settings



- **Connection name:** Enter a name for the connection. This field is required.
- **Profile type:** In the list, select either **Native** or **Plugin**. The default is **Native**.
- **Configure Native profile type:** These settings apply to the VPN built into users'Windows devices.
  - **Server address:** Type the FQDN or IP address for the VPN server. This field is required.
  - **Remember credential:** Select whether to cache the credential. The default is **Off**. When enabled, credentials are cached whenever possible.
  - **DNS Suffix:** Type the DNS suffix.
  - **Tunnel type:** In the list, select the type of VPN tunnel to use. The default is **L2TP**. Possible options are:
    - **L2TP:** Layer 2 Tunneling Protocol with pre-shared key authentication.
    - **PPTP:** Point-to-Point Tunneling.
    - **IKEv2:** Internet Key Exchange version 2.
  - **Authentication method:** In the list, select the authentication method to use. The default is **EAP**. Possible options are:
    - **EAP:** Extended Authentication Protocol.
    - **MSChapV2:** Use the Microsoft Challenge-Handshake Authentication Protocol for mutual authentication. This option isn't available when you select **IKEv2** for the tunnel type.
  - **EAP method:** In the list, select the EAP method to be used. The default is **TLS**. This field isn't available when MSChapV2 authentication is enabled. Possible options are:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

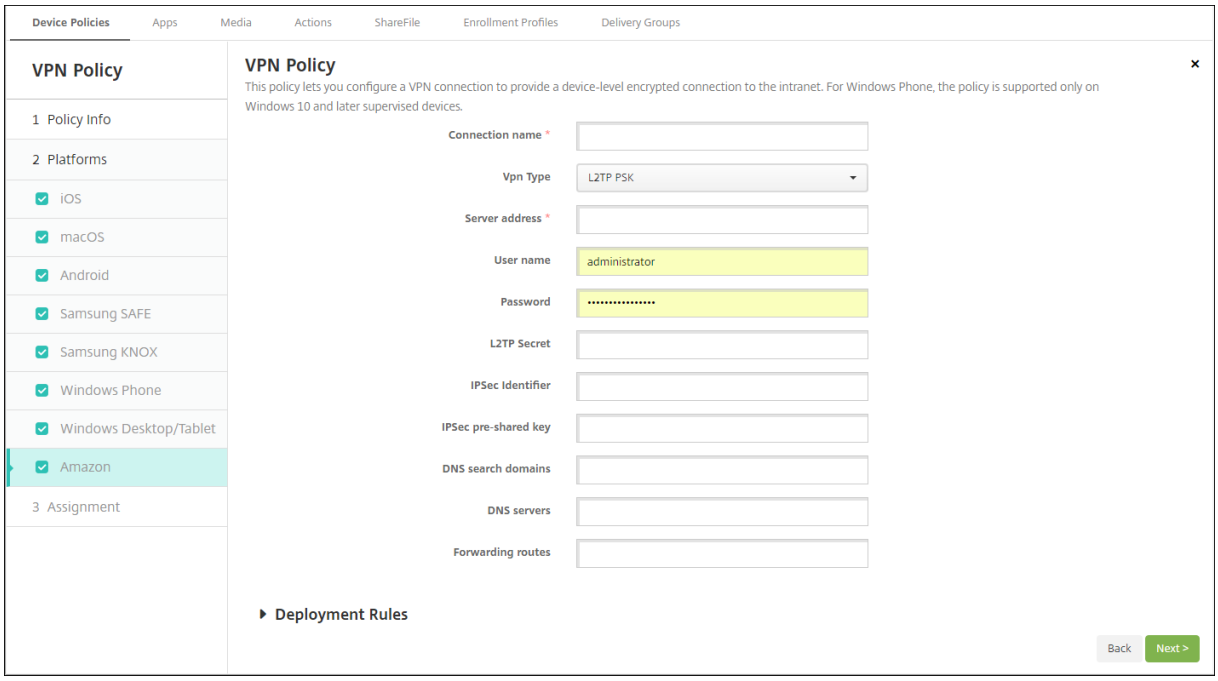
    - **TLS:** Transport Layer Security
    - **PEAP:** Protected Extensible Authentication Protocol
  - **Trusted networks:** Type a list of networks separated by commas that do not require a VPN connection for access. For example, when users are on your company wireless network, they can access protected resources directly.
  - **Require smart card certificate:** Select whether to require a smart card certificate. The default is **Off**.
  - **Automatically select client certificate:** Select whether to automatically choose the client certificate to use for authentication. The default is **Off**. This option is unavailable when you enable **Require smart card certificate**.
  - **Always on VPN:** Select whether the VPN is always on. The default is **Off**. When enabled, the VPN connection stays on until the user manually disconnects.
  - **Bypass For Local:** Type the address and port number to allow local resources to bypass the proxy server.

- **Configure Plugin profile type:** These settings apply to VPN plug-ins got from the Windows Store and installed on users' devices.

  - **Server address:** Type the FQDN or IP address for the VPN server. This field is required.
  - **Remember credential:** Select whether to cache the credential. The default is **Off**. When enabled, credentials are cached whenever possible.
  - **DNS Suffix:** Type the DNS suffix.
  - **Client app ID:** Type the package family name for the VPN plug-in.
  - **Plugin Profile XML:** Select the custom VPN plug-in profile to be used by clicking **Browse** and navigating to the file's location. Contact the plug-in provider for format and details.
  - **Trusted networks:** Type a list of networks separated by commas that do not require a VPN connection for access. For example, when users are on your company wireless network, they can access protected resources directly.
  - **Always on VPN:** Select whether the VPN is always on. The default is **Off**. When enabled, the VPN connection stays on until the user manually disconnects.
  - **Bypass For Local:** Type the address and port number to allow local resources to bypass the proxy server.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Amazon settings



- **Connection name:** Enter a name for the connection.
- **VPN type:** Select the connection type. Possible options are:
  - **L2TP PSK:** Layer 2 Tunneling Protocol with pre-shared key authentication. This setting is the default.
  - **L2TP RSA:** Layer 2 Tunneling Protocol with RSA authentication.
  - **IPSEC XAUTH PSK:** Internet Protocol Security with pre-shared key and extended authentication.
  - **IPSEC HYBRID RSA:** Internet Protocol Security with hybrid RSA authentication.
  - **PPTP:** Point-to-Point Tunneling.

The following sections list the configuration options for each of the preceding connection types.

Configure L2TP PSK settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **L2TP Secret:** Type the shared secret key.
- **IPSec Identifier:** Type the name of the VPN connection that users see on their devices when connecting.
- **IPSec pre-shared key:** Type the secret key.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **DNS search domains:** Type the domains against which a user device's search domain list can match.
- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.

Configure L2TP RSA settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **L2TP Secret:** Type the shared secret key.
- **DNS search domains:** Type the domains against which a user device's search domain list can match.
- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **Server certificate:** In the list, select the server certificate to be used.
- **CA certificate:** In the list, select the CA certificate to be used.
- **Identity credential:** In the list, select the identity credential to be used.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.

Configure IPSEC XAUTH PSK settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **IPSec Identifier:** Type the name of the VPN connection that users see on their devices when connecting.
- **IPSec pre-shared key:** Type the shared secret key.
- **DNS search domains:** Type the domains against which a user device's search domain list can match.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.

Configure IPSEC AUTH RSA settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **DNS search domains:** Type the domains against which a user device's search domain list can match.
- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **Server certificate:** In the list, select the server certificate to be used.
- **CA certificate:** In the list, select the CA certificate to be used.
- **Identity credential:** In the list, select the identity credential to be used.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.

Configure IPSEC HYBRID RSA settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **DNS search domains:** Type the domains against which a user device's search domain list can match.
- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **Server certificate:** In the list, select the server certificate to be used.
- **CA certificate:** In the list, select the CA certificate to be used.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Click **Save** to save the route or click **Cancel** to not save the route.

Configure PPTP settings for Amazon

- **Server address:** Type the IP address for the VPN server.
- **User name:** Type an optional user name.
- **Password:** Type an optional password.
- **DNS search domains:** Type the domains against which a user device's search domain list can match.
- **DNS servers:** Type the IP addresses of DNS servers to be used for resolving the specified domains.
- **PPP encryption (MPPE):** Select whether to enable data encryption with Microsoft Point-to-Point Encryption (MPPE). The default is **Off**.
- **Forwarding routes:** If your corporate VPN server supports forwarding routes, for each forwarding route to use, click **Add** and do the following:
  - **Forward route:** Type the IP address for the forwarding route.
  - Click **Save** to save the route or click **Cancel** to not save the route.

Wallpaper device policy

September 6, 2025

The Wallpaper device policy lets you add a .png or .jpg file to set wallpaper on an iOS device lock screen, home screen, or both. This policy is available for supervised devices only. To use different wallpapers on iPads and iPhones, you need to create different wallpaper policies and deploy them to the appropriate users.

The following table lists the Apple recommended image dimensions for iOS devices.

iPhone

Device	Image dimensions in pixels
iPhone 12 Pro Max	2778 x 1284
iPhone 12 & iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device	Image dimensions in pixels
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 2nd Gen	1334 x 750
iPhone 7 Plus, 8 Plus	2208 x 1242
iPhone 7, 8	1334 x 750
iPhone 8 Plus	1334 x 750
iPhone 8	1334 x 750

iPad

Device	Image dimensions in pixels
iPad Pro (1st, 2nd, and 3rd Gen 12.9")	2732 x 2048
iPad Pro 10.5 inch	2224 x 1668
iPad Pro (9.7 inch)	1536 x 2048
iPad Air 2	2048 x 1536

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Apply to:** In the list, select **Lock screen**, **Home (icon list) screen**, or **Lock and home screens** to set where the wallpaper is to appear.
- **Wallpaper file:** To select the wallpaper file, click **Browse** and then navigate to the file location.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Web Content Filter device policy

September 6, 2025

You can filter web content on iOS devices by using the Apple auto-filter function with specific sites that you add to allow or block lists. Web Content Filter device policy is available only on iOS devices in Supervised mode. For information about placing an iOS device into Supervised mode, see Deploy devices using Apple Configurator 2.

> **Note:**
>
> - Android devices don't support web content filtering.
> - From iOS version 16.5 and later, the Web Content Filter device policy stops recognizing `https://localhost` in the allow list. This results in some apps becoming unresponsive. Also, adding a derivative of the URL such as `http://localhost:`, `http://localhost:*`, and so on to the allow list doesn't resolve the issue.

To add or configure this policy, go to **Configure** > **Device Policies**. For more information, see Device policies.

iOS settings

- **Filter type:** Click **Built-in** or **Plug-in** in the drop-down list, and then follow the procedures that follow for the option you choose. The default is **Built-in**.

Built-in filter type

- **Web Content Filter**
  - **Auto filter enabled:** Whether to use the Apple auto-filter function to analyze websites for inappropriate content. The default is **Off**.
  - **Permitted URLs:** This list is ignored when **Auto filter enabled** is set to **Off**. When **Auto filter enabled** is set to **On**, the items in this list are always accessible whether the auto filter allows access or not. For each URL you want to add to the allow list, click **Add** and do the following:
    - Type the URL of the permitted website. You must add `https://` or `https://` before the web address.
    - Click **Save** to save the website to the allow list or click **Cancel** not to save it.
  - **Blocked URLs:** Items in this list are always blocked. For each URL you want to add to the block list, click **Add** and do the following:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

        * Enter the URL of the website to be blocked. You must add `https://` or `https://` before the web address.
        * Click **Save** to save the website to the block list or click **Cancel** not to save it.

- **Bookmark allow list**

    - **Bookmark allow list:** Specifies the sites that users can access. To enable access to websites, add their URL.

        * **URL:** The URL of each website that users can access. For example, to enable access to the Citrix Secure Hub store, add the Citrix Endpoint Management server URL to the **URL** list. You must add `https://` or `https://` before the web address. This field is required.
        * **Bookmark folder:** Enter an optional bookmark folder name. If this field is left blank, the bookmark is added to the default bookmarks directory.
        * **Title:** Enter a descriptive title for the website. For example, type "Google"for the URL `https://google.com`.
        * Click **Save** to save the website to the allow list or click **Cancel** not to save it.

Plug-in filter type

- **Filter name:** Enter a unique name for the filter.
- **Identifier:** Enter the bundle ID of the plug-in that provides the filtering service.
- **Service address:** Enter an optional server address. Valid formats are IP address, host name, or URL.
- **User name:** Enter an optional user name for the service.
- **Password:** Enter an optional password for the service.
- **Certificate:** Click an optional identity certificate in the drop-down list that has to be used to authenticate the user to the service. The default is **None**.
- **Filter WebKit traffic:** Select whether to filter WebKit traffic.
- **Filter Socket traffic:** Select whether to filter socket traffic.
- **Custom Data:** For each custom key you want to add to the web filter, click **Add** and then do the following:

    - **Key:** Type the custom key.
    - **Value:** Type a value for the custom key.
    - Click **Save** to save the custom key or click **Cancel** not to save it.

- **Policy settings**

    - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**

        * **Select date:** Click the calendar to select the specific date for removal.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    - **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.

Web clip device policy

September 6, 2025

You can place shortcuts, or web clips, to websites to appear alongside apps on user devices. You can specify your own icons to represent the web clips for iOS, iPadOS, macOS, and Android devices. Windows tablet requires just a label and a URL. For iOS and iPadOS devices, configure the home screen layout device policy to organize the web clips you create. If you restrict access to apps on iOS, make sure that you configure the restriction device policy to allow web clips. For information on configuring these policies, see Home screen layout device policy and Restrictions device policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

iOS settings

- **Label:** Type the label that is to appear with the web clip.
- **URL:** Type the URL associated with the web clip. The URL must begin with a protocol, for example, `https://server`.
- **Removable:** Select whether users can remove the web clip. The default is **Off**. This option isn't supported on shared iPads.
- **Icon to be updated:** Select the icon to be used for the web clip by clicking **Browse** and navigating to the file location.
- **Precomposed icon:** Select whether the icon has effects (rounded corners, drop shadow, and reflective shine) applied to it. The default is **Off**, which adds the effects.
- **Full screen:** Select whether the linked webpage opens in full-screen mode. This setting also enables an iPad to only open a single website. Alternatively, to set up iPads to run in Kiosk mode, use the App lock device policy. For more information, see Configure an iPad as a kiosk. The default is **Off**.
- **Policy settings**
    - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
        - **Select date:** Click the calendar to select the specific date for removal.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

        * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs. Only available for iOS 6.0 and later.
    - **Profile scope:** Select whether the policy applies to a User or an entire System. The default value is **System**. Only available for iOS 9.3 and later.

macOS settings

- **Label:** Type the label that is to appear with the web clip.
- **URL:** Type the URL associated with the web clip. The URL must begin with a protocol, for example, `https://server`.
- **Icon to be updated:** Select the icon to be used for the web clip by clicking Browse and navigating to the file location.
- **Policy settings**
    - **Remove policy:** Choose a method for scheduling policy removal. Available options are **Select date** and **Duration until removal (in hours)**
        * **Select date:** Click the calendar to select the specific date for removal.
        * **Duration until removal (in hours):** Type a number, in hours, until policy removal occurs.
    - **Allow user to remove policy:** You can select when users can remove the policy from their device. Select **Always**, **Passcode required**, or **Never** from the menu. If you select **Passcode required**, type a passcode in the **Removal passcode** field.

Android settings

- **Rule:** Select whether this policy adds or removes a web clip. The default is **Add**.
- **Label:** Type the label that is to appear with the web clip.
- **URL:** Type the URL associated with the web clip.
- **Define an icon:** Select whether to use an icon file. The default is **Off**.
- **Icon file:** If **Define an icon** is **On**, select the icon file to use by clicking **Browse** and navigating to the file location.

Windows Desktop/Tablet settings

- **Name:** Type the label that is to appear with the web clip.
- **URL:** Type the URL associated with the web clip.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Windows Agent device policy

March 7, 2024

Use the Windows Agent device policy to run PowerShell scripts on managed Windows desktops and tablets. You can point to script files uploaded to Citrix Endpoint Management as an enterprise app and to other servers that host scripts. For information about adding enterprise apps, see Add apps.

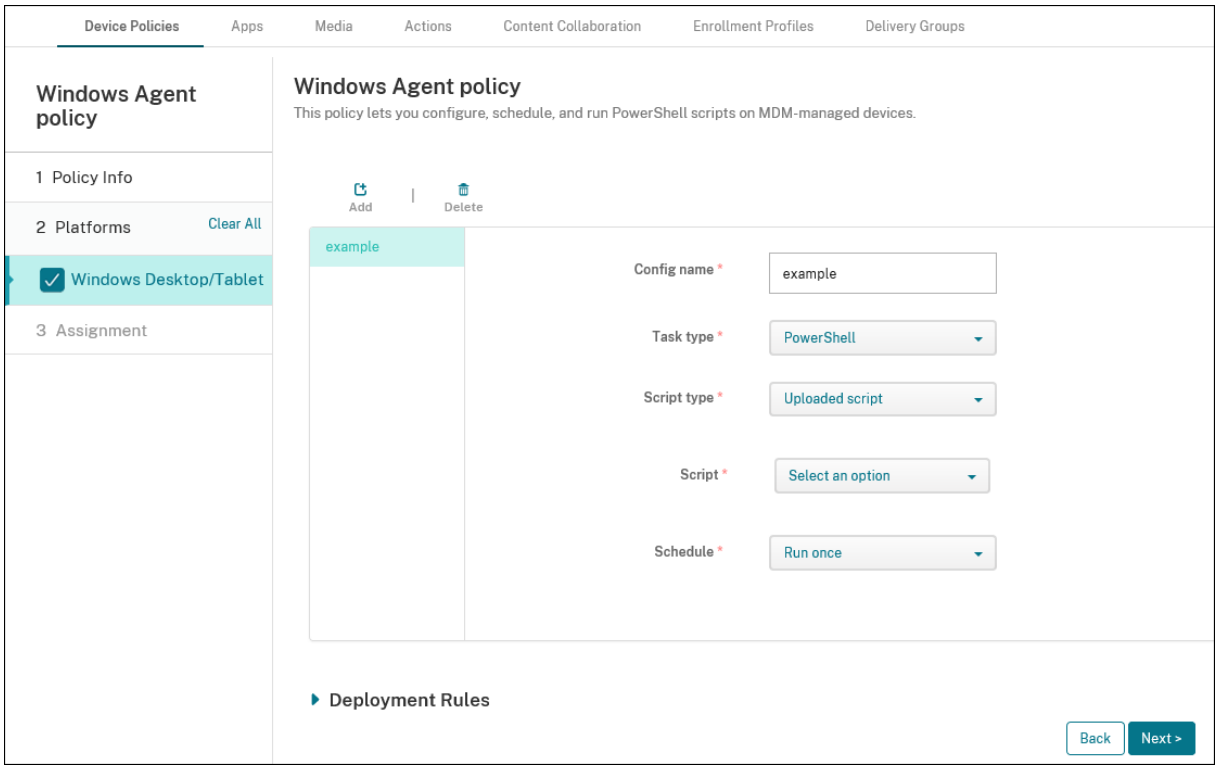
All scripts run under privileged status, you don't need to run scripts as an administrator.

After deploying and running the script, you can configure automated actions based on the results of the script. For instance, you run a script that monitors a registry key and returns a result. Based on the returned result, an automated action runs. The action grants or denies access to an app, marks the device as out of compliance, or has other effects.

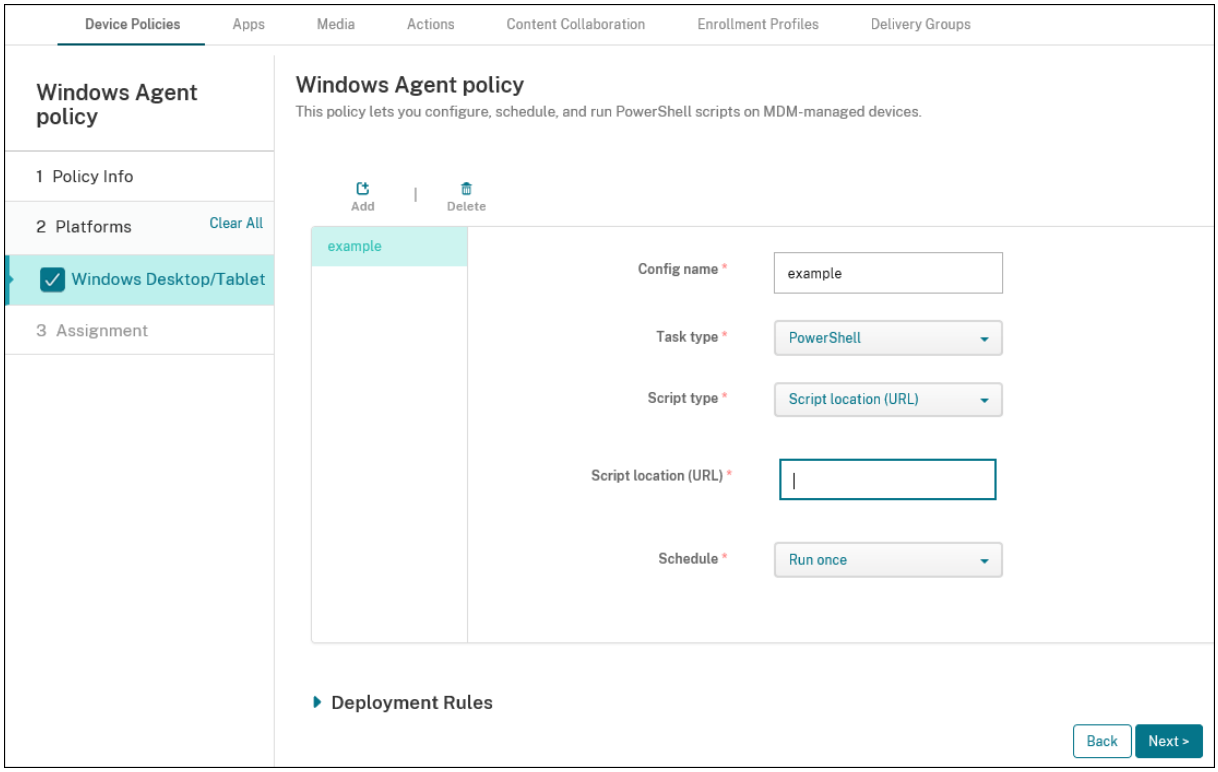
You can also use this policy to deploy customized MSI installers by configuring a PowerShell script that points to an .msi file and an .mst file.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows Desktop and Tablet settings



© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Config name:** Type a descriptive name for your configuration.
- **Task type:** Select **PowerShell**.
- **Script type:** Select **Uploaded script** for scripts that you've uploaded to Citrix Endpoint Management or select **Script location (URL)** for scripts hosted externally. For more information on how to upload a script to Citrix Endpoint Management, see Add `Win32` apps as Enterprise apps.
  - **Select script:** If you chose **Uploaded script**, select the script to run.
  - **Script location (URL):** If you chose **Script location (URL)**, enter the location of the script to run. This URL must deliver the script as a payload. Citrix Endpoint Management doesn't support URLs that deliver scripts as a JavaScript download. The script must also be publicly available.
- **Schedule:** Select **Run once** to run the selected script one time or select **Run on a recurring basis** to run the script regularly.
  - **Run every (hours):** Type the number of hours between script runs.

To check on the status of a script, navigate to **Manage > Devices** in your console. Select the device on which you want to check the script status and click **Edit**. Under **Properties**, you can check the status of your scripts by clicking **Download** under the **Windows Agent** heading.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Deploy a PowerShell script to trigger an automated action

1. Create a PowerShell script to monitor a registry key. The following PowerShell script checks to see if the firewall is enabled.

```
$body = @{
  }

$firewallEnabled = Get-ItemPropertyValue HKLM:\SYSTEM\
   CurrentControlSet\Services\SharedAccess\Parameters\
   FirewallPolicy\StandardProfile -Name EnableFirewall
if($firewallEnabled -eq 1){

$body["firewallEnabled"]="true"
 }
  else {

$body["firewallEnabled"]="false"
 }

$body | ConvertTo-Json -Depth 10
```

   This script returns a value of either

```
{

    "firewallEnabled":  "true"
 }
```

   or

```
{

    "firewallEnabled":  "false"
 }
```

2. Upload the script to the Citrix Endpoint Management console as an enterprise app or host the script at an accessible URL.
3. Configure the Windows Agent device policy described in this article. Make sure that the script is scheduled to run immediately.
4. After the script runs, determine the script status.
   a) Navigate to **Manage > Devices** in your console.
   b) Select the device to check its script status and then click **Edit**.
   c) Click **Download** under the **Windows Agent** heading.
5. Configure an automated action based on the status received. For more information on configuring automated actions, see Create an automated action based on a Windows Agent device

© 1997–2025 Citrix Systems, Inc. All rights reserved.

policy result. That section shows the specific automated actions created for the example script and Windows Agent device policy.

Windows GPO Configuration device policy

September 6, 2025

The Windows GPO Configuration device policy allows you to:

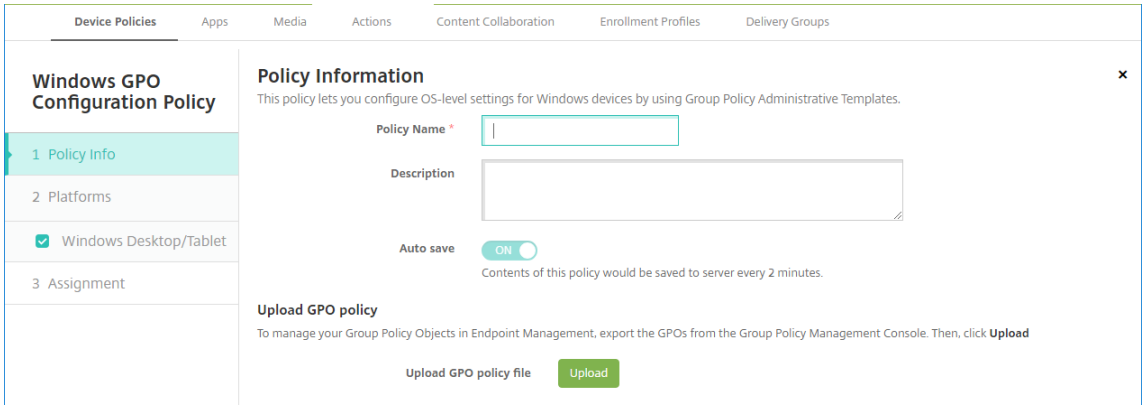
- Use the Citrix Endpoint Management console to import Group Policy Objects (GPOs) and deploy them to Windows 10 and Windows 11 devices.
- Configure GPOs for any Windows device supported by Citrix Workspace Environment Management.
- Configure GPOs at a device and user level.

Import GPOs for deployment to Windows 10 and Windows 11 devices

Rather than relying on an AD administrator to use the Group Policy Management console to manage GPOs, you can import and deploy GPOs through the Citrix Endpoint Management console.

To create a backup of your GPOs in Citrix Endpoint Management:

1. Request that your AD administrator export GPOs from the Group Policy Management console and provide the files to you.
2. In the Citrix Endpoint Management console, go to **Configure > Device Policies** and create a **Windows GPO Configuration** policy.
3. Click **Upload**, locate the file, and then click **Open** to import the file.



For information about configuring GPOs, see in this article, Windows desktop and tablet settings.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure GPOs for deployment to Citrix Workspace Environment Management

The Windows GPO Configuration device policy allows you to configure GPOs for any Windows device supported by Citrix Workspace Environment Management (WEM). Citrix Endpoint Management pushes the policies to the Citrix WEM service. The WEM service then applies the GPOs to devices and their apps by using the WEM agent installed on devices.

For information about installing the Workspace Environment Management agent, see Install and configure.

This policy uses all Windows OS ADMX files. If you want to upload a third-party ADMX file, use the App Configuration device policy. For more information on uploading third-party ADMX files, see Application Configuration device policy.

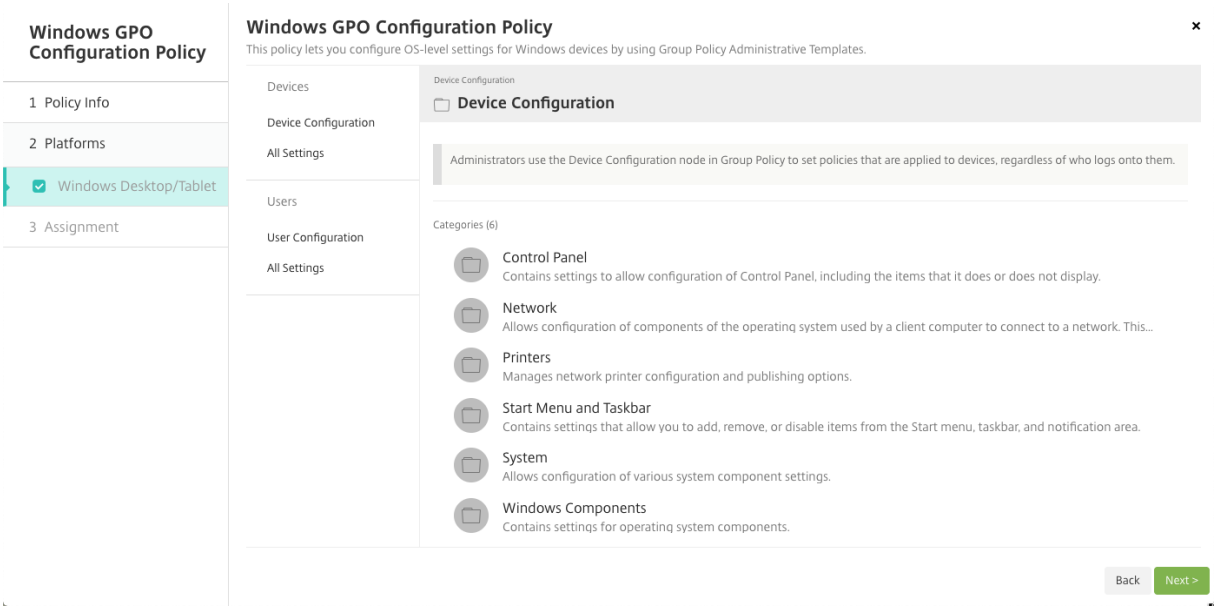
- You can push GPO configurations to any device that WEM supports, even if Citrix Endpoint Management doesn't support the device natively. For a list of the devices supported, see Operating System requirements.
- This policy requires that a device has the WEM agent installed and configured. There is no need to MDM or MAM enroll the devices.
- Citrix Endpoint Management pushes GPO settings through the WEM channel. (Microsoft doesn't support pushing device-level settings through the MDM channel.) Devices which receive the Windows GPO Configuration device policy run in the Citrix Endpoint Management mode called WEM. In the **Manage > Devices** list of enrolled devices, the **Mode** column for WEM-managed devices lists **WEM**.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Windows desktop and tablet settings

This policy allows you to configure GPOs at a device and user level.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Select and configure the Windows GPO to deploy to your Windows devices. You can modify **Device Configuration** and **User Configuration**. Policies are listed in a tree structure. Click **All Settings** to display every setting. For information about the settings, download a GPO reference sheet from Microsoft.

To configure a setting, you first enable it. During configuration, Citrix Endpoint Management auto-saves the changes so that those settings persist. If you try to leave the page before a setting has been saved, a pop-up message indicates that there are unsaved changes.

If a setting has two options, a radio button selection appears. With more than two options, a menu appears.

> **Note:**
>
> If you need to check which settings you configured, you can do the following.
>
> 1. In the Citrix Endpoint Management console, open the **Windows GPO Configuration** policy you want to edit.
> 2. Under **Devices** or **Users**, select **All Settings**.
> 3. Sort the table by **Status**, ascending. All unconfigured policies have the status **Not Configured**. The policies you configure are listed at the top.

Windows Hello for Business device policy

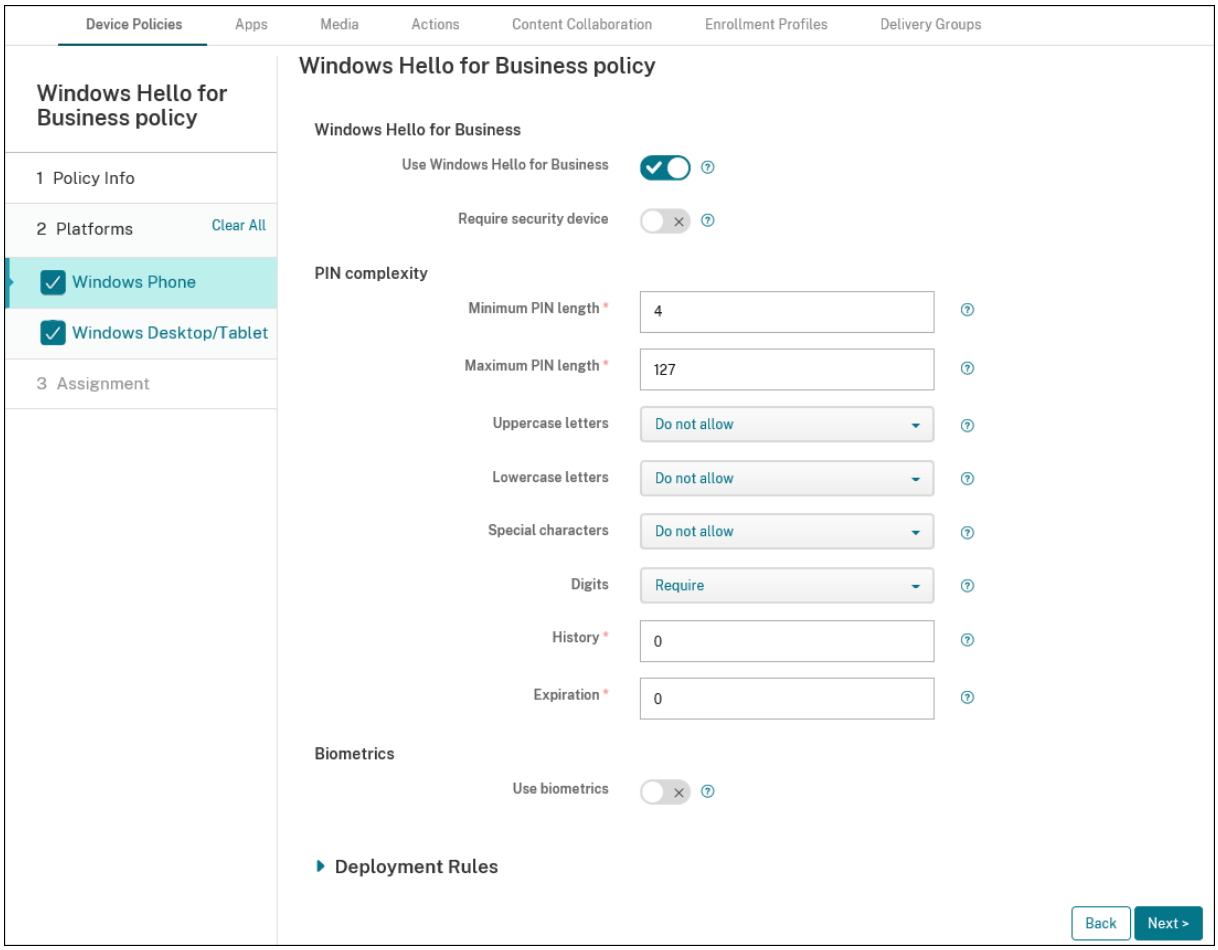
March 7, 2024

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Windows Hello for Business allows users to sign on to Windows devices by using their Active Directory or Azure Active Directory account. You use the **Windows Hello for Business** device policy to enable the feature so users can provision Windows Hello for Business on their device. The policy also lets you configure passcode limitations and other security features.

Go to **Configure > Device Policies** to add the **Windows Hello for Business** device policy. Configure these settings:

Windows Desktop/Tablet settings



- **Use Windows Hello for Business:** Enable the feature to allow users to provision Windows Hello for Business on their device.
- **Require security device:** Require that users have a Trusted Platform Module (TPM) to sign on.
- **Minimum/Maximum PIN length:** Minimum and maximum length for user PINs. **Minimum PIN Length** defaults to **4**. **Maximum PIN Length** defaults to **127**.
- **Uppercase letters**, **Lowercase letters**, **Special characters:** Select whether to **Allow**, **Require**, or **Do not allow** each type of character. Defaults to **Do not allow**.
- **Digits:** Whether to **Allow**, **Require**, or **Do not allow** digits. Defaults to **Require**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **History:** The number of past PINs that users can't reuse. Defaults to **0**, meaning users can reuse all PINs.
- **Expiration:** The number of days before a user must change their PIN. Defaults to **0**, which means that PINs don't expire.
- **Use biometrics:** Allow the use of biometrics instead of PINs for user sign-on.

Add apps

September 6, 2025

Adding apps to Citrix Endpoint Management provides mobile application management (MAM) capabilities. Citrix Endpoint Management assists with application delivery, software licensing, configuration, and application life cycle management.

MDX-enabling apps is an important part of preparing some types of apps for distribution to user devices. For an introduction to MDX, see Citrix Endpoint Management components and MAM SDK overview.

- Citrix recommends use of the MAM SDK to MDX-enable apps. Or, you can continue to MDX-wrap apps until the MDX Toolkit is deprecated. See Deprecation.
- You can't use the MDX Toolkit to wrap Citrix mobile productivity apps. Get the mobile productivity app MDX files from Citrix downloads.

When you add apps to the Citrix Endpoint Management console, you:

- Configure app settings
- Optionally arrange apps into categories to organize them in Citrix Secure Hub
- Optionally define workflows to require approval before allowing users to access an app
- Deploy apps to users

This article covers the general workflows for adding apps. See the following articles for platform specifics:

- Distribute Android Enterprise apps
- Distribute Apple apps

> **Important:**
>
> Citrix Endpoint Management supports adding and maintaining up to 300 apps. Going over this limit causes your system to become unstable.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App types and features

The following table summarizes the types of apps that you can deploy with Citrix Endpoint Management.

App type	Sources	Notes	See
MDX	iOS and Android apps you develop for your users. Citrix mobile productivity apps.	Develop iOS or Android apps with the MAM SDK or wrap them with the MDX Toolkit. For the mobile productivity apps, download the public-store MDX files from Citrix downloads. Then add the apps to Citrix Endpoint Management.	Add an MDX app
Public app store	Free or paid apps from public app stores such as Google Play or the Apple App Store.	Upload the apps, MDX-enable the apps, then add the apps to Citrix Endpoint Management.	Add a public app store app
Web and SaaS	Your internal network (web apps) or a public network (SaaS).	Citrix Endpoint Management provides mobile single sign-on to native SaaS apps from iOS and Android devices enrolled in MDM. Or, use Security Assertion Markup Language (SAML) application connectors	Add a Web or SaaS app

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App type	Sources	Notes	See
Enterprise	Private apps, including Win32 apps, that aren't MDX-enabled. Private Android Enterprise apps that are MDX-enabled. Enterprise apps are in Content Delivery Network locations or Citrix Endpoint Management servers.	Add the apps to Citrix Endpoint Management.	Add an enterprise app
Web link	Internet web addresses, intranet web addresses, or web apps that don't require single sign-on.	Configure web links in Citrix Endpoint Management.	Add a Web link

When planning app distribution, consider these features:

- About silent installations
- About required and optional apps
- About app categories
- Deliver enterprise apps from the Citrix CDN
- Enable Microsoft 365 apps
- Apply workflows
- App store and Citrix Secure Hub branding
- Citrix Virtual Apps and Desktops™ through the app store

About silent installations

Citrix supports the silent installation and upgrade of iOS, Android Enterprise, and Samsung apps. Silent installation means that users aren't prompted to install apps that you deploy to the device. The apps install automatically in the background.

Prerequisites to implement silent installation:

- For iOS, put the managed iOS device in supervised mode. For more information, see Import iOS & macOS Profile device policy.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- For Android Enterprise, the apps install in the Android work profile on the device. For details, see Android Enterprise.
- For Samsung devices, enable Samsung Knox on the device.

  To do so, you set the Samsung MDM license key device policy to generate Samsung ELM and Knox license access codes. For details, see Samsung MDM license key device policies.

About required and optional apps

When you add apps to a delivery group, you choose whether they're optional or required. Citrix recommends deploying apps as **Required**.

- Required apps install silently on user devices, minimizing interaction. Having this feature enabled also allows apps to update automatically.
- Optional apps allow users to choose what apps to install, but users must start the installation manually through Citrix Secure Hub.

For apps marked as required, users can promptly receive updates in situations such as:

- You upload a new app and mark it as required.
- You mark an existing app as required.
- A user deletes a required app.
- A Citrix Secure Hub update is available.

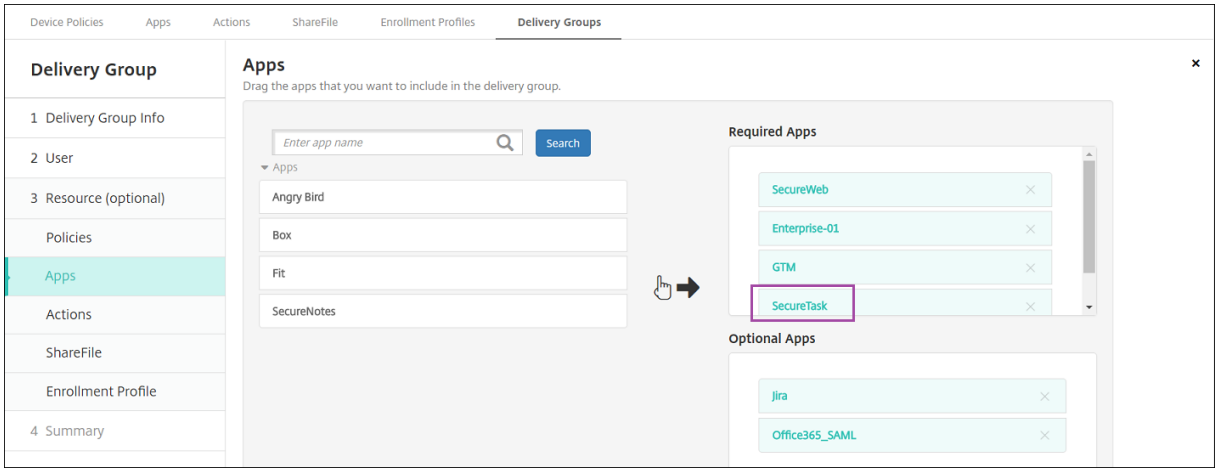
Requirements for forced deployment of required apps

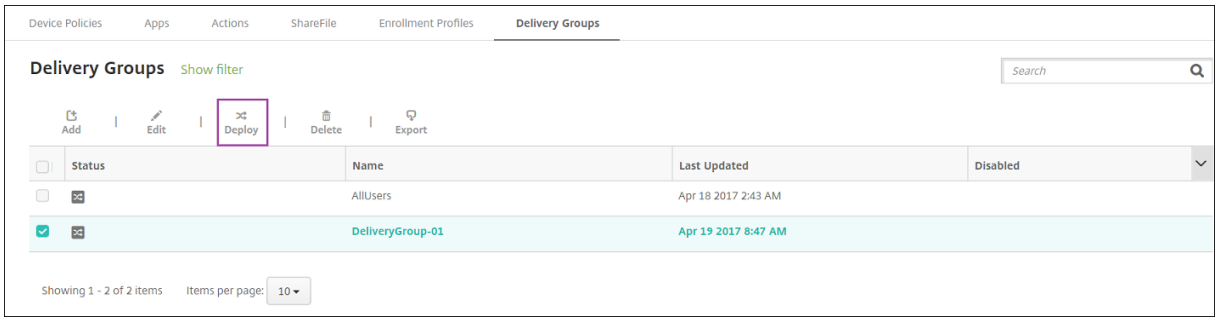
- Citrix Secure Hub 10.5.15 for iOS and 10.5.20 for Android (minimum versions)
- MAM SDK or MDX Toolkit 10.6 (minimum version)
- After you upgrade Citrix Endpoint Management and Citrix Secure Hub: Users with enrolled devices must sign off and then sign on to Citrix Secure Hub to get the required app deployment updates.

Examples

The following examples show the sequence of adding an app named Secure Tasks to a delivery group and then deploying the delivery group.

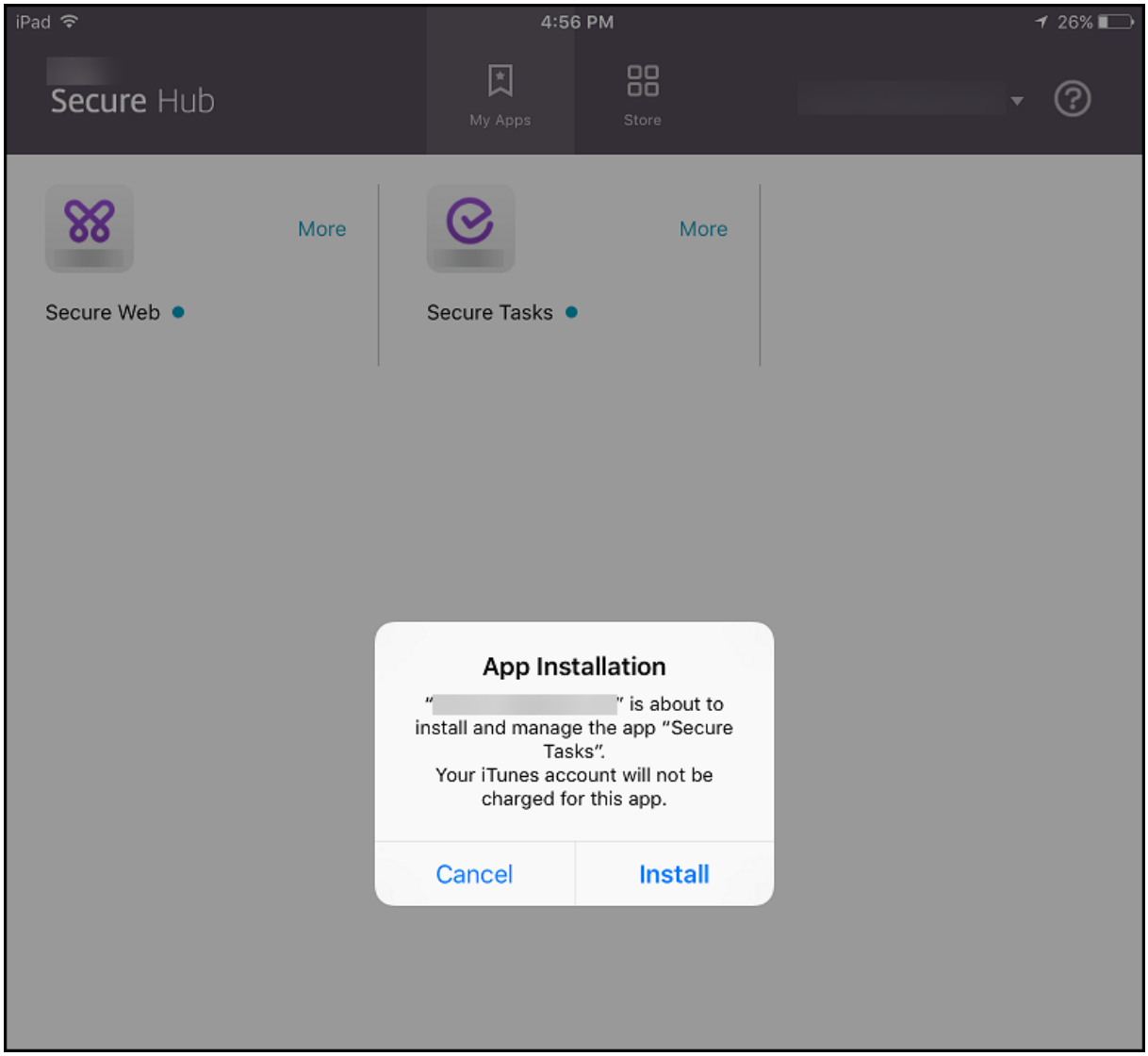
© 1997–2025 Citrix Systems, Inc. All rights reserved.

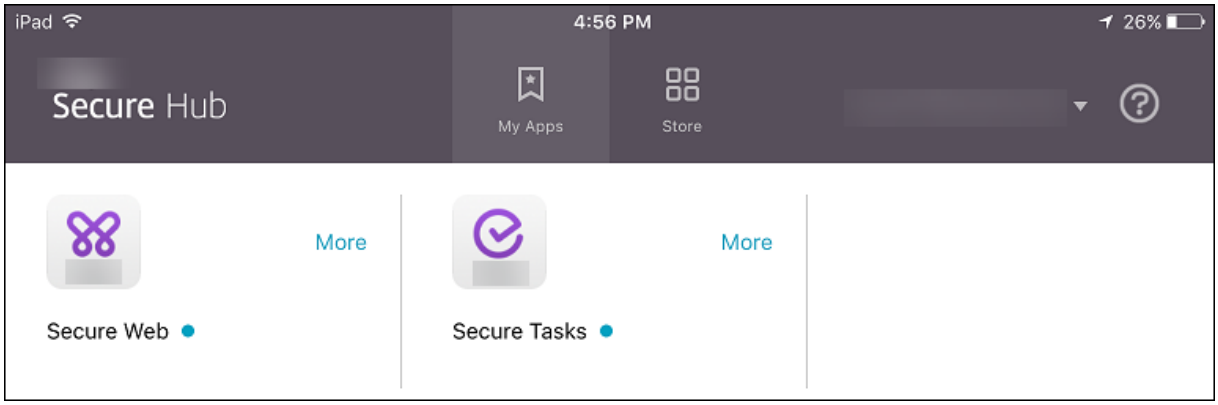




After the sample app, Secure Tasks, deploys to the user device, Citrix Secure Hub prompts the user to install the app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.





Important:

MDX-enabled required apps, including enterprise apps and public app store apps, upgrade immediately. This upgrade occurs even if you configure an MDX policy for an app update grace

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> period and the user chooses to upgrade the app later.

iOS required app workflow for enterprise and public store apps

1. Deploy the mobile productivity app during initial enrollment. The required app is installed on the device.
2. Update the app on the Citrix Endpoint Management console.
3. Use the Citrix Endpoint Management console to deploy the required apps.
4. The app on the home screen is updated. And, for public store apps, the upgrade starts automatically. Users aren't prompted to update.
5. Users open the app from the home screen. Apps upgrade immediately even if you set an App update grace period and the user taps to upgrade the app later.

Android required app workflow for enterprise apps

1. Deploy the mobile productivity app during initial enrollment. The required app is installed on the device.
2. Use the Citrix Endpoint Management console to deploy the required apps.
3. The app is upgraded. (Nexus devices prompt for install updates, but Samsung devices do a silent install.)
4. Users open the app from the home screen. Apps upgrade immediately even if you set an App update grace period and the user taps to upgrade the app later. (Samsung devices do a silent install.)

Android required app workflow for public store apps

1. Deploy the mobile productivity app during initial enrollment. The required app is installed on the device.
2. Update the app on the Citrix Endpoint Management console.
3. Use the Citrix Endpoint Management console to deploy the required apps. Or, open the Citrix Secure Hub Store on the device. The update icon appears in the store.
4. App upgrade starts automatically. (Nexus devices prompt users to install the update.)
5. Open the app on the home screen. The app is upgraded. Users aren't prompted for a grace period. (Samsung devices do a silent install.)

Uninstall an app when the app is configured as required

You can allow users to uninstall an app that is configured as required. Go to **Configure > Delivery Groups** and move the app from **Required Apps** to **Optional Apps**.

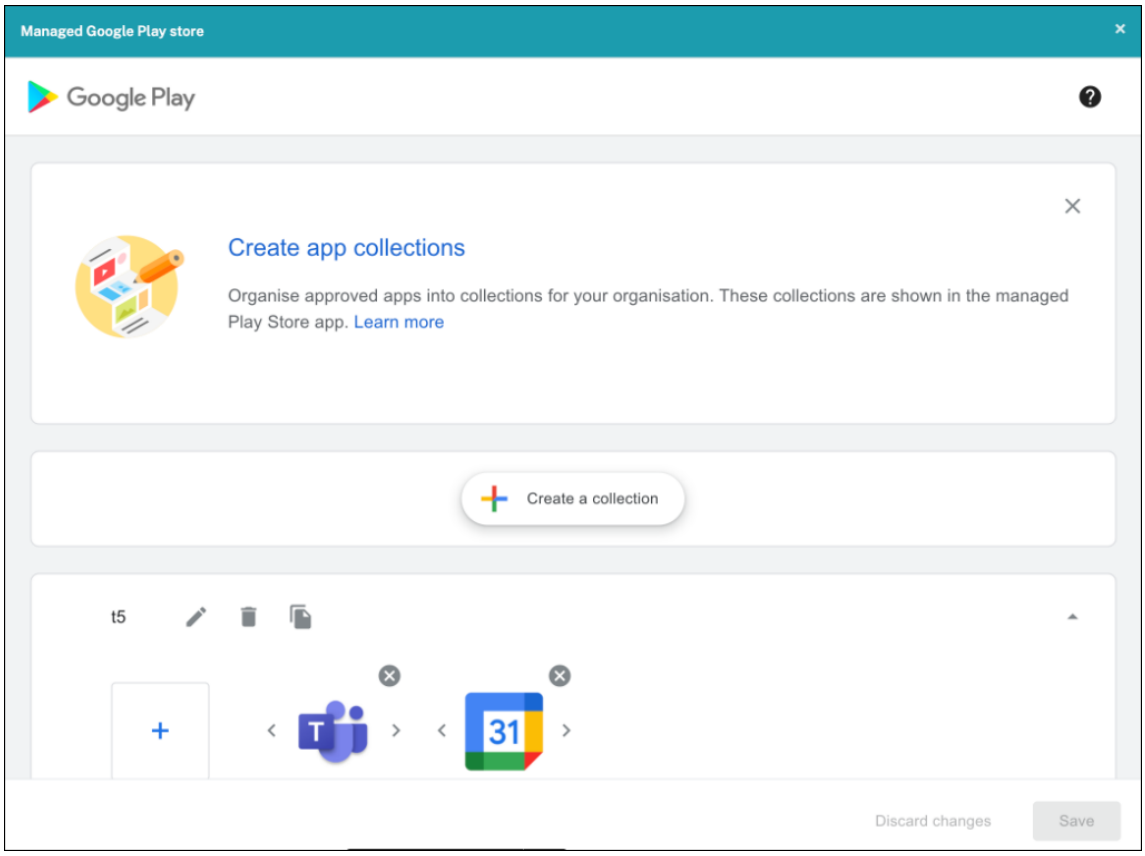
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Recommended: Use a special delivery group to temporarily change an app to optional, so that specific users can uninstall the app. You can then change an existing required app to optional, deploy the app to that delivery group, and then uninstall the app from those devices. After that, if you want future enrollments for that delivery group to require the app, you can set the app back to required.

Organize apps (Android Enterprise)

When users log on to Citrix Secure Hub, they receive a list of the apps, web links, and stores that you set up in Citrix Endpoint Management. In Android Enterprise, you can organize these apps into collections to let users access only certain apps, stores, or web links. For example, you create a Finance collection and then add apps to the collection that only pertain to finance. Or, you can configure a Sales collection to which you assign sales apps.

1. In the Citrix Endpoint Management console, click **Configure > Apps > Organize Apps**. The **Managed Google Play store** window appears.



2. Click **Create a collection** and select the apps to be added to that collection.
3. When you're done adding collections, click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> IT admins need to approve an app before it can be added to a collection on the Managed Google Play window. An IT admin can approve an app by going to https://play.google.com/work. In a future release, you won't need to approve an app before adding it to a collection.

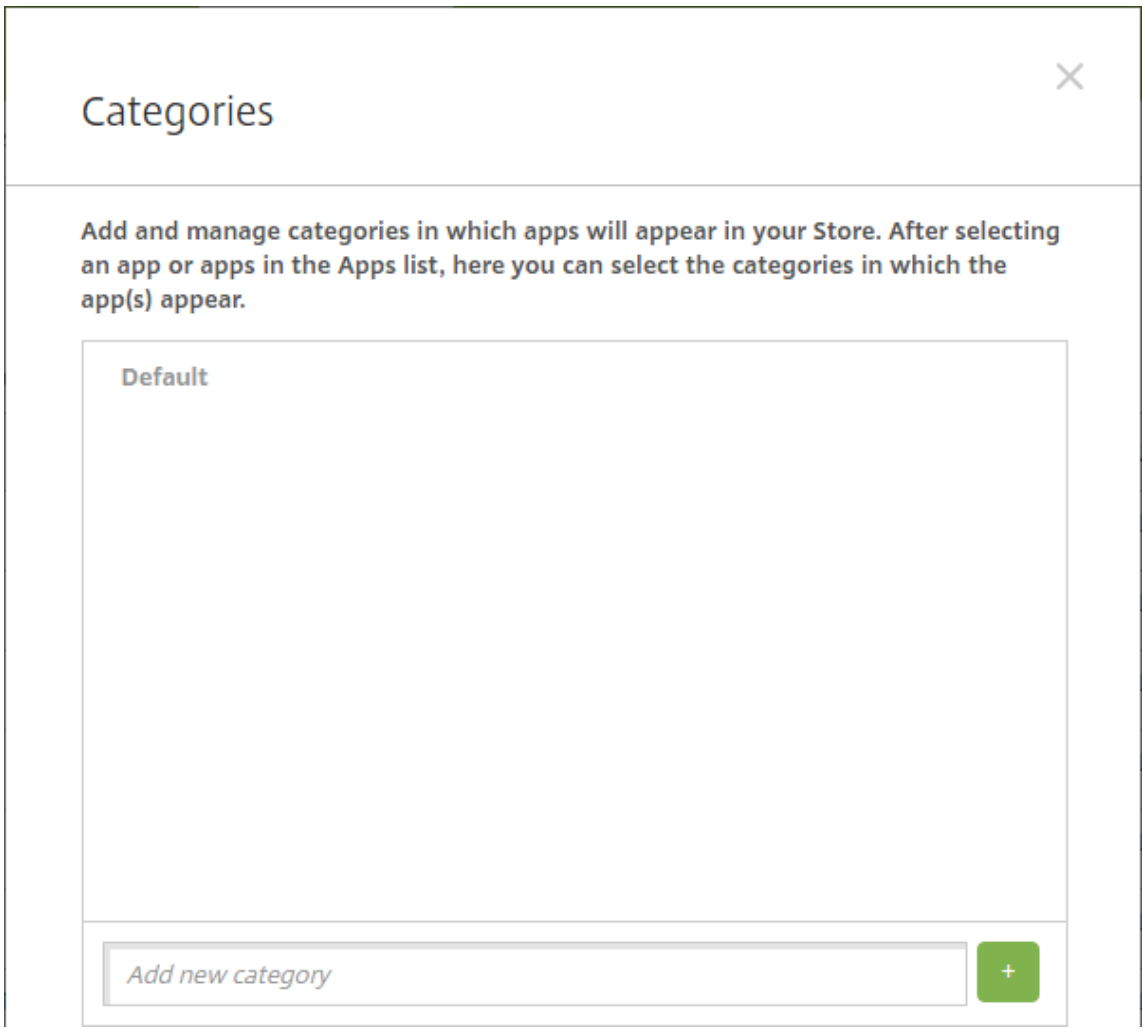
About app categories (iOS and MDX)

When users log on to Citrix Secure Hub, they receive a list of the apps, web links, and stores that you set up in Citrix Endpoint Management. In iOS or MDX, you can use app categories to let users access only certain apps, stores, or web links. For example, you can create a Finance category and then add apps to the category that only pertain to finance. Or, you can configure a Sales category to which you assign sales apps.

When you add or edit an app, web link, or store, you can add the app to one or more of the configured categories.

1. In the Citrix Endpoint Management console, click **Configure > Apps > Category**. The **Categories** dialog box appears.

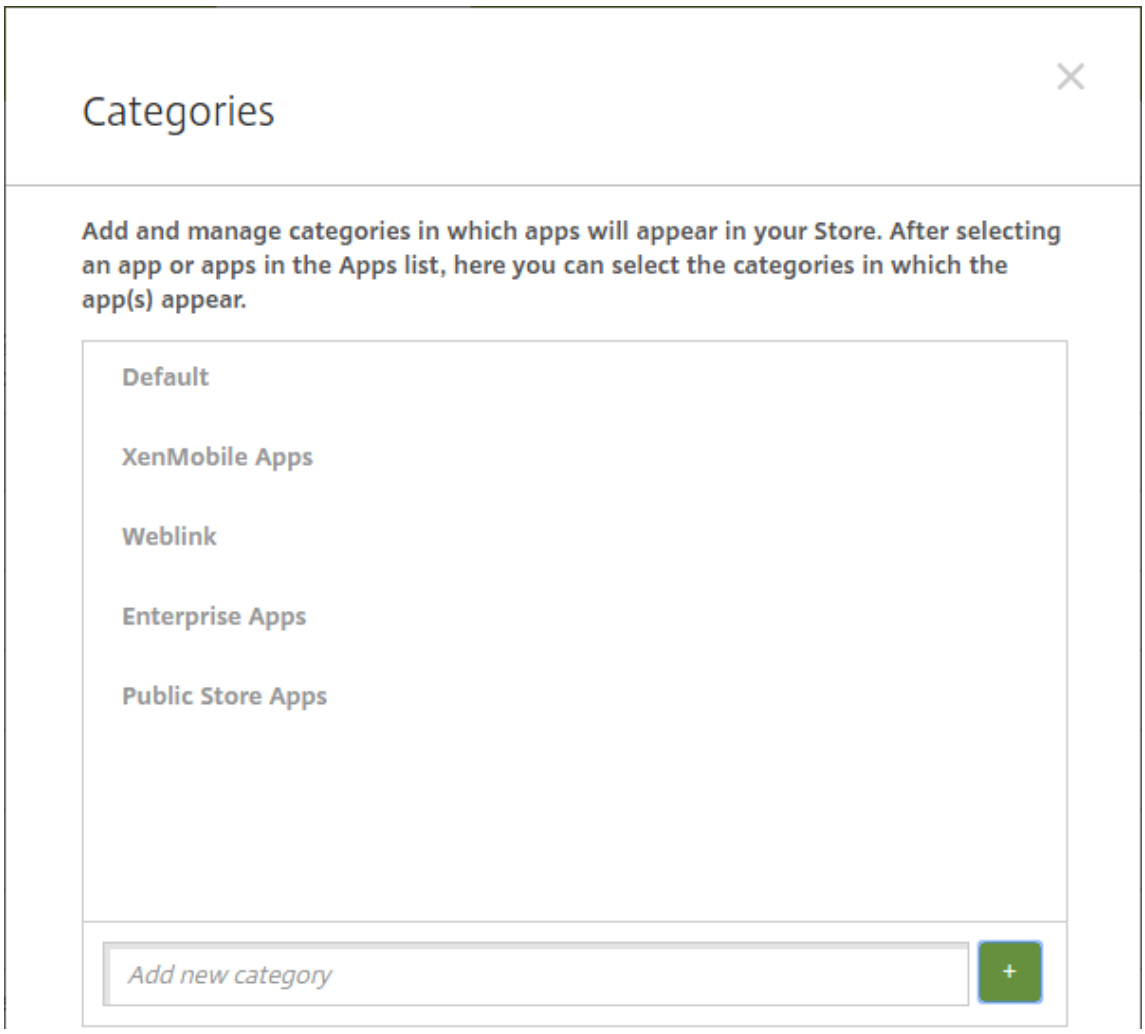
© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. For each category you want to add, do the following:

   - Type the name of the category that you want to add in the **Add a new category** field at the bottom of the dialog box. For example, you might type Enterprise Apps to create a category for enterprise apps.
   - Click the plus sign (+) to add the category. The newly created category is added and appears in the **Categories** dialog box.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. When you're done adding categories, close the **Categories** dialog box.
4. On the **Apps** page, you can place an existing app into a new category.
    - Select the app that you want to categorize.
    - Click **Edit**. The **App Information** page appears.
    - In the **App category** list, apply the new category by selecting the category checkbox. Clear the checkboxes for any existing categories that you don't want to apply to the app.
    - Click the **Delivery Groups Assignments** tab or click **Next** on each of the following pages to step through the remaining app set-up pages.
    - Click **Save** on the **Delivery Groups Assignments** page to apply the new category. The new category is applied to the app and appears in the **Apps** table.

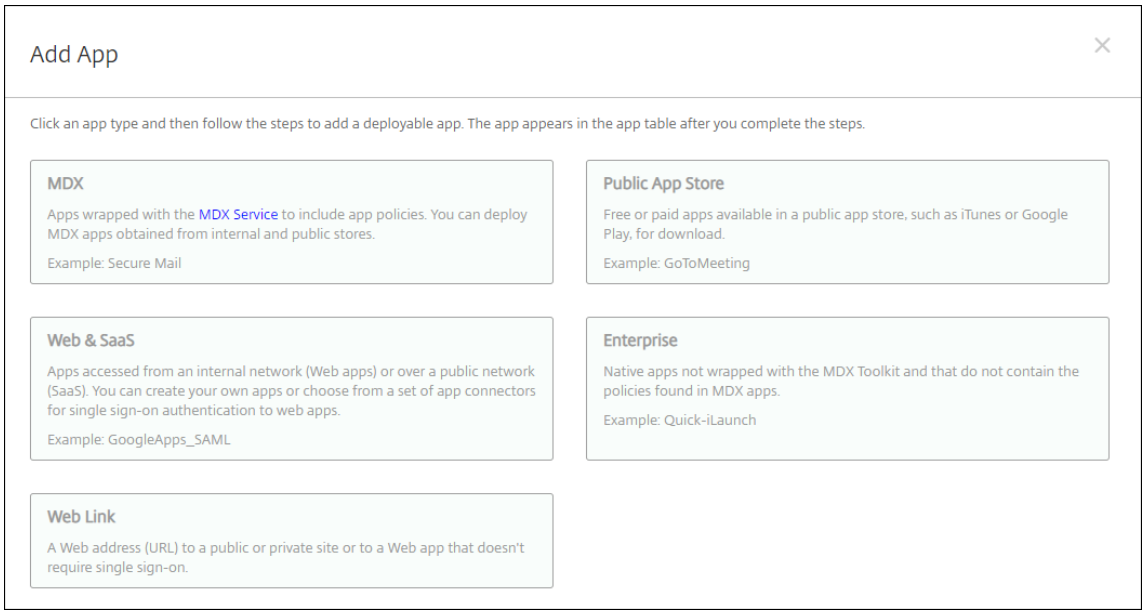
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Add an MDX app

When you receive an MDX file for an iOS or Android app, you can upload the app to Citrix Endpoint Management. After you upload the app, you can configure app details and policy settings. For information about the app policies that are available for each device platform type, see:

- MAM SDK overview
- MDX Policies at a Glance

1. For Citrix mobile productivity apps, download the public-store MDX files: Go to https://www.citrix.com/downloads. Navigate to **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.
2. For other types of MDX apps, get the MDX file.
3. In the Citrix Endpoint Management console, click **Configure > Apps > Add**. The **Add App** dialog box appears.

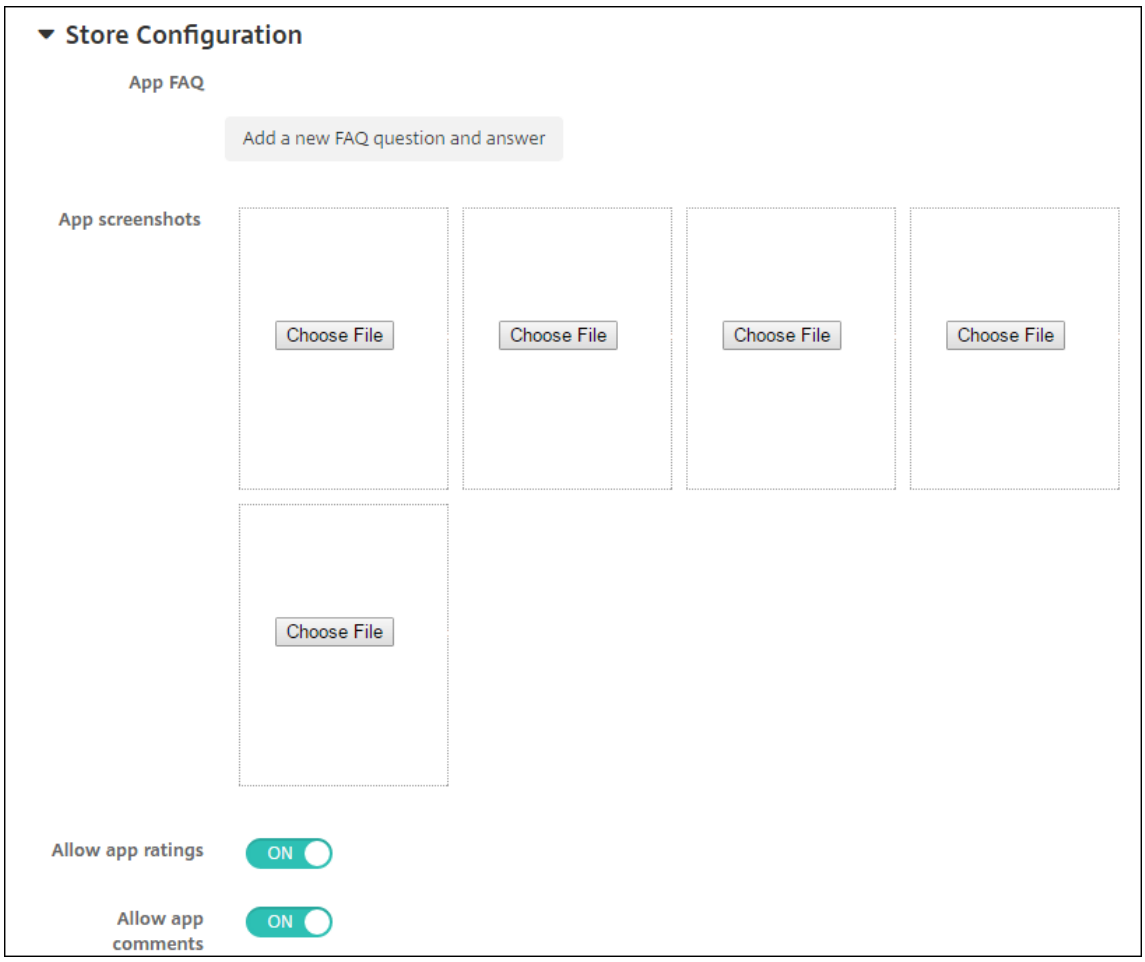


4. Click **MDX**. The **MDX App Information** page appears.
5. On the **App Information** pane, type the following information:
   - **Name:** Type a descriptive name for the app. The name appears under **App Name** on the **Apps** table.
   - **Description:** Type an optional description of the app.
   - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see About app categories.
6. Click **Next**. The **App Platforms** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

7. Under **Platforms**, select the platforms you want to add. If you're only configuring for one platform, clear the others.
8. To select an MDX file to upload, click **Upload** and navigate to the file location.
9. In the **App details** page, configure these settings:
    - **File name:** Type the file name associated with the app.
    - **App Description:** Type a description for the app.
    - **App version:** Optionally, type the app version number.
    - **Package ID:** Type the package ID for the app from the managed Google Play Store.
    - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
    - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
    - **Excluded devices:** Optionally, type the manufacturer or models of devices that can't run the app.
    - **Remove app if MDM profile is removed:** Select whether to remove the app from an iOS device when the MDM profile is removed. The default is **On**.
    - **Prevent app data backup:** Select whether to prevent users from backing up app data on iOS devices. The default is **On**.
    - **Product track:** Specify which product track that you want to push to iOS devices. If you have a track designed for testing, you can select and assign it to your users. The default is **Production**.
    - **Force app to be managed:** For an app that installs as unmanaged, select whether to prompt users to allow the app to be managed on unsupervised iOS devices. The default is **On**.
    - **App deployed via volume purchase:** Select whether to deploy the app by using Apple volume purchase. If **On**, and you deploy an MDX version of the app and use volume purchase to deploy the app, Citrix Secure Hub shows only the volume purchase instance. Default is **Off**.
10. Configure the **MDX Policies**. MDX policies vary by platform and include options for policy areas, including authentication, device security, and app restrictions. In the console, each of the policies has a tooltip that describes the policy.
11. Configure the deployment rules. For information, see Configure deployment rules.
12. Expand **Store Configuration**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

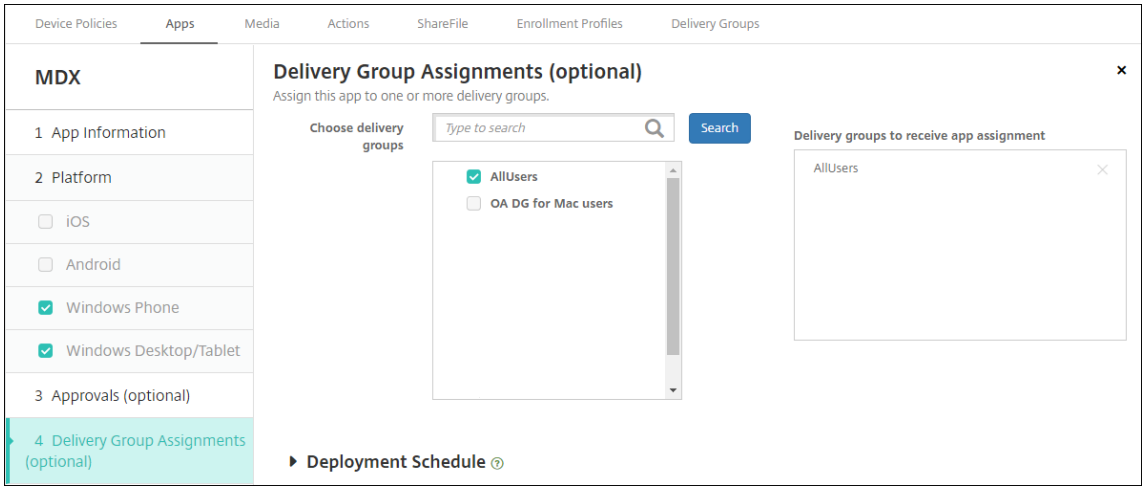


Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

13. Click **Next**. The **Delivery Group Assignment** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



14. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.
15. Expand **Deployment Schedule** and then configure the following settings:

    - **Deploy:** Choose whether to deploy the app to devices. The default is **On**.
    - **Deployment schedule:** Choose whether to deploy the app **Now** or **Later**. If you select **Later**, configure a date and time to deploy the app. The default is **Now**.
    - **Deployment condition:** Choose **On every connection** to deploy the app every time the device connects. Choose **Only when previous deployment has failed** to deploy the app when the device failed to receive the app previously. The default is **On every connection**.

    The **Deploy for always-on connection** option applies when you've configured the scheduling background deployment key in **Settings > Server Properties**.

    The always-on option:

    - Isn't available for iOS devices
    - Isn't available for Android and Android Enterprise customers who began using Citrix Endpoint Management with version 10.18.19 or later
    - Isn't recommended for Android and Android Enterprise customers who began using Citrix Endpoint Management before version 10.18.19

    The deployment schedule that you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.
16. Click **Save**.

Add a public app store app

You can add free or paid apps to Citrix Endpoint Management that are available in a public app store, such as the Apple App Store.

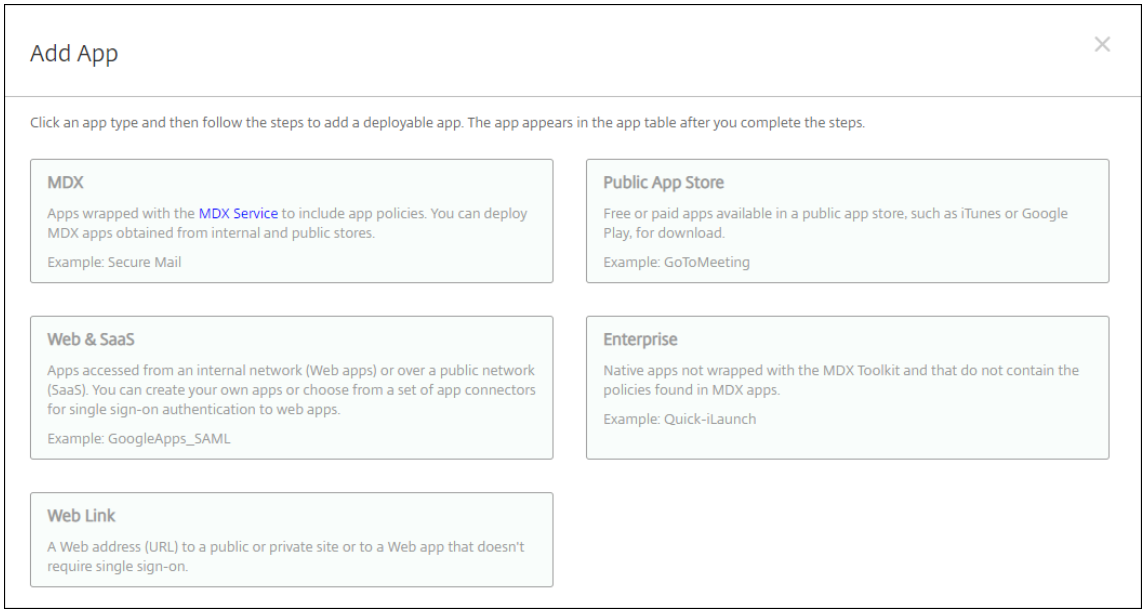
© 1997–2025 Citrix Systems, Inc. All rights reserved.

You can configure settings to retrieve app names and descriptions from the Apple App Store. When you retrieve the app information from the store, Citrix Endpoint Management overwrites the existing name and description. Manually configure Google Play store app information.

> **Note:**
>
> Paid apps for Android through Android Enterprise Managed Google Play is no longer supported by Google. For more information, see Managed Google Play Help documentation.

Configure app information and choose platforms to deliver the app to:

1. In the Citrix Endpoint Management console, click **Configure > Apps > Add**. The **Add App** dialog box appears.



2. Click **Public App Store**. The **App Information** page appears.
3. On the **App Information** pane, type the following information:
   - **Name:** Type a descriptive name for the app. This name appears under **App Name** on the **Apps** table.
   - **Description:** Type an optional description of the app.
   - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see About app categories.
4. Click **Next**. The **App Platforms** page appears.
5. Under **Platforms**, select the platforms you want to add. If you're only configuring for one platform, clear the others.

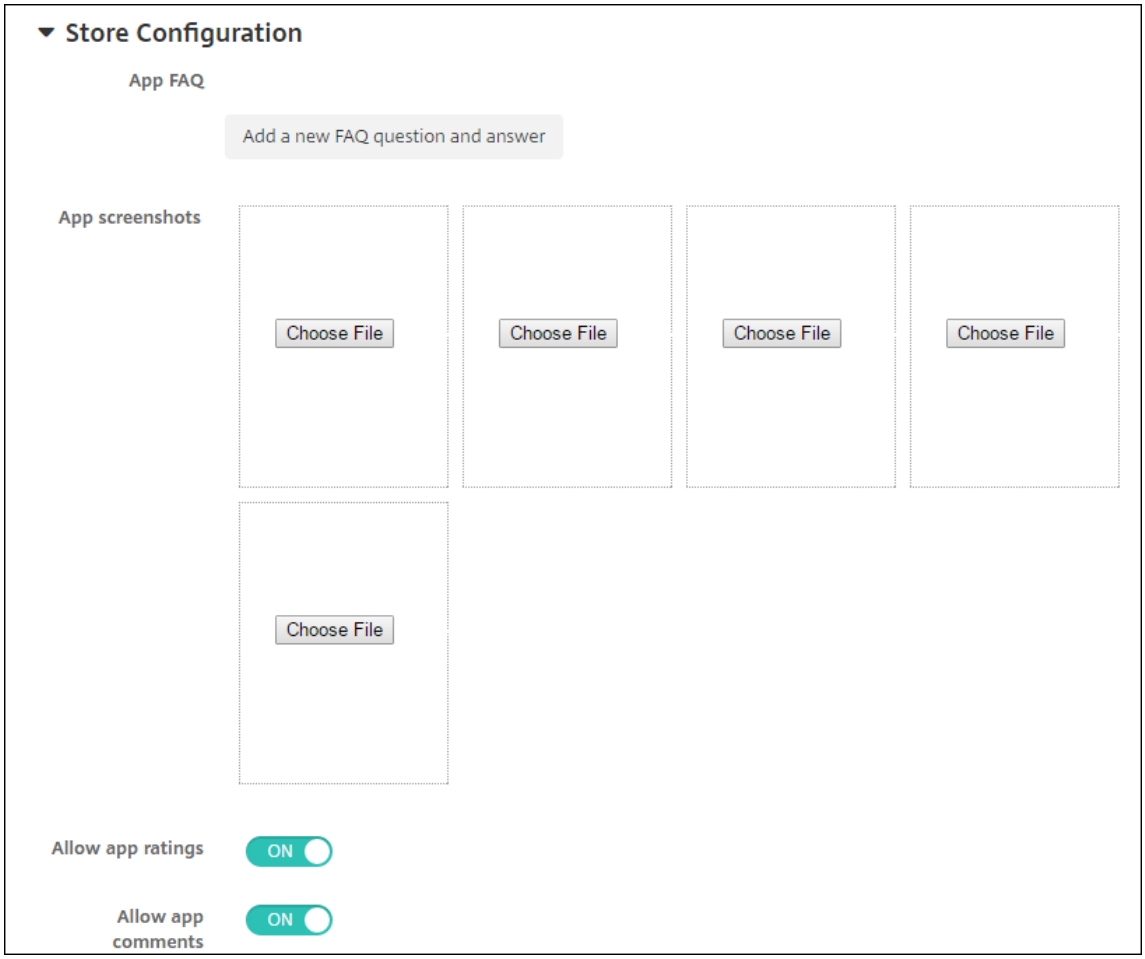
Next you configure the app settings for each platform. See:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Configure app settings for Google Play apps
- Managed app store apps
- Configure app settings for iOS apps

When you finish configuring the settings for a platform, set the platform deployment rules and app store configuration.

1. Configure the deployment rules. For information, see Configure deployment rules.
2. Expand **Store Configuration**.



Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

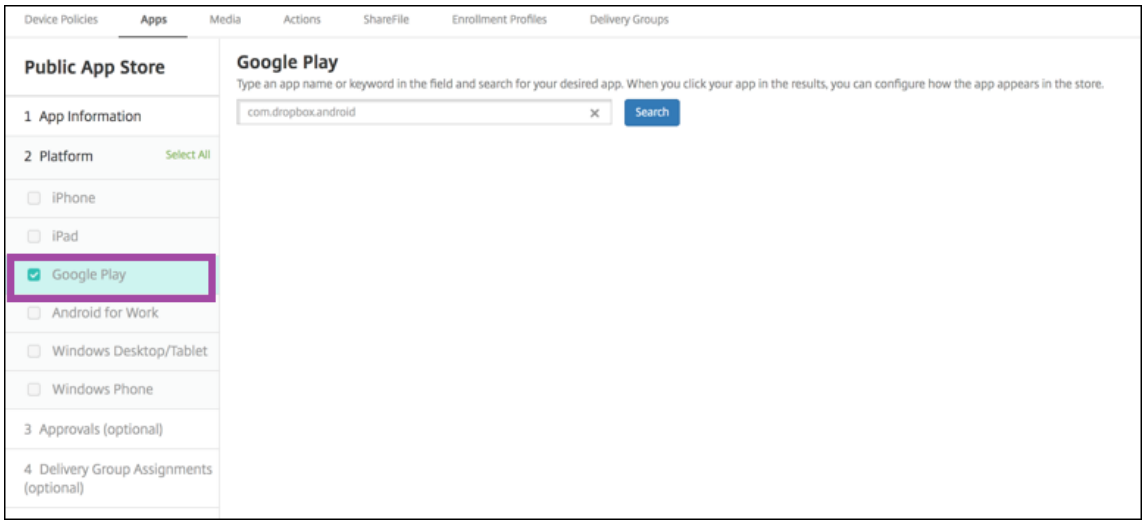
Configure app settings for Google Play apps

© 1997–2025 Citrix Systems, Inc. All rights reserved.

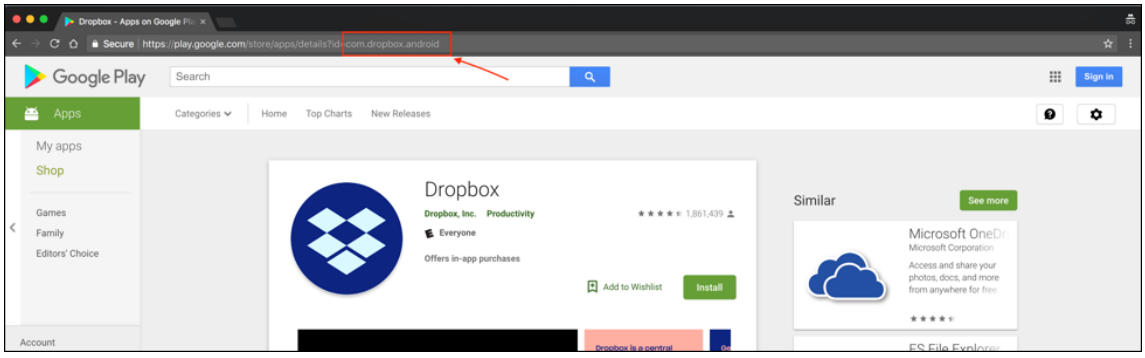
> **Note:**
>
> To make all apps in the Google Play store accessible from managed Google Play, use the **Access all apps in the managed Google Play store** server property. (See Server properties.) Setting this property to **true** allows all Android Enterprise users to access public Google Play store apps. You can then use the Restrictions device policy to control access to these apps.

Configuring settings for Google Play store apps requires different steps than apps for other platforms. Manually configure Google Play store app information.

1. Make sure that **Google Play** is selected under **Platforms**.

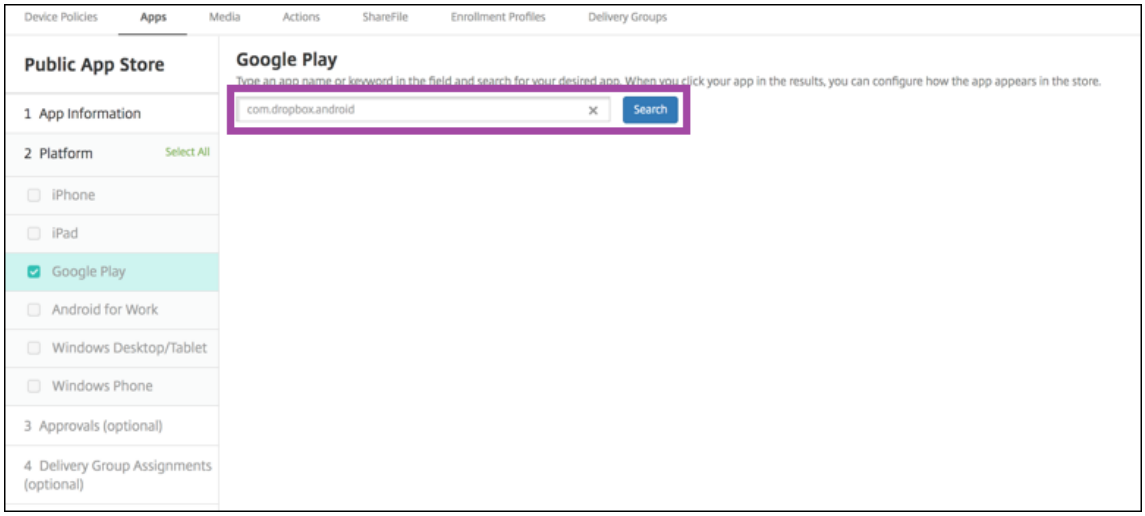


2. Go to the Google Play store. From the Google Play store, copy the package ID. The ID can be found in the URL of the app.

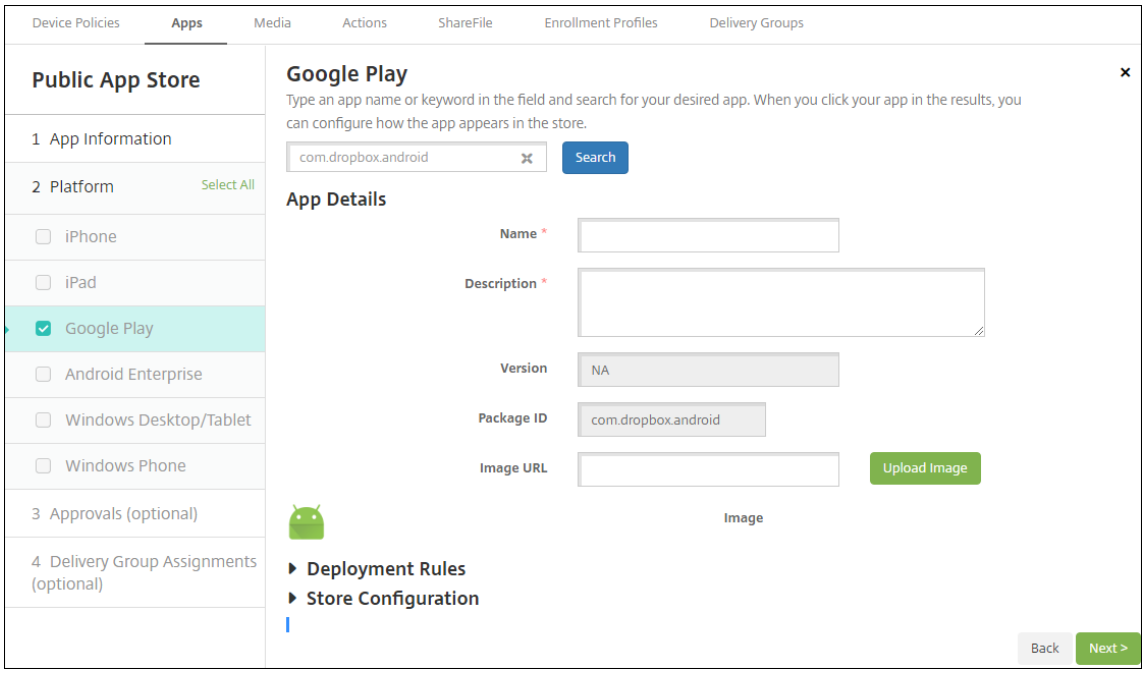


3. When adding a Public Store app in the Citrix Endpoint Management console, paste the package ID in the search bar. Click **Search**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. If the package ID is valid, a UI appears allowing you to enter app details.



5. You can configure the URL for the image to appear with the app in the store. To use the image from the Google Play store:

   a) Go the Google Play store. Right-click the app image and copy the image address.

   b) Paste the image address into the **Image URL** field.

   c) Click **Upload image**. The image appears beside **Image**.

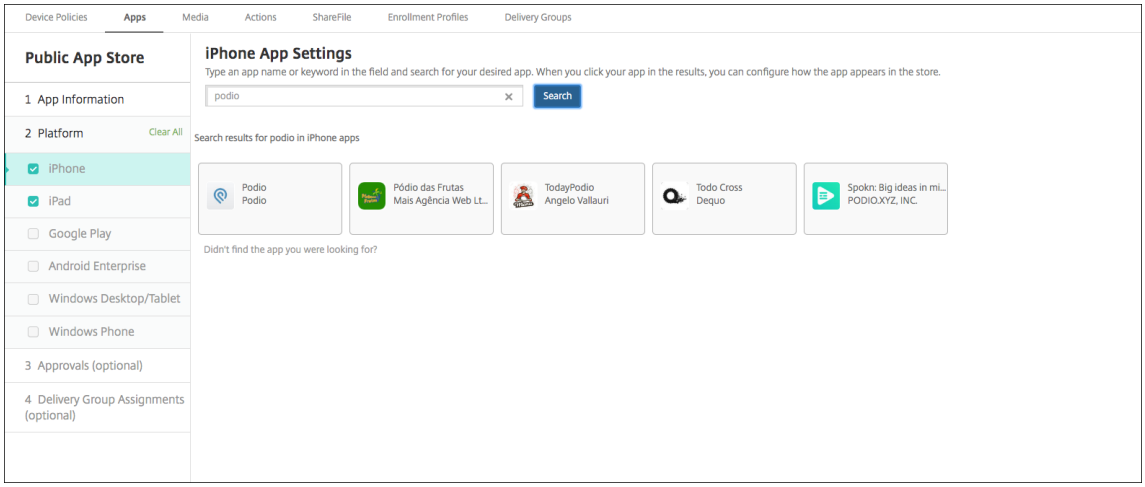
If you don't configure an image, the generic Android image appears with the app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

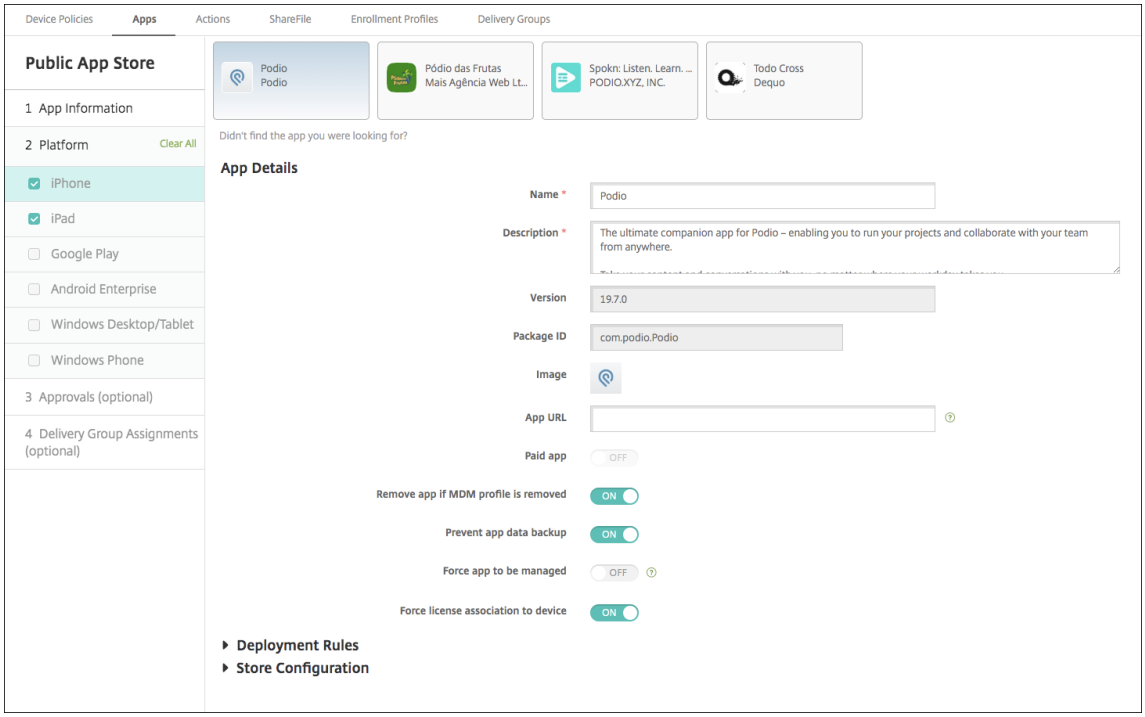
Configure app settings for iOS apps

1. Type the app name in the search box and click **Search**. Apps matching the search criteria appear. Apps matching the search criteria appear.

   The following figure shows the result of searching for **podio** in apps on an iPhone.



2. Click the app that you want to add.
3. The **App Details** fields pre-populate with information related to the chosen app (including the name, description, version number, and associated image).



4. Configure the settings:

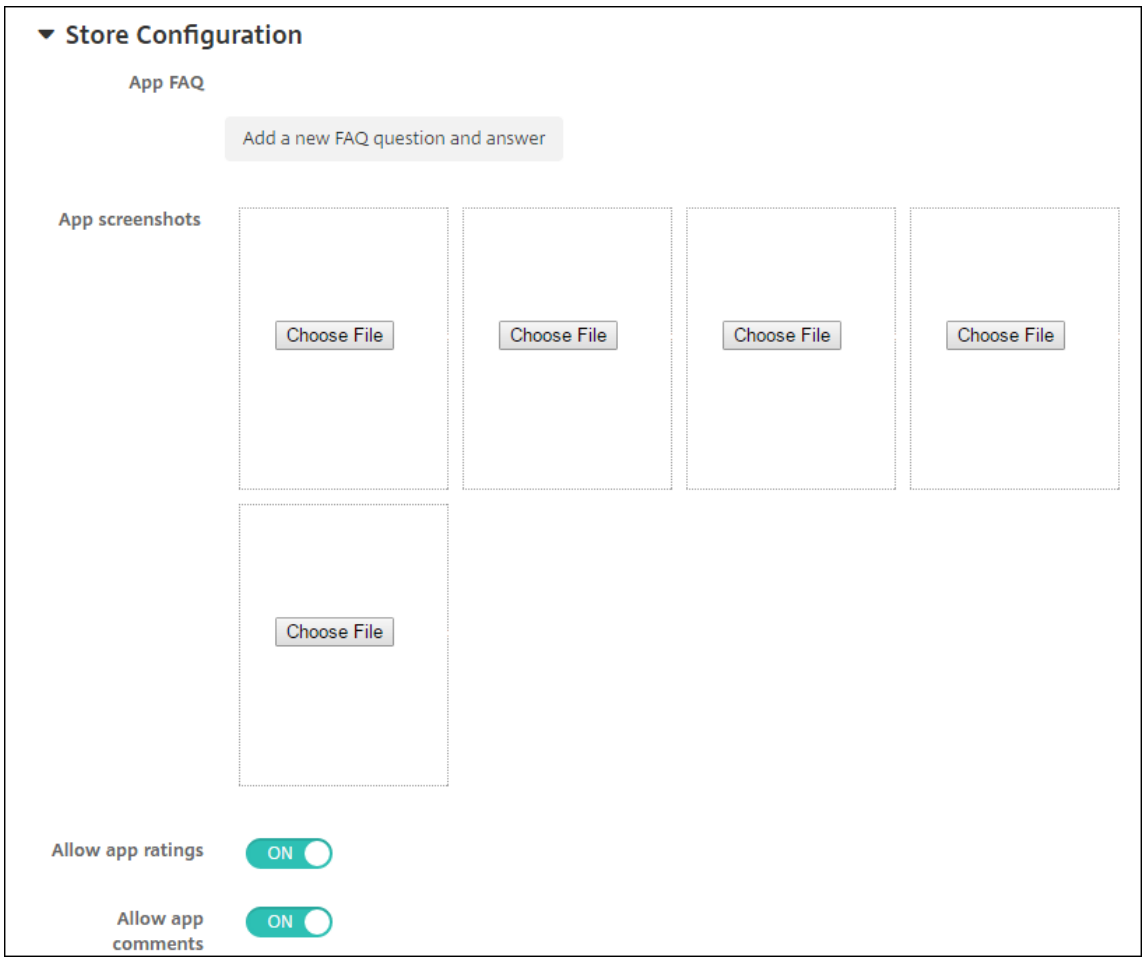
   - If necessary, change the name and description for the app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **App URL:** Enter a comma-separated list of URLs to launch your apps from the Citrix Workspace app. This field is only available for iPhone and iPad devices.
- **Paid app:** This field is preconfigured and cannot be changed.
- **Remove app if MDM profile is removed:** Select whether to remove the app if the MDM profile is removed. The default is **On**.
- **Prevent app data backup:** Select whether to prevent the app from backing up data. The default is **On**.
- **Product track:** Specify which product track that you want to push to user devices. If you have a track designed for testing, you can select and assign it to your users. The default is **Production**.
- **Force app to be managed:** For an app that installs as unmanaged, select whether to prompt users to allow the app to be managed on unsupervised iOS devices. The default is **Off**. For iOS devices enrolled through user enrollment, Citrix Endpoint Management doesn't enforce this setting and doesn't prompt users to allow app management.
- **Force license to association to device:** Select whether to associate an app (developed with device association enabled) to a device rather than to a user. If the app you chose does not support assignment to a device, you can't change this setting.

5. Configure the deployment rules. For information, see Configure deployment rules.
6. Expand **Store Configuration**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

7. For iPhone or iPad, expand **Volume Purchase**.

   a) To enable Citrix Endpoint Management to apply a volume purchase license for the app: In the **Volume purchase license** list, click **Upload a volume purchase license**.

   b) In the dialog box that appears, import the license.

      The License Assignment table shows the number of licenses in use for the app, out of the total licenses available.

      You can disassociate Volume Purchase licenses for an individual user. Doing so ends the license assignments and frees licenses.

   c) When you add your volume purchase account, enable **App Auto Update**. This setting

© 1997–2025 Citrix Systems, Inc. All rights reserved.

makes sure that apps on user devices automatically update when an update appears in the Apple store. If an app has the **Force app to be managed** setting enabled, it updates without prompting the user. The update happens whether the app is required or optional.

8. After you complete the **Volume Purchase** settings, click **Next**. The **Approvals** page appears.

   To use workflows to require approval before allowing users to access the app, see Apply workflows. If you don't need approval workflow, continue with the next step.

9. Click **Next**. The **Delivery Group Assignment** page appears.
10. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.
11. Expand **Deployment Schedule** and then configure the following settings:

    - **Deploy:** Choose whether to deploy the app to devices. The default is **On**.
    - **Deployment schedule:** Choose whether to deploy the app **Now** or **Later**. If you select **Later**, configure a date and time to deploy the app. The default is **Now**.
    - **Deployment condition:** Choose **On every connection** to deploy the app every time the device connects. Choose **Only when previous deployment has failed** to deploy the app when the device failed to receive the app previously. The default is **On every connection**.

    The **Deploy for always-on connection** option applies when you've configured the scheduling background deployment key in **Settings > Server Properties**.

    The always-on option:

    - Isn't available for iOS devices
    - Isn't available for Android and Android Enterprise customers who began using Citrix Endpoint Management with version 10.18.19 or later
    - Isn't recommended for Android and Android Enterprise customers who began using Citrix Endpoint Management before version 10.18.19

    The deployment schedule that you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

12. Click **Save**.

Add a Web or SaaS app

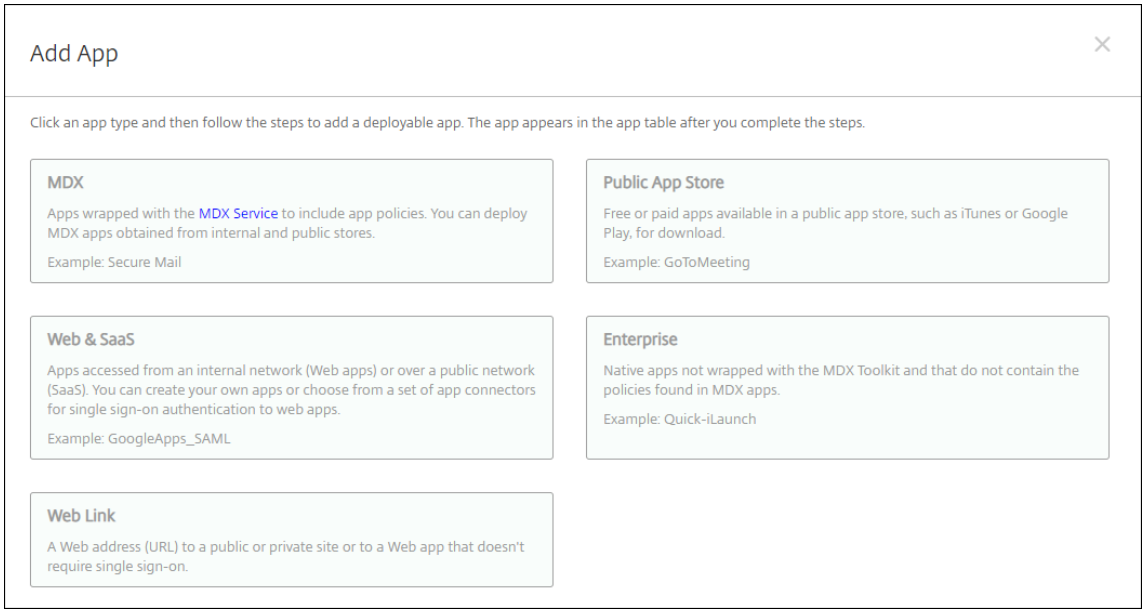
Using the Citrix Endpoint Management console, you can give users single sign-on (SSO) authorization to your enterprise, web, and SaaS apps.

You can build your own connector in Citrix Endpoint Management when you add a Web app or SaaS app. For a list of connector types available in Citrix Endpoint Management, see Application connector types.

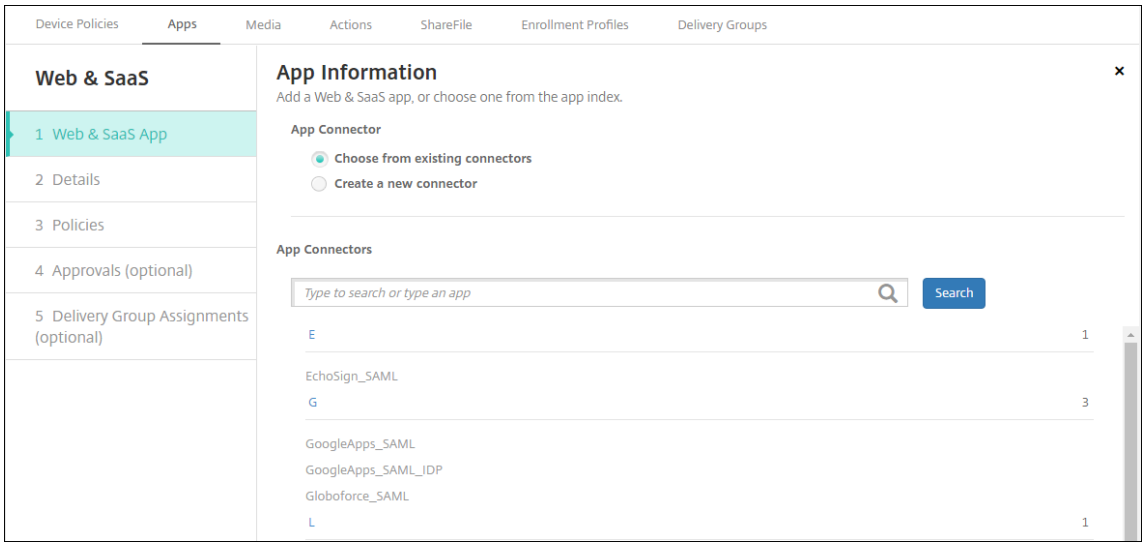
© 1997–2025 Citrix Systems, Inc. All rights reserved.

If an app is available for SSO only: After you save the settings, the app appears on the **Apps** tab in the Citrix Endpoint Management console.

1. In the Citrix Endpoint Management console, click **Configure > Apps > Add**. The **Add App** dialog box appears.



2. Click **Web & SaaS**. The **App Information** page appears.



3. Configure an existing or new app connector as follows.

To configure an existing app connector

1. In the **App Information** page, **Choose from existing connectors** is already selected, as shown previously. Click the connector that you want to use in the **App Connectors** list. The app con-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

nector information appears.

2. Configure these settings:

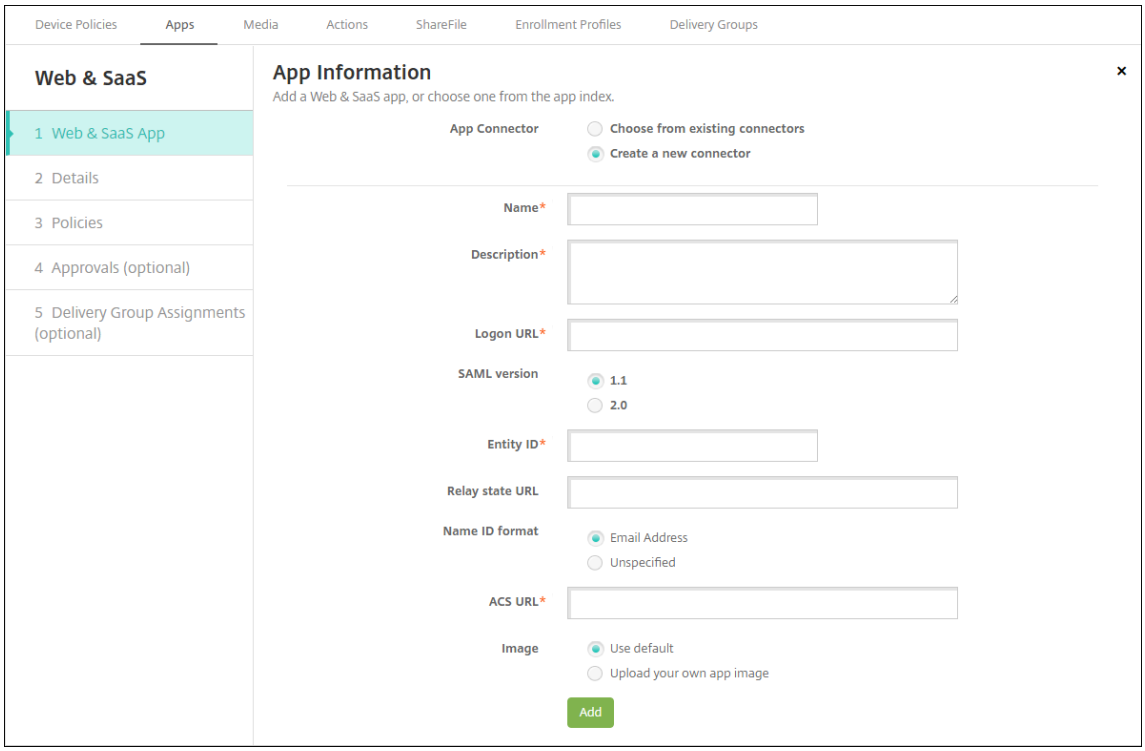
   - **App name:** Accept the pre-filled name or type a new name.
   - **App description:** Accept the pre-filled description or type one of your own.
   - **URL:** Accept the pre-filled URL or type the web address for the app. Depending on the connector you choose, this field can have a placeholder that you must replace before you can move to the next page.
   - **Domain name:** If applicable, type the domain name of the app. This field is required.
   - **App is hosted in internal network:** Select whether the app is running on a server in your internal network. If users connect from a remote location to the internal app, they must connect through NetScaler Gateway. Setting this option to **On** adds the VPN keyword to the app and allows users to connect through NetScaler Gateway. The default is **Off**.
   - **App category:** Click an optional category in the drop-down list to apply to the app.
   - **User account provisioning:** Select whether to create user accounts for the app. If you use the Globoforce_SAML connector, you must enable this option to provide seamless SSO integration.
   - If you enable **User account provisioning**, configure these settings:
     - **Service Account**
       - **User name:** Type the name of the app administrator. This field is required.
       - **Password:** Type the app administrator password. This field is required.
     - **User Account**
       - **When user entitlement ends:** Click the action in the drop-down list to take when users are no longer allowed access to the app. The default is **Disable account**.
     - **User Name Rule**
       - For each user name rule you want to add, do the following:
         - **User attributes:** Click the user attribute in the drop-down list to add to the rule.
         - **Length (characters):** Click the number in the drop-down list of characters from the user attribute to use in the user name rule. The default is **All**.
         - **Rule:** Each user attribute you add is automatically appended to the user name rule.
   - **Password Requirement**
     - **Length:** Type the minimum user password length. The default is **8**.
   - **Password Expiration**
     - **Validity (days):** Type the number of days the password is valid. Valid values are **0**–**90**. The default is 90.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Automatically reset password after it expires:** Select whether to reset the password automatically when it expires. The default is **Off**. If you don't enable this field, users can't open the app after their passwords expire.

To configure a new app connector

1. In the **App Information** page, select **Create a new connector**. The app connector fields appear.



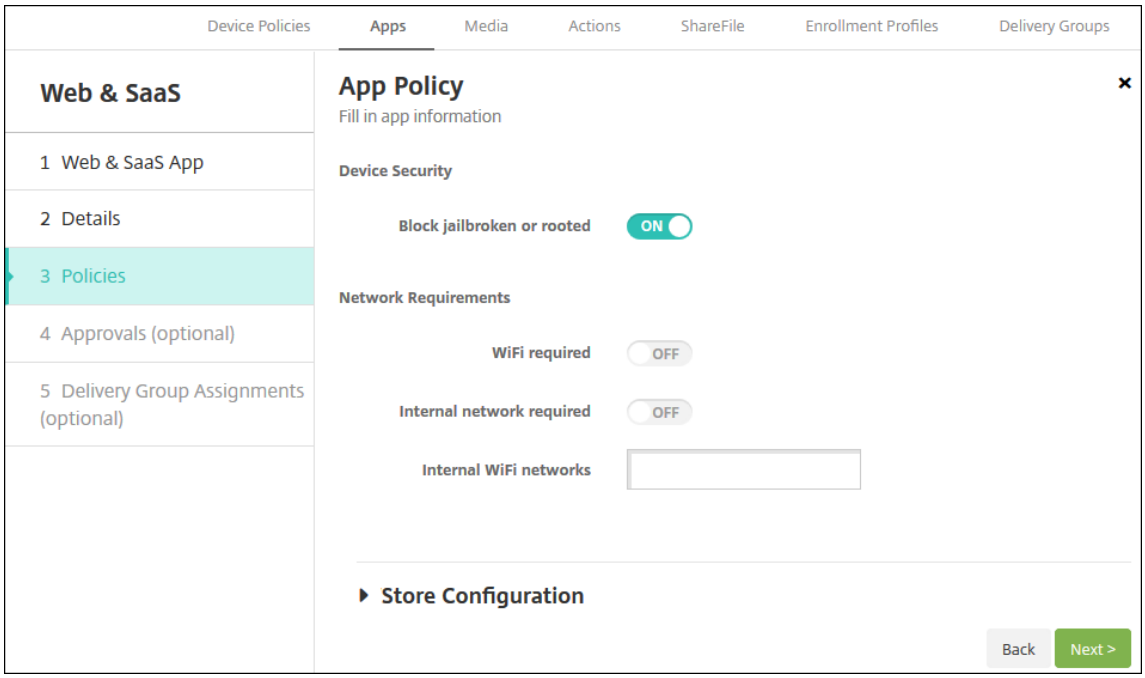
2. Configure these settings:

   - **Name:** Type a name for the connector. This field is required.
   - **Description:** Type a description for the connector. This field is required.
   - **Logon URL:** Type, or copy and paste, the URL where users log on to the site. For example, if the app you want to add has a logon page, open a web browser and go to the logon page for the app. For example, it might be `https://www.example.com/logon`. This field is required.
   - **SAML version:** Select either **1.1** or **2.0**. The default is **1.1**.
   - **Entity ID:** Type the identity for the SAML app.
   - **Relay state URL:** Type the web address for the SAML application. The relay state URL is the response URL from the app.
   - **Name ID format:** Select either **Email Address** or **Unspecified**. The default is **Email Address**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **ACS URL:** Type the Assertion Consumer Service URL of the identity provider or service provider. The ACS URL gives users SSO capability.
- **Image:** Select whether to use the default Citrix image or to upload your own app image. The default is Use default.
  - To upload your own image, click **Browse** and navigate to the file location. The file must be a .PNG file. You can't upload a JPEG or GIF file. When you add a custom graphic, you can't change it later.

3. When you're finished, click **Add**. The **Details** page appears.
4. Click **Next**. The **App Policy** page appears.

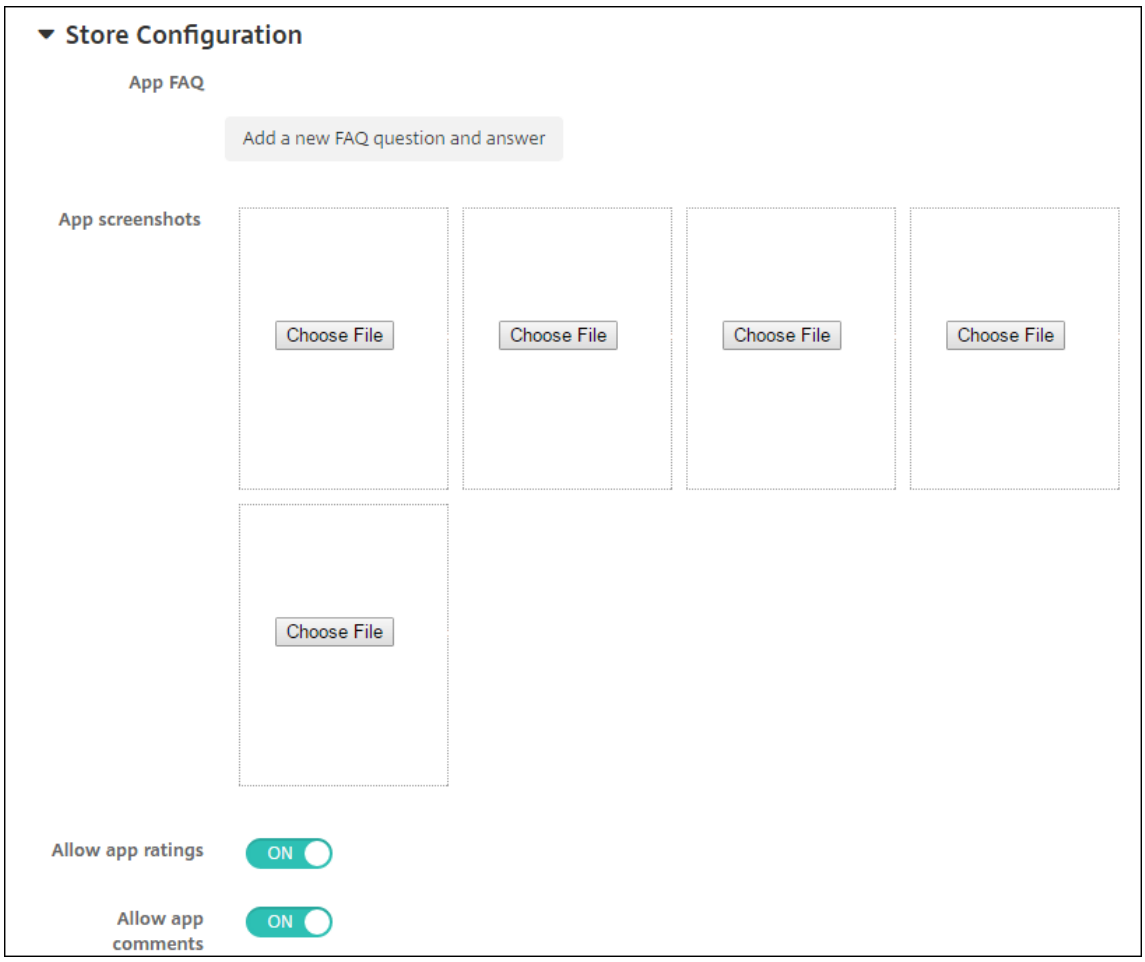


5. Configure these settings:

- **Device Security**
- **Block jailbroken or rooted:** Select whether to block jailbroken or rooted devices from accessing the app. The default is **On**.
- **Network Requirements**
- **WiFi required:** Select whether a Wi-Fi connection is required to run the app. The default is **Off**.
- **Internal network required:** Select whether an internal network is required to run the app. The default is **Off**.
- **Internal WiFi networks:** If you enabled **Wi-Fi required**, type the internal Wi-Fi network to use.

6. Expand **Store Configuration**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

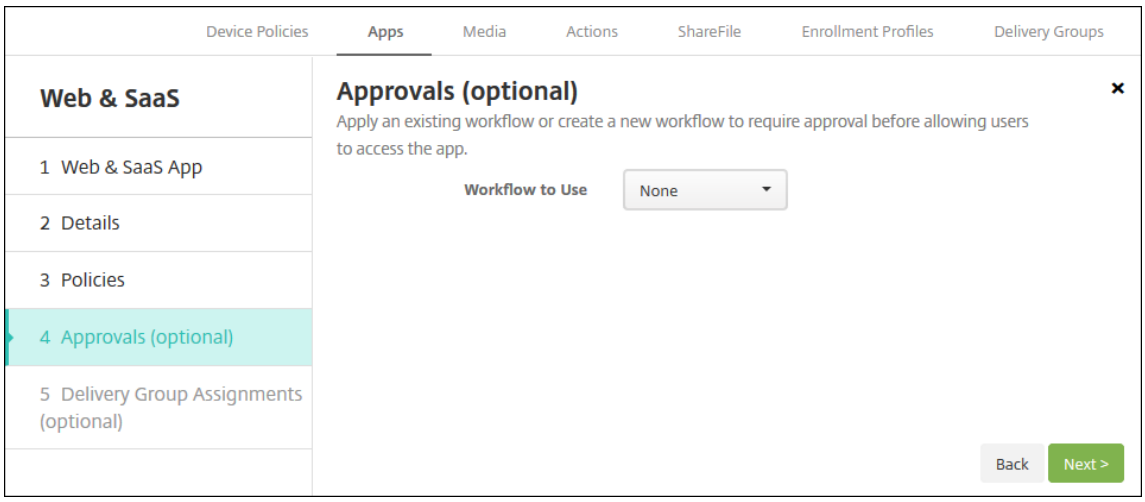


Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

7. Click **Next**. The **Approvals** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



To use workflows to require approval before allowing users to access the app, see Apply workflows. If you don't need approval workflow, continue with the next step.

8. Click **Next**. The **Delivery Group Assignment** page appears.
9. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups. The groups you select appear in the **Delivery groups to receive app assignment** list.
10. Expand **Deployment Schedule** and then configure the following settings:

    - **Deploy:** Choose whether to deploy the app to devices. The default is **On**.
    - **Deployment schedule:** Choose whether to deploy the app **Now** or **Later**. If you select **Later**, configure a date and time to deploy the app. The default is **Now**.
    - **Deployment condition:** Choose **On every connection** to deploy the app every time the device connects. Choose **Only when previous deployment has failed** to deploy the app when the device failed to receive the app previously. The default is **On every connection**.

    The **Deploy for always-on connection** option applies when you've configured the scheduling background deployment key in **Settings > Server Properties**.

    The always-on option:

    - Isn't available for iOS devices
    - Isn't available for Android and Android Enterprise customers who began using Citrix Endpoint Management with version 10.18.19 or later
    - Isn't recommended for Android and Android Enterprise customers who began using Citrix Endpoint Management before version 10.18.19

    The deployment schedule that you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

11. Click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Add an enterprise app

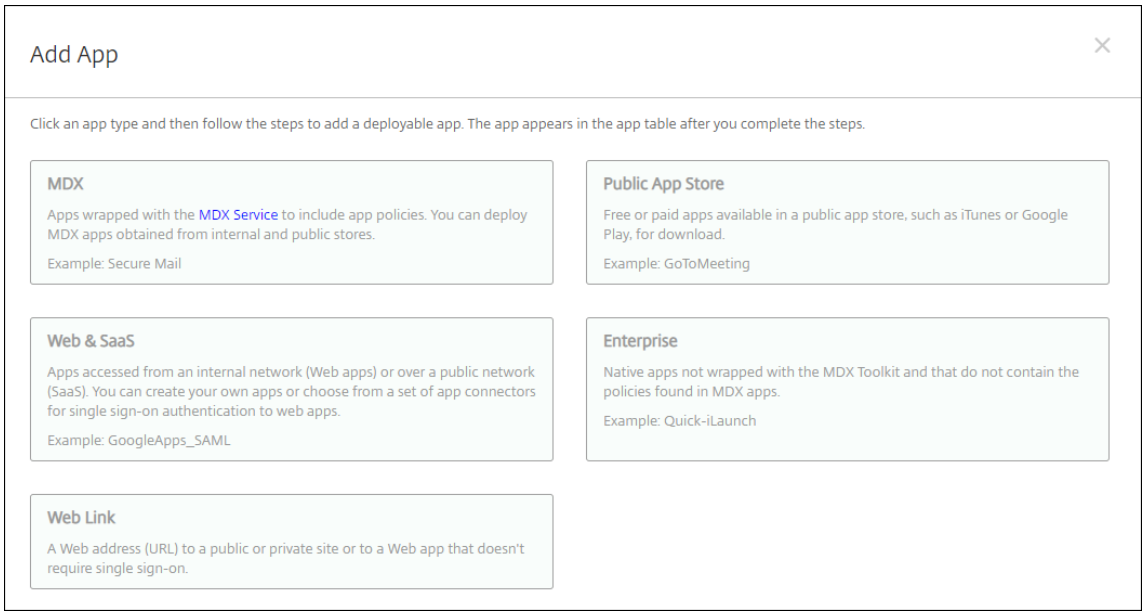
Enterprise apps in Citrix Endpoint Management are private apps that you develop or get from another source. Except for private Android Enterprise apps delivered as MDX-enabled apps, enterprise apps aren't prepared with the MAM SDK or MDX Toolkit. You can upload an enterprise app on the **Apps** tab in the Citrix Endpoint Management console. Enterprise apps support the following platforms (and corresponding file types):

- iOS (.ipa file)
- macOS (.pkg file)

  Citrix Endpoint Management does not limit the size of PKG files you upload but limits file upload times. By default, you must complete your upload within 100 s. For more information, see Server properties.
- Android (.apk file)
- Android Enterprise (.apk file)
- See also: Add Win32 apps as Enterprise apps
- See also: MDX-enabled private apps

Adding apps downloaded from the Google Play store as enterprise apps isn't supported. Add apps from the Google Play store as public app store apps instead. See Add a public app store app.

1. In the Citrix Endpoint Management console, click **Configure > Apps > Add**. The **Add App** dialog box appears.



2. Click **Enterprise**. The **App Information** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. On the **App Information** pane, type the following information:

    - **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
    - **Description:** Type an optional description of the app.
    - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see About app categories.

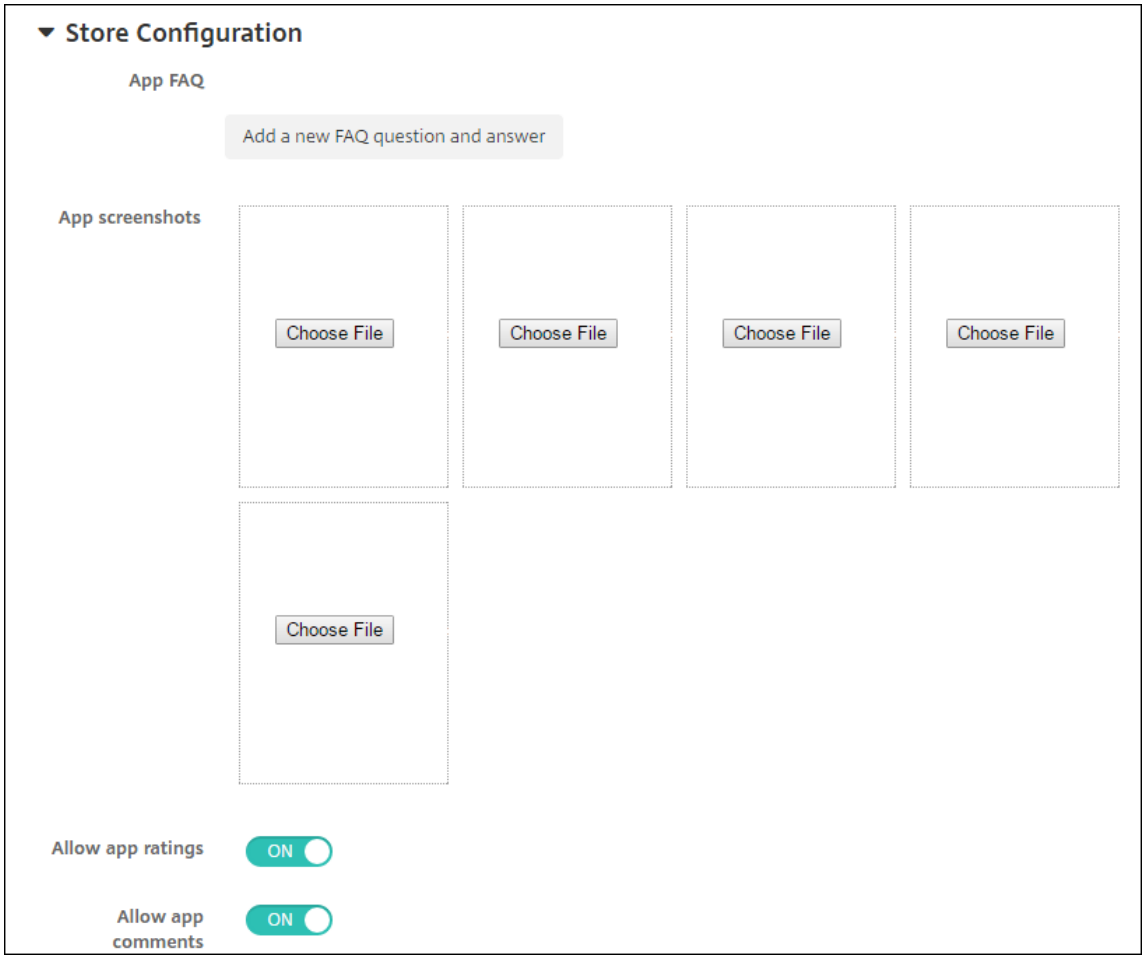
4. Click **Next**. The **App Platforms** page appears.
5. Under **Platforms**, select the platforms you want to add. If you're only configuring for one platform, clear the others.
6. For each platform you chose, select the file to upload by clicking **Upload** and navigating to the file location.
7. Click **Next**. The app information page for the platform appears.
8. Configure the settings for the platform type, such as:

    - **File name:** Optionally, type a new name for the app.
    - **App description:** Optionally, type a new description for the app.
    - **App version:** You can't change this field.
    - **Minimum OS version:** Optionally, type the oldest operating system version that the device can run to use the app.
    - **Maximum OS version:** Optionally, type the most recent operating system that the device must run to use the app.
    - **Excluded devices:** Optionally, type the manufacturer or models of devices that can't run the app.
    - **Package ID:** Unique identifier of your app.
    - **Remove app if MDM profile is removed:** Select whether to remove the app from a device when the MDM profile is removed. The default is **On**. This setting doesn't apply to macOS.
    - **Prevent app data backup:** Select whether to prevent the app from backing up data. The default is **On**. This setting doesn't apply to macOS.
    - **Force app to be managed:** Select whether to install an app as a managed app on unsupervised devices. The device type determines how Citrix Endpoint Management processes this setting when enabled. If you enable this setting, the app updates without prompting the user. The update happens whether the app is required or optional. The default is **Off**.
        - For iOS devices, if the app was already installed, users receive a prompt to allow the app to be managed. If you deploy an app to devices where the app doesn't exist, the app installs as a managed app whatever the state of this setting. Available on iOS 9.0 and later. For iOS devices enrolled through user enrollment, Citrix Endpoint Management doesn't enforce this setting and doesn't prompt users to allow app management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- For macOS devices, enable the setting, and then deploy the app to the devices. The app automatically installs as a managed app. Users don't receive any prompts. If you deploy an app to devices where the app doesn't exist, the app installs as a managed app whatever the state of this setting. Available on macOS 11.0 and later.

9. Configure the deployment rules. For information, see Configure deployment rules.
10. Expand **Store Configuration**.



Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

11. Click **Next**. The **Approvals** page appears.

To use workflows to require approval before allowing users to access the app, see Apply workflows. If you don't need an approval workflow, continue to the next step.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

12. Click **Next**. The **Delivery Group Assignment** page appears.
13. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.
14. Expand **Deployment Schedule** and then configure the following settings:

    - **Deploy:** Choose whether to deploy the app to devices. The default is **On**.
    - **Deployment schedule:** Choose whether to deploy the app **Now** or **Later**. If you select **Later**, configure a date and time to deploy the app. The default is **Now**.
    - **Deployment condition:** Choose **On every connection** to deploy the app every time the device connects. Choose **Only when previous deployment has failed** to deploy the app when the device failed to receive the app previously. The default is **On every connection**.

    The **Deploy for always-on connection** option applies when you've configured the scheduling background deployment key in **Settings > Server Properties**.

    The always-on option:

    - Isn't available for iOS devices
    - Isn't available for Android and Android Enterprise customers who began using Citrix Endpoint Management with version 10.18.19 or later
    - Isn't recommended for Android and Android Enterprise customers who began using Citrix Endpoint Management before version 10.18.19

    The deployment schedule that you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.
15. Click **Save**.

Add Win32 apps as Enterprise apps

You can upload MSI, APPX, AppxBundle, PS1, or EXE files for Win32 apps to Citrix Endpoint Management for deployment to managed Windows 10 and Windows 11 Desktop and Tablet devices. After you use Citrix Endpoint Management to deploy the files, the Windows device then installs the app as follows:

- If the upgraded app removes the old version during installation, then the device includes only the upgraded app.
- If the upgraded app can't remove the old version, but the new version can install, then the device includes both versions of the app. Citrix Endpoint Management no longer has the information for the old version.
- If the upgraded app can't install when an old version exists, the new app doesn't install. In that case, first deploy the App Uninstall device policy to remove the old version. Then, deploy the new version.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Requirements

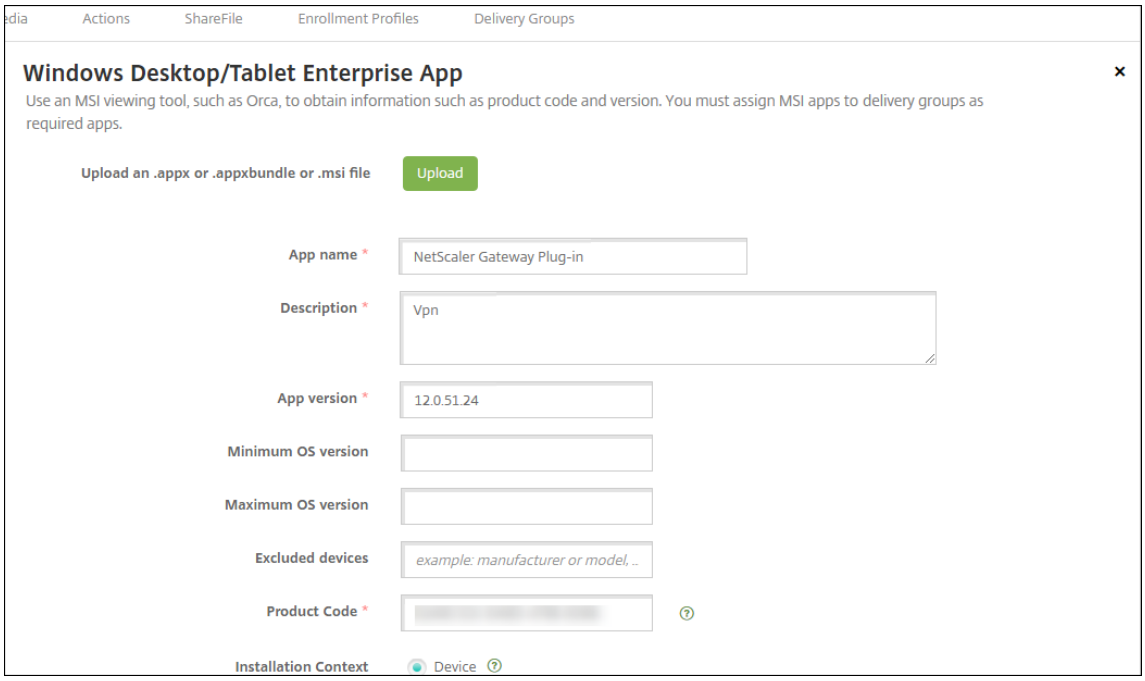
- Windows 10 (version 1607 or later) or Windows 11
- Windows 10 Professional or Windows 11 Professional
- Windows 10 Enterprise or Windows 11 Enterprise
- Standalone Win32 MSI apps installed with the /quiet option. For this deployment use case, Microsoft doesn't support MSIs with more than one app, nested MSIs, or interactive installation.

Look up metadata When you add a Win32 app to Citrix Endpoint Management, specify the metadata for the app. To look up the metadata, use the Orca application on a Windows computer and make note of the following information:

- Product code
- Product name
- Product version
- Package install type, either per user or per machine

Add a Win32 app to Citrix Endpoint Management

1. Go to **Configure > Apps**, click **Enterprise**, and type a name for the app in the **App Information** page.
2. Clear all Platform checkboxes except for **Windows Desktop/Tablet**.
3. On the **Windows Desktop/Tablet Enterprise App** page, click **Upload** and navigate to the file.
4. Configure these settings:

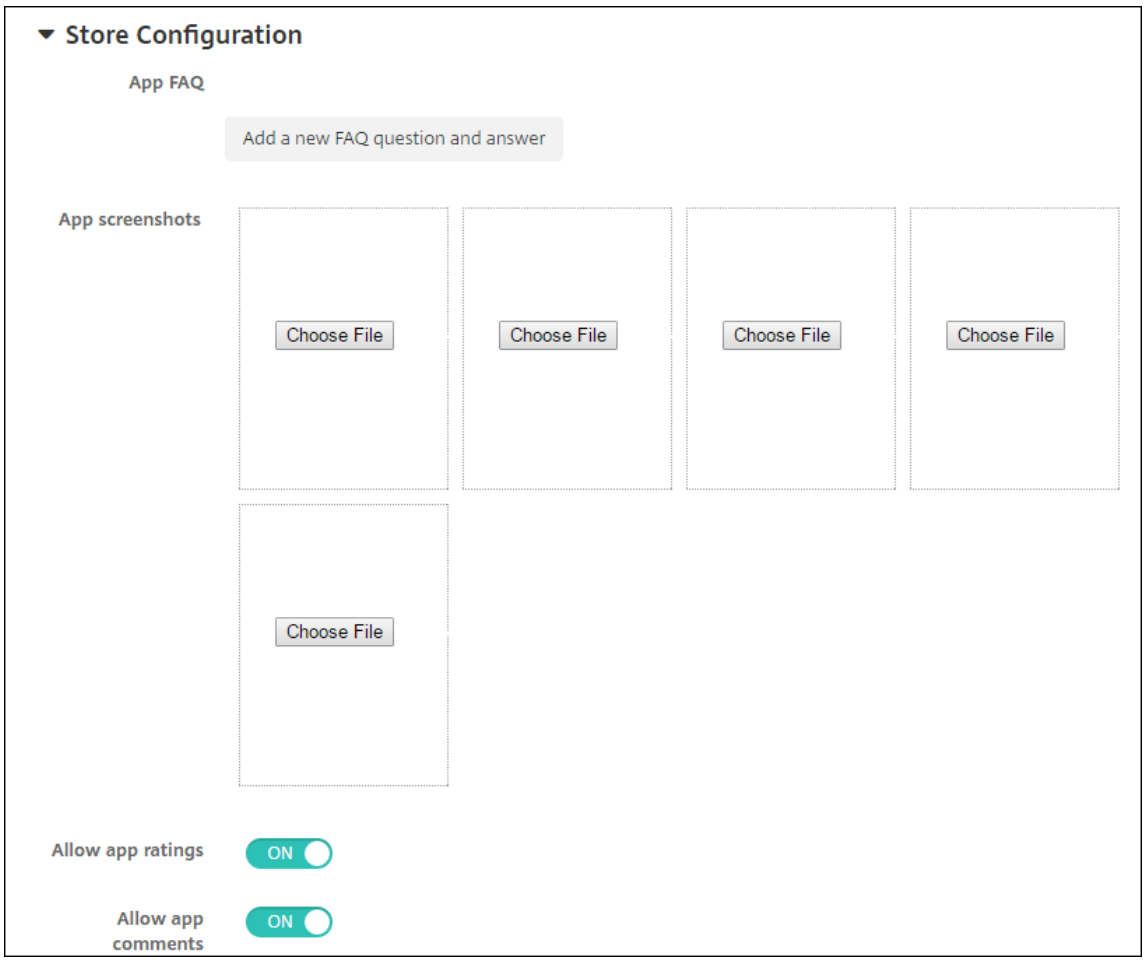


© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **App name:** The name of the app, from the app metadata.
- **Description:** A description for the app.
- **App version:** The app version number, from the app metadata.
- **Minimum OS version:** Optional. The oldest operating system version that the device can run to use the app.
- **Maximum OS version:** Optional. The most recent operating system that the device must run to use the app.
- **Excluded devices:** Optional. The manufacturer or models of devices that can't run the app.
- **Product Code:** The MSI app product code, in UUID format, from the app metadata.
- **Installation Context:** Based on the app metadata, select whether the app is to install for the device or user. This setting isn't available for EXE files.
- **Command Line:** The command-line options to use when calling MSIEXEC.exe
- **Install Command Line:** Add command line arguments for installing EXE files silently.
- **Uninstall Command Line:** Add command line arguments for uninstalling EXE files silently.
- **Retry Count:** The number of times you can retry a download and installation operation before marking the installation as failed.
- **Time Out:** The number of minutes that the installation process runs before the installer interprets the installation as failed and no longer monitors the process.
- **Retry Interval:** The number of minutes between retry operations.

5. Configure the deployment rules. For information, see Configure deployment rules.
6. Expand **Store Configuration**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Optionally, you can configure the following:

- **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
- **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
- **Allow app ratings:** Allow users to rate the app in the app store.
- **Allow app comments:** Allow users to leave comments on the app in the app store.

7. Click **Next** until you get to the **Summary** page and then click **Save**.
8. Go to **Configure > Delivery Groups** and add the Win32 app as a required app.
9. After you deploy the app, let your users know that the app is available.

Upgrade a Win32 app

1. Look up the metadata for the app, as described earlier in "Look up metadata."
2. Go to **Configure > Apps** to upload the new version of the app. Update the **App version**. If the new version of the app has a different **Product Code**, update that setting.
3. Submit the changes and deploy the app.

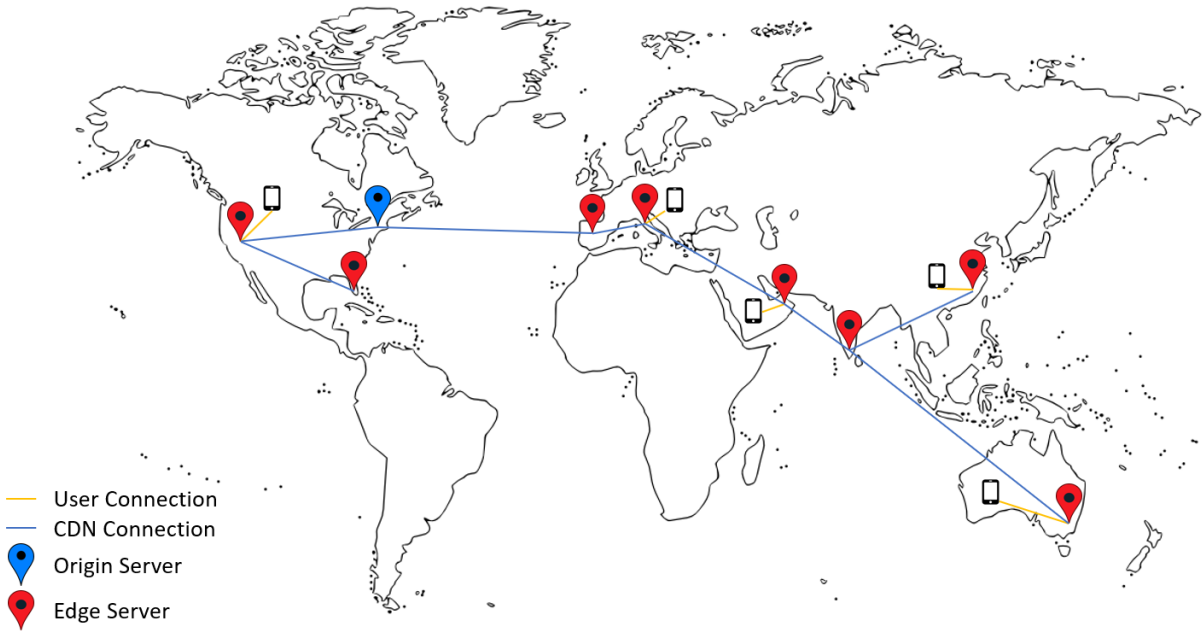
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Deliver enterprise and MDX apps from the Citrix CDN

You can deliver enterprise and MDX apps from the Citrix Content Delivery Network (CDN). A CDN refers to a geographically distributed group of servers that work together to securely provide fast delivery of application content. A local server delivers the apps to mobile devices.

A CDN improves app download times by distributing content geographically closer to the mobile devices through a nearby CDN distribution point. CDN delivers apps from the closest Point of Presence (POP) location to a user.

The following diagram shows an example of how CDN distributes apps to the Edge Server closest to mobile device users. An Edge Server caches content from the originating server when mobile devices request apps.



Users can connect to apps by using Citrix Secure Hub. When you add an app, Citrix Endpoint Management creates the app connector for it.

The Citrix CDN support for enterprise apps is available for the following platforms:

- iOS (MDM or MAM enrollment)
- Android (MDM or MAM enrollment)
- Windows desktop or tablet (MDM enrollment)
- macOS (MDM enrollment)

The Citrix CDN support for MDX apps is available for the following platforms:

- iOS (MDM or MAM enrollment)
- Android (MDM or MAM enrollment)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

How CDN works

At the core of the CDN service, servers are linked together with the goal of delivering apps faster. That goal is achieved by placing the apps securely on different distribution points worldwide. The mobile devices' DNS server used during the initial connection to the Citrix Endpoint Management server is what determines the distribution point.

For example: Suppose that the DNS server IP of the mobile device originates in Fort Lauderdale, Florida. The CDN uses a local distribution point closest to that location to deliver the app to the mobile device. That use of the CDN results in improved app download time.

When a mobile device first requests or pushes an enterprise app, Citrix Endpoint Management copies the app to the local distribution point and keeps the app there for 24 hours for other local device downloads.

Deliver enterprise apps from the Citrix CDN

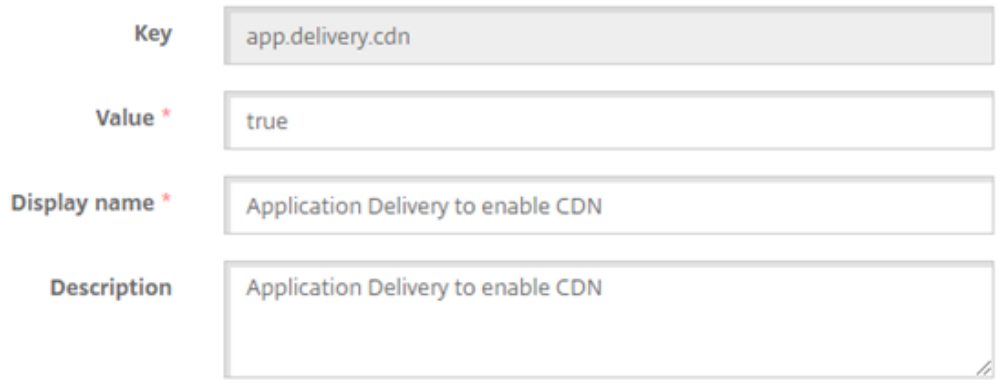
With Citrix Endpoint Management release 19.4.1, enterprise app delivery defaults to CDN delivery for all new multitenancy customers. For existing customers before this release, follow the instructions in this section.

For enterprise apps already on the Citrix Endpoint Management server, Citrix Endpoint Management continues to deliver those apps from the server until those apps get reuploaded after you complete the following steps.

> **Important:**
>
> Only Citrix Cloud administrators can enable CDN for an account. The server property `app.delivery.cdn` is visible in Citrix Endpoint Management only when you log on as a Citrix Cloud administrator. For information about Citrix Cloud administrators, see Manage Citrix Cloud administrators.

1. Enable CDN for your account: In the Citrix Endpoint Management console: Go to **Settings > Server Properties**.
2. Search for `app.delivery.cdn` and then click **Edit**.
3. Change the value to **true**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. In the Citrix Endpoint Management console, upload your enterprise apps again:

    a) Go to **Configure > Apps** and filter the app list by **Type** (**Enterprise**) and **Platform**.
    b) Select an app, click **Edit**, click **Next**, and click **Upload**.
    c) Repeat the prior step for each enterprise app.

Deliver MDX apps from the Citrix CDN

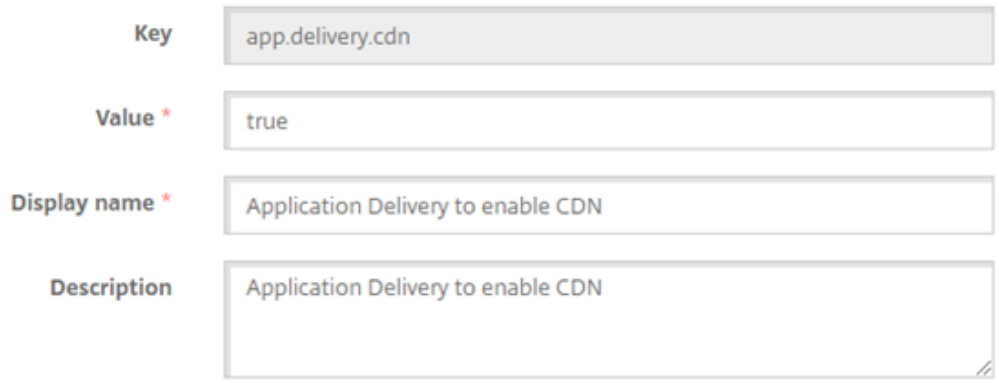
With Citrix Endpoint Management release 20.12.0, MDX app delivery defaults to CDN delivery for all new multitenancy customers. For existing customers before this release, follow the instructions in this section.

For MDX apps already on the Citrix Endpoint Management server, Citrix Endpoint Management continues to deliver those apps from the server until those apps get reuploaded after you complete the following steps.

> **Important:**
>
> Only Citrix Cloud administrators can enable CDN for an account. The server property `app.delivery.cdn` is visible in Citrix Endpoint Management only when you log on as a Citrix Cloud administrator. For information about Citrix Cloud administrators, see Manage Citrix Cloud administrators.

1. Enable CDN for your account: In the Citrix Endpoint Management console: Go to **Settings > Server Properties**.
2. Search for `app.delivery.cdn` and then click **Edit**.
3. Change the value to **true**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. In the Citrix Endpoint Management console, upload your MDX apps again:

    a) Go to **Configure > Apps** and filter the app list by **Type** (**MDX**) and **Platform**.
    b) Select an app, click **Edit**, click **Next**, and click **Upload**.
    c) Repeat the prior step for each MDX app.

Add a Web link

A web link is a web address to an internet or intranet site. A web link can also point to a web application that doesn't require SSO. After you finish configuring a web link, the link appears as an icon in the app store. When users log on with Citrix Secure Hub, the link appears with the list of available apps and desktops.

You can configure web links from the **Apps** tab in the Citrix Endpoint Management console. When you finish configuring the web link, the link appears as a link icon in the list in the **Apps** table. When users log on with Citrix Secure Hub, the link appears with the list of available apps and desktops.

Watch this video to learn more:

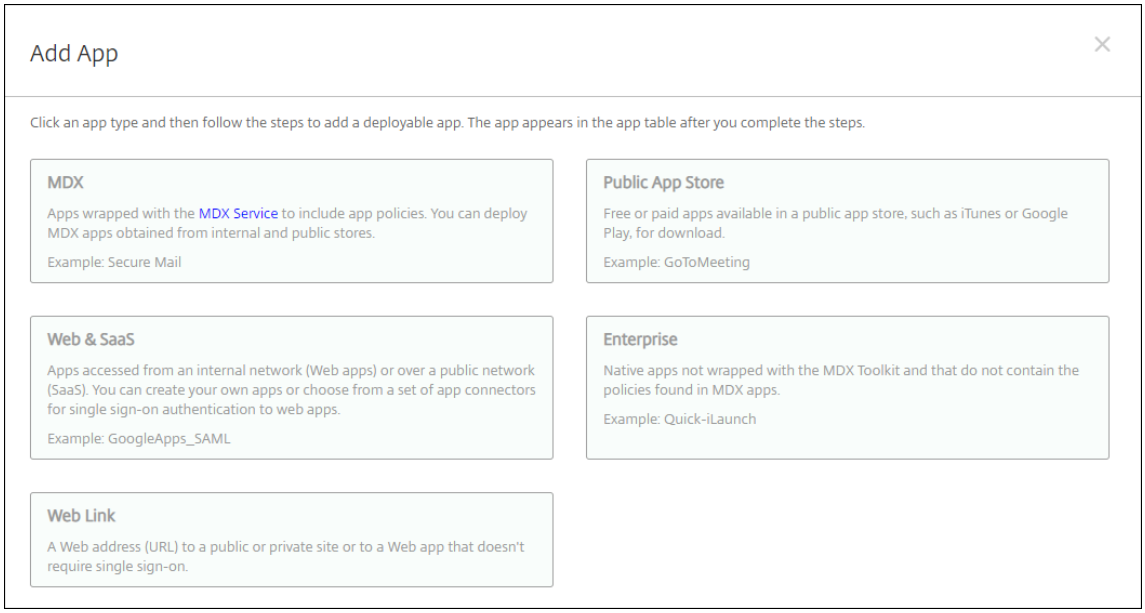
© 1997–2025 Citrix Systems, Inc. All rights reserved.

To add the link, you provide the following information:

- Name for the link
- Description of the link
- Web address (URL)
- Category
- Role
- Image in .png format (optional)

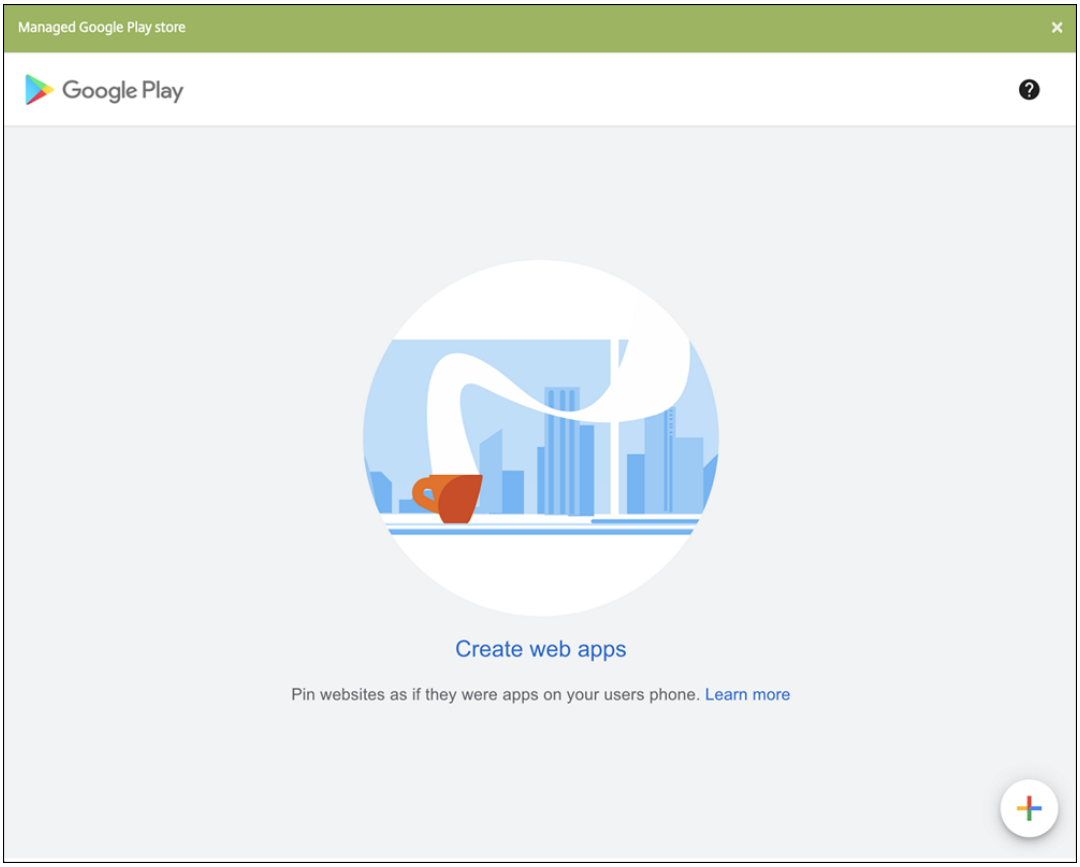
1. In the Citrix Endpoint Management console, click **Configure > Apps > Add**. The **Add App** dialog box appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. Click **Web Link**. The **App Information** page appears.
3. On the **App Information** pane, type the following information:
   - **Name:** Type a descriptive name for the app. This name is listed under App Name on the Apps table.
   - **Description:** Type an optional description of the app.
   - **App category:** Optionally, in the list, click the category to which you want to add the app. For more information about app categories, see About app categories.
4. Click **Next**. The **App Platforms** page appears.
5. Under **Platforms**, select **Other platforms** to add a web app for iOS, Android (legacy DA), and Windows 8, or select **Android Enterprise**. Clear the checkbox for any platforms that you don't want to include.
   - If you select **Other platforms**, continue to the next step to configure the settings.
   - If you select **Android Enterprise**, click the **Upload** button to open the managed Google Play store. You do not need to register for a developer account to publish a web app. Click the **Plus** icon in the lower right corner to continue.

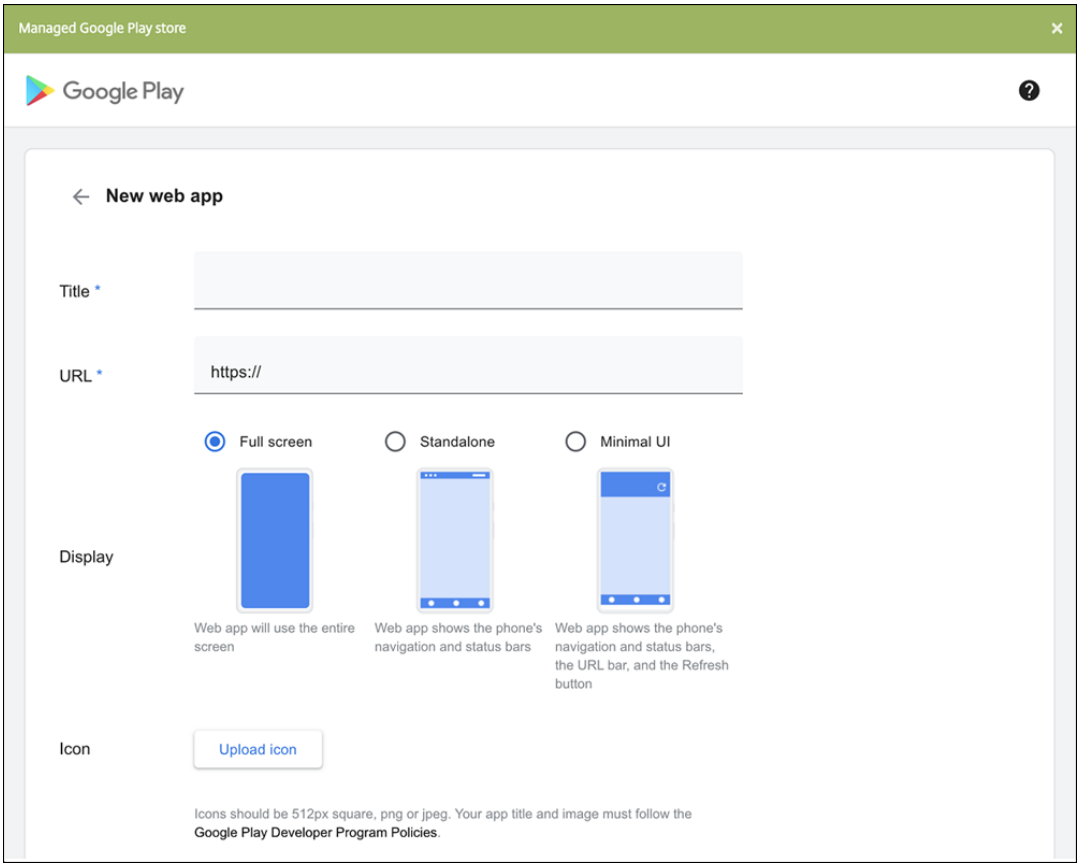
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure these settings:

- **Title:** Type the name for the web app.
- **URL:** Type the web address for the app.
- **Display:** Choose how to display the web app on the user devices. The available options are **Full screen**, **Standalone**, and **Minimal UI**.
- **Icon:** Upload your own image for the web app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



When finished, click **Create**. It might take up to 10 minutes for your web app to publish.

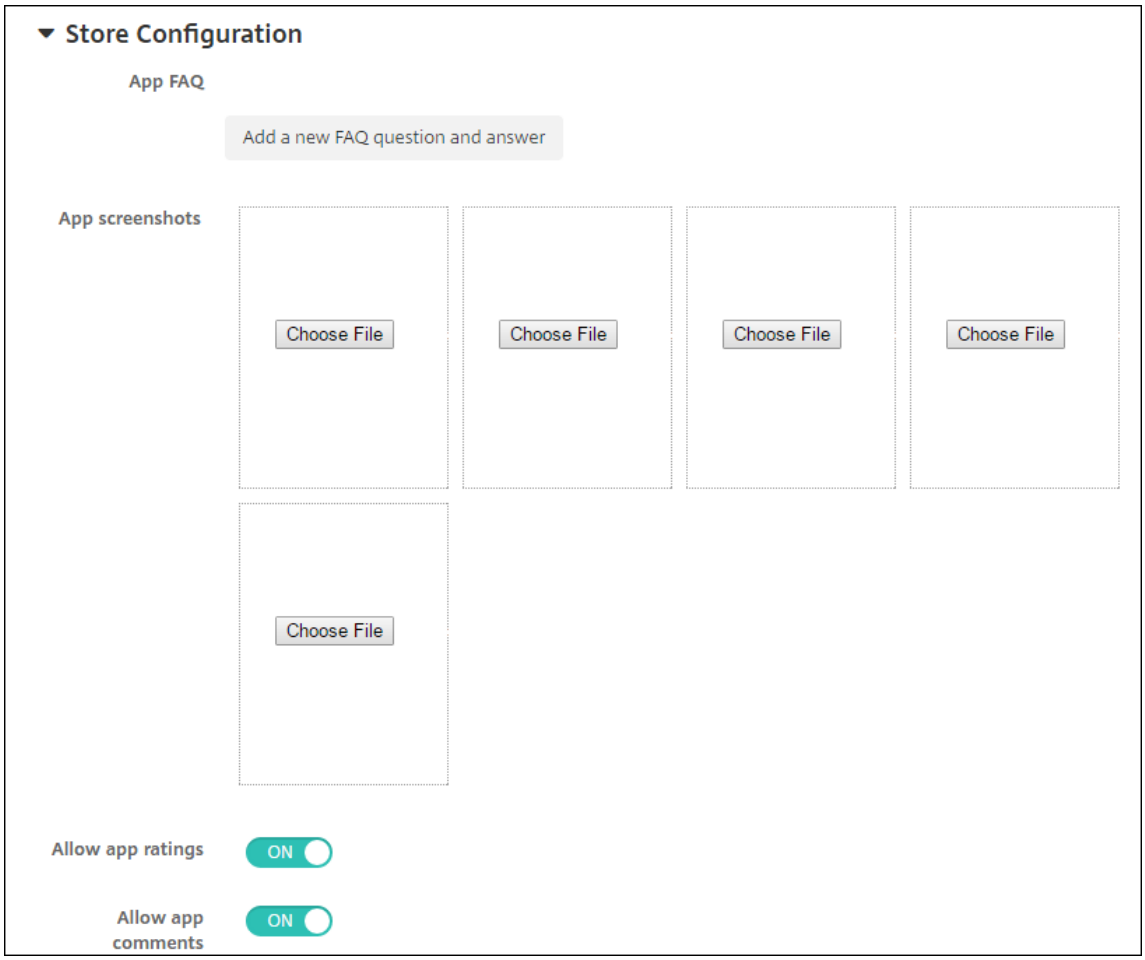
6. For platforms other than Android Enterprise, configure these settings:

   - **App name:** Accept the pre-filled name or type a new name.
   - **App description:** Accept the pre-filled description or type one of your own.
   - **URL:** Accept the pre-filled URL or type the web address for the app. Depending on the connector you choose, this field can have a placeholder that you must replace before you can move to the next page.
   - **App is hosted in internal network:** Select whether the app is running on a server in your internal network. If users connect from a remote location to the internal app, they must connect through NetScaler Gateway. Setting this option to **On** adds the VPN keyword to the app and allows users to connect through NetScaler Gateway. The default is **Off**.
   - **App category:** Click an optional category in the drop-down list to apply to the app.
   - **Image:** Select whether to use the default Citrix image or to upload your own app image. The default is Use default.
     - To upload your own image, click **Browse** and navigate to the file location. The file must be a .PNG file. You can't upload a JPEG or GIF file. When you add a custom graphic, you can't change it later.

7. Configure the deployment rules. For information, see Configure deployment rules.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

8. Expand **Store Configuration**.



   Optionally, you can configure the following:

   - **App FAQ:** Click **Add a new FAQ question and answer** to create a FAQ for the app.
   - **Add screenshots for phones/tablets:** Add screen captures that appear in the app store.
   - **Allow app ratings:** Allow users to rate the app in the app store.
   - **Allow app comments:** Allow users to leave comments on the app in the app store.

9. Click **Next**. The **Delivery Group Assignment** page appears.
10. Next to **Choose delivery groups**, type to find a delivery group or select a group or groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.
11. Expand **Deployment Schedule** and then configure the following settings:

    - **Deploy:** Choose whether to deploy the app to devices. The default is **On**.
    - **Deployment schedule:** Choose whether to deploy the app **Now** or **Later**. If you select **Later**, configure a date and time to deploy the app. The default is **Now**.
    - **Deployment condition:** Choose **On every connection** to deploy the app every time the device connects. Choose **Only when previous deployment has failed** to deploy the app

© 1997–2025 Citrix Systems, Inc. All rights reserved.

when the device failed to receive the app previously. The default is **On every connection**.

The **Deploy for always-on connection** option applies when you've configured the scheduling background deployment key in **Settings > Server Properties**.

The always-on option:

- Isn't available for iOS devices
- Isn't available for Android and Android Enterprise customers who began using Citrix Endpoint Management with version 10.18.19 or later
- Isn't recommended for Android and Android Enterprise customers who began using Citrix Endpoint Management before version 10.18.19

The deployment schedule that you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

12. Click **Save**.

Enable Microsoft 365 apps

You can open the MDX container to allow Citrix Secure Mail, Citrix Secure Web, and Citrix Files to transfer documents and data to Microsoft Office 365 apps. For details, see Allowing Secure Interaction with Office 365 Apps.

Apply workflows

Configure these settings to assign or create a workflow:

- **Workflow to Use:** Click an existing workflow in the drop-down list or click **Create a new workflow**. The default is **None**.

  If you select **Create a new workflow**, configure these settings.

  - **Name:** Type a unique name for the workflow.
  - **Description:** Optionally, type a description for the workflow.
  - **Email Approval Templates:** In the list, select the email approval template to be assigned. When you click the eye icon to the right of this field, a dialog box appears where you can preview the template.
  - **Levels of manager approval:** In the list, select the number of levels of manager approval required for this workflow. The default is 1 level. Possible options are:
    * Not Needed
    * 1 level

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    * 2 levels
    * 3 levels

- **Select Active Directory domain:** In the list, select the appropriate Active Directory domain to be used for the workflow.
- **Find additional required approvers:** Type the name of the additional required person in the search field and then click **Search**. Names originate in the Active Directory.
- When the name appears in the field, select the checkbox next to the name. The name and email address appear in the **Selected additional required approvers** list.

  To remove a person from the **Selected additional required approvers** list, do one of the following:

    * Click **Search** to see a list of all the persons in the selected domain.
    * Type a full or partial name in the search box, and then click **Search** to limit the search results.
    * Persons in the **Selected additional required approvers** list have check marks next to their name in the search results list. Scroll through the list and clear the checkbox next to each name you want to remove.

App store and Citrix Secure Hub branding

You can set how apps appear in the store and add your logo to Citrix Secure Hub and the app store. These branding features are available for iOS and Android devices.

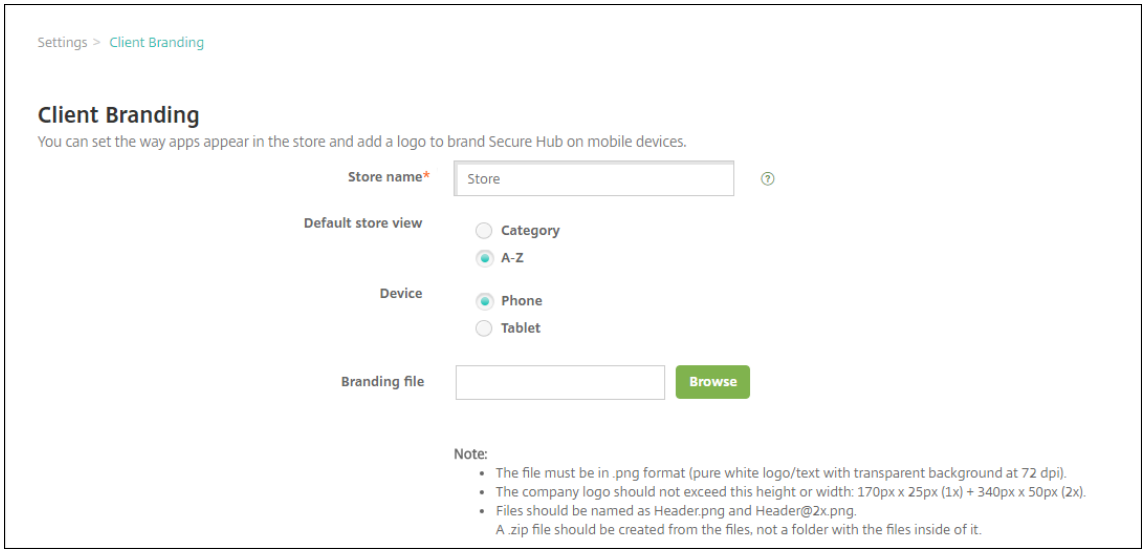
Before you begin, make sure you have your custom image ready and accessible.

The custom image must meet these requirements:

- The file must be in .png format
- Use a pure white logo or text with a transparent background at 72 dpi.
- The company logo can't be more than this height or width: 170 px x 25 px (1x) and 340 px x 50 px (2x).
- Name the files as `Header.png` and `Header@2x.png`.
- Create a .zip file from the files, not a folder with the files inside it.

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Client**, click **Client Branding**. The **Client Branding** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure the following settings:

- **Store name:** The store name appears in the user's account information. Changing the name also changes the URL used to access store services. You typically do not need to change the default name.

  > **Important:**
  >
  > The Store name can only have alphanumeric characters.

- **Default store view:** Select either **Category** or **A-Z**. The default is **A-Z**
- **Device option:** Select either **Phone** or **Tablet**. The default is **Phone**.
- **Branding file:** To select a branding image or .zip file of images, click **Browse** and navigate to the file location.

3. Click **Save**.

To deploy this package to user devices, create a deployment package and then deploy the package.

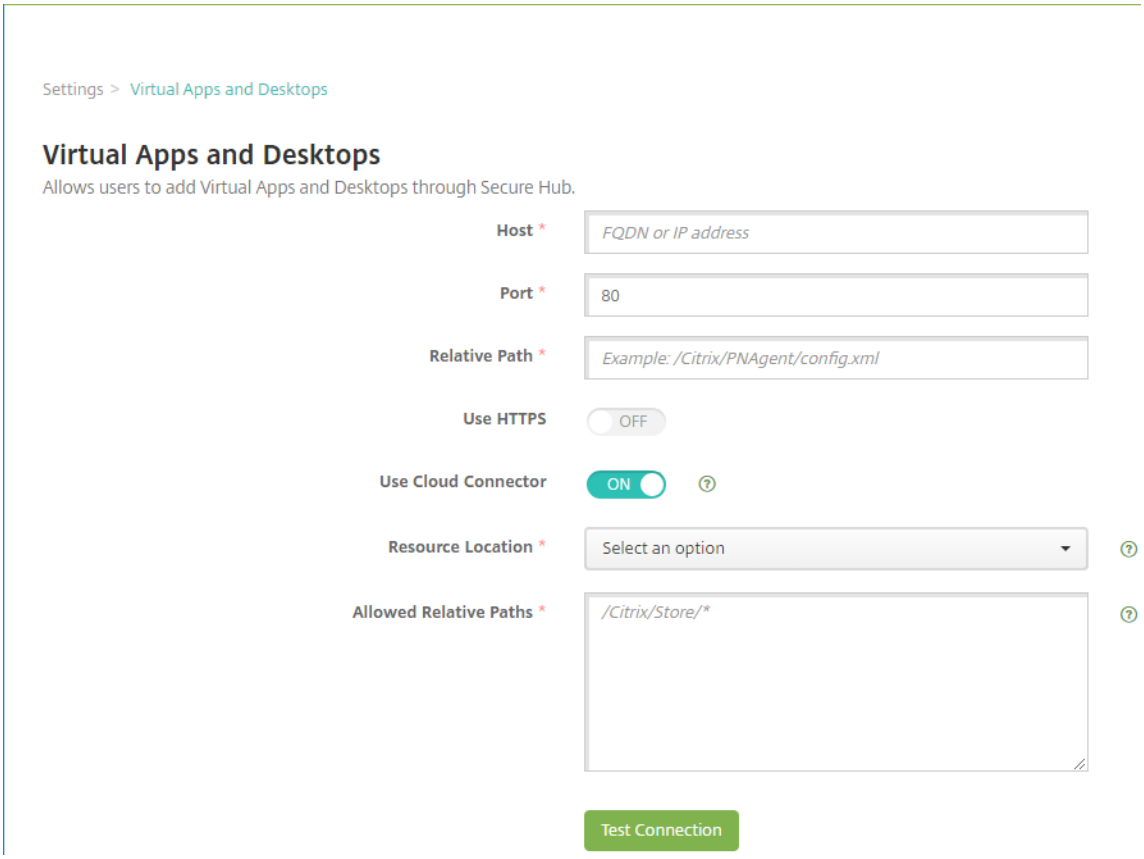
Citrix Virtual Apps™ and Desktops through the app store

Citrix Endpoint Management can collect apps from Citrix Virtual Apps and Desktops and make the apps available to mobile device users in the app store. Users subscribe to the apps directly inside the app store and launch them from Citrix Workspace. The Citrix Workspace app must be installed on user devices to launch the apps.

To configure this setting, you need the fully qualified domain name (FQDN) or IP address and port number for an on-premises StoreFront.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. In the Citrix Endpoint Management web console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **Virtual Apps and Desktops**. The **Virtual Apps and Desktops** page appears.



3. Configure these settings:

   - **Host:** Type the fully qualified domain name (FQDN) or IP address for StoreFront.
   - **Port:** Type the port number for StoreFront. The default is 80.
   - **Relative Path:** Type the path. For example, /Citrix/PNAgent/config.xml
   - **Use HTTPS:** Select whether to enable secure authentication between StoreFront and the client device. The default is **Off**.
   - **Use Cloud Connector:** Choose **On** to use Cloud Connector for connections to the StoreFront server. Then, specify a **Resource Location** and **Allowed Relative Paths** for the connection.
     - **Resource Location:** Choose from the resource locations defined in Citrix Cloud Connector.
     - **Allowed Relative Paths:** The relative paths allowed for the specified resource location. Specify one path per line. You can use the asterisk (*) wildcard.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Suppose that the resource location is `https://StoreFront.company.com` and you want to provide access to the following URLs:

- `https://StoreFront.company.com/Citrix/PNAgent/Config.xml`
- `https://StoreFront.company.com/Citrix/PNAgent/enum.aspx`
- `https://StoreFront.company.com/Citrix/PNAgent/launch.aspx`

To allow all requests with the URL `https://StoreFront.company.com/Citrix/PNAgent/*`, enter this path: `/Citrix/PNAgent/*`

Citrix Endpoint Management blocks all other paths.

4. Click **Test Connection** to verify that Citrix Endpoint Management can connect to the specified StoreFront server.
5. Click **Save**.

App connector types

September 6, 2025

The following table lists the connectors and the types of connectors that are available in Citrix Endpoint Management when you add a Web or SaaS app. You can also add a connector to Citrix Endpoint Management when you add a Web or SaaS app.

The table indicates whether the connector supports user account management, which lets you create accounts automatically or by using a workflow.

Connector name	SSO SAML	Supports user account management
EchoSign_SAML	Y	Y
Globoforce_SAML		**Note:** When using this connector, you must enable User Management for Provisioning to make sure seamless SSO integration.
GoogleApps_SAML	Y	Y
GoogleApps_SAML_IDP	Y	Y
Lynda_SAML	Y	Y
Office365_SAML	Y	Y

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Connector name	SSO SAML	Supports user account management
Salesforce_SAML	Y	Y
Salesforce_SAML_SP	Y	Y
SandBox_SAML	Y	
SuccessFactors_SAML	Y	
ShareFile_SAML	Y	
ShareFile_SAML_SP	Y	
WebEx_SAML_SP	Y	Y

Citrix Launcher

February 22, 2024

Citrix Launcher lets you customize the user experience for Android Enterprise devices and legacy Android devices deployed by Citrix Endpoint Management. With Citrix Launcher, you can prevent users from accessing certain device settings and restrict devices to one app or a small set of apps.

The minimum Android version supported for Citrix Secure Hub management of Citrix Launcher is Android 6.0.

Use a **Launcher Configuration Policy** to control these Citrix Launcher features:

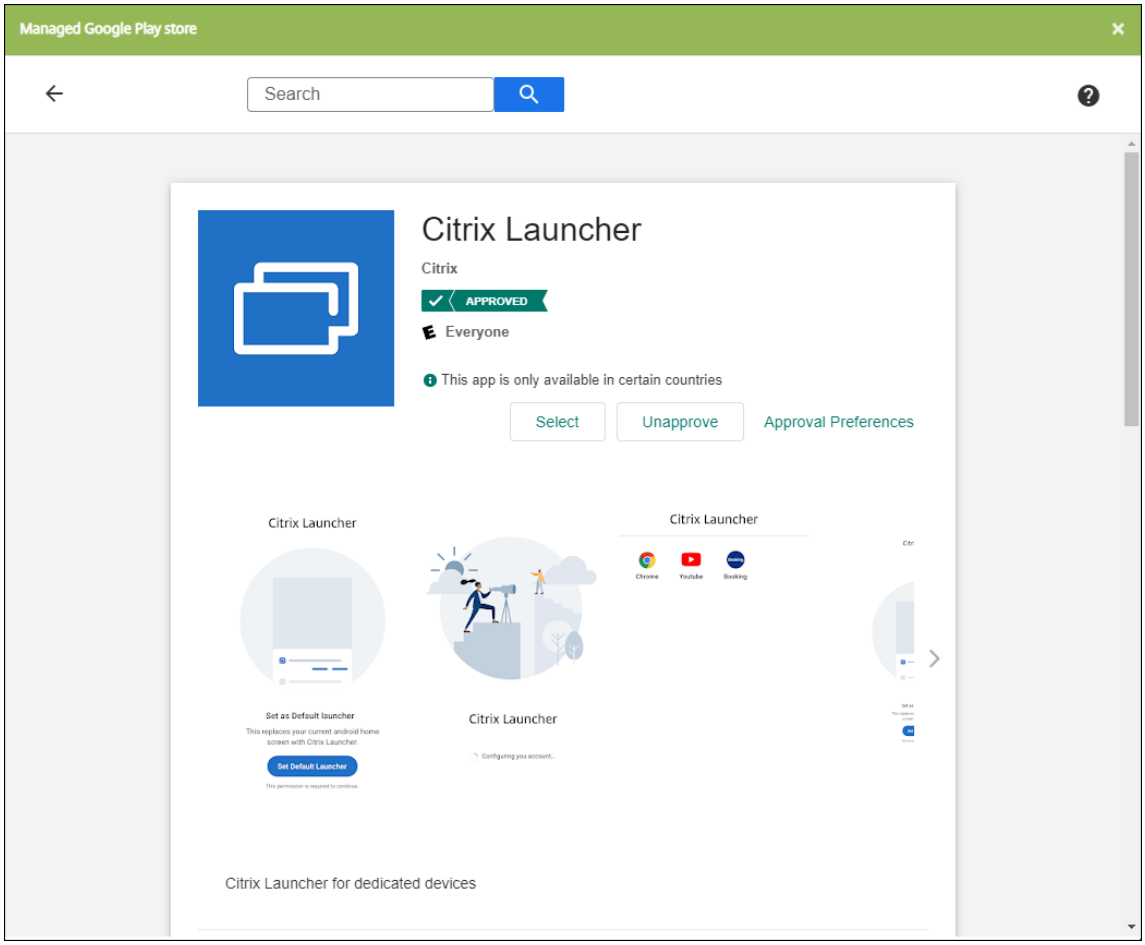
- Manage Android Enterprise devices and legacy Android devices so that users can access only the apps that you specify.
- Optionally specify a custom logo image for the Citrix Launcher icon and a custom background image for Citrix Launcher.
- Specify a password that users must type to exit the launcher.

Citrix Launcher isn't intended to be an extra layer of security over what the device platform already provides.

Set up Citrix Launcher for Android Enterprise devices

1. Add the Citrix Launcher app (com.citrix.launcher.droid) to Citrix Endpoint Management as a public store app. In **Configure > Apps**, click **Add**, and then click **Public App Store**. For more information, see Add a public app store app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. In the Kiosk device policy, specify which apps must be available on company-owned devices for dedicated use (also known as Android corporate owned single-use (COSU) devices). Go to **Configure > Device Policies**, click **Add**, and select **Kiosk**. Then select the Citrix Launcher app and any additional apps in the allow list. If you previously added apps to the list, you don't need to upload the apps again. For more information, see Android Enterprise settings.
3. Add the Launcher Configuration device policy. Go to **Configure > Device Policies**, click **Add**, and select **Launcher Configuration**. In the Launcher Configuration policy, add any of the apps that you specified in the Kiosk policy. You don't need to add all the apps you specified in the Kiosk policy. You must add the Citrix Launcher app only in the Kiosk policy. For more information, see Launcher Configuration Policy.
4. Create a delivery group and deploy resources. For more information, see the Add a delivery group and deploy resources section in this article.

After you deploy Citrix Launcher on company-owned Android Enterprise devices for dedicated use, Citrix Endpoint Management installs the app and replaces the default Citrix Secure Hub launcher. If you exit the Citrix Launcher app, Citrix Secure Hub becomes the default launcher again.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Set up Citrix Launcher for legacy Android devices

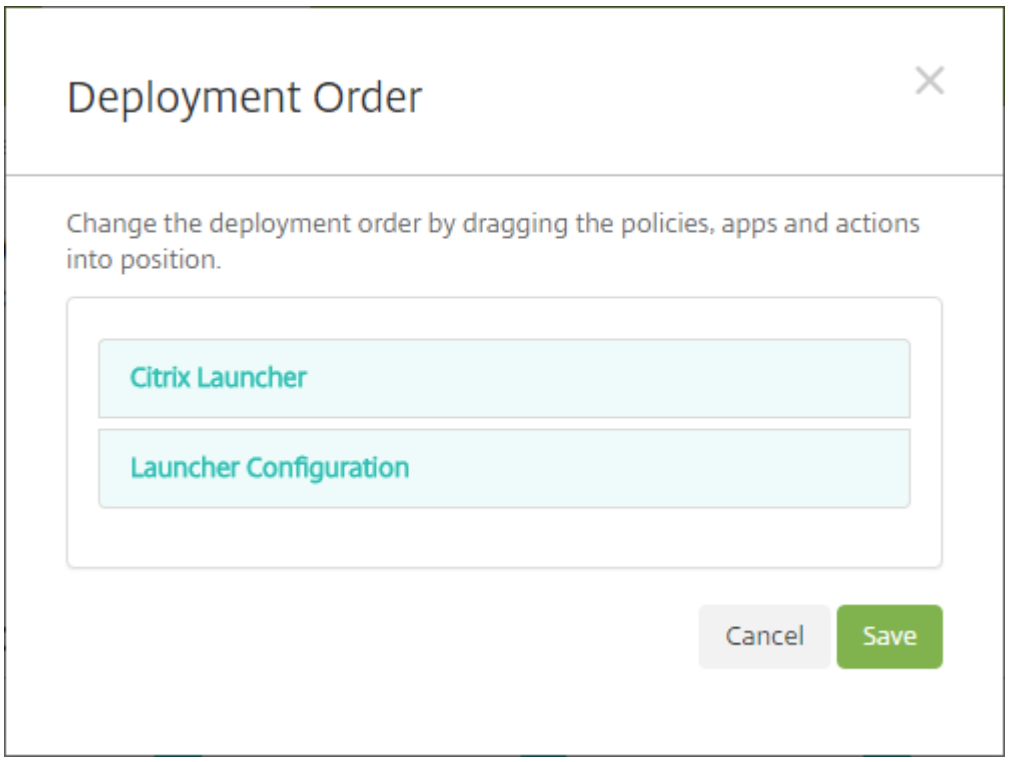
> **Note:**
>
> In August 2020, Citrix deprecated support for the CitrixLauncher.apk for legacy Android devices. You can continue using the legacy Citrix Launcher app (com.citrix.launcher) for Android devices without receiving the new feature updates.

1. To locate the Citrix Launcher app, go to the Citrix Endpoint Management download page and search for **Citrix Launcher**. Download the latest file. The file is ready for upload into Citrix Endpoint Management and doesn't require wrapping.
2. Add the Launcher Configuration device policy. Go to **Configure > Device Policies**, click **Add**, and select **Launcher Configuration**. For more information, see Launcher Configuration Policy.
3. Add the Citrix Launcher app to Citrix Endpoint Management as an enterprise app. In **Configure > Apps**, click **Add** and then click **Enterprise**. For more information, see Add an enterprise app.
4. Create a delivery group and deploy resources. For more information, see the Add a delivery group and deploy resources section in this article.

Add a delivery group and deploy resources

1. Create a delivery group for Citrix Launcher with the following configuration in **Configure > Delivery groups**.
    - On the **Policies** page, add a **Launcher Configuration Policy**.
    - On the **Apps** page, drag **Citrix Launcher** to **Required Apps**.
    - On the **Summary** page, click **Deployment Order** and make sure that the **Citrix Launcher** app precedes the **Launcher Configuration** policy.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. Deploy resources to a delivery group by sending a push notification to all users in the delivery group. For more information about adding resources to a delivery group, see Deploy resources.

Manage devices without Citrix Launcher

Instead of using Citrix Launcher, you can use features that are already available.

To provision dedicated devices:

1. Create an enrollment profile by setting the **Device owner mode** to **Dedicated device**. See Provisioning dedicated Android Enterprise devices and Enrollment profiles.
2. Create a Kiosk device policy to add apps to the allow list and set lock task mode. If you previously added apps to the list, you don't need to upload the apps again. For more information, see Android Enterprise settings.
3. Enroll each device in the enrollment profile that you created.

Add apps using Apple Volume Purchase

February 29, 2024

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Apple Business Manager (ABM) and Apple School Manager (ASM) let you buy licenses for apps and books in volume and synchronize the Volume Purchase information with Citrix Endpoint Management. You can then use Citrix Endpoint Management to deploy these apps and books to iOS and macOS devices. Buying contents in volume simplifies the process of finding, buying, and distributing apps and books for an organization.

For more information about buying contents using ABM or ASM, see the Apple Business Manager User Guide or Apple School Manager User Guide. This article describes how to synchronize volume-purchased licenses from ABM and ASM to Citrix Endpoint Management and how to manage the licenses.

> **Note:**
>
> The apple Volume Purchase Program (VPP) is no longer available as of January 14, 2021. The Volume Purchase function was integrated in ABM and ASM. If you currently use the Device Enrollment Program (DEP) or VPP, you can upgrade to ABM or ASM. For more information, see the Apple documentation Upgrade from Apple Deployment Programs.

About Apple Volume Purchase

When you buy contents in volume using ABM or ASM, note the following:

- You can buy licenses for the following content:
  - Public apps and books
  - Custom apps that are developed specifically for your organization
- You can deploy volume-purchased apps and books to organization-owned devices and BYO devices. Organization-owned devices enrolled through ABM or ASM support MDM or MDM+MAM enrollment but not MAM enrollment.
- For more information about distributing apps, see Distribute Apple apps.
- For a list of known issues, see Knowledge Center article CTX222633.

Add a Volume Purchase account

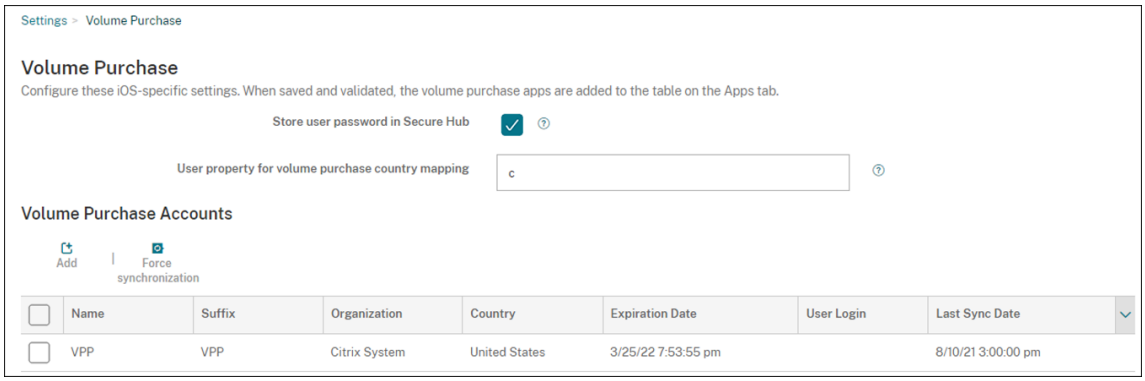
After you buy content in the ABM or ASM portal, download the content token associated with Citrix Endpoint Management from the portal. Next, in Citrix Endpoint Management, create a Volume Purchase account based on this content code. This code lets Citrix Endpoint Management synchronize the content licenses from ABM or ASM.

With the Volume Purchase, you can buy content and deploy it to devices by using managed licenses. If you currently use redemption codes and want to change to managed licenses, see the Apple support document.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To add a Volume Purchase account in Citrix Endpoint Management

1. In the ABM or ASM portal, buy the content as needed and then download the content code file to a secure location.
2. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
3. Click **Volume purchase**. The **Volume purchase** configuration page appears.



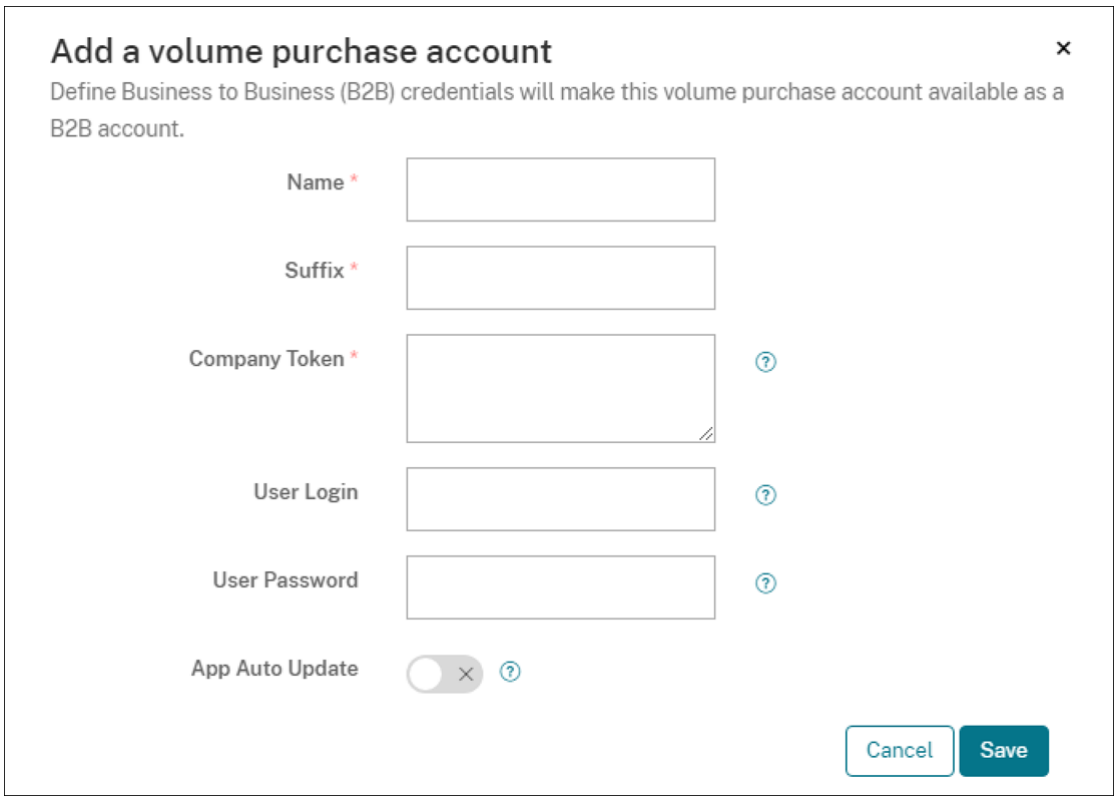
4. Configure the following settings:

   - **Store user password in Citrix Secure Hub:** Select whether to store a user name and password in Citrix Secure Hub for Citrix Endpoint Management authentication. The default is **On**.
   - **User property for Volume purchase country mapping:** Type a country mapping code to allow users to download apps from the country-specific app store. Contact your content manager for this code.

     Citrix Endpoint Management uses the country mapping code to choose the property pool of the Volume Purchase. For example, if the user property is United States, the user can't download apps if the mapping code is for the United Kingdom.

5. Click **Add**. The **Add a Volume Purchase account** dialog box appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. Configure the following account settings:

> **Note:**
>
> If you use Apple Configurator 1, upload a license file as follows: Click **Configure > Apps**, go to a platform page of an app, and then expand **Volume purchase**.

- **Name:** Type a descriptive name for the account.
- **Suffix:** Type the suffix to appear with the app names inherited from the Apple stores. For example, if you enter **VP**, the **Citrix Secure Mail** app appears in the apps list as **Citrix Secure Mail - VP**.
- **Company Token:** Copy and paste the content token that you downloaded in Step 1.
- **User Login:** (Optional) Type a user name for the administrator of this Volume Purchase account. If configured, the user name and password are required for synchronizing volume-purchased custom apps into Citrix Endpoint Management.
- **User Password:** (Optional) Type a password for the user name you typed.
- **App Auto Update:** If turned **On**, volume-purchased apps and optional apps in the Citrix Endpoint Management console update automatically when a new version is available. You must still update enterprise apps and public app store apps in the Citrix Endpoint Management console manually. If this setting is set as **Off**, you can still update volume-purchased apps in the Citrix Endpoint Management console manually. Once an app updates in the console, devices with the app installed receive that update as well. The default is **Off**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

After the volume account is added successfully, a message appears, notifying you of the following:

- On the **Configure > Apps** page, the volume-purchased apps appear in the App list. The app names appear with the suffix that you configured.
- On the **Configure > Media** page, the volume-purchased books appear in the Media list. The book names appear with the suffix that you configured.

Configure volume-purchased apps

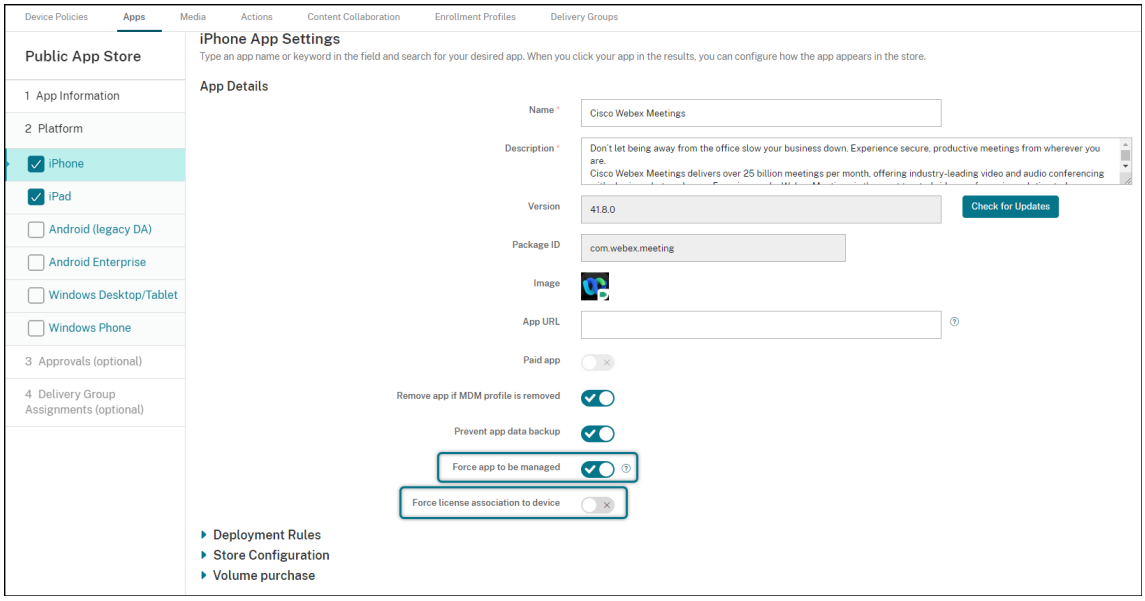
After you add a Volume Purchase account, the app information is synchronized to Citrix Endpoint Management and appears on the **Configure > Apps** page. You can now configure these apps, tune your delivery group, and adjust device policy settings for iOS and macOS devices. After you complete the configuration, users can enroll their devices.

When configuring a volume-purchased app, note the following settings:

- On the **Configure > Apps** page:
  - To let Citrix Endpoint Management deploy an app to a device rather than to a user, turn on **Force license association to device**. When this setting is on, users don't have to use their Apple ID and can download the apps without signing into their App Store account.
  - We recommend you turn on **Force app to be managed** for an app so that it automatically installs as a managed app.

> **Note:**
>
> To enable the **Force app to be managed** setting to take effect, you must configure the `apple.app.force.managed` server property to **True** on the **Settings > Server Properties** page. For more information, see Server properties

© 1997–2025 Citrix Systems, Inc. All rights reserved.



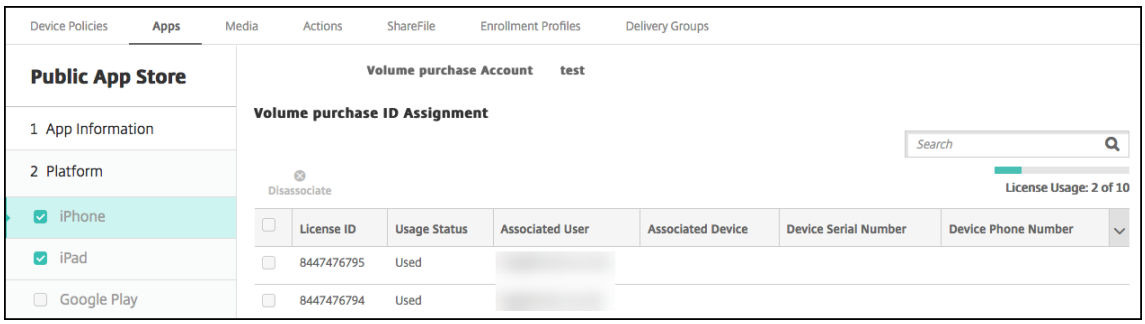
- On the **Configure > Delivery Group** page:

  To have the app install silently on user devices with minimal user interaction, go to the **Apps** page and then drag the app to the **Required Apps** list. By default, apps except Citrix Secure Hub are **Optional Apps**, which means users must start the app installation manually through Citrix Secure Hub.

Track and manage the use of app licenses

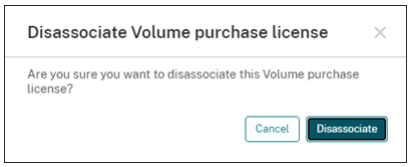
You can track the license usage for an app. If needed, you can take back a used license, making it available to another user or device.

1. Click **Configure > Apps**.
2. Select an app and click **Edit**.
3. Go to the **Platform** page and then expand **Volume purchase**.
   In the **Volume purchase ID Assignment** table, you can track how many licenses are used and by which user or device.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. To take back a license, select the license and then click **Disassociate**.

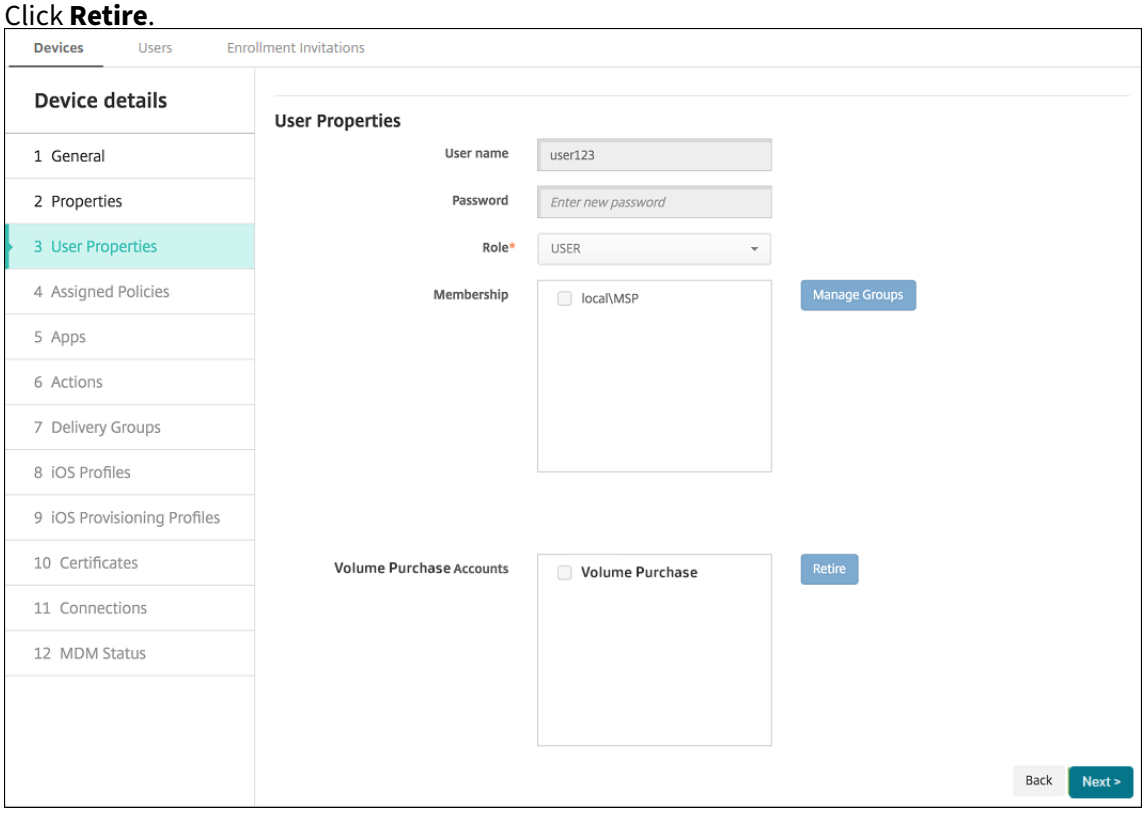


5. Click **Disassociate** to confirm the action.

Retire a user from the Volume Purchase account

If you associate app licenses to users, you can retire users from the Volume Purchase accounts to take back all licenses that are assigned to those users. A use case includes when a user leaves your organization.

1. Click **Manage > Devices**
2. Select the device belonging to the target user and then click **Edit**.
3. Go to the **User Properties** page and select the Volume Purchase accounts as needed.
4. Click **Retire**.



Citrix Endpoint Management revokes app licenses in the selected Volume Purchase accounts from the user.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Synchronize the app information

Citrix Endpoint Management periodically synchronizes the app information with ABM or ASM. If needed, you can manually synchronize the app information. Synchronization makes sure that the app licenses and other app information reflect all changes. Such changes include when you manually delete an app from the Volume Purchase account.

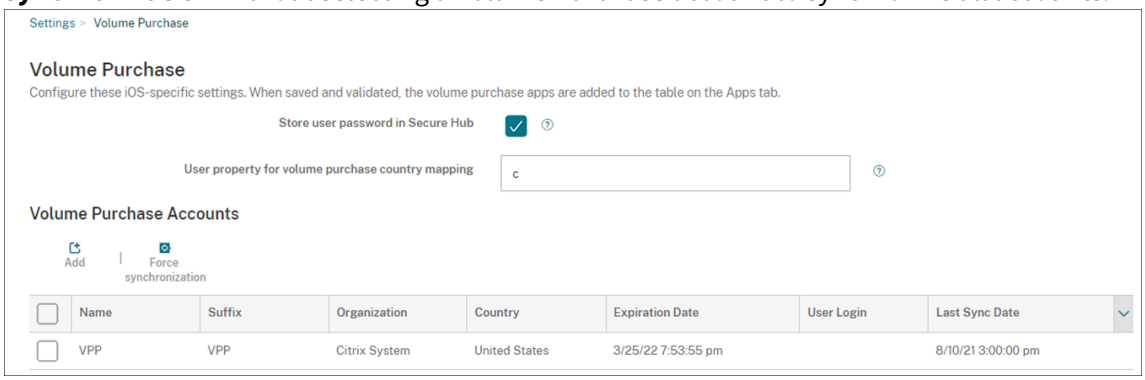
Change the default synchronization interval

By default, Citrix Endpoint Management refreshes the Volume Purchase license baseline at least every 1440 minutes (24 hours). A Citrix Cloud administrator can change the default interval through the server property, `vpp.baseline`. For more information, see Server properties.

Manually synchronize the app information

You can force a synchronization with ABM or ASM to get the latest app information immediately.

1. Click **Settings > Volume Purchase**
2. Select a Volume Purchase account and then click **Force synchronization**. Or click **Force synchronization** without selecting a Volume Purchase account to synchronize all accounts.



3. Confirm the synchronization action. The synchronization starts.

   The synchronization might take several minutes depending on the number of Volume Purchase licenses. After the synchronization completes, Citrix Endpoint Management refreshes the **Volume Purchase** page and updates the sync date and time in the new **Last Sync Date** column.

Check for the app updates

If you turn on the **App Auto Update** setting when adding a Volume Purchase account, Citrix Endpoint Management periodically checks for the new versions for volume-purchased apps and optional apps

© 1997–2025 Citrix Systems, Inc. All rights reserved.

and makes updates. If needed, you can manually check for the new version for any app and apply the app updates to Citrix Endpoint Management.

Once Citrix Endpoint Management receives a new version of a required app, it pushes the new version to the device for silent installation without prompting users.

To check and apply the new version for an app

1. Click **Configure > Apps**. The **Apps** page appears.
2. Select an app and click **Edit**.
3. Go to the **Platform** page, and then click **Check for Updates** next to **Version**.
4. In the **Update** dialog box that appears, apply the update if a new version is available.

Renew the content token for your Volume Purchase account

A content token expires annually. When the token is nearing expiration, Citrix Endpoint Management displays a license expiration warning. Renew the content token in time to prevent interruption for your users.

1. From the ABM or ASM portal, download an updated token.
2. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
3. Click **Volume Purchase**. The Volume Purchase configuration page appears.
4. Edit your Volume Purchase account with the updated token info.

Use ShareFile with Citrix Endpoint Management

September 6, 2025

> **Disclaimer:**
>
> This feature will be deprecated if ShareFile (now Progress) discontinues support.

Citrix Endpoint Management has two options for integrating with ShareFile. They are Citrix Files and storage zone connectors.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Files

You can configure Citrix Endpoint Management to provide access to your ShareFile account. That configuration:

- Gives mobile users access to the full ShareFile feature set, such as file sharing, file sync, and storage zone connectors.
- Can provide Citrix Files with single sign-on authentication of mobile productivity app users and comprehensive access control policies.
- Provides ShareFile configuration, service level monitoring, and license usage monitoring through the Citrix Endpoint Management console.

For more information about configuring Citrix Endpoint Management for Enterprise accounts, see SAML for single sign-on with Citrix Files.

Storage zone connectors

You can configure Citrix Endpoint Management to provide access only to storage zone connectors that you create through the Citrix Endpoint Management console. That configuration:

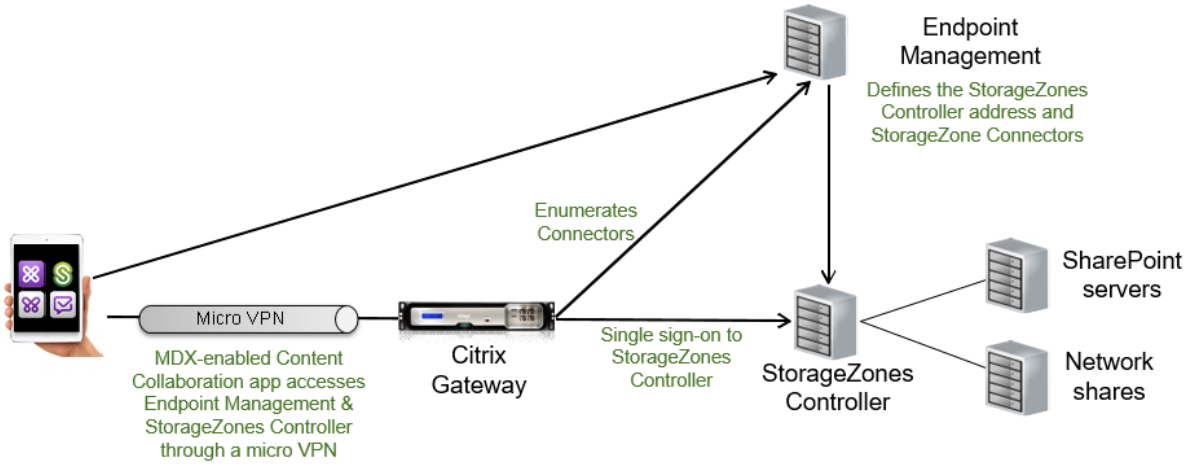
- Provides secure mobile access to existing on-premises storage repositories, such as SharePoint sites and network file shares.
- Doesn't require that you set up a ShareFile subdomain or host Citrix Files data.
- Provides users with mobile access to data through the Citrix mobile productivity apps for Citrix Files for iOS and Android. Users can edit Microsoft Office documents. Users can also preview and annotate Adobe PDF files from mobile devices.
- Complies with security restrictions against leaking user information outside of the corporate network.
- Provides simple setup of storage zone connectors through the Citrix Endpoint Management console. If you later decide to use the full Citrix Files functionality with Citrix Endpoint Management, you can change the configuration in the Citrix Endpoint Management console.

For an Citrix Endpoint Management integration with storage zone connectors only:

- ShareFile uses your single sign-on configuration to NetScaler Gateway to authenticate with the storage zones controller.
- Citrix Endpoint Management doesn't authenticate through SAML because the Citrix Files control plane isn't used.

The following diagram shows the high-level architecture for Citrix Endpoint Management use with storage zone connectors.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Requirements

- Minimum component versions:
  - ShareFile for iOS (MDX) 5.3
  - ShareFile for Android (MDX) 5.3
  - Storage zones controller 5.11.20
    This article has instructions for how to configure storage zones controller 5.0
- Make sure that the server to run the storage zones controller meets the system requirements. For requirements, see System requirements.

The requirements for storage zones for Citrix Files Data and for Restricted storage zones don't apply to an Citrix Endpoint Management integration with storage zone connectors only.

Citrix Endpoint Management doesn't support Documentum connectors.

- To run PowerShell scripts:
  - Run the scripts in the 32-bit (x86) version of PowerShell.

Installation tasks

Complete the following tasks, in the order presented, to install and set up storage zones controller. These steps are specific to Citrix Endpoint Management integration with storage zone connectors only. Some of these articles are in the storage zones controller documentation.

1. Configure NetScaler for storage zones controller

   You can use NetScaler Gateway as a DMZ proxy for the storage zones controller.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Install an SSL certificate

   A storage zones controller that hosts standard zones requires an SSL certificate. A storage zones controller that hosts restricted zones and uses an internal address doesn't require an SSL certificate.

3. Prepare your server

   IIS and ASP.NET setup is required for storage zone connectors.

4. Install storage zones controller
5. Prepare storage zones controller for use with storage zone connectors-only
6. Specify a proxy server for storage zones

   The storage zones controller console enables you to specify a proxy server for the storage zones controller. You can also specify a proxy server using other methods.

7. Configure the domain controller to trust the storage zones controller for delegation

   Configure the domain controller to support NTLM or Kerberos authentication on network shares or SharePoint sites.

8. Join a secondary storage zones controller to a storage zone

   To configure a storage zone for high availability, connect at least two storage zones controllers to it.

Install storage zones controller

1. Download and install the storage zones controller software:

   a) From ShareFile Tool/App Downloads, log on and download the latest storage zones controller installer.

   b) Installing the storage zones controller changes the default website on the server to the installation path of the controller. Enable **Anonymous Authentication** on the default website.

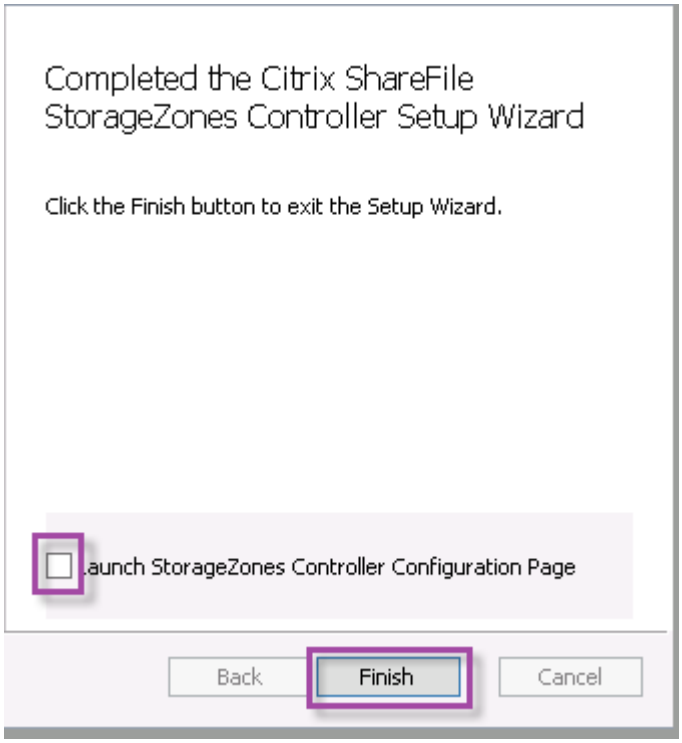
2. On the server where you want to install storage zones controller, run StorageCenter.msi.

   The storage zones controller setup wizard starts.

3. Respond to the prompts:

   - In the **Destination Folder** page, if Internet Information Services (IIS) is installed in the default location, leave the defaults. If not, browse to the IIS installation location.
   - When installation is complete, clear the checkbox for **Launch Storage Zones Controller Configuration Page** and then click **Finish**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. When prompted, restart the storage zones controller.
5. To test that the installation was successful, navigate to `https://localhost/`. (If you get a certificate error, consider connecting with HTTP instead.) If the installation is successful, the Citrix Files logo appears.

   If the Citrix Files logo does not appear, clear the browser cache and try again.

   > **Important:**
   >
   > If you plan to clone the storage zones controller, capture the disk image before you continue with configuring the storage zones controller.

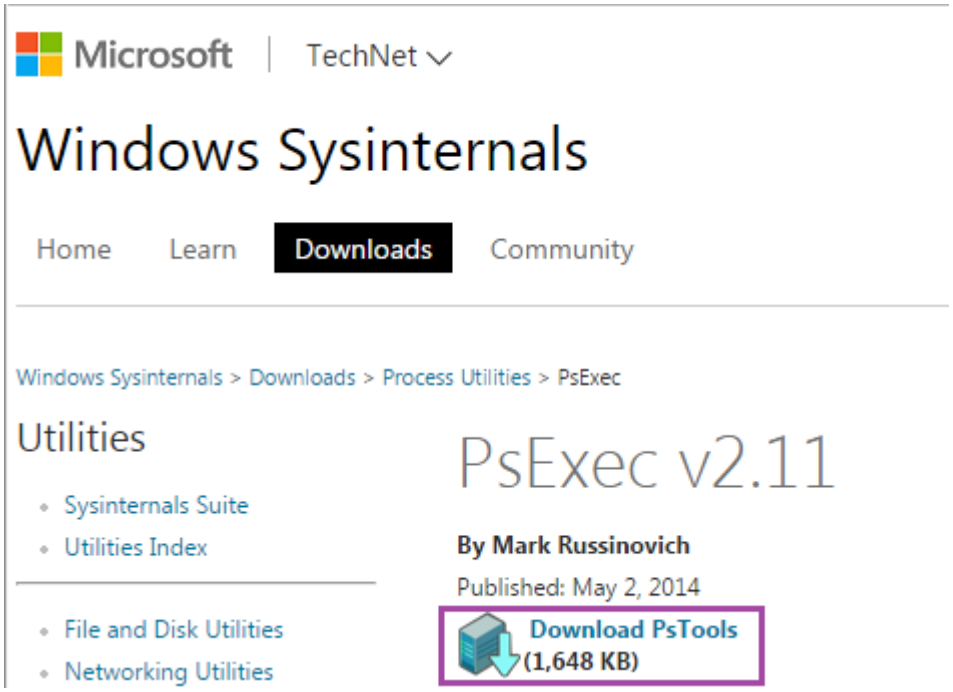
Prepare storage zones controller for use with storage zone connectors-only

For an integration only with storage zone connectors, you don't use the storage zones controller administrative console. That interface requires a Citrix Files administrator account, which isn't necessary for this solution. As a result, you run a PowerShell script to prepare the storage zones controller for use without the Citrix Files control plane. The script does the following:

- Registers the current storage zones controller as a primary storage zones controller. You can later join a secondary storage zones controller to the primary controller.
- Creates a zone and sets the passphrase for it.

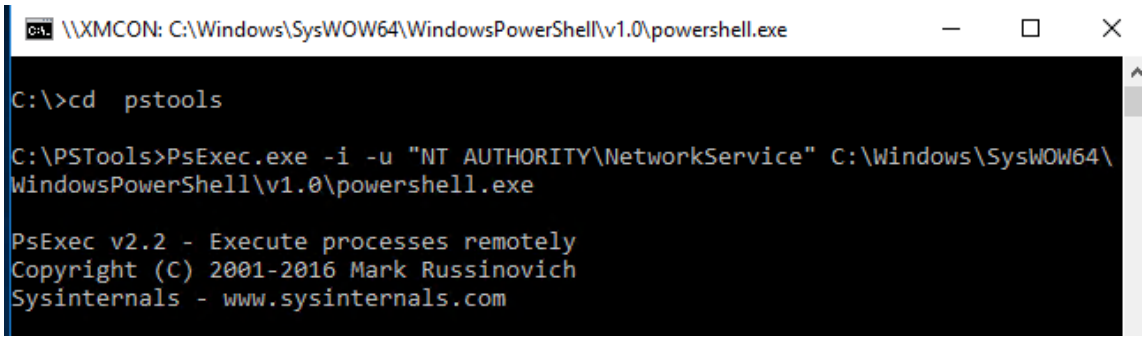
© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. From your storage zones controller server, download the PsExec tool: Navigate to Microsoft Windows Sysinternals and then click **Download PsTools**. Extract the tool to the root of the C drive.



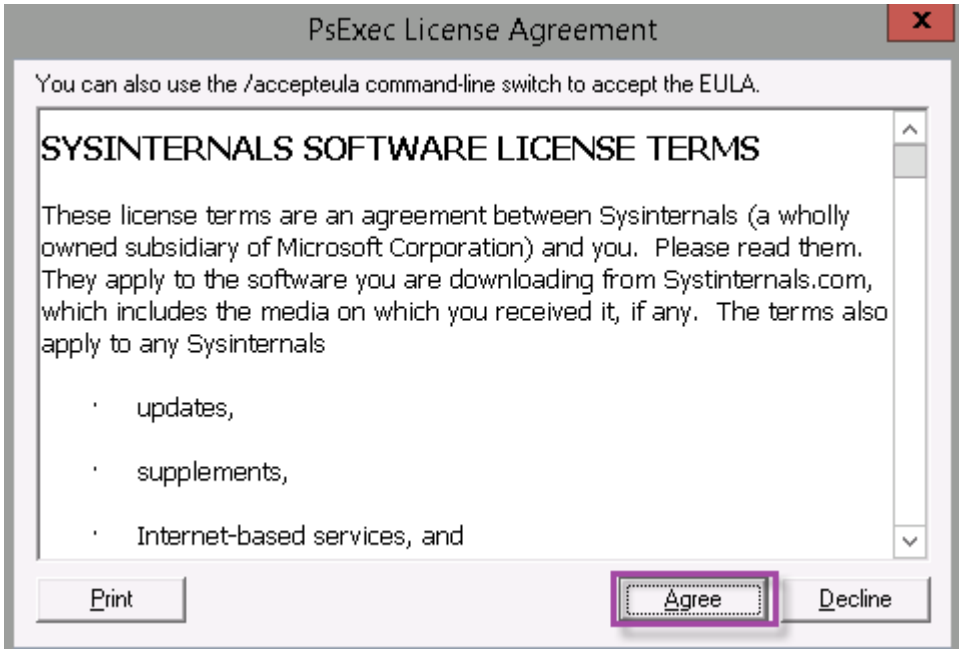
2. Run the PsExec tool: Open the Command Prompt as the Administrator User and then type the following:

```
```
cd c:\pstools
PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
```
```



3. When prompted, click **Agree** to run the Sysinternals tool.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



A PowerShell widow opens.

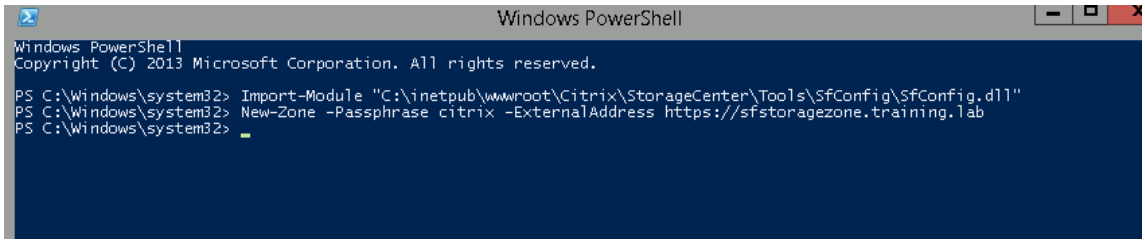
4. In the PowerShell window, type the following:

```
```
Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
    SfConfig\SfConfig.dll"
New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
    com
```
```

Where:

Passphrase: Is the passphrase that you want to assign to the site. Make a note of it. You cannot recover the passphrase from the controller. If you lose the passphrase, you cannot reinstall storage zones, join more storage zones controllers to the storage zone, or recover the storage zone if the server fails.

ExternalAddress: Is the external fully qualified domain name of the storage zones controller server.



Your primary storage zones controller is now ready.

Before you log in to Citrix Endpoint Management to create storage zone connectors: Complete

© 1997–2025 Citrix Systems, Inc. All rights reserved.

the following configuration, if applicable:

Specify a proxy server for storage zones

Configure the domain controller to trust the storage zones controller for delegation

Join a secondary storage zones controller to a storage zone

To create storage zone connectors, see Define storage zones controller connections in Citrix Endpoint Management.

Join a secondary storage zones controller to a storage zone

To configure a storage zone for high availability, connect at least two storage zones controllers to it. To join a secondary storage zones controller to a zone, install a storage zones controller on a second server. Then join that controller to the zone of the primary controller.

1. Open a PowerShell window on the storage zones controller server that you want to join to the primary server.
2. In the PowerShell window, type the following:

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP
   >
   ```

   For example:

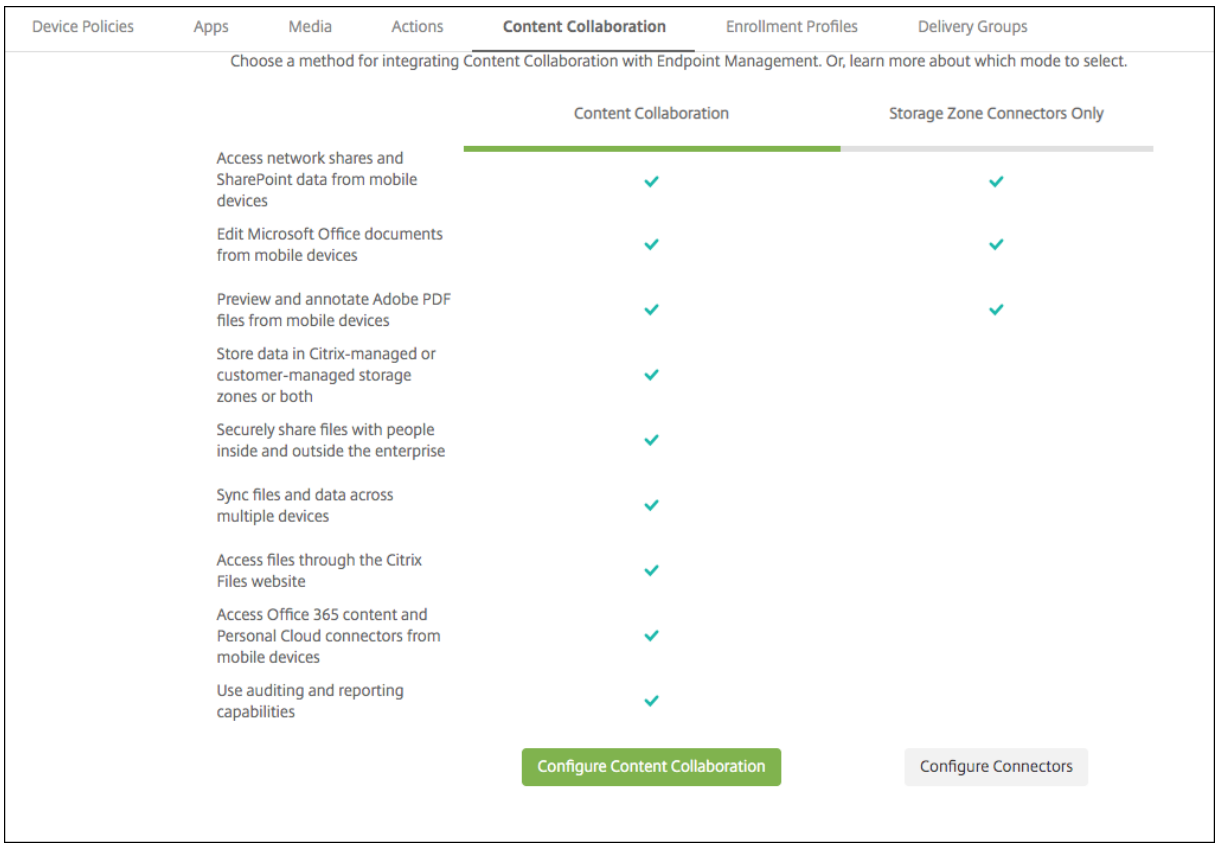
   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

Define storage zones controller connections in Citrix Endpoint Management

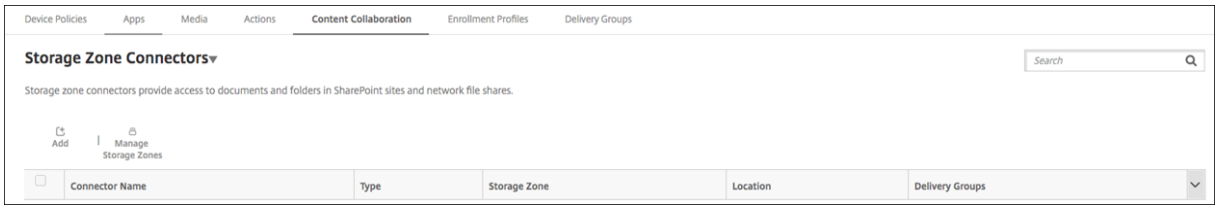
Before you add storage zone connectors, you configure the connection information for each storage zones controller enabled for storage zone connectors. You can define storage zones controllers as described in this section, or when you add a connector.

On your first visit to the **Configure > ShareFile** page, the page summarizes the differences between using Citrix Endpoint Management for Enterprise accounts and storage zone connectors.

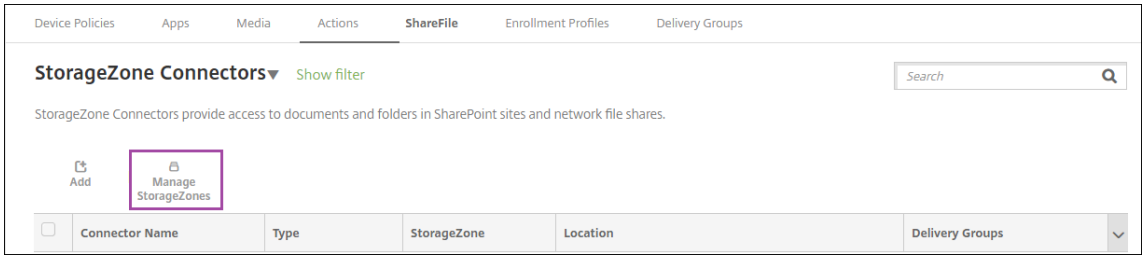
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Click **Configure Connectors** to continue with the configuration steps in this article.

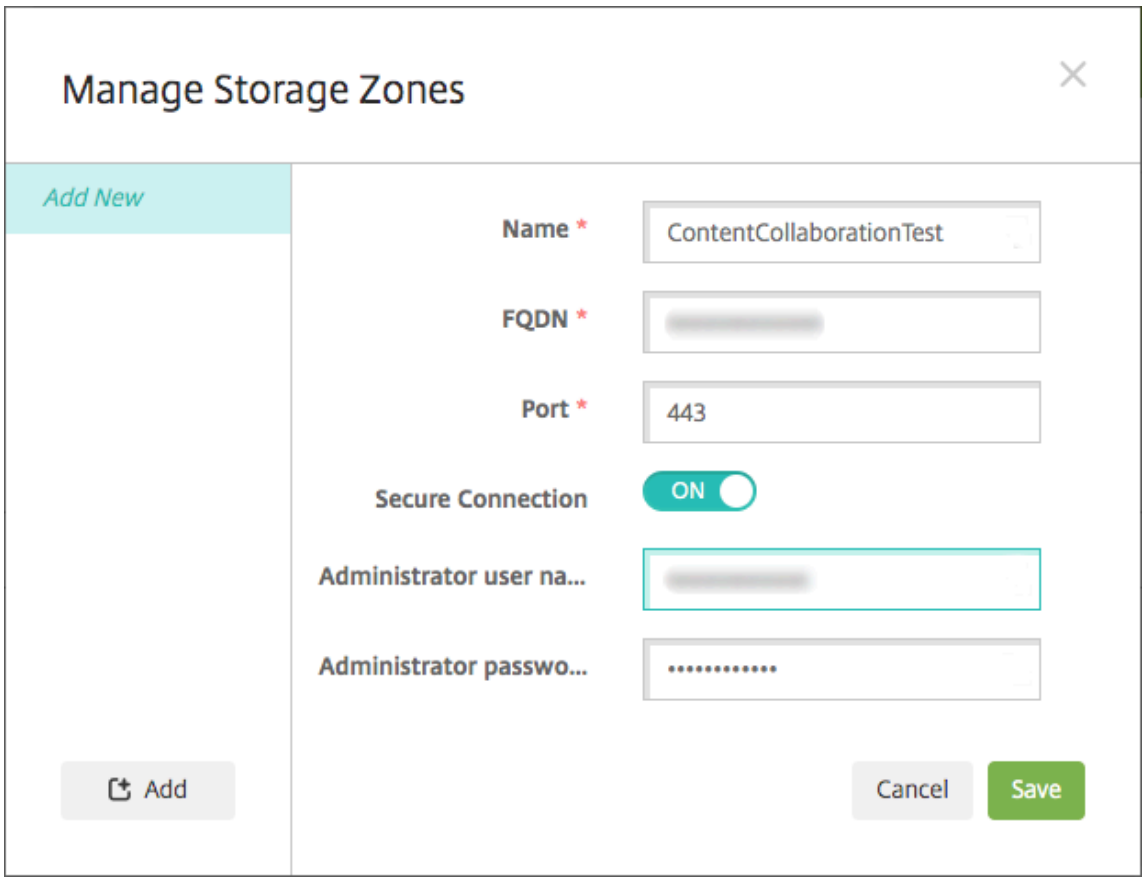


1. In **Configure > ShareFile**, click **Manage Storage Zones**.



2. In **Manage Storage Zones**, add the connection information.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Name:** A descriptive name for the storage zone, used to identify the storage zone in Citrix Endpoint Management. Don't include a space or special characters in the name.
- **FQDN and Port:** The fully qualified domain name and port number for a storage zones controller that is reachable from the Citrix Endpoint Management server.
- **Secure Connection:** If you use SSL for connections to the storage zones controller, use the default setting, On. If you don't use SSL for connections, change this setting to Off.
- **Administrator user name** and **Administrator password:** An administrator service account user name (in the form domain\admin) and password. Else, a user account with read and write permissions on the storage zones controllers.

3. Click **Save**.
4. To test the connection, verify that the Citrix Endpoint Management server can reach the fully qualified domain name of the storage zones controller on port 443.
5. To define another storage zones controller connection, click the **Add** button in **Manage Storage Zones**.

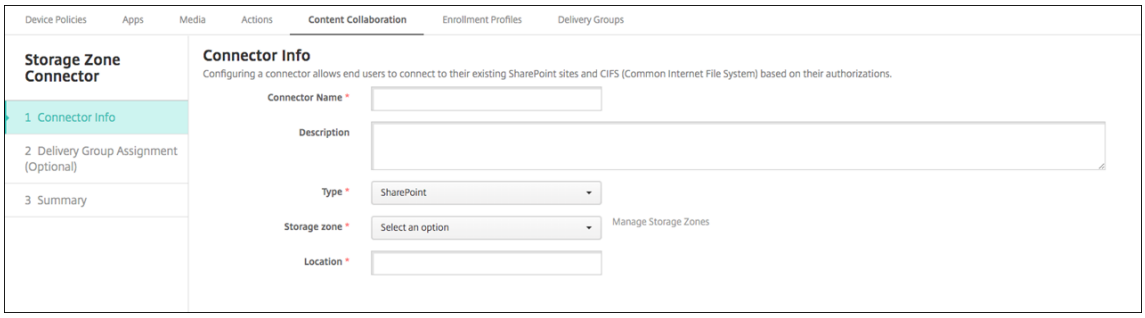
   To edit or delete the information for a storage zones controller connection, select the connection name in **Manage Storage Zones**. Then, click **Edit** or **Delete**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Add a storage zone connector in Citrix Endpoint Management

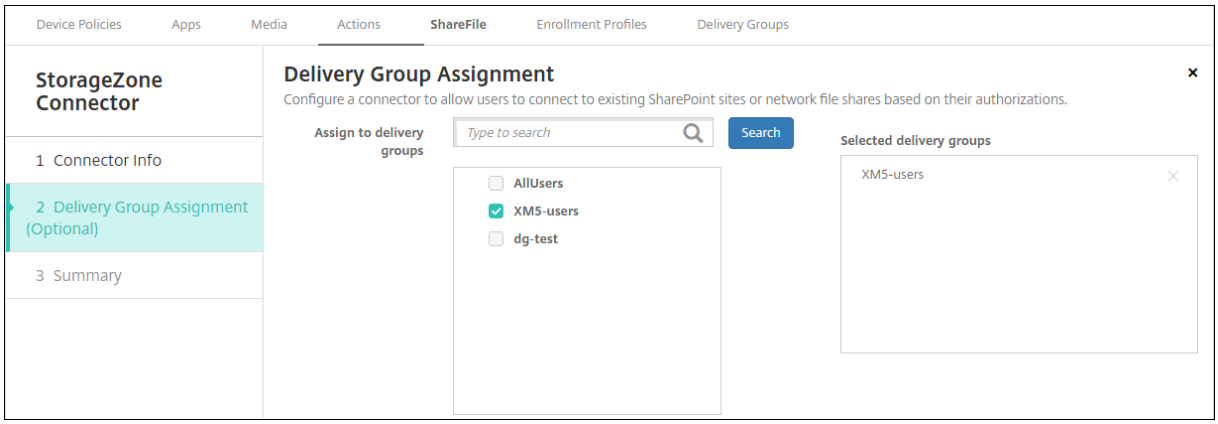
1. Go to **Configure > ShareFile** and then click **Add**.

2. On the **Connector Info** page, configure these settings:



   - **Connector Name:** A name that identifies the storage zone connector in Citrix Endpoint Management.
   - **Description:** Optional notes about this Connector.
   - **Type:** Choose either **SharePoint** or **Network**.
   - **Storage zone:** Choose the storage zone associated with the connector. If the storage zone isn't listed, click **Manage Storage Zones** to define the storage zones controller.
   - **Location:** For SharePoint, specify the URL of the SharePoint root-level site, site collection, or document library, in the form `https://sharepoint.company.com`. For a network share, specify the fully qualified domain name of the Uniform Naming Convention (UNC) path, in the form \\server\share.

3. On the **Delivery Group Assignment** page, optionally assign the Connector to delivery groups. Else, you can associate connectors to delivery groups using **Configure > Delivery Groups**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. On the **Summary** page, you can review the options you configured. To adjust the configuration, click **Back**.
2. Click **Save** to save the connector.
3. Test the connector:

    a) When you wrap the Citrix Files clients, set the Network access policy to **Tunneled - Web SSO**.

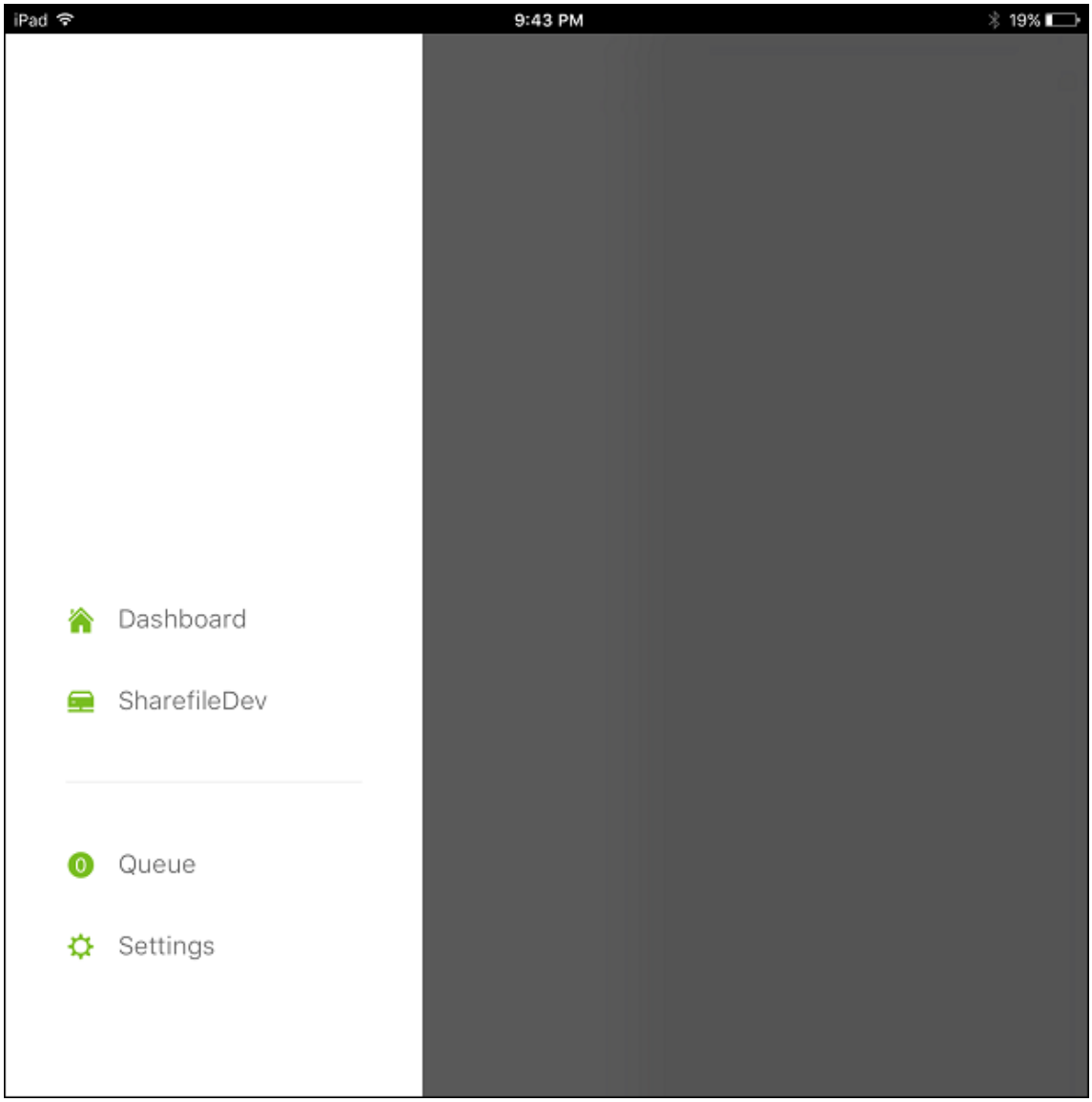
    In this mode of tunneling, the MDX framework terminates SSL/HTTP traffic from an MDX app. MDX then starts new connections to internal connections for the user. This policy setting enables the MDX framework to detect and respond to authentication challenges issued by web servers.

    b) Add the Citrix Files clients to Citrix Endpoint Management. For details, see To add Citrix Files clients to Citrix Endpoint Management.

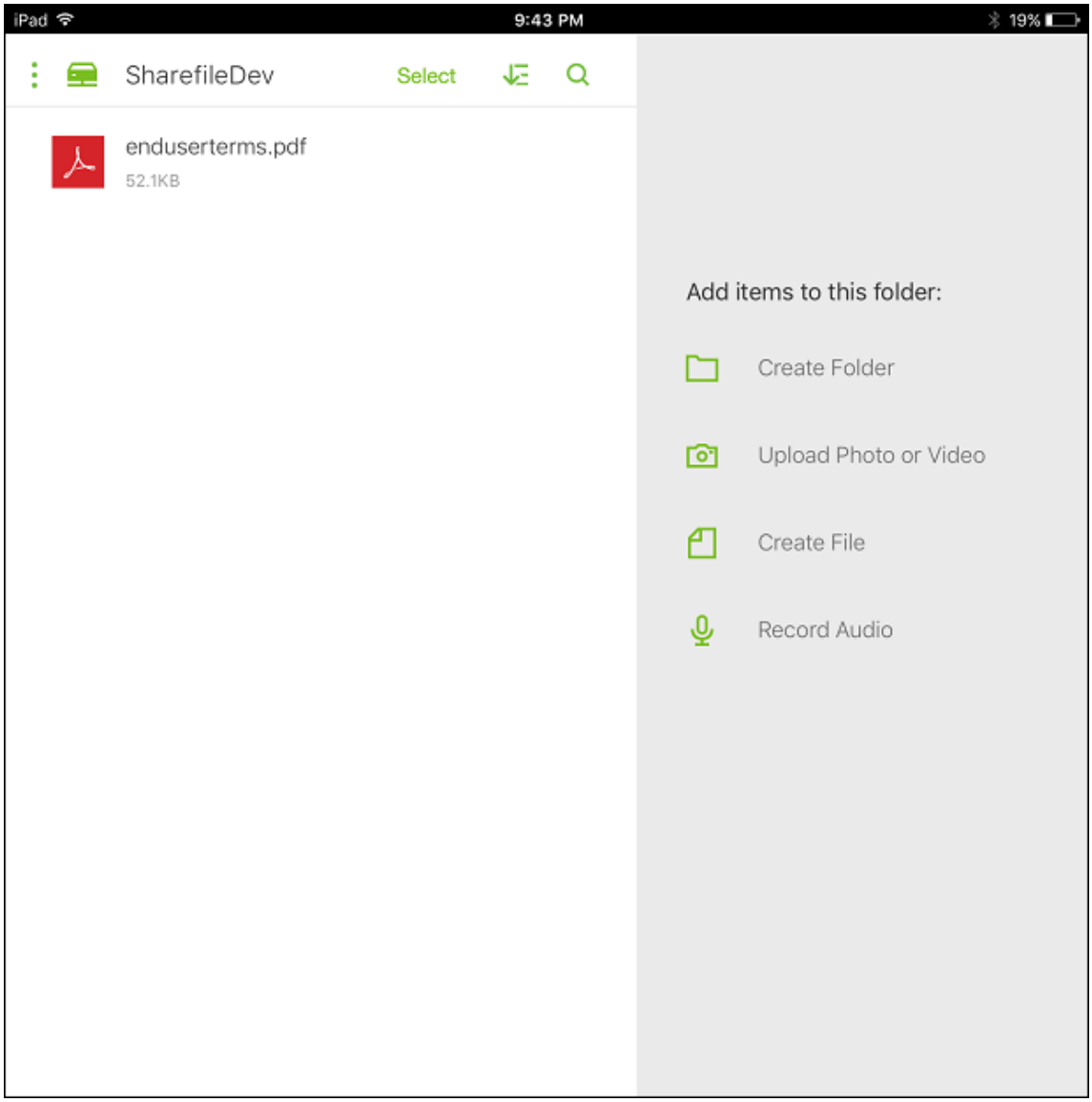
    c) From a supported device, verify single sign-on to Citrix Files and connectors.

In the following samples, SharefileDev is the name of a connector.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

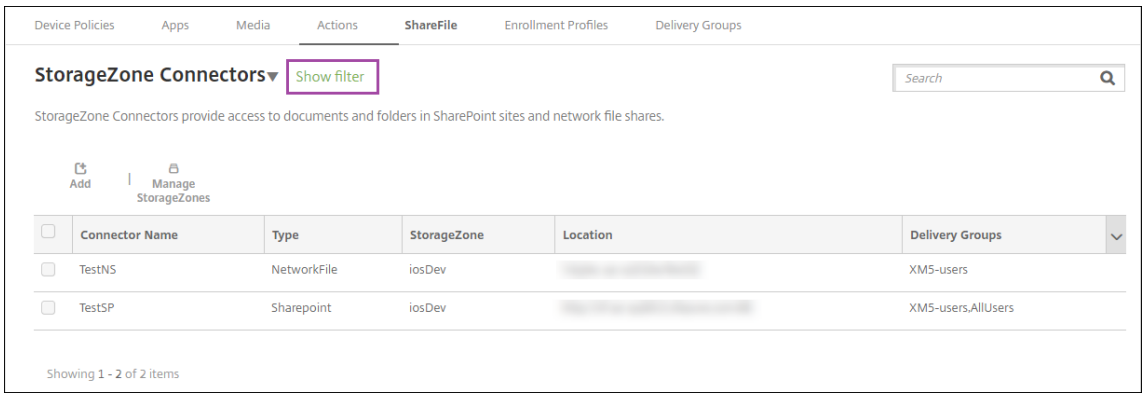


Filter the storage zone connectors list

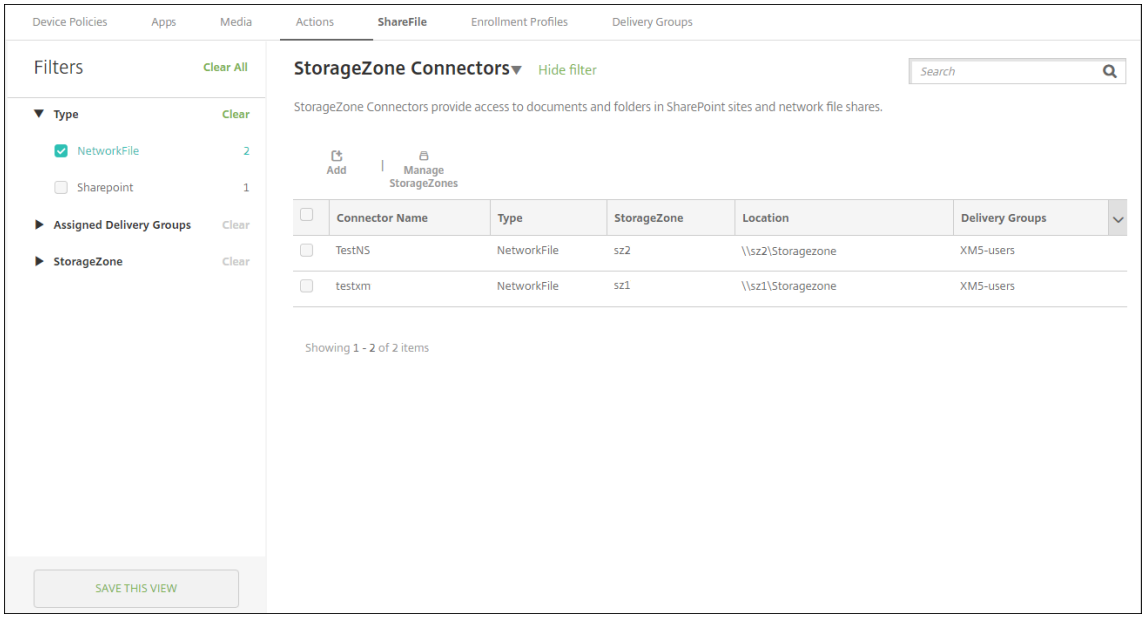
You can filter the list of storage zone connectors by connector type, assigned delivery groups, and storage zone.

1. Go to **Configure > ShareFile** and then click **Show filter**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

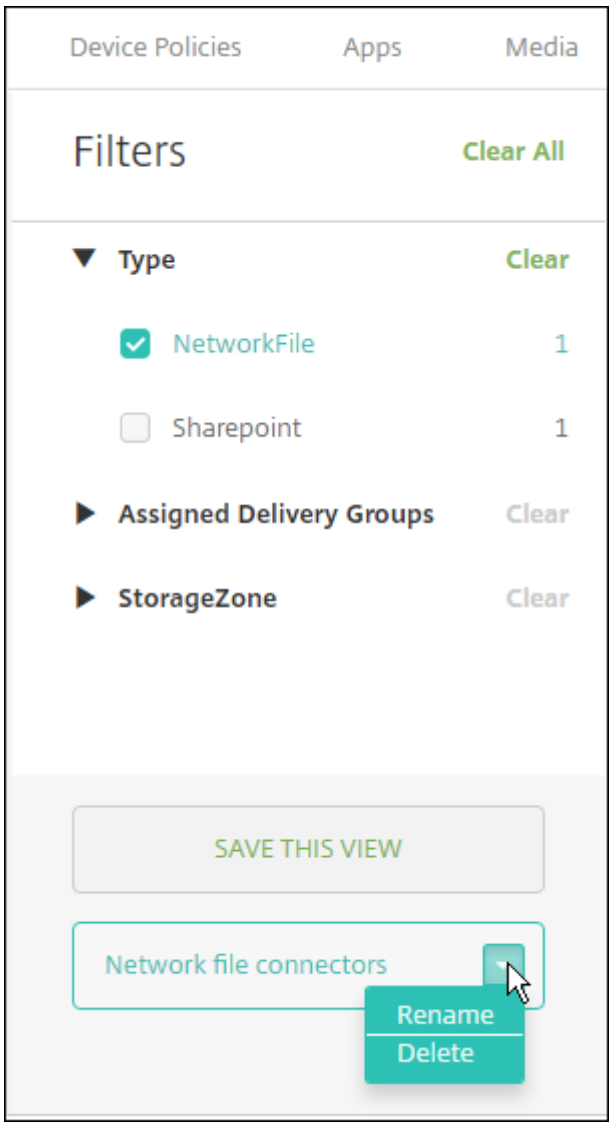


2. Expand the filter headings to make selections. To save a filter, click **Save This View**, type the filter name, and click **Save**.



3. To rename or delete a filter, click the arrow icon beside the filter name.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

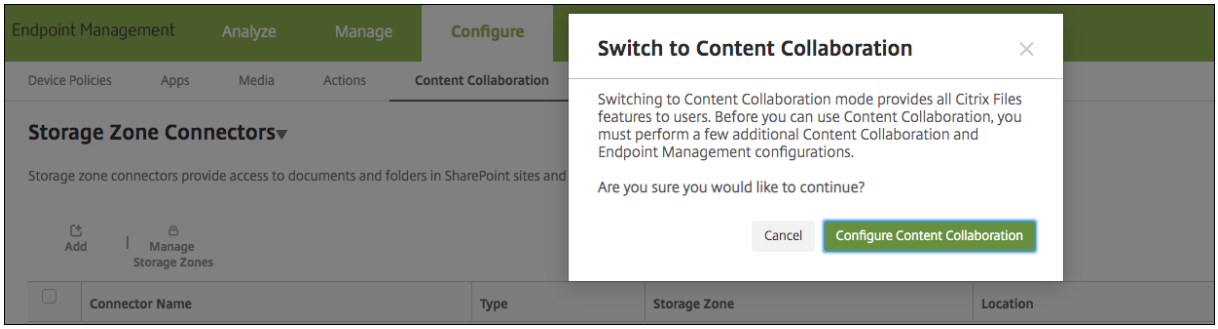


Switch to Enterprise account

After integrating storage zone connectors with Citrix Endpoint Management, you can later switch to the full Enterprise feature set. Citrix Endpoint Management keeps your existing storage zone connector integration settings.

Go to **Configure > ShareFile**, click the **Storage Zone Connectors** drop-down menu, and then click **Configure ShareFile**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



For information about configuring Enterprise accounts, see SAML for single sign-on with Citrix Files.

SmartAccess for HDX™ apps

September 6, 2025

This feature allows you to control access to HDX apps based on device properties, user properties of a device, or applications installed on a device. You use this feature by setting automated actions to mark the device as out of compliance to deny that device access. HDX apps used with this feature are configured in Citrix Virtual Apps and Desktops by using a SmartAccess policy that denies access to out-of-compliance devices. Citrix Endpoint Management communicates the status of the device to StoreFront using a signed, encrypted tag. StoreFront then allows or denies access based on the access control policy of the app.

To use this feature, your deployment requires:

- Citrix Virtual Apps and Desktops™
- Citrix Endpoint Management
- Citrix Endpoint Management configured with a SAML certificate to be used for signing and encrypting tags. The same certificate without private key is uploaded on the StoreFront server.

To start using this feature:

- Configure the Citrix Endpoint Management server certificate to the StoreFront store
- Configure at least one Citrix Virtual Apps™ and Desktops delivery group with the required SmartAccess policy
- Set the automated action in Citrix Endpoint Management

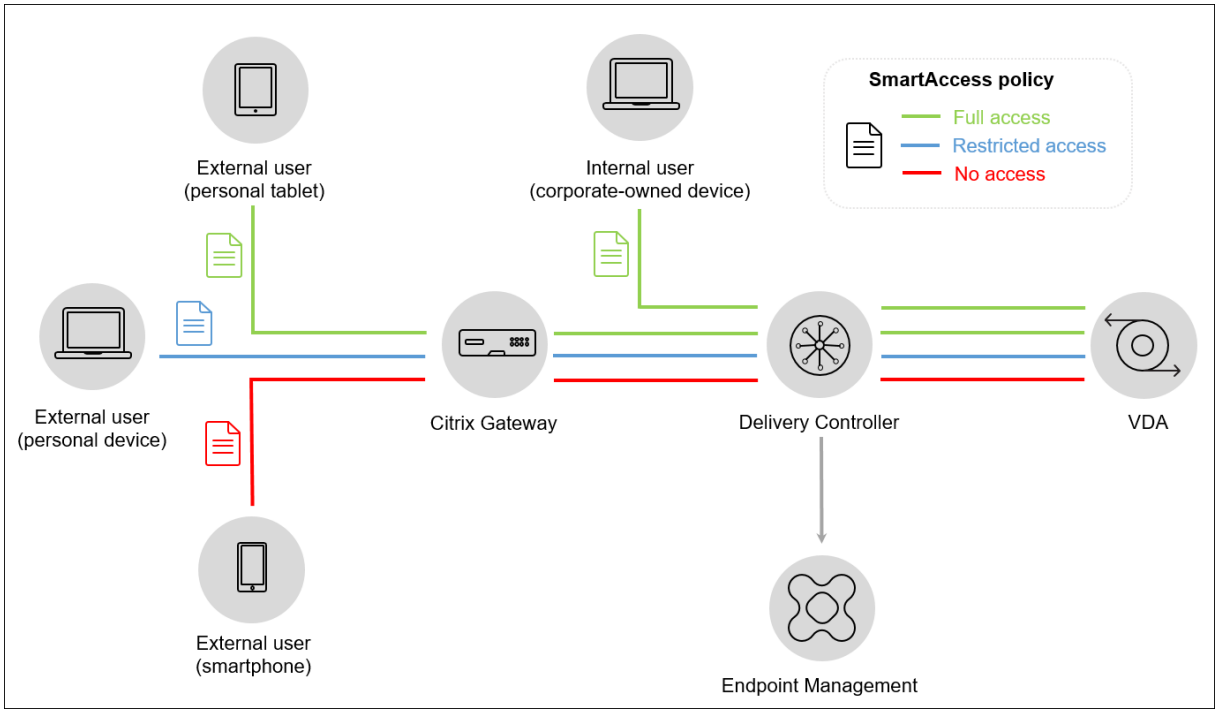
SmartAccess to HDX apps for endpoints

With this feature, you can apply policy-based access control to restrict device access to HDX apps. You can apply these access levels to HDX apps:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Full access**. A device can access all HDX apps that the Citrix Secure Hub store provides.
- **Restricted access**. A device can access one or more but not all HDX apps.
- **No access**. A device cannot access any HDX apps.

The following graphic illustrates how access control works. An attempt to launch an HDX app in Citrix Secure Hub triggers a request to a Delivery Controller. The Delivery Controller then forwards the request to the Citrix Endpoint Management server for validation. The result of the validation determines the level of access the device has. For example, access to an HDX app is denied if the device is jailbroken.



Export and configure the Citrix Endpoint Management server certificate and upload it to the StoreFront store

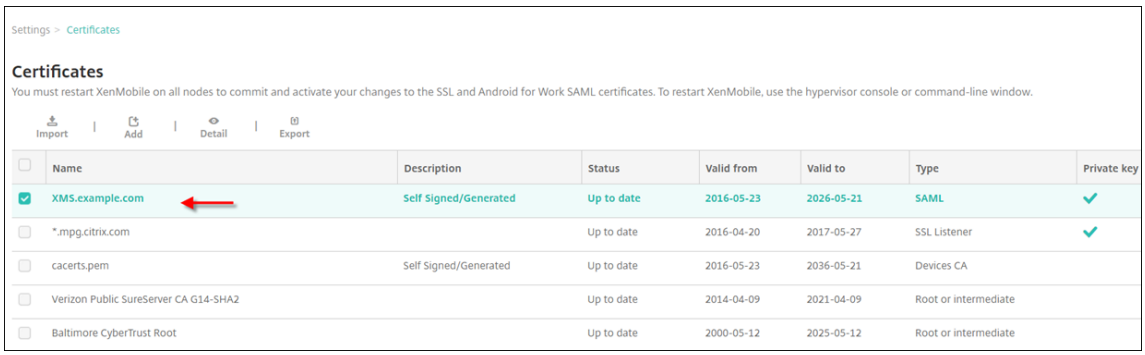
SmartAccess uses signed and encrypted tags to communicate between the Citrix Endpoint Management and StoreFront servers. To enable that communication, you add the Citrix Endpoint Management server certificate to the StoreFront store.

For more information about integrating StoreFront and Citrix Endpoint Management when Citrix Endpoint Management is enabled with domain and certificate-based authentication, see the Support Knowledge Center.

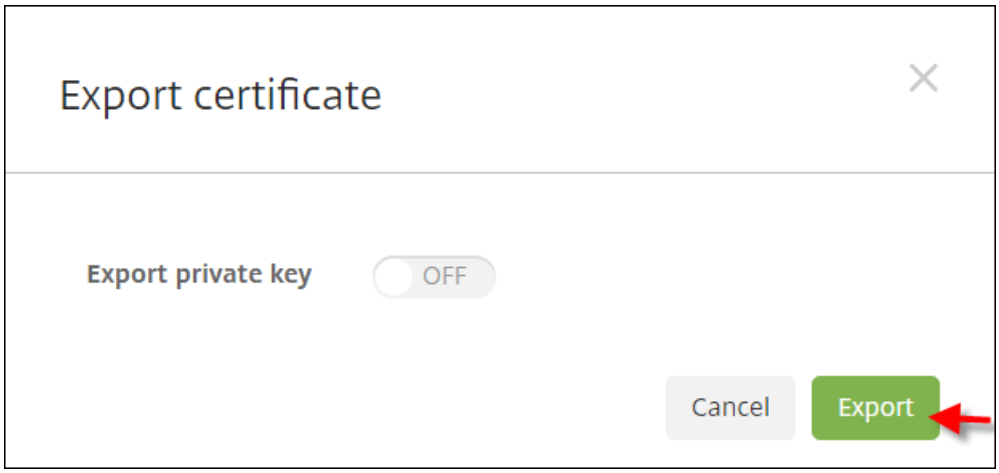
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Export the SAML certificate from Citrix Endpoint Management

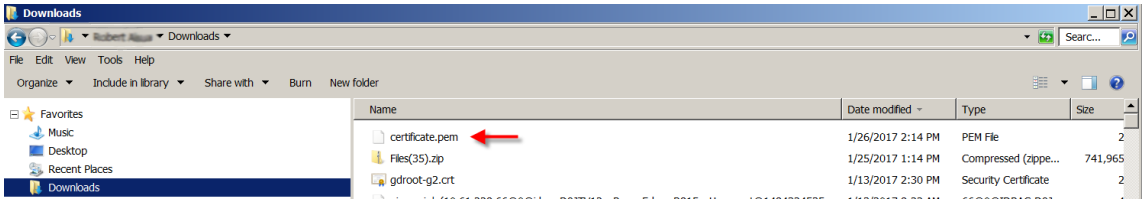
1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears. Click **Certificates**.
2. Locate the SAML certificate for the Citrix Endpoint Management server.



3. Make sure that **Export private key** is set to **Off**. Click **Export** to export the certificate to your download directory.



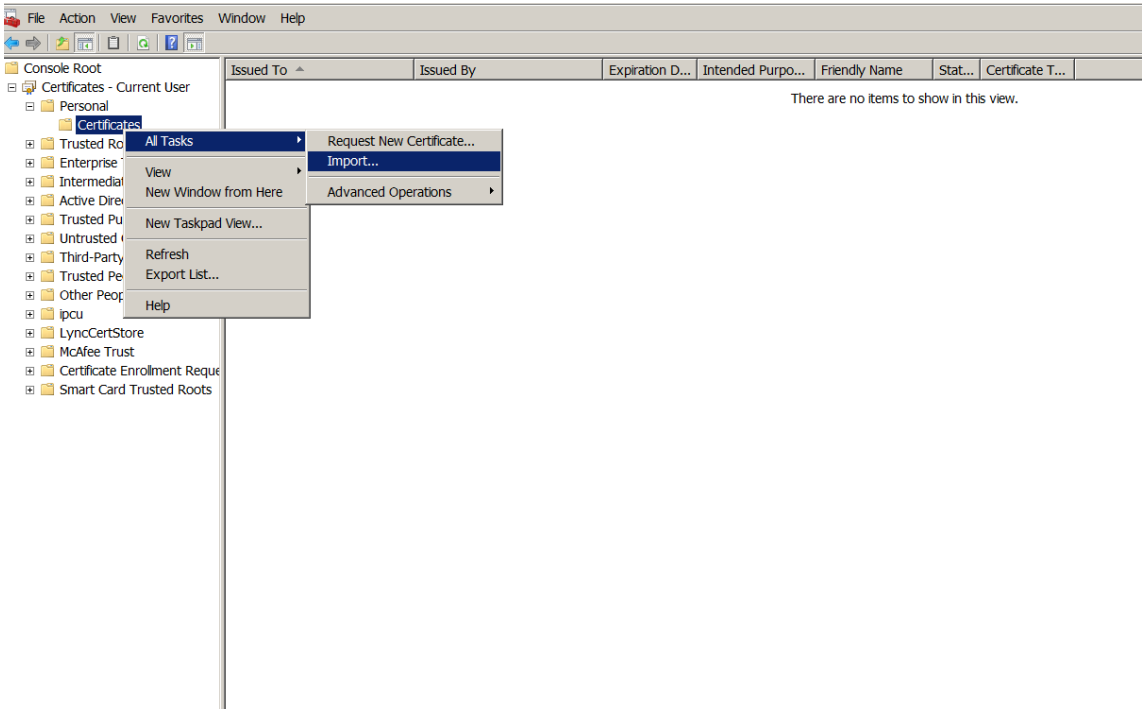
4. Locate the certificate in your download directory. The certificate is in PEM format.



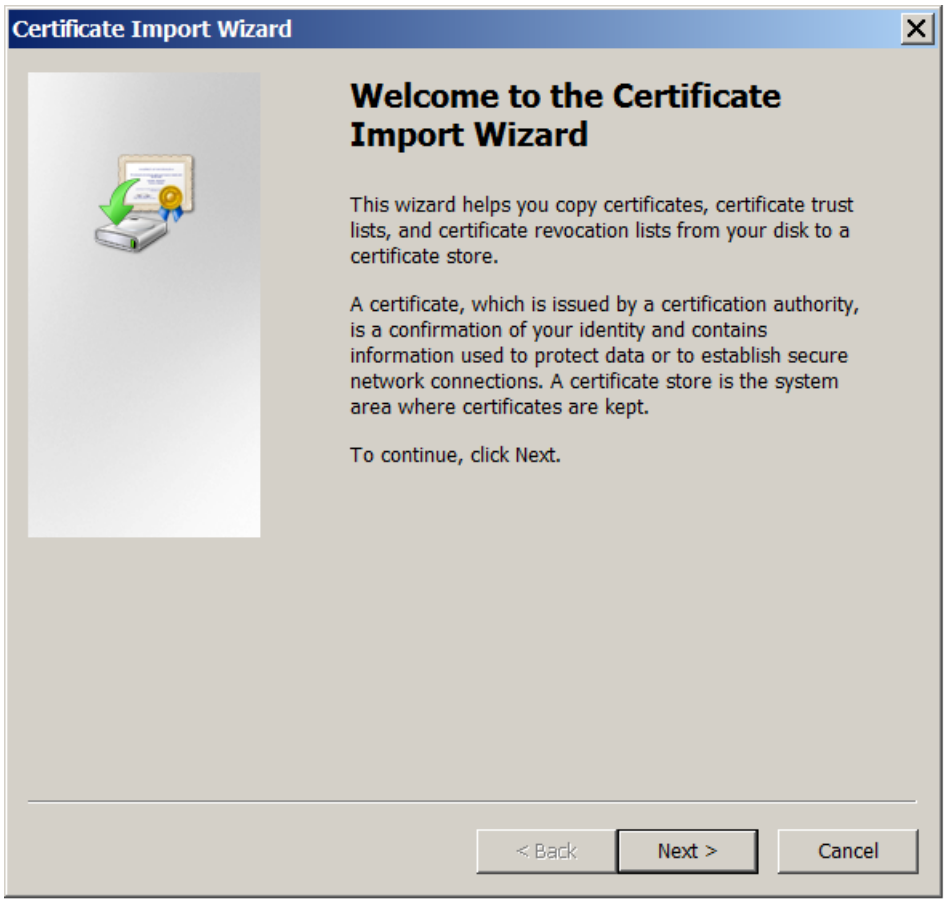
Convert the certificate from PEM to CER

1. Open the Microsoft Management Console (MMC) and right-click **Certificates > All Tasks > Import**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

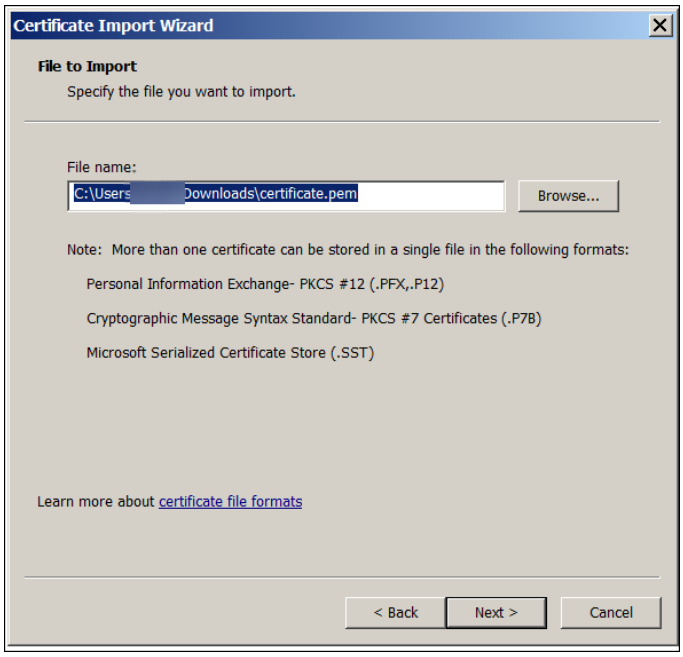


2. When the certificate import wizard appears, click **Next**.

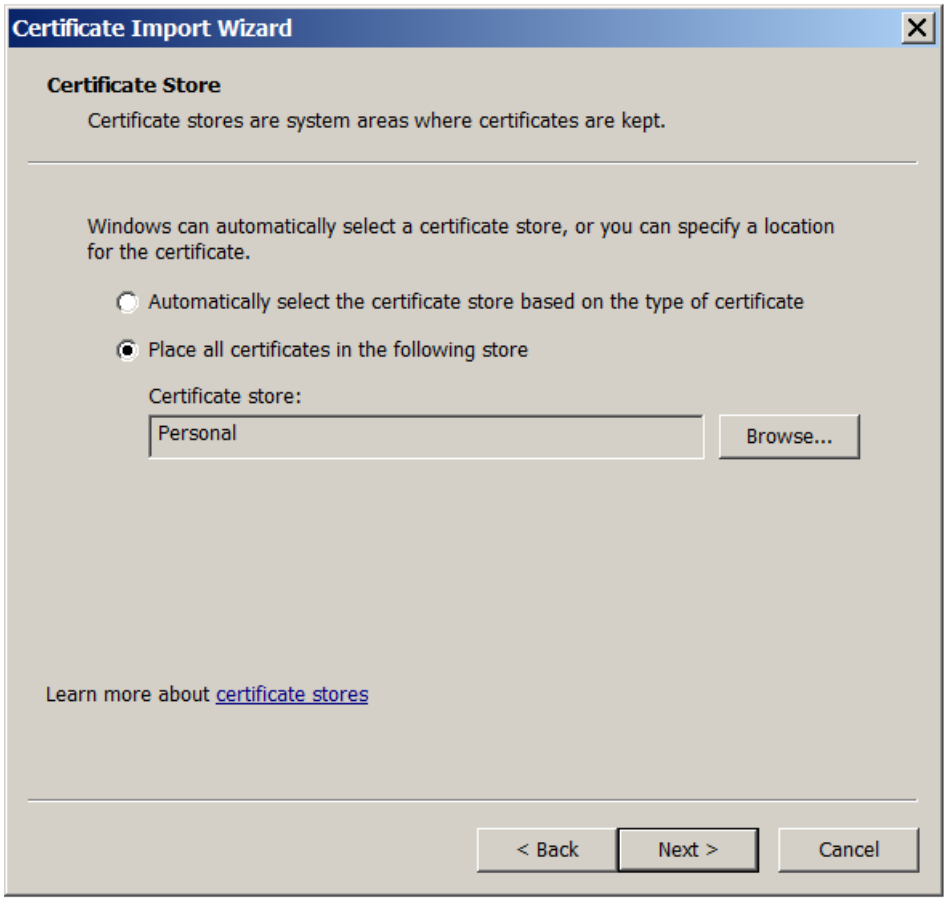


© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. Browse to the certificate in the download directory.

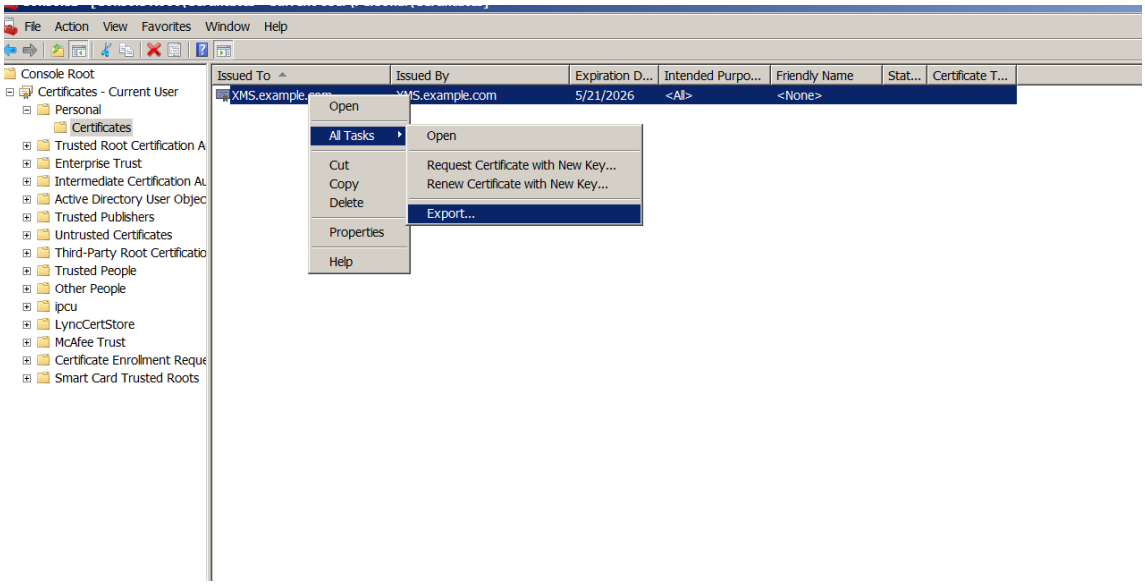


4. Select **Place all certificates in the following store** and select **Personal** as the certificate store. Click **Next**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

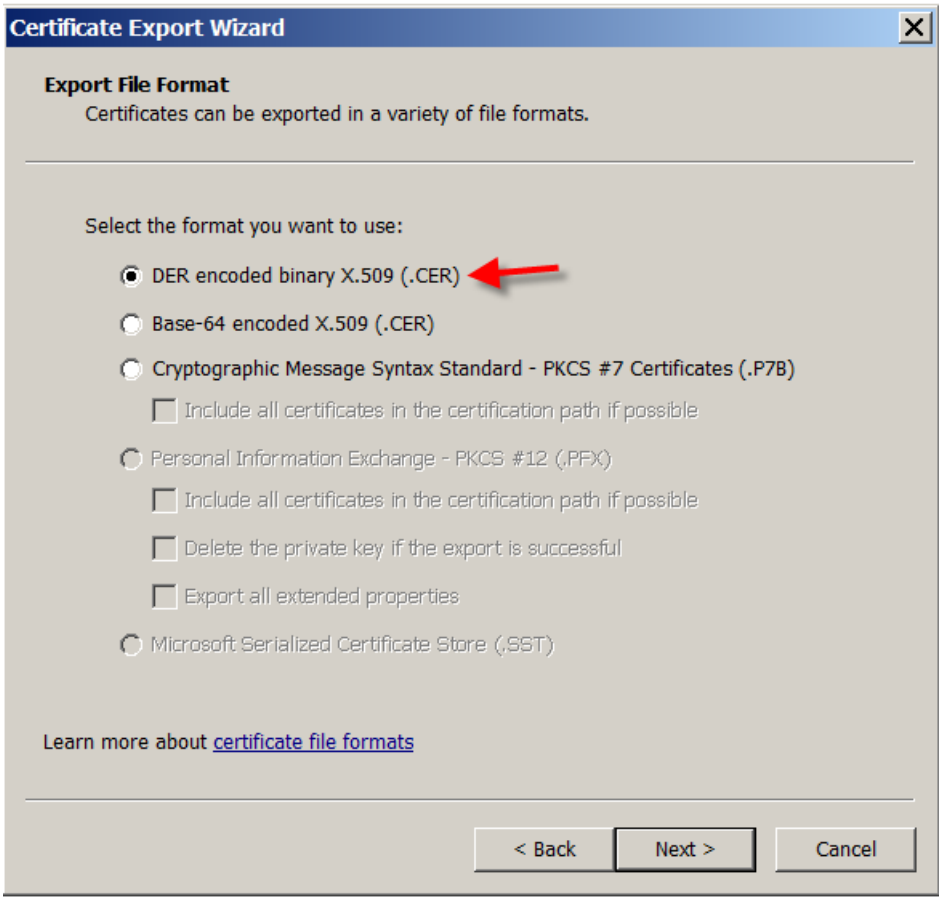
5. Review your selections and click **Finish**. Click **OK** to dismiss the confirmation window.
6. In the MMC, right-click the certificate and then choose **All Tasks > Export**.



7. When the certificate export wizard appears, click **Next**.

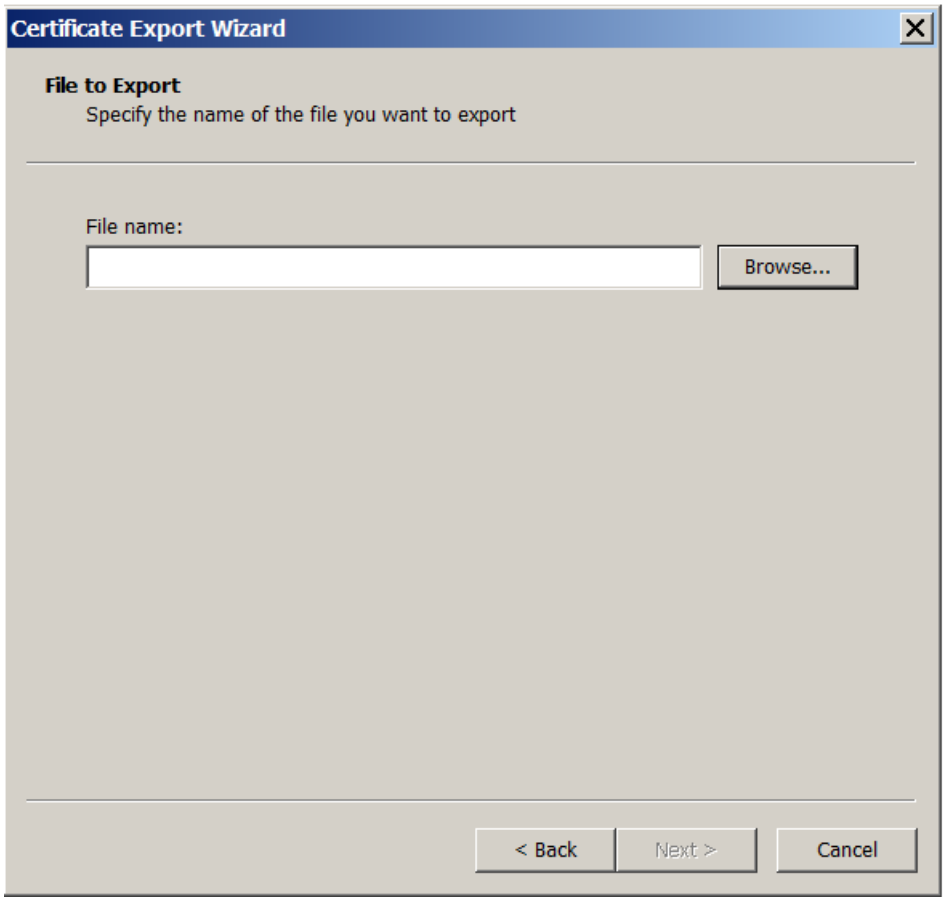
© 1997–2025 Citrix Systems, Inc. All rights reserved.

8. Choose the format **DER encoded binary X.509 (.CER)**. Click **Next**.

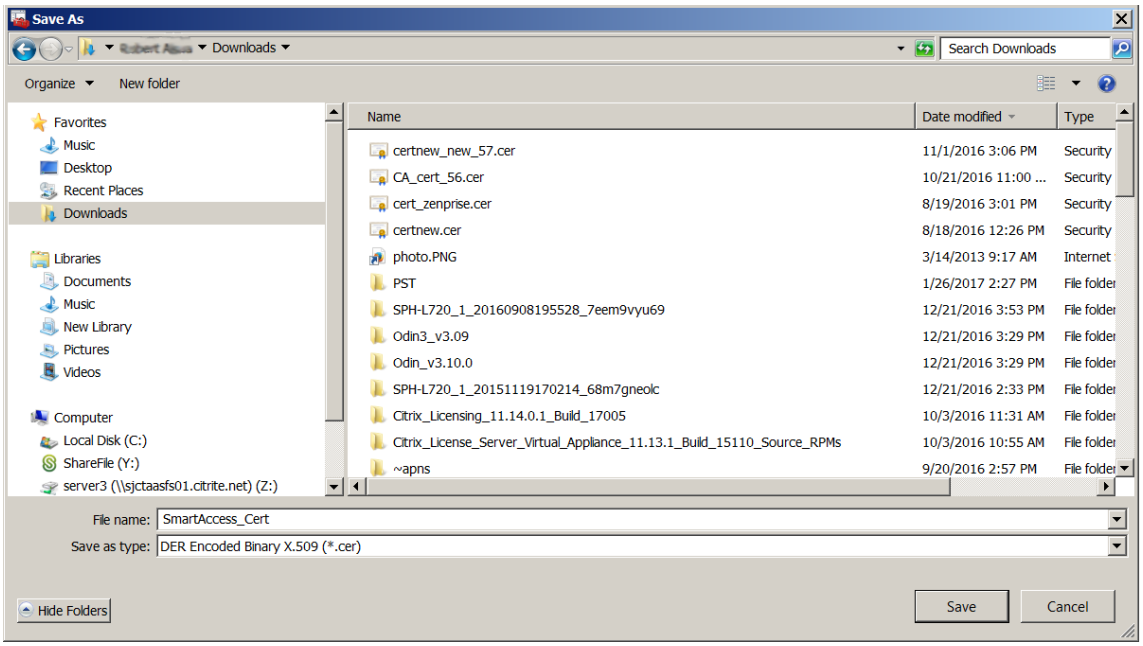


9. Browse to the certificate. Type a name for the certificate and then click **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

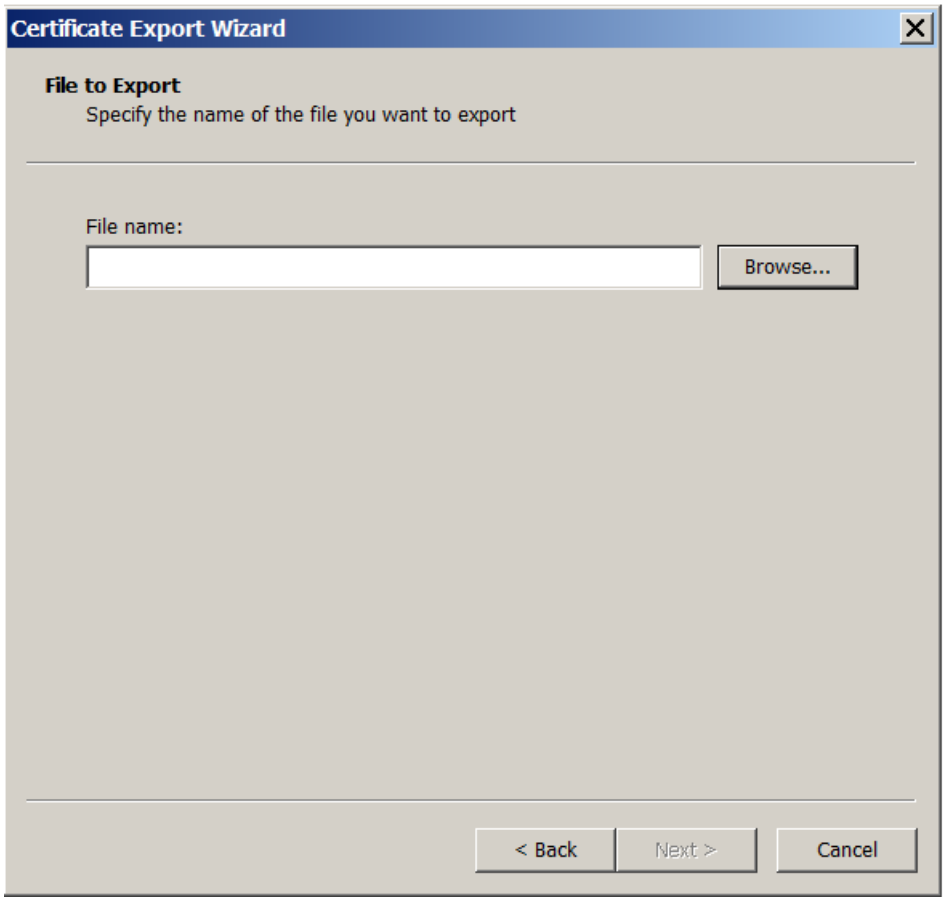


10. Save the certificate.



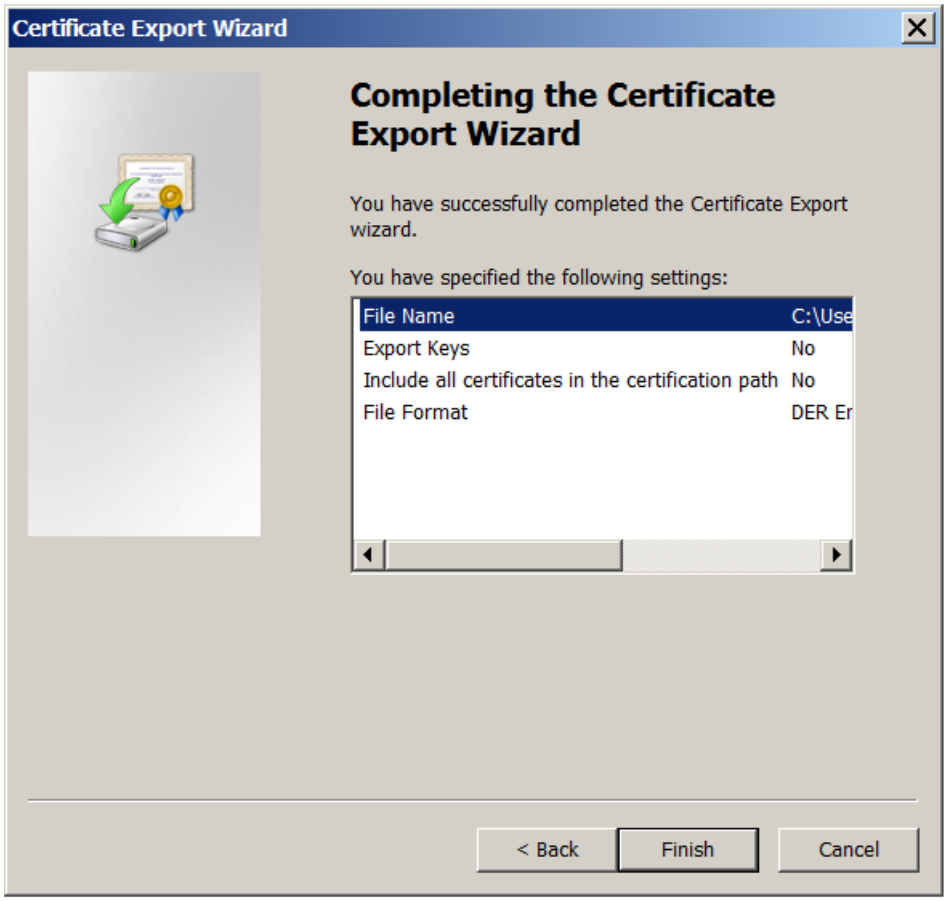
11. Browse to the certificate and click **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

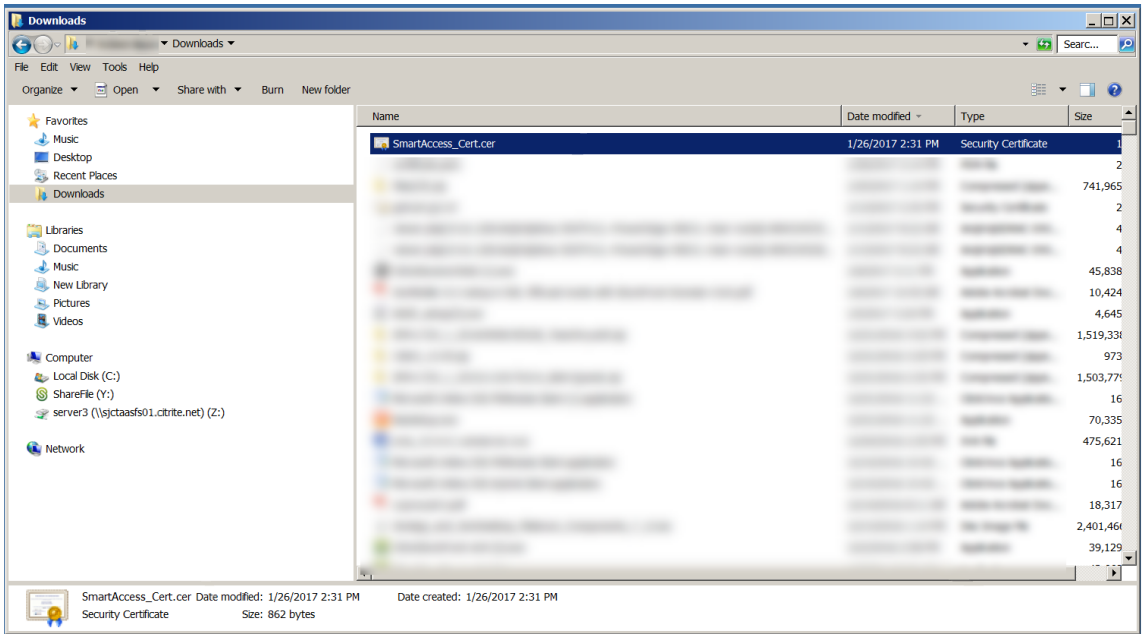


12. Review your selections and click **Finish**. Click **OK** to dismiss the confirmation window.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



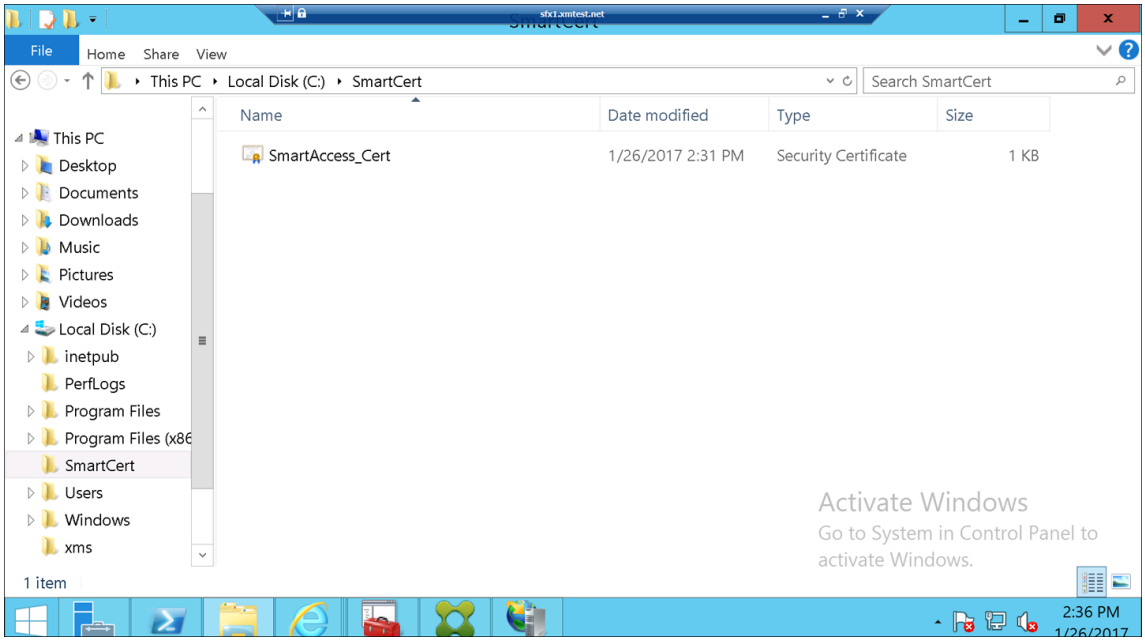
13. Locate the certificate in your download directory. The certificate is in CER format.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Copy the certificate to the StoreFront Server

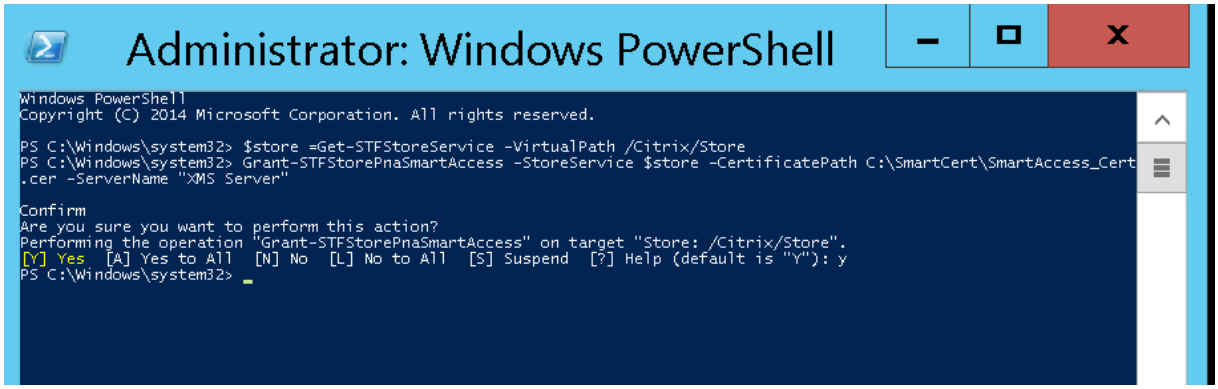
1. On the StoreFront server, create a folder called **SmartCert**.
2. Copy the certificate to the **SmartCert** folder.



Configure the certificate on the StoreFront store

On the StoreFront server, run this PowerShell command to configure the converted Citrix Endpoint Management server certificate on the store:

```
Grant-STFStorePnaSmartAccess –StoreService $store –
    CertificatePath “C:\xms\xms.cer” –ServerName “XMS server”
```



If there are any existing certificates on the StoreFront store, run this PowerShell command to revoke them:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
Revoke-STFStorePnaSmartAccess –StoreService $store –All
```

Else, you can run any of these PowerShell commands on the StoreFront server to revoke existing certificates on the StoreFront store:

- Revoke by name:

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store

Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “
    My XM Server"
```

- Revoke by thumbprint:

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store

Revoke-STFStorePnaSmartAccess –StoreService $store –
    CertificateThumbprint "[Thumbprint]
```

- Revoke by server object:

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store

$access = Get-STFStorePnaSmartAccess –StoreService $store

Revoke-STFStorePnaSmartAccess –StoreService $store –SmartAccess
    $access.AccessConditionsTrusts[0]
```

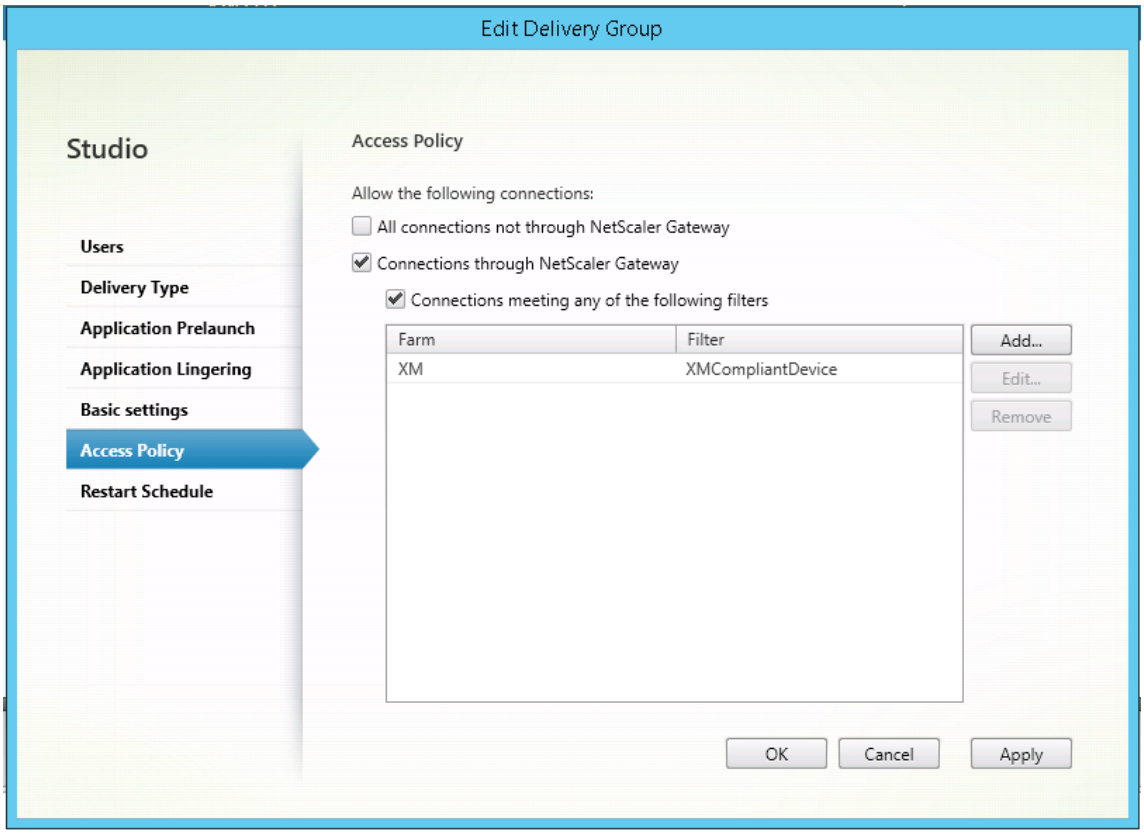
Configure the SmartAccess policy for Citrix Virtual Apps and Desktops

To add the required SmartAccess policy to the delivery group delivering the HDX app:

1. Open Citrix Studio from the Citrix Cloud console.
2. Select **Delivery Groups** in the Studio navigation pane.
3. Select a group delivering the apps that you want to control access to. Then select **Edit Delivery Group** in the **Actions** pane.
4. On the **Access Policy** page, select **Connections through NetScaler Gateway** and **Connection meeting any of the following**.
5. Click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

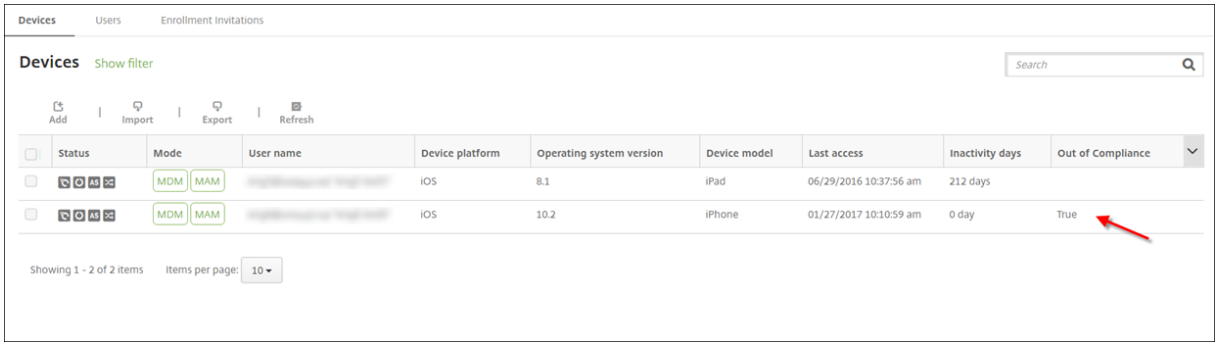
6. Add an access policy where **Farm** is **XM** and **Filter** is **XMCompliantDevice**.



7. Click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

Set automated actions in Citrix Endpoint Management

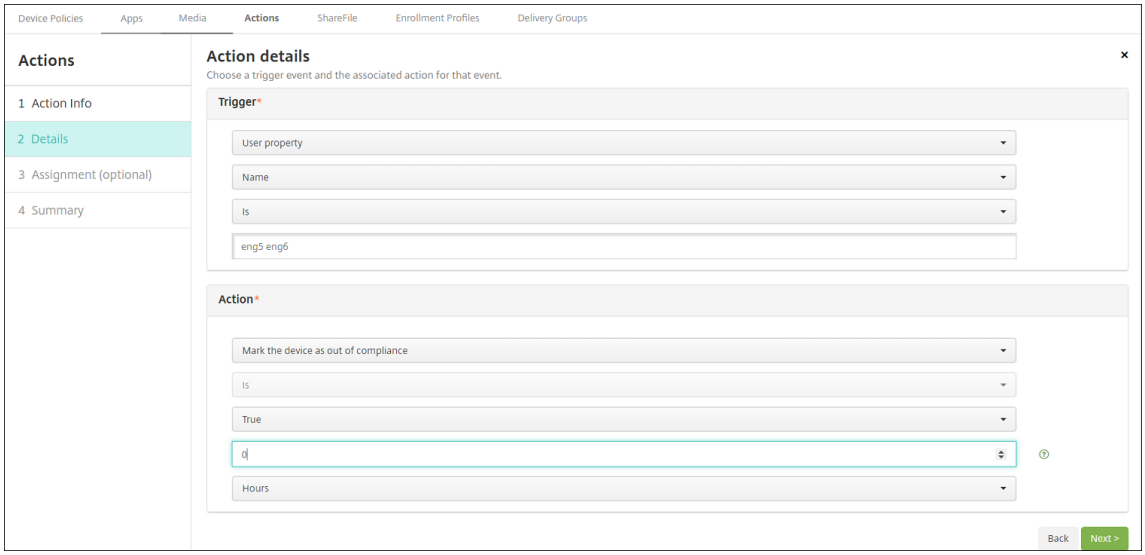
The SmartAccess policy that you set in the delivery group for an HDX app denies access to a device when the device in out of compliance. Use automated actions to mark the device as out of compliance.



1. From the Citrix Endpoint Management console, click **Configure > Actions**. The **Actions** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Click **Add** to add an action. The **Action Information** page appears.
3. On the **Action Information** page, type a name and description for the action.
4. Click **Next**. The **Action details** page appears. In the following example, a trigger is created that immediately marks devices as out of compliance if they have the user property name **eng5** or **eng6**.



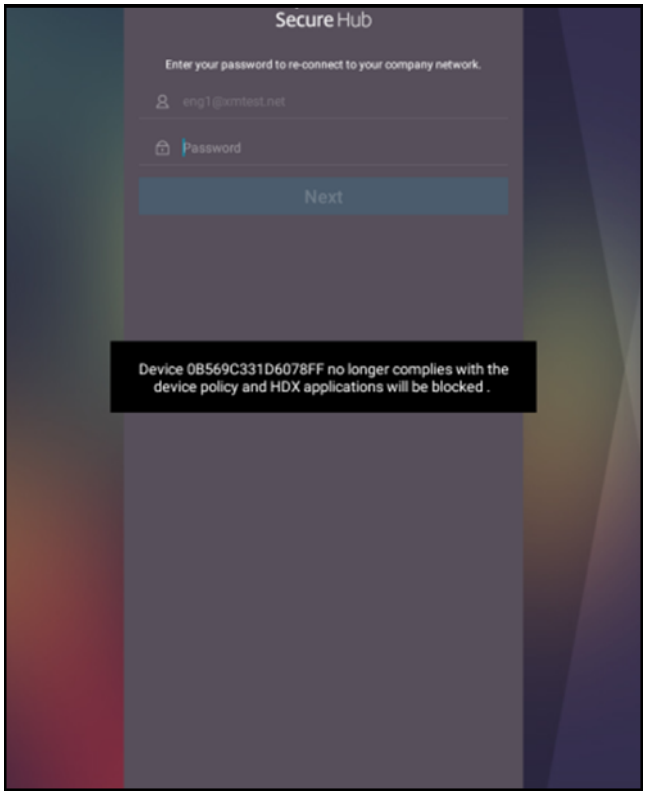
5. In the **Trigger** list, choose **Device property**, **User property**, or **Installed app name**. SmartAccess doesn't support event triggers.
6. In the **Action** list:
   - Choose **Mark the device as out of compliance**.
   - Choose **Is**.
   - Choose **True**.
   - To set the action to mark the device as out of compliance immediately when the trigger condition is met, set the time frame to **0**.
7. Choose the Citrix Endpoint Management delivery group or groups to apply this action to.
8. Review the summary of the action.
9. Click **Next** and then click **Save**.

When the device is marked out of compliance, the HDX apps no longer appear in the Citrix Secure Hub store. The user is no longer subscribed to the app. No notification is sent to the device and nothing in the Citrix Secure Hub store indicates that the HDX apps were previously available.

If you want users to be notified when a device is marked out of compliance, create a notification and then create an automated action to send that notification.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

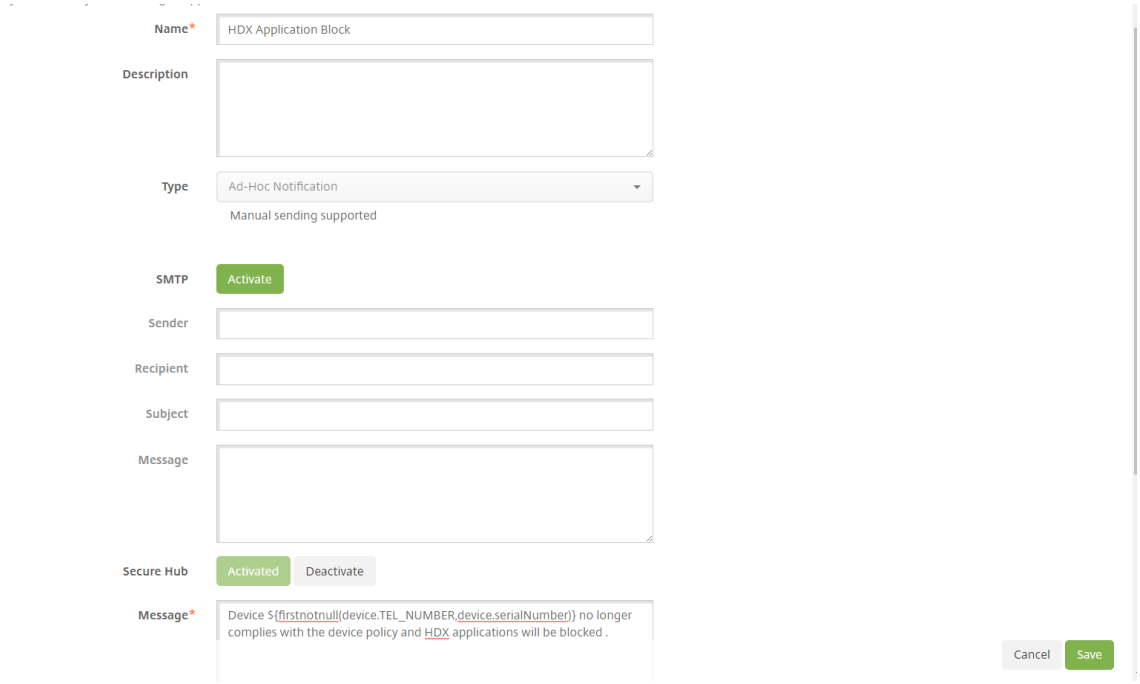
This example creates and sends this notification when a device is marked out of compliance: "Device serial number or telephone number no longer follows the device policy and HDX applications are blocked."



Create the notification users see when a device is marked as out of compliance

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
2. Click **Notification Templates**. The **Notification Templates** page appears.
3. Click **Add** to add on the **Notification Templates** page.
4. Configure these settings:
   - **Name:** HDX Application Block
   - **Description:** Agent notification when a device is out of compliance
   - **Type:** Ad Hoc Notification
   - **Citrix Secure Hub:** Activated
   - **Message:** Device `${ firstnotnull(device.TEL_NUMBER,device.serialNumber ) }` no longer follows the device policy and HDX applications are blocked.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

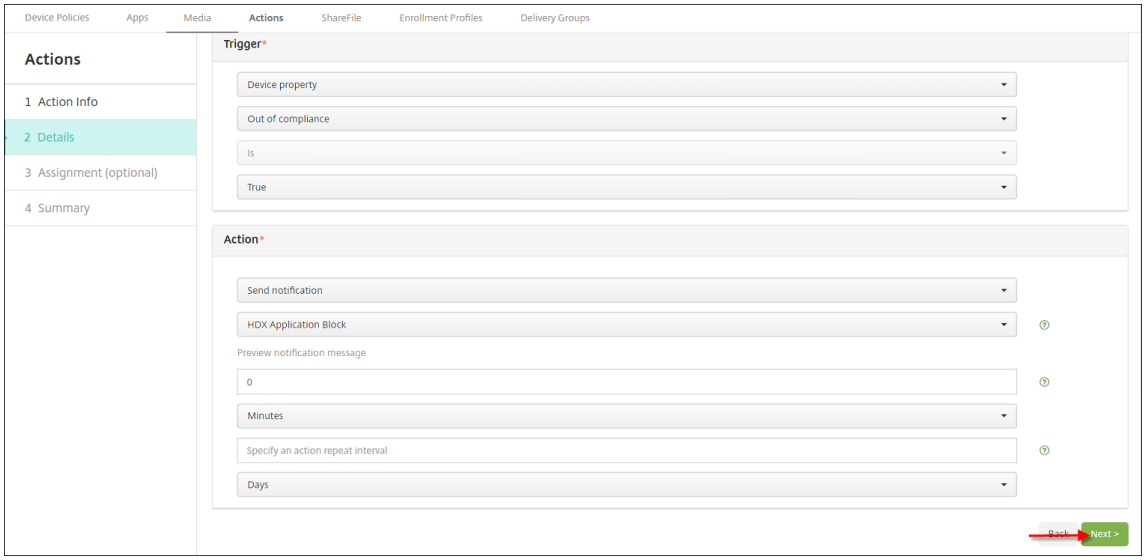


5. Click **Save**.

Create the action that sends the notification when a device is marked out of compliance

1. From the Citrix Endpoint Management console, click **Configure > Actions**. The **Actions** page appears.
2. Click **Add** to add an action. The **Action Information** page appears.
3. On the **Action Information** page, enter a name and description for the action:
   - Name: HDX blocked notification
   - **Description:** HDX blocked notification because device is out of compliance
4. Click **Next**. The **Action details** page appears.
5. In the **Trigger** list:
   - Choose **Device property**.
   - Choose **Out of compliance**.
   - Choose **Is**.
   - Choose **True**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. In the **Action** list, specify the actions that occur when the trigger is met:
   - Choose **Send notification**
   - Choose **HDX Application Block, the notification you created**.
   - Choose **0**. Setting this value to 0 causes the notification to be sent when the trigger condition is met.
7. Select the Citrix Endpoint Management delivery group or groups to apply this action to. In this example, choose **AllUsers**.
8. Review the summary of the action.
9. Click **Next** and then click **Save**.

For more information on setting automated actions, see Automated actions.

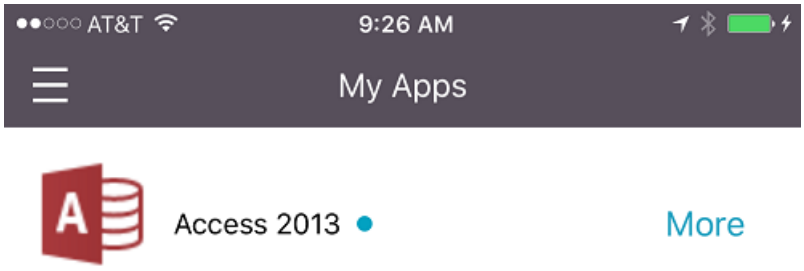
How users regain access to HDX apps

Users can gain access to HDX apps again after the device is brought back into compliance:

1. On the device, go to the Citrix Secure Hub store to refresh the apps in the store.
2. Go to the app and tap **Add** to the app.

After the app is added, it appears in My Apps with a blue dot next to it, because it is a newly installed app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



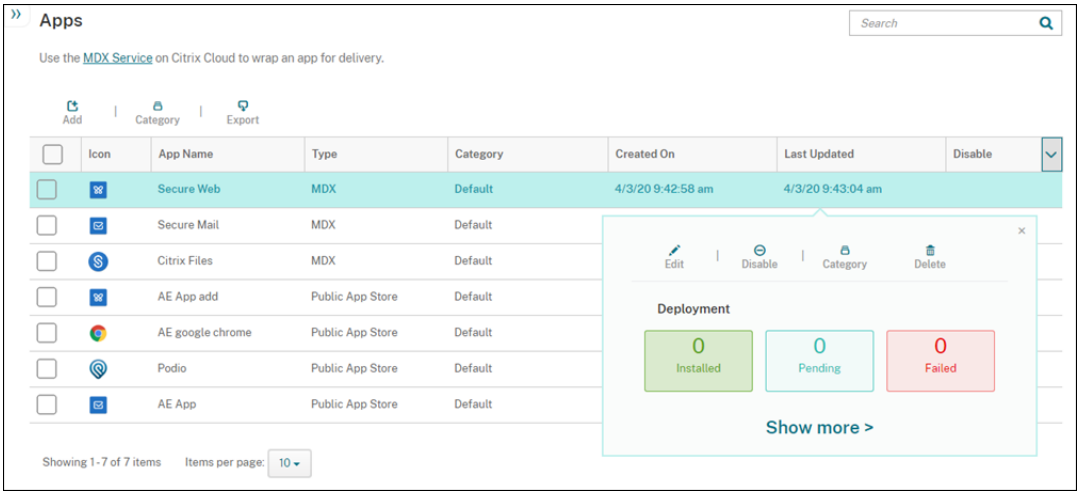
Upgrade MDX or enterprise apps

September 6, 2025

To upgrade an MDX or Enterprise app in Citrix Endpoint Management, disable the app in the Citrix Endpoint Management console, and then upload the new version of the app.

1. In the Citrix Endpoint Management console, click **Configure > Apps**. The **Apps** page appears.
2. For managed devices (devices enrolled in Citrix Endpoint Management for Mobile Device Management), skip to Step 3. For unmanaged devices (devices enrolled in Citrix Endpoint Management for enterprise app management purposes only), do the following:
    a) In the **Apps** table, select the checkbox next to the app or click the line that has the app you want to update.
    b) Click **Disable** in the menu that appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



c) Click **Disable** in the confirmation dialog box. *Disabled* appears in the **Disable** column for the app.

> **Note:**
>
> While the app is disabled, users can't reconnect to the app after they log off. Disabling an app is optional, but we recommend disabling the app to avoid app functionality issues. For example, users requesting to download the app at the same time you upload the new version might result in an issue.

3. In the **Apps** table, click the checkbox next to the app or click the line that has the app you want to update.
4. Click **Edit** in the menu that appears. The **App Information** page appears with the platforms you originally chose for the app selected.
5. Configure these settings:
   - **Name:** Optionally, change the app name.
   - **Description:** Optionally, change the app description.
   - **App category:** Optionally, change the app category.
6. Click **Next**. The first selected platform page appears. Do the following for each selected platform:
   a) Choose the replacement file that you want to upload by clicking **Upload** and navigating to the file location. The app uploads to Citrix Endpoint Management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

If you're uploading an app for Android Enterprise, a managed Google Play window appears. Upload the new version of the app here. For more details, see Distribute Android Enterprise apps.

b) Optionally, change the app details and policy settings for the platform.

c) Optionally, configure deployment rules and the app store. For information, see Add an MDX app.

7. Click **Save**. The **Apps** page appears.
8. If you disabled the app in Step 2, do the following:

a) In the **Apps** table, click to select the app you updated and then in the menu that appears, click **Enable**.

b) In the confirmation dialog box that appears, click **Enable**. Users can now access the app and receive a notification prompting them to upgrade the app.

Add media

September 6, 2025

You add media to Citrix Endpoint Management so you can deploy the media to user devices. You can use Citrix Endpoint Management to deploy Apple Books that you get through Apple Volume Purchase.

After you configure a Volume Purchase account in Citrix Endpoint Management, your bought and free books appear in **Configure** > **Media**. From the **Media** pages, you configure books for deployment to iOS devices by choosing delivery groups and specifying deployment rules.

The first time that a user receives a book and accepts the Volume Purchase license, deployed books install on the device. The books appear in the Apple Book app. You can't disassociate the book license from the user or remove the book from the device. Citrix Endpoint Management installs books as required media. If a user deletes an installed book from their device, the book stays in the Apple Book app, ready for download.

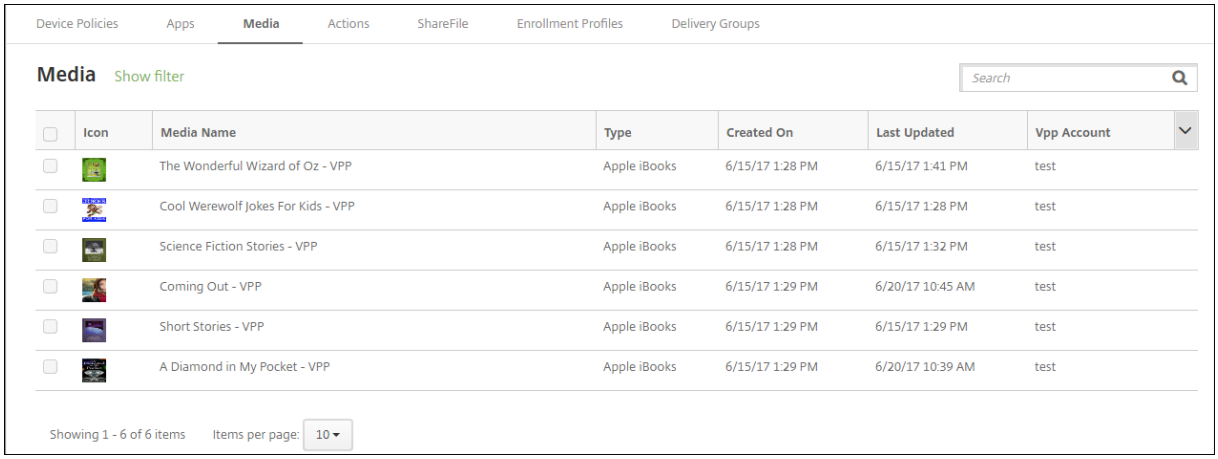
Prerequisites

- iOS devices
- Configure Apple Volume Purchase in Citrix Endpoint Management, as described in Apple Volume Purchase.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

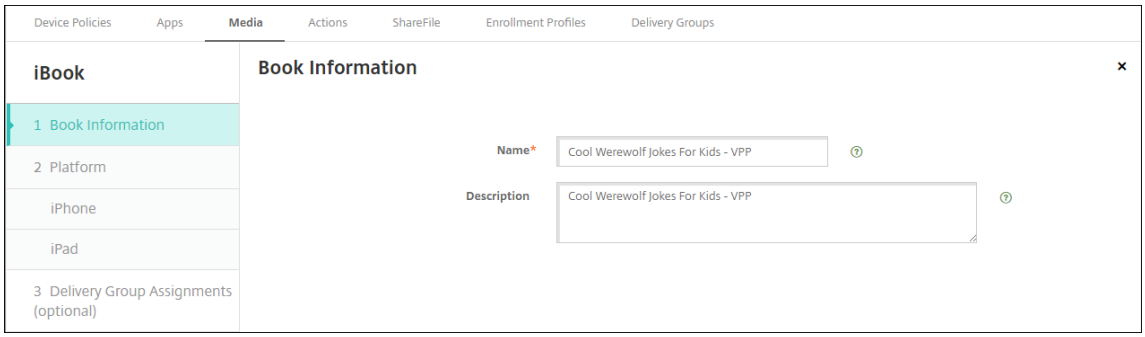
Configure books

Apple Books got through the Volume Purchase appear on the **Configure** > **Media** page.



To configure an Apple Book for deployment

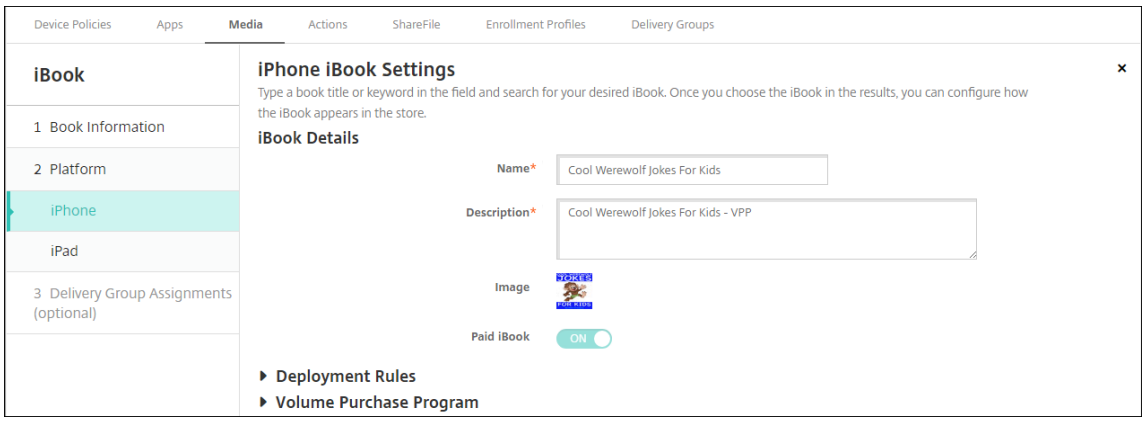
1. In **Configure > Media**, select a book and click **Edit**. The **Book Information** page appears.



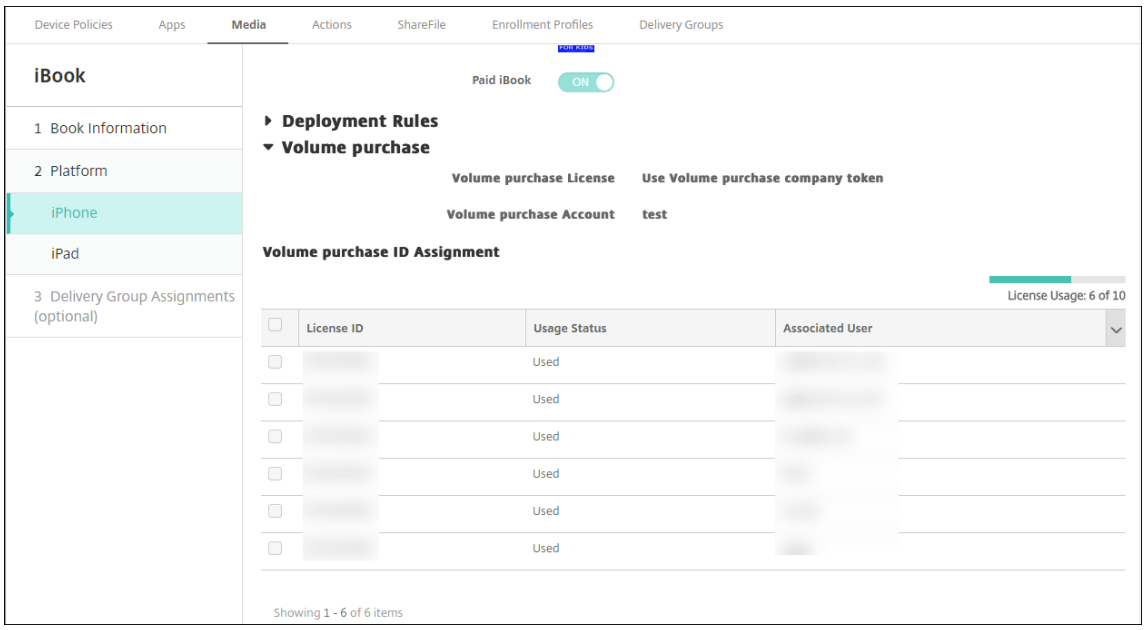
   The **Name** and **Description** appear only in the Citrix Endpoint Management console and logs.

2. In the **iPhone iBook Settings** and **iPad iBook Settings** pages: While you can optionally change the book name and description, Citrix® recommends that you don't change these settings. The image is for your information and isn't editable. **Paid iBook** indicates that a book is bought through Apple Volume Purchase.

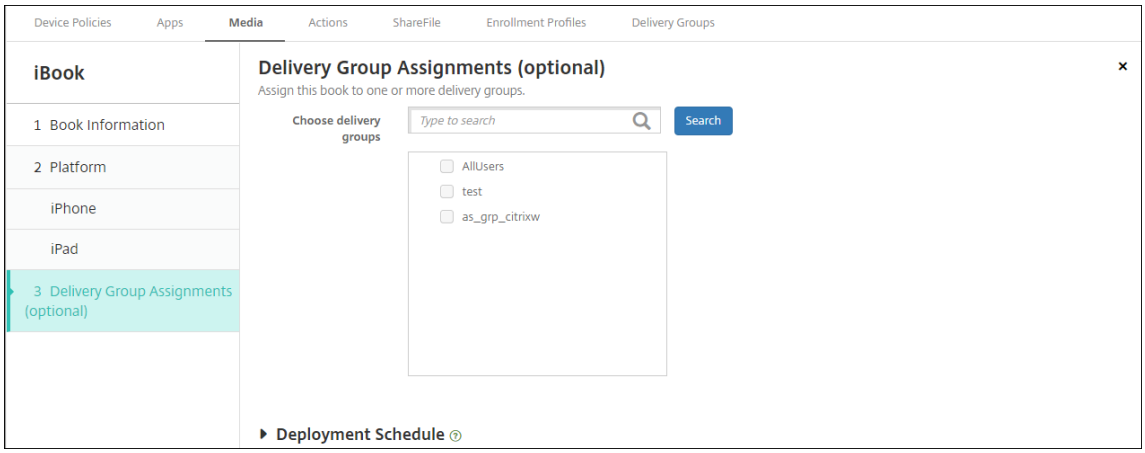
© 1997–2025 Citrix Systems, Inc. All rights reserved.



You can also specify deployment rules or view the Volume Purchase information.



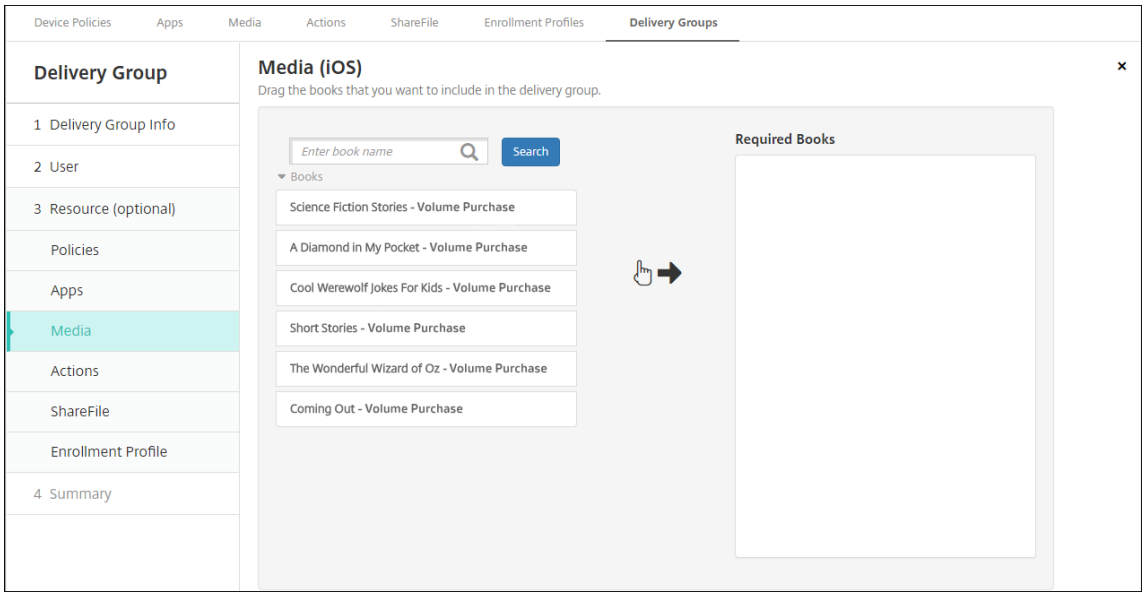
3. Optionally, assign the book to delivery groups and set a deployment schedule.



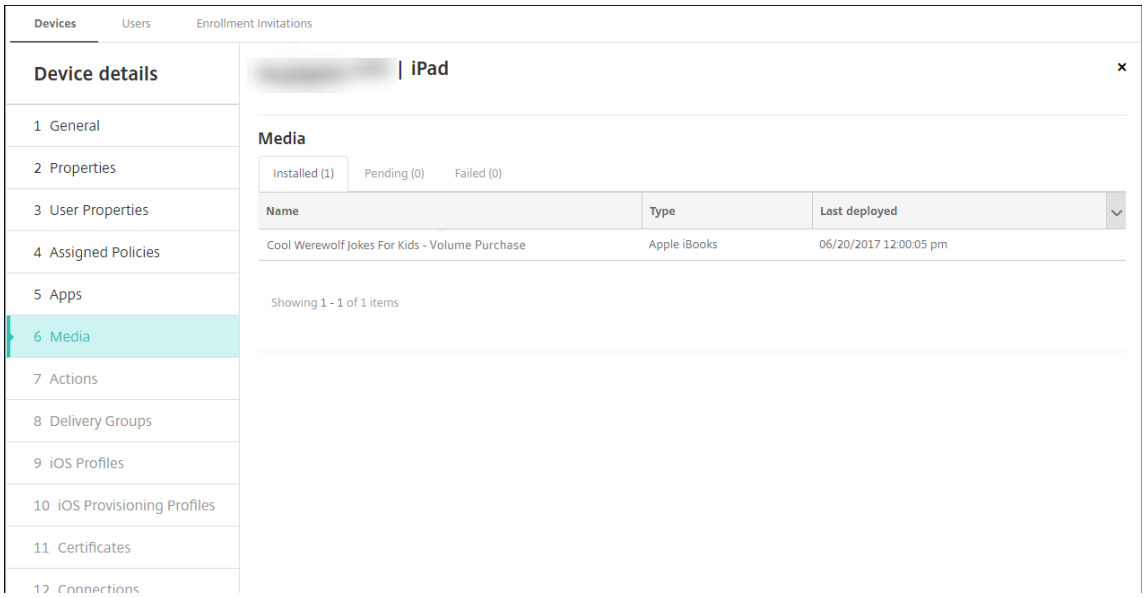
You can also assign books to delivery groups from the **Media** tab for **Configure > Delivery**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Groups. Citrix Endpoint Management supports required book deployment only.



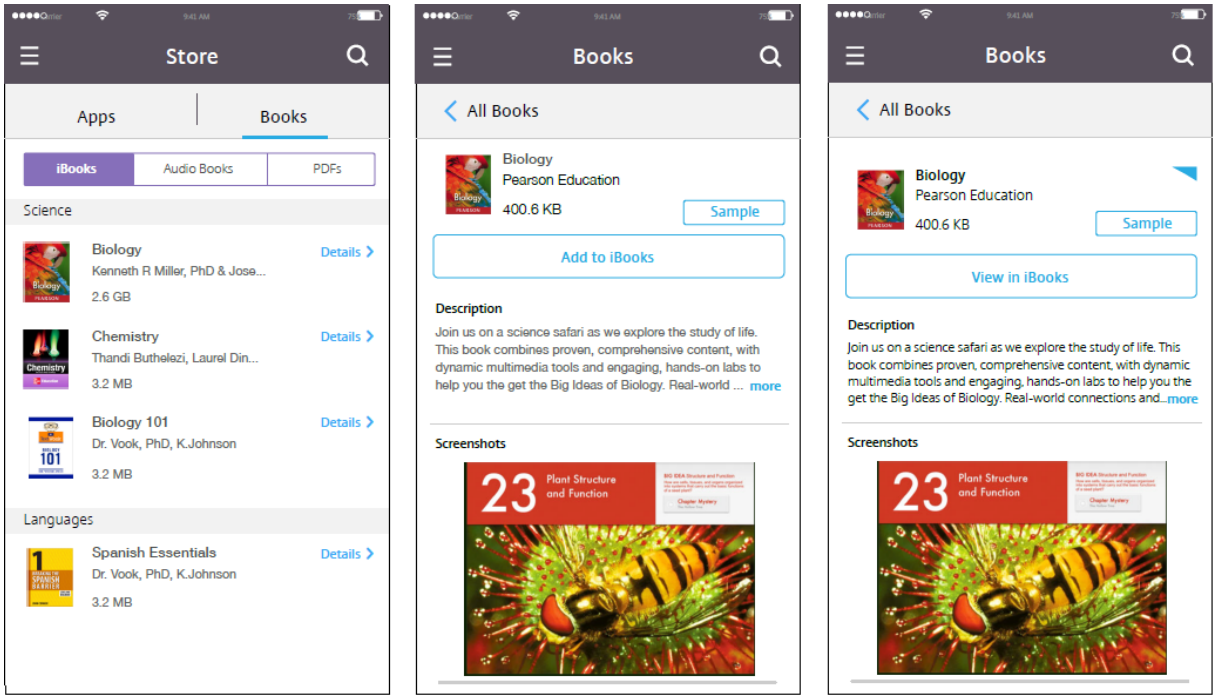
4. Use the **Media** tab for **Manage > Devices** to view deployment status.



> **Note:**
>
> On the **Configure** > **Media** page, if you select a book and click **Delete**, Citrix Endpoint Management removes the book from the list. However, the next time Citrix Endpoint Management syncs with Apple Volume Purchase, the book reappears on the list unless it has been removed from Apple Volume Purchase. Deleting a book from the list doesn't remove the book from the device.

Books appear on user devices as shown in the following example.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Deploy resources

February 20, 2024

Device configuration and management typically involve creating resources (policies, apps, and media) and actions in the Citrix Endpoint Management console and then packaging them using delivery groups. Delivery groups define categories of users so you can deploy specified policies, apps, media, and actions to their devices. Using the Citrix Endpoint Management console, you can:

- Add, manage, and deploy delivery groups.
- Change the order in which Citrix Endpoint Management pushes resources and actions in a delivery group to devices. This order is called the *deployment order*.

  You can specify deployment order in the Citrix Endpoint Management console. However, when a user is in multiple delivery groups that have duplicate or conflicting policies, Citrix Endpoint Management determines deployment order. See Calculation steps.

About delivery groups

Inclusion in a delivery group is typically based on user characteristics, such as company, country, department, office address, and title. Delivery groups give you greater control over who gets which re-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

sources and when they get them. You can deploy a delivery group to all users or to a defined group of users.

Installing and configuring Citrix Endpoint Management creates the default delivery group, AllUsers. This group has all local and Active Directory users. You can't delete the AllUsers group, but you can disable it when you don't want to push resources to all users. For details, see Enable and disable the AllUsers delivery group.

When you deploy a resource to a delivery group, you send a push notification to all users in the delivery group. For Apple devices, use the Apple Push Notification service (APNs) to send notifications. For more information see APNs certificates). For Android devices, use Firebase Cloud Messaging (FCM). For more information, see Firebase Cloud Messaging. For Windows devices, use the Windows Push Notification Service (WNS).

About deploying resources

When you work on pushing resources to devices, consider:

- **Deployment order:** Deployment order is the sequence in which Citrix Endpoint Management pushes resources (policies, apps, and media) and actions to a device. The deployment order applies to devices in a delivery group with an enrollment profile configured for device management (MDM) or for a combination of application management (MAM) and MDM.
- **Deployment rules:** Citrix Endpoint Management uses deployment rules that you specify for user and device properties to filter policies, apps, media, actions, and delivery groups. For example, a deployment rule might specify to push the deployment package when a domain name matches a particular value.

  Within a delivery group, you can specify a subset of users and devices that receive the resources based on their user and device properties. User and device property filtering within a delivery group takes precedence over deployment rules set on the resource.
- **Deployment schedule:** Citrix Endpoint Management uses the deployment schedule that you specify for policies, apps, media, and actions to control deployment of those items. You can specify that a deployment occurs now, on a set date and time, or when deployment conditions are met. You specify the schedule when you create the rule. See Configure deployment rules.

Before adding delivery groups, consider how deployment order, rules, and schedule relate to your deployment goals.

Deployment order

Deployment order is the sequence in which Citrix Endpoint Management pushes resources to devices. Deployment order is important when there are prerequisites for resources and dependencies between

© 1997–2025 Citrix Systems, Inc. All rights reserved.

resources. Resources include policies, apps, actions, and delivery groups.

For example, if you're pushing out a Wi-Fi policy that has certificate-based authentication, you must push the certification policy out before the Wi-Fi policy. Else, errors occur. Conversely, for some policies (such as Terms and Conditions, software inventory, and actions), deployment order doesn't matter.

When you add a delivery group, you can specify the order in which resources are deployed to devices. However, Citrix Endpoint Management always identifies each situation in which a user is in multiple delivery groups that have duplicate or conflicting policies. In these cases, Citrix Endpoint Management calculates a deployment order both for the objects that it delivers to a device and for the actions it performs.

When determining deployment order, Citrix Endpoint Management applies filters and control criteria, such as deployment rules and deployment schedule, to resources. The following table shows which of these criteria you can apply to each type of resource.

Resource	Device platform	Deployment rules	Deployment schedule	User/groups
Device policy	Y	Y	Y	-
App	Y	Y	Y	-
Media	Y	Y	Y	-
Action	-	Y	Y	-
Delivery group	-	Y	-	Y

Calculation steps

When Citrix Endpoint Management needs to calculate deployment order, it does these steps.

> **Note:**
>
> The device platform doesn't affect the calculation steps.

1. Determine all the delivery groups for a specific user, based on the filters of users, groups, and deployment rules.
2. Create an ordered list of all resources (policies, apps, media, and actions) in the selected delivery groups. The list is based on the filters of device platform, deployment rules, and deployment schedule. The ordering algorithm is as follows:
    a) Place resources from delivery groups that have an admin-defined deployment order ahead of resources from delivery groups without one. For details, see Example of calculation with user-defined order.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

b) As a tie-breaker among delivery groups, order resources from delivery groups in reverse alphabetical order by delivery group name. For example, Citrix Endpoint Management places resources from delivery group B ahead of resources from delivery group A.

c) While sorting, if an admin-defined deployment order is specified for the resources of a delivery group, maintain that order. Otherwise, sort the resources within that delivery group alphabetically by resource name.

d) If the same resource appears more than once, remove the duplicate resource. Deliver only the first of these resources.

Resources associated with an admin-defined order deploy before resources without an admin-defined order.

Example of calculation with admin-defined order Suppose that you have two delivery groups:

- Delivery group Account Managers 1: With *unspecified* order for resources. Has the policies **Network** and **Passcode**.
- Delivery group Account Managers 2: With *specified* order for resources. Has the policies **Connection scheduling**, **Restrictions**, **Passcode**, and **Network**, in order.

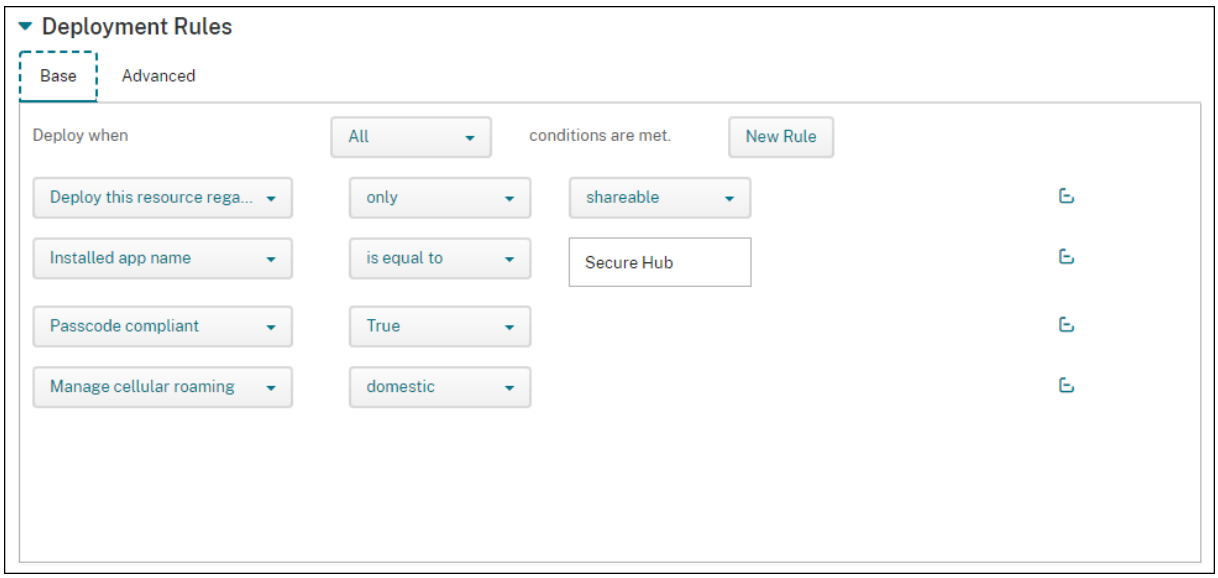
If the calculation algorithm ordered deployment groups only by name, Citrix Endpoint Management might deploy in this order, starting with the delivery group Account Managers 1: **Network**, **Passcode**, **Connection scheduling**, and **Restrictions**. Citrix Endpoint Management might ignore **Passcode** and **Network**, both duplicates, from the Account Managers 2 delivery group.

However, the Account Managers 2 group has an admin-specified deployment order. So the calculation algorithm places resources from the Account Managers 2 delivery group higher in the list than the resources from the Account Managers 1 delivery group. As a result, Citrix Endpoint Management deploys the policies in this order: **Connection scheduling**, **Restrictions**, **Passcode**, and **Network**. Citrix Endpoint Management ignores the policies **Network** and **Passcode** from the Account Managers 1 delivery group, because they're duplicates. The algorithm respects the order specified by the Citrix Endpoint Management administrator.

Configure deployment rules

Configure deployment rules to deliver resources when specific conditions are met. You can configure base or advanced deployment rules.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



When adding a deployment rule using the base editor, first select when to deploy the resource.

- **All:** Deliver the resource when the user or device meets all the conditions you configure.
- **Any:** Deliver the resource when the user or device meets at least one of the conditions you configure.

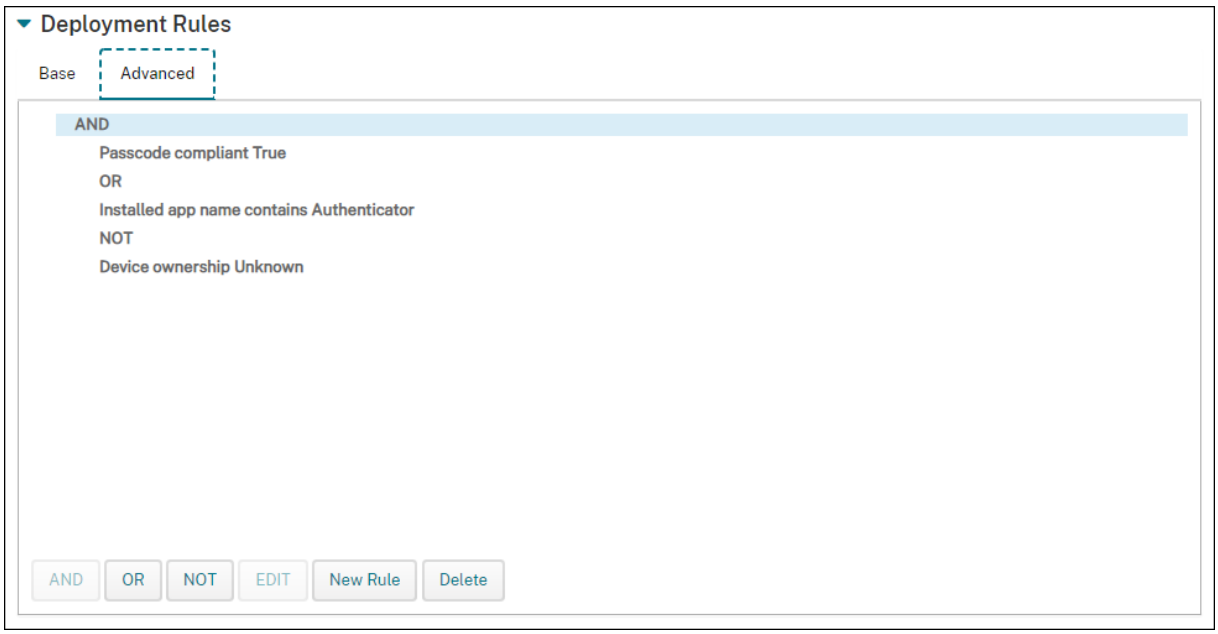
Click **New Rule** to choose a rule from a list of available rules to add. The available rules vary based on the resource being deployed and the platform for which you configure the resource. Within each rule are conditions.

You can specify to deploy the resource:

- Only when the selected property exists or except when the selected property exists.
- When the property matches the text you type exactly, the property has the text you type, or the property doesn't match the text you type.
- When the device or user is compliant with the property you select or isn't compliant with the property you select.
- When the device or user properties match a condition you select from a predefined list.

Use the advanced editor to create more complex deployment rules. You can choose from more rules and you can combine different Boolean logic operators when creating an advanced rule.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Work with delivery groups

You can work with delivery groups in the following ways:

- Add a delivery group
- Deploy to delivery groups
- Delete a delivery group
- Edit a delivery group
- Enable and disable the AllUsers delivery group.

Add a delivery group

When you create a delivery group, you specify whether the user assignments are managed in Citrix Endpoint Management or in Citrix Cloud. You can't change this specification after you create the delivery group.

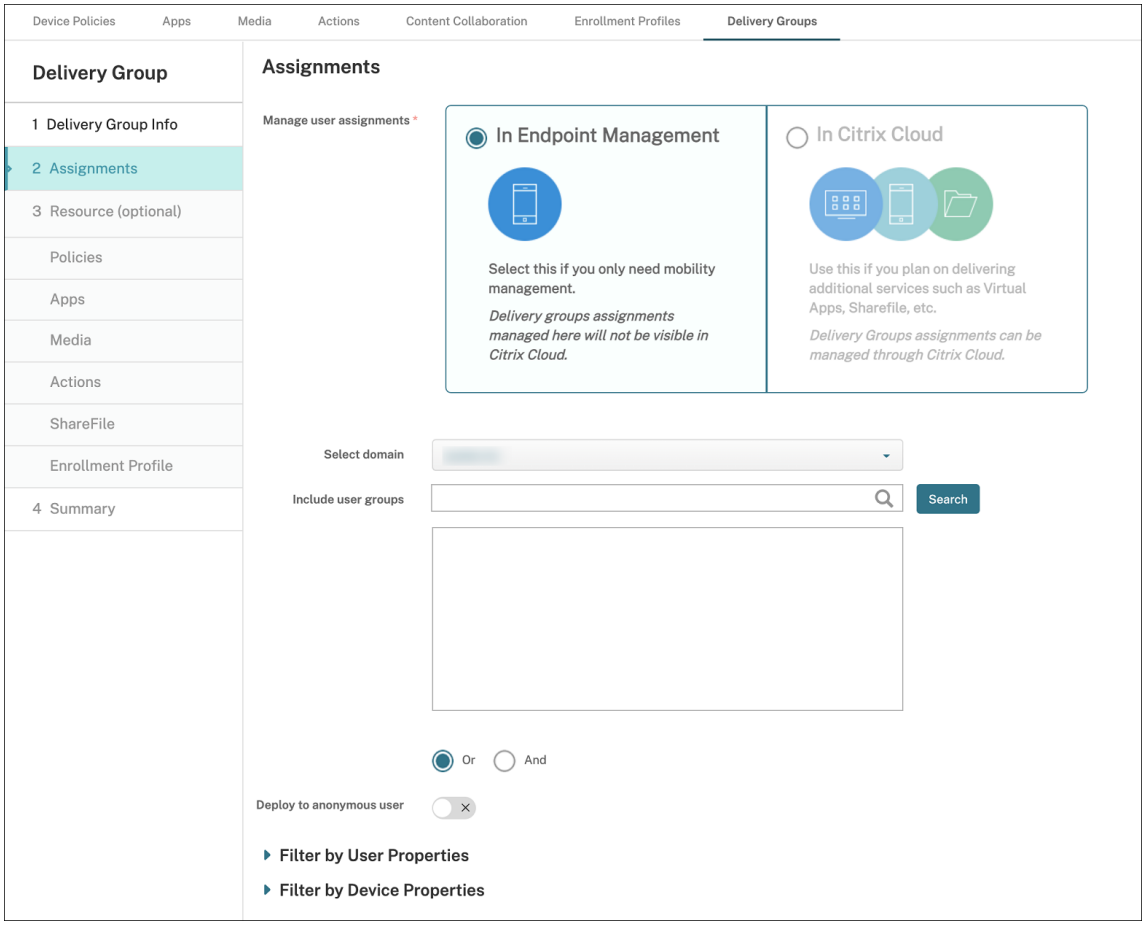
If you plan to use the delivery group to deliver other Citrix Cloud services, specify to manage the user assignments in Citrix Cloud. Other Citrix Cloud services include Citrix Virtual Apps and Desktops, ShareFile, or Secure Browser Service. You can add Active Directory users only to delivery groups managed in Citrix Cloud.

If you need only mobility management for a delivery group of users and apps, set **Manage user assignments** to **In Citrix Endpoint Management**. You can't see delivery groups with users managed in Citrix Endpoint Management in Citrix Cloud. So you can't use delivery groups managed in Citrix Endpoint Management to deliver other services.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> We recommend adding delivery groups before creating device policies and enrollment profiles. For information on creating them, see Device policies and Enrollment profiles.

1. In the Citrix Endpoint Management console, click **Configure > Delivery Groups**.
2. From the **Delivery Groups** page, click **Add**.
3. In the **Delivery Group Information** page, type a name and description for the delivery group and then click **Next**.
4. On the **Assignments** page, specify how to manage the delivery group assignments.



- **Manage user assignments:**
  - **In Citrix Endpoint Management:** Select this option if you plan to create a delivery group for users and apps that need only mobility management. You can't see delivery groups whose user assignments are managed in Citrix Endpoint Management in Citrix Cloud and you can't use them to deliver other services.
  - **In Citrix Cloud:** Select this option if you plan to use the delivery group to deliver other services. Those services might include Citrix Virtual Apps and Desktops or ShareFile.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. Add users to the delivery group.

> **Important:**
>
> You can't change the **Manage user assignments** setting after creating the delivery group.

   - **Select domain:** From the list, select the domain from which to choose users.
   - **Include user groups:** Do one of the following:
     - In the list of user groups, click the groups you want to add. The selected groups appear in the **Selected user groups** list.
     - Click **Search** to see a list of all user groups in the selected domain. You can also type a full or partial group name in the search box and then click **Search** to narrow your search.

     To remove a user group from the **Selected user groups** list, do one of the following:

     - In the **Selected user groups** list, click the **X** next to each group you want to remove.
     - Click **Search** to see a list of all user groups in the selected domain. Or, type a full or partial group name before you click **Search** to narrow your search. Clear the checkbox of each group that you want to remove.
   - **Or/And:** Select whether users are in any group (Or) or whether they must be in all groups (And) for the resource to be deployed to them.
   - **Deploy to anonymous user:** Select whether to deploy to unauthenticated users in the delivery group. Unauthenticated users are users that you can't authenticate but you allowed their devices to connect to Citrix Endpoint Management anyway.

6. Expand **Filter by User Properties** or **Filter by Device Properties** to specify how the delivery group manages resources.

   - If you choose **Filter by Device Properties**, expand the device platform to configure the deployment rules:
     - **Device Properties - Android** (see Create a rule to deploy resources to Android devices)
     - **Device Properties - iOS**
     - **Device Properties - Windows Desktop/Tablet only**
   - The **Base** tab appears by default. Under the **Base** tab, specify when to deploy the policy. You can choose to deploy the policy when **All** conditions are met or when **Any** conditions are met. The default option is set as **All**.
     - Click **New Rule** to define the conditions.
     - In the lists, choose the conditions. For example, select Device ownership and BYOD.
     - Click **New Rule** for each condition that you want to add.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Click the **Advanced** tab to combine the rules with Boolean options. The conditions you chose on the **Base** tab appear.
  - Click **AND**, **OR**, or **NOT**, and then click **New Rule**.
  - In the lists, choose the conditions to add to the rule and then click the plus sign (+) on the right side.
    At any time, you can click to select a condition and then click **Edit** to change the condition or **Delete** to remove the condition.

7. Click **Next** to go to the **Policies** page. You optionally add policies, apps, media, or actions for the delivery group here. For details, see:

   - Add policies to a delivery group
   - Add apps to a delivery group
   - Add media to a delivery group
   - Add actions to a delivery group

8. When you're satisfied with your delivery group, click **Summary** to see a summary of the configuration.
9. Click **Save**. The new delivery group appears on the **Delivery Groups** page.

Add policies to a delivery group

1. From the **Resources (optional)** list, click **Policies**.
2. For each policy you want to add, do the following:

   - Scroll through the list of available policies to find the policy you want to add. Or, type a full or partial policy name in the search box, and then click **Search**.
   - Drag the policy that you want to add into the box on the right.

   To remove a policy from the box, click the **X** next to the policy name.
3. Click **Next** to go to the **Apps** page.

Add apps to a delivery group

1. For each app you want to add, do the following:

   - Scroll through the list of available apps to find the app you want to add. Or, type a full or partial app name in the search box, and then click **Search**.
   - Drag the app into either the **Required Apps** box or the **Optional Apps** box.

   For apps marked as required, users can promptly receive updates in situations such as when:

   - You upload a new app and mark that it is required.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- You mark an existing app required.
- A user deletes a required app.
- A Citrix Secure Hub update is available.

For information about forced deployment of required apps, including how to enable the feature, see About required and optional apps.

To remove an app from the box, click the **X** next to the app name.

2. Click **Next** to go to the **Media** page.

Add media to a delivery group

1. For each book you want to add, do the following:

   - Scroll through the list of available books to find the book you want to add. Or, type a full or partial book name in the search box, and then click **Search**.
   - Drag the book that you want to add into the **Required Books** box.

   For books marked as required, users promptly receive updates in situations such as when:

   - You upload a new book and mark that it is required.
   - You mark an existing book required.
   - A user deletes a required book.
   - A Citrix Secure Hub update is available.

   To remove a book from the box, click the **X** next to the book name.

2. Click **Next** to go to the **Actions** page.

Add actions to a delivery group

1. For each action you want to add, do the following:

   - Scroll through the list of available actions to find the action you want to add. Or, type a full or partial action name in the search box, and then click **Search**.
   - Drag the action that you want to add into the box on the right.

   To remove an action from the box, click the **X** next to the action name.

2. Click **Next** to go to the **ShareFile** page.

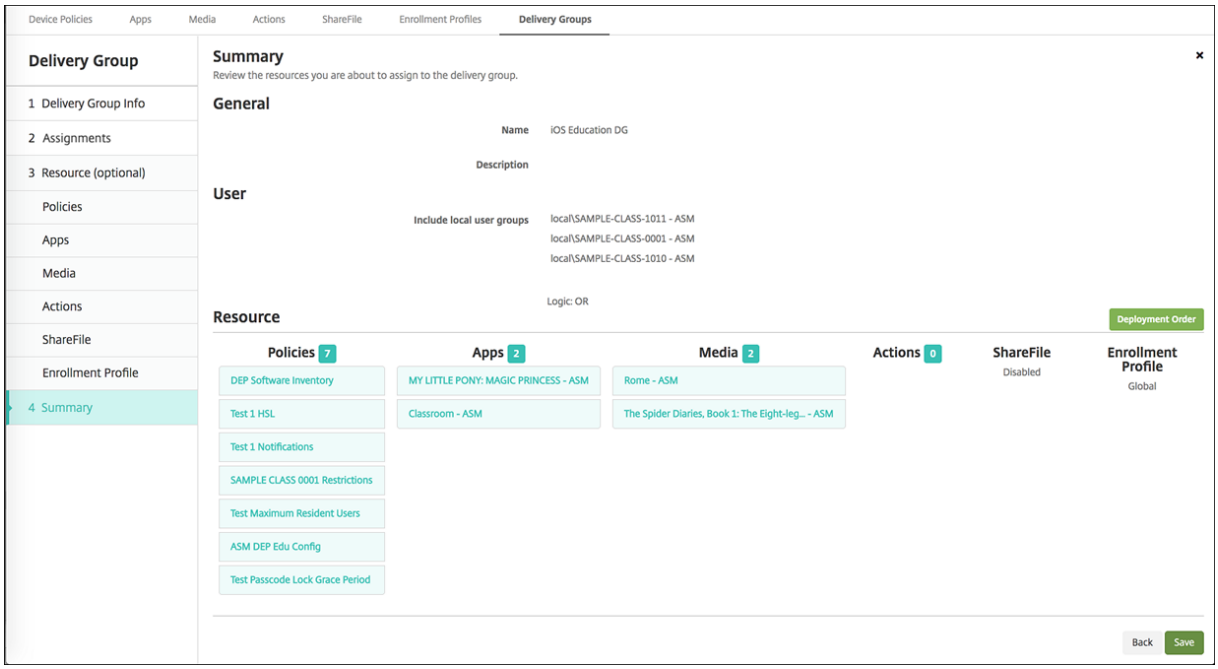
Apply the ShareFile configuration The ShareFile page differs depending on whether you configured Citrix Endpoint Management (**Configure > ShareFile**) for Enterprise accounts or for storage zone connectors.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- If you configured Enterprise accounts for use with Citrix Endpoint Management, set **Enable ShareFile** to **On**. This setting provides the delivery group single sign-on access to ShareFile content and data.
- If you configured storage zone connectors for use with Citrix Endpoint Management, drag the storage zone connectors to include in the delivery group to the box on the right.

Review configured options and change deployment order On the Summary page, you can review the options you've configured for the delivery group and change the deployment order of resources. The Summary page shows your resources by category. The Summary page doesn't show the deployment order.

> **Note:**
>
> Click **Back** to return to previous pages change the configuration.



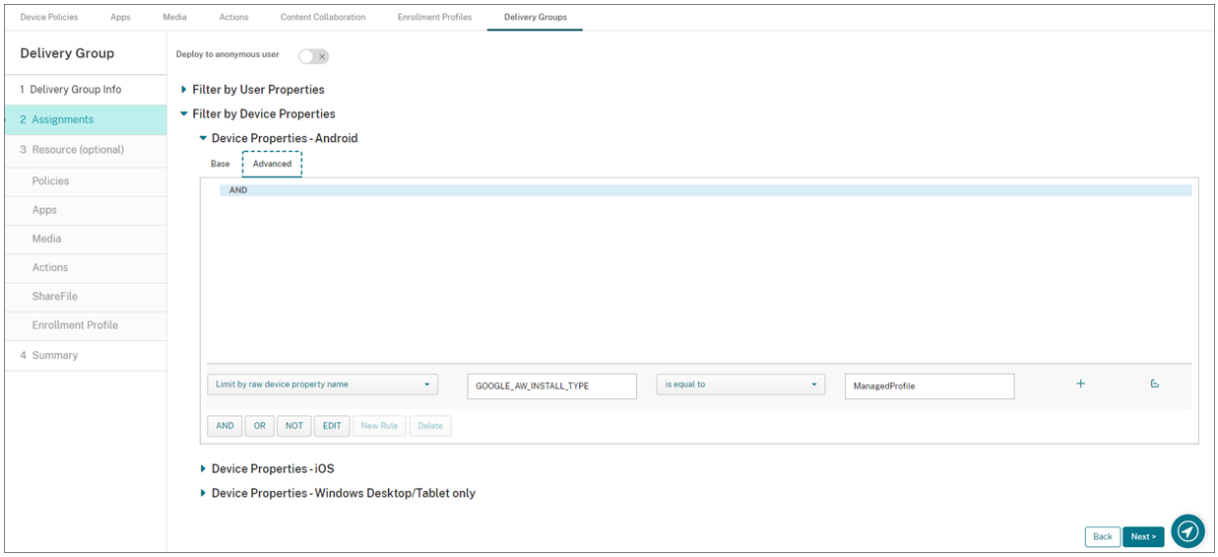
To view or change the deployment order:

1. Click **Deployment Order**.
2. In the Deployment Order dialog box, drag a resource to the place in the order where you want to deploy it. The resources deploy in top-to-bottom order.
3. Click **Save** to save the deployment order.

When you have finished configuring the delivery group, on the Summary page, click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Create a rule to deploy resources to Android Enterprise You can manage the deployment of a delivery group to Android Enterprise devices by using the Android device property rules. If you enroll multiple devices to the same user, you can create advanced filters for Android Enterprise based on device enrollment mode or the device application package ID.



To deploy a delivery group to Android Enterprise devices by using device enrollment mode:

1. Create a delivery group.
2. On the **Assignments** page, expand **Filter by Device Properties**.
3. In **Device Properties** –**Android**, open the **Advanced tab** and click **New rule**.
4. In the list, choose the condition to add to the rule:
    - For new Android Enterprise devices, choose **Limit by raw device property name** and type **GOOGLE_AW_INSTALL_TYPE** in the first value field. Then you must set the condition to equal one of the enrollment modes.
    - For existing Android Enterprise devices, choose **Limit by known device property name** and select **Android Enterprise install type** in the first value field. Then you must set the condition to equal one of the enrollment modes.
5. In the second field, type an enrollment mode for your Android Enterprise devices:
    - **DeviceAdministrator:** Specifies company-owned devices intended only for work use (also known as device owner mode)
    - **ManagedProfile:** Specifies BYOD—personal devices enrolled with work Profile Management (also known as profile-owner mode)
    - **CorporateOwnedSingleUse:** Specifies dedicated devices (formerly known as corporate-owned, single-use devices)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **CorporateOwnedPersonallyEnabled:** Specifies fully managed devices with a work profile (formerly known as corporate-owned, personally enabled devices)

6. Finish configuring the delivery group as described Add a delivery group.

   For more information, see Device deployment scenarios and profiles.

To deploy a delivery group to Android Enterprise devices by using the device application package ID:

1. In **Device Properties** –**Android**, open the **Advanced tab** and click **New rule**.
2. In the list, choose **Installed app name** and enter the application package ID.

Edit a delivery group

You can't change the name of an existing delivery group. To update other settings, go to **Configure > Delivery Groups**, select the group you want to edit, and then click **Edit**.

Enable and disable the AllUsers delivery group

AllUsers is the only delivery group that you can enable or disable. You cannot delete AllUsers as you can other delivery groups.

From the **Delivery Groups** page, choose the AllUsers delivery group by selecting the checkbox next to **AllUsers** or by clicking in the line containing **AllUsers**. Then do one of the following:

- Click **Disable** to disable the AllUsers delivery group. This command is available only if the AllUsers group is enabled (the default). **Disabled** appears under the **Disabled** heading in the delivery group table.
- Click **Enable** to enable the AllUsers delivery group. This command is available only if the AllUsers group is disabled. **Disabled** no longer appears under the **Disabled** heading in the delivery group table.

Deploy to delivery groups

Deploying to a delivery group means to send a push notification to all users with Apple, Android, and Windows tablet devices.

For users with other platform devices, if those devices are already connected to Citrix Endpoint Management, they receive the resources immediately. Otherwise, based on their scheduling policy, they receive the resources the next time that they connect.

For updated apps to appear in the Updated Available list in the app store on Android devices, first deploy an App Inventory policy to the user devices.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. On the **Delivery Groups** page, do one of the following:

   - To deploy to more than one delivery group at a time, select the checkboxes next to the groups you want to deploy.
   - To deploy to a single delivery group, either select the checkbox next to its name or click the line containing its name.

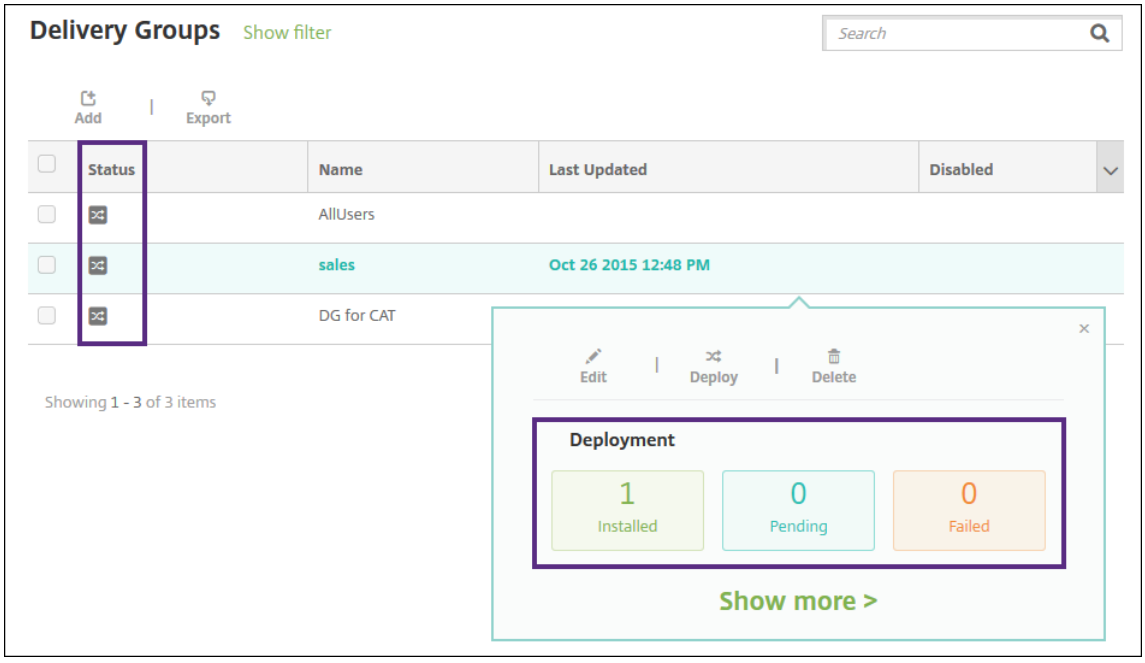
2. Click **Deploy**.

   Depending on how you select a single delivery group, the **Deploy** command appears over or to the right of the delivery group.

   Verify that the groups you want to deploy apps, policies, and actions to are listed. Then click **Deploy**. The apps, policies, and actions are deployed to the selected groups based on device platform and scheduling policy.

   You can check deployment status on the **Delivery Groups** page in one of these ways:

   - Look at the deployment icon under the **Status** heading for the delivery group, which indicates any deployment failure.
   - Click the line that has the delivery group to display an overlay that shows **Installed**, **Pending**, and **Failed** deployments.



Clone a delivery group

Clone a delivery group when you want to create a delivery group that is similar to an existing one. Use the clone as the starting point for your new delivery group. Then make your changes to the clone,

© 1997–2025 Citrix Systems, Inc. All rights reserved.

such as adding enrollment profiles or new sets of AD users.

1. In the Citrix Endpoint Management console, click **Configure** and then select the **Delivery Groups** tab.
2. From the list of delivery groups, select the one you want to use as the basis for the new group.
3. Select **Clone**.
4. In the Clone a Delivery Group dialog box, enter the name of the new group and, optionally, a description.
5. Select **Clone**.

Delete delivery groups

You can't delete the AllUsers delivery group, but you can disable it when you don't want to push resources to all users. See Enable and disable the AllUsers delivery group.

> **Important:**
>
> You cannot undo a delete.

1. On the **Delivery Groups** page, do one of the following:
   - To delete more than one delivery group at a time, select the checkboxes next to the groups you want to delete.
   - To delete a single delivery group, either select the checkbox next to its name or click the line containing its name.
2. Click **Delete**.

   Depending on how you select a single delivery group, the **Delete** command appears over or to the right of the delivery group.
3. In the **Delete** dialog box, click **Delete**.

Export the Delivery Groups table

1. Click **Export** above the **Delivery Groups** table. Citrix Endpoint Management extracts the information in the **Delivery Groups** table and converts it to a .csv file.
2. Open or save the .csv file by following the usual steps for your browser.

Macros

September 6, 2025

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management provides macros as a way to populate user or device property data within the text field of the following items:

- Policies
- Notifications
- Enrollment templates
- Device configuration XML file
- Automated actions
- Credential provider Certificate Signing Requests

Citrix Endpoint Management replaces a macro with the corresponding user or system values. For example, you can prepopulate the mailbox value for a user in a single Exchange profile across thousands of users.

Macro syntax

A macro can take the following form:

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)] }`

Enclose all syntax following the dollar sign ($) in curly brackets ({ }).

- Qualified property names reference either a user property, a device property, or a custom property.
- Qualified property names consist of a prefix, followed by the actual property name.
- User properties take the form `${ user.[PROPERTYNAME] (prefix="user.")}`.
- Device properties take the form `${ device.[PROPERTYNAME] (prefix="device.") }`.
- Property names are case-sensitive.
- A function can be a limited list or a link to a third-party reference that defines functions. This macro for a notification message includes the function `firstnotnull`:

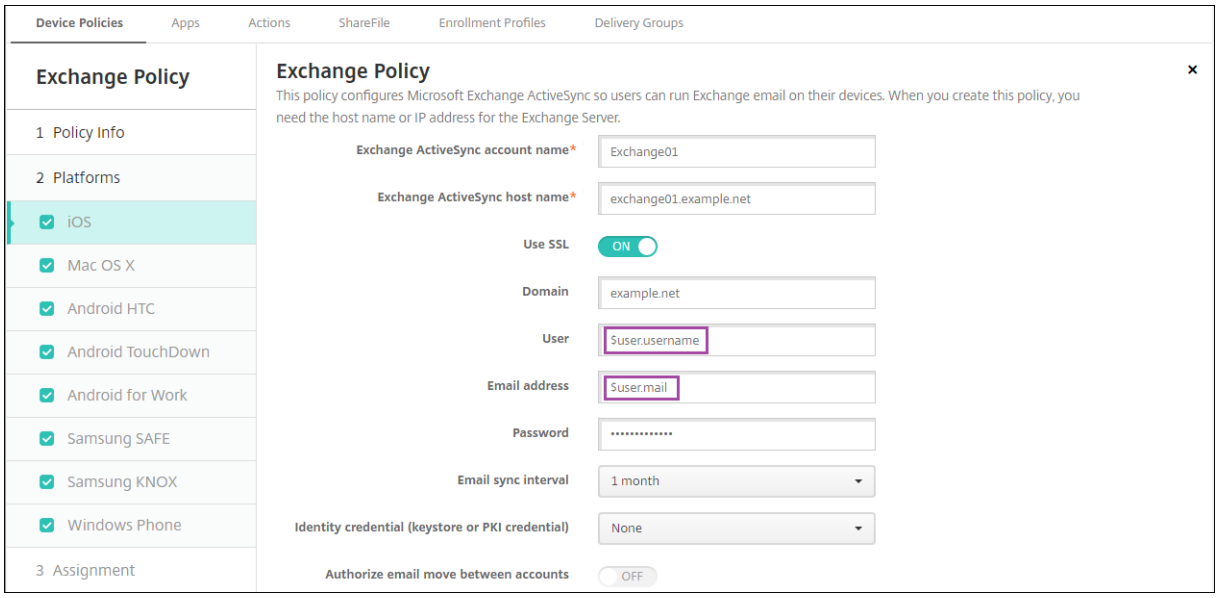
Device `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` has been blocked…

- For custom macros (properties that you define), the prefix is `${ custom }`. You can leave out the prefix.

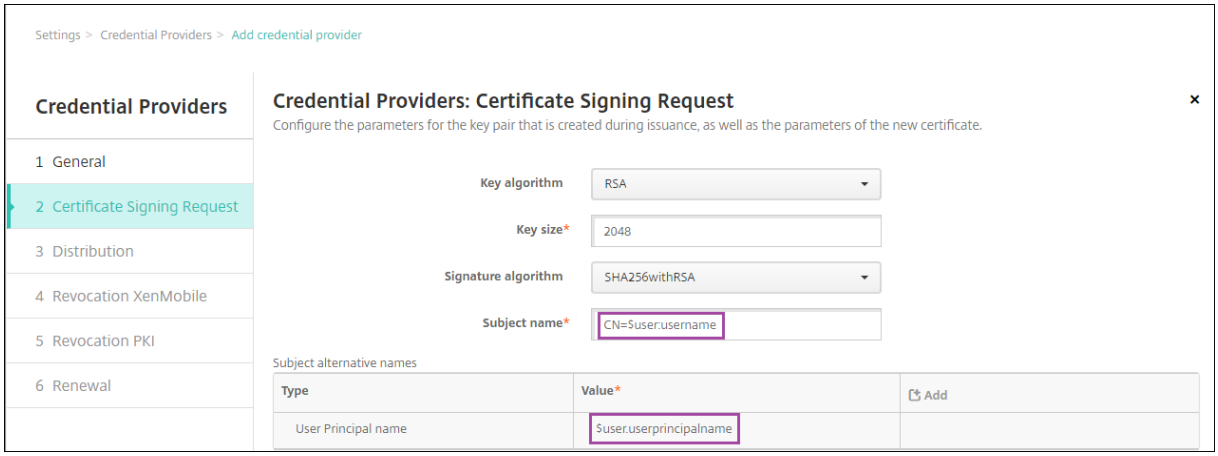
Here's an example of a commonly used macro, `${ user.username }` that populates the user name value in the text field of a policy. This macro is useful for configuring Exchange ActiveSync profiles and other profiles used by many users. The following example shows how to use macros in an

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Exchange policy. The macro for **User** is `${ user.username }`. The macro for **Email address** is `${ user.mail }`.



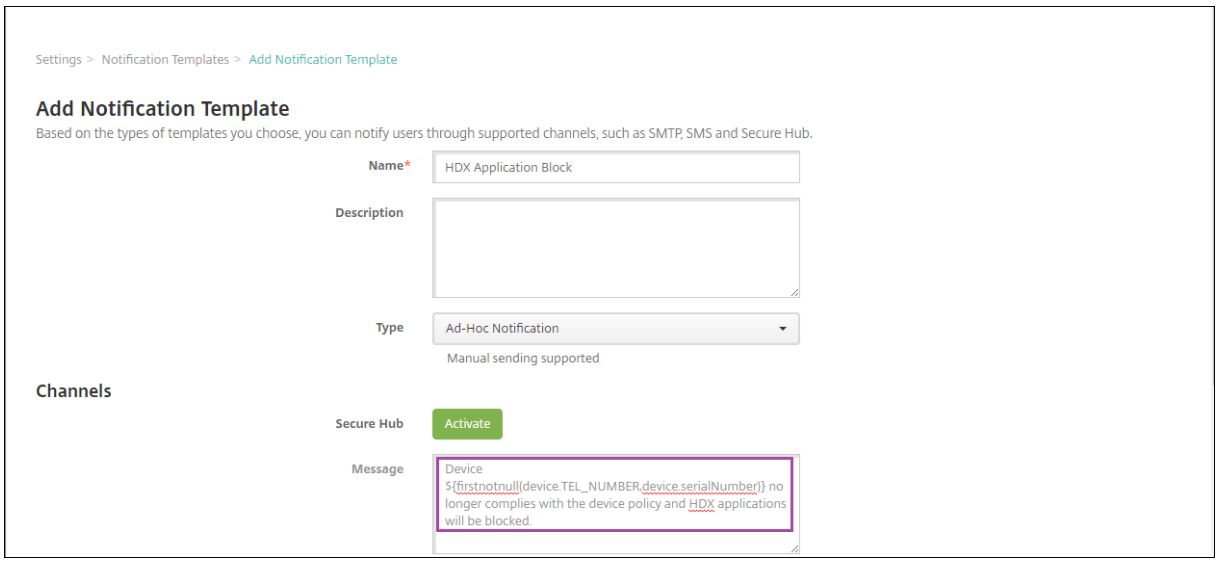
The following example shows how to use macros for a certificate signing request. The macro for **Subject name** is **CN=$user.username**. The macro for the **Value** of a **Subject alternative name** is **$user.userprincipalname**.



The following example shows how to use macros in a notification template. The example template defines the message sent to a user when HDX™ applications are blocked because of a non-compliant device. The macro for the **Message** is:

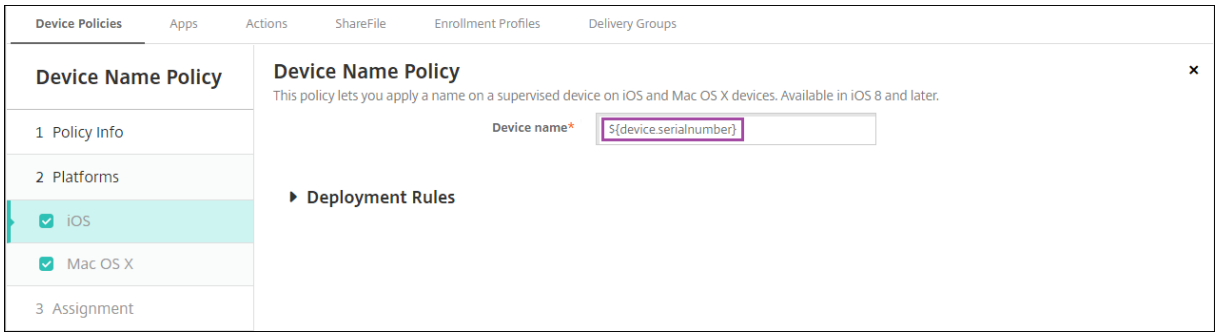
Device `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` no longer follows the device policy and HDX applications are blocked.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



For more examples of macros used in notifications, go to **Settings > Notification Templates**, select a pre-defined template, and click **Edit**.

The following example shows a macro in the Device Name device policy. You can type a macro, a combination of macros, or a combination of macros and text to name each device uniquely. For example, use `${ device.serialnumber }` to set the device names to the serial number of each device. Use `${ device.serialnumber } ${ user.username }` to include the user name in the device name. The Device Name device policy works on supervised iOS and macOS devices.



Macros for default notification templates

You can use the following macros in the default notification templates:

- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`
- `${ enrollment.andriod.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`
- `${ enrollment.pin }`
- `${ enrollment.url }`

© 1997–2025 Citrix Systems, Inc. All rights reserved.

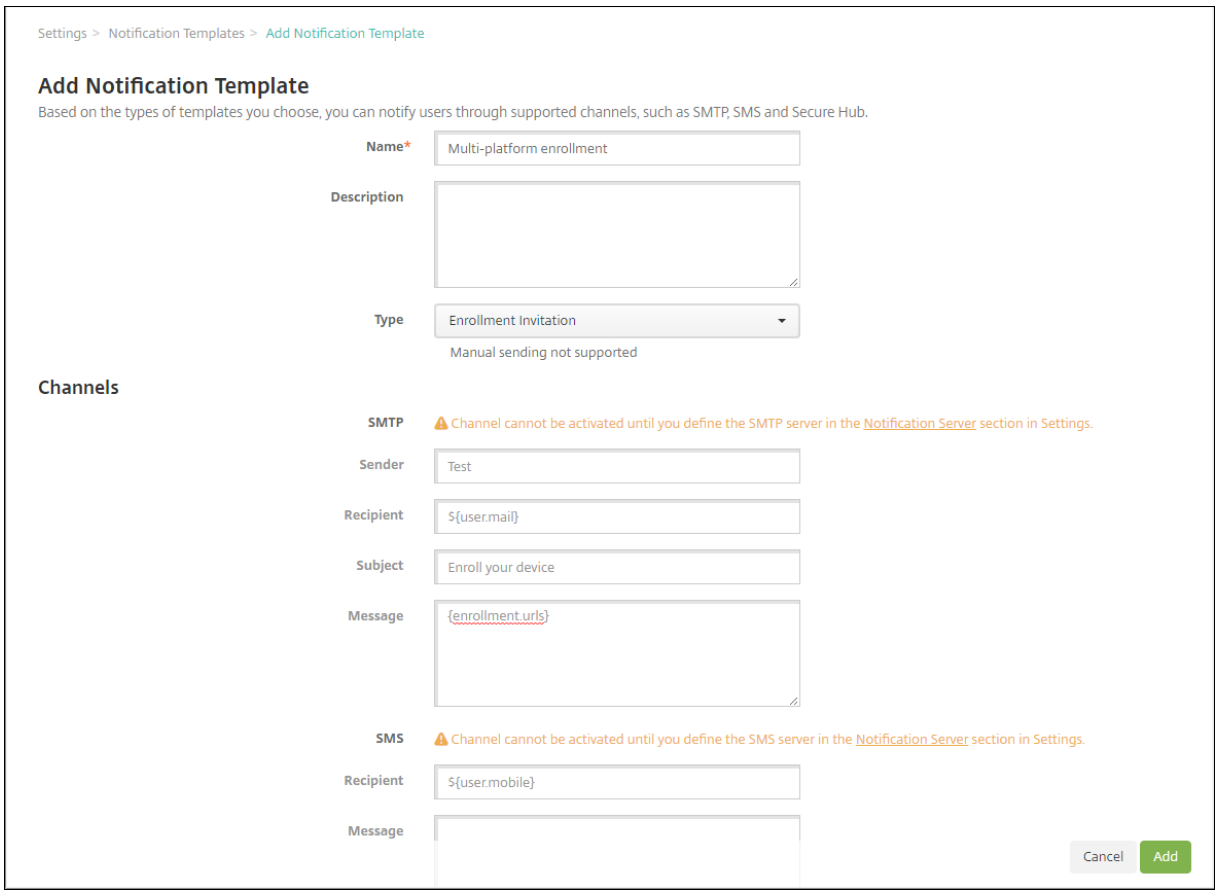
- ${ enrollment.urls }
- ${ enrollment.ios.url }
- ${ enrollment.macos.url }
- ${ enrollment.android.url }
- ${ enrollment.ios.platform }
- ${ enrollment.macos.platform }
- ${ enrollment.android.platform }
- ${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}
- ${ firstnotnull(device.TEL_NUMBER,user.mobile)}
- ${ outofcompliance.reason(smg_block)}
- ${ outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${ vpp.account }
- ${ vpp.appname }
- ${ vpp.url }
- ${ zdmserver.hostPath } /enroll

> **Note:**
>
> The Citrix Endpoint Management console includes the terms “blacklist”and “whitelist”. We are changing those terms in an upcoming version to “block list”and “allow list”.

This example shows how to create a notification that includes enrollment URLs for many device platforms. The macro for the **Message** is:

${enrollment.urls}

© 1997–2025 Citrix Systems, Inc. All rights reserved.



These examples show how to create messages for notifications that prompt the users to click the enrollment URL for their device platforms:

Example 1:

```
To enroll, click the link below that applies to your device platform:

${
 enrollment.ios.platform }
  - ${
 enrollment.ios.url }


${
 enrollment.macos.platform }
  - ${
 enrollment.macos.url }


${
 enrollment.android.platform }
  - ${
 enrollment.android.url }
```

Example 2:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
To enroll an iOS device, click the link ${
 enrollment.ios.url }
 .

To enroll a macOS device, click the link ${
 enrollment.macos.url }
 .

To enroll an Android device, click the link ${
 enrollment.android.url }
 .
```

Macros for specific policies

For the Device Name device policy (for iOS and macOS), you can use these macros for the **Device name:**

- `${ device.serialnumber }`
- `${ user.username } @example.com`
- `${ device.serialnumber }`
- `${ device.serialnumber }`
- `${ user.username }`
- `${ enrollment.pin }`
- `${ user.dnsroot }`

For the Cellular device policy (for iOS), you can use macros for the values of non-string fields, such as Proxy server port. For example, you can now use a macro such as `${ device.xyz }` or `${ setting.xyz }`, which expands into an integer.

For a device configuration XML file that you import into Citrix Endpoint Management by using the **Import iOS & macOS Profile** device policy, you can use macros for the values of non-string fields.

For the Samsung MDM License Key device policy, you can use this macro for the **ELM license key:**

- `${ elm.license.key }`

For the Web clip device policy, you can use this macro for the **URL:**

- `${ webeas-url }`

Macros to get built-in device properties

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Display name	Macros
Device ID	`$device.id`
Device GUID	`$device.uniqueid`
Device IMEI	`$device.imei`
OS Family	`$device.OSFamily`
Serial Number	`$device.serialNumber`

Macros for all device properties

Display name: Account Suspended?

- **Web element:** `GOOGLE_AW_DIRECTORY_SUSPENDED`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_SUSPENDED }`

Display name: Activation lock bypass code

- **Web element:** `ACTIVATION_LOCK_BYPASS_CODE`
- **Macros:** `${ device.ACTIVATION_LOCK_BYPASS_CODE }`

Display name: Activation lock enabled

- **Web element:** `ACTIVATION_LOCK_ENABLED`
- **Macros:** `${ device.ACTIVATION_LOCK_ENABLED }`

Display name: Active Apple App Store account

- **Web element:** `ACTIVE_ITUNES`
- **Macros:** `${ device.ACTIVE_ITUNES }`

Display name: Administrator disabled

- **Web element:** `ADMIN_DISABLED`
- **Macros:** `${ device.ADMIN_DISABLED }`

Display name: AIK Present?

- **Web element:** `WINDOWS_HAS_AIK_PRESENT`
- **Macros:** `${ device.WINDOWS_HAS_AIK_PRESENT }`

Display name: Amazon MDM API available

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `AMAZON_MDM`
- **Macros:** `${ device.AMAZON_MDM }`

Display name: Android Enterprise Device ID

- **Web element:** `GOOGLE_AW_DEVICE_ID`
- **Macros:** `${ device.GOOGLE_AW_DEVICE_ID }`

Display name: Android Enterprise Enabled Device?

- **Web element:** `GOOGLE_AW_ENABLED_DEVICE`
- **Macros:** `${ device.GOOGLE_AW_ENABLED_DEVICE }`

Display name: Android Enterprise Install Type

- **Web element:** `GOOGLE_AW_INSTALL_TYPE`
- **Macros:** `${ device.GOOGLE_AW_INSTALL_TYPE }`

Display name: Antispyware Signature status

- **Web element:** `ANTI_SPYWARE_SIGNATURE_STATUS`
- **Macros:** `${ device.ANTI_SPYWARE_SIGNATURE_STATUS }`

Display name: Antispyware Status

- **Web element:** `ANTI_SPYWARE_STATUS`
- **Macros:** `${ device.ANTI_SPYWARE_STATUS }`

Display name: Antivirus Signature Status

- **Web element:** `ANTI_VIRUS_SIGNATURE_STATUS`
- **Macros:** `${ device.ANTI_VIRUS_SIGNATURE_STATUS }`

Display name: Antivirus Status

- **Web element:** `ANTI_VIRUS_STATUS`
- **Macros:** `${ device.ANTI_VIRUS_STATUS }`

Display name: ASM Deployment Program activation lock bypass code

- **Web element:** `DEP_ACTIVATION_LOCK_BYPASS_CODE`
- **Macros:** `${ device.DEP_ACTIVATION_LOCK_BYPASS_CODE }`

Display name: ASM Deployment Program escrow key

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `DEP_ESCROW_KEY`
- **Macros:** `${ device.DEP_ESCROW_KEY }`

Display name: Asset tag

- **Web element:** `ASSET_TAG`
- **Macros:** `${ device.ASSET_TAG }`

Display name: Automatically check software updates

- **Web element:** `AutoCheckEnabled`
- **Macros:** `${ device.AutoCheckEnabled }`

Display name: Automatically download software updates in the background

- **Web element:** `BackgroundDownloadEnabled`
- **Macros:** `${ device.BackgroundDownloadEnabled }`

Display name: Automatically install app updates

- **Web element:** `AutomaticAppInstallationEnabled`
- **Macros:** `${ device.AutomaticAppInstallationEnabled }`

Display name: Automatically install OS updates

- **Web element:** `AutomaticOSInstallationEnabled`
- **Macros:** `${ device.AutomaticOSInstallationEnabled }`

Display name: Automatically install security updates

- **Web element:** `AutomaticSecurityUpdatesEnabled`
- **Macros:** `${ device.AutomaticSecurityUpdatesEnabled }`

Display name: Autoupdate Status

- **Web element:** `AUTOUPDATE_STATUS`
- **Macros:** `${ device.AUTOUPDATE_STATUS }`

Display name: Available RAM

- **Web element:** `MEMORY_AVAILABLE`
- **Macros:** `${ device.MEMORY_AVAILABLE }`

Display name: Available software updates

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `AVAILABLE_OS_UPDATE_HUMAN_READABLE`
- **Macros:** `${ device.AVAILABLE_OS_UPDATE_HUMAN_READABLE }`

Display name: Available storage space

- **Web element:** `FREEDISK`
- **Macros:** `${ device.FREEDISK }`

Display name: Backup battery

- **Web element:** `BACKUP_BATTERY_PERCENT`
- **Macros:** `${ device.BACKUP_BATTERY_PERCENT }`

Display name: Baseband firmware version

- **Web element:** `MODEM_FIRMWARE_VERSION`
- **Macros:** '${device.MODEM_FIRMWARE_VERSION}

Display name: Battery Charging

- **Web element:** `BATTERY_CHARGING_STATUS`
- **Macros:** `${ device.BATTERY_CHARGING_STATUS }`

Display name: Battery charging

- **Web element:** `BATTERY_CHARGING`
- **Macros:** `${ device.BATTERY_CHARGING }`

Display name: Battery Remaining

- **Web element:** `BATTERY_ESTIMATED_CHARGE_REMAINING`
- **Macros:** `${ device.BATTERY_ESTIMATED_CHARGE_REMAINING }`

Display name: Battery Runtime

- **Web element:** `BATTERY_RUNTIME`
- **Macros:** `${ device.BATTERY_RUNTIME }`

Display name: Battery Status

- **Web element:** `BATTERY_STATUS`
- **Macros:** `${ device.BATTERY_STATUS }`

Display name: BES PIN

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `BES_PIN`
- **Macros:** `${ device.BES_PIN }`

Display name: BES server agent ID

- **Web element:** `AGENT_ID`
- **Macros:** `${ device.AGENT_ID }`

Display name: BES server name

- **Web element:** `BES_SERVER`
- **Macros:** `${ device.BES_SERVER }`

Display name: BES server version

- **Web element:** `BES_VERSION`
- **Macros:** `${ device.BES_VERSION }`

Display name: BIOS Info

- **Web element:** `BIOS_INFO`
- **Macros:** `${ device.BIOS_INFO }`

Display name: BitLocker Status

- **Web element:** `WINDOWS_HAS_BIT_LOCKER_STATUS`
- **Macros:** `${ device.WINDOWS_HAS_BIT_LOCKER_STATUS }`

Display name: Bluetooth MAC address

- **Web element:** `BLUETOOTH_MAC`
- **Macros:** `${ device.BLUETOOTH_MAC }`

Display name: Boot Debugging Enabled?

- **Web element:** `WINDOWS_HAS_BOOT_DEBUGGING_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED }`

Display name: Boot Manager Rev List Version

- **Web element:** `WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION`
- **Macros:** `${ device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION }`

Display name: Carrier Code

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `CARRIER_CODE`
- **Macros:** `${ device.CARRIER_CODE }`

Display name: Carrier settings version

- **Web element:** `CARRIER_SETTINGS_VERSION`
- **Macros:** `${ device.CARRIER_SETTINGS_VERSION }`

Display name: Catalog URL

- **Web element:** `CatalogURL`
- **Macros:** `${ device.CatalogURL }`

Display name: Cellular altitude

- **Web element:** `GPS_ALTITUDE_FROM_CELLULAR`
- **Macros:** `${ device.GPS_ALTITUDE_FROM_CELLULAR }`

Display name: Cellular course

- **Web element:** `GPS_COURSE_FROM_CELLULAR`
- **Macros:** `${ device.GPS_COURSE_FROM_CELLULAR }`

Display name: Cellular horizontal accuracy

- **Web element:** `GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR`
- **Macros:** `${ device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR }`

Display name: Cellular latitude

- **Web element:** `GPS_LATITUDE_FROM_CELLULAR`
- **Macros:** `${ device.GPS_LATITUDE_FROM_CELLULAR }`

Display name: Cellular longitude

- **Web element:** `GPS_LONGITUDE_FROM_CELLULAR`
- **Macros:** `${ device.GPS_LONGITUDE_FROM_CELLULAR }`

Display name: Cellular speed

- **Web element:** `GPS_SPEED_FROM_CELLULAR`
- **Macros:** `${ device.GPS_SPEED_FROM_CELLULAR }`

Display name: Cellular technology

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `CELLULAR_TECHNOLOGY`
- **Macros:** `${ device.CELLULAR_TECHNOLOGY }`

Display name: Cellular timestamp

- **Web element:** `GPS_TIMESTAMP_FROM_CELLULAR`
- **Macros:** `${ device.GPS_TIMESTAMP_FROM_CELLULAR }`

Display name: Cellular vertical accuracy

- **Web element:** `GPS_VERTICAL_ACCURACY_FROM_CELLULAR`
- **Macros:** `${ device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR }`

Display name: Change Password at Next Login?

- **Web element:** `GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`
- **Macros:** '${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

Display name: Client device ID

- **Web element:** `CLIENT_DEVICE_ID`
- **Macros:** `${ device.CLIENT_DEVICE_ID }`

Display name: Cloud backup enabled

- **Web element:** `CLOUD_BACKUP_ENABLED`
- **Macros:** `${ device.CLOUD_BACKUP_ENABLED }`

Display name: Code Integrity Enabled?

- **Web element:** `WINDOWS_HAS_CODE_INTEGRITY_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED }`

Display name: Code Integrity Rev List Version

- **Web element:** `WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION`
- **Macros:** `${ device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION }`

Display name: Color

- **Web element:** `COLOR`
- **Macros:** `${ device.COLOR }`

Display name: CPU clock speed

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `CPU_CLOCK_SPEED`
- **Macros:** `${ device.CPU_CLOCK_SPEED }`

Display name: CPU type

- **Web element:** `CPU_TYPE`
- **Macros:** `${ device.CPU_TYPE }`

Display name: Creation Time

- **Web element:** `GOOGLE_AW_DIRECTORY_CREATION_TIME`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_CREATION_TIME }`

Display name: Critical software updates

- **Web element:** `AVAILABLE_OS_UPDATE_IS_CRITICAL`
- **Macros:** `${ device.AVAILABLE_OS_UPDATE_IS_CRITICAL }`

Display name: Current carrier network

- **Web element:** `CARRIER`
- **Macros:** `${ device.CARRIER }`

Display name: Current mobile country code

- **Web element:** `CURRENT_MCC`
- **Macros:** `${ device.CURRENT_MCC }`

Display name: Current mobile network code

- **Web element:** `CURRENT_MNC`
- **Macros:** `${ device.CURRENT_MNC }`

Display name: Data roaming allowed

- **Web element:** `DATA_ROAMING_ENABLED`
- **Macros:** `${ device.DATA_ROAMING_ENABLED }`

Display name: Date of the last iCloud backup

- **Web element:** `LAST_CLOUD_BACKUP_DATE`
- **Macros:** `${ device.LAST_CLOUD_BACKUP_DATE }`

Display name: Default catalog

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `IsDefaultCatalog`
- **Macros:** `${ device.IsDefaultCatalog }`

Display name: Apple Deployment Program account name

- **Web element:** `BULK_ENROLLMENT_DEP_ACCOUNT_NAME`
- **Macros:** `${ device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME }`

Display name: Apple Deployment Program Policy

- **Web element:** `WINDOWS_HAS_DEP_POLICY`
- **Macros:** `${ device.WINDOWS_HAS_DEP_POLICY }`

Display name: Apple Deployment Program profile assigned

- **Web element:** `PROFILE_ASSIGN_TIME`
- **Macros:** `${ device.PROFILE_ASSIGN_TIME }`

Display name: Apple Deployment Program profile pushed

- **Web element:** `PROFILE_PUSH_TIME`
- **Macros:** `${ device.PROFILE_PUSH_TIME }`

Display name: Apple Deployment Program profile removed

- **Web element:** `PROFILE_REMOVE_TIME`
- **Macros:** `${ device.PROFILE_REMOVE_TIME }`

Display name: Apple Deployment Program registration by

- **Web element:** `DEVICE_ASSIGNED_BY`
- **Macros:** `${ device.DEVICE_ASSIGNED_BY }`

Display name: Apple Deployment Program registration date

- **Web element:** `DEVICE_ASSIGNED_DATE`
- **Macros:** `${ device.DEVICE_ASSIGNED_DATE }`

Display name: Description

- **Web element:** `DESCRIPTION`
- **Macros:** `${ device.DESCRIPTION }`

Display name: Device model

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** SYSTEM_OEM
- **Macros:** ${ device.SYSTEM_OEM }

Display name: Device name

- **Web element:** DEVICE_NAME
- **Macros:** ${ device.DEVICE_NAME }

Display name: Device Type

- **Web element:** DEVICE_TYPE
- **Macros:** ${ device.DEVICE_TYPE }

Display name: Do Not Disturb activated

- **Web element:** DO_NOT_DISTURB
- **Macros:** ${ device.DO_NOT_DISTURB }

Display name: ELAM Driver Loaded?

- **Web element:** WINDOWS_HAS_ELAM_DRIVER_LOADED
- **Macros:** ${ device.WINDOWS_HAS_ELAM_DRIVER_LOADED }

Display name: Encryption Compliance

- **Web element:** ENCRYPTION_COMPLIANCE
- **Macros:** ${ device.ENCRYPTION_COMPLIANCE }

Display name: ENROLLMENT_KEY_GENERATION_DATE

- **Web element:** ENROLLMENT_KEY_GENERATION_DATE
- **Macros:** ${ device.ENROLLMENT_KEY_GENERATION_DATE }

Display name: Enterprise ID

- **Web element:** ENTERPRISEID
- **Macros:** ${ device.ENTERPRISEID }

Display name: External storage 1: available space

- **Web element:** EXTERNAL_STORAGE1_FREE_SPACE
- **Macros:** ${ device.EXTERNAL_STORAGE1_FREE_SPACE }

Display name: External storage 1: available space

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `EXTERNAL_STORAGE1_FREE_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE1_FREE_SPACE }`

Display name: External storage 1: name

- **Web element:** `EXTERNAL_STORAGE1_NAME`
- **Macros:** `${ device.EXTERNAL_STORAGE1_NAME }`

Display name: External storage 1: total space

- **Web element:** `EXTERNAL_STORAGE1_TOTAL_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE1_TOTAL_SPACE }`

Display name: External storage 2: available space

- **Web element:** `EXTERNAL_STORAGE2_FREE_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE2_FREE_SPACE }`

Display name: External storage 2: name

- **Web element:** `EXTERNAL_STORAGE2_NAME`
- **Macros:** `${ device.EXTERNAL_STORAGE2_NAME }`

Display name: External storage 2: total space

- **Web element:** `EXTERNAL_STORAGE2_TOTAL_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE2_TOTAL_SPACE }`

Display name: External storage encrypted

- **Web element:** `EXTERNAL_ENCRYPTION`
- **Macros:** `${ device.EXTERNAL_ENCRYPTION }`

Display name: FileVault Enabled

- **Web element:** `IS_FILEVAULT_ENABLED`
- **Macros:** `${ device.IS_FILEVAULT_ENABLED }`

Display name: Firewall Status

- **Web element:** `DEVICE_FIREWALL_STATUS`
- **Macros:** `${ device.DEVICE_FIREWALL_STATUS }`

Display name: Firewall Status

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `DEVICE_FIREWALL_STATUS`
- **Macros:** `${ device.DEVICE_FIREWALL_STATUS }`

Display name: Firewall Status

- **Web element:** `FIREWALL_STATUS`
- **Macros:** `${ device.FIREWALL_STATUS }`

Display name: Firmware version

- **Web element:** `FIRMWARE_VERSION`
- **Macros:** `${ device.FIRMWARE_VERSION }`

Display name: First synchronization

- **Web element:** `ZMSP_FIRST_SYNC`
- **Macros:** `${ device.ZMSP_FIRST_SYNC }`

Display name: Google Directory Alias

- **Web element:** `GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS }`

Display name: Google Directory Family Name

- **Web element:** `GOOGLE_AW_DIRECTORY_FAMILY_NAME`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_FAMILY_NAME }`

Display name: Google Directory Name

- **Web element:** `GOOGLE_AW_DIRECTORY_NAME`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_NAME }`

Display name: Google Directory Primary Email

- **Web element:** `GOOGLE_AW_DIRECTORY_PRIMARY`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_PRIMARY }`

Display name: Google Directory User ID

- **Web element:** `GOOGLE_AW_DIRECTORY_USER_ID`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_USER_ID }`

Display name: GPS altitude

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `GPS_ALTITUDE_FROM_GPS`
- **Macros:** `${ device.GPS_ALTITUDE_FROM_GPS }`

Display name: GPS course

- **Web element:** `GPS_COURSE_FROM_GPS`
- **Macros:** `${ device.GPS_COURSE_FROM_GPS }`

Display name: GPS horizontal accuracy

- **Web element:** `GPS_HORIZONTAL_ACCURACY_FROM_GPS`
- **Macros:** `${ device.GPS_HORIZONTAL_ACCURACY_FROM_GPS }`

Display name: GPS latitude

- **Web element:** `GPS_LATITUDE_FROM_GPS`
- **Macros:** `${ device.GPS_LATITUDE_FROM_GPS }`

Display name: GPS longitude

- **Web element:** `GPS_LONGITUDE_FROM_GPS`
- **Macros:** `${ device.GPS_LONGITUDE_FROM_GPS }`

Display name: GPS speed

- **Web element:** `GPS_SPEED_FROM_GPS`
- **Macros:** `${ device.GPS_SPEED_FROM_GPS }`

Display name: GPS timestamp

- **Web element:** `GPS_TIMESTAMP_FROM_GPS`
- **Macros:** `${ device.GPS_TIMESTAMP_FROM_GPS }`

Display name: GPS vertical accuracy

- **Web element:** `GPS_VERTICAL_ACCURACY_FROM_GPS`
- **Macros:** `${ device.GPS_VERTICAL_ACCURACY_FROM_GPS }`

Display name: Hardware Device ID

- **Web element:** `HW_DEVICE_ID`
- **Macros:** `${ device.HW_DEVICE_ID }`

Display name: Hardware encryption capabilities

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `HARDWARE_ENCRYPTION_CAPS`
- **Macros:** `${ device.HARDWARE_ENCRYPTION_CAPS }`

Display name: HAS_CONTAINER

- **Web element:** `HAS_CONTAINER`
- **Macros:** `${ device.HAS_CONTAINER }`

Display name: Hash of the Apple App Store account currently logged on

- **Web element:** `ITUNES_STORE_ACCOUNT_HASH`
- **Macros:** `${ device.ITUNES_STORE_ACCOUNT_HASH }`

Display name: Home carrier network

- **Web element:** `SIM_CARRIER_NETWORK`
- **Macros:** `${ device.SIM_CARRIER_NETWORK }`

Display name: Home mobile country code

- **Web element:** `SIM_MCC`
- **Macros:** `${ device.SIM_MCC }`

Display name: Home mobile network code

- **Web element:** `SIM_MNC`
- **Macros:** `${ device.SIM_MNC }`

Display name: ICCID

- **Web element:** `ICCID`
- **Macros:** `${ device.ICCID }`

Display name: Identity

- **Web element:** `AS_DEVICE_IDENTITY`
- **Macros:** `${ device.AS_DEVICE_IDENTITY }`

Display name: IMEI/MEID number

- **Web element:** `IMEI`
- **Macros:** `${ device.IMEI }`

Display name: IMSI

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `SIM_ID`
- **Macros:** `${ device.SIM_ID }`

Display name: Internal storage encrypted

- **Web element:** `LOCAL_ENCRYPTION`
- **Macros:** `${ device.LOCAL_ENCRYPTION }`

Display name: IP location

- **Web element:** `IP_LOCATION`
- **Macros:** `${ device.IP_LOCATION }`

Display name: IPV4 Address

- **Web element:** `IP_ADDRESSV4`
- **Macros:** `${ device.IP_ADDRESSV4 }`

Display name: IPV6 Address

- **Web element:** `IP_ADDRESSV6`
- **Macros:** `${ device.IP_ADDRESSV6 }`

Display name: Issued At

- **Web element:** `WINDOWS_HAS_ISSUED_AT`
- **Macros:** `${ device.WINDOWS_HAS_ISSUED_AT }`

Display name: Jailbroken/Rooted

- **Web element:** `ROOT_ACCESS`
- **Macros:** `${ device.ROOT_ACCESS }`

Display name: Kernel Debugging Enabled?

- **Web element:** `WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED }`

Display name: Kiosk mode

- **Web element:** `IS_KIOSK`
- **Macros:** `${ device.IS_KIOSK }`

Display name: Last known IP address

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `LAST_IP_ADDR`
- **Macros:** `${ device.LAST_IP_ADDR }`

Display name: Last policy update time

- **Web element:** `LAST_POLICY_UPDATE_TIME`
- **Macros:** `${ device.LAST_POLICY_UPDATE_TIME }`

Display name: Last scan date

- **Web element:** `PreviousScanDate`
- **Macros:** `${ device.PreviousScanDate }`

Display name: Last scan result

- **Web element:** `PreviousScanResult`
- **Macros:** `${ device.PreviousScanResult }`

Display name: Last scheduled software updates

- **Web element:** `AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME`
- **Macros:** `${ device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME }`

Display name: Last scheduled software updates failure message

- **Web element:** `AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG`
- **Macros:** `${ device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG }`

Display name: Last scheduled software updates status

- **Web element:** `AVAILABLE_OS_UPDATE_INSTALL_STATUS`
- **Macros:** `${ device.AVAILABLE_OS_UPDATE_INSTALL_STATUS }`

Display name: Last synchronization

- **Web element:** `ZMSP_LAST_SYNC`
- **Macros:** `${ device.ZMSP_LAST_SYNC }`

Display name: Locator service enabled

- **Web element:** `DEVICE_LOCATOR`
- **Macros:** `${ device.DEVICE_LOCATOR }`

Display name: MAC Address

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `MAC_ADDRESS`
- **Macros:** `${ device.MAC_ADDRESS }`

Display name: MAC Address Network Connection

- **Web element:** `MAC_NETWORK_CONNECTION`
- **Macros:** `${ device.MAC_NETWORK_CONNECTION }`

Display name: MAC Address Type

- **Web element:** `MAC_ADDRESS_TYPE`
- **Macros:** `${ device.MAC_ADDRESS_TYPE }`

Display name: Mailbox Setup

- **Web element:** `GOOGLE_AW_DIRECTORY_MAILBOX_SETUP`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP }`

Display name: Main battery

- **Web element:** `MAIN_BATTERY_PERCENT`
- **Macros:** `${ device.MAIN_BATTERY_PERCENT }`

Display name: MDM lost mode enabled

- **Web element:** `IS_MDM_LOST_MODE_ENABLED`
- **Macros:** `${ device.IS_MDM_LOST_MODE_ENABLED }`

Display name: MDX_SHARED_ENCRYPTION_KEY

- **Web element:** `MDX_SHARED_ENCRYPTION_KEY`
- **Macros:** `${ device.MDX_SHARED_ENCRYPTION_KEY }`

Display name: MEID

- **Web element:** `MEID`
- **Macros:** `${ device.MEID }`

Display name: Mobile phone number

- **Web element:** `TEL_NUMBER`
- **Macros:** `${ device.TEL_NUMBER }`

Display name: Model ID

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `MODEL_ID`
- **Macros:** `${ device.MODEL_ID }`

Display name: Model Number

- **Web element:** `MODEL_NUMBER`
- **Macros:** `${ device.MODEL_NUMBER }`

Display name: Network Adapter Type

- **Web element:** `NETWORK_ADAPTER_TYPE`
- **Macros:** `${ device.NETWORK_ADAPTER_TYPE }`

Display name: Operating system build

- **Web element:** `SYSTEM_OS_BUILD`
- **Macros:** `${ device.SYSTEM_OS_BUILD }`

Display name: Operating System Edition

- **Web element:** `OS_EDITION`
- **Macros:** `${ device.OS_EDITION }`

Display name: Operating system language (locale)

- **Web element:** `SYSTEM_LANGUAGE`
- **Macros:** `${ device.SYSTEM_LANGUAGE }`

Display name: Operating system version

- **Web element:** `SYSTEM_OS_VERSION`
- **Macros:** `${ device.SYSTEM_OS_VERSION }`

Display name: Organization address

- **Web element:** `ORGANIZATION_ADDRESS`
- **Macros:** `${ device.ORGANIZATION_ADDRESS }`

Display name: Organization email

- **Web element:** `ORGANIZATION_EMAIL`
- **Macros:** `${ device.ORGANIZATION_EMAIL }`

Display name: Organization magic

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `ORGANIZATION_MAGIC`
- **Macros:** `${ device.ORGANIZATION_MAGIC }`

Display name: Organization name

- **Web element:** `ORGANIZATION_NAME`
- **Macros:** `${ device.ORGANIZATION_NAME }`

Display name: Organization phone number

- **Web element:** `ORGANIZATION_PHONE`
- **Macros:** `${ device.ORGANIZATION_PHONE }`

‘**Display name:** Out of Compliance

- **Web element:** `OUT_OF_COMPLIANCE`
- **Macros:** `${ device.OUT_OF_COMPLIANCE }`

Display name: Owned by

- **Web element:** `CORPORATE_OWNED`
- **Macros:** `${ device.CORPORATE_OWNED }`

Display name: Passcode compliant

- **Web element:** `PASSCODE_IS_COMPLIANT`
- **Macros:** `${ device.PASSCODE_IS_COMPLIANT }`

Display name: Passcode compliant with configuration

- **Web element:** `PASSCODE_IS_COMPLIANT_WITH_CFG`
- **Macros:** `${ device.PASSCODE_IS_COMPLIANT_WITH_CFG }`

Display name: Passcode present

- **Web element:** `PASSCODE_PRESENT`
- **Macros:** `${ device.PASSCODE_PRESENT }`

Display name: PCR0

- **Web element:** `WINDOWS_HAS_PCR0`
- **Macros:** `${ device.WINDOWS_HAS_PCR0 }`

Display name: Perimeter breach

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `GPS_PERIMETER_BREACH`
- **Macros:** `${ device.GPS_PERIMETER_BREACH }`

Display name: Periodic check

- **Web element:** `PerformPeriodicCheck`
- **Macros:** `${ device.PerformPeriodicCheck }`

Display name: Personal Hotspot activated

- **Web element:** `PERSONAL_HOTSPOT_ENABLED`
- **Macros:** `${ device.PERSONAL_HOTSPOT_ENABLED }`

Display name: PIN code for geofence

- **Web element:** `PIN_CODE_FOR_GEO_FENCE`
- **Macros:** `${ device.PIN_CODE_FOR_GEO_FENCE }`

Display name: Platform

- **Web element:** `SYSTEM_PLATFORM`
- **Macros:** `${ device.SYSTEM_PLATFORM }`

Display name: Platform API level

- **Web element:** `API_LEVEL`
- **Macros:** `${ device.API_LEVEL }`

Display name: Policy name

- **Web element:** `POLICY_NAME`
- **Macros:** `${ device.POLICY_NAME }`

Display name: Primary Phone Number

- **Web element:** `IDENTITY1_PHONENUMBER`
- **Macros:** `${ device.IDENTITY1_PHONENUMBER }`

Display name: Primary SIM Carrier Operator

- **Web element:** `IDENTITY1_CARRIER_NETWORK_OPERATOR`
- **Macros:** `${ device.IDENTITY1_CARRIER_NETWORK_OPERATOR }`

Display name: Primary SIM ICCID

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** IDENTITY1_ICCID
- **Macros:** ${ device.IDENTITY1_ICCID }

Display name: Primary SIM IMEI

- **Web element:** IDENTITY1_IMEI
- **Macros:** ${ device.IDENTITY1_IMEI }

Display name: Primary SIM IMSI

- **Web element:** IDENTITY1_IMSI
- **Macros:** ${ device.IDENTITY1_IMSI }

Display name: Primary SIM Roaming

- **Web element:** IDENTITY1_ROAMING
- **Macros:** ${ device.IDENTITY1_ROAMING }

Display name: Primary SIM Roaming

- **Web element:** IDENTITY1_ROAMING_COMPLIANCE
- **Macros:** ${ device.IDENTITY1_ROAMING_COMPLIANCE }

Display name: Product name

- **Web element:** PRODUCT_NAME
- **Macros:** ${ device.PRODUCT_NAME }

Display name: Publisher Device ID

- **Web element:** PUBLISHER_DEVICE_ID
- **Macros:** ${ device.PUBLISHER_DEVICE_ID }

Display name: Reset Count

- **Web element:** WINDOWS_HAS_RESET_COUNT
- **Macros:** ${ device.WINDOWS_HAS_RESET_COUNT }

Display name: Restart Count

- **Web element:** WINDOWS_HAS_RESTART_COUNT
- **Macros:** ${ device.WINDOWS_HAS_RESTART_COUNT }

Display name: Safe Mode Enabled?

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `WINDOWS_HAS_SAFE_MODE`
- **Macros:** `${ device.WINDOWS_HAS_SAFE_MODE }`

Display name: SBCP Hash

- **Web element:** `WINDOWS_HAS_SBCP_HASH`
- **Macros:** `${ device.WINDOWS_HAS_SBCP_HASH }`

Display name: Screen: height

- **Web element:** `SCREEN_HEIGHT`
- **Macros:** `${ device.SCREEN_HEIGHT }`

Display name: Screen: number of colors

- **Web element:** `SCREEN_NB_COLORS`
- **Macros:** `${ device.SCREEN_NB_COLORS }`

Display name: Screen: size

- **Web element:** `SCREEN_SIZE`
- **Macros:** `${ device.SCREEN_SIZE }`

Display name: Screen: width

- **Web element:** `SCREEN_WIDTH`
- **Macros:** `${ device.SCREEN_WIDTH }`

Display name: Screen: X-axis resolution

- **Web element:** `SCREEN_XDPI`
- **Macros:** `${ device.SCREEN_XDPI }`

Display name: Screen: Y-axis resolution

- **Web element:** `SCREEN_YDPI`
- **Macros:** `${ device.SCREEN_YDPI }`

Display name: Secondary Phone Number

- **Web element:** `IDENTITY2_PHONENUMBER`
- **Macros:** `${ device.IDENTITY2_PHONENUMBER }`

Display name: Secondary SIM Carrier Operator

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** IDENTITY2_CARRIER_NETWORK_OPERATOR
- **Macros:** ${ device.IDENTITY2_CARRIER_NETWORK_OPERATOR }

Display name: Secondary SIM ICCID

- **Web element:** IDENTITY2_ICCID
- **Macros:** ${ device.IDENTITY2_ICCID }

Display name: Secondary SIM IMEI

- **Web element:** IDENTITY2_IMEI
- **Macros:** ${ device.IDENTITY2_IMEI }

Display name: Secondary SIM IMSI

- **Web element:** IDENTITY2_IMSI
- **Macros:** ${ device.IDENTITY2_IMSI }

Display name: Secondary SIM Roaming

- **Web element:** IDENTITY2_ROAMING
- **Macros:** ${ device.IDENTITY2_ROAMING }

Display name: Secondary SIM Roaming Compliance

- **Web element:** IDENTITY2_ROAMING_COMPLIANCE
- **Macros:** ${ device.IDENTITY2_ROAMING_COMPLIANCE }

Display name: Secure Boot Enabled?

- **Web element:** WINDOWS_HAS_SECURE_BOOT_ENABLED
- **Macros:** ${ device.WINDOWS_HAS_SECURE_BOOT_ENABLED }

Display name: Secure Boot Status

- **Web element:** SECURE_BOOT_STATE
- **Macros:** ${ device.SECURE_BOOT_STATE }

Display name: SecureContainer Enabled

- **Web element:** DLP_ACTIVE
- **Macros:** ${ device.DLP_ACTIVE }

Display name: Security patch level

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `SYSTEM_SECURITY_PATCH_LEVEL`
- **Macros:** `${ device.SYSTEM_SECURITY_PATCH_LEVEL }`

Display name: Serial number

- **Web element:** `SERIAL_NUMBER`
- **Macros:** `${ device.SERIAL_NUMBER }`

Display name: SMS capable

- **Web element:** `IS_SMS_CAPABLE`
- **Macros:** `${ device.IS_SMS_CAPABLE }`

Display name: Supervised

- **Web element:** `SUPERVISED`
- **Macros:** `${ device.SUPERVISED }`

Display name: Suspension Reason

- **Web element:** `GOOGLE_AW_DIRECTORY_SUSPENTION_REASON`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON }`

Display name: Tampered Status

- **Web element:** `TAMPERED_STATUS`
- **Macros:** `${ device.TAMPERED_STATUS }`

Display name: Terms & Conditions

- **Web element:** `TERMS_AND_CONDITIONS`
- **Macros:** `${ device.TERMS_AND_CONDITIONS }`

Display name: Terms And Agreement Accepted?

- **Web element:** `GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS }`

Display name: Test Signing Enabled?

- **Web element:** `WINDOWS_HAS_TEST_SIGNING_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_TEST_SIGNING_ENABLED }`

Display name: Total RAM

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `MEMORY`
- **Macros:** `${ device.MEMORY }`

Display name: Total storage space

- **Web element:** `TOTAL_DISK_SPACE`
- **Macros:** `${ device.TOTAL_DISK_SPACE }`

Display name: TPM version

- **Web element:** `TPM_VERSION`
- **Macros:** `${ device.TPM_VERSION }`

Display name: UDID

- **Web element:** `UDID`
- **Macros:** `${ device.UDID }`

Display name: User Account Control Status

- **Web element:** `UAC_STATUS`
- **Macros:** `${ device.UAC_STATUS }`

Display name: User agent

- **Web element:** `USER_AGENT`
- **Macros:** `${ device.USER_AGENT }`

Display name: User defined #1

- **Web element:** `USER_DEFINED_1`
- **Macros:** `${ device.USER_DEFINED_1 }`

Display name: User defined #2

- **Web element:** `USER_DEFINED_2`
- **Macros:** `${ device.USER_DEFINED_2 }`

Display name: User defined #3

- **Web element:** `USER_DEFINED_3`
- **Macros:** `${ device.USER_DEFINED_3 }`

Display name: User language (locale)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `USER_LANGUAGE`
- **Macros:** `${ device.USER_LANGUAGE }`

Display name: Vendor

- **Web element:** `VENDOR`
- **Macros:** `${ device.VENDOR }`

Display name: Voice capable

- **Web element:** `IS_VOICE_CAPABLE`
- **Macros:** `${ device.IS_VOICE_CAPABLE }`

Display name: Voice roaming allowed

- **Web element:** `VOICE_ROAMING_ENABLED`
- **Macros:** `${ device.VOICE_ROAMING_ENABLED }`

Display name: VSM Enabled?

- **Web element:** `WINDOWS_HAS_VSM_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_VSM_ENABLED }`

Display name: Wi-Fi MAC address

- **Web element:** `WIFI_MAC`
- **Macros:** `${ device.WIFI_MAC }`

Display name: WINDOWS_ENROLLMENT_KEY

- **Web element:** `WINDOWS_ENROLLMENT_KEY`
- **Macros:** `${ device.WINDOWS_ENROLLMENT_KEY }`

Display name: WinPE Enabled?

- **Web element:** `WINDOWS_HAS_WINPE`
- **Macros:** `${ device.WINDOWS_HAS_WINPE }`

Display name: WNS Notification Status

- **Web element:** `PROPERTY_WNS_PUSH_STATUS`
- **Macros:** `${ device.PROPERTY_WNS_PUSH_STATUS }`

Display name: WNS Notification URL

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web element:** `PROPERTY_WNS_PUSH_URL`
- **Macros:** `${ device.PROPERTY_WNS_PUSH_URL }`

Display name: WNS Notification URL expiry date

- **Web element:** `PROPERTY_WNS_PUSH_URL_EXPIRY`
- **Macros:** `${ device.PROPERTY_WNS_PUSH_URL_EXPIRY }`

Display name: Citrix Endpoint Management agent ID

- **Web element:** `ENROLLMENT_AGENT_ID`
- **Macros:** {device.ENROLLMENT_AGENT_ID}‘

Display name: Citrix Endpoint Management agent revision

- **Web element:** `EW\\_REVISION`
- **Macros:** `\${ device.EW\\_REVISION }`

Display name: Citrix Endpoint Management agent version

- **Web element:** `EW\\_VERSION`
- **Macros:** `\${ device.EW\\_VERSION }`

Display name: Zebra API available

- **Web element:** `ZEBRA\\_MDM`
- **Macros:** `\${ device.ZEBRA\\_MDM }`

Display name: Zebra MXMF version

- **Web element:** `ZEBRA\\_MDM\\_VERSION`
- **Macros:** `\${ device.ZEBRA\\_MDM\\_VERSION }`

Display name: Zebra Patch version

- **Web element:** `ZEBRA\\_PATCH\\_VERSION`
- **Macros:** `\${ device.ZEBRA\\_PATCH\\_VERSION }`

Macros to get built-in user properties

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Display name	Macros
domainname (domain name; default domain)	\${ user.domainname }
loginname (user name plus domain name)	\${ user.loginname }
username (login name minus the domain, if any)	\${ user.username }

Macros for all user properties

Display name	Web element	Macros
Active Directory failed logon tries	badpwdcount	\${ user.badpwdcount }
ActiveSync user email	asuseremail	\${ user.asuseremail }
ASM data source	asmpersonsource	\${ user.asmpersonsource }
ASM Deployment Program account name	asmdepaccount	\${ user.asmdepaccount }
ASM managed Apple ID	asmpersonmanagedappleid	\${ user.asmpersonmanagedappleid }
ASM passcode type	asmpersonpasscodetype	\${ user.asmpersonpasscodetype }
ASM person ID	asmpersonid	\${ user.asmpersonid }
ASM person status	asmpersonstatus	\${ user.asmpersonstatus }
ASM person title	asmpersontitle	\${ user.asmpersontitle }
ASM person unique ID	asmpersonuniqueid	\${ user.asmpersonuniqueid }

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Display name	Web element	Macros
ASM source system ID	asmpersonsourcesystemid	\${ user.asmpersonsourcesystemid }
ASM student grade	asmpersongrade	\${ user.asmpersongrade }
BES user email	besuseremail	\${ user.besuseremail }
Company	company	\${ user.company }
Company name	companyname	\${ user.companyname }
Country	c	\${ user.c }
Department	department	\${ user.department }
Description	description	\${ user.description }
Disabled user	disableduser	\${ user.disableduser }
Display name	displayname	\${ user.displayname }
Distinguished name	distinguishedname	\${ user.distinguishedname }
Domain name	domainname	\${ user.domainname }
Email	mail	\${ user.mail }
First name	givenname	\${ user.givenname }
Home address	homestreetaddress	\${ user.homestreetaddress }
Home city	homecity	\${ user.homecity }
Home country	homecountry	\${ user.homecountry }
Home fax	homefax	\${ user.homefax }
Home phone	homephone	\${ user.homephone }
Home state/region	homestate	\${ user.homestate }

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Display name	Web element	Macros
Home zip or post code	homezip	\${ user.homezip }
IP phone	ipphone	\${ user.ipphone }
Middle initial	middleinitial	\${ user.middleinitial }
Middle name	middlename	\${ user.middlename }
Mobile	mobile	\${ user.mobile }
Name	cn	\${ user.cn }
Office address	physicaldeliveryofficename	\${ user.physicaldeliveryofficename }
Office city	l	\${ user.l }
Office fax number	facsimiletelephonenumber	\${ user.facsimiletelephonenumber }
Office state/province	st	\${ user.st }
Office street address	officestreetaddress	\${ user.officestreetaddress }
Office telephone number	telephonenumber	\${ user.telephonenumber }
Office zip or post code	postalcode	\${ user.postalcode }
P.O. box	postofficebox	\${ user.postofficebox }
Pager	pager	\${ user.pager }
Primary group ID	primarygroupid	\${ user.primarygroupid }
SAM account	samaccountname	\${ user.samaccountname }
Street address	streetaddress	\${ user.streetaddress }
Surname	sn	\${ user.sn }
Title	title	\${ user.title }

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Display name	Web element	Macros
User logon name	`userprincipalname`	`\${ user.userprincipalname }`

Automated actions

February 20, 2024

You create automated actions in Citrix Endpoint Management to program a reaction to:

- Events
- User or device properties
- The existence of apps on user devices

When you create an automated action, the triggers defined for the action determine what happens on the user device when it is connected to Citrix Endpoint Management. When an event is triggered, you can send a notification to the user to correct an issue before more serious action is taken.

The effects that you set to happen automatically range from the following:

- Fully or selectively wiping the device.
- Setting the device to out of compliance.
- Revoking the device.
- Sending a notification to the user to correct an issue before more severe action is taken.

You can configure app lock and app wipe actions for MAM-only mode.

You can use automated actions to mark Windows 10 and Windows 11 devices joined to Azure Active Directory (AD) out of compliance in Azure AD.

> **Note:**
>
> Before you can notify users, you must configure notification servers in the Citrix Endpoint Management settings for SMTP so that Citrix Endpoint Management can send the messages. For more information, see Notifications. Set up any notification templates you plan to use before proceeding. For more information, see Notifications. Set u, see Create, and update notification templates.

Example actions

Here are some examples of using automated actions:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Example one

- You want to detect an app that you previously blocked (for example, "Words with Friends"). You can specify a trigger that sets the user device out of compliance after detecting the "Words with Friends"app. The action then notifies users that they must remove the app to bring their device back into compliance. You can also set a time limit for how long to wait for users to comply. After that time limit, a defined action occurs, such as selectively wiping the device.

Example two

- You want to verify if customers are using the latest firmware and block access to resources if users have to update their devices. You can specify a trigger that sets the user device out of compliance when a user device doesn't have the latest version. You use automated actions to block resources and to notify customers.

Example three

- A user device is put into an out-of-compliance state and the user then fixes the device. You can configure a policy to deploy a package that resets the device into a compliant state.

Example four

- You want to mark user devices that have been inactive for a certain time period as out of compliance. You can create an automated action for inactive devices as follows:

    1. In the Citrix Endpoint Management console, go to **Settings > Network Access Control** and then select **Inactive Devices**. For more information about the **Inactive Devices** setting, see Network Access Control.
    2. Follow the steps to add an action, as outlined in Add, and manage actions. The only difference is that you configure the settings as follows on the **Action details** page:
        - **Trigger**. Select **Device property**, **Out of compliance**, and **True**.
        - **Action**. Select **Send notification** and select a template that you created by using **Notification Template** in **Settings**. Then set the delay in days, hours, or minutes before doing the action. Set the interval at which the action repeats until the user addresses the triggering issue.

    > **Tip:**
    >
    > To delete inactive devices in bulk, use the Citrix Endpoint Management Public REST API. You first manually get the device IDs for inactive devices that you want to delete and then run the delete API to delete them in bulk.

Add and manage actions

To add, edit, and filter automated actions:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. From the Citrix Endpoint Management console, click **Configure > Actions**. The **Actions** page appears.
2. On the **Actions** page, do one of the following:
   - Click **Add** to add an action.
   - Select an existing action to edit or delete. Click the option that you want to use.
3. The **Action Information** page appears.
4. On the **Action Information** page, enter or modify the following information:
   - **Name:** Type a name to identify the action. This field is required.
   - **Description:** Describe what the action is meant to do.
5. Click **Next**. The **Action details** page appears.

   The following example shows how to set up a **Event** trigger. If you select a different trigger, the resulting options differ from the options shown here.

6. On the **Action details** page, enter or modify the following information:

   In the **Trigger** list, click the event trigger type for this action. Select one of the following triggers:
   - **Event:** Checks whether the device status matches the non-compliance event you choose, then reacts to it.
   - **Device property:** Checks for a specific value for a device attribute on a device that is MDM-managed, then reacts to it. For more information, see the Device property names and values PDF.
   - **User property:** Reacts to a specific value for a user attribute, usually from Active Directory.

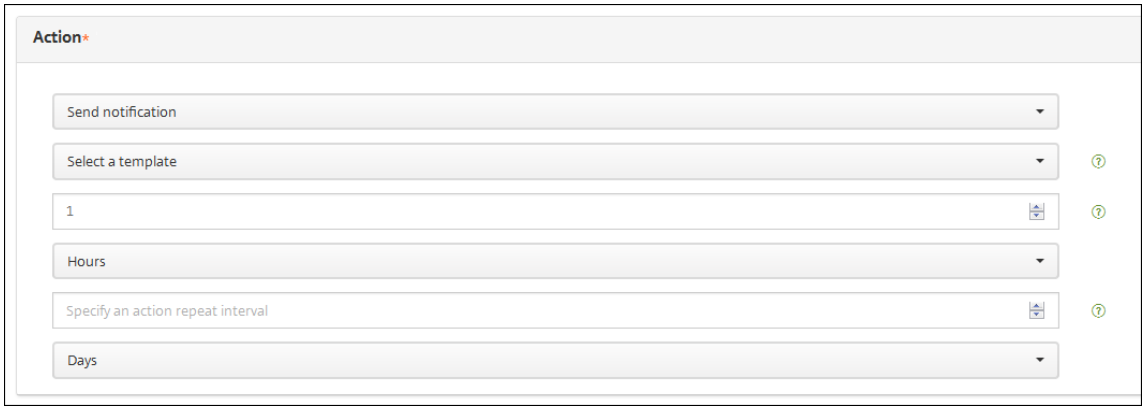
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Installed app name:** Reacts to an app being installed. Doesn't apply to MAM-only mode. Requires the app inventory policy to be enabled on the device. The app inventory policy is enabled on all platforms by default. For details, see App inventory device policy.
- **Policy returned value:** Checks if the value returned from PowerShell scripts meets certain logic criteria. The Windows Agent policy must be enabled and configured. For more information on the Windows Agent policy, see Windows Agent device policy.

7. In the next list, click the response to the trigger.
8. In the **Action** list, click the action to be done when the trigger criterion is met. Except for the **Send notification** action, you choose a time frame in which users can resolve the issue that caused the trigger. If the issue isn't resolved within that time frame, the selected action is taken. For a definition of the actions, see Security actions.

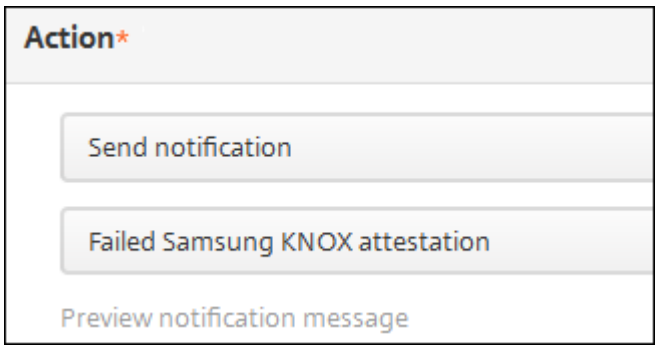
   If you pick **Send notification**, use the following steps to send a notification action.
9. In the next list, select the template to use for the notification. Notification templates relevant to the selected event appear. If there's no template for the notification type, you are prompted to configure a template with the message: No template for this event type. Create a template using **Notification Template** in **Settings**.

   To notify users, use **Settings > Notification Server** to configure settings for SMTP so that Citrix Endpoint Management can send the messages. See Notifications. Also, before proceeding, use **Settings > Notification Template** to set up any notification templates you plan to use. See Create and update notification templates.



   After you select the template, click **Preview notification message**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



10. In the following fields, set the delay in days, hours, or minutes before doing the action. Set the interval at which the action repeats until the user addresses the triggering issue.

11. In **Summary**, verify that you created the automated action as you intended.

12. After you configure the action details, you can configure the deployment rules for each platform individually. To do so, complete step 13 for each platform you choose.
13. Configure deployment rules. For general information about configuring deployment rules, see Deploy resources.

    For this example:

    - Device ownership must be **BYOD**.
    - The device must be passcode compliant.
    - Device mobile country code cannot be only Andorra.

14. When you are done configuring the platform deployment rules for the action, click **Next**. The **Actions assignment** page appears, where you assign the action to a delivery group or groups. This step is optional.
15. Next to **Choose delivery groups**, type to find a delivery group or select groups in the list. The groups you select appear in the **Delivery groups to receive app assignment** list.
16. Expand **Deployment Schedule** and then configure the following settings:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Next to **Deploy**, click **On** to schedule deployment or click **Off** to prevent deployment. The default option is set as **On**. If you choose **Off**, no other options are required.
- Next to **Deployment schedule**, click **Now**, or **Later**. The default option is set as **Now**.
- If you click **Later**, click the calendar icon and then select the date and time for deployment.
- Next to **Deployment condition**, click **On every connection**, or **Only when previous deployment has failed**. The default option is set as **On every connection**.
- Next to **Deploy for always-on connection**, click **On**, or **Off**. The default option is set as **Off**.

  This option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.

  > **Note:**
  >
  > This option applies when you have configured the scheduling background deployment key in **Settings > Server Properties**.
  >
  > The always-on option:
  >
  > - Is not available for iOS devices
  > - Is not available for Android and Android Enterprise customers who began using Citrix Endpoint Management with version 10.18.19 or later
  > - Is not recommended for Android and Android Enterprise customers who began using Citrix Endpoint Management with before version 10.18.19
  >
  > The deployment schedule that you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

17. Click **Next**. The **Summary** page appears, where you can verify the action configuration.
18. Click **Save** to save the action.

App lock and app wipe actions for MAM-only mode

You can wipe or lock apps on a device for all four categories of triggers listed in the Citrix Endpoint Management console: event, device property, user property, and installed app name.

To configure an automatic app wipe or app lock

1. In the Citrix Endpoint Management console, click **Configure > Actions**.
2. On the **Actions** page, click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. On the **Action Information** page, enter a name for the action and an optional description.
4. On the **Action Details** page, select the trigger you want.
5. In **Action**, select an action.

   For this step, keep the following conditions in mind:

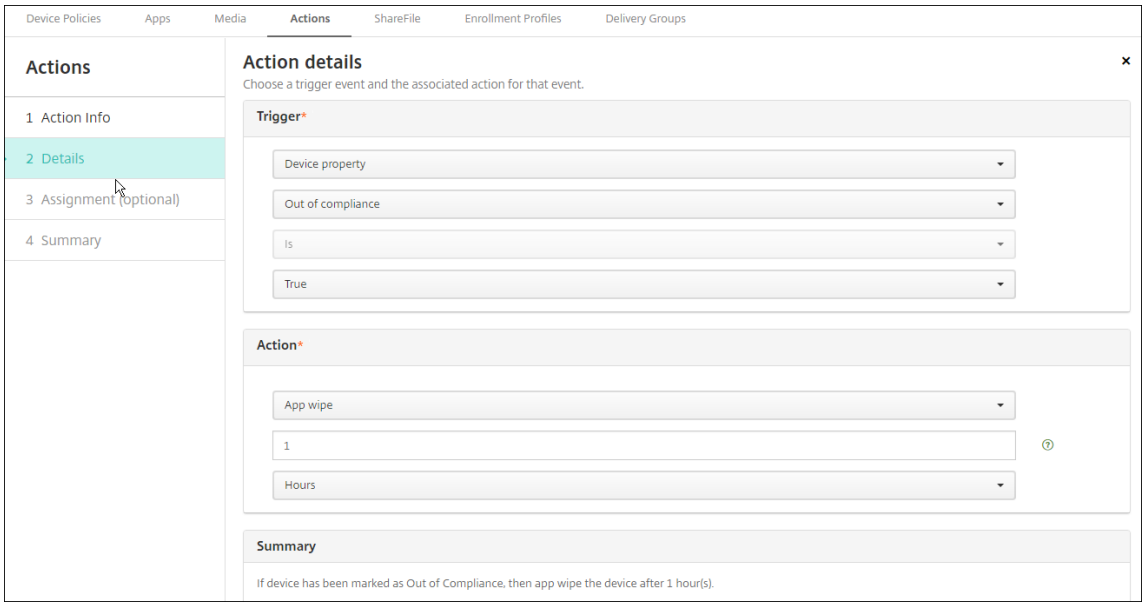
   When the trigger type is set as **Event** and the value is not **Active Directory disabled user**, the **App wipe** and **App lock** actions don't appear.

   When the trigger type is set as **Device property** and the value is **MDM lost mode enabled**, the following actions don't appear:

   - Selectively wipe the device
   - Completely wipe the device
   - Revoke the device

   For each option, a 1 hour delay is automatically set, but you can select the delay period in minutes, hours or days. The intent of the delay is to give users time to fix an issue before the action occurs. For more information about the App wipe and App lock actions, see Security actions.

   > **Note:**
   >
   > If you set the trigger to **event**, the repeat interval is automatically a minimum of 1 hour. The device must carry out a refresh of the policies to synchronize with the server for the notification to come in. Typically, a device synchronizes with the server when users sign on or manually refresh their policies through Citrix Secure Hub.
   >
   > An extra delay of approximately 1 hour might occur before any action is carried out, to allow the Active Directory database to synchronize with Citrix Endpoint Management.

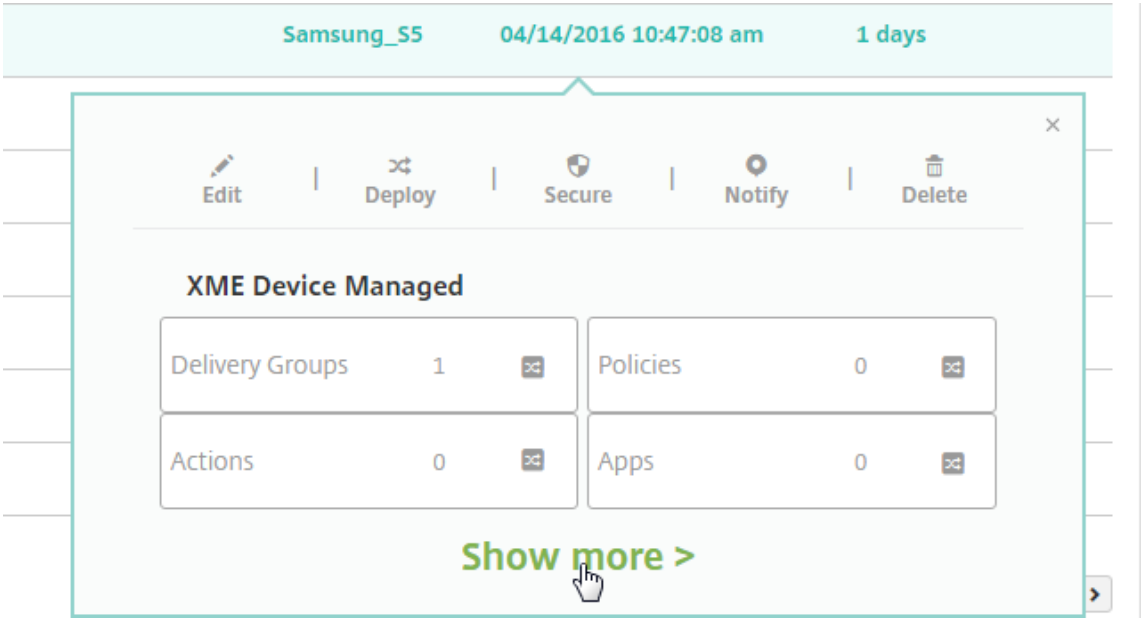


© 1997–2025 Citrix Systems, Inc. All rights reserved.

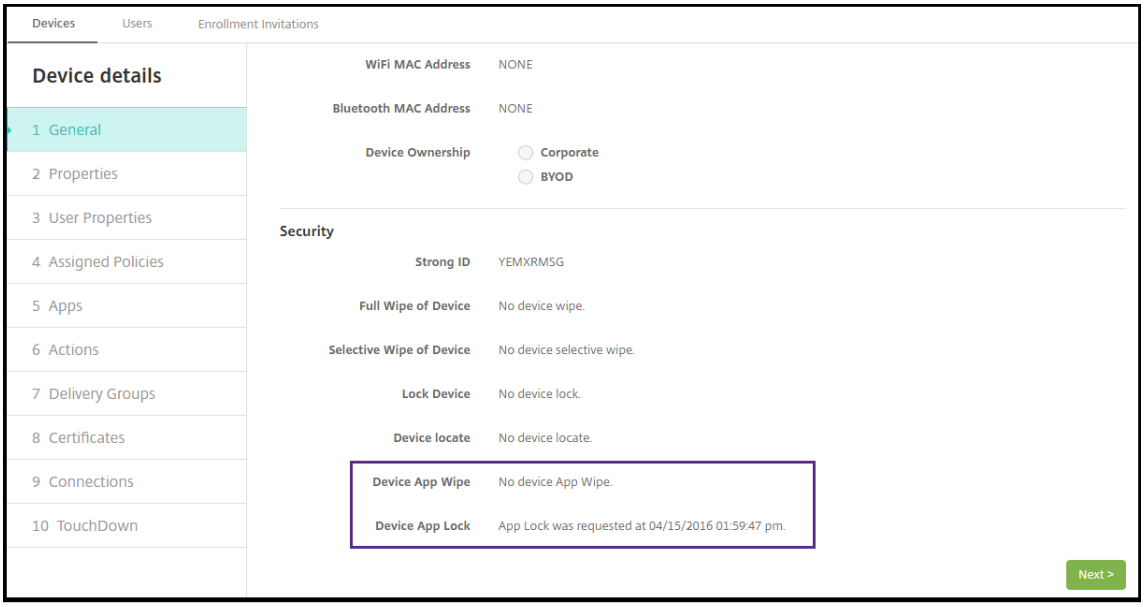
6. Configure the deployment rules and then click **Next**.
7. Configure delivery group assignments and a deployment schedule and then click **Next**.
8. Click **Save**.

To check app lock or app wipe status

1. Go to **Manage > Devices**, click a device, and then click **Show more**.

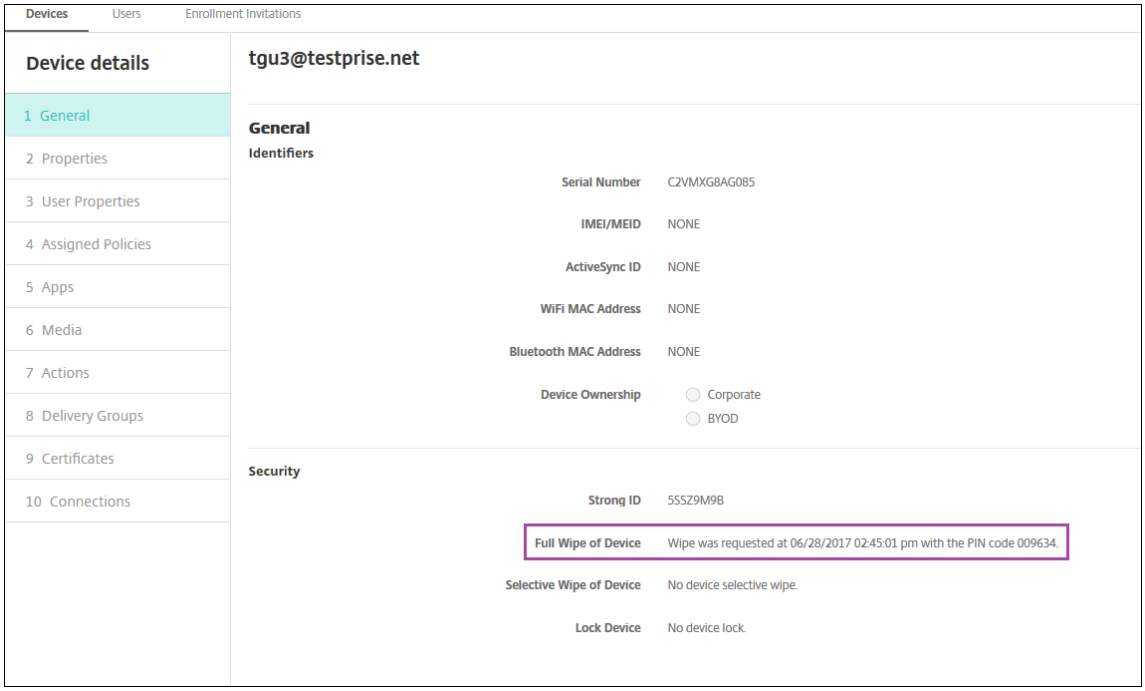


2. Scroll to **Device App Wipe** and **Device App Lock**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

After a device gets wiped, the user is prompted to enter a PIN code. If the user forgets the code, you can look it up in the Device Details.



Marking Windows 10 and Windows 11 devices out of compliance in Azure AD

When Windows 10 and Windows 11 devices that are joined to Azure AD are marked out-of-compliance by Citrix Endpoint Management, they can also be marked out-of-compliance in Azure AD. To enable this functionality, add permissions to the on-premises MDM application to access the Microsoft Graph API in the Azure AD portal.

1. Log in to the Azure AD portal with your Azure AD administrator credentials.
2. In the Azure AD portal, navigate to **Azure Active Directory > Mobility (MDM and MAM)**. Choose **On-premises MDM application**.
3. Click **On-premises Application Settings > Required Permissions > Add > Select an API > Microsoft Graph**. Click **Select** and save.
4. Under **Required permissions**, select **Microsoft Graph**. Under **Enable Access**, select **Read and write directory data**.
5. Under **Required permissions**, select **Microsoft Graph**. Then click **Grant permissions**.
6. Click **Yes** to grant permission.

When an Azure AD enrolled device running Windows 10 or Windows 11 is out of compliance, Citrix Endpoint Management also marks the device as out of compliance in Azure AD.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Create an automated action based on a Windows Agent device policy result

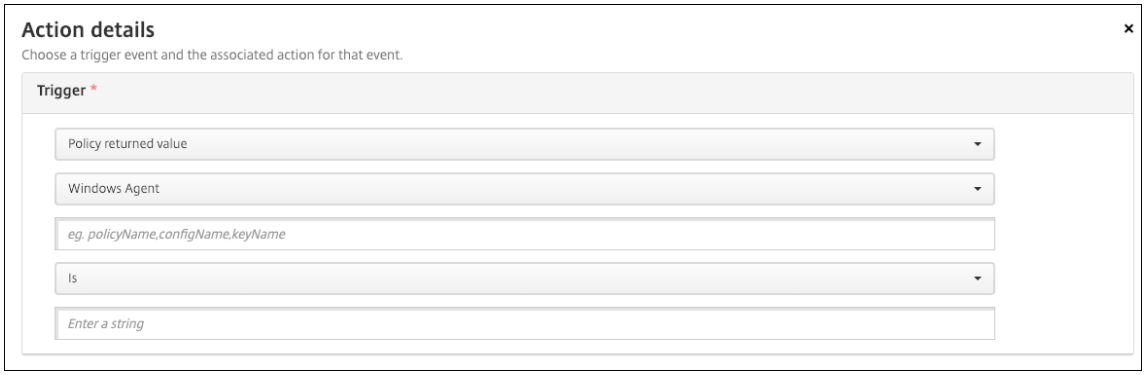
Use the Windows Agent device policy to deploy scripts that monitor registry values on managed Windows desktops and tablets. Based on the values returned from a script, you can then configure an automated action to run.

1. Configure a Windows Agent device policy and check the values returned by the script. For information on the Windows Agent device policy, see Windows Agent device policy.

   That article and this section include a sample that's based on a script named `EntApp_2019_checkFirew`. The related Windows Agent device policy defines a config named `cName_checkFirewall`. That config runs the sample script.

   After the script runs on a device, you get the info required to create an action, as described in the Windows Agent device policy.

2. In the Citrix Endpoint Management console, click **Configure > Actions**.
3. On the **Actions** page, click **Add**.
4. On the **Action Information** page, enter a name for the action and an optional description.
5. On the **Action Details** page, select the **Policy returned value** trigger.

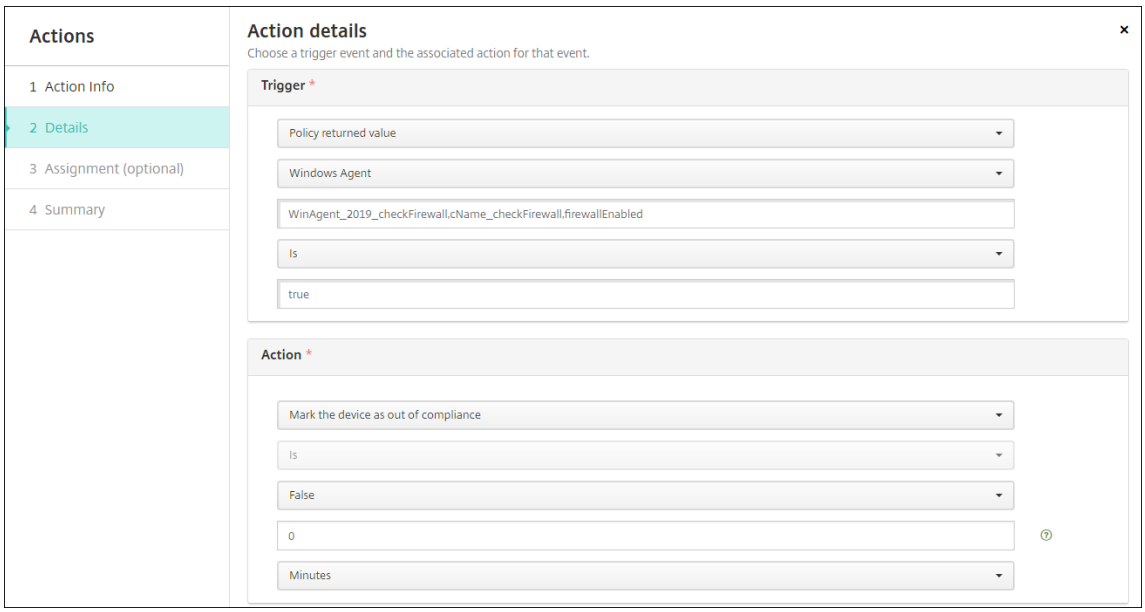


6. In the fields that appear, define the trigger and the action:

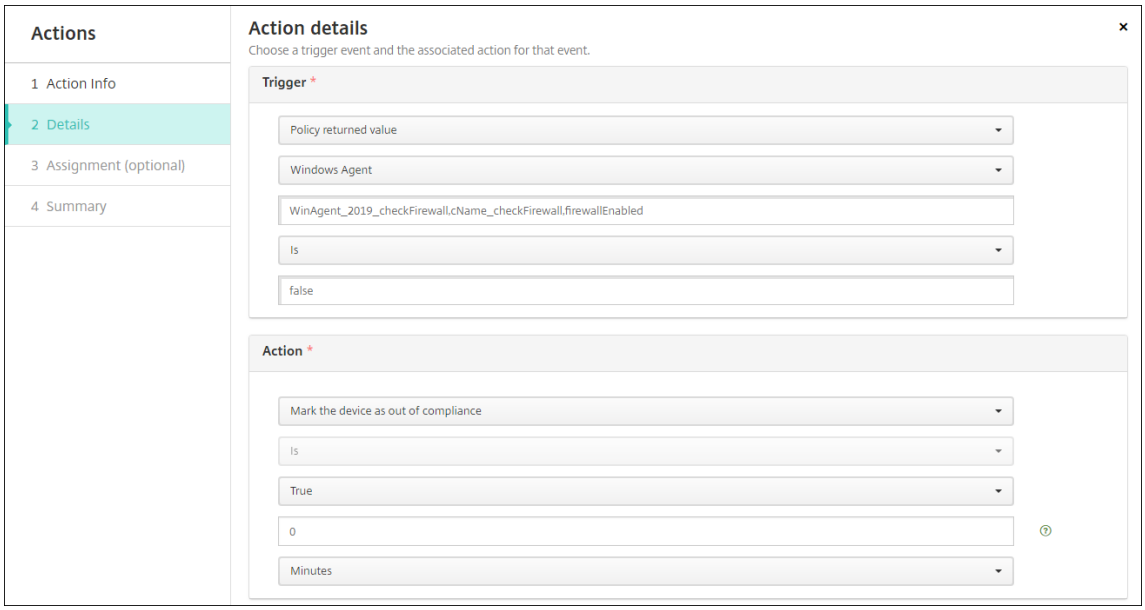
   - **Windows Agent settings:** Type the policy name, config name, and key name for the Windows Agent policy you created.
   - **Drop-down menu:** Select **Is**, **Is Not**, **Contains**, or **Does Not Contain** logic. This logic applies to the next field and causes the action to trigger if the logic applies.
   - **Enter a string:** Enter the string that resulted from running the PowerShell script uploaded in your policy. For information about finding that string, see Windows Agent device policy.
   - **Action:** Select an action, a value for the action, and choose a time frame for resolving the action.

   In our example: If the key name `firewallEnabled` returns the value **`true`**, the following action marks the device as in compliance.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



If the key name `firewallEnabled` returns the value **`false`**, the following action marks the device as out of compliance.



7. If needed, set a deployment schedule and choose delivery groups.

Monitor and support

September 6, 2025

You can use the Citrix Endpoint Management Dashboard and the Citrix Endpoint Management Sup-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

port page to monitor and troubleshoot your Citrix Endpoint Management server. Use the Citrix Endpoint Management Support page to access support-related information and tools.

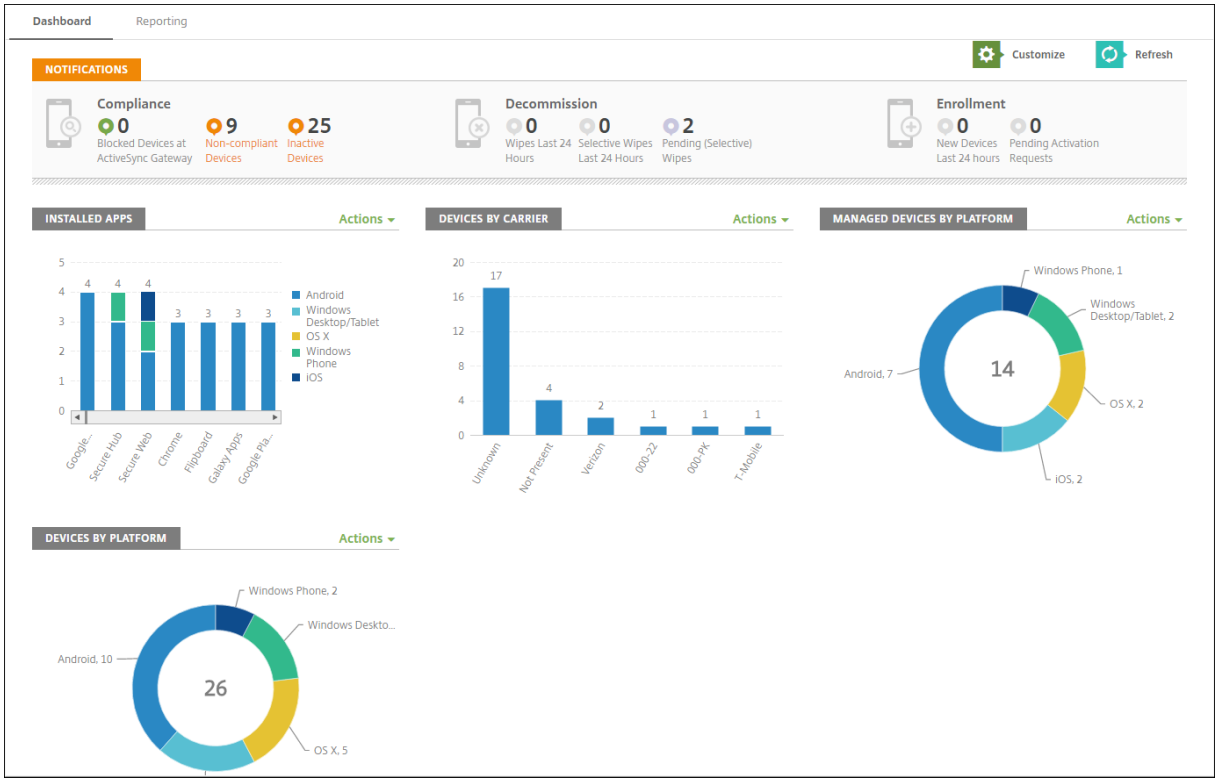
In the Citrix Endpoint Management console, click the wrench icon in the upper-right corner.

The **Troubleshooting and Support** page appears.

Use the Citrix Endpoint Management **Troubleshooting and Support** page to:

- Access diagnostics.
- Access links to Citrix Product Documentation and the Knowledge Center.
- Access log operations.
- Use advanced configuration options.
- Access a set of tools and utilities.

You can also view information at a glance by accessing your Citrix Endpoint Management console dashboard. With this information, you can see issues and successes quickly by using widgets.



The dashboard is usually the page that first appears when you sign on to the Citrix Endpoint Man-

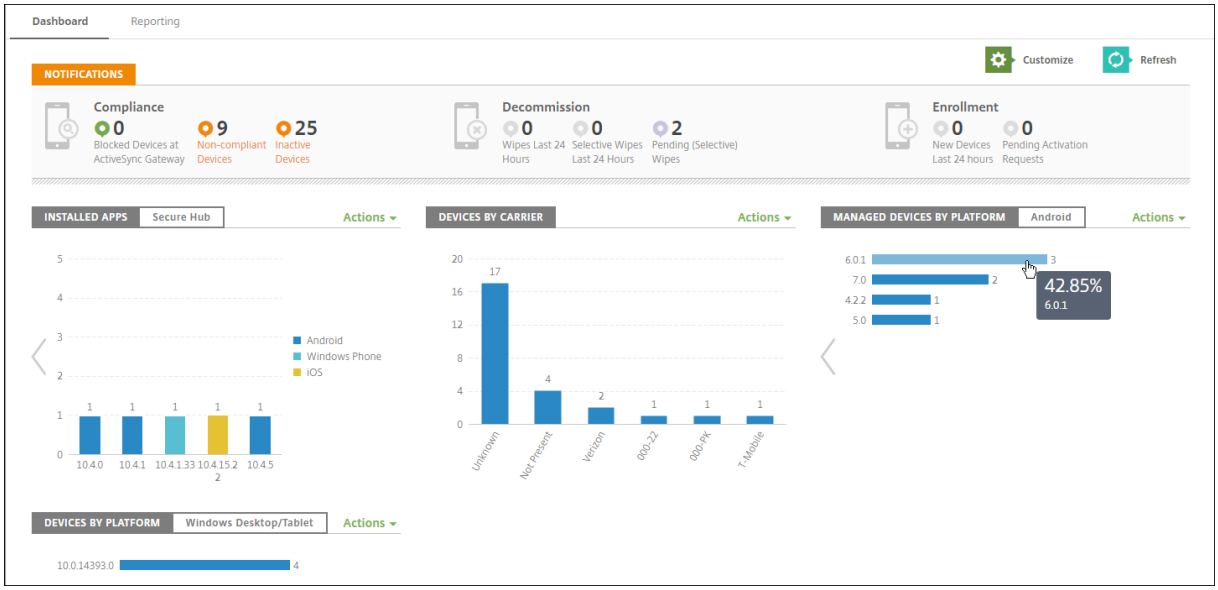
© 1997–2025 Citrix Systems, Inc. All rights reserved.

agement console. To access the dashboard from elsewhere in the console, click **Analyze**. Click **Customize** on the dashboard to edit the layout of the page and to edit the widgets that appear.

- **My Dashboards:** You can save up to four dashboards. You can edit these dashboards separately and view each one by selecting the saved dashboard.
- **Layout Style:** In this row, you can select how many widgets appear on your dashboard and how the widgets are laid out.
- **Widget Selection:** You can choose which information appears on your dashboard.
  - **Notifications:** Mark the checkbox above the numbers on the left to add a Notifications bar above your widgets. This bar shows the number of compliant devices, inactive devices, and devices wiped or enrolled in the last 24 hours.
  - **Devices By Platform:** Displays the number of managed and unmanaged devices by platform.
  - **Devices By Carrier:** Displays the number of managed and unmanaged devices by carrier. Click each bar to see a breakdown by platform.
  - **Managed Devices By Platform:** Displays the number of managed devices by platform.
  - **Unmanaged Devices By Platform:** Displays the number of unmanaged devices by platform. Devices that appear in this chart might have an agent installed, but their privileges are revoked or the devices are wiped.
  - **Devices By ActiveSync Gateway Status:** Displays the number of devices grouped by ActiveSync Gateway status. The information shows Blocked, Allowed, or Unknown status. You can click each bar to break down the data by platform.
  - **Devices By Ownership:** Displays the number of devices grouped by ownership status. The information shows corporate-owned, employee-owned, or unknown ownership status.
  - **Failed Delivery Group Deployments:** Displays the total number of failed deployments per package. Only packages that have failed deployments appear.
  - **Devices By Blocked Reason:** Displays the number of devices blocked by ActiveSync
  - **Installed Apps:** Type an app name for a graph of app information.
  - **Volume Purchase Apps License Usage:** Displays license usage statistics for the Apple Volume Purchase apps.

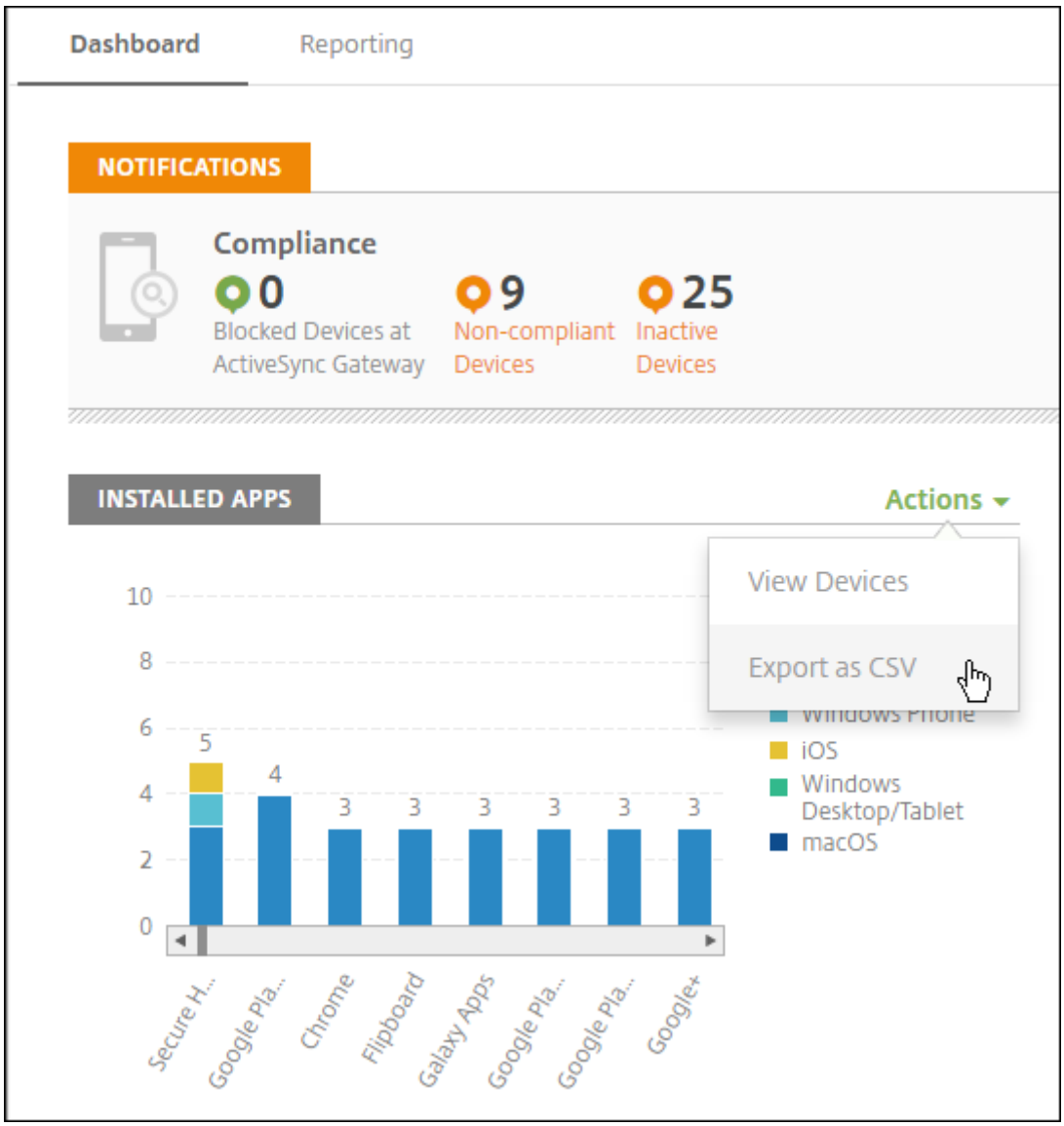
With each widget, you can click the individual parts to drill down for more information.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



You can also export the information as a .csv file by clicking the **Action** menu.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Monitor page for help desk administrators

You can monitor and troubleshoot Citrix Endpoint Management on the **Monitor** page. This interface is customized for help desk administrators to carry out user-based troubleshooting efficiently.

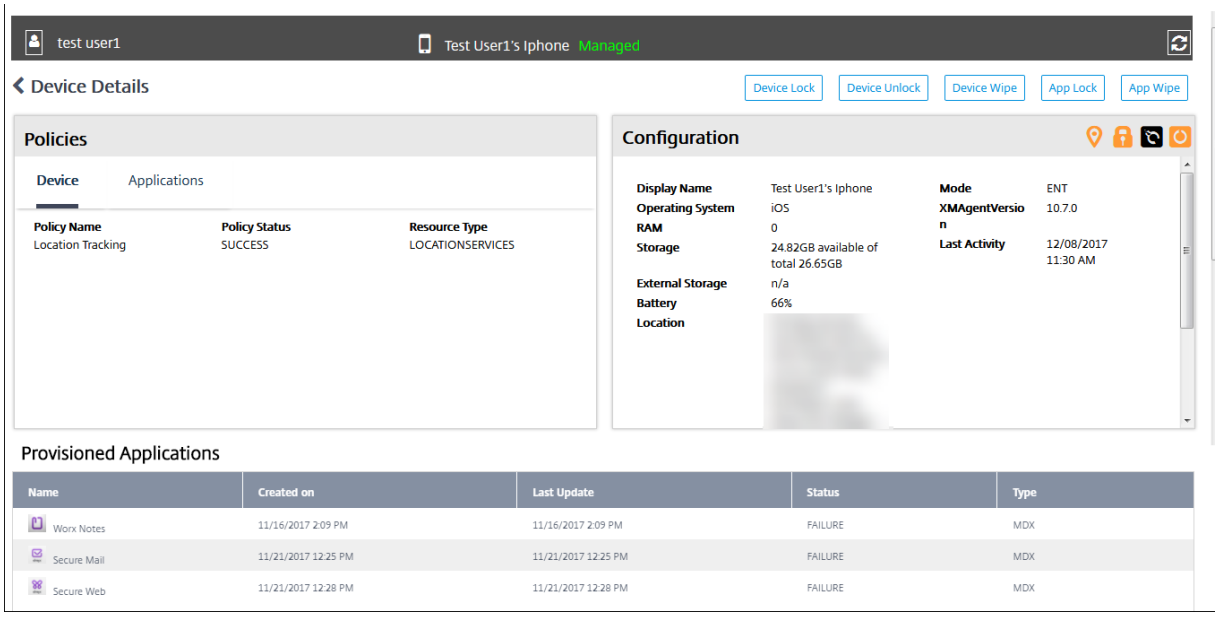
Help Desk administrators must have the following permissions to access the **Monitor** page and all available workflows:

- Authorized access
  - Admin console access
  - Public api access
- Console Features

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Monitor
- Devices
- Full Wipe Device
- View Locations
  - Locate Device
  - Track Device
- Lock device
- Unlock device
- App Lock
- App Wipe
- App

The **Monitor** page gives you a combined view of device policies and configuration. The view includes troubleshooting actions such as app lock/unlock, app wipe, device lock/unlock, and device wipe.



Use the **Monitor** page to:

- Search for an Active Directory (AD) user and device you want to troubleshoot.
- Analyze the **Device Details** page that has the following:
  - **Policies:** Displays device and app policies for the selected device and app. For information about modifying policies, see Device policies and Add apps.
  - **Configuration:** Displays the device configuration. This panel includes icons that indicate whether the device has location services enabled, is jailbroken, and is MDM or MAM managed. The panel also shows the storage encryption status.
  - **Running Applications** table: Displays the details of the applications currently running on the device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Troubleshoot the device. Security actions available on this page are based on the enrollment of the device, and the permissions available to the logged in administrator:
  - Device lock/unlock
  - Device wipe
  - App lock/unlock (available if the device is MAM enrolled)
  - App wipe (available if the device is MAM enrolled)

For more information about the actions you can take, see Security actions.

The Monitor page might not operate as expected 60 minutes after it was last loaded, because it does not handle refreshes of the login token. As a workaround, refresh the token by reloading the page: Click the **Citrix Cloud** link on your service console and then click **Citrix Endpoint Management > Manage > Monitor**.

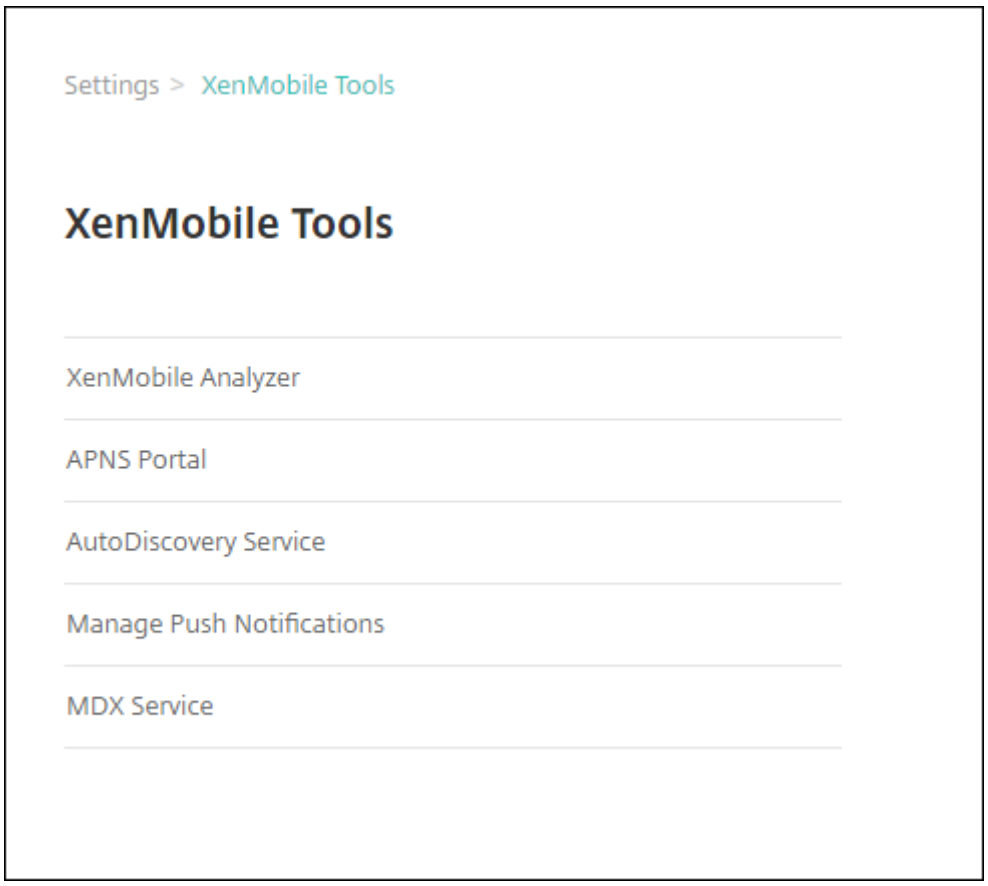
Access to Citrix Endpoint Management Tools from the console

You can access these Citrix Endpoint Management Tools from the Citrix Endpoint Management console:

- **APNs Portal** –Submit a request to Citrix to sign an APNs certificate, which you then submit to Apple.
- **Auto Discovery Service** –Request and configure AutoDiscovery for Citrix Endpoint Management in your domain.
- **Manage Push Notifications** –Manage push notifications for iOS and Windows mobile apps.

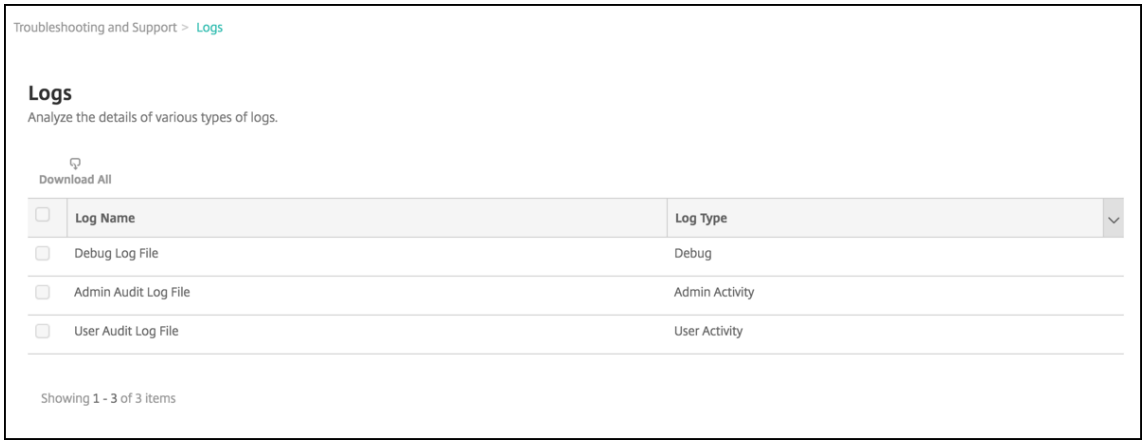
To access these tools, go to **Settings > Citrix Endpoint Management Tools**. This page is available to users with the Cloud Admin or Customer Admin role.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



View and analyze log files in Citrix Endpoint Management

1. In the Citrix Endpoint Management console, click the wrench icon in the upper-right corner of the console. The **Troubleshooting and Support** page opens.
2. Under **Log Operations**, click **Logs**. The **Logs** page appears. Individual logs appear in a table.

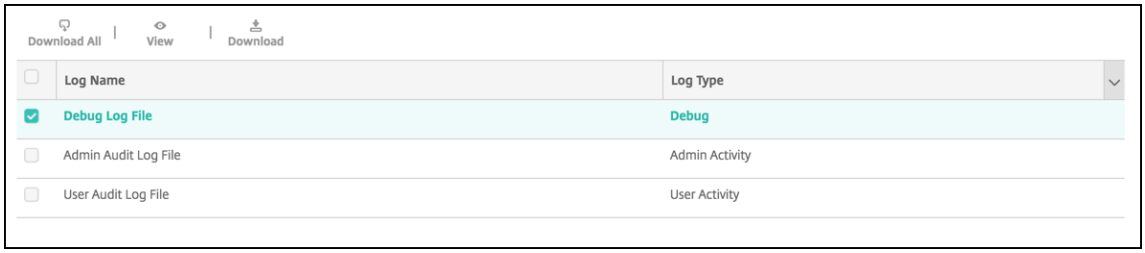


3. Select the log that you want to view:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Debug Log Files have information useful for Citrix Support, such as error messages and server-related actions.
- Admin Audit Log Files have audit information about activity on the Citrix Endpoint Management console.
- User Audit Log Files have information related to configured users.

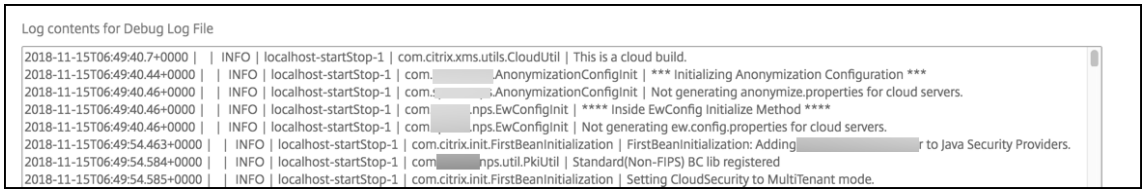
4. Use the actions at the top of the table to download all, view, or download a single log.



> **Note:**
>
> If you select multiple log files, only **Download All** is available.

5. Do one of the following:

- **Download All:** The console downloads all the logs present on the system (including debug, admin audit, user audit, server logs, and so on).
- **View:** Shows the contents of the selected log below the table.
- **Download:** The console downloads only the single log file type selected. The console also downloads any archived logs for that same type.



Citrix Endpoint Management uses the log4j syslog appender to send RFC5424 formatted syslog messages. The syslog message data is plain text with no specific format.

Connectivity checks

March 4, 2024

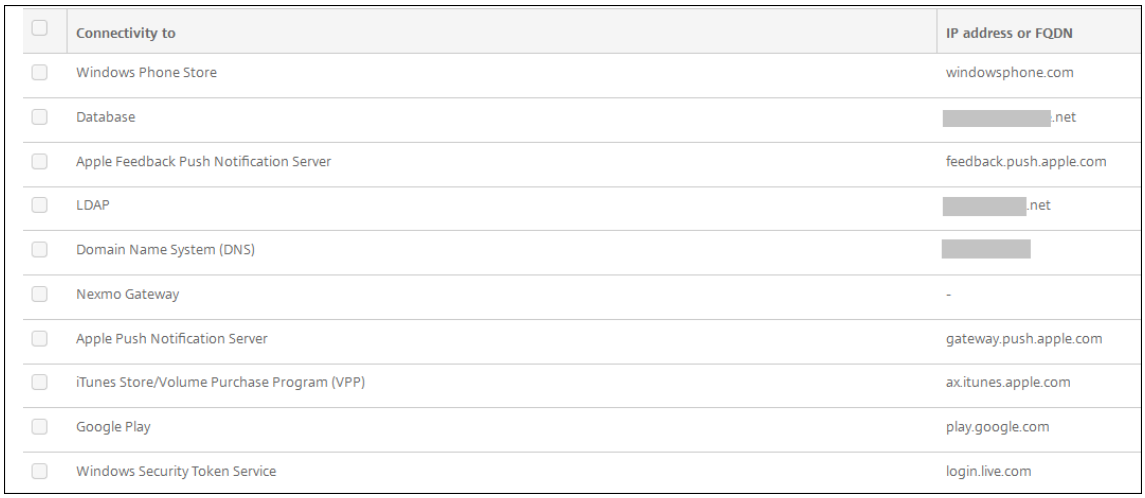
From the Citrix Endpoint Management **Troubleshooting and Support** page, you can check the Citrix Endpoint Management connection to NetScaler Gateway and to other servers and locations. To run Citrix Endpoint Management connectivity checks, you need the Support or the Admin role. Set this

© 1997–2025 Citrix Systems, Inc. All rights reserved.

role using Role-Based Access Control (RBAC). For more information on assigning roles, see Configure roles with RBAC.

Run Citrix Endpoint Management connectivity checks

1. In the Citrix Endpoint Management console, click the wrench icon in the upper-right corner of the console. The **Troubleshooting and Support** page appears.
2. Under **Diagnostics**, click **Citrix Endpoint Management Connectivity Checks**. The **Citrix Endpoint Management Connectivity Checks** page appears. If your Citrix Endpoint Management environment has clustered nodes, all nodes are shown.



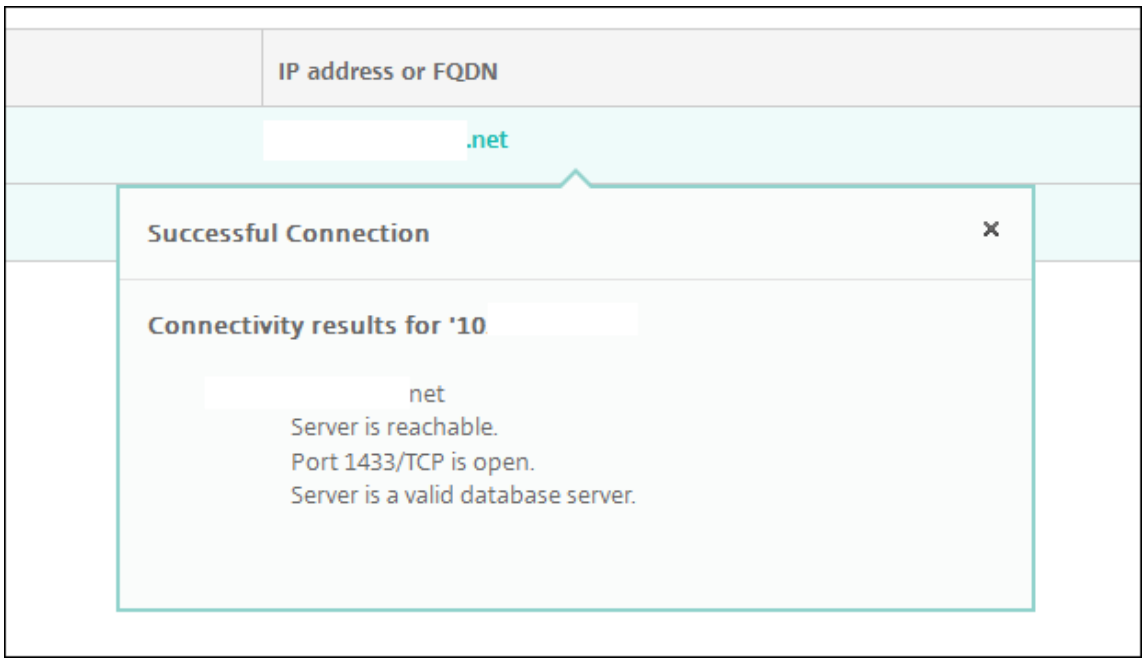
Connectivity to	IP address or FQDN
Windows Phone Store	windowsphone.com
Database	[redacted].net
Apple Feedback Push Notification Server	feedback.push.apple.com
LDAP	[redacted].net
Domain Name System (DNS)	[redacted]
Nexmo Gateway	-
Apple Push Notification Server	gateway.push.apple.com
iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
Google Play	play.google.com
Windows Security Token Service	login.live.com

3. Select the servers that you want to include in the connectivity test and then click **Test Connectivity**. The test results page appears.

Connectivity to	IP address or FQDN	
Database	net	✓
Windows Phone Store	windowsphone.com	✓

4. Select a server in the test results table to see detailed results for that server.

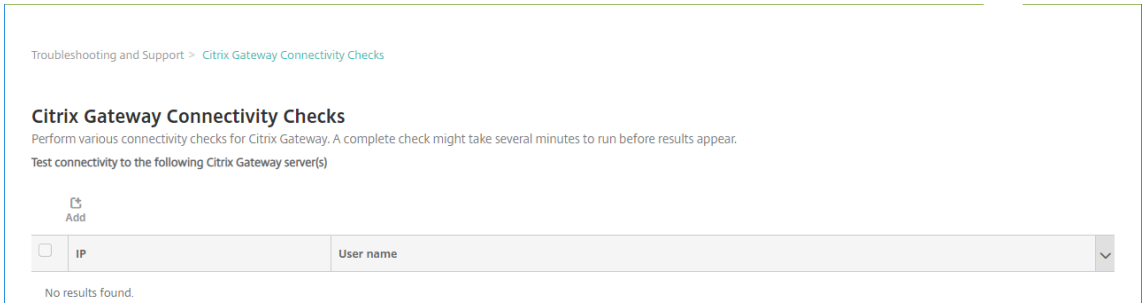
© 1997–2025 Citrix Systems, Inc. All rights reserved.



For more information about connectivity checks that Citrix Endpoint Management can do and their details, see Connectivity check details.

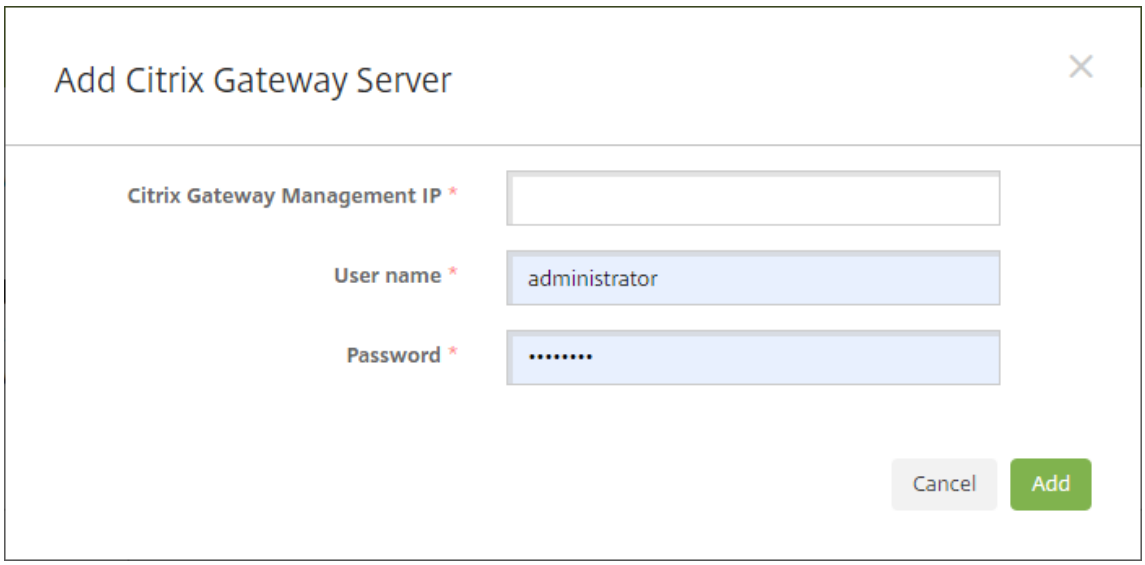
Conducting NetScaler Gateway connectivity checks

1. On the **Troubleshooting and Support** page, under **Diagnostics**, click **NetScaler Gateway Connectivity Checks**. The **NetScaler Gateway Connectivity Checks** page appears. The table is empty if there's no connection between Citrix Endpoint Management and NetScaler Gateway.



2. Click **Add**. The **Add NetScaler Gateway Server** dialog box appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. In **NetScaler Gateway Management IP**, type the management IP address for the server running NetScaler Gateway that you want to test.

   If you're conducting a connectivity check for a NetScaler Gateway server that has already been added before, the IP address is provided.

4. Type your administrator credentials for this NetScaler Gateway.

   If you're conducting a connectivity check for a NetScaler Gateway server that has already been added before, the user name is provided.

5. Click **Add**. The NetScaler Gateway is added to the table on the **NetScaler Gateway Connectivity Checks** page.

6. Select the NetScaler Gateway server and then click **Test Connectivity**. The results appear in a test results table.

7. Select a server in the test results table to see detailed results for that server.

Connectivity check details

The following table lists various connectivity checks that Citrix Endpoint Management can do and include details about each check.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Connectivity to	IP address or FQDN	Details
Apple Push Notification Server	api.push.apple.com	Checks the connectivity between the Apple Push Notification Server and the Citrix Endpoint Management node. Apple Push Notification Server is required to send messages to iOS and macOS devices.
Apple Feedback Push Notification Server	feedback.push.apple.com	Checks connectivity between Apple Feedback Server and the Citrix Endpoint Management node. Apple Feedback Push Notification Server gives you information about failed remote notifications sent to iOS and macOS devices.
Citrix License Server	IP address of License Server	Checks connectivity between Citrix License Server and the Citrix Endpoint Management node. Servers running Citrix products contact Citrix License Server to get licenses.
NetScaler Gateway	FQDN of NetScaler Gateway configured in Citrix Endpoint Management	Checks connectivity between NetScaler Gateway and the Citrix Endpoint Management node. NetScaler Gateway is used by Citrix Endpoint Management client apps (such as Citrix Secure Mail and Citrix Secure Web) to connect through a VPN server for access to internal networks.
Database	IP address or FQDN of Database Server	Checks connectivity between the Citrix Endpoint Management database and the Citrix Endpoint Management node.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Connectivity to	IP address or FQDN	Details
Domain Name System (DNS)	IP address configured in Citrix Endpoint Management	Checks connectivity between the DNS server and the Citrix Endpoint Management node.
Secure Ticket Authority service	localhost	Checks the Citrix Endpoint Management node connection to authentication services, STA (Secure Ticket Authority) services, and cluster services.
Firebase Cloud Messaging (FCM) Server		Checks connectivity between FCM Server and the Citrix Endpoint Management node. Using FCM, you can notify a client app that a new email or other data is available to sync. You can send notification messages to drive user engagement and retention. FCM is a replacement for Google Cloud Messaging (GCM).
Google Play	play.google.com	Checks connectivity between Google Store Server and the Citrix Endpoint Management node. Google Play is used to offer services that include a managed, private enterprise app delivery store.
iTunes Store/Volume Purchase	vpp.itunes.apple.com	Checks connectivity between Apple Store Server and the Citrix Endpoint Management node. The Apple Store is used to offer services that include a managed, private enterprise app delivery store.
LDAP	IP address or FQDN of LDAP configured in Citrix Endpoint Management	Checks connectivity between the LDAP server and the Citrix Endpoint Management node.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Connectivity to	IP address or FQDN	Details
Microsoft Push Notification Server	sin.notifiy.windows.com	Checks connectivity between Windows Notification Server and the Citrix Endpoint Management node. Windows Notification Server is used to send messages to Windows devices.
ShareFile Service	IP address or FQDN of ShareFile Service configured in Citrix Endpoint Management	Checks connectivity between ShareFile Service and Citrix Endpoint Management. ShareFile The Service is a secure cloud-based platform for businesses to store and share large files.
Windows Desktop/Tablet Store	windows.microsoft.com	Checks connectivity between the Windows Desktop/Tablet Store and the Citrix Endpoint Management node. Windows Desktop/Tablet Store is used to offer services that include a managed, private enterprise app delivery store.
Windows Security Token Service	login.live.com	Checks connectivity between Windows Security Token Server and the Citrix Endpoint Management node. Windows Security Token Service supports two-factor authentication (domain plus security token) for Windows devices.

Mobile Service Provider

September 6, 2025

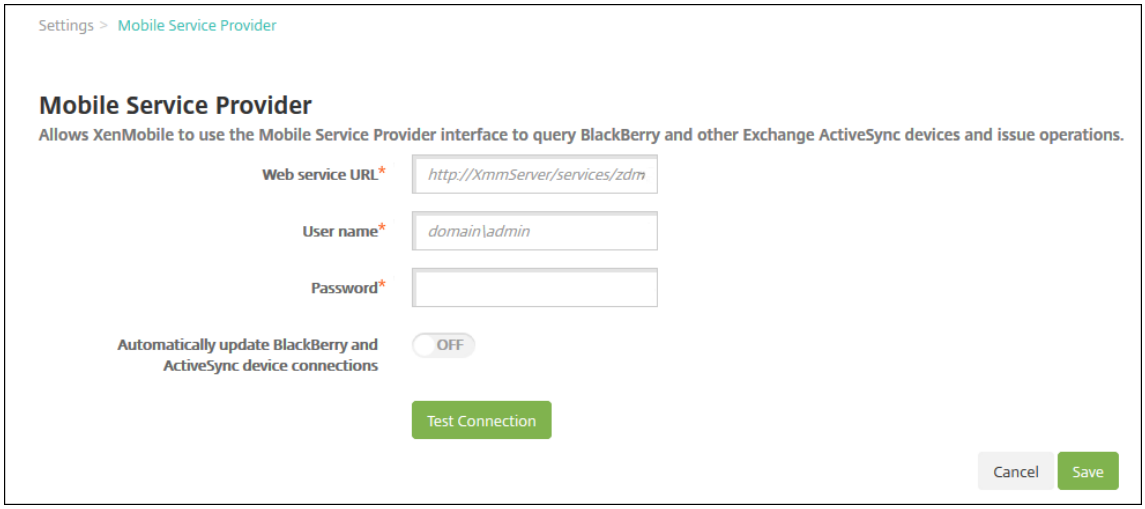
© 1997–2025 Citrix Systems, Inc. All rights reserved.

You can enable Citrix Endpoint Management to use the Mobile Service Provider interface to query BlackBerry and Exchange ActiveSync devices and issue operations.

For example, suppose that your organization has 1,000 users and each user uses one or more devices. After you direct all users to enroll their devices with Citrix Endpoint Management, the Citrix Endpoint Management console indicates the number of devices that users enroll. By configuring this setting, you can determine how many devices connect to the Exchange Server. In this way, you can do the following:

- Determine if any users still have to enroll their devices.
- Issue commands to user devices that connect to the Exchange Server, such as data wipes.

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Server**, click **Mobile Service Provider**. The **Mobile Service Provider** page appears.



3. Configure these settings:
   - **Web service URL:** Type the URL of the Web service; for example, `https://XmmServer/services/xdmservice`.
   - **User name:** Type the user name in the format `domain\\admin`.
   - **Password:** Type the password.
   - **Automatically update BlackBerry and ActiveSync device connections:** Select whether to automatically update device connections. The default is **Off**
   - Click **Test Connection** to verify connectivity.
4. Click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Reports

September 6, 2025

Citrix Endpoint Management provides the following pre-defined reports that let you analyze your app and device deployments. Each report appears as a table and a chart. You can sort and filter the tables by column. You can select elements in the chart from more detailed information.

- **Total Apps Deployment Attempts:** Lists deployed apps that users tried to install on their devices.
- **Apps by Platform:** Lists apps and app versions by device platform and version.
- **Apps by Type:** Lists apps by version, type, and category.
- **Device Enrollment:** Lists all enrolled devices.
- **Devices & Apps:** Lists devices that are running managed apps.
- **Inactive Devices:** A list of devices that haven't had any activity for the number of days specified by the Citrix Endpoint Management server property `device.inactivity.days.threshold`.
- **Jailbroken/Rooted Devices:** Lists jailbroken iOS devices and rooted Android devices.
- **Terms & Conditions:** Lists users who have accepted and declined Terms and Conditions agreements. You can select areas of the chart to view more details.
- **Top 10 Failed Deployments:** Lists up to 10 apps that have failed to deploy.
- **Blocked Apps by Device & User**: Lists apps on the block list that users have on their devices.
- **Non-Compliant Devices:** Lists devices that don't meet compliance criteria. Criteria include whether the device is jailbroken, the OS version running, and if the device has a passcode. The report also displays the user name associated with the device and if the device is encrypted. For iOS devices, the encryption column displays N/A.

You can export the data in each table in .csv format, which opens in programs such as Microsoft Excel. Charts for each report can be exported in PDF format.

The **Reporting** tab includes device details, such as serial number, IMEI/MEID, apps, and connections. For more comprehensive reporting about a specific device, go to **Manage > Devices**, click that device, click **Show more**, and then view the **Device details** page. The **Device details** page lists device security properties, device properties, assigned policies, apps, actions, certificates, and more. For information about the **Device details** page, see Get information about devices.

The following aspects determine how Citrix Endpoint Management collects information about apps deployed to or installed on managed devices:

- Device type
- Enrollment method
- Whether the App inventory device policy is deployed

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For Android devices, the behavior is different depending on the device type and the enrollment method. The following table indicates where apps are listed for **Android Enterprise** (**Device details** page, reports, or not available). App lists include all apps unless otherwise indicated.

	MDM+MAM (all apps)	MDM (all apps)
Required apps (the App inventory policy isn't deployed)	**Device details** page and reports	Public apps; **Device details** page and reports
Optional apps (the App inventory policy isn't deployed)	Not available	Not available
Required apps (the App inventory policy is deployed)	**Device details** page and reports	**Device details** page and reports
Optional apps (the App inventory policy is deployed)	Enterprise, MDX, public, and Web link apps; reports	**Device details** page and reports

The following table indicates where apps are listed for **Android (legacy DA)** (**Device details** page, reports, or not available). App lists include all apps unless otherwise indicated.

	MDM+MAM (all apps)	MDM (public and enterprise apps)	MAM
Required apps (the App inventory policy isn't deployed)	**Device details** page and reports	**Device details** page and reports	N/A
Optional apps (the App inventory policy isn't deployed)	**Device details** page and reports	**Device details** page and reports	Not available
Required apps (the App inventory policy is deployed)	**Device details** page and reports	**Device details** page and reports	N/A
Optional apps (the App inventory policy is deployed)	**Device details** page and reports	**Device details** page and reports	Not available

For iOS devices, the behavior is different depending on the enrollment method. The following table indicates where apps are listed (**Device details** page or reports). App lists include all apps unless otherwise indicated.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

	MDM+MAM (all apps)	MDM (public and enterprise apps)	MAM (all apps)
Required apps (the App inventory policy isn't deployed)	**Device details** page and reports	**Device details** page and reports	**Device details** page and reports. Those apps are shown in a pending state (even if they aren't installed) or remain in a pending state after they're installed manually.
Optional apps (the App inventory policy isn't deployed)	**Device details** page and reports	**Device details** page and reports	Web, SaaS, and Web link apps are listed on the **Device details** page as installed apps. They aren't listed in the reports. Enterprise, MDX, and public apps aren't listed on the **Device details** page after they're installed manually. Apps aren't listed in reports after they're installed manually.
Required apps (the App inventory policy is deployed)	**Device details** page and reports	**Device details** page and reports	The App inventory policy can't be deployed to devices. Apps are listed on the **Device details** page and in the reports. Those apps are shown in a pending state (even if they aren't installed) or remain in a pending state after they're installed manually.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

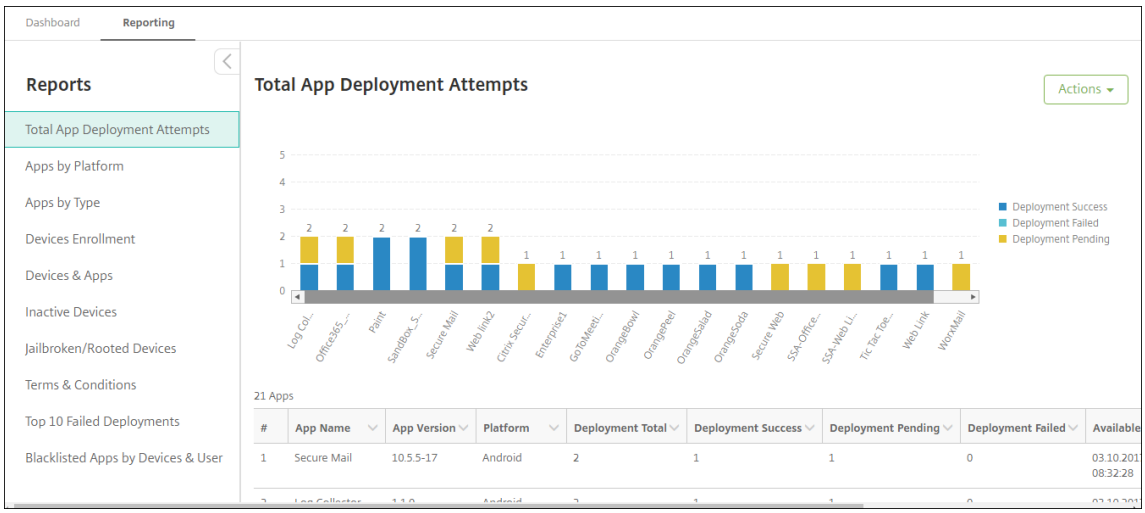
	MDM+MAM (all apps)	MDM (public and enterprise apps)	MAM (all apps)
Optional apps (the App inventory policy is deployed)	**Device details** page and reports	**Device details** page and reports	The App inventory policy can't be deployed to devices. Web, SaaS, and Web link apps are listed on the **Device details** page as installed apps. They aren't listed in the reports. Enterprise, MDX, and public apps aren't listed on the **Device details** page after they're installed manually. Apps aren't listed in reports after they're installed manually.

For macOS and Windows devices, Citrix Endpoint Management collects an inventory of apps *only* when the App inventory policy is deployed.

To generate a report

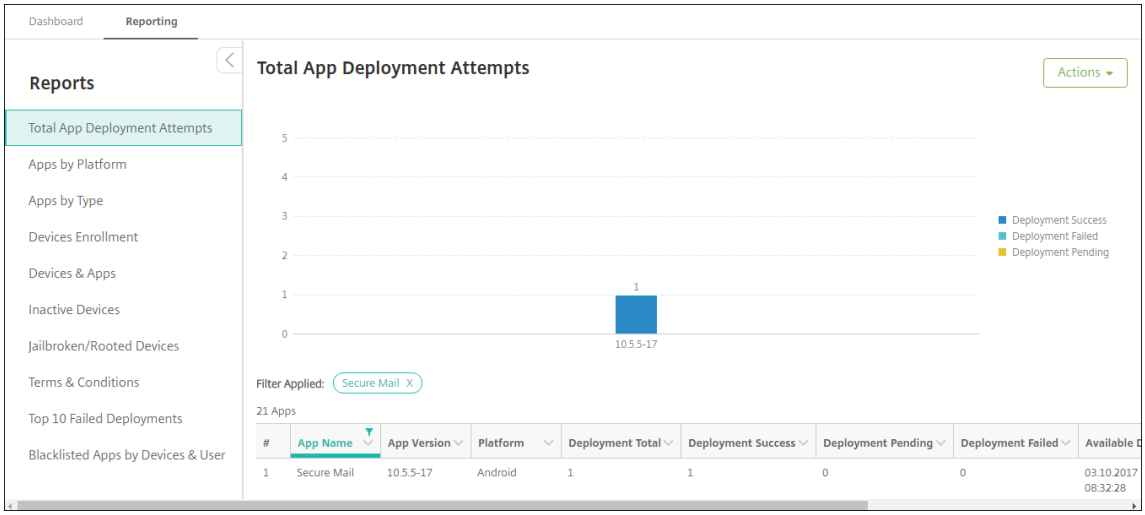
1. In the Citrix Endpoint Management console, click **Analyze > Reporting**. The **Reporting** page appears.
2. Click the report that you want to generate.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



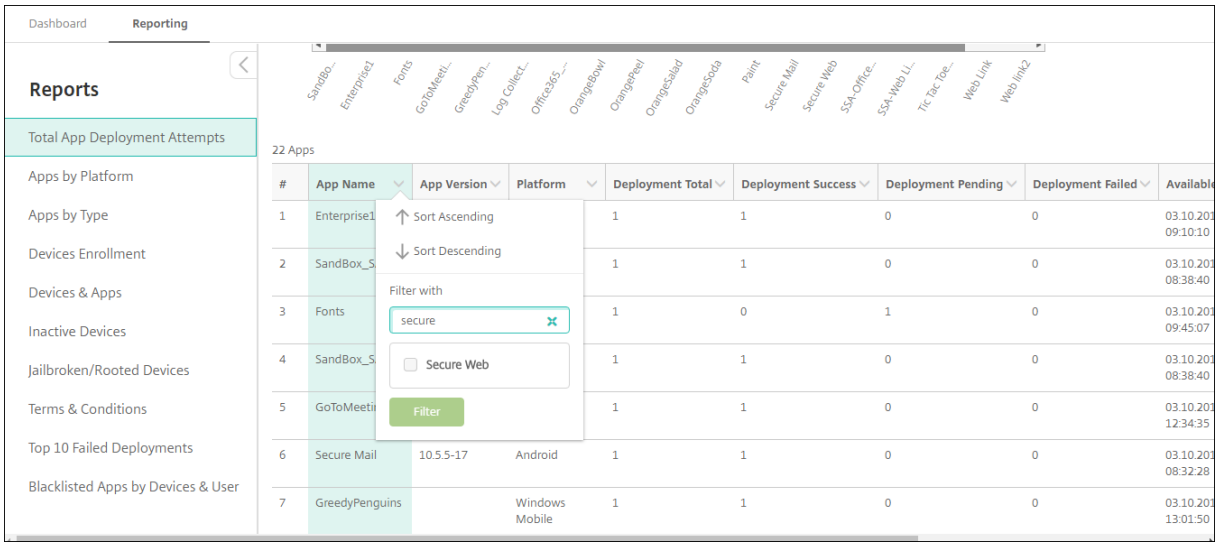
To view more details of a report

1. Click the areas of the chart to drill down and see more detailed information.



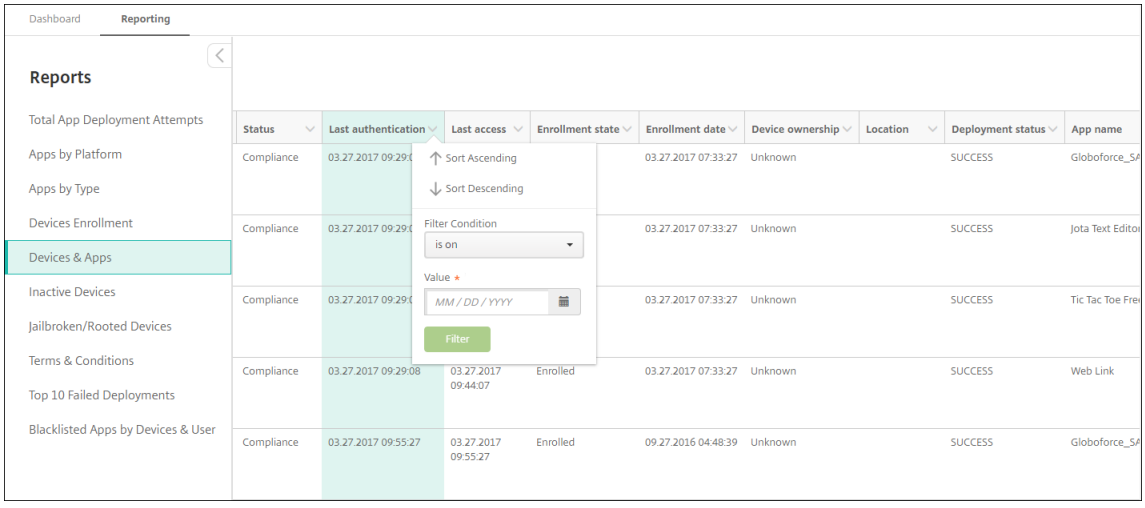
© 1997–2025 Citrix Systems, Inc. All rights reserved.

To sort, filter, or search a table column, click the column heading



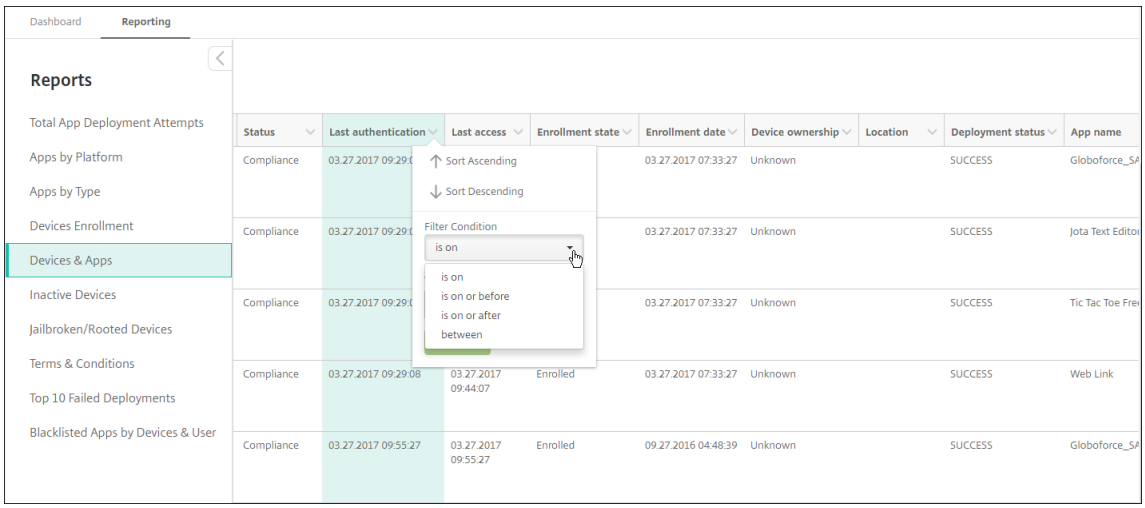
To filter the report by date

1. Click a column heading to view the filter settings.

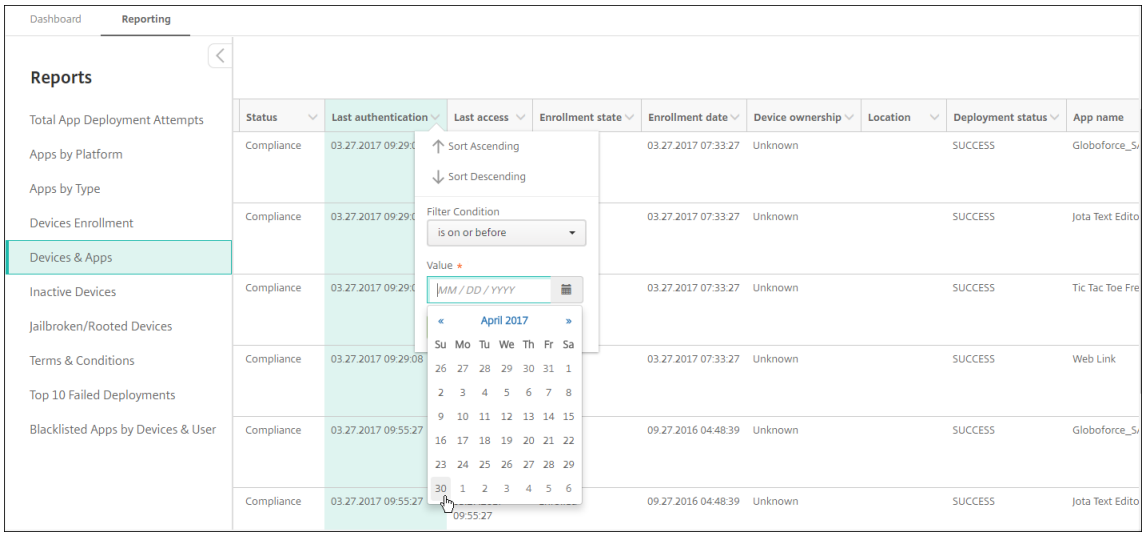


2. From **Filter Condition**, choose how you want to restrict the dates reported.

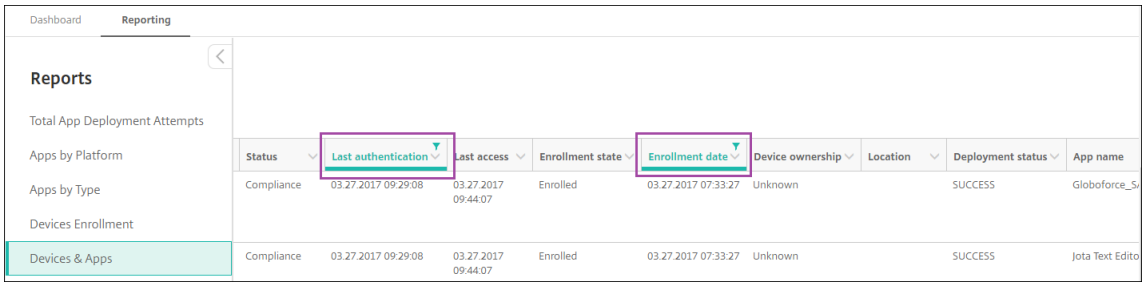
© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Use the date chooser to specify dates.

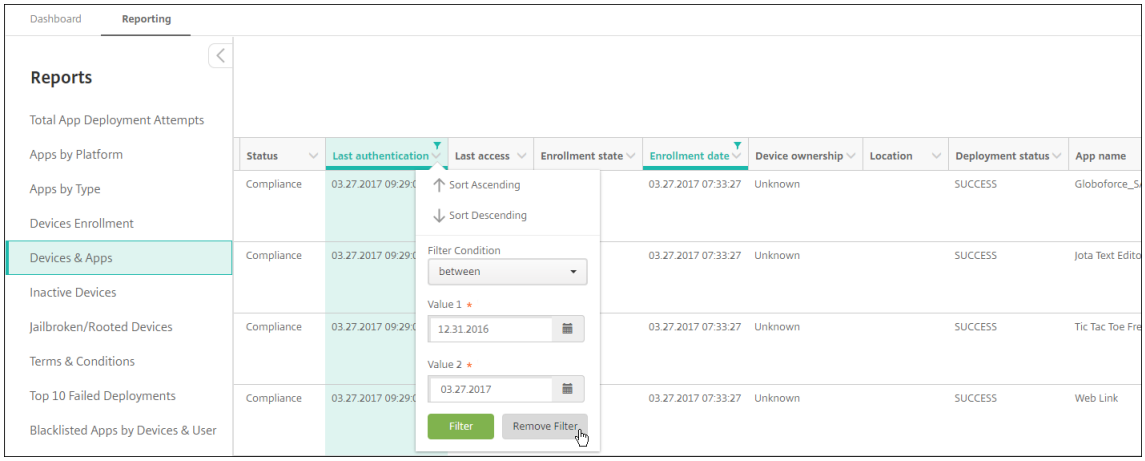


4. A column with a date filter displays as shown the following example.



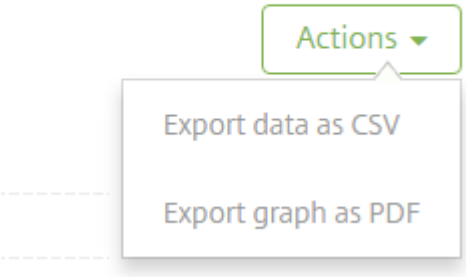
5. To remove a filter, click the column heading and then click **Remove Filter**

© 1997–2025 Citrix Systems, Inc. All rights reserved.



To export a chart or table

- To export the chart in PDF format, click **Actions** then **Export graph as PDF**.
- To export the table data in CSV format, click **Actions** then **Export data as CVS**.



REST APIs

September 6, 2025

With the Citrix Endpoint Management REST API, you can:

- Call services that display in the Citrix Endpoint Management console
- Call REST services by using any REST client

The API does not require you to sign on to the Citrix Endpoint Management console to call the services.

For the complete current set of available APIs, download the Public API for REST Services PDF.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

There are APIs available to manage your mobile and desktop endpoint devices and configure settings for your Workspace apps. Go to https://developer.cloud.com/citrixworkspace and navigate to **Citrix Endpoint Management > Mobile Application Integration**.

Permissions required to access the REST API

Access to the REST API requires one of the following permissions:

- Citrix Cloud administrator
- Public API access permission set as part of role-based access configuration. For information, see Configuring roles with RBAC.
- Super user permission

To access the REST API using your Citrix Cloud account, generate the **API** keys:

1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. Select **API Access > Secure Clients**.
3. Type a name for your secure client and click **Create Client**.

Citrix Cloud then creates the secure client ID and client secret. Download a copy of this information and save it securely offline for your reference. Citrix Cloud doesn't store the unique identifiers after you close the dialog box.

To invoke the REST API services

You can call the REST API services by using the REST client or cURL commands. The following examples use the Advanced REST client for Chrome.

> **Note:**
>
> In the following examples, change the host name and port number to match your environment.

Log in

The example shown here covers logging in using a token retrieved through the Citrix Cloud API.

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login/cloud`

Method type: POST

Content type: application/json

Request sample:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
{

 "bearerToken": "eyJ0eOiJSUzJiibGcI1AiONiJ9.
    eyJkIjoMDExN1c2VIXiMzNDc1OTk4...qf0iQ"
 }
```

You must retrieve the bearer token using the Citrix Cloud API `https://trust.citrixworkspacesapi.net/Help/Api/POST-customer-tokens-clients`. For information, see the Developer documentation.

Response sample:

```
{

 "auth_token": "q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"
 }
```

Related information

- Citrix Endpoint Management REST API

ActiveSync Gateway

September 6, 2025

ActiveSync is a mobile data synchronization protocol developed by Microsoft. ActiveSync synchronizes data with handheld devices and desktop (or laptop) computers.

You can configure the ActiveSync Gateway rules in Citrix Endpoint Management. The ActiveSync gateway keeps a list of ActiveSync IDs for all devices configured in Citrix Endpoint Management. Based on the rules you configure, you can allow or deny devices access to ActiveSync data, based on those ActiveSync IDs. For example, if you activate the rule **Missing Required Apps**, Citrix Endpoint Management checks the App Access Policy for required apps. If the required apps are missed, the policy denies access to ActiveSync data. For each rule, you can choose either **Allow** or **Deny**. The default setting is set as **Allow**.

For more information about the App Access device policy, see App access device policy.

Citrix Endpoint Management supports the following rules:

Anonymous Devices: Checks if a device is in anonymous mode. This check is available if Citrix Endpoint Management can't reauthenticate the user when a device tries to reconnect.

Forbidden Apps: Checks if a device has forbidden apps, as defined in an App Access policy.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Implicit Allow and Deny: This action is the default for the ActiveSync Gateway. The gateway creates a Device List of all devices that do not meet any of the other filter rule criteria. The gateway then allows or denies connections based on that list. If no rule matches, the default is set as **Implicit Allow**.

Inactive Devices: Checks if a device is inactive as defined by the **Device Inactivity Days Threshold** setting in **Server Properties**.

Missing Required Apps: Checks if a device is missing the required apps, as defined in an App Access policy.

Non-suggested Apps: Checks if a device has non-suggested apps, as defined in an App Access policy.

Noncompliant Password: Checks if the user password is compliant. On iOS and Android devices, Citrix Endpoint Management can determine whether the password currently on the device is compliant with the passcode policy sent to the device. For instance, on iOS, the user has 60 minutes to set a password if Citrix Endpoint Management sends a passcode policy to the device. Before the user sets the password, the passcode might be non-compliant.

Out of Compliance Devices: Checks whether a device is out of compliance, based on the Out of Compliance device property. Automated actions or third parties using Citrix Endpoint Management APIs usually change that property.

Revoked Status: Checks whether the device certificate was revoked. A revoked device can't re-enroll until it is authorized again.

Rooted Android and Jailbroken iOS Devices: Checks whether an Android or iOS device is jailbroken.

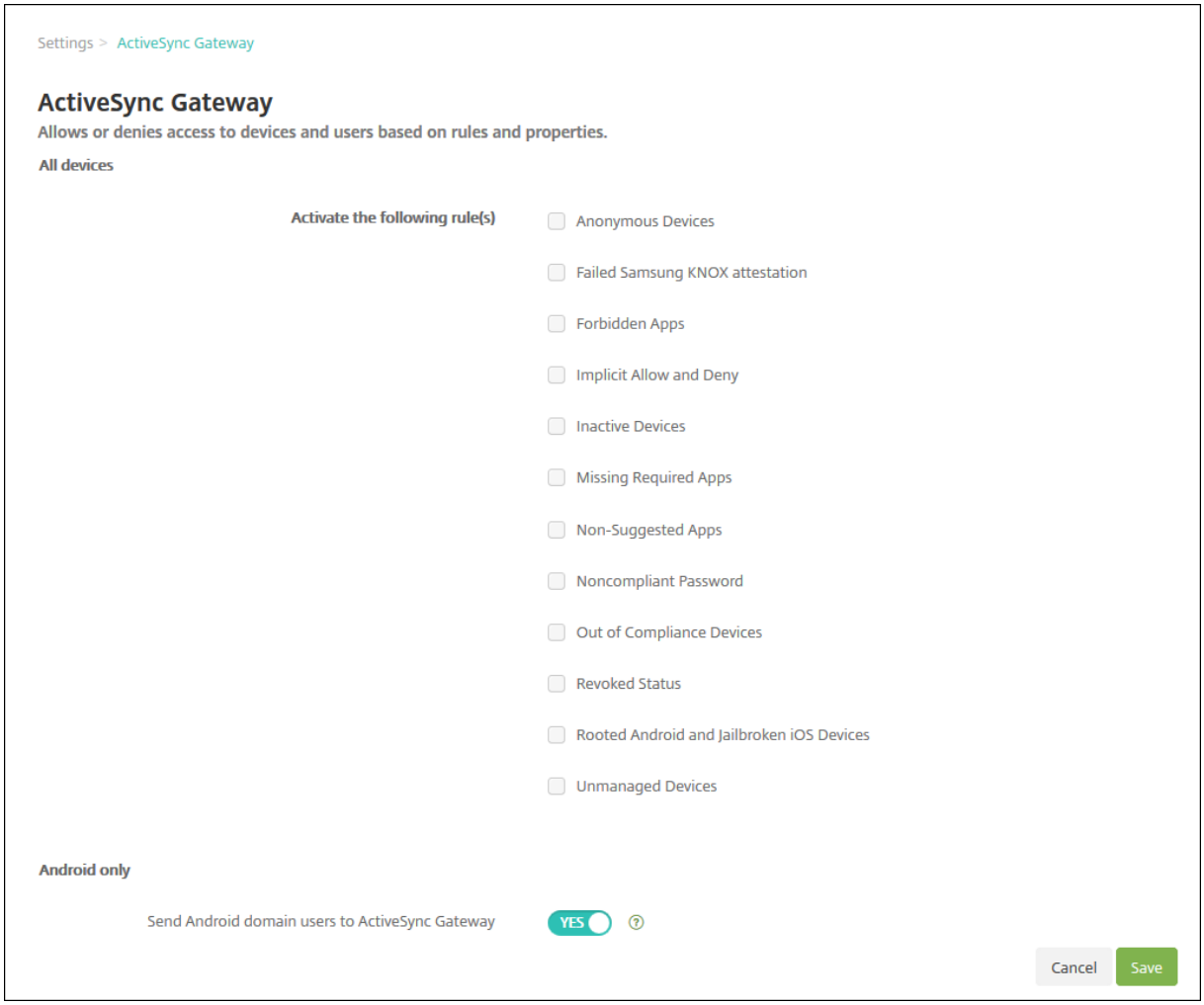
Unmanaged Devices: Check whether a device is still in a managed state, controlled by Citrix Endpoint Management. For example, a device enrolled in MAM or an unenrolled device isn't managed.

Send Android domain users to ActiveSync Gateway: Click **YES** to make Citrix Endpoint Management send the user name and ActiveSync ID of Android device owners to the ActiveSync Gateway. Turn this feature off unless you're running a legacy configuration. In more recent configurations, this feature allows any device access to ActiveSync data as long as the user name associated with the device exists on the Gateway.

To configure the ActiveSync Gateway settings

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Server**, click **ActiveSync Gateway**. The **ActiveSync Gateway** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



1. In **Activate the following rules**, select one or more rules you want to activate.
2. In **Android-only**, in **Send Android domain users to ActiveSync Gateway**, click **YES** to make sure that Citrix Endpoint Management sends Android device information to the ActiveSync Gateway.
3. Click **Save**.

Citrix Endpoint Management connector for Exchange ActiveSync

September 6, 2025

XenMobile Mail Manager is now a Citrix Endpoint Management connector for Exchange ActiveSync. For details about the Citrix unified portfolio, see the Citrix product guide.

The connector extends the capabilities of Citrix Endpoint Management in the following ways:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Dynamic Access Control for Exchange Active Sync (EAS) devices. EAS devices can be automatically allowed or blocked access to Exchange services.
- The ability for Citrix Endpoint Management to access EAS device partnership information provided by Exchange.
- The ability for Citrix Endpoint Management to wipe a mobile device based on EAS status.
- The ability for Citrix Endpoint Management to access information about Blackberry devices, and to do control operations such as Wipe and ResetPassword.

To wipe a device based on EAS status, configure an automated action with an ActiveSync trigger. See Automated Actions.

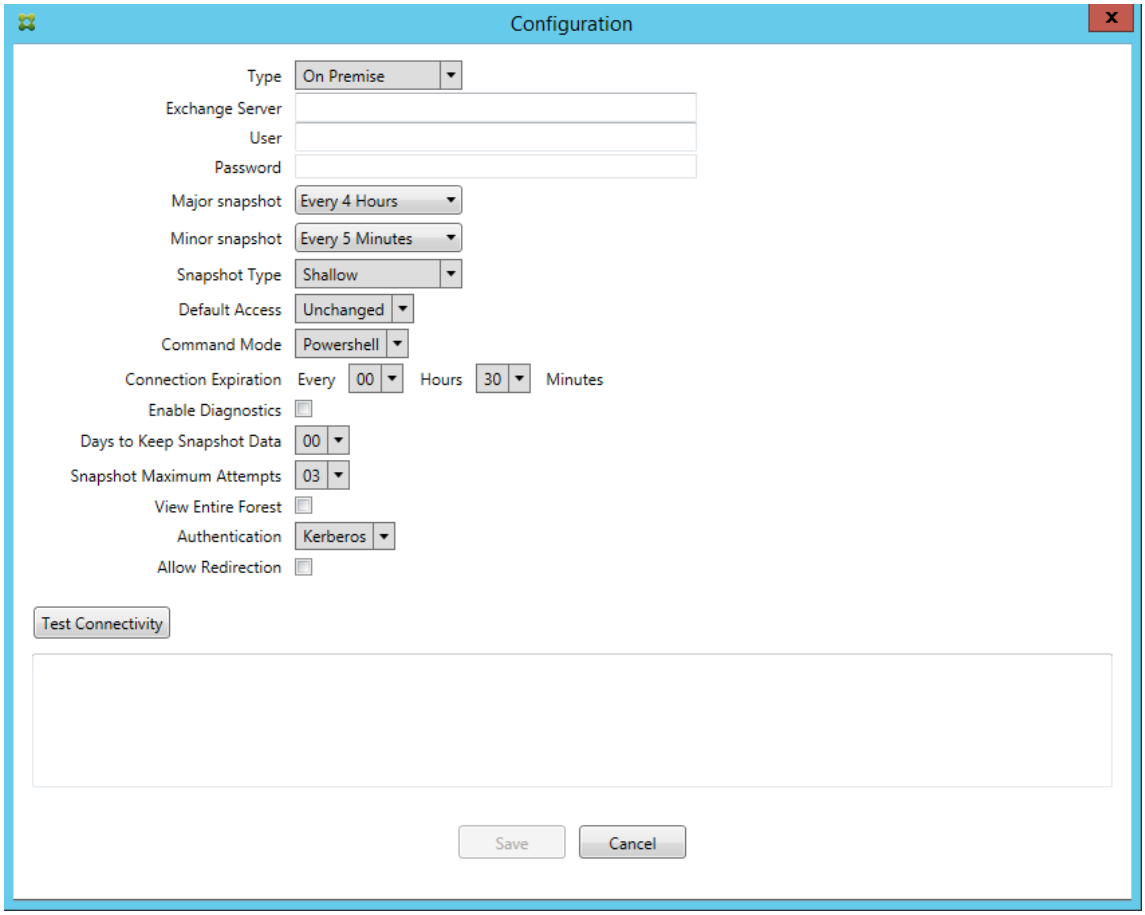
> **Important:**
>
> Starting in October 2022, the Citrix Endpoint Management and NetScaler Gateway connectors for Exchange ActiveSync no longer supports Exchange Online given the authentication changes announced by Microsoft here. The Citrix Endpoint Management connector for Exchange continues to work with Microsoft Exchange Server (on-premises).

What's new in version 10.1.10

The following issues are fixed in version 10.1.10:

- Customers who experience frequent network issues might not be able to complete a Snapshot within the previously provided three attempts. With this release, an admin can configure the maximum number of attempts (1-10). This fix allows for a snapshot to incur multiple breaks in communication without abandoning the snapshot process completely. [CXM-70837]

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- In previous versions, the Snapshot type did not appear in the list of Exchange Configurations. Now, the snapshot type appears. [CXM-70846]
- The PSRemotingTransport exception reported by PowerShell indicates that the session to Exchange is no longer viable. The status is added to the Critical Errors list in the configuration file by default. By doing so, when the PSRemotingTransportException is detected, the connection is marked as in Error for disposal later. The next communication uses a valid connection or creates a connection. [XMHELP-2184, CXM-70836]
- When a configuration change is saved, it's possible that not all previously configured internal components were disposed of properly before loading the new configuration. This issue might lead to unpredictable behavior. The behavior depends on the specific change and if the change conflicted with the previous configuration. In this release, all internal components are disposed of before loading the new configuration. [XMHELP-2259, CXM-71388]

What's new in version 10.1.9

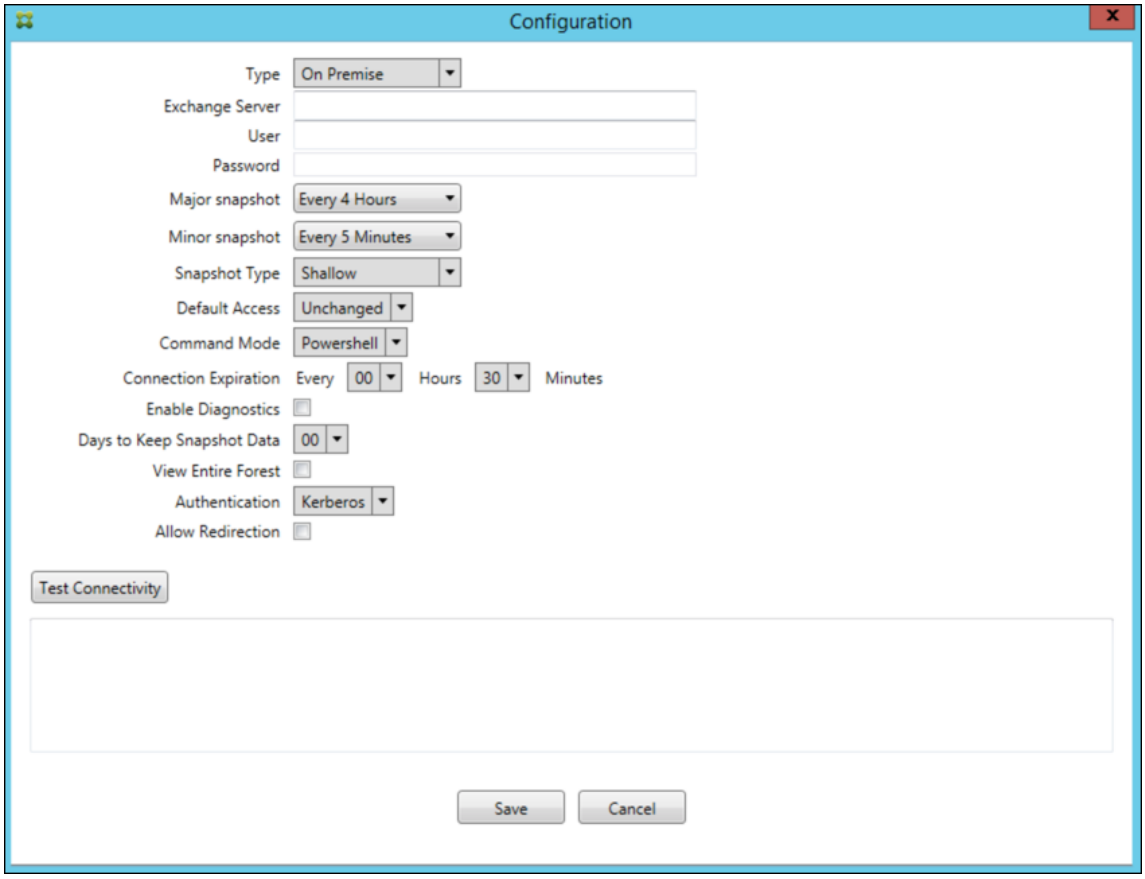
The following issues are fixed in version 10.1.9:

- Configuration changes are now handled in a more consistent manner. When the service detects a change in configuration, each internal subsystem is stopped, which means that any active or

© 1997–2025 Citrix Systems, Inc. All rights reserved.

scheduled processing is interrupted. Next, the new configuration is loaded and the subsystems are started again, which means that all schedules and other internal infrastructure are reestablished with the new settings. This issue corrects a known issue in version 10.1.8. [CXM-47709, CXM-61330]

- During an upgrade, the existing database configuration wasn't merged into the new configuration file. The database configuration is now merged into the upgraded configuration file. [CXM-49326]
- In the snapshot-related diagnostics files, the column headers were missing. The headers are restored. [CXM-62680]
- When upgrading from a previous version, the defaults section of the configuration file was being overwritten by the analogous section of the configuration file in use. This issue prevented additions or improvements to the defaults section from being loaded by the service after the upgrade. From this version, the defaults section always reflects the latest configuration. [CXM-62681]
- Admins can no longer access certain options by pressing Shift when running the application. These options were previously available with Citrix® permission. Some options are now fully available, such as Allow Redirection, and others, such as Hang Detection and Count Correction, are deprecated. [CXM-62767]



© 1997–2025 Citrix Systems, Inc. All rights reserved.

What's new in earlier versions

The following section lists the new features and fixed issues in earlier versions of the Citrix Endpoint Management connector for Exchange ActiveSync.

What's new in version 10.1.8

- It's possible that Exchange throttles back the Citrix Endpoint Management connector for the Exchange ActiveSync service from issuing commands too frequently. This issue is common in connections to Office 365. The effect of throttling requires that the service pause for a specified period before sending the next command. The Configure console now shows the amount of time remaining in the pause. [CXM-48044]
- When modifications are made to the "Watchdog"and/or "SpecialistsDefaults"sections of the configuration file (config.xml), the changes aren't reflected in the configuration file after an upgrade. With this release, the modifications are merged correctly into the new configuration file. [CXM-52523]
- More detail has been added to the analytics sent to Google Analytics, especially concerning snapshots. [CXM-56691]
- The Exchange test connectivity feature would attempt to initialize the connection only once. Because Office 365 connections can be throttled, it was possible that a test connectivity would appear to fail when throttled. Citrix Endpoint Management connector for Exchange ActiveSync now tries to start a connection up to three times. [CXM-58180]
- To effect policies on Exchange, the Citrix Endpoint Management connector for Exchange ActiveSync must compile a **Set-CASMailbox** command that includes all pertinent devices for each mailbox, in two lists: allow and block. If a device isn't included in either list, Exchange falls back to its default access state. If that default access state is different than the desired state for a device, that device becomes out of compliance. So, a user might lose access to their email if the Exchange default access state is blocked and it should be allowed. Or, a user whose access to email should be blocked may be granted access. Citrix Endpoint Management connector for Exchange ActiveSync now makes sure that all devices with a valid desired state are included in each **Set-CasMailbox** command. [CXM-61251]

The following issue is known in version 10.1.8:

If an admin makes a change in the Configure application that modifies configuration data, while the service is doing long-duration operations, such as a snapshot or policy evaluation, the service may enter an indeterminate state. A possible symptom may be that policy changes aren't processed, or snapshots aren't started. To return the service to a working state, the service must be restarted. You may need to use the Windows Services manager to terminate the service process before starting the service. [CXM-61330]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

What's new in version 10.1.7

- XenMobile Mail Manager is now a Citrix Endpoint Management connector for Exchange ActiveSync.
- We've deprecated the **Disable Pipelining** option in the Exchange configuration dialog box. You can achieve the same functionality by configuring multiple steps for each command in the config.xml file. [CXM-54593]

The following issues are fixed in version 10.1.7:

- In the Snapshot History window, error messages might be shown with little context. Now, error messages are prefixed with the context of where they occurred. [CXM-49157]
- The XmmGoogleAnalytics .dll did not have the corresponding file version for the release. [CXM-52518]
- To improve diagnostics, we recently changed the string format for a list of device IDs used to set a mailbox Allowed/Blocked state. A specification of too many devices, however, exceeded the maximum string size. Now, we use an internal array data structure. This structure does not have a size limit and also formats the data appropriately for diagnostic purposes. [CXM-52610]
- When device policies that aren't in sync with Exchange are detected, their commands may include devices that do not belong to the relevant mailbox. Citrix Endpoint Management connector for Exchange ActiveSync now makes sure that commands to Exchange represent only devices that belong to their respective mailboxes. [CXM-54842]
- In some environments, a Microsoft assembly isn't available. The required assembly is now explicitly installed with the application. [CXM-55439]
- If the Distinguished Names for devices or mailboxes have spaces between the attribute name and the equals, or spaces after the equals and before the value, the Citrix Endpoint Management connector for Exchange ActiveSync may not properly match a device with its mailbox and the opposite way. The result might be that some devices and/or mailboxes are rejected during the snapshot reconciliation. [CXM-56088]

> **Note:**
>
> The following What's New sections refer to the Citrix Endpoint Management connector for Exchange ActiveSync by its former name of XenMobile Mail Manager. The name changed from version 10.1.7.

Update in version 10.1.6.20

An update to 10.1.6 has the following fix in version 10.1.6.20:

- When device policies that aren't in sync with Exchange are detected, their commands may include devices that do not belong to the relevant mailbox. XenMobile® Mail Manager now insures

© 1997–2025 Citrix Systems, Inc. All rights reserved.

that commands to Exchange represent only devices that belong to their respective mailboxes. [CXM-54842]

What's new in version 10.1.6

XenMobile Mail Manager version 10.1.6 has the following fixed issues and enhancements:

- The snapshot history window, at times, enters a state where the window is no longer updating. The windows refresh mechanism is improved to update more reliably. [CXM-47983]
- Two separate modes and code paths were used for partitioned and non-partitioned snapshots. Because non-partitioned snapshots are equivalent to partitioned snapshots with a configuration using a single "*"partition, the non-partitioned snapshot mode is eliminated. The default snapshot mode is now partitioned snapshots with 36 partitions (0–9, A–Z). [CXM-49093]
- In the Snapshot History window, error messages are overwritten by status messages. Now, the XenMobile Mail Manager provides two separate fields so that users can view status and errors simultaneously. [CXM-51942]
- When connecting to Exchange Online (Office 365), snapshot-related queries might result in a truncated dataset. This issue may occur when the XenMobile Mail Manager runs a multi-command pipelined script. The upstream command can't pass the data quickly enough to the downstream command, which then completes the work prematurely. Incomplete data occurs as a result. XenMobile Mail Manager can now mimic the pipeline itself and wait until the upstream command is done before invoking the downstream command. This change should result in all data being processed and captured. [CXM-52280]
- If a non-resolvable error occurs in a policy update command to Exchange, the same command is returned to the work queue repeatedly for a long period. This situation resulted in the command being sent to Exchange many times. In this version of XenMobile Mail Manager, a command that results in an error is only returned to the work queue a discrete number of times. [CXM-52633]
- If a policy update for a specific mailbox involved the allowing or blocking of all devices: The issued **Set-CASMailbox** command would fail because of the empty list being converted to an empty string instead of a **NULL**. The proper data is now sent. [CXM-53759]
- When processing a new device, Exchange can return the state as "DeviceDiscovery"for some time (usually 15 minutes). XenMobile Mail Manager wasn't specifically handling this state. XenMobile Mail Manager now handles the state. In the Monitor tab of the UI, users can filter for devices in this state. [CXM-53840]
- XenMobile Mail Manager did not check for the ability to write to the XenMobile Mail Manager database. So, if permissions were restricted, the behavior might not be predicted. XenMobile Mail Manager now captures and validates required permissions from the database. XenMobile Mail Manager indicates reduced permissions when either testing the connection (message shown) or in the Database indicator (hover for message) at the bottom of the main Configure window. [CXM-54219]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Depending on the current workload, when directed to, the XenMobile Mail Manager service may not stop promptly. So, the service appears to be in an unresponsive state. Improvements allow ongoing tasks to be interrupted, resulting in a more graceful shutdown. [CXM-54282]

What's new in version 10.1.5

XenMobile Mail Manager version 10.1.5 has the following fixed issues:

- When Exchange is applying throttling to XenMobile Mail Manager activity, there's no indication (outside of the logs) that the throttling is occurring. With this release, a user can hover over the active snapshot and a "throttling"state appears. Also, while XenMobile Mail Manager is being throttled, the start of a major snapshot is prohibited until Exchange lifts the throttling embargo. [CXM-49617]
- If XenMobile Mail Manager is being throttled by Exchange during a major snapshot: It's possible that an insufficient amount of time is allowed to elapse before running the next attempt of a snapshot. This issue results in further throttling and a failed snapshot. XenMobile Mail Manager now waits a minimum of the time that Exchange specifies to wait between snapshot attempts. [CXM-49618]
- When diagnostics is enabled, the commands file shows **Set-CasMailbox** commands that have missing hyphens before each property name. This issue only occurs in the formatting of the diagnostics file and not the actual command to Exchange. The missing hyphen prevents a user from cutting the command and directly pasting it to a PowerShell prompt for testing or validation. The hyphens have been added. [CXM-52520]
- If a mailbox identity is of the form `lastname, firstname`, Exchange adds a backslash before the comma when returning data from a query. This backslash must be stripped when the XenMobile Mail Manager uses the identity to query for more data. [CXM-52635]

Known limitations

> **Note:**
>
> The following limitation is resolved in version 10.1.6.

XenMobile Mail Manager has a known limitation that can cause commands to Exchange to fail. To apply policy changes to Exchange, a **Set_CASMailbox** command is issued by the XenMobile Mail Manager. This command can take two lists of devices: one to Allow and one to Block. The command is applied to the devices partnered with a mailbox.

These lists are limited to 256 characters each by the Microsoft API. If one of those lists exceeds the limitation, the command fails in its entirety, preventing the policies for those devices of the mailbox to be set. The error reported, which appear in the XenMobile Mail Manager logs, would look like the following. The example is for the blocked list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

“Message:’Cannot bind parameter ‘ActiveSyncBlockedDeviceIDs’to the target. Exception setting “ActiveSyncBlockedDeviceIDs”: “The length of the property is too long. The maximum length is 256 and the length of the value provided is …”

Device ID lengths can vary, but a good guideline is that about 10 devices or more simultaneously Allowed or Blocked might exceed the limit. Although having that many devices associated with a specific mailbox is rare, it is a possibility. Until the Mail Manager is improved to handle such a scenario, we recommend that you limit the number of devices associated with a user and mailbox to 10 or fewer. [CXM-52633]

What’s new in version 10.1.4

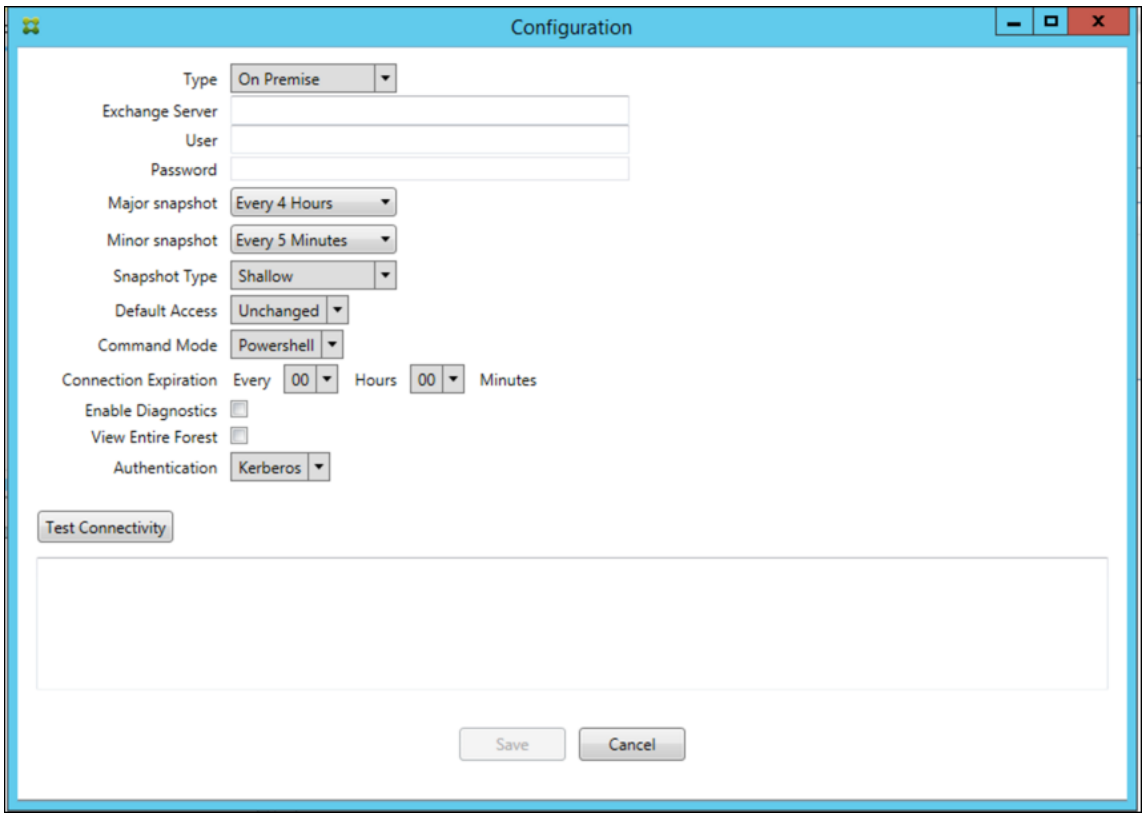
XenMobile Mail Manager version 10.1.4 has the following fixed issues:

- Because of its weakening security, the PCI Council is deprecating TLS 1.0 and TLS 1.1. Support for 1.2 is added to the XenMobile Mail Manager. [CXM-38573, CXM-32560]
- XenMobile Mail Manager includes a new diagnostic file. When **Enable Diagnostics** is selected in the Exchange specification, a new Snapshot History file is generated. With every snapshot attempt, a line is added to the file with the results of the snapshot. [CXM-49631]
- In the Commands diagnostic file, the list of devices allowed or blocked did not appear for the **Set-CASMailbox** command. Instead the internal class name was shown in the file for the related arguments. XenMobile Mail Manager now shows the list of deviceIDs as a comma-delimited list. [CXM-50693]
- When an attempt to acquire a connection to the Exchange fails because of a bad specification: An incorrect message overrides the error message: “All connections in use”. More descriptive messages now appear, such as “All connections are inoperable”, “Connection pool is empty”, “All connections are throttled”, and “No available connections”. [CXM-50783]
- Sometimes, Allow/Block/Wipe commands are queued up in the XenMobile Mail Manager internal cache multiple times. This issue causes a delay in the command being sent to Exchange. XenMobile Mail Manager now only queues up one instance of each command. [CXM-51524]

What’s new in version 10.1.3

- **Google Analytics support:** We want to know how you use the XenMobile Mail Manager so we can focus on where we can make the product better.
- **Setting for enabling diagnostics:** An **Enable Diagnostic** checkbox appears in the Configure console on the **Configuration** dialog box.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Fixed issues in version 10.1.3

- In the **Snapshot History** window, tooltips that show the current state of the snapshot do not reflect the actual state. [CXM-5570]
  Occasionally, the XenMobile Mail Manager can't write to the Commands diagnostics file. When this occurs, the command history isn't logged in its entirety. [CXM-49217]
- When an error occurs with a connection, the connection may not be marked as "errored". As a result, a subsequent command may attempt to use the connection and cause another error. [CXM-49495]
- When throttling from the Exchange Server occurs, an exception might be thrown in the Check Health routine. As a result, connections that have experienced an error or have expired might not be purged. Also, the XenMobile Mail Manager might not create connections until the throttling time expires. [CXM-49794].
- When the max session count for Exchange is exceeded, XenMobile Mail Manager reports the error "Device Capture Failed,"which isn't an accurate message. Instead, the message should indicate that the two sessions that the XenMobile Mail Manager normally uses for Exchange communication are in use. [CXM-49994]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

What's new in version 10.1.2

- **Improved connection to Exchange:** XenMobile Mail Manager uses PowerShell sessions to communicate with Exchange. A PowerShell session, especially when dealing with Office 365, can become unstable after a while, blocking subsequent commands from succeeding. XenMobile Mail Manager can now set an expiration period for connections. When the connection reaches its expiration time, the XenMobile Mail Manager gracefully shuts down the PowerShell session and creates a session. By doing so, the PowerShell session is less likely to become unstable, significantly reducing the chance of a snapshot failure.
- **Improved snapshot workflow:** Major snapshots are a time-consuming and process-intensive operation. If an error occurs during a snapshot, the XenMobile Mail Manager now attempts multiple times (up to three) to complete a snapshot. Subsequent attempts do not start from the beginning. XenMobile Mail Manager continues from where it left off. This enhancement improves the success rate of snapshots in general by allowing transient errors to pass while a snapshot is still in progress.
- **Improved diagnostics:** Troubleshooting snapshot operations are now easier with three new diagnostics files optionally generated during a snapshot. These files help identify PowerShell command issues, mailboxes with missing information, and devices that can't be related to a mailbox. An admin can use these files to identify data that may not be correct in Exchange.
- **Improved memory usage:** XenMobile Mail Manager is now more efficient in its use of memory. Admins can schedule the XenMobile Mail Manager to restart automatically to provide a clean slate to the system.
- **Microsoft .NET Framework 4.6 prerequisite:** The prerequisite version of Microsoft .NET Framework is now version 4.6.

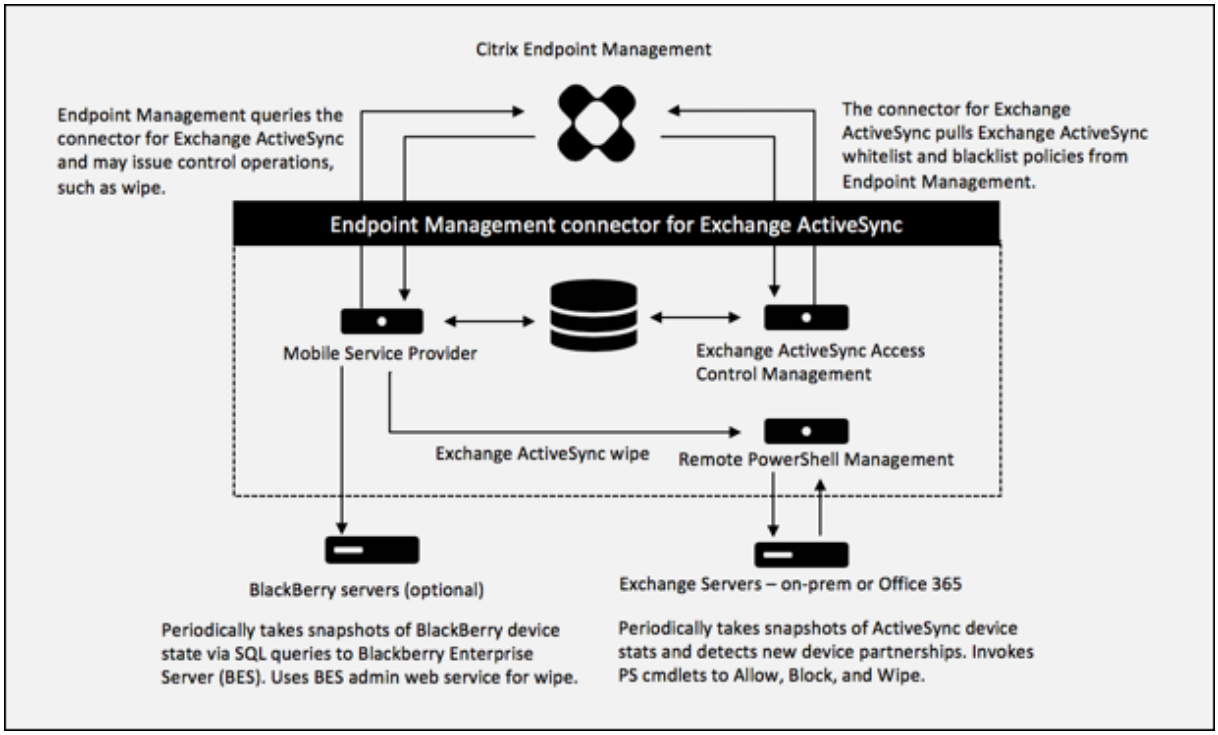
Fixed issues

- Prompt for credentials error: Office 365 session instability often caused this error. The Improved Connection to Exchange enhancement addresses the problem. (XMHELP-293, XMHELP-311, XMHELP-801)
- Mailbox and device count inaccuracies: XenMobile Mail Manager has an improved Mailbox-to-Device association algorithm. The Improved Diagnostics feature helps in the identification of mailboxes and devices that the XenMobile Mail Manager deems aren't within its realm of responsibility. (XMHELP-623)
- Allow/Block/Wipe commands not being recognized: A bug was fixed where sometimes, XenMobile Mail Manager allow/block/wipe commands aren't recognized. (XMHELP-489)
- Memory management: Better memory management and mitigation. (XMHELP-419)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Architecture

The following diagram shows the main components of the Citrix Endpoint Management connector for Exchange ActiveSync. For a detailed reference architecture diagram, see Architecture.



The two main components are:

- **Exchange ActiveSync Access Control Management:** Communicates with Citrix Endpoint Management to retrieve an Exchange ActiveSync policy from Citrix Endpoint Management, and merges this policy with any locally defined policy to determine the Exchange ActiveSync devices that should be allowed or denied access to Exchange. Local policy allows extending the policy rules to allow access control by Active Directory Group, User, Device Type, or Device User Agent (generally the mobile platform version).
- **Remote PowerShell Management:** Responsible for scheduling and invoking remote PowerShell commands to enact the policy compiled by Exchange ActiveSync Access Control Management. Periodically takes a snapshot of the Exchange ActiveSync database to detect new or changed Exchange ActiveSync devices.

System requirements and prerequisites

The following minimum system requirements are required to use the Citrix Endpoint Management connector for Exchange ActiveSync:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Windows Server 2016, Windows Server 2012 R2, or Windows Server 2008 R2 Service Pack 1. Must be an English-based server. Support for Windows Server 2008 R2 Service Pack 1 ends on January 14, 2020 and support for Windows Server 2012 R2 ends on October 10, 2023.
- Microsoft SQL Server 2016 Service Pack 2, SQL Server 2014 Service Pack 3, or SQL Server 2012 Service Pack 4.
- Microsoft .NET Framework 4.6.
- Blackberry Enterprise Service, version 5 (optional).

Minimum supported versions of Microsoft Exchange Server:

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013 (support ends April 11, 2023)
- Exchange Server 2010 Service Pack 3 (support ends January 14, 2020)

Prerequisites

- Windows Management Framework must be installed.
  - PowerShell V5, V4, and V3
- The PowerShell execution policy must be set to RemoteSigned via Set-ExecutionPolicy RemoteSigned.
- TCP port 80 must be open between the computer running the connector for Exchange ActiveSync and the remote Exchange Server.

Device email clients: Not all email clients consistently return the same ActiveSync ID for a device. Because the connector for Exchange ActiveSync expects a unique ActiveSync ID for each device, only email clients that consistently generate the same, unique ActiveSync ID for each device is supported. These email clients have been tested by Citrix and done without errors:

- Samsung native email client
- iOS native email client

Exchange: The requirements for the on-premises computer running Exchange are as follows:

The credentials specified in the Exchange Configuration UI must be able to connect to the Exchange Server and be given full access to run the following Exchange-specific PowerShell cmdlets.

- **For Exchange Server 2010 SP2:**
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - `Get-ActiveSyncDevice`
  - `Get-ActiveSyncDeviceStatistics`
  - `Clear-ActiveSyncDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`

- **For Exchange Server 2013 and Exchange Server 2016:**

  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`

- If the connector for Exchange ActiveSync is configured to view the entire forest, permission must have been granted to run: **Set-AdServerSettings -ViewEntireForest $true**
- The supplied credentials must have been granted the right to connect to the Exchange Server via the remote Shell. By default, the user who installed Exchange has this right.
- To establish a remote connection and run remote commands, the credentials must correspond to a user who is an administrator on the remote machine. You can use Set-PSSessionConfiguration to eliminate the administrative requirement, but discussion of that command is beyond the scope of this document. For more information, see the Microsoft article About Session Configurations.
- The Exchange Server must be configured to support remote PowerShell requests via HTTP. Typically, an administrator running the following PowerShell command on the Exchange Server is all that is required: WinRM QuickConfig.
- Exchange has many throttling policies. One of the policies controls how many concurrent PowerShell connections are allowed per user. The default number of simultaneous connections allowed for a user is 18 on Exchange 2010. When the connection limit is reached, the connector for Exchange ActiveSync isn't able to connect to Exchange Server. There are ways to change the maximum allowed simultaneous connections via PowerShell that are beyond the scope of this documentation. If interested, investigate Exchange throttling policies as related to remote management with PowerShell.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Requirements for Office 365 Exchange

- **Permissions:** The credentials specified in the Exchange Configuration UI must be able to connect to Office 365 and be given full access to run the following Exchange-specific PowerShell cmdlets:
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`
- **Privileges:** The supplied credentials must have been granted the right to connect to the Office 365 server via the remote Shell. By default, the Office 365 online administrator has the requisite privileges.
- **Throttling policies:** Exchange has many throttling policies. One of the policies controls how many concurrent PowerShell connections are allowed per user. The default number of simultaneous connections allowed for a user is three on Office 365. When the connection limit is reached, the connector for Exchange ActiveSync isn't able to connect to Exchange Server. There are ways to change the maximum allowed simultaneous connections via PowerShell that are beyond the scope of this documentation. If interested, investigate Exchange throttling policies as related to remote management with PowerShell.

Install and configure

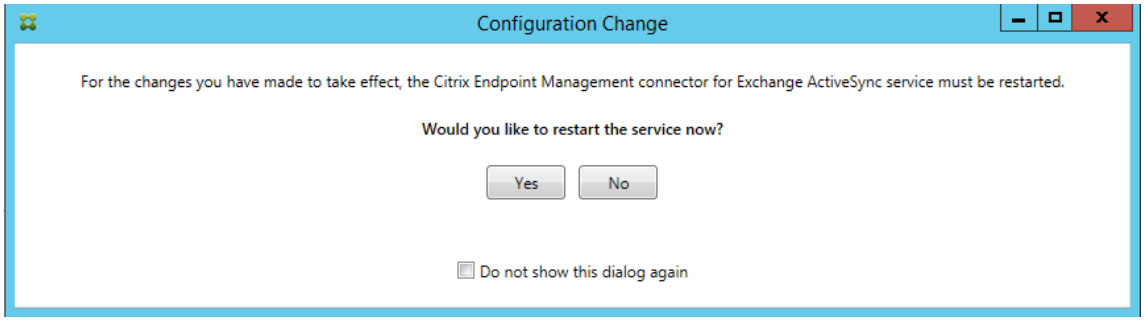
1. Click the XmmSetup.msi file and then follow the prompts in the installer to install the Citrix Endpoint Management connector for Exchange ActiveSync.
2. Leave **Launch the Configure utility** selected in the last screen of the setup wizard. Or, from the **Start** menu, open the connector for Exchange ActiveSync.
3. Configure the following database properties:
   - Select the **Configure > Database** tab.
   - Enter the name of the SQL Server (defaults to localhost).
   - Keep the database as the default **CitrixXmm**.
4. Select one of the following authentication modes used for SQL:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **SQL:** Enter the user name and password of a valid SQL user.
- **Windows Integrated:** If you select this option, the logon credentials of the XenMobile Mail Manager Service must be changed to a Windows account that has permissions to access the SQL Server. To do this, open **Control Panel > Administrative Tools > Services**, right-click the XenMobile Mail Manager Service entry and then click the **Log On** tab.

If Windows Integrated is also chosen for the BlackBerry database connection, the Windows account specified here must also be given access to the BlackBerry database.

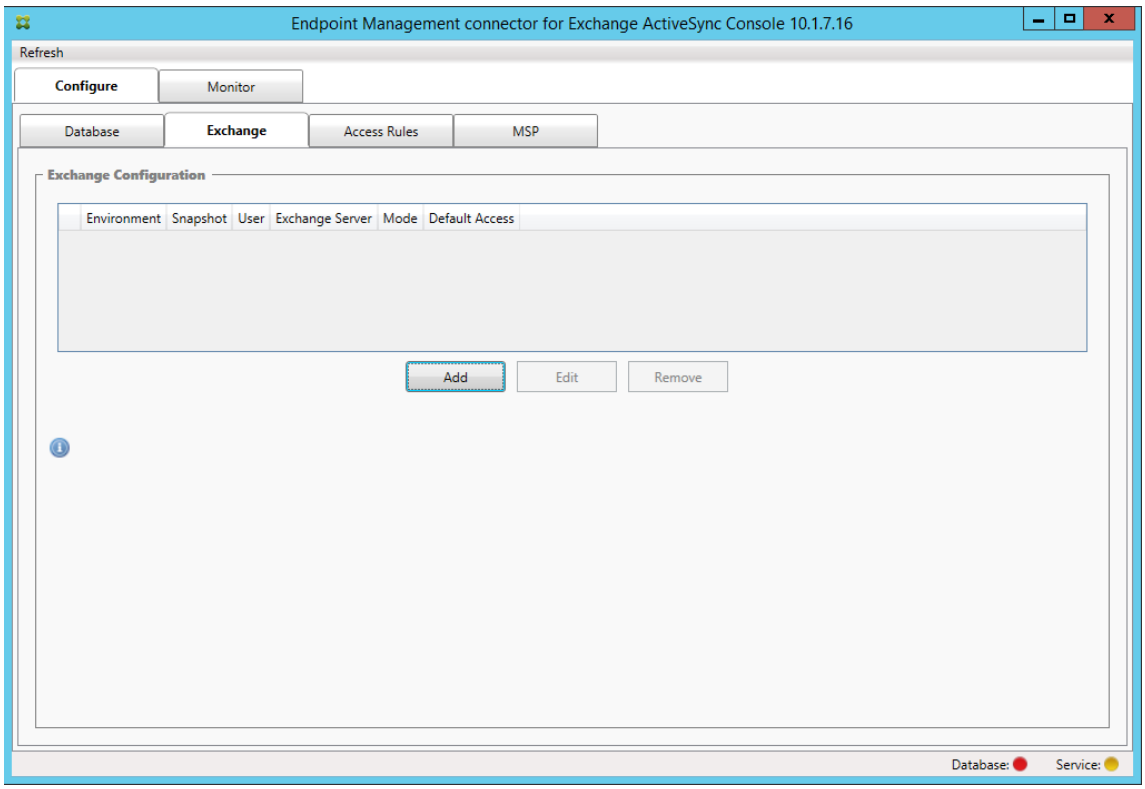
5. Click **Test Connectivity** to check that a connection can be made to the SQL Server and then click **Save**.
6. A message prompts you to restart the service. Click **Yes**.



7. Configure one or more Exchange Servers:

- If managing a single Exchange environment, specify a single server only. If managing multiple Exchange environments, specify a single Exchange Server for each Exchange environment.
- Click the **Configure > Exchange** tab and then click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



8. Select the type of Exchange Server environment: **On Premise** or **Office 365**.

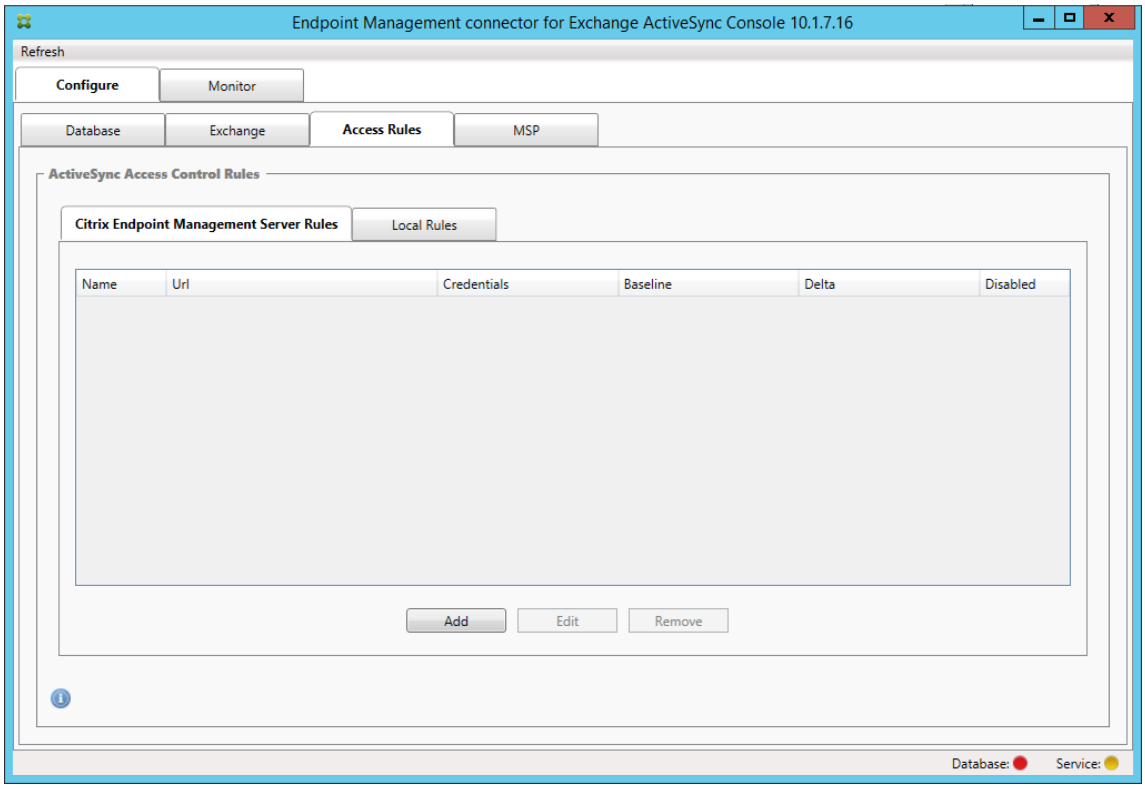
   - If you select **On Premise**, enter the name of the Exchange Server to use for Remote PowerShell commands.
   - Enter the **user name** of a Windows identity that has appropriate rights on the Exchange Server as specified within the Requirements section and then enter the **Password** for the user.
   - Select the schedule for running Major snapshots. A major snapshot detects every Exchange ActiveSync partnership.
   - Select the schedule for running Minor snapshots. A minor snapshot detects newly created Exchange ActiveSync partnerships.
   - Select the Snapshot Type: **Deep** or **Shallow**. Shallow snapshots are typically much faster and are sufficient to do all the Exchange ActiveSync Access Control functions of the connector for Exchange ActiveSync.
   - Select the Default Access: **Allow**, **Block**, or **Unchanged**. This setting controls how all devices other than those devices identified by explicit Citrix Endpoint Management or Local rules are treated. If you select **Allow**, ActiveSync access to all such devices is allowed. If you select **Block**, access is denied. If you select **Unchanged**, no change is made.
   - Select the ActiveSync Command Mode: **PowerShell** or **Simulation**.
   - In **PowerShell** mode, the connector for Exchange ActiveSync issues PowerShell commands to enact the desired access control. In Simulation mode, the connector for

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Exchange ActiveSync does not issue PowerShell commands, but logs the intended command and intended outcomes to the database. In Simulation mode, the user can then use the **Monitor** tab to see what would have happened if PowerShell mode was enabled.

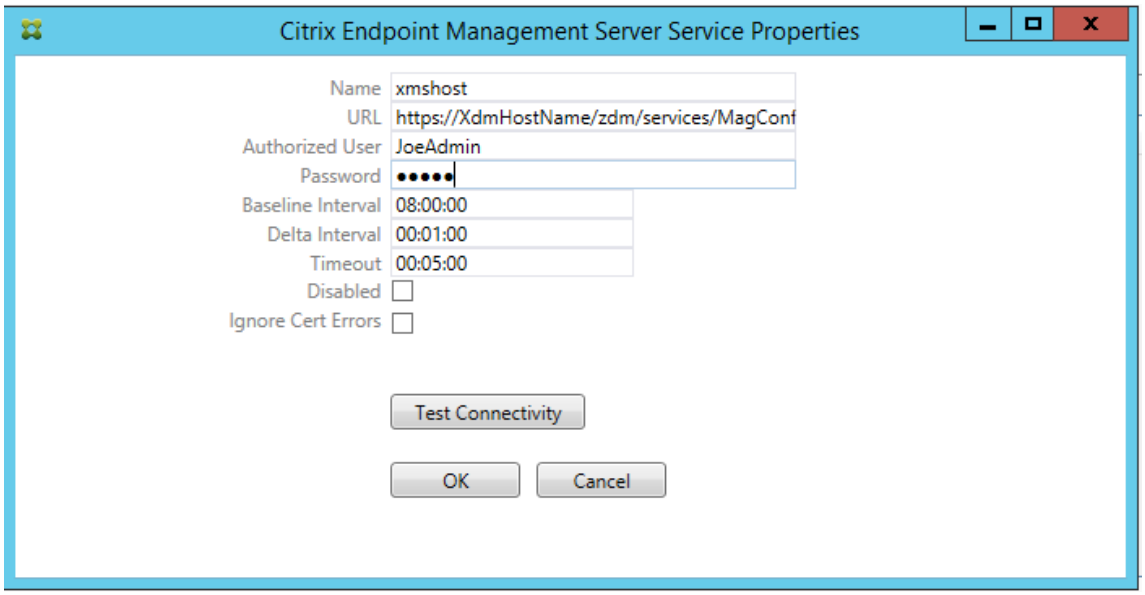
- In **Connection Expiration**, set the hours and minutes for the life of a connection. When a connection reaches the age specified, the connection is marked as expired, so that the connection is never used again. When the expired connection is no longer used, the connector for Exchange ActiveSync gracefully shuts down the connection. When a connection is needed again, a new connection is initialized if none is available. If none is specified, the default of 30 minutes is used.
- Select **View Entire Forest** to configure the connector for Exchange ActiveSync to view the entire Active Directory forest in the Exchange environment.
- Select the authentication protocol: **Kerberos** or **Basic**. The connector for Exchange ActiveSync supports Basic authentication for on-premises deployments. This enables the connector to be used when the connector server is not a member of the domain in which the Exchange server resides.
- Click **Test Connectivity** to check that a connection can be made to the Exchange Server and then click **Save**.
- A message prompts you to restart the service. Click **Yes**.

9. Configure the access rules: Select the **Configure > Access Rules** tab, click the **Citrix Endpoint Management Rules** tab, and then click **Add**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

10. On the **Citrix Endpoint Management server Service Properties** page, modify the URL string to point to the Citrix Endpoint Management server. For example, if the instance name is `zdm`, enter `https://<XdmHostName>/zdm/services/MagConfigService`. In the example, replace `XdmHostName` with the IP or DNS address of the Citrix Endpoint Management server.

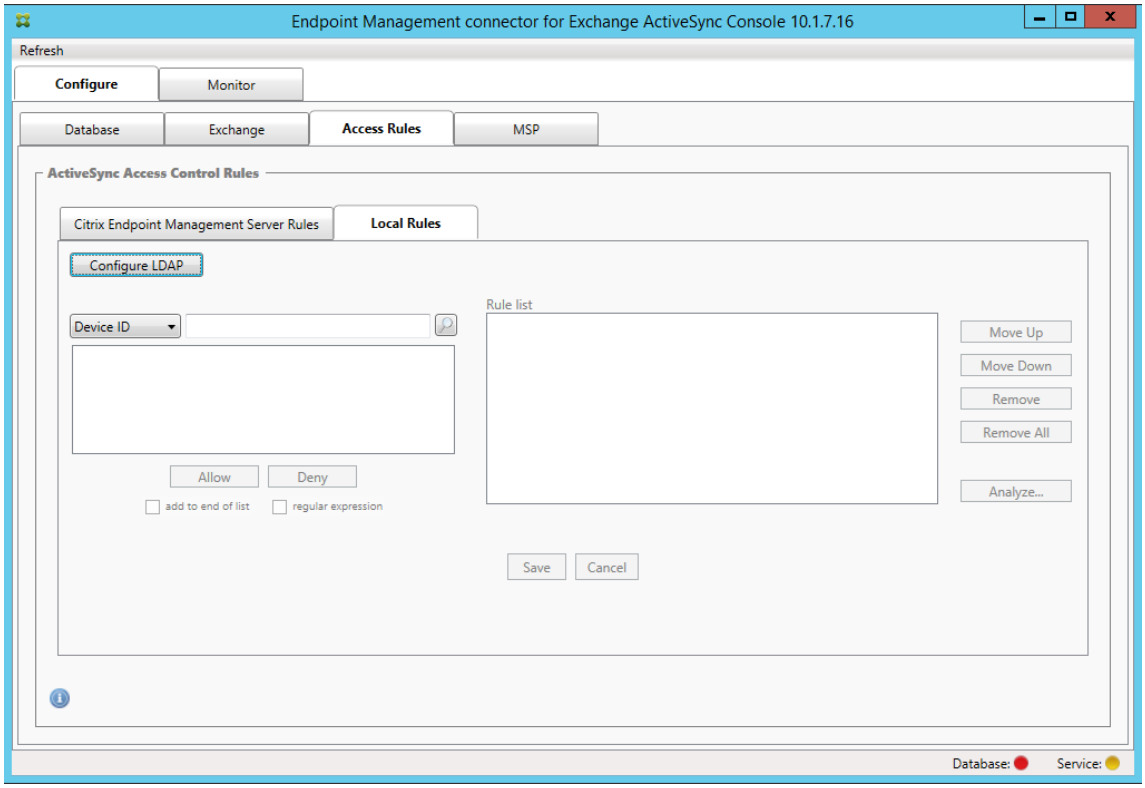


    - Enter an authorized user of the server.
    - Enter the password of the user.
    - Keep the default values for the **Baseline Interval**, **Delta Interval**, and **Timeout** values.
    - Click **Test Connectivity** to check the connection to the server and then click **OK**.

    If the **Disabled** checkbox is selected, the Citrix Endpoint Management Mail Service doesn't collect policies from Citrix Endpoint Management.

11. Click the **Local Rules** tab.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



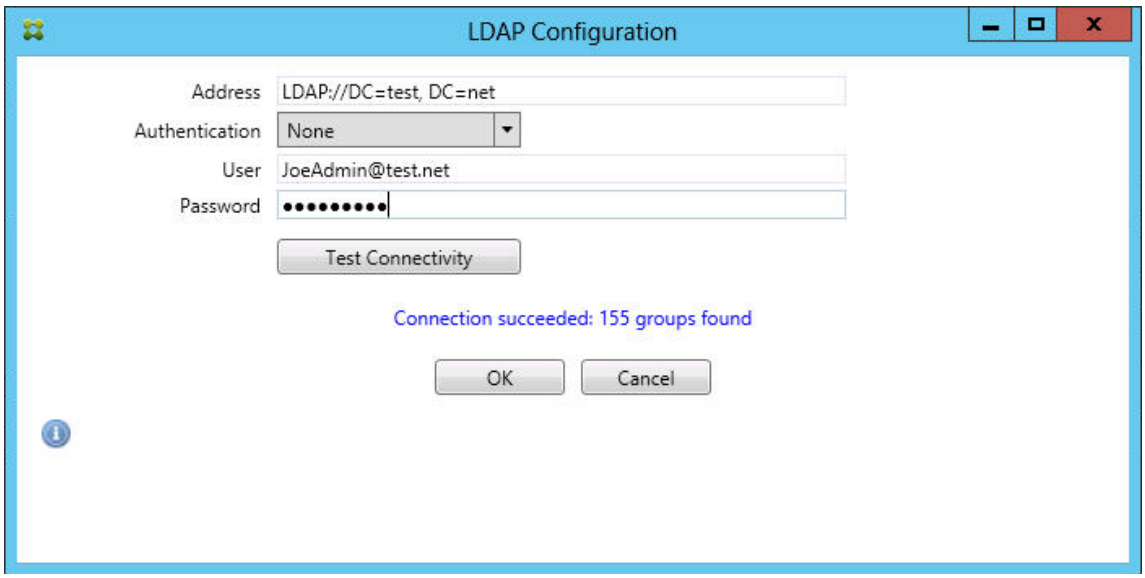
- You can add local rules based on ActiveSync Device ID, Device Type, AD Group, User, or device UserAgent. In the list, select the appropriate type.
- Enter text or text fragments in the text box. Optionally, click the query button to view the entities that match the fragment.

For all types other than Group, the system relies on the devices that have been found in a snapshot. So, if you're just starting and haven't completed a snapshot, no entities are available.

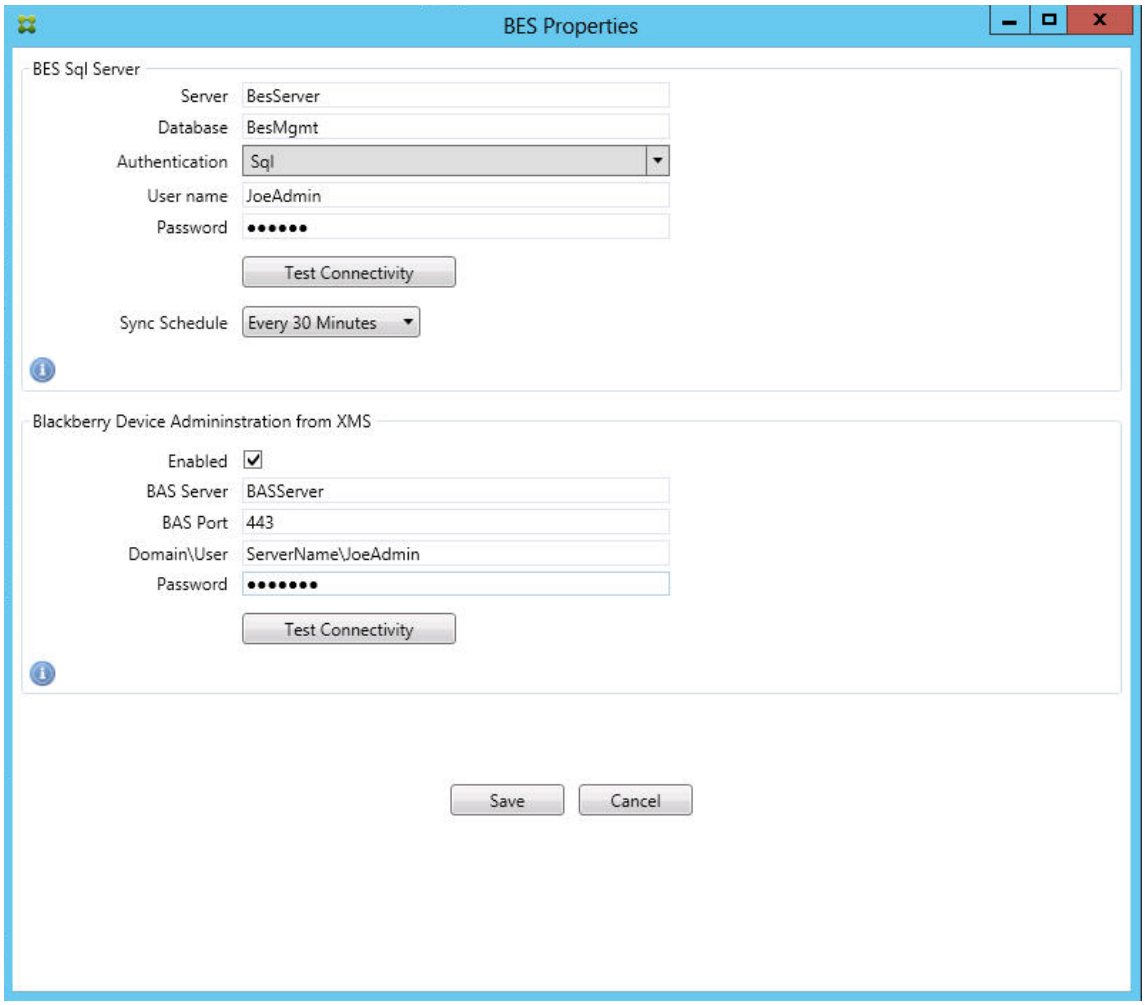
- Select a text value and then click **Allow** or **Deny** to add it to the **Rule List** pane on the right side. You can change the order of the rules or remove them using the buttons to the right of the **Rule List** pane. The order is important because, for a given user and device, rules are evaluated in the order shown and a match on a higher rule (nearer the top) causes subsequent rules to have no effect. For example, if you have a rule allowing all iPad devices and a subsequent rule blocking the user Matt, Matt's iPad will still be allowed because the iPad rule has a higher effective priority than the Matt rule.
- To do an analysis of the rules within the rules list to find any potential overrides, conflicts, or supplemental constructs, click **Analyze** and then click **Save**.

12. If you want to construct local rules that operate on Active Directory Groups, click **Configure LDAP** and then configure the LDAP connection properties.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



13. Optionally, configure one or more instances of BlackBerry Enterprise Server (BES): Click **Add** and then enter the server name of the BES SQL Server



© 1997–2025 Citrix Systems, Inc. All rights reserved.

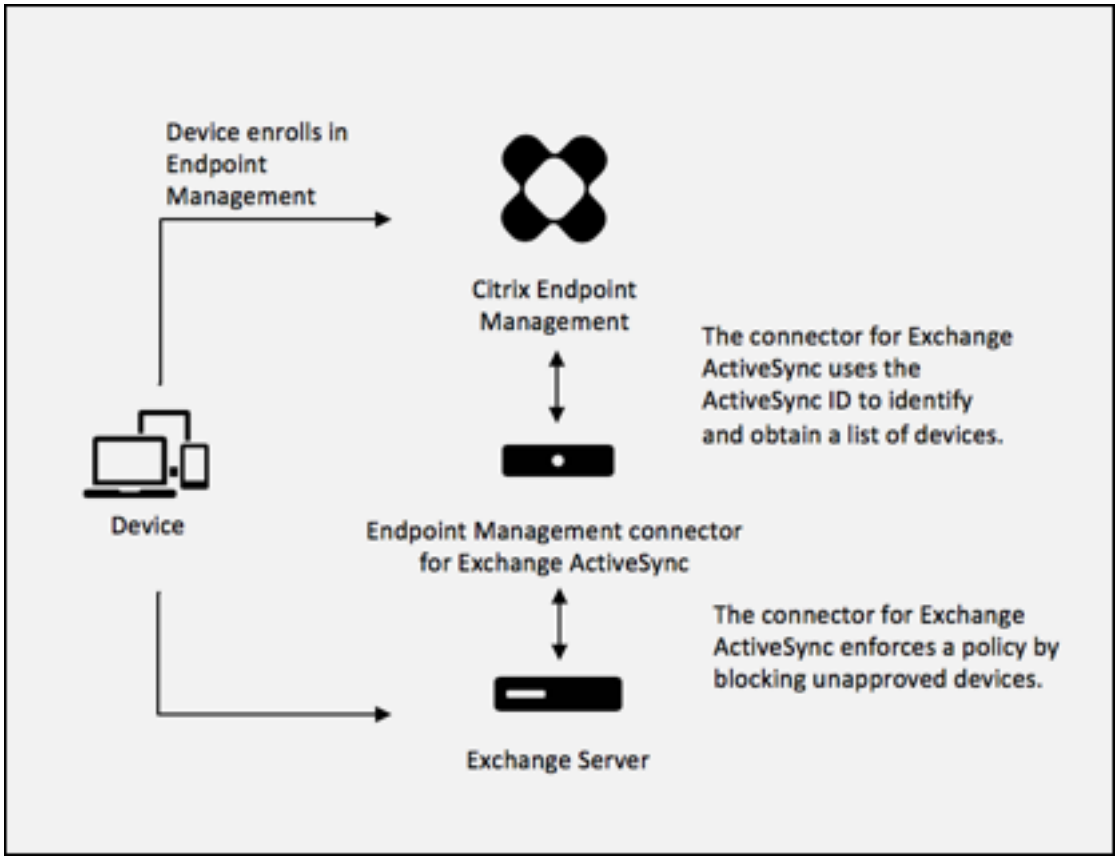
- Enter the database name of the BES management database.
- Select the **Authentication** mode. If you select Windows Integrated authentication, the user account of the connector for the Exchange ActiveSync service is the account that is used to connect to the BES SQL Server. If you also choose Windows Integrated for the connector database connection, the Windows account specified here must also be given access to the connector database.
- If you select **SQL authentication**, enter the user name and password.
- Set the **Sync Schedule**. This is the schedule used to connect to the BES SQL Server and checks for any device updates.
- Click **Test Connectivity** to check connectivity to the SQL Server. If you select Windows Integrated, this test uses the current logged on user and not the connector service user and so it does not accurately test SQL authentication.
- To support remote Wipe and ResetPassword of BlackBerry devices from Citrix Endpoint Management, select the **Enabled** checkbox.
- Enter the BES fully qualified domain name (FQDN).
- Enter the BES port used for the admin web service.
- Enter the fully qualified user and password required by the BES service.
- Click **Test Connectivity** to test the connection to the BES and then click **Save**.

Enforce email policies with ActiveSync IDs

Your corporate email policy may dictate that certain devices aren't approved for corporate email use. To follow this policy, you want to make sure that employees can't access corporate email from such devices. Citrix Endpoint Management connector for Exchange ActiveSync and Citrix Endpoint Management work together to enforce such an email policy. Citrix Endpoint Management sets the policy for corporate email access. When an unapproved device enrolls with Citrix Endpoint Management, the connector for Exchange ActiveSync enforces the policy.

The email client on a device advertises itself to Exchange Server (or Office 365) using the device ID, also known as the ActiveSync ID, which is used to identify the device. Citrix Secure Hub gets a similar identifier and sends the identifier to Citrix Endpoint Management when the device is enrolled. By comparing the two device IDs, the connector for Exchange ActiveSync can determine whether a specific device should have corporate email access. The following figure illustrates this concept:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



If Citrix Endpoint Management sends the connector for Exchange ActiveSync an ActiveSync ID that is different from the ID the device publishes to Exchange, the connector can't indicate to Exchange what to do with the device.

Matching ActiveSync IDs works reliably on most platforms. However, Citrix has found that on some Android implementations, the ActiveSync ID from the device is different from the ID that the mail client advertises to Exchange. To mitigate this problem, you can do the following:

- On Android platforms, Citrix recommends that you use Citrix Secure Mail.

To guarantee that your corporate email access policy is enforced properly, you can adopt a defensive security stance. Configure the Citrix Endpoint Management connector for Exchange ActiveSync to block emails by setting the static policy to **Deny** by default. This means that if an employee configures another email client on an Android device, and ActiveSync ID detection does not work, corporate email denies access to the employee.

Access control rules

Citrix Endpoint Management connector for Exchange ActiveSync provides a rule-based approach for dynamically configuring access control for Exchange ActiveSync devices. A connector access control rule consists of two parts: a matching expression and a desired access state (Allow or Block). A rule

© 1997–2025 Citrix Systems, Inc. All rights reserved.

may be evaluated against a given Exchange ActiveSync device to determine if the rule applies to, or matches the device. There are multiple kinds of matching expressions; for example, a rule may match all devices of a given Device Type, or a specific Exchange ActiveSync device ID, or all devices of a specific user, and so on.

At any point during the adding, removing, and rearranging of the rules in the rule list, clicking the **Cancel** button reverts the rules list back to the state at which it was when first opened. Unless you click **Save**, any changes made to this window are lost if you close the Configure tool.

Citrix Endpoint Management connector for Exchange ActiveSync has three types of rules: local rules, Citrix Endpoint Management server rules (also known as XDM rules), and the default access rule.

Local rules: Local rules have the highest priority: If a device is matched by a local rule, rule evaluation stops. Neither the Citrix Endpoint Management server rules nor the default access rule will be consulted. Local rules are configured locally to the connector for Exchange ActiveSync via the **Configure > Access Rules > Local Rules** tab. Support matching is based on a user's membership within a given Active Directory group. Support matching is based on regular expressions for the following fields:

- Active Sync Device ID
- ActiveSync Device Type
- User Principal Name (UPN)
- ActiveSync User Agent (typically the device platform or email client)

As long as a major snapshot has completed and found devices, you can add either a normal or regular expression rule. If a major snapshot hasn't completed, you can only add regular expression rules.

Citrix Endpoint Management server rules: Citrix Endpoint Management server rules are references to an external Citrix Endpoint Management server that provides rules about managed devices. The Citrix Endpoint Management server can be configured with its own high-level rules that identify the devices to be allowed or blocked based on properties known to Citrix Endpoint Management, such as whether the device is jailbroken or whether the device has forbidden apps. Citrix Endpoint Management evaluates the high-level rules and produces a set of allowed or blocked ActiveSync Device IDs, which are then delivered to the XenMobile Mail Manager.

Default access rule: The default access rule is unique in that it can potentially match every device and is always evaluated last. This rule is the catch-all rule, which means that if a given device does not match a local or Citrix Endpoint Management server rule, the desired access state of the device is determined by the desired access state of the default access rule.

- **Default Access –Allow:** Any device that isn't matched by either a local or Citrix Endpoint Management server rule will be allowed.
- **Default Access –Block:** Any device that isn't matched by either a local or Citrix Endpoint Management server rule will be blocked.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Default Access - Unchanged:** Any device that isn't matched by either a local or Citrix Endpoint Management server rule will not have its access state modified in any way by the connector for Exchange ActiveSync. If a device has been placed into Quarantine mode by Exchange, no action is taken. For example, the only way to remove a device from Quarantine mode is to have an explicitly Local or XDM rule override the quarantine.

About Rule Evaluations

For each device that Exchange reports to the connector for Exchange ActiveSync, the rules are evaluated in sequence, from highest to lowest priority as follows:

- Local rules
- Citrix Endpoint Management server rules
- Default access rule

When a match is found, evaluation stops. For example, if a local rule matches a given device, the device will not be evaluated against any of the Citrix Endpoint Management server rules or the default access rule. This holds true within a given rule type as well. For example, if there's more than a single match for a given device in the local rule list, when the first match is met, evaluation stops.

The connector for Exchange ActiveSync reevaluates the currently defined set of rules when device properties change, or when devices are added or removed, or when the rules themselves change. Major snapshots pick up device property changes and removals at configurable intervals. Minor Snapshots pick up new devices at configurable intervals.

Exchange ActiveSync has rules governing access as well. It is important to understand how these rules work in the context of the connector for Exchange ActiveSync. Exchange may be configured with three levels of rules: personal exemptions, device rules, and organization settings. The connector for Exchange ActiveSync automates access control by programmatically issuing Remote PowerShell requests to affect the personal exemptions lists. These are lists of allowed or blocked Exchange ActiveSync device IDs associated with a given mailbox. When deployed, the connector for Exchange ActiveSync effectively takes over management of the exemption lists capability within Exchange. See the Microsoft article, Device management with Exchange and Configuration Manager.

Analyzing is useful in situations in which multiple rules for the same field have been defined. You can troubleshoot the relationships between rules. You do analysis from the perspective of rule fields. For example, rules are analyzed in groups based on the field that is being matched, such as ActiveSync device ID, ActiveSync device type, User, User Agent.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Rule terminology

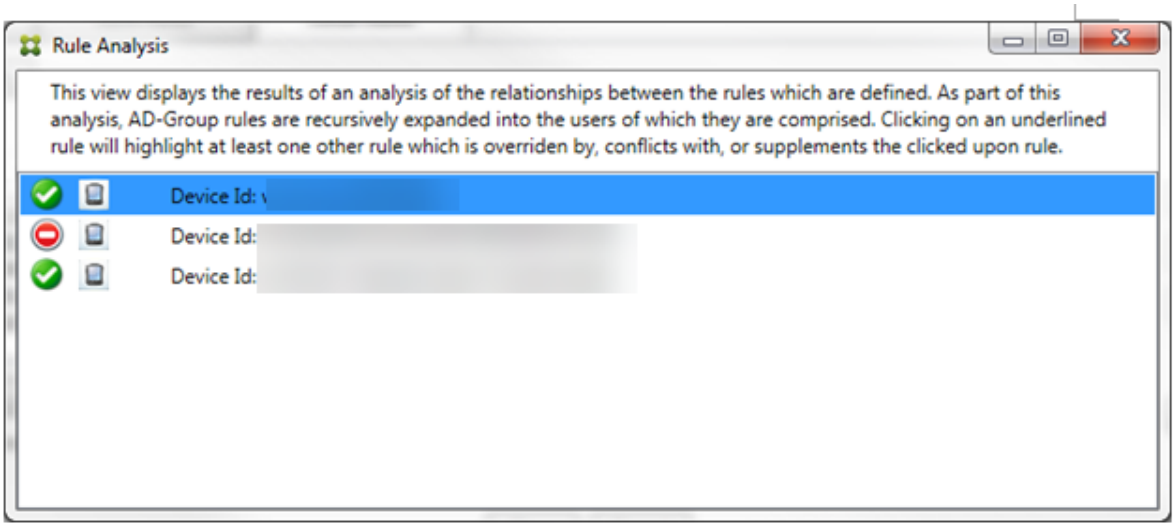
- **Overriding rule:** An override occurs when more than a single rule can apply to the same device. Because rules are evaluated by priority in the list, the later rule instances which might apply might never be evaluated.
- **Conflicting rule:** A conflict occurs when more than a single rule can apply to the same device but the access (Allow/Block) does not match. If the conflicting rules aren't regular expression rules, a conflict always implicitly connotes an override
- **Supplemental rule:** A supplement occurs when more than one rule is a regular expression rule and so there might be a need to make sure that the two (or more) regular expressions can either be combined into a single regular expression rule, or aren't duplicating functionality. A supplementary rule may also conflict in its access (Allow/Block).
- **Primary rule:** The primary rule is the rule that has been clicked within the dialog box. The rule is indicated visually by a solid border line that surrounds it. The rule will also have one or two green arrows pointing up or down. If an arrow points up, the arrow indicates that there are ancillary rules that precede the primary rule. If an arrow points down, this indicates that there are ancillary rules that come after the primary rule. Only a single primary rule can be active at any time.
- **Ancillary rule:** An ancillary rule is related in some way to the primary rule either through override, conflict, or a supplementary relationship. The rules are indicated visually by a dashed border that surrounds them. For each primary rule, there can be between one and many ancillary rules. When clicking any underlined entry, the ancillary rule or rules that are highlighted are always from the perspective of the primary rule. For example, the ancillary rule is overridden by the primary rule, or the ancillary rule conflicts in its access with the primary rule, or the ancillary rule supplements the primary rule.

How types of rules appear in the Rule Analysis dialog box

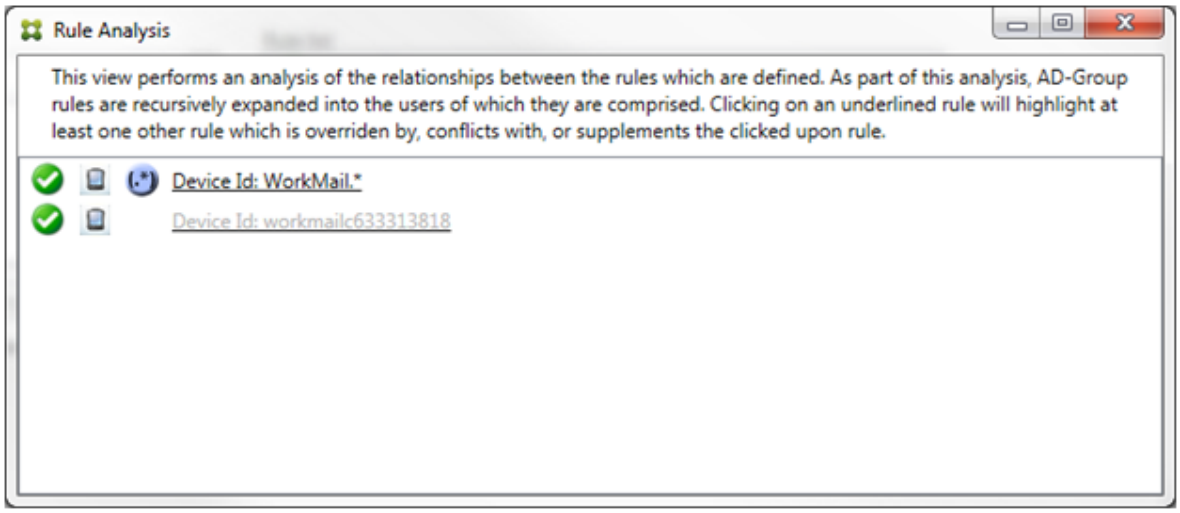
When there are no conflicts, overrides, or supplements, the **Rule Analysis** dialog box has no underlined entries. Clicking any of the items has no impact; for example, normal selected item visuals occur.

The **Rule Analysis** window has a checkbox which, when selected, displays only those rules which are conflicts, overrides, redundancies, or supplements.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

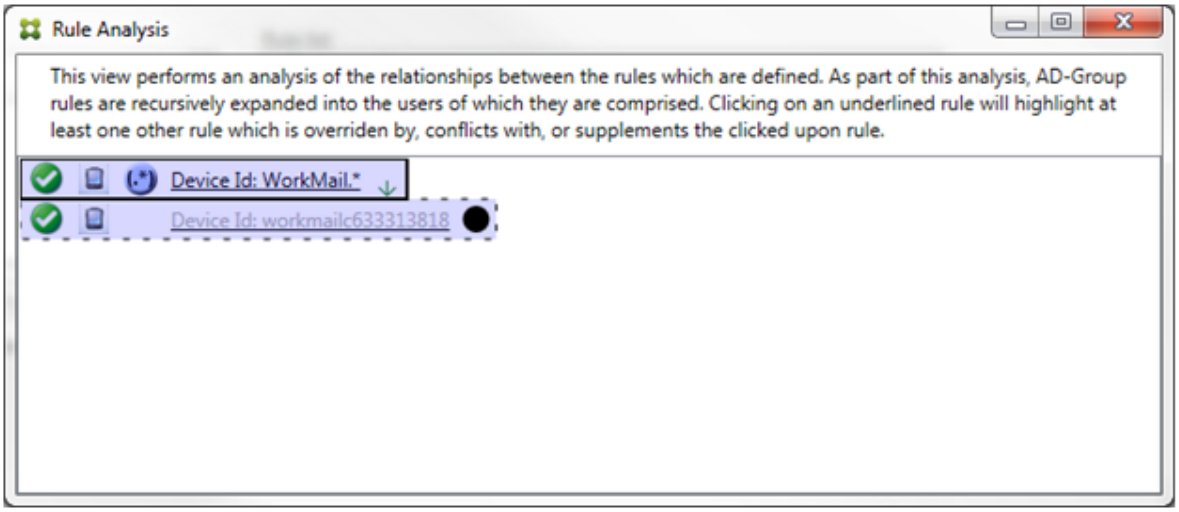


When an override occurs, at least two rules will be underlined: the primary rule and the ancillary rule or rules. At least one ancillary rule appears in a lighter font to indicate that the rule has been overridden by a higher priority rule. You can click the overridden rule to find out which rule or rules have overridden the rule. Anytime an overridden rule has been highlighted either because of the rule being the primary or ancillary rule, a black circle appears next to it as a further visual indication that the rule is inactive. For example, before clicking the rule, the dialog box appears as follows:

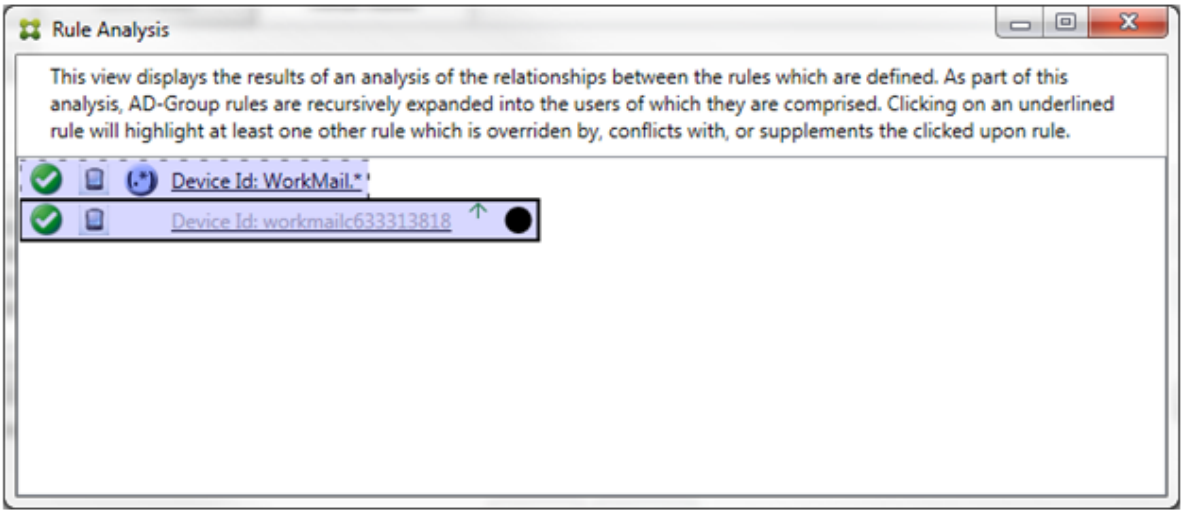


When you click the highest-priority rule, the dialog box appears as follows:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



In this example, the regular expression rule `WorkMail.*` is the primary rule (indicated by the solid border) and the normal rule `workmailc633313818` is an ancillary rule (indicated by the dashed border). The black dot next to the ancillary rule is a visual cue that further indicates that the rule is inactive (will never be evaluated) because of the higher-priority regular expression rule that precedes it. After clicking the overridden rule, the dialog box appears as follows:

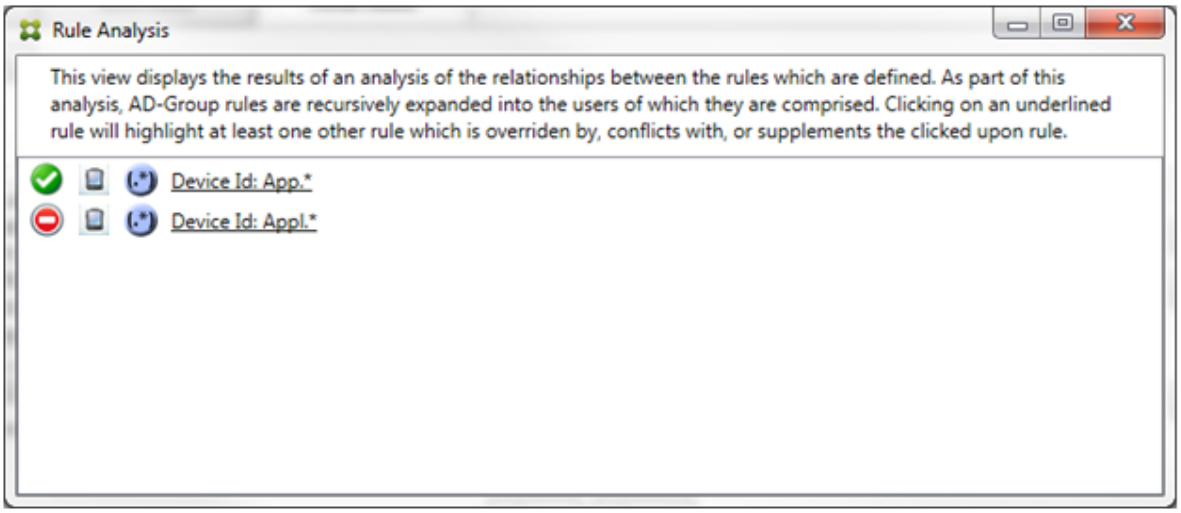


In the preceding example, the regular expression rule `WorkMail.*` is the ancillary rule (indicated by the dashed border) and the normal rule `workmailc633313818` is a primary rule (indicated by the solid border). For this simple example, there's not much difference. For a more complicated example, see the complex expression example later in this topic. In a scenario with many rules defined, clicking the overridden rule would quickly identify which rule or rules had overridden it.

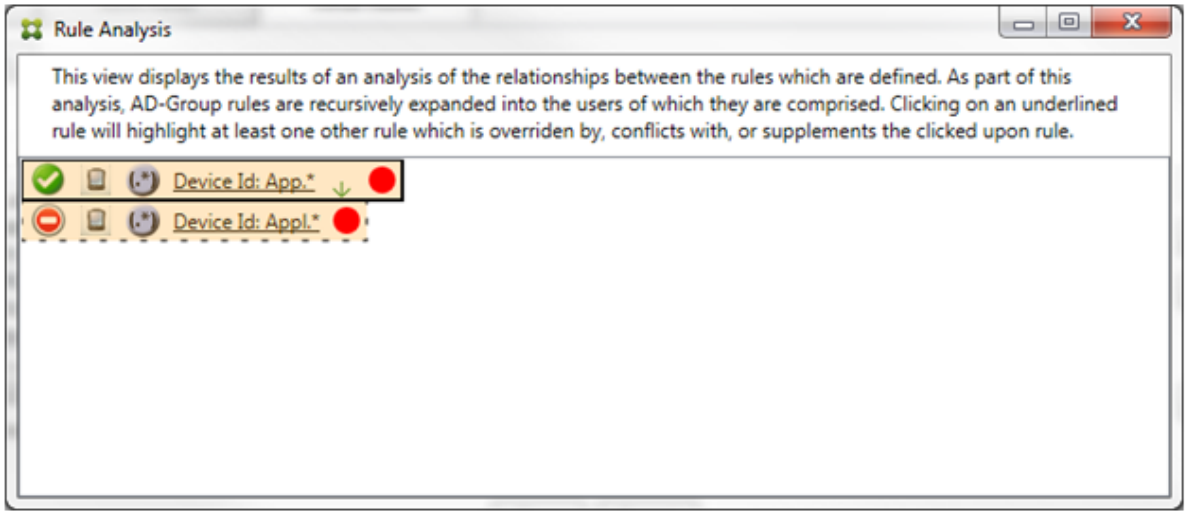
When a conflict occurs, at least two rules will be underlined, the primary rule and the ancillary rule or rules. The rules in conflict are indicated by a red dot. Rules that only conflict with one another are only possible with two or more regular expression rules defined. In all other conflict scenarios, there will not only be a conflict, but an override at play. Before clicking either of the rules in a simple example,

© 1997–2025 Citrix Systems, Inc. All rights reserved.

the dialog box appears as follows:



By inspecting the two regular expression rules, it's evident that the first rule allows all devices with a device ID that has "App"and that the second rule denies all devices with a device ID that has `Appl`. Also, even though the second rule denies all devices with a device ID that has `Appl`, no devices with that match criteria will ever be denied because of the higher precedence of the allow rule. After clicking the first rule, the dialog box appears as follows:

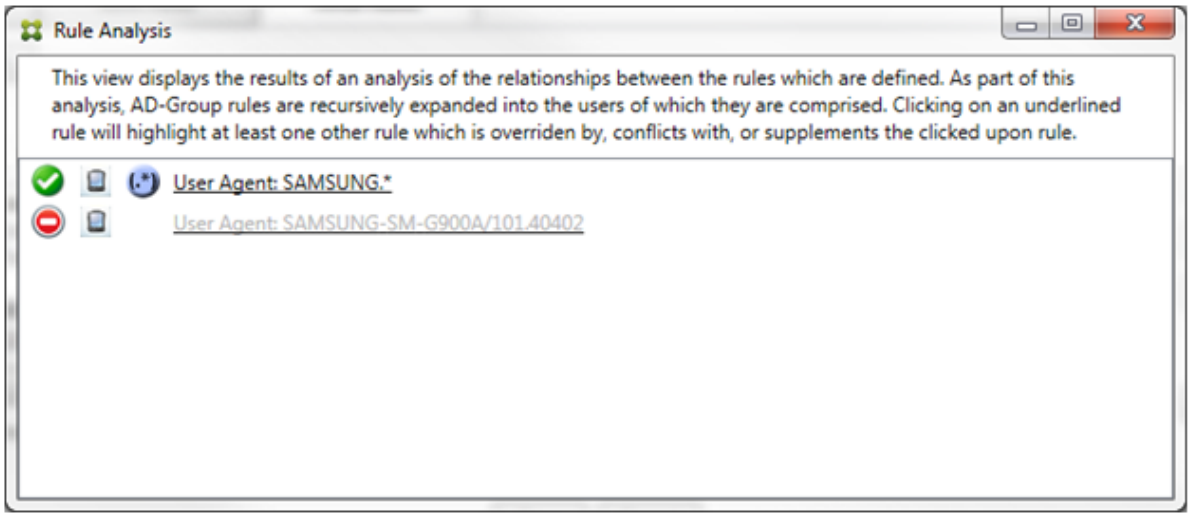


In the preceding scenario, both the primary rule (regular expression rule `App.*`) and the ancillary rule (regular expression rule `Appl.*`) are both highlighted in yellow. This is simply a visual warning to alert you to the fact that you've applied more than a single regular expression rule to a single matchable field, which can mean a redundancy issue or something more serious.

In a scenario with both a conflict and override, both the primary rule (regular expression rule `App.*`) and the ancillary rule (regular expression rule `Appl.*`) are highlighted in yellow. This is simply a visual warning to alert you to the fact that you've applied more than a single regular expression rule

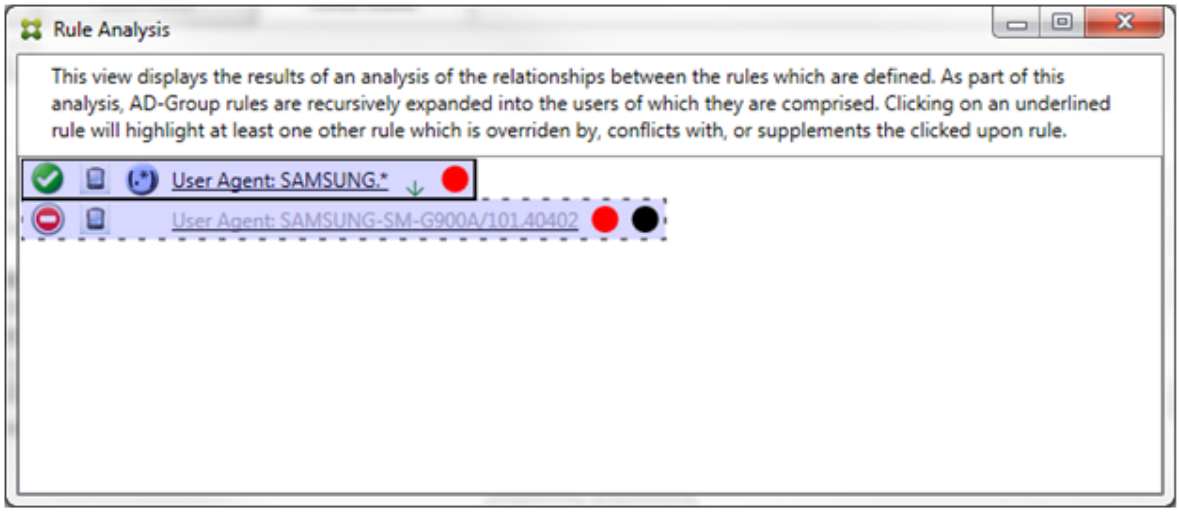
© 1997–2025 Citrix Systems, Inc. All rights reserved.

to a single matchable field, which can mean a redundancy issue or something more serious.



It is easy to see in the preceding example that the first rule (regular expression rule `SAMSUNG.*`) not only overrides the next rule (normal rule `SAMSUNG-SM-G900A/101.40402`), but that the two rules differ in their access (primary specifies Allow, ancillary specifies Block). The second rule (normal rule `SAMSUNG-SM-G900A/101.40402`) is displayed in lighter text to indicate that it has been overridden and is therefore inactive.

After clicking the regular expression rule, the dialog box appears as follows:

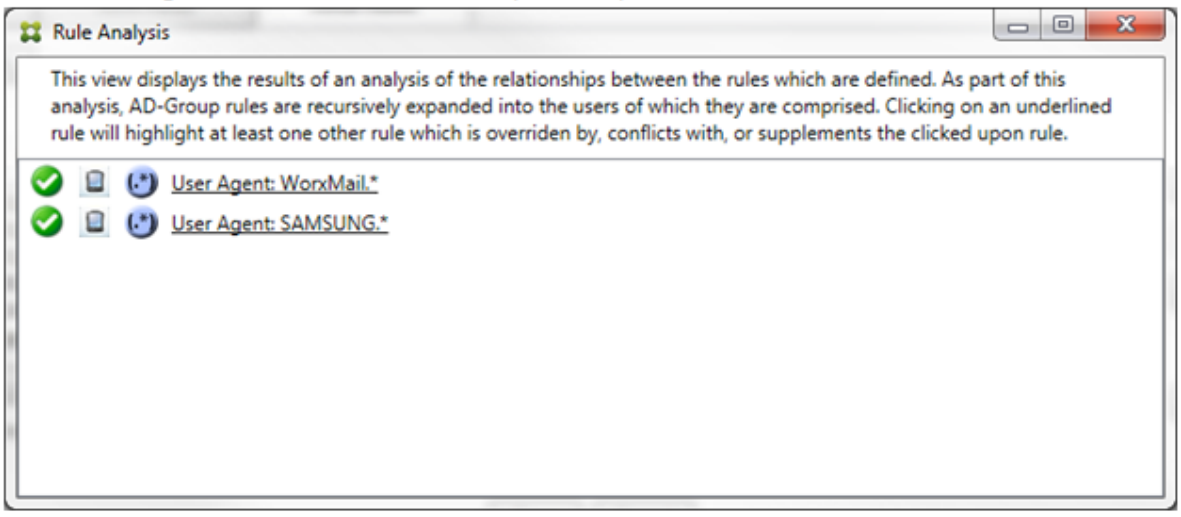


The primary rule (regular expression rule `SAMSUNG.*`) is followed by a red dot to indicate that its access state conflicts with one or more ancillary rules. The ancillary rule (normal rule `SAMSUNG-SM-G900A/101.40402`) is followed by a red dot to indicate that its access state conflicts with the primary rule. That rule is also followed by a black dot to indicate that it is overridden and therefore inactive.

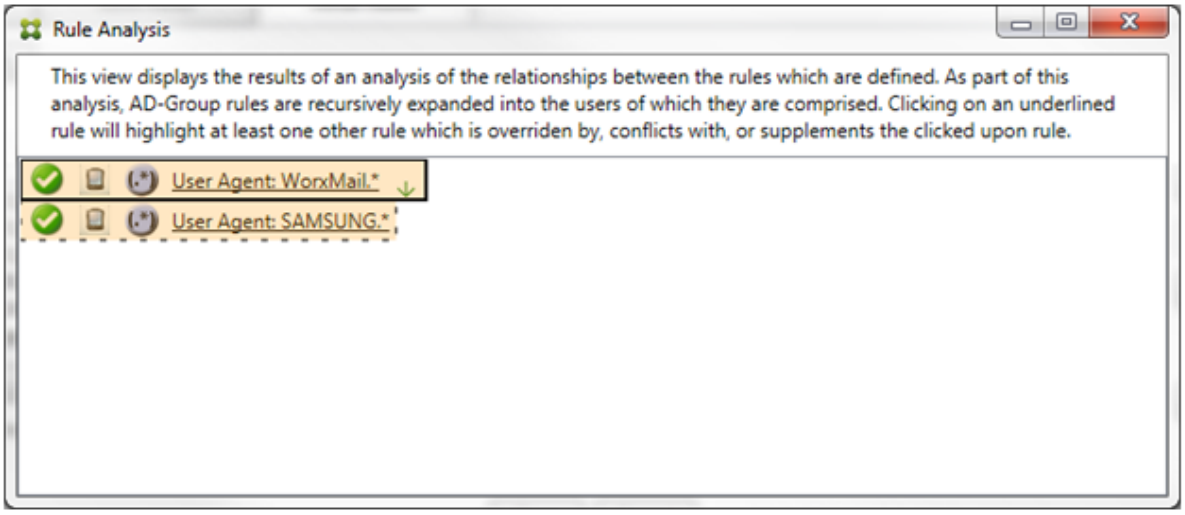
At least two rules will be underlined, the primary rule and the ancillary rule or rules. Rules that only

© 1997–2025 Citrix Systems, Inc. All rights reserved.

supplement one another will only involve regular expression rules. When the rules supplement one another, they are indicated with a yellow overlay. Before clicking either of the rules, in a simple example, the dialog box appears as follows:



Visual inspection easily reveals that both rules are regular expression rules which have both been applied to the ActiveSync device ID field in the Citrix Endpoint Management connector for Exchange ActiveSync. After clicking the first rule, the dialog box looks as follows:

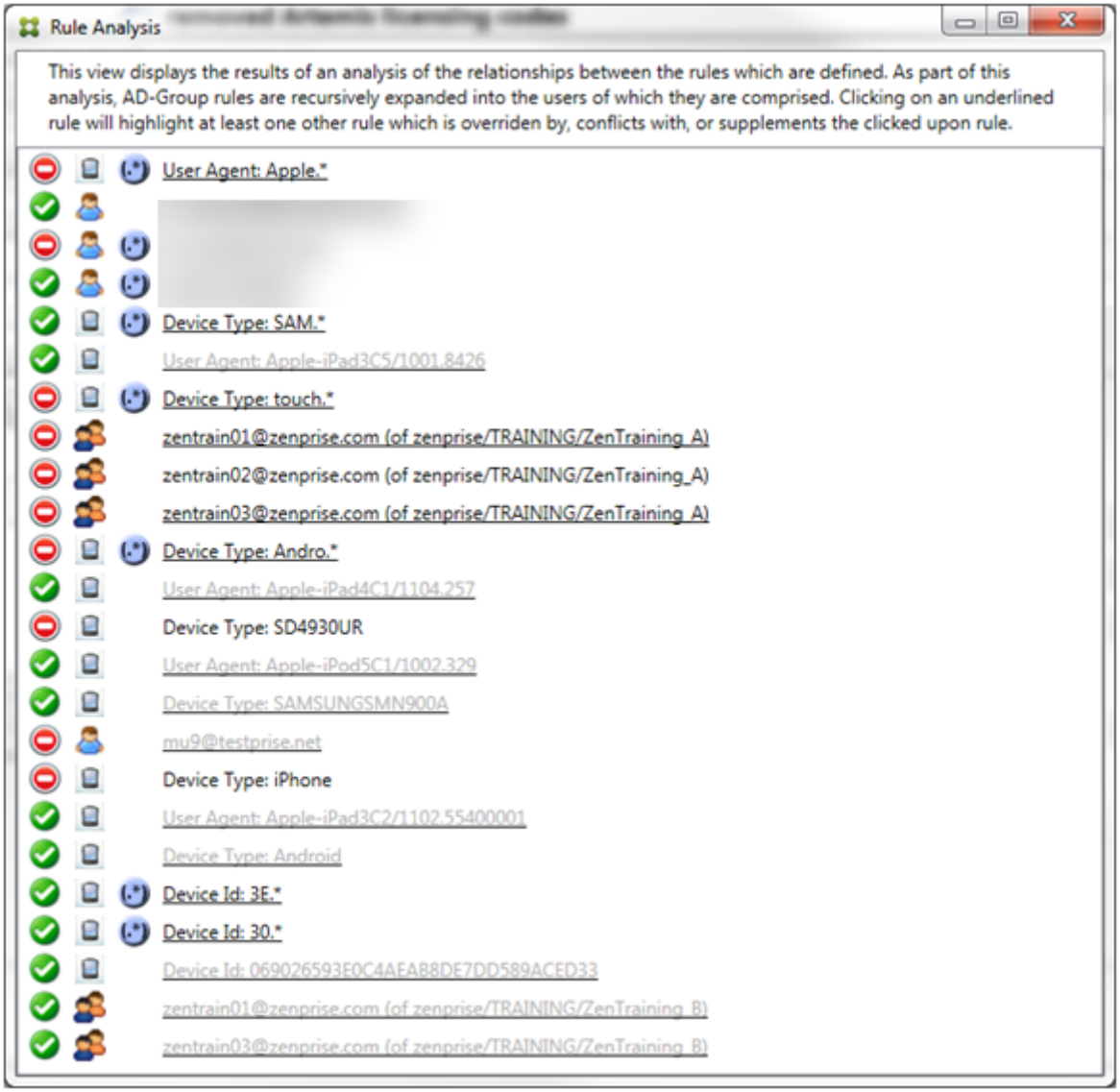


The primary rule (regular expression rule `WorkMail.*`) is highlighted with a yellow overlay to indicate that there exists at least one more ancillary rule which is a regular expression. The ancillary rule (regular expression rule `SAMSUNG.*`) is highlighted with a yellow overlay to indicate that both it and the primary rule are regular expression rules being applied to the same field within the connector for Exchange ActiveSync. In this case, that field is the ActiveSync device ID. The regular expressions may or may not overlap. It is up to you to decide if your regular expressions are properly crafted.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Example of a complex expression

Many potential overrides, conflicts, or supplements can occur, making it impossible to give an example of all possible scenarios. The following example discusses what not to do, while also serving to illustrate the full power of the rule analysis visual construct. Most of the items are underlined in the following figure. Many of the items render in a lighter font, which indicates that the rule in question has been overridden by a higher priority rule in some manner. Several regular expression rules are included in the list as well, as indicated by the icon.

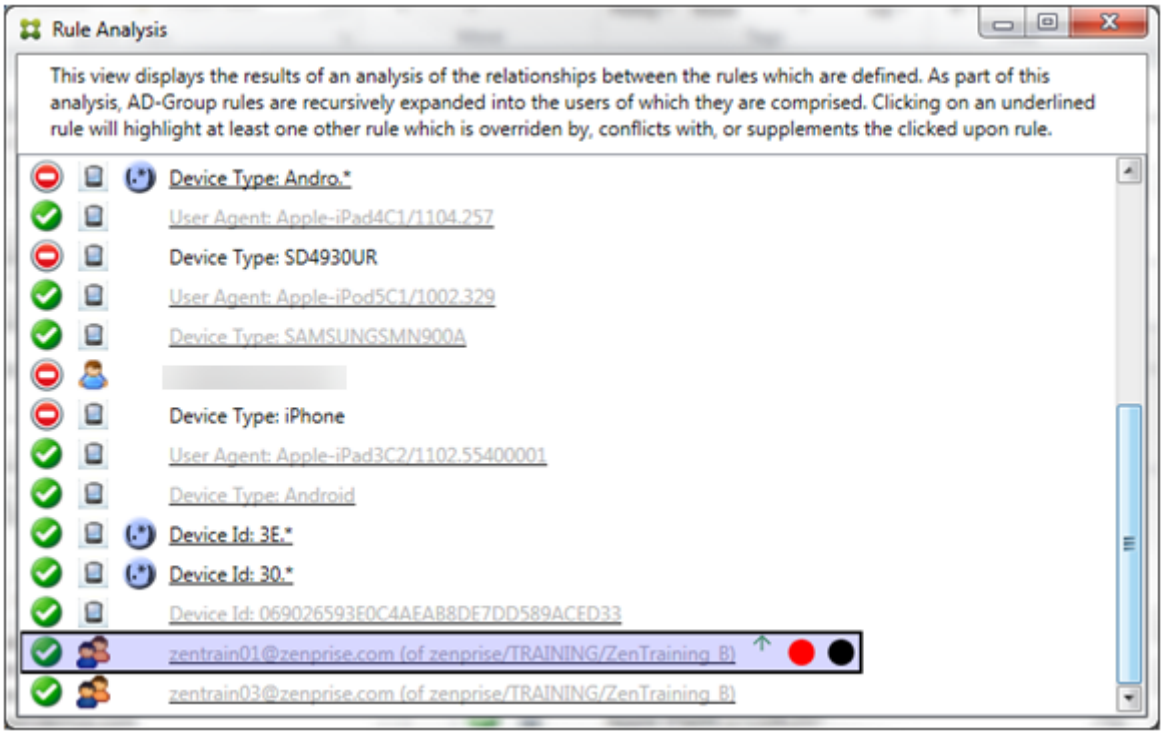


How to analyze an override

To see which rule or rules have overridden a particular rule, you click the rule.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Example 1: This example examines why zentrain01@zenprise.com has been overridden.

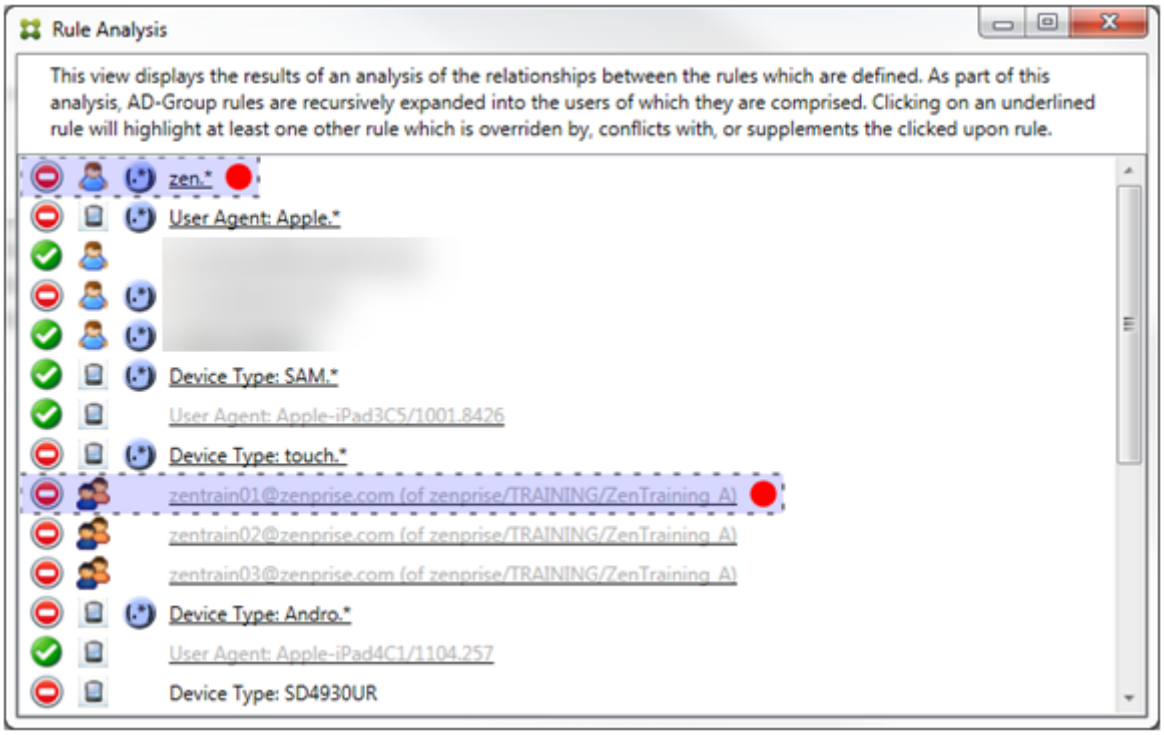


The primary rule (AD-Group rule zenprise/TRAINING/ZenTraining B, of which zentrain01@zenprise.com is a member) has the following characteristics:

- Is highlighted in blue and has a solid border.
- Has an upwards pointing green arrow (to indicate that the ancillary rules are all to be found above it).
- Is followed by both a red circle and black circle to indicate respectively that one or more ancillary rule conflicts with its access and that the primary rule has been overridden and is hence inactive.

When you scroll up, you see the following:

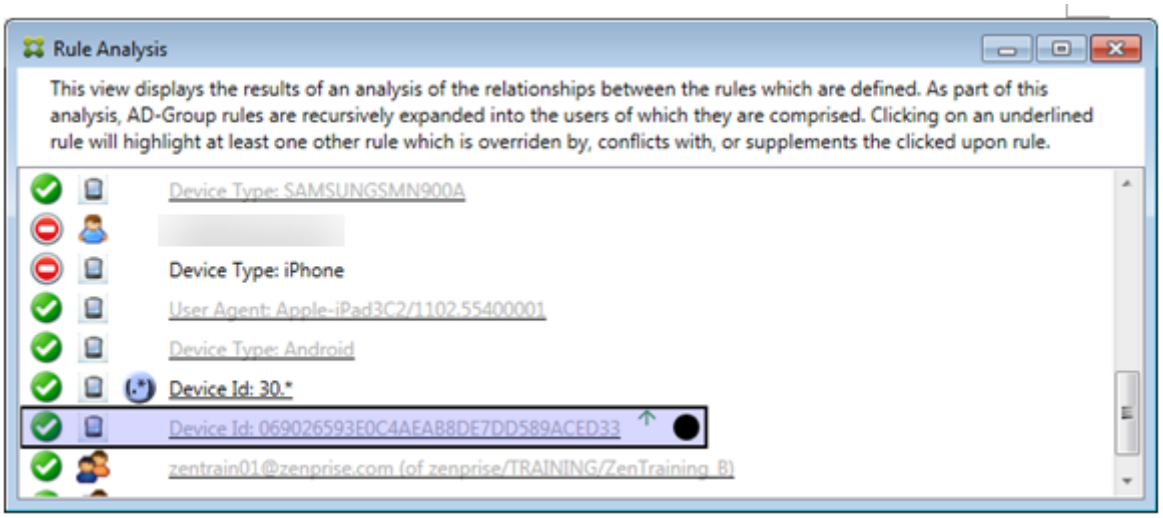
© 1997–2025 Citrix Systems, Inc. All rights reserved.



In this case, there are two ancillary rules that override the primary rule: the regular expression rule `zen.*` and the normal rule `zentrain01@zenprise.com` (of `zenprise`/`TRAINING`/`ZenTraining A`). In the case of the latter ancillary rule, what has occurred is that the Active Directory Group rule `ZenTraining A` has the user `zentrain01@zenprise.com`, and the Active Directory Group rule `ZenTraining B` also has the user `zentrain01@zenprise.com`. Because the ancillary rule has a higher precedence than the primary rule, however, the primary rule has been overridden. The primary rule's access is Allow, and because both of the ancillary rule's access is Block, all are followed with a red circle to further indicate an access conflict.

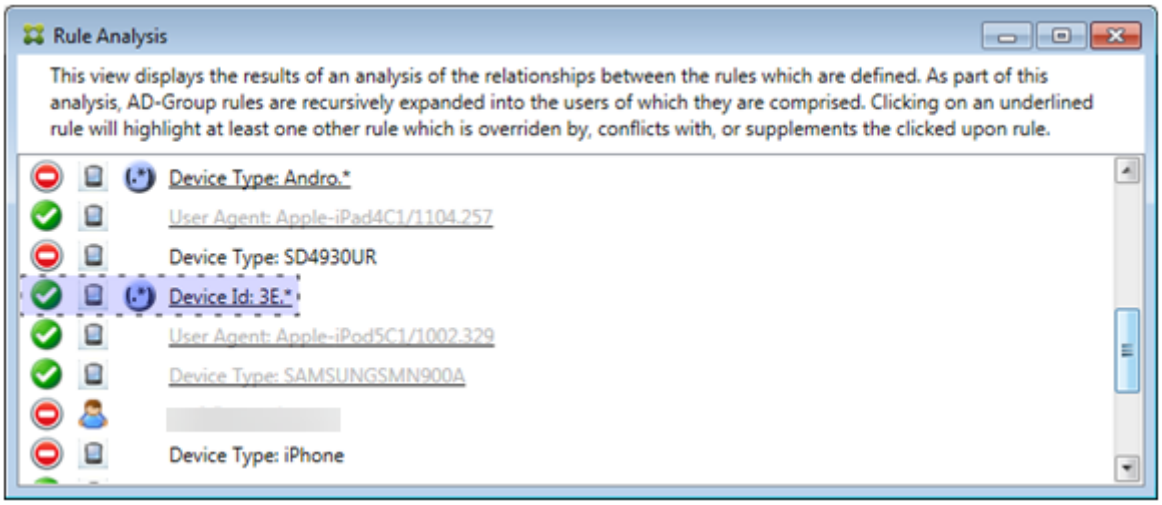
Example 2: This example shows why the device with an ActiveSync device ID of `069026593E0C4AEAB8DE7DD589ACED33` has been overridden:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The primary rule (normal device ID rule `069026593E0C4AEAB8DE7DD589ACED33`) has the following characteristics:

- Is highlighted in blue and has a solid border.
- Has an upwards pointing green arrow (to indicate that the ancillary rule is to be found above it).
- Is followed by a black circle to indicate an ancillary rule has overridden the primary rule and is hence inactive.



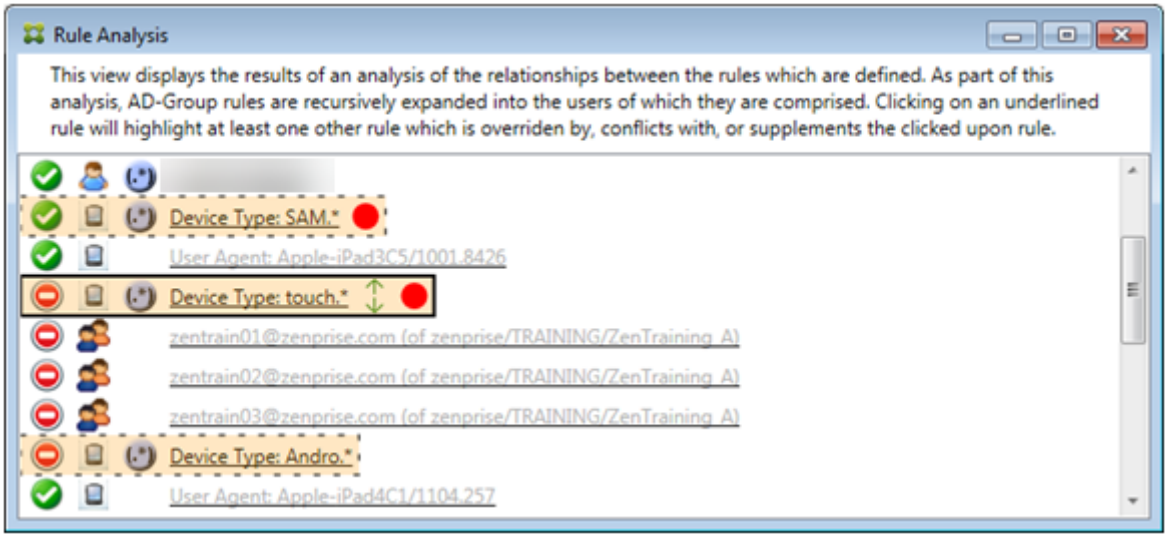
In this case, a single ancillary rule overrides the primary rule: The regular expression ActiveSync device ID rule is `3E.*` Because the regular expression `3E.*` would match `069026593E0C4AEAB8DE7DD589ACED33`, the primary rule will never be evaluated.

How to analyze a supplement and conflict

In this case, the primary rule is the regular expression ActiveSync device type rule `touch.*` The characteristics are as follows:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Is indicated by a solid border with a yellow overlay as a warning that there is more than a single regular expression rule operating against a particular rule field, in this case ActiveSync device type.
- Two arrows are pointing up and down respectively, indicating that there is at least one ancillary rule with higher priority and at least one ancillary rule with lower priority.
- The red circle next to it indicates that at least one ancillary rule has its access set to **Allow** which conflicts with the primary rule's access of **Block**
- There are two ancillary rules: the regular expression ActiveSync device type rule `SAM.*` and the regular expression ActiveSync device type rule `Andro.*`.
- Both of the ancillary rules are bordered with dashes to indicate that they're ancillary.
- Both of the ancillary rules are overlaid with yellow to indicate that they're also applied to the rule field of the ActiveSync device type.
- You must make sure in such scenarios that their regular expression rules aren't redundant.



How to further analyze the rules

This example explores how rule relationships are always from the perspective of the primary rule. The preceding example showed how a click the regular expression rule applied to the rule field of device type with a value of `touch.*`. Clicking the ancillary rule `Andro.*` shows a different set of ancillary rules highlighted.

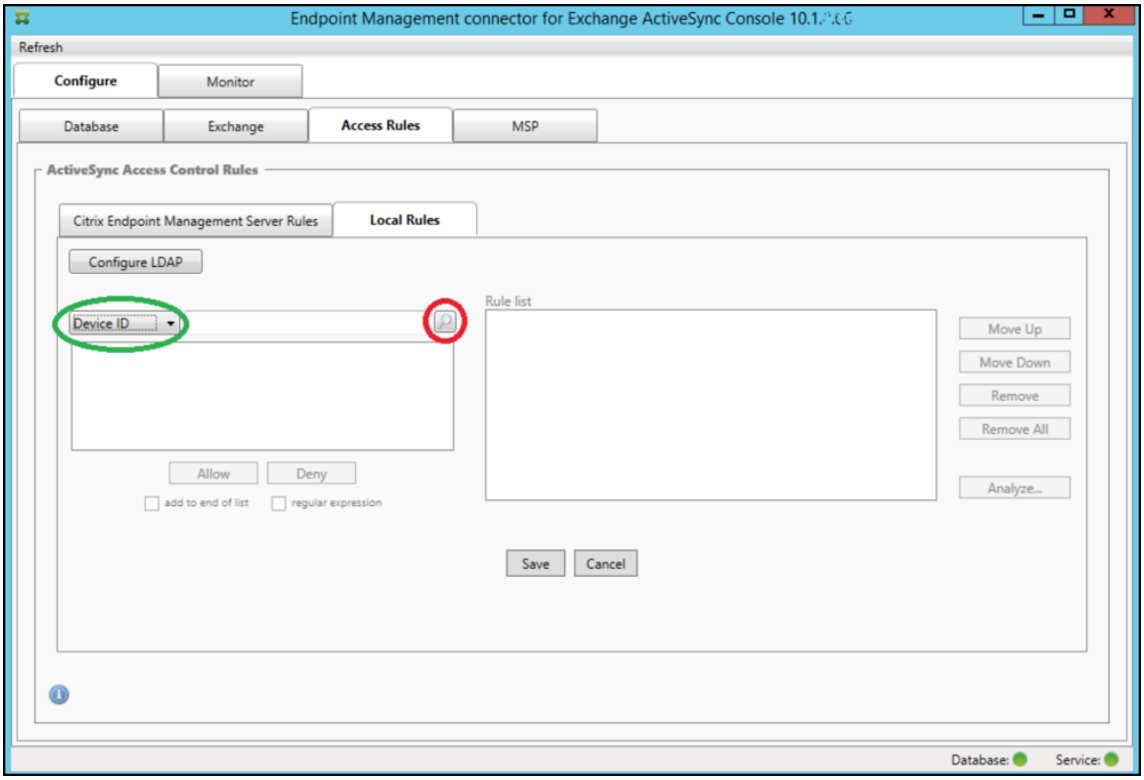
© 1997–2025 Citrix Systems, Inc. All rights reserved.

The example shows an overridden rule that is included in the rule relationship. This rule is the normal ActiveSync device type rule `Android`, which is overridden (indicated by the lightened font and the black circle next to it) and also conflicts in its access with the primary rule regular expression ActiveSync device type rule `Andro.*`. That rule was formerly an ancillary rule before being clicked. In the preceding example, the normal ActiveSync device type rule `Android`, wasn't displayed as an ancillary rule because, from the perspective of the then primary rule (the regular expression ActiveSync device type rule `touch.*`), it wasn't related to it.

To configure a normal expression local rule

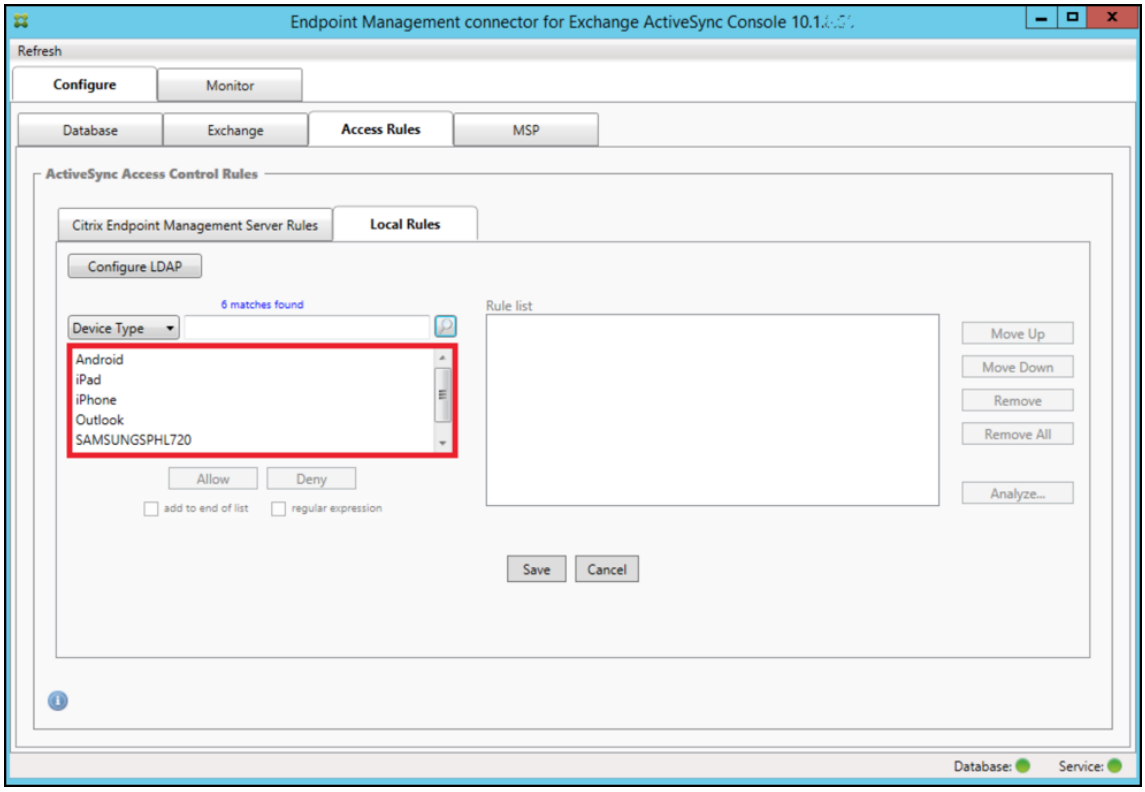
1. Click the **Access Rule**s tab.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. In the **Device ID** list, select the field for which you want to create a Local Rule.
3. Click the magnifying glass icon to display all of the unique matches for the chosen field. In this example, the field **Device Type** has been chosen and the choices are shown in the following list box:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

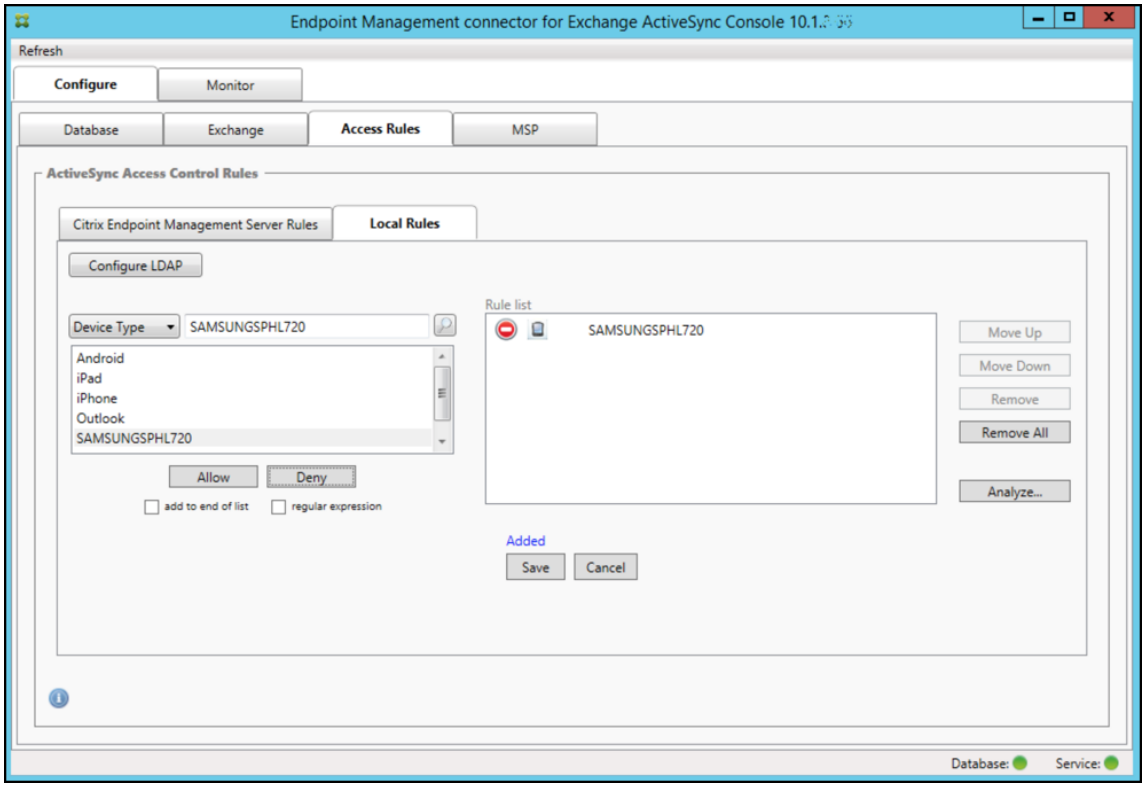


4. Click one of the items in the results list box and then click one of the following options:

   - **Allow** means that Exchange will be configured to allow ActiveSync traffic for all matching devices.
   - **Deny** means that Exchange will be configured to deny ActiveSync traffic for all matching devices.

   In this example, all devices that have a device type of SamsungSPhl720 are denied access.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



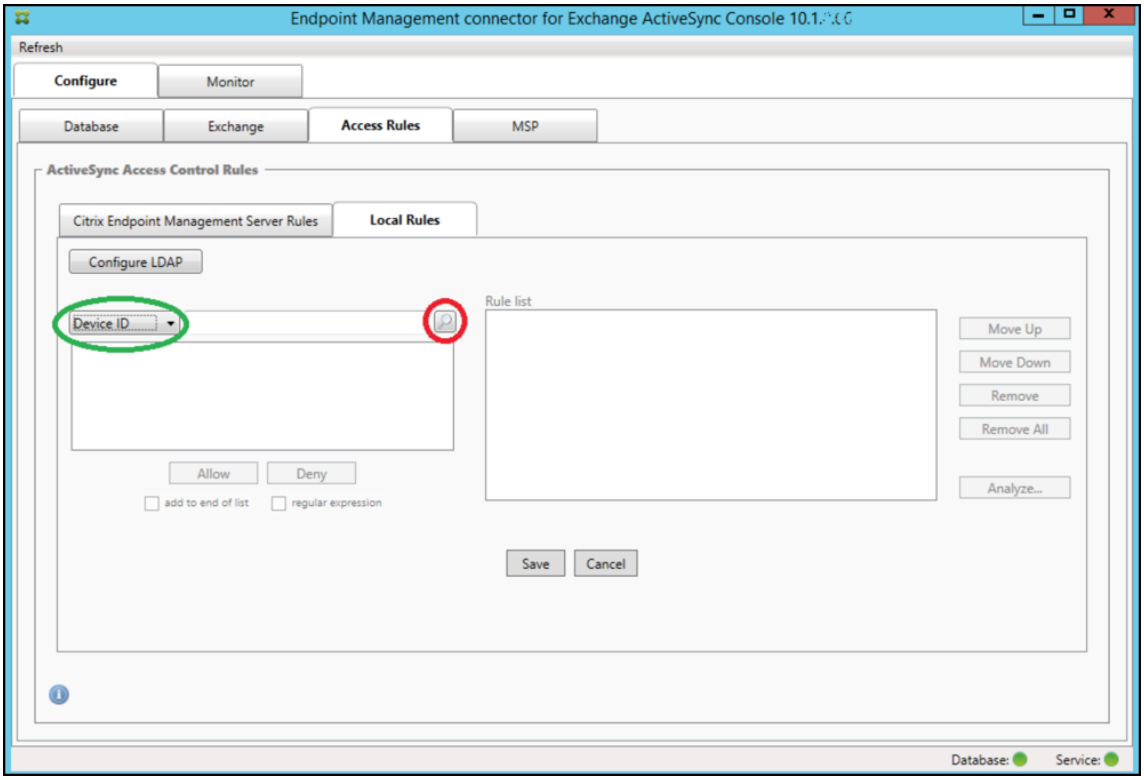
To add a regular expression

Regular expression local rules can be distinguished by the icon which appears next to them - . To add a regular expression rule, you can either build a regular expression rule from an existing value from the results list for a given field (as long as a major snapshot has completed), or you can simply type in the regular expression that you want.

To build a regular expression from an existing field value

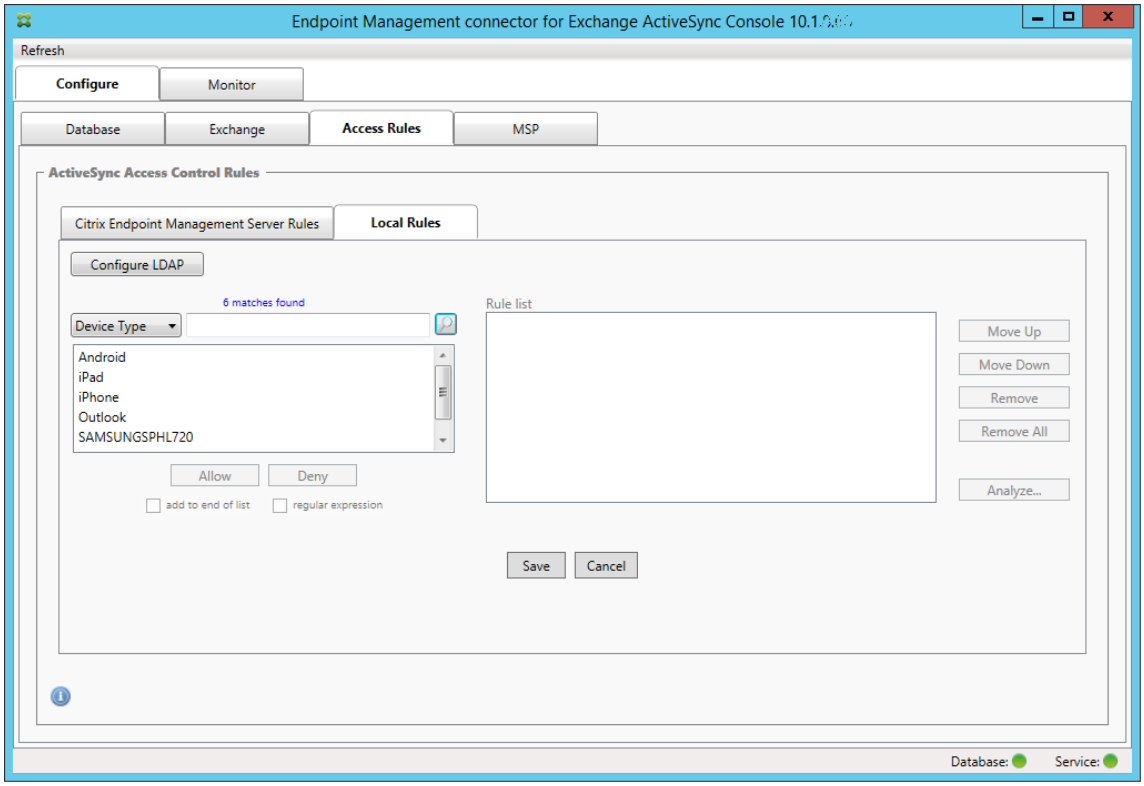
1. Click the **Access Rules** tab.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

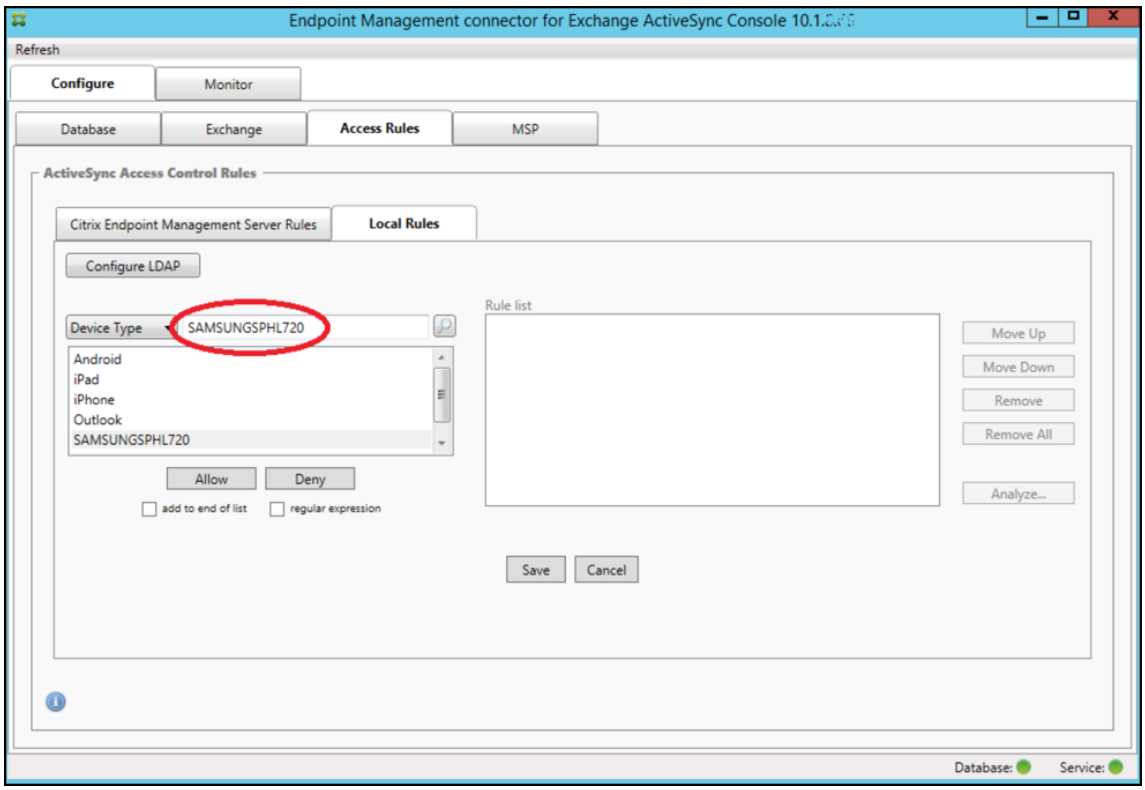


2. In the **Device ID** list, select the field for which you want to create a regular expression Local Rule.
3. Click the magnifying glass icon to display all of the unique matches for the chosen field. In this example, the field **Device Type** has been chosen and the choices are shown in the following list box:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Click one of the items in the results list. In this example, **SAMSUNGSPHL720** has been selected and appears in the text box next to **Device Type**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

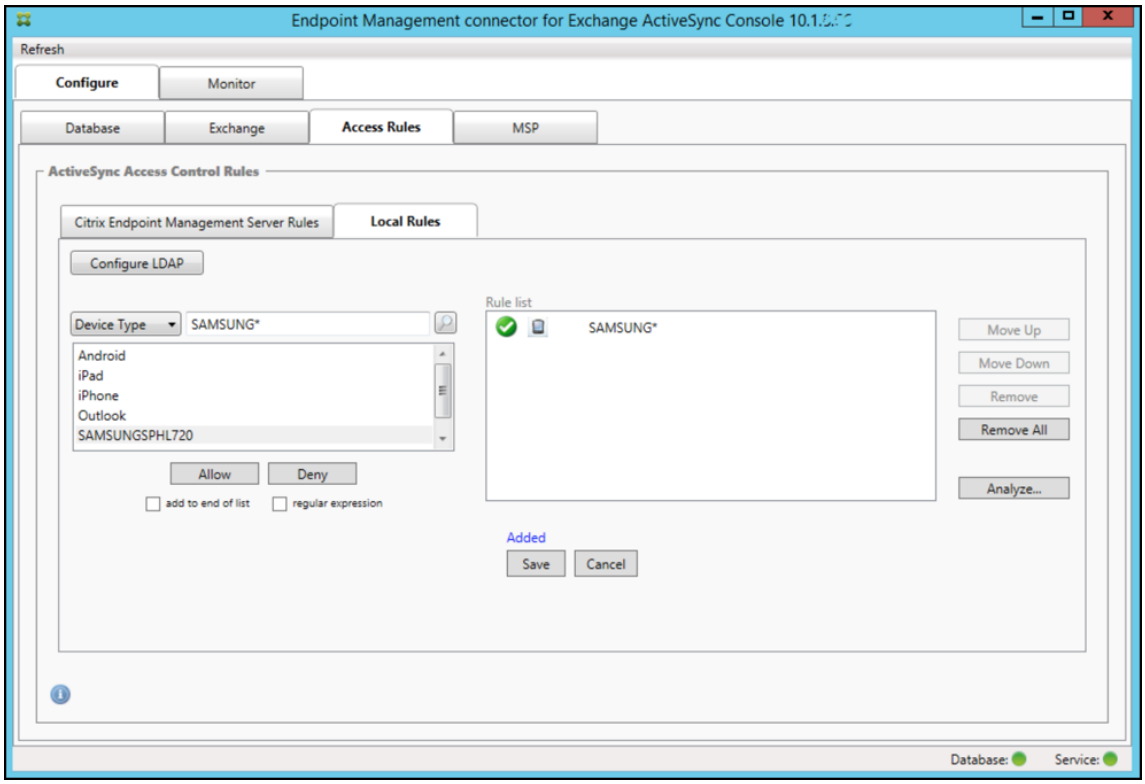
5. To allow all device types that have “Samsung”in their device type value, add a regular expression rule by following these steps:

   a) Click within the selected item text box.

   b) Change the text from **SAMSUNGSPHL720** to **SAMSUNG.***.

   c) Ensure that the regular expression checkbox is selected.

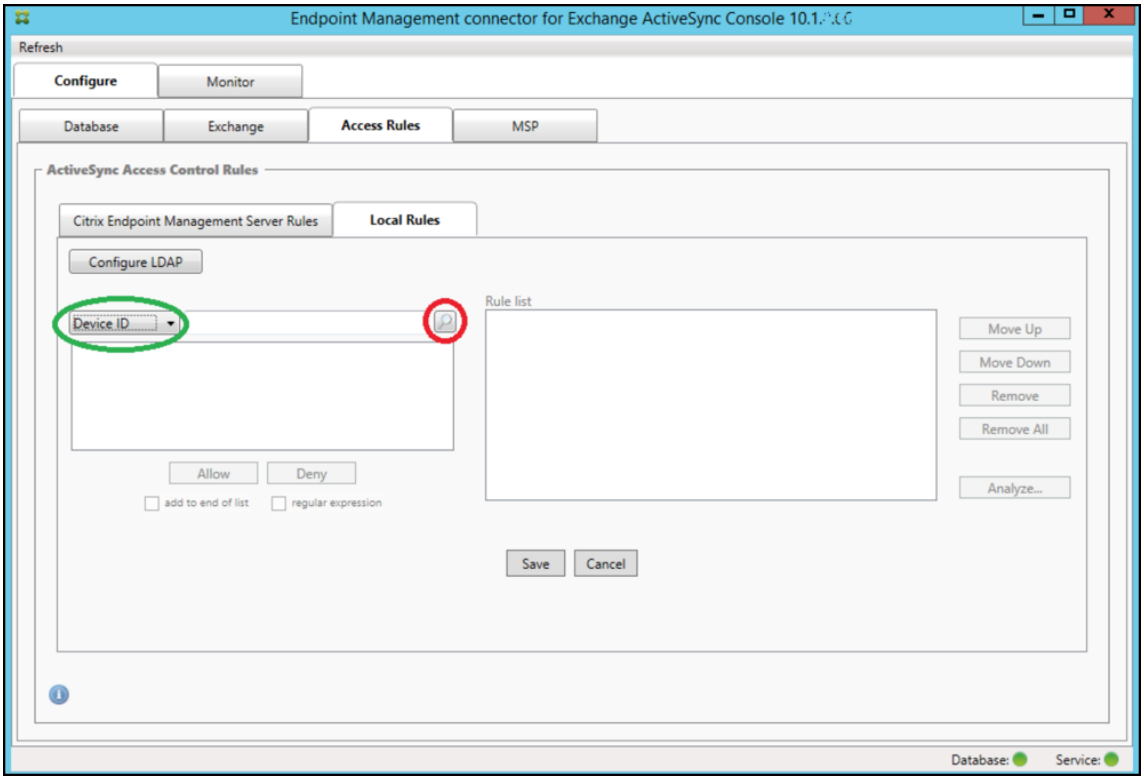
   d) Click **Allow**.



To build an access rule

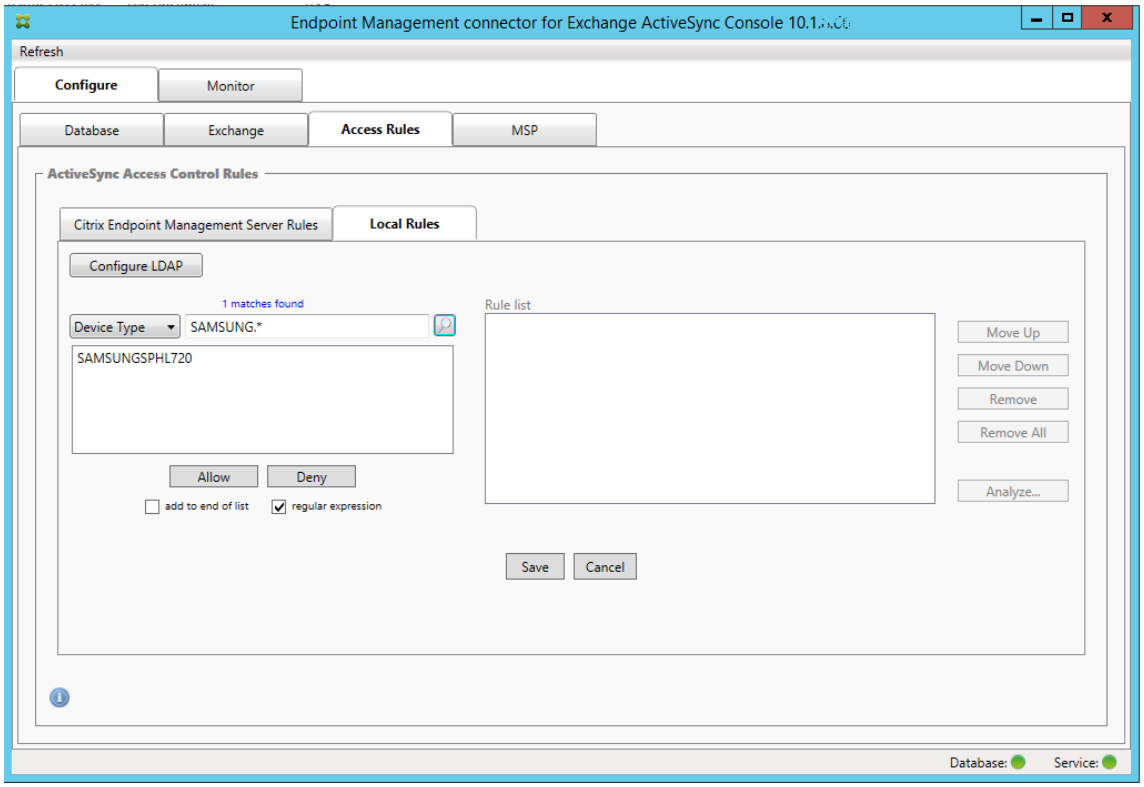
1. Click the **Local Rules** tab.
2. To enter the regular expression, you must make use of both the Device ID list and the selected item text box.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Select the field that you want to match against. This example uses **Device Type**.
4. Type in the regular expression. This example uses `samsung.*`
5. Ensure that the regular expression checkbox is selected and then click **Allow** or **Deny**. In this example, the choice is set as **Allow**. The final result is as follows:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

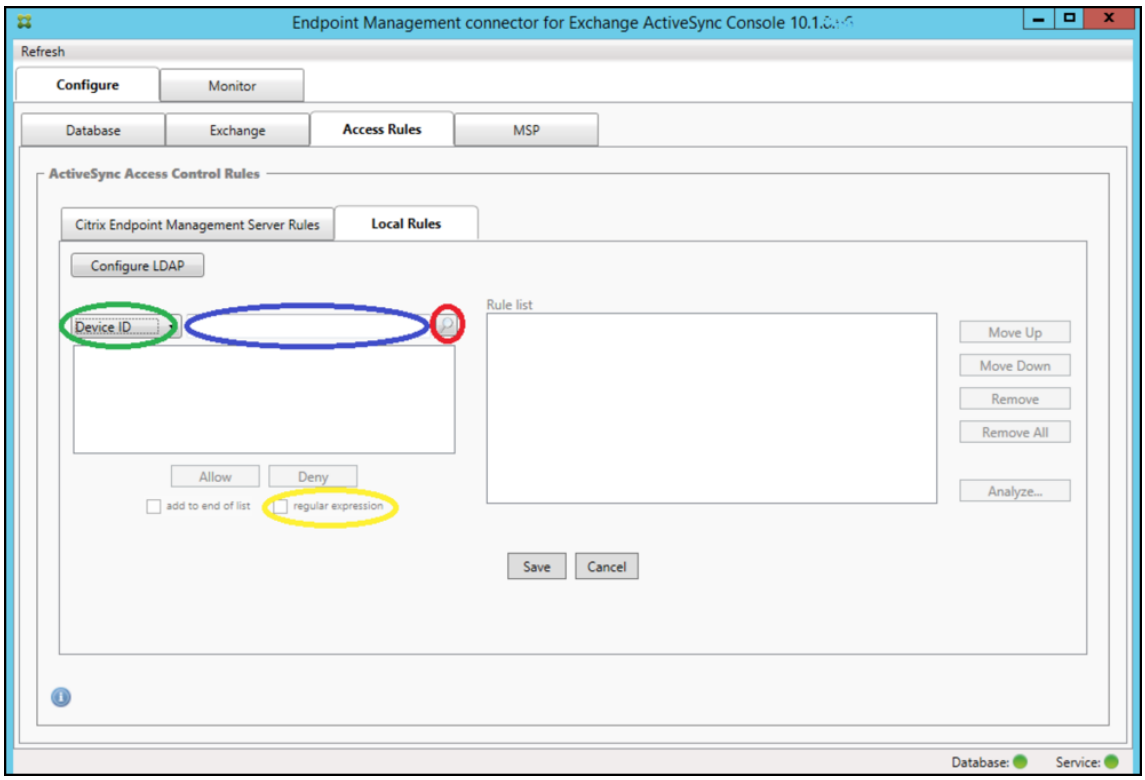


To find devices

By selecting the regular expression checkbox, you can run searches for specific devices that match the given expression. This feature is only available if a major snapshot has successfully completed. You can use this feature even if there is no plan to use regular expression rules. For example, assume that you want to find all devices that have the text `workmail` in their ActiveSync device ID. To do so, follow this procedure.

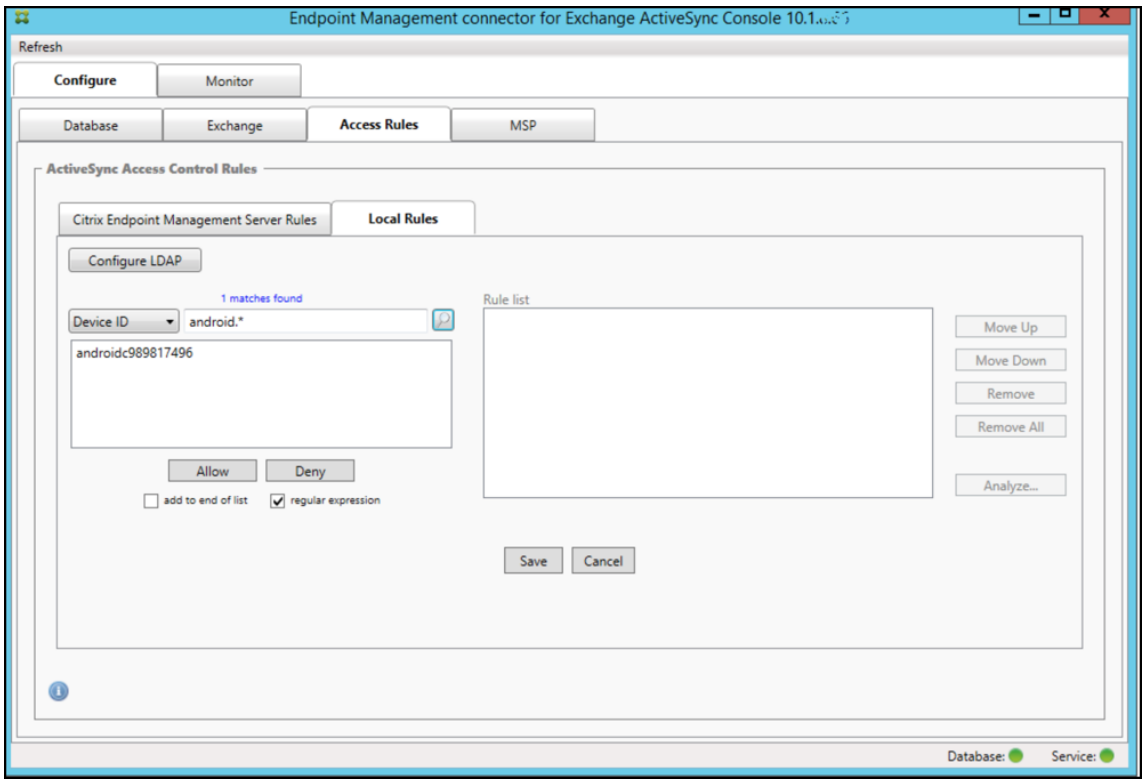
1. Click the **Access Rules** tab.
2. Make sure that the device match field selector is set to Device ID (the default).

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Click within the selected item text box (as shown in blue in the preceding figure) and then type `workmail.*`.
4. Ensure the regular expression checkbox is selected and then click the magnifying glass icon to display the matches as shown in the following figure.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



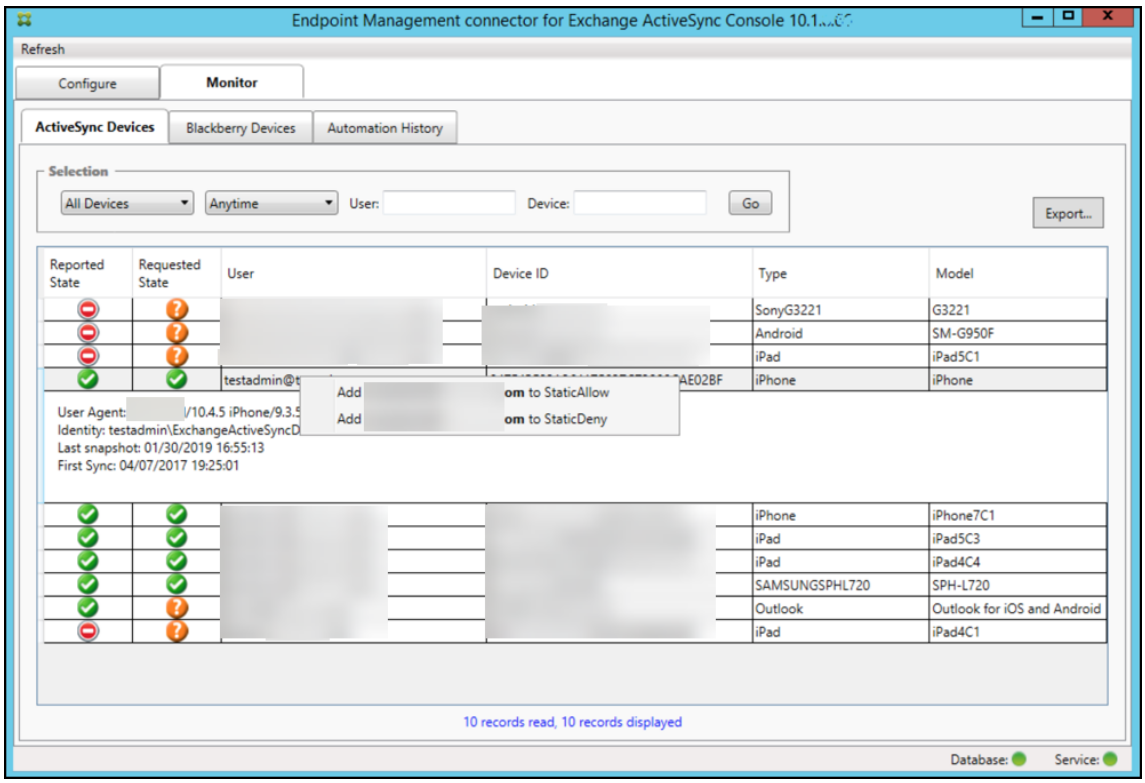
To add an individual user, device, or device type to a static rule

You can add static rules based on user, device ID, or device type on the **ActiveSync Devices** tab.

1. Click the **ActiveSync Devices** tab.
2. In the list, right-click a user, device, or device type and select whether to allow or deny your selection.

   The following image shows the Allow/Deny option when user1 is selected.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Device monitoring

The **Monitor** tab in the Citrix Endpoint Management connector for Exchange ActiveSync lets you browse the Exchange ActiveSync and BlackBerry devices that have been detected and the history of automated PowerShell commands that have been issued. The **Monitor** tab has the following three tabs:

- **ActiveSync Devices:**
  - You can export the displayed ActiveSync device partnerships by clicking the **Export** button.
  - You can add Local (static) rules by right-clicking the **User**, **Device ID**, or **Type** columns and selecting the appropriate allow or block rule type.
  - To collapse an expanded row, Ctrl-click the expanded row.
- **Blackberry Devices**
- **Automation History**

The **Configure** tab shows the history of all snapshots. Snapshot history shows when the snapshot took place, how long it took, how many devices were detected and any errors that occurred:

- On the **Exchange** tab, click the Info icon for the desired Exchange Server.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Troubleshooting and diagnostics

Citrix Endpoint Management connector for Exchange ActiveSync logs errors and other operational information to its log file: *Install Folder*\log\XmmWindowsService.log. The connector for Exchange ActiveSync also logs significant events to the Windows Event Log.

To change the logging level

Citrix Endpoint Management connector for Exchange ActiveSync includes the following logging levels: Error, Info, Warn, Debug, and Trace.

> **Note:**
>
> Each successive level generates more detail (more data). For example, the Error level provides the least detail, but the Trace level provides the most detail.

To change the logging level, do the following:

1. In `C:\Program Files\Citrix\Citrix` Citrix Endpoint Management connector, open the nlog.config file.
2. In the `<rules>` section, change the *minilevel* parameter to the logging level you prefer. For example:

```
1      <rules >
2
3      <logger name="*" writeTo="file" minlevel="Debug" />
4
5      </rules>
```

3. Save the file.

   The changes take effect immediately. You don't need to restart the connector for Exchange ActiveSync.

Common errors

The following list includes common errors:

- The connector for the Exchange ActiveSync service doesn't start

  Check the log file and the Windows Event Log for errors. Typical causes are as follows:

  - The connector for the Exchange ActiveSync service cannot access the SQL Server. This may be caused by these issues:
    - The SQL Server service isn't running.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

* Authentication failure.

If Windows Integrated authentication is configured, the user account of the connector for the Exchange ActiveSync service must be an allowed SQL logon. The account of the connector for the Exchange ActiveSync service defaults to Local System, but may be changed to any account that has local administrator privileges. If SQL authentication is configured, the SQL logon must be properly configured in SQL.

Troubleshooting tools

A set of PowerShell utilities for troubleshooting is available in the **Support\PowerShell** folder.

A troubleshooting tool does in-depth analysis of user mailboxes and devices, detecting error conditions and potential areas of failure, and in-depth RBAC analysis of users. It can save a raw output of all cmdlets to a text file.

NetScaler Gateway connector for Exchange ActiveSync

September 6, 2025

XenMobile NetScaler Connector is now the NetScaler Gateway connector for Exchange ActiveSync. For more details about the Citrix unified portfolio, see the Citrix product guide.

The connector for Exchange ActiveSync provides a device-level authorization service of ActiveSync clients to NetScaler Gateway acting as a reverse proxy for the Exchange ActiveSync protocol. You control authorization through a combination of:

- Policies that you define in Citrix Endpoint Management
- Rules defined locally by the NetScaler Gateway connector for Exchange ActiveSync

For more information, see ActiveSync Gateway.

For a detailed reference architecture diagram, see Architecture.

The current version of the NetScaler Gateway connector for Exchange ActiveSync is version 8.5.3.

To download the connector:

1. Go to https://www.citrix.com/downloads.
2. Navigate to **Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10 > Server Components**.
3. On the **NetScaler Gateway Connector** tile, click **Download File**.

To install the connector, see Installing the NetScaler Gateway connector for Exchange ActiveSync).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> Starting in October 2022, the Citrix Endpoint Management and NetScaler Gateway connectors for Exchange ActiveSync will no longer support Exchange Online given the authentication changes announced by Microsoft here. The Citrix Endpoint Management connector for Exchange continues to work with Microsoft Exchange Server (on-premises).

What's new in version 8.5.3

- This release adds support for ActiveSync protocols 16.0 and 16.1.
- More detail has been added to the analytics sent to Google Analytics, especially concerning snapshots. [CXM-52261]

What's new in earlier versions

> **Note:**
>
> The following What's new section refers to the NetScaler Gateway connector for Exchange ActiveSync by its former name, XenMobile NetScaler Connector. The name changed from version 8.5.2.

What's new in version 8.5.2

- XenMobile NetScaler Connector is now the NetScaler Gateway connector for Exchange ActiveSync.

The following issues are fixed in this version:

- If more than one criterion is used in defining a policy rule and if a criterion involves the user ID, the following issue can occur: If a user has more aliases, the aliases aren't also checked when applying the rule. [CXM-55355]

What's new in version 8.5.1.11

- **System requirement change:** The current version of NetScaler Connector requires Microsoft .NET Framework 4.5.
- **Google Analytics support:** We want to know how you use the Connector so we can focus on where we can make the product better.
- **Support for TLS 1.1 and 1.2:** Due to its weakening security, the PCI Council is deprecating TLS 1.0 and TLS 1.1. Support for TLS 1.2 is added to the XenMobile NetScaler Connector.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Monitoring NetScaler Gateway connector for Exchange ActiveSync

The NetScaler Gateway connector for the Exchange ActiveSync configuration utility provides detailed logging. Use the logs to view all traffic passing through your Exchange Server that the Secure Mobile Gateway either allows or blocks.

Use the **Log** tab to view the history of the ActiveSync requests forwarded to the connector for Exchange ActiveSync for authorization.

Also, to make sure that the connector for the Exchange ActiveSync web service is running, load the following URL into a browser on the connector server `https://<host:port>/services/ActiveSync/Version`. If the URL returns the product version as a string, the web service is responsive.

To simulate ActiveSync traffic with the connector for Exchange ActiveSync

You can use the NetScaler Gateway connector for Exchange ActiveSync to simulate ActiveSync traffic with your policies. In the connector configuration utility, click the **Simulator** tab. The results show how your policies apply according to the rules you configured.

Choosing filters for the connector for Exchange ActiveSync

The NetScaler Gateway connector for Exchange ActiveSync filters work by analyzing a device for a given policy violation or property setting. If the device meets the criteria, the device is placed in a Device List. This Device List is neither an allow list or a block list. It is a list of devices that meet the criteria defined. The following filters are available for the connector for Exchange ActiveSync within Citrix Endpoint Management. The two options for each filter are **Allow** or **Deny**.

- **Anonymous Devices:** Allows or denies devices that are enrolled in Citrix Endpoint Management but the user's identity is unknown. For example, an enrolled user has an unknown identity if the user has an expired Active Directory password or unknown credentials.
- **Forbidden Apps:** Allows or denies devices based on the Device List defined by block lists in policies and the presence of apps on a block list.
- **Implicit Allow/Deny:** Creates a Device List of all devices that do not meet any of the other filter rule criteria and allows or denies based on that list. The Implicit Allow/Deny option makes sure that the connector for Exchange ActiveSync status in the Devices tab is enabled and shows the connector status for your devices. The Implicit Allow/Deny option also controls all other connector filters that aren't selected. For example, the connector denies apps on the block list. However, the connector allows all other filters because the Implicit Allow/Deny option is set to **Allow**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Inactive devices:** Creates a Device List of devices that haven't communicated with Citrix Endpoint Management within a specified time. These devices are considered inactive. The filter allows or denies the devices accordingly.
- **Missing required apps:** When a user enrolls, the user receives a list of required apps that must be installed. The missing required apps filter indicates that one or more of the apps is no longer present; for example, the user deleted one or more apps.
- **Non-Suggested Apps:** When a user enrolls, the user receives a list of the apps to install. The non-suggested apps filter checks the device for apps that aren't in that list.
- **Noncompliant password:** Creates a Device List of all devices that do not have a passcode on the device.
- **Out of Compliance Devices:** Allows you to deny or allow devices that meet your own internal IT compliance criteria. Compliance is an arbitrary setting defined by the device property named Out of Compliance, which is a Boolean flag that can be either **True** or **False**. (You can create this property manually and set the value. Or you can use automated actions to create this property on a device, based on whether the device meets specific criteria.)
  - **Out of Compliance = True:** If a device does not meet the compliance standards and policy definitions set by your IT department, the device is out of compliance.
  - **Out of Compliance = False:** If a device does meet the compliance standards and policy definitions set by your IT department, the device is compliant.
- **Revoked Status:** Creates a Device List of all revoked devices and allows or denies based on revoked status.
- **Rooted Android/Jailbroken iOS Devices:** Creates a Device List of all devices flagged as rooted and allows or denies based on rooted status.
- **Unmanaged Devices:** Creates a Device List of all devices in the Citrix Endpoint Management database. Deploy the Mobile Application Gateway in a Block Mode.

To configure a connection to NetScaler Gateway connector for Exchange ActiveSync

The NetScaler Gateway connector for Exchange ActiveSync communicates with Citrix Endpoint Management and other remote configuration providers through Citrix Secure Web services.

1. In the connector for the Exchange ActiveSync configuration utility, click the **Config Providers** tab and then click **Add**.
2. In the **Config Providers** dialog box, in **Name**, enter a user name that has administrative privileges and are used for basic HTTP authorization with the Citrix Endpoint Management server.
3. In **Url**, enter the web address of the Citrix Endpoint Management GCS, typically in the format `https://<FQDN>/<instanceName>/services/<MagConfigService>`. The *MagConfigService* name is case-sensitive.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. In **Password**, enter the password to use for basic HTTP authorization with the Citrix Endpoint Management server.
5. In **Managing Host**, enter the connector for the Exchange ActiveSync server name.
6. In **Baseline Interval**, specify a time period for when to pull a new refreshed dynamic ruleset from Citrix Endpoint Management.
7. In **Delta interval**, specify a time period for when to pull an update of the dynamic rules.
8. In **Request Timeout**, specify the server request timeout interval.
9. In **Config Provider**, select if the configuration provider server instance is providing the policy configuration.
10. In **Events Enabled**, enable this option if you want the connector for Exchange ActiveSync to notify Citrix Endpoint Management when a device is blocked. This option is required if you're using the connector rules in any of your Citrix Endpoint Management Automated Actions.
11. Click **Save** and then click **Test Connectivity** to test gateway-to-configuration provider connectivity. If the connection fails, check that the local firewall settings allow the connection or contact your administrator.
12. When the connection succeeds, clear the **Disabled** checkbox and then click **Save**.

When you add a configuration provider, the connector for Exchange ActiveSync automatically creates one or more policies associated with the provider. A template definition contained in `config\policyTemplates.xml` in the `NewPolicyTemplate` section defines the policies. For each Policy element defined within this section, a new policy is created.

The operator can add, remove, or modify policy elements if the following is true: The policy element conforms to the schema definition and the standard substitution strings (enclosed in braces) aren't modified. Next, add new groups for the provider and update the policy to include the new groups.

To import a policy from Citrix Endpoint Management

1. In the connector for the Exchange ActiveSync configuration utility, click the **Config Providers** tab and then click **Add**.
2. In the **Config Providers** dialog box, in **Name**, enter a user name for basic HTTP authorization with Citrix Endpoint Management. The user must have administrative privileges.
3. In **Url**, enter the web address of the Citrix Endpoint Management Gateway Configuration Service (GCS), typically in the format `https://<xdmHost>/xdm/services/<MagConfigService>`. The MagConfigService name is case-sensitive.
4. In **Password**, enter the password that is used for basic HTTP authorization with the Citrix Endpoint Management server.
5. Click **Test Connectivity** to test gateway-to-configuration provider connectivity. If the connection fails, check that your local firewall settings allow the connection or check with your admin-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

istrator.

6. When a connection is successfully made, clear the **Disabled** checkbox and then click **Save**.
7. In **Managing Host**, leave the default DNS name of the local host computer. This setting used to coordinate communication with Citrix Endpoint Management when multiple Forefront Threat Management Gateway (TMG) servers are configured in an array.

   After you save the settings, open the GCS.

Configuring NetScaler Gateway connector for Exchange ActiveSync policy mode

The NetScaler Gateway connector for Exchange ActiveSync can run in the following six modes:

- **Allow All:** This policy mode grants access for all traffic passing through the connector for Exchange ActiveSync. No other filtering rules are used.
- **Deny All:** This policy mode blocks access for all traffic passing through the connector for Exchange ActiveSync. No other filtering rules are used.
- **Static Rules: Block Mode:** This policy mode runs static rules with an implicit deny or block statement at the end. The connector for Exchange ActiveSync blocks devices that aren't allowed or permitted via other filter rules.
- **Static Rules: Permit Mode:** This policy mode runs static rules with an implicit permit or allow statement at the end. Devices that aren't blocked or denied via other filter rules are allowed through the connector for Exchange ActiveSync.
- **Static + ZDM Rule**s: Block Mode. This policy mode runs static rules first, followed by dynamic rules from Citrix Endpoint Management with an implicit deny or block statement at the end. Devices are permitted or denied based on defined filters and Citrix Endpoint Management rules. Any devices that do not match on defined filters and rules are blocked.
- **Static + ZDM Rule**s: Permit Mode. This policy mode runs static rules first, followed by dynamic rules from Citrix Endpoint Management with an implicit permit or allow statement at the end. Devices are permitted or denied based on defined filters and Citrix Endpoint Management rules. Any devices that do not match on defined filters and rules are allowed.

The connector for the Exchange ActiveSync process permits or blocks for dynamic rules based on unique ActiveSync IDs for iOS and Windows-based mobile devices received from Citrix Endpoint Management. Android devices differ in their behavior based on the manufacturer and some do not readily expose a unique ActiveSync ID. To compensate, Citrix Endpoint Management sends user ID information for Android devices to make a permit or block decision. As a result, if a user has only one Android device, permits and blocks function normally. If the user has multiple Android devices, all the devices are allowed because Android devices can't be differentiated. You can configure the gateway to statically block these devices by ActiveSyncID, if they're known. You can also configure the gateway to block based on device type or user agent.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To specify the policy mode, in the SMG Controller Configuration utility, do the following:

1. Click the **Path Filters** tab and then click **Add**.
2. In the **Path Properties** dialog box, select a policy mode from the **Policy** list and then click **Save**.

You can review the rules on the **Policies** tab of the configuration utility. The rules are processed on the connector for Exchange ActiveSync from top to bottom. The Allow policies are displayed with a green check mark. The Deny policies are shown as a red circle with a line through it. To refresh the screen and see the most updated rules, click **Refresh**. You can also modify the ordering of rules in the config.xml file.

To test the rules, click the **Simulator** tab. Specify values in the fields. You can get the values from the logs. A result message specifies Allow or Block.

To configure static rules

Enter static rules with values that the ISAPI filtering of the ActiveSync connection HTTP requests reads. Static rules enable the connector for Exchange ActiveSync to permit or block traffic by the following criteria:

- **User:** The connector for Exchange ActiveSync uses the authorized user value and name structure that was captured during device enrollment. That structure is commonly found as `domain\username` as referenced by the server running Citrix Endpoint Management connected to the Active Directory via LDAP. The **Log** tab in the connector configuration utility shows the values that pass through the connector. The values get passed if the connector must determine the value structure or if the structure differs.
- **DeviceID (ActiveSyncID):** Also known as the ActiveSyncID of the connected device. This value is commonly found within the specific device properties page in the Citrix Endpoint Management console. This value can also be screened from the **Log** tab in the connector for the Exchange ActiveSync configuration utility.
- **DeviceType:** The connector for Exchange ActiveSync can determine if a device is an iPhone, iPad, or other device type and can permit or block based on that criteria. As with other values, the connector configuration utility can reveal all connected device types being processed for the ActiveSync connection.
- **UserAgent:** Contains information on the ActiveSync client that is used. Usually, the value specified corresponds to a specific operating system build and version for the mobile device platform.

The connector for the Exchange ActiveSync configuration utility running on the server always manages the static rules.

1. In the SMG Controller Configuration utility, click the **Static Rules** tab and then click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. In the **Static Rule Properties** dialog box, specify the values that you want to use as criteria. For example, you can enter a user to allow access by entering the user name (for example, AllowedUser) and then clearing the **Disabled** checkbox.
3. Click **Save**.

   The static rule is now in effect. Also, you can use regular expressions to define values, but you must enable the rule processing mode in the config.xml file.

To configure dynamic rules Device policies and properties in Citrix Endpoint Management define dynamic rules and can trigger a dynamic connector for the Exchange ActiveSync filter. The triggers are based on the presence of a policy violation or property setting. The connector for Exchange ActiveSync filters work by analyzing a device for a given policy violation or property setting. If the device meets the criteria, the device is placed in a Device List. This Device List is not an allow list or a block list. It is a list of devices that meets the criteria defined. The following configuration options enable you to define whether you want to allow or deny the devices in the Device List by using the connector for Exchange ActiveSync.

> **Note:**
>
> Use the Citrix Endpoint Management console to configure dynamic rules.

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Server**, click **ActiveSync Gateway**. The ActiveSync Gateway page appears.
3. In **Activate the following rules**, select one or more rules you want to activate.
4. In Android-only, in **Send Android domain users to ActiveSync Gateway**, click **YES** to make sure that Citrix Endpoint Management sends Android device information to the Secure Mobile Gateway.

   With this option enabled, Citrix Endpoint Management sends Android device information to the connector if Citrix Endpoint Management doesn't have the ActiveSync identifier for the device user.

To configure custom policies by editing the connector for the Exchange ActiveSync XML file You can view the basic policies in the default configuration on the **Policies** tab of the connector for the Exchange ActiveSync configuration utility. If you want to create custom policies, you can edit the NetScaler Gateway connector for the Exchange ActiveSync XML configuration file (config\config.xml).

1. Find the **PolicyList** section in the file and then add a new **Policy** element.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. If a new group is also required, such as another static group or a group to support another GCP, add the new **Group** element to the **GroupList** section.
3. Optionally, you can change the ordering of groups within an existing policy by rearranging the **GroupRef** elements.

Configuring the connector for Exchange ActiveSync XML File The connector for Exchange ActiveSync uses an XML configuration file to dictate the actions of the connector. Among other entries, the file specifies the group files and associated actions the filter take when evaluating HTTP requests. By default, the file is named config.xml and can be found at the following location: ..\Program Files\Citrix\XenMobile NetScaler Connector\config.

GroupRef Nodes

The GroupRef nodes define the logical group names. The defaults are AllowGroup and DenyGroup.

> **Note:**
>
> The order of the GroupRef nodes as they appear in the GroupRefList node is significant.

The ID value of a GroupRef node identifies a logical container or collection of members that are used for matching specific user accounts or devices. The action attributes specify how the filter treats a member that matches a rule in the collection. For example, a user account or device that matches a rule in the AllowGroup set "passes."To pass means to be allowed to access the Exchange CAS. A user account or device that matches a rule in the DenyGroup set is "rejected."Rejected means not to be allowed to access the Exchange CAS.

When a particular user account/device or combination meets rules in both groups, a precedence convention is used to direct the request's outcome. Precedence is embodied in the order of the GroupRef nodes in the config.xml file from top to bottom. The GroupRef nodes are ranked in priority order. Rules for a given condition in the Allow group will always take precedence over rules for the same condition in the Deny group.

Group Nodes

Also, the config.xml defines Group nodes. These nodes link the logical containers AllowGroup and DenyGroup to external XML files. Entries stored in the external files form the basis of the filter rules.

> **Note:**
>
> In this version, only external XML files are supported.

The default installation implements two XML files in the configuration: allow.xml and deny.xml.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configuring NetScaler Gateway connector for Exchange ActiveSync

You can configure the NetScaler Gateway connector for Exchange ActiveSync to selectively block or allow ActiveSync requests based on the following properties: **Active Sync Service ID**, **Device type**, **User Agent** (device operating system), **Authorized user**, and **ActiveSync Command**.

The default configuration supports a combination of static and dynamic groups. You maintain static groups by using the SMG Controller Configuration utility. The static groups can consist of known categories of devices, such as all devices using a given user agent.

An external source called a Gateway Configuration Provider maintains dynamic groups. The connector for Exchange ActiveSync connects the groups on a periodic basis. Citrix Endpoint Management can export groups of allowed and blocked devices and users to the connector for Exchange ActiveSync.

An external source called a Gateway Configuration Provider maintains dynamic groups. The connector for Exchange ActiveSync collects dynamic groups periodically. Citrix Endpoint Management can export groups of allowed and blocked devices and users to the connector.

A policy is an ordered list of groups in which each group has an associated action (allow or block) and a list of group members. A policy can have any number of groups. Group ordering within a policy is important because when a match is found the action of the group is taken, and subsequent groups aren't evaluated.

A member defines a way to match the properties of a request. It can match a single property, such as device ID, or multiple properties, such as device type and user agent.

Choosing a Security Model for NetScaler Gateway connector for Exchange ActiveSync

Establishing a security model is essential to a successful mobile device deployment for organizations of any size. It is common to use protected or quarantined network control to allow access to a user, computer, or device by default. This practice isn't always ideal. Every organization that manages IT security might have a slightly different or tailored approach to security for mobile devices.

The same logic applies to mobile device security. Using a permissive model is a weak choice because of the multitude of mobile devices and types, mobile devices per user, and available operating system platforms and apps. In most organizations, the restrictive model is the most logical choice.

The configuration scenarios that Citrix allows for integrating the connector for Exchange ActiveSync with Citrix Endpoint Management are as follows:

Permissive Model (Permit Mode)

The permissive security model operates on the premise that everything is either allowed or granted access by default. Only through rules and filtering is something blocked and a restriction applied.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The permissive security model is good for organizations that have a relatively loose security concern about mobile devices. The model only applies restrictive controls to deny access where appropriate (when a policy rule is failed).

Restrictive Model (Block Mode)

The restrictive security model is based on the premise that nothing is allowed or granted access by default. Everything passing through the security check point is filtered and inspected, and is denied access unless the rules allowing access are passed. The restrictive security model is good for organizations that have a relatively tight security criterion about mobile devices. The mode only grants access for use and functionality with the network services when all rules to allow access have passed.

Managing NetScaler Gateway connector for Exchange ActiveSync

You can use the NetScaler Gateway connector for Exchange ActiveSync to build access control rules. The rules either allow or block access to ActiveSync connection requests from managed devices. Access is based on device status, app allow or block lists, and other compliance conditions.

By using the connector for the Exchange ActiveSync configuration utility, you can build dynamic and static rules that enforce corporate email policies. Those rules and policies allow you to block users who are in violation of compliance standards. You can also set up email attachment encryption, so that all attachments that pass through your Exchange Server to managed devices are encrypted. Only authorized users with managed devices can view encrypted attachments.

To uninstall the XNC

1. Run XncInstaller.exe with an administrator account.
2. Follow the onscreen instructions to complete the uninstallation.

To install, upgrade, or uninstall the connector for Exchange ActiveSync

1. Run XncInstaller.exe with an administrator account to install the connector for Exchange ActiveSync or allow for upgrade or removal of an existing connector.
2. Follow the onscreen instructions to complete the installation, upgrade, or uninstallation.

After you install the connector for Exchange ActiveSync, you must manually restart the Citrix Endpoint Management configuration service and the notification service.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Installing NetScaler Gateway connector for Exchange ActiveSync

You can install the connector for Exchange ActiveSync on its own server or on the same server where you installed Citrix Endpoint Management.

You can consider installing the connector for Exchange ActiveSync on its own server (separate from Citrix Endpoint Management) for the following reasons:

- If your Citrix Endpoint Management server is hosted remotely in the cloud (physical location)
- If you do not want restarts of the Citrix Endpoint Management server to affect the connector for Exchange ActiveSync (availability)
- If you want to devote a server's system resources entirely to the connector for Exchange ActiveSync (performance)

The CPU load that the connector for Exchange ActiveSync puts on a server depends on how many devices are managed. A general recommendation is to provision for one more CPU core if the connector is deployed on the same server as Citrix Endpoint Management. For large numbers of devices (more than 50,000), you might need to provision more cores if you do not have a clustered environment. The memory footprint of the connector isn't significant enough to warrant more memory.

NetScaler Gateway connector for Exchange ActiveSync system requirements

The NetScaler Gateway connector for Exchange ActiveSync communicates with NetScaler Gateway over an SSL bridge configured on the NetScaler Gateway appliance. The bridge enables the appliance to bridge all secure traffic directly to Citrix Endpoint Management. The connector for Exchange ActiveSync the following minimum system configuration:

Component	Requirement
Computer and processor	733 MHz Pentium III 733 MHz or higher processor. 2.0 GHz Pentium III or higher processor (recommended)
Citrix Gateway	Citrix Gateway appliance with software version 10
Memory	1 GB
Hard disk	NTFS-formatted local partition with 150 MB of available hard-disk space

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Component	Requirement
Operating system	Windows Server 2016, Windows Server 2012 R2, or Windows Server 2008 R2 Service Pack 1. Must be an English-based server. Support for Windows Server 2008 R2 Service Pack 1 ends on January 14, 2020 and support for Windows Server 2012 R2 ends on October 10, 2023.
Other devices	Network adapter compatible with the host operating system for communication with the internal network
Microsoft .NET Framework	Version 8.5.1.11 requires Microsoft .NET Framework 4.5.
Display	VGA or higher-resolution monitor

The host computer for the connector for Exchange ActiveSync requires the following minimum available hard disk space:

- **Application:** 10–15 MB (100 MB recommended)
- **Logging:** 1 GB (20 GB recommended)

For information about platform support for the connector for Exchange ActiveSync, see Supported device operating systems.

Device email clients

Not all email clients consistently return the same ActiveSync ID for a device. Because the connector for Exchange ActiveSync expects a unique ActiveSync ID for each device, the following is true: Only email clients that consistently generate the same, unique ActiveSync ID for each device is supported. Citrix has tested these email clients and the clients have done without errors:

- Samsung native email client
- iOS native email client

Deploying NetScaler Gateway connector for Exchange ActiveSync

The NetScaler Gateway connector for Exchange ActiveSync enables you to use NetScaler Gateway to proxy and load balance Citrix Endpoint Management server communication with Citrix Endpoint Management managed devices. The connector for Exchange ActiveSync communicates periodically with

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management to synchronize policies. You can cluster the connector for Exchange ActiveSync and Citrix Endpoint Management, together or independently.

The connector for Exchange ActiveSync components

- **The connector for Exchange ActiveSync service:** This service provides a REST web service interface that NetScaler Gateway can invoke to determine if an ActiveSync request from a device is authorized.
- **Citrix Endpoint Management configuration service:** This service communicates with Citrix Endpoint Management to synchronize Citrix Endpoint Management policy changes with the connector for Exchange ActiveSync.
- **Citrix Endpoint Management notification service:** This service sends notifications of unauthorized device access to Citrix Endpoint Management. In this way, Citrix Endpoint Management can take appropriate measures, such as notifying the user why the device was blocked.
- **The connector for Exchange ActiveSync configuration utility:** This application allows the administrator to configure and monitor the connector for Exchange ActiveSync.

To set up listening addresses for NetScaler Gateway connector for Exchange ActiveSync

For the NetScaler Gateway connector for Exchange ActiveSync to receive requests from NetScaler Gateway to authorize ActiveSync traffic, do the following. Specify the port on which the connector for Exchange ActiveSync listens to NetScaler Gateway web service calls.

1. From the **Start** menu, select the connector for the Exchange ActiveSync configuration utility.
2. Click the **Web Service** tab and then type the listening addresses for the connector web service. You can select **HTTP** or **HTTPS** or both. If the connector for Exchange ActiveSync is co-resident with Citrix Endpoint Management (installed on the same server), select port values that do not conflict with Citrix Endpoint Management.
3. After the values are configured, click **Save** and then click **Start Service** to start the web service.

To configure device access control policies in NetScaler Gateway connector for Exchange ActiveSync

To configure the access control policy you want to apply to your managed devices, do the following:

1. In the connector for the Exchange ActiveSync configuration utility, click the **Path Filters** tab.
2. Select the first row, **Microsoft-Server-ActiveSync is for ActiveSync** and then click **Edit**.
3. From the **Policy** list, select the desired policy. For a policy that is inclusive of Citrix Endpoint Management policies, select **Static + ZDM: Permit Mode or Static + ZDM: Block Mode**. These

© 1997–2025 Citrix Systems, Inc. All rights reserved.

policies combine local (or static) rules with the rules from Citrix Endpoint Management. Permit Mode means that all devices not explicitly identified by the rules are permitted access to ActiveSync. Block Mode means that such devices are blocked.

4. After setting the policies, click **Save**.

To configure communication with Citrix Endpoint Management

Specify the name and properties of the Citrix Endpoint Management server that you want to use with the NetScaler Gateway connector for Exchange ActiveSync and NetScaler Gateway.

> **Note:**
>
> This task assumes that you have already installed and configured Citrix Endpoint Management. The Exchange ActiveSync configuration utility uses the term Config Provider for Citrix Endpoint Management.

1. In the connector for the Exchange ActiveSync configuration utility, click the **Config Providers** tab and then click **Add**.
2. Enter the name and URL of the Citrix Endpoint Management server that you're using in this deployment. If you have multiple Citrix Endpoint Management servers deployed in a multitenant deployment, this name must be unique for each server instance.
3. In **Url**, enter the Web address of the Citrix Endpoint Management GlobalConfig Provider (GCP), typically in the format `https://<FQDN>/<instanceName>/services/<MagConfigService>`. The *MagConfigService* name is case-sensitive.
4. In **Password**, enter the password to use for basic HTTP authorization with the Citrix Endpoint Management web server.
5. In **Managing Host**, enter the server name where you installed the connector for Exchange ActiveSync.
6. In **Baseline Interval**, specify a time period for when a new refreshed dynamic ruleset is pulled from Citrix Endpoint Management.
7. In **Request Timeout**, specify the server request timeout interval.
8. In **Config Provider**, select if the config provider server instance is providing the policy configuration.
9. In **Events Enabled**, enable this option if you want Secure Mobile Gateway to notify Citrix Endpoint Management when a device is blocked. This option is required if you're using the Secure Mobile Gateway rules in any of your Citrix Endpoint Management Automated Actions.
10. After configuring the server, click **Test Connectivity** to test the connection to Citrix Endpoint Management.
11. When connectivity has been established, click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Deploying NetScaler Gateway connector for Exchange ActiveSync for redundancy and scalability

To scale your NetScaler Gateway connector for Exchange ActiveSync and Citrix Endpoint Management deployment, you can install instances of the connector for Exchange ActiveSync on multiple Windows Servers. All connector instances point to the same Citrix Endpoint Management instance. Then you can use NetScaler Gateway to load balance the servers.

There are two modes for the connector for Exchange ActiveSync configuration:

- In non-shared mode, each connector for an Exchange ActiveSync instance communicates with an Citrix Endpoint Management server and keeps its own private copy of the resulting policy. For example, for a cluster of Citrix Endpoint Management servers you can run a connector instance on each Citrix Endpoint Management server. The connector then gets policies from the local Citrix Endpoint Management instance.
- In shared mode, one connector for an Exchange ActiveSync node is designated the primary node. The connector communicates with Citrix Endpoint Management. The other nodes share the resulting configuration through a Windows network share or by Windows (or third-party) replication.

The entire connector for Exchange ActiveSync configuration is in a single folder (consisting of a few XML files). The connector process detects changes to any file in this folder and automatically reloads the configuration. There is no failover for the primary node in shared mode. However, the system can tolerate the primary server being down for a few minutes (for example, to restart). The last known good configuration is cached in the connector process.

Advanced concepts

September 6, 2025

The Citrix Endpoint Management Advanced Concepts articles offer a deeper dive into product information about Citrix Endpoint Management. The aim is to help reduce deployment time through expert techniques. The articles might cite the technical experts who have authored the content.

For decision points, recommendations, common questions, and use cases for your Citrix Endpoint Management environment, see Citrix Endpoint Management deployment in this section.

For community support forums on Citrix Endpoint Management, see Citrix Discussions.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management deployment

February 22, 2024

There's a lot to consider when you're planning an Citrix Endpoint Management deployment. What devices do you choose? How do you manage them? How do you make sure that your network stays secure while still providing a good user experience? What hardware do you need in place and how do you troubleshoot it? The articles in this section aim to help answer such questions. Included are use cases and recommendations on topics that cover your deployment concerns.

Keep in mind that a guideline or recommendation might not apply to all environments or use cases. Be sure to set up a test environment before going live with an Citrix Endpoint Management deployment.

The articles in this section cover these areas:

- **Assess:** Common use cases and questions to consider when planning your deployment.
- **Design & Configure:** Recommendations for designing and configuring your environment
- **Operate & Monitor:** Making sure the smooth operation of your running environment.

Assess

As with any deployment, assessing your needs must be your first priority. What is your primary need for Citrix Endpoint Management? Is it necessary to manage every device in your environment, just the apps, or both? What level of security is needed for your Citrix Endpoint Management environment? Let's look at common use cases and questions for you to consider when planning your deployment.

- Management modes
- Device requirements
- Security and user experience
- Apps
- User communities
- Email strategy
- Citrix Endpoint Management integration

Design and Configure

Once you finish assessing your deployment needs, you can decide how to design and configure your environment. The items to plan include:

- Choosing the hardware for your server

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Setting up policies for apps and devices
- Getting users enrolled

This section includes use cases and recommendations for each of these scenarios and more.

- Integrating with NetScaler Gateway and Citrix ADC
- SSO and proxy considerations for MDX apps
- Authentication
- Server properties
- Device and app policies
- User enrollment options

Operate and Monitor

After your Citrix Endpoint Management environment is up and running, you'll want to monitor it to make sure the smooth operation. The monitoring section discusses where you can find the various logs and messages Citrix Endpoint Management and its components generate, and how to read those logs. This section also includes various common troubleshooting steps that you can follow to reduce customer support feedback time.

- App provisioning and deprovisioning
- Dashboard-based operations
- Role-based Access Control and Citrix Endpoint Management support
- Monitor and support
- Citrix support process

Management modes

February 23, 2024

Management modes is a term that includes Mobile Device Management (MDM) and Mobile App Management (MAM). You can configure:

- Enrollment profiles to enroll Android and iOS devices into MDM, MAM, or both (MDM+MAM). If you choose MDM+MAM, you can give users the ability to opt out of MDM.
- Enrollment profiles to enroll Windows 10 and Windows 11 devices into MDM.

You specify enrollment options in enrollment profiles, which you attach to delivery groups. For information about enrollment options, see Enrollment profiles. The following sections focus on considerations for managing devices and apps.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Mobile Device Management (MDM)

Using MDM, you can configure, secure, and support mobile devices. MDM enables you to protect devices and data on devices at a system level. You can configure policies, actions, and security functions. For example, you can wipe a device selectively if the device is lost, stolen, or out of compliance.

Even if you don't choose to manage apps on devices, you can deliver mobile apps, such as public app store and enterprise apps.

The following are common use cases for MDM:

- MDM is a consideration for corporate-owned devices where device-level management policies or certain restrictions are required. Those restrictions include full wipe, selective wipe, or geolocation.
- When customers require management of an actual device, but do not require MDX policies.
- When users only need email delivered to their native email clients on their mobile devices, and Exchange ActiveSync or Client Access Server is already externally accessible. In this use case, you can use MDM to configure email delivery.
- When you deploy native enterprise apps (non-MDX), public app store apps, or MDX apps delivered from public stores. Consider that an MDM solution alone might not prevent data leakage of confidential information between apps on the device. Data leakage might occur with copy and paste or Save As operations in Office 365 apps.

Mobile app management (MAM)

MAM protects app data and lets you control app data sharing. MAM also allows for the management of corporate data and resources, separately from personal data. With Citrix Endpoint Management configured for MAM, you can use MDX-enabled mobile apps to provide per-app containerization and control.

By using MDX policies, Citrix Endpoint Management provides app-level control over network access (such as micro VPN), app and device interaction, and app access.

MAM is often suitable for bring-your-own (BYO) devices because although the device is unmanaged, corporate data is protected. MDX has many MAM-only policies that don't require an MDM control.

MAM also supports the Citrix mobile productivity apps. This support includes:

- Secure email delivery to Citrix Secure Mail
- Data sharing between the secured Citrix mobile productivity apps
- Secure data storage in Citrix Files.

For details, see Mobile productivity apps.

MAM is often suitable for the following examples:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- You deliver mobile apps, such as MDX apps, managed at the app level.
- You are not required to manage devices at a system level.

MDM+MAM

Citrix Endpoint Management lets you specify whether users can opt out of device management. This flexibility is useful for environments that include a mix of use cases. These environments might require management of a device through MDM policies to access your MAM resources.

MDM+MAM is suitable for the following examples:

- You have a single use case in which both MDM and MAM are required. MDM is required to access your MAM resources.
- Some use cases require MDM while some do not.
- Some use cases require MAM while some do not.

Device Management and MDM Enrollment

An Citrix Endpoint Management Enterprise environment can include a mixture of use cases, some of which require device management through MDM policies to allow access to MAM resources.

Before deploying Citrix mobile productivity apps to users, fully assess your use cases and decide whether to require MDM enrollment. If you later decide to change the requirement for MDM enrollment, users might need to re-enroll their devices. For more information, see Enrollment profiles.

For information about enrollment and NetScaler Gateway, see Integrating with NetScaler Gateway and Citrix ADC.

The following is a summary of the advantages and disadvantages (along with mitigations) of requiring MDM enrollment.

When MDM enrollment is optional

Advantages

- Users can access MAM resources without putting their devices under MDM management. This option can increase user adoption.
- Ability to secure access to MAM resources to protect enterprise data.
- MDX policies such as **App Passcode** can control app access for each MDX app.
- Configuring NetScaler Gateway, Citrix Endpoint Management, and per-application time-outs, along with Citrix PIN, provide an extra layer of protection.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- While MDM actions do not apply to the device, some MDX policies are available to deny MAM access. The denial is based on system settings such as jailbroken, or rooted devices.
- Users can choose whether to enroll their device with MDM during first-time use.

Disadvantages

- MAM resources are available to devices not enrolled in MDM.
- MDM policies and actions are available only to MDM-enrolled devices.

Mitigation options

- Have users agree to a company terms and conditions that hold them responsible if they choose to go out of compliance. Have administrators monitor unmanaged devices.
- Manage application access and security by using application timers. Reduced time-out values increase security, but can affect the user experience.

When MDM enrollment is required

Advantages

- Ability to restrict access to MAM resources only to MDM-managed devices.
- MDM policies and actions can apply to all devices in the environment as you wanted.
- Users are not able to opt out of enrolling their device.

Disadvantages

- Requires all users to enroll with MDM.
- Might reduce adoption for users who object to corporate management of their personal devices.

Mitigation options

- Educate users about what Citrix Endpoint Management actually manages on their devices and what information administrators can access.

Device requirements

February 23, 2024

© 1997–2025 Citrix Systems, Inc. All rights reserved.

An important point to consider for any deployment is the set of devices you plan to roll out. On the iOS, Android, and Windows platforms, the options are many. For a list of devices that Citrix Endpoint Management supports, see Supported device platforms.

In a bring your own device (BYOD) environment, a mixture of supported platforms is possible. Consider the limitations in the Supported device platform article, however, when informing users about the devices they can enroll. Even if you only allow one or two devices in your environment, Citrix Endpoint Management functions slightly different on the iOS, Android, and Windows devices. Different feature sets are available on each platform.

Also, not all app designs target both tablet and phone form factors. Before you make widespread changes, test the apps to make sure that they fit the device screen that you want to roll out.

You can consider enrollment factors as well. Apple and Google offer enterprise enrollment programs. Through the Apple Deployment Program and Google Android Enterprise, you can buy devices that are preconfigured and ready for employees to use.

For more information about enrollment, see User enrollment options.

Security and user experience

September 6, 2025

Security is important to any organization, but you need to achieve a balance between security and user experience. For example, you might have a highly secured environment that is difficult for users to use. Or, your environment might be so user-friendly that access control is not as strict. The other sections in this virtual handbook cover security features in detail. The purpose of this article is to give a general overview of common security concerns and the security options available in Citrix Endpoint Management.

Here are some key considerations to keep in mind for each use case:

- Do you want to secure certain apps, the entire device, or both?
- How do you want your users to authenticate their identity? Do you want to use LDAP, certificate-based authentication, or a combination of the two?
- How long do you want a user's session to last before it times out? Keep in mind that there are different time-out values for background services, Citrix ADC, and for being able to access apps while offline.
- Do you want users to set up a device-level passcode and an app-level passcode? How many sign-in attempts do you want to allow? Keep in mind the additional per-app authentication requirements that might be implemented with MAM and how users might perceive them.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- What other restrictions do you want to place on users? Do you want to give users access to cloud services such as Siri? What can they do with each app you make available to them and what can they not do? Do you want to deploy corporate network (Wi-Fi) policies to prevent cellular data plans from being used from inside the office?

App versus Device

One of the first things to consider is whether you want to secure:

- Only certain apps (mobile app management, or MAM)
- The entire device (Mobile Device Management, or MDM).
- MDM+MAM

Most commonly, if you don't require device-level control, you only need to manage mobile apps, especially if your organization supports Bring Your Own Device (BYOD).

Users with devices that Citrix Endpoint Management doesn't manage can install apps through the app store. Instead of device-level controls, such as selective or full wipe, you control access to the apps through app policies. Depending on the values you set, the policies require the device to check Citrix Endpoint Management periodically to confirm that the apps are still allowed to run.

MDM allows you to secure an entire device, including the ability to take inventory of all the software on a device. MDM allows you to prevent enrollment if the device is jailbroken, rooted, or has unsafe software installed. Taking this level of control, however, makes users leery of allowing that much power over their personal devices and can reduce enrollment rates.

Authentication

Authentication is where a great deal of the user experience takes place. If your organization is already running Active Directory, using Active Directory is the simplest way to have your users access the system.

Another significant part of the authentication user experience is time-outs. A high security environment might have users sign on every time they access the system. That option might not be ideal for all organizations or use cases.

User Entropy

For added security, you can enable a feature called *user entropy*. Citrix Secure Hub and some other apps often share common data like passwords, PINs, and certificates to make sure everything functions properly. This information is stored in a generic vault within Citrix Secure Hub. If you enable user entropy through the **Encrypt Secrets** option, Citrix Endpoint Management creates a vault called

© 1997–2025 Citrix Systems, Inc. All rights reserved.

UserEntropy. Citrix Endpoint Management moves the information from the generic vault into this new vault. For Citrix Secure Hub or another app to access the data, users must enter a password or PIN.

Enabling user entropy adds another layer of authentication in several places. As a result, whenever an app requires access to shared data in the UserEntropy vault (including passwords, PINs, and certificates), users must authenticate.

You can learn more about user entropy by reading About the MDX Toolkit. To turn on user entropy, you can find the related settings in the Client properties.

Policies

Both MDX and MDM policies give a great deal of flexibility to organizations, but they can also restrict users. You might want that restriction in some situations, but policies can also make a system unusable. For instance, you might want to block access to cloud applications such as Siri or iCloud that have the potential to send sensitive data to outside locations. You can set up a policy to block access to these services, but keep in mind that such a policy can have unintended consequences. For example, the iOS keyboard mic relies on cloud access.

Apps

Enterprise Mobility Management (EMM) segments into Mobile Device Management (MDM) and Mobile Application Management (MAM). While MDM enables organizations to secure and control mobile devices, MAM eases application delivery and management. With the increasing adoption of BYOD, you can typically implement a MAM solution, such as Citrix Endpoint Management, to assist with the following:

- app delivery
- software licensing
- configuration
- app life cycle management

With Citrix Endpoint Management, you can add more security to these apps by configuring specific MAM policies and VPN settings to prevent data leaks and other security threats. Citrix Endpoint Management provides organizations with the flexibility to include both MDM and MAM functionality in the same environment.

In addition to the ability to deliver apps to mobile devices, Citrix Endpoint Management offers app containerization through MDX technology. MDX secures apps through encryption that is separate from device-level encryption provided by the platform. You can wipe or lock apps. Apps are subject to granular policy-based controls. Independent software vendors (ISVs) can apply these controls using the Mobile Apps SDK.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

In a corporate environment, users use various mobile apps to aid in their job role. The apps can include apps from the public app store, in-house developed apps, or native apps. Citrix Endpoint Management categorizes these apps as follows:

Public apps: These apps include free or paid apps available in a public app store, such as the Apple App Store or Google Play. Vendors outside of the organization often make their apps available in public app stores. This option lets their customers download the apps directly from the Internet. You might use many public apps in your organization depending on users' needs. Examples of such apps include GoToMeeting, Salesforce, and EpicCare apps.

Citrix® does not support downloading app binaries directly from public app stores, then wrapping them with the MDX Toolkit for enterprise distribution. To MDX-enable third-party applications, contact your app vendor to get the app binaries. You can wrap the binaries by using the MDX Toolkit or integrate the MAM SDK with the binaries.

In-house apps: Many organizations have in-house developers who create apps that provide specific functionality and are independently developed and distributed within the organization. In certain cases, some organizations might also have apps that ISVs provide. You can deploy such apps as native apps or you can containerize the apps by using a MAM solution, such as Citrix Endpoint Management. For example, a healthcare organization can create an in-house app that allows physicians to view patient information on mobile devices. An organization can then MAM SDK enable or MDM-wrap the app to secure patient information and enable VPN access to the back-end patient database server.

Web and SaaS apps: These apps include apps accessed from an internal network (web apps) or over a public network (SaaS). Citrix Endpoint Management also allows you to create custom web and SaaS apps using a list of app connectors. These app connectors can facilitate single sign-on (SSO) to existing Web apps. For details, see App connector types. For example, you can use Google Apps SAML for SSO based on Security Assertion Markup Language (SAML) to Google Apps.

Mobile productivity apps: Mobile productivity apps are Citrix-developed apps that are included with the Citrix Endpoint Management license. For details, see About mobile productivity apps. Citrix also offers other business-ready apps. ISVs develop business-ready apps by using the Mobile Apps SDK.

HDX apps: HDX apps are Windows-hosted apps that you publish with StoreFront. If you have a Citrix Virtual Apps and Desktops environment, you can integrate the apps with Citrix Endpoint Management to make the apps available to the enrolled users.

Depending on the type of mobile apps that you plan to deploy and manage with Citrix Endpoint Management, the underlying configuration and architecture differ. Suppose that many groups of users with various levels of permissions consume a single app. In that case, you can create separate delivery groups to deploy two versions of the app. Make sure that the user group membership is mutually exclusive to avoid policy mismatches on user devices.

You might also want to manage iOS application licensing by using Apple Volume Purchase. This option requires that you register for the Apple Volume Purchase program. And, you must use the Citrix

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Endpoint Management console to configure Volume Purchase settings. That configuration allows you to distribute the apps with the Volume Purchase licenses. Various such use cases make it important to assess and plan your MAM strategy before implementing the Citrix Endpoint Management environment. You can start planning your MAM strategy by defining the following:

Types of apps: List the different types of apps that you plan to support. Then, categorize the apps, such as public, native, Citrix mobile productivity apps, Web, in-house, and ISV apps. Also, categorize the apps for different device platforms, such as iOS and Android. This categorization helps you to align the Citrix Endpoint Management settings that are required for each type of app. For example: Certain apps might not qualify for wrapping. Or, a few apps might require use of the Mobile Apps SDK to enable special APIs for interaction with other apps.

Network requirements: Configure apps with specific network access requirements with the appropriate settings. For example, certain apps might need access to your internal network through a VPN. Some apps might require Internet access to route access via the DMZ. To allow such apps to connect to the required network, you have to configure various settings accordingly. Define per-app network requirements to help finalize your architectural decisions up front. That work streamlines the overall implementation process.

Security requirements: Define the security requirements that apply to either individual apps or all the apps. Some settings, such as the MDX policies, apply to individual apps. Session and authentication settings apply across all apps. Some apps might have specific encryption, containerization, wrapping, authentication, geofencing, passcode, or data sharing requirements. Outline those requirements in advance to simplify your deployment.

Deployment requirements: You might want to use a policy-based deployment to allow only compliant users to download the published apps. For example, you might want certain apps to require that:

- device platform-based encryption is enabled
- the device is managed
- the device meets a minimum operating system version
- certain apps are available only to corporate users

Outline such requirements in advance so that you can configure the appropriate deployment rules or actions.

Licensing requirements: Record app-related licensing requirements. Such notes help you to manage license usage effectively and to decide if you need to configure specific features in Citrix Endpoint Management to facilitate licensing. For example, if you deploy a free or paid iOS app, Apple enforces licensing requirements on the app by making users sign on to their Apple Store account. You can register for Apple Volume Purchase to distribute and manage these apps through Citrix Endpoint Management. Volume Purchase allows users to download the apps without having to sign into their Apple

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Store account. Also, tools, such as Samsung Knox, have special licensing requirements, which you need to complete before deploying those features.

Allow list and block list requirements: You likely want to prevent users from installing or using some apps. Create an allow list of apps that make a device out of compliance. Then, set up policies to trigger when a device becomes non-compliant. On the other hand, an app might be acceptable for use but might fall under the block list for some reason. In that case, you can add the app to an allow list and indicate that the app is acceptable to use, but isn't required. Also, keep in mind that the apps pre-installed on new devices can include some commonly used apps that are not part of the operating system. Those apps might conflict with your block list strategy.

Apps use case

A healthcare organization plans to deploy Citrix Endpoint Management to serve as a MAM solution for their mobile apps. Mobile apps are delivered to corporate and BYOD users. IT decides to deliver and manage the following apps:

- **Mobile productivity apps:** iOS and Android apps provided by Citrix.
- **Citrix Files:** App to access shared data and to share, sync, and edit files.

Public app store

- **Citrix Secure Hub:** Client used by all mobile devices to communicate with Citrix Endpoint Management. IT pushes security settings, configurations, and mobile apps to mobile devices via the Citrix Secure Hub client. Android and iOS devices enroll in Citrix Endpoint Management through Citrix Secure Hub.
- **Citrix Workspace app:** Mobile app that allows users to open on mobile devices apps hosted by Citrix Virtual Apps.
- **GoToMeeting:** An online meeting, desktop sharing, and video conferencing client that lets users meet with other computer users, customers, clients, or colleagues via the Internet in real time.
- **SalesForce1:** Salesforce1 lets users access Salesforce from mobile devices and brings all Chatter, CRM, custom apps, and business processes together in a unified experience for any Salesforce user.
- **RSA SecurID:** Software-based token for two-factor authentication.
- **EpicCare apps:** These apps give healthcare practitioners secure and portable access to patient charts, patient lists, schedules, and messaging.
  - **Haiku:** Mobile app for the iPhone and Android phones.
  - **Canto:** Mobile app for the iPad
  - **Rover:** Mobile apps for iPhone and iPad.

HDX: Citrix Virtual Apps delivers HDX apps to Citrix Workspace.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Epic Hyperspace:** Epic client application for electronic health record management.

ISV

- **Vocera:** HIPAA compliant voice-over IP and messaging mobile app that extends the benefits of Vocera voice technology anytime, anywhere via iPhone and Android smartphones.

In-house apps

- **HCMail:** App that helps compose encrypted messages, search address books on internal mail servers, and send the encrypted messages to the contacts using an email client.

In-house web apps

- **PatientRounding:** Web application used to record patient health information by different departments.
- **Outlook Web Access:** Allows the access of email via a web browser.
- **SharePoint:** Used for organization-wide file and data sharing.

The following table lists the basic information required for MAM configuration.

App Name	App Type	MDX Wrapping	iOS	Android
Citrix Secure Mail	Mobile productivity app	No for version 10.4.1 and later	Yes	Yes
Citrix Secure Web	Mobile productivity app	No for version 10.4.1 and later	Yes	Yes
Citrix Files	Mobile productivity app	No for version 10.4.1 and later	Yes	Yes
Citrix Secure Hub	Public App	NA	Yes	Yes
Citrix Workspace app	Public App	NA	Yes	Yes
GoToMeeting	Public App	NA	Yes	Yes
SalesForce1	Public App	NA	Yes	Yes
RSA SecurID	Public App	NA	Yes	Yes
Epic Haiku	Public App	NA	Yes	Yes
Epic Canto	Public App	NA	Yes	No
Epic Rover	Public App	NA	Yes	No
Epic Hyperspace	HDX™ App	NA	Yes	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App Name	App Type	MDX Wrapping	iOS	Android
Vocera	ISV App	Yes	Yes	Yes
HCMail	In-House App	Yes	Yes	Yes
PatientRounding	Web App	NA	Yes	Yes
Outlook Web Access	Web App	NA	Yes	Yes
SharePoint	Web App	NA	Yes	Yes

The following tables list specific requirements that you can consult when configuring MAM policies in Citrix Endpoint Management.

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Device platform-based encryption
Citrix Secure Mail	Y	Selectively Allowed	Allowed	Not required
Citrix Secure Web	Y	Allowed	Allowed	Not required
Citrix Files	Y	Allowed	Allowed	Not required
Citrix Secure Hub	Y	N/A	N/A	N/A
Citrix Workspace app	Y	N/A	N/A	N/A
GoToMeeting	N	N/A	N/A	N/A
SalesForce1	N	N/A	N/A	N/A
RSA SecurID	N	N/A	N/A	N/A
Epic Haiku	Y	N/A	N/A	N/A
Epic Canto	Y	N/A	N/A	N/A
Epic Rover	Y	N/A	N/A	N/A
Epic Hyperspace	Y	N/A	N/A	N/A
Vocera	Y	Blocked	Blocked	Not required
HCMail	Y	Blocked	Blocked	Required
PatientRounding	Y	N/A	N/A	Required
Outlook Web Access	Y	N/A	N/A	Not required

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Device platform-based encryption
SharePoint	Y	N/A	N/A	Not required

App Name	Proxy Filtering	Licensing	Geofencing	Mobile Apps SDK	Minimum Operating System Version
Citrix Secure Mail	Required	N/A	Selectively Required	N/A	Enforced
Citrix Secure Web	Required	N/A	Not required	N/A	Enforced
Secure Notes	Required	N/A	Not required	N/A	Enforced
Citrix Files	Required	N/A	Not required	N/A	Enforced
Citrix Secure Hub	Not required	Volume Purchase	Not required	N/A	Not enforced
Citrix Workspace app	Not required	Volume Purchase	Not required	N/A	Not enforced
GoToMeeting	Not required	Volume Purchase	Not required	N/A	Not enforced
SalesForce1	Not required	Volume Purchase	Not required	N/A	Not enforced
RSA SecurID	Not required	Volume Purchase	Not required	N/A	Not enforced
Epic Haiku	Not required	Volume Purchase	Not required	N/A	Not enforced
Epic Canto	Not required	Volume Purchase	Not required	N/A	Not enforced
Epic Rover	Not required	Volume Purchase	Not required	N/A	Not enforced
Epic Hyperspace	Not required	N/A	Not required	N/A	Not enforced
Vocera	Required	N/A	Required	Required	Enforced
HCMail	Required	N/A	Required	Required	Enforced

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App Name	Proxy Filtering	Licensing	Geofencing	Mobile Apps SDK	Minimum Operating System Version
PatientRounding	Required	N/A	Not required	N/A	Not enforced
Outlook Web Access	Required	N/A	Not required	N/A	Not enforced
SharePoint	Required	N/A	Not required	N/A	Not enforced

User Communities

Every organization consists of diverse user communities that operate in different functional roles. These user communities do different tasks and office functions using various resources that you provide through user devices. Users might work from home or in remote offices using mobile devices that you provide. Or, users might own their mobile devices, which allow them to access tools that are subject to certain security compliance rules.

As more user communities start using mobile devices in their job roles, Enterprise Mobility Management (EMM) becomes critical to prevent data leaks. EMM is also critical to enforce an organization's security restrictions. For efficient and more sophisticated Mobile Device Management, you can categorize your user communities. Doing so simplifies the mapping of users to resources and aligns the appropriate security policies to users.

The following example illustrates how the user communities of a healthcare organization are classified for EMM.

User communities use case

This example healthcare organization provides technology resources and access to many users, including network and affiliate employees and volunteers. The organization has chosen to roll out the EMM solution to non-executive users only.

User roles and functions for this organization can be broken into subgroups including: clinical, non-clinical, and contractors. Selected users receive corporate mobile devices, while others can access limited company resources from their personal devices. To enforce the right level of security restrictions and prevent data leaks, the organization decided that corporate IT manages each enrolled device. Those devices might be corporate-owned or Bring Your Own Device (BYOD). Also, users can only enroll a single device.

The following section provides an overview of the roles and functions of each subgroup:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Clinical

- Nurses
- Physicians (Doctors, Surgeons, and so on)
- Specialists (Dieticians, anesthesiologists, radiologists, cardiologists, oncologists, and so on)
- Outside physicians (Non-employee physicians and office workers that work from remote offices)
- Home Health Services (Office and mobile workers doing physician services for patient home visits)
- Research Specialist (Knowledge Workers and Power Users at six Research Institutes doing clinical research to find answers to issues in medicine)
- Education and Training (Nurses, physicians, and specialists in education and training)

Non-Clinical

- Shared Services (Office workers doing various back-office functions, including HR, Payroll, Accounts Payable, and Supply Chain Service)
- Physician Services (Office workers doing various healthcare management, administrative services, and business process solutions to providers, including: Administrative Services, Analytics and Business Intelligence, Business Systems, Client Services, Finance, Managed Care Administration, Patient Access Solutions, Revenue Cycle Solutions, and so on)
- Support Services (Office workers doing various non-clinical functions including: Benefits Administration, Clinical Integration, Communications, Compensation and Performance Management, Facility and Property Services, HR Technology Systems, Information Services, Internal Audit and Process Improvement, and so o.)
- Philanthropic Programs (Office and mobile workers that do various functions in support of philanthropic programs)

Contractors

- Manufacturer and vendor partners (Onsite and remotely connected via site-to-site VPN providing various non-clinical support functions)

Based on the preceding information, the organization created the following entities. For more information about delivery groups in Citrix Endpoint Management, see Deploy resources.

Active Directory Organizational Units (OUs) and Groups For OU **=** Citrix Endpoint Management Resources:

- OU = Clinical; Groups =
  - XM-Nurses

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - XM-Physicians
  - XM-Specialists
  - XM-Outside Physicians
  - XM-Home Health Services
  - XM-Research Specialist
  - XM-Education and Training

- OU = Non-Clinical; Groups =

  - XM-Shared Services
  - XM-Physician Services
  - XM-Support Services
  - XM-Philanthropic Programs

Citrix Endpoint Management Local Users and Groups For Group= Contractors, Users =

- Vendor1
- Vendor2
- Vendor 3
- …Vendor 10

Citrix Endpoint Management Delivery Groups

- Clinical-Nurses
- Clinical-Physicians
- Clinical-Specialists
- Clinical-Outside Physicians
- Clinical-Home Health Services
- Clinical-Research Specialist
- Clinical-Education and Training
- Non-Clinical-Shared Services
- Non-Clinical-Physician Services
- Non-Clinical-Support Services
- Non-Clinical-Philanthropic Programs

Delivery Group and User Group mapping

Active Directory Groups	Citrix Endpoint Management Delivery Groups
XM-Nurses	Clinical-Nurses

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Active Directory Groups	Citrix Endpoint Management Delivery Groups
XM-Physicians	Clinical-Physicians
XM-Specialists	Clinical-Specialists
XM-Outside Physicians	Clinical-Outside Physicians
XM-Home Health Services	Clinical-Home Health Services
XM-Research Specialist	Clinical-Research Specialist
XM-Education and Training	Clinical-Education and Training
XM-Shared Services	Non-Clinical-Shared Services
XM-Physician Services	Non-Clinical-Physician Services
XM-Support Services	Non-Clinical-Support Services
XM-Philanthropic Programs	Non-Clinical-Philanthropic Programs

Delivery Group and Resource mapping The following tables illustrate the resources assigned to each delivery group in this use case. The first table shows the mobile app assignments. The second table shows the public app, HDX apps, and device management resources.

Citrix Endpoint Management Delivery Groups	Citrix Mobile Apps	Public Mobile Apps	HDX Mobile Apps
Clinical-Nurses	X		
Clinical-Physicians			
Clinical-Specialists			
Clinical-Outside Physicians	X		
Clinical-Home Health Services	X		
Clinical-Research Specialist	X		
Clinical-Education and Training		X	X
Non-Clinical-Shared Services		X	X
Non-Clinical-Physician Services		X	X

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management Delivery Groups	Citrix Mobile Apps	Public Mobile Apps	HDX Mobile Apps
Non-Clinical-Support Services	X	X	X
Non-Clinical-Philanthropic Programs	X	X	X
Contractors	X	X	X

Citrix Endpoint Management Delivery Groups	Public App: RSA SecurID	Public App: EpicCare Haiku	HDX App: Epic Hyperspace	Passcode Policy	Device Restrictions	Automated Actions	Network Policy
Clinical-Nurses							X
Clinical-Physicians					X		
Clinical-Specialists							
Clinical-Outside Physicians							
Clinical-Home Health Services							
Clinical-Research Specialist							
Clinical-Education and Training		X	X				

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management Delivery Groups	Public App: RSA SecurID	Public App: EpicCare Haiku	HDX App: Epic Hyperspace	Passcode Policy	Device Restrictions	Automated Actions	Network Policy
Non-Clinical-Shared Services		X	X				
Non-Clinical-Physician Services		X	X				
Non-Clinical-Support Services		X	X				

Notes and considerations

- Citrix Endpoint Management creates a default delivery group named All Users during the initial configuration. If you do not disable this delivery group, all Active Directory users have the right to enroll into Citrix Endpoint Management.
- Citrix Endpoint Management synchronizes Active Directory users and groups on demand using a dynamic connection to the LDAP server.
- If a user is part of a group that is not mapped in Citrix Endpoint Management, that user cannot enroll. Likewise, if a user is a member of many groups, Citrix Endpoint Management only categorizes the user as part of the groups mapped to Citrix Endpoint Management.

Security requirements

The scope of security considerations related to an Citrix Endpoint Management environment can quickly become overwhelming. There are many interlocking pieces and settings. You might not know where to begin or what to choose to make sure an acceptable level of protection is available. To make these choices simpler, Citrix provides recommendations for High, Higher, and Highest Security, as outlined in the following table.

Security concerns aren't the only consideration for the mode in which your devices enroll: MAM, MDM+MAM with MDM optional, or MDM+MAM with MDM required. It is important to also review the

© 1997–2025 Citrix Systems, Inc. All rights reserved.

requirements of the use case and decide if you can mitigate security concerns before choosing your management mode.

High: Using these settings provides an optimal user experience while maintaining a basic level of security acceptable to most organizations.

Higher: These settings create a stronger balance between security and usability.

Highest: Following these recommendations provides a high level of security at the cost of usability and user adoption.

Management mode security considerations

The following table specifies the management modes for each security level.

High Security	Higher Security	Highest Security
MAM, MDM+MAM	MDM+MAM	MDM+MAM

Notes:

- Depending on the use case, a MAM-only deployment can meet security requirements and provide a good user experience.
- For use cases like BYOD in which all business and security requirements might be satisfied with app containerization only, Citrix recommends MAM-only mode.
- For high security environments (and corporate issued devices), Citrix recommends MDM+MAM to take advantage of all security capabilities available.

Citrix ADC and NetScaler Gateway security considerations

The following table specifies the Citrix ADC and NetScaler Gateway recommendations for each security level.

High Security	Higher Security	Highest Security
Citrix ADC is recommended. NetScaler Gateway is required for MAM and MDM+MAM	Standard NetScaler for XenMobile wizard configuration with SSL bridge if Citrix Endpoint Management is in the DMZ.	SSL Offload with end-to-end encryption

Notes:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Exposing the Citrix Endpoint Management server to the Internet via NAT or existing third-party proxies/load-balancers might be an option for MDM. However, in that case, the SSL traffic terminates on an Citrix Endpoint Management server, which poses a potential security risk.
- For high security environments, NetScaler Gateway with the default Citrix Endpoint Management configuration typically meets or exceeds security requirements.
- For MDM enrollments with the highest security needs, SSL termination at NetScaler Gateway enables you to inspect traffic at the perimeter, while maintaining end-to-end SSL encryption.
- Options to define SSL/TLS ciphers.
- For more information, see Integrating with NetScaler Gateway and Citrix ADC.

Enrollment security considerations

The following table specifies the Citrix ADC and NetScaler Gateway recommendations for each security level.

High Security	Higher Security	Highest Security
Active Directory Group membership only. All users Delivery Group disabled.	Invitation only enrollment security mode. Active Directory Group membership only. All users Delivery Group disabled	Enrollment security mode tied to Device ID. Active Directory Group membership only. All users Delivery Group disabled

> **Notes:**
>
> - Citrix generally recommends that you restrict enrollment to users in predefined Active Directory groups only. This restriction requires disabling the built-in All users delivery group.
> - You can use enrollment invitations to restrict enrollment to users with an invitation. Enrollment invitations aren't available for Windows devices.
> - You can use one-time PIN (OTP) enrollment invitations as a two-factor authentication solution and to control the number of devices a user can enroll. (OTP invitations aren't available for Windows devices.)

Device passcode security considerations

The following table specifies the device passcode recommendations for each security level.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

High Security	Higher Security	Highest Security
Recommended. High security is required for device-level encryption. Can be enforced with MDM. Can be set as required for MAM-only by using the MDX policy, Non-compliant device behavior.	Enforced by using an MDM, MAM, or MDM+MAM policy.	Enforced by using an MDM and MDX policy. MDM Complex passcode policy.

Notes:

- Citrix recommends the use of a device passcode.
- You can enforce a device passcode via an MDM policy.
- You can use an MDX policy to make a device passcode a requirement for using managed apps; for example, for BYOD use cases.
- Citrix recommends combining the MDM and MDX policy options for increased security for MDM+MAM enrollments.
- For environments with the highest security requirements, you can configure complex passcode policies and enforced them with MDM. You can configure automatic actions to notify administrators or issue selective/full device wipes when a device doesn't follow a passcode policy.

Apps

September 6, 2025

The Enterprise Mobility Management (EMM) segments into Mobile Device Management (MDM) and Mobile Application Management (MAM). While MDM enables organizations to secure and control mobile devices, MAM helps with application delivery and management. With the increasing adoption of BYOD, you can typically implement a MAM solution, such as Citrix Endpoint Management. Citrix Endpoint Management assists with application delivery, software licensing, configuration, and application life cycle management. You can require or allow users to also opt into MDM management.

With Citrix Endpoint Management, you secure apps by configuring MAM policies and VPN settings to prevent data leaks and other security threats. Citrix Endpoint Management provides organizations with the flexibility to enroll devices as MAM-only or MDM+MAM.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Along with the ability to deliver apps to mobile devices, Citrix Endpoint Management offers app containerization through MDX technology. The apps are subject to granular policy-based controls. Independent software vendors (ISVs) can apply these controls using the Mobile Apps SDK.

In a corporate environment, users use various mobile apps to aid in their job role. The apps can include apps from the public app store, in-house developed apps, or native apps. Citrix Endpoint Management categorizes these apps as follows:

- **Public apps:** These apps include free or paid apps available in a public app store, such as the Apple App Store or Google Play. Vendors outside of the organization often make their apps available in public app stores. This option lets their customers download the apps directly from the Internet. You might use many public apps in your organization depending on users' needs. Examples of such apps include GoToMeeting, Salesforce, and EpicCare apps.
  - **If you use the MAM SDK:** Obtain the app binaries from your app vendor. Then, integrate the MAM SDK into the app.
  - **If you use the MDX Toolkit:** Citrix® does not support downloading app binaries directly from public app stores, and then wrapping them with the MDX Toolkit for enterprise distribution. To wrap third-party applications, work with your app vendor to get the app binaries. You can then wrap the binaries by using the MDX Toolkit.
- **In-house apps:** Many organizations have in-house developers who create apps that provide specific functionality and are independently developed and distributed within the organization. In certain cases, some organizations might also have apps that ISVs provide. You can deploy such apps as native apps or you can containerize the apps by using a MAM solution, such as Citrix Endpoint Management.

  For example, a healthcare organization might create an in-house app that allows physicians to view patient information on mobile devices. An organization can then secure patient information and enable VPN access to the patient database by using one of the following:
  - MAM SDK
  - MDX Toolkit
- **Web and SaaS apps:** These apps include apps accessed from an internal network (web apps) or over a public network (SaaS). Citrix Endpoint Management also allows you to create custom web and SaaS apps using a list of app connectors. These app connectors can facilitate single sign-on (SSO) to existing Web apps. For details, see App connector types. For example, you can use Google Apps SAML for SSO based on Security Assertion Markup Language (SAML) to Google Apps.
- **Mobile productivity apps:** Mobile productivity apps are Citrix-developed apps that are included with the Citrix Endpoint Management license. For details, see About mobile produc-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

tivity apps. Citrix also offers other business-ready apps that ISVs develop by using the Mobile Apps SDK.

- **HDX apps:** HDX apps are Windows-hosted apps that you publish with StoreFront. If you use Citrix Virtual Apps and Desktops and Citrix Workspace, HDX apps are available to enrolled users.

Depending on the type of mobile apps you plan to deploy and manage with Citrix Endpoint Management, the underlying configuration might differ. For example, many groups of users with different levels of permissions might consume a single app. In that case you can create separate delivery groups to deploy two separate versions of the same app. Also, you must make sure that the user group membership is mutually exclusive to avoid policy mismatches on users' devices.

You can also manage iOS application licensing by using Apple Volume Purchase. This option requires you to register for the Volume Purchase program and configure the Volume Purchase settings in the Citrix Endpoint Management console. That configuration allows you to distribute the apps with the Volume Purchase licenses. Various use cases make it important to assess and plan your MAM strategy before implementing the Citrix Endpoint Management environment. You can start planning your MAM strategy by defining the following:

- **Types of apps:** List the different types of apps that you plan to support and categorize them, such as public, native, Web, in-house, or ISV apps. Also, categorize the apps for different device platforms, such as iOS and Android. This categorization helps with aligning the various Citrix Endpoint Management settings that are required for each type of app. For example, a few apps might require use of the Mobile Apps SDK to enable special APIs for interaction with other apps.
- **Network requirements:** Configure the settings of apps that have specific network access requirements. For example, certain apps might need access to your internal network through a VPN. Some apps might require Internet access to route access via the DMZ. To allow such apps to connect to the required network, you must configure various settings accordingly. Defining per-app network requirements help in completing your architectural decisions early on, which streamlines the overall implementation process.
- **Security requirements:** You can define security requirements to apply to either individual apps or all apps.

  - Settings, such as the MDX policies, apply to individual apps
  - Session and authentication settings apply across all apps
  - Some apps might have specific containerization, MDX, authentication, geofencing, passcode, or data sharing requirements

  Outline those requirements in advance to simplify your deployment. For details on security in Citrix Endpoint Management, see Security and user experience.

- **Deployment requirements:** You might want to use a policy-based deployment to allow only compliant users to download the published apps. For example, certain apps can require that

© 1997–2025 Citrix Systems, Inc. All rights reserved.

the device is managed or that the device meets a minimum operating system version. You might also want certain apps to be available only to corporate users. Outline such requirements in advance so that you can configure the appropriate deployment rules or actions.

- **Licensing requirements:** Keep a record of the app-related licensing requirements. Your notes can help you manage license usage effectively and decide whether to configure specific features in Citrix Endpoint Management to facilitate licensing. For example, if you deploy a free or paid iOS app, Apple enforces licensing requirements on the app. As a result, users must sign in to their Apple App Store account.

  However, you can register for Apple Volume Purchase to distribute and manage these apps by using Citrix Endpoint Management. Volume Purchase allows users to download the apps without having to sign into their Apple App Store account.

  Some platforms have special licensing requirements to complete before deploying those features.

- **Allow list and block list requirements:** You might identify apps that you do not want users to install or use. Creating a block list defines an out of compliance event. You can then set up policies to trigger when the event occurs. On the other hand, an app might be acceptable for use but can fall under the block list for some reason. In that case, you can add the app to an allow list and indicate that the app is acceptable to use but is not required. Also, keep in mind that the apps pre-installed on new devices can include some commonly used apps that are not part of the operating system. Such apps can conflict with your block list strategy.

Use Case

A healthcare organization plans to deploy Citrix Endpoint Management to serve as a MAM solution for their mobile apps. Mobile apps are delivered to corporate and BYOD users. IT decides to deliver and manage the following apps:

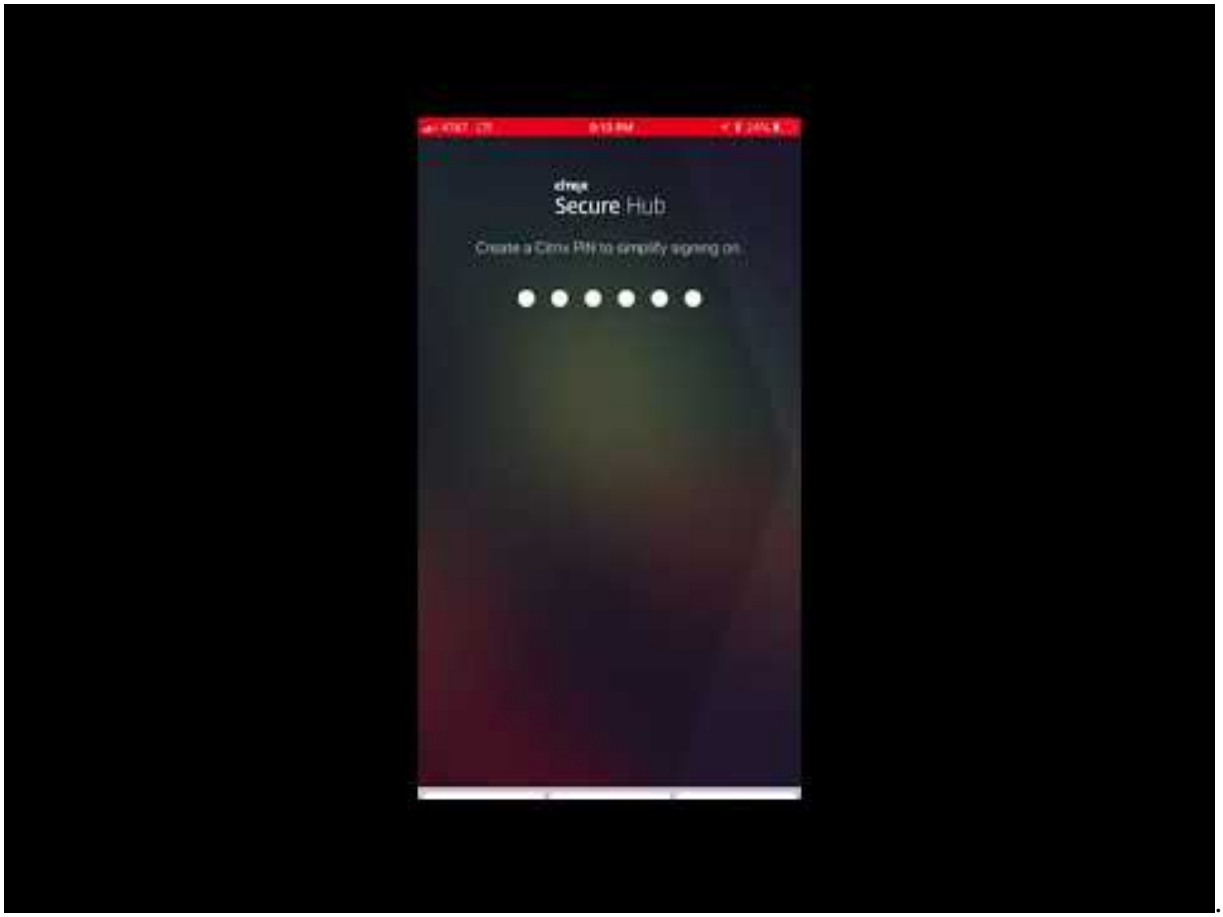
Mobile productivity apps: iOS and Android apps provided by Citrix. For details, see Mobile productivity apps.

Citrix Secure Hub: For customers who onboarded before Citrix Endpoint Management 10.18.14: You push security settings, configurations, and mobile apps to mobile devices by using Citrix Secure Hub. Android and iOS devices enroll in Citrix Endpoint Management through Citrix Secure Hub.

For new customers from Citrix Endpoint Management 10.18.14: Citrix Secure Hub supports the use of the Workspace app store. When opening Citrix Secure Hub, users no longer see the Citrix Secure Hub store. Now, an Add Apps button takes users to the Workspace apps store.

The following is a video that shows an iOS device performing an enrollment to Citrix Endpoint Management using the Citrix Workspace app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Citrix Workspace app: The Citrix Workspace app incorporates existing Citrix Receiver technology, Citrix Secure Hub, and other Citrix Workspace client technologies. Citrix Workspace app provides end users with a unified, contextual experience.

GoToMeeting: An online meeting, desktop sharing, and video conferencing client that lets users meet with other computer users, customers, clients, or colleagues via the Internet in real time.

SalesForce1: Salesforce1 lets users access Salesforce from mobile devices and brings all Chatter, CRM, custom apps, and business processes together in a unified experience for any Salesforce user.

RSA SecurID: Software-based token for two-factor authentication.

EpicCare apps: These apps give healthcare practitioners secure and portable access to patient charts, patient lists, schedules, and messaging.

Haiku: Mobile app for the iPhone and Android phones.

Canto: Mobile app for the iPad

Rover: Mobile apps for iPhone and iPad.

HDX: These apps are delivered via Citrix Virtual Apps in Citrix Workspace.

- **Epic Hyperspace:** Epic client application for electronic health record management.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

ISV:

- **Vocera:** HIPAA compliant voice-over IP and messaging mobile app that extends the benefits of Vocera voice technology anytime, anywhere via iPhone and Android smartphones.

In-house apps:

- **HCMail:** App that helps compose encrypted messages, search address books on internal mail servers, and send the encrypted messages to the contacts using an email client.

In-house web apps:

- **PatientRounding:** Web application used to record patient health information by different departments.
- **Outlook Web Access:** Allows the access of email via a web browser.
- **SharePoint:** Used for organization-wide file and data sharing.

The following table lists the basic information required for MAM configuration.

App Name	App Type	MDX-enabled	iOS	Android
Citrix Secure Mail	Mobile productivity app	No	Yes	Yes
Citrix Secure Web	Mobile productivity app	No	Yes	Yes
Citrix Files	Mobile productivity app	No	Yes	Yes
Citrix Secure Hub	Public App	N/A	Yes	Yes
Citrix Workspace app	Public App	N/A	Yes	Yes
GoToMeeting	Public App	N/A	Yes	Yes
SalesForce1	Public App	N/A	Yes	Yes
RSA SecurID	Public App	N/A	Yes	Yes
Epic Haiku	Public App	N/A	Yes	Yes
Epic Canto	Public App	N/A	Yes	No
Epic Rover	Public App	N/A	Yes	No
Epic Hyperspace	HDX App	N/A	Yes	Yes
Vocera	ISV App	Yes	Yes	Yes
HCMail	In-House App	Yes	Yes	Yes

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App Name	App Type	MDX-enabled	iOS	Android
PatientRounding	Web App	N/A	Yes	Yes
Outlook Web Access	Web App	N/A	Yes	Yes
SharePoint	Web App	N/A	Yes	Yes

The following table lists specific requirements that you can consult configuring MAM policies in Citrix Endpoint Management.

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Proxy Filtering	Licensing	Geofencing	Mobile Apps SDK	Minimum Operating System Version
Citrix Secure Mail	Y	Selectively Allowed	Allowed	Required	N/A	Selectively Required	N/A	Enforced
Citrix Secure Web	Y	Allowed	Allowed	Required	N/A	Not required	N/A	Enforced
Citrix Files	Y	Allowed	Allowed	Required	N/A	Not required	N/A	Enforced
Citrix Secure Hub	Y	N/A	N/A	Not required	Volume Purchase	Not required	N/A	Not enforced
Citrix Workspace app	Y	N/A	N/A	Not required	Volume Purchase	Not required	N/A	Not enforced
GoToMeeting	N	N/A	N/A	Not required	Volume Purchase	Not required	N/A	Not enforced
SalesForce1	N	N/A	N/A	Not required	Volume Purchase	Not required	N/A	Not enforced

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Proxy Filtering	Licensing	Geofencing	Mobile Apps SDK	Minimum Operating System Version
RSA SecurID	N	N/A	N/A	Not required	Volume Purchase	Not required	N/A	Not enforced
Epic Haiku	Y	N/A	N/A	Not required	Volume Purchase	Not required	N/A	Not enforced
Epic Canto	Y	N/A	N/A	Not required	Volume Purchase	Not required	N/A	Not enforced
Epic Rover	Y	N/A	N/A	Not required	Volume Purchase	Not required	N/A	Not enforced
Epic Hyperspace	Y	N/A	N/A	Not required	N/A	Not required	N/A	Not enforced
Vocera	Y	Blocked	Blocked	Required	N/A	Required	Required	Enforced
HCMail	Y	Blocked	Blocked	Required	N/A	Required	Required	Enforced
PatientRounding	Y	N/A	N/A	Required	N/A	Not required	N/A	Not enforced
Outlook Web Access	Y	N/A	N/A	Required	N/A	Not required	N/A	Not enforced
SharePoint	Y	N/A	N/A	Required	N/A	Not required	N/A	Not enforced

User communities

September 6, 2025

Every organization consists of diverse user communities that operate in different functional roles.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

These user communities do different tasks and office functions using various resources that you provide through user mobile devices. Users might work from home or in remote offices using mobile devices that you provide. Or, users might use personal mobile devices, which allow them to access tools that are subject to certain security compliance rules.

With more user communities using mobile devices, Enterprise Mobility Management (EMM) becomes critical to prevent a data leak and to enforce organizational security restrictions. For efficient and more sophisticated Mobile Device Management, you can categorize your user communities. Doing so simplifies the mapping of users to resources and makes sure that the right security policies apply to the right users.

Categorizing user communities can include the use of the following components:

- Active Directory Organizational Units (OUs) and Groups

  Users added to specific Active Directory security groups can receive policies and resources such as apps. Removing users from the Active Directory security groups removes access to previously allowed Citrix Endpoint Management resources.

- Citrix Endpoint Management local users and groups

  For users who don't have an account in Active Directory, you can create the users as local Citrix Endpoint Management users. You can add local users to delivery groups and provision resources to them in the same manner as Active Directory users.

- Citrix Endpoint Management delivery groups

  If many groups of users with different levels of permissions are to consume a single app, you might want to create separate delivery groups. With separate delivery groups, you can deploy two separate versions of the same app. Citrix® recommends creating delivery groups before you create device policies.

- Delivery group and user group mapping

  Delivery group to Active Directory group mappings can be either one-to-one, or one-to-many. Assign base policies and apps to a one-to-many delivery group mapping. Assign function-specific policies and apps to one-to-one delivery group mappings.

- Delivery Group and Resource Mapping of Apps

  Assign specific apps to each delivery group.

- Delivery Group and Resource Mapping of MDM Resources

  Assign apps and specific device management resources to each delivery group. For example, configure a delivery group with any mix of the following: Types of apps (public, HDX™, and so on), specific apps per app type, and resources such as device policies and automated actions.

The following example illustrates how the user communities of a healthcare organization are classified for EMM.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Use case

This example healthcare organization provides technology resources and access to many users, including network and affiliate employees and volunteers. The organization has chosen to roll out the EMM solution to non-executive users only.

You can divide user roles and functions for this organization into subgroups including: clinical, non-clinical, and contractors. A selected set of users receives corporate mobile devices, while others can access limited company resources from their personal devices (BYOD). To enforce the appropriate level of security restrictions and prevent data leaks, the organization decided that corporate IT manages each enrolled device. Also, users can only enroll a single device.

The following sections provide an overview of the roles and functions of each subgroup.

Clinical

- Nurses
- Physicians (Doctors, Surgeons, and so on)
- Specialists (Dieticians, anesthesiologists, radiologists, cardiologists, oncologists, and so on)
- Outside physicians (Non-employee physicians and office workers that work from remote offices)
- Home Health Services (Office and mobile workers doing physician services for patient home visits)
- Research Specialist (Knowledge Workers and Power Users at six Research Institutes doing clinical research to find answers to issues in medicine)
- Education and Training (Nurses, physicians, and specialists in education and training)

Non-clinical

- Shared Services (Office workers doing various back-office functions including: HR, Payroll, Accounts Payable, Supply Chain Service, and so on)
- Physician Services (Office workers doing various healthcare management, administrative services, and business process solutions to providers, including: Administrative Services, Analytics and Business Intelligence, Business Systems, Client Services, Finance, Managed Care Administration, Patient Access Solutions, Revenue Cycle Solutions, and so on)
- Support Services (Office workers doing various non-clinical functions including: Benefits Administration, Clinical Integration, Communications, Compensation and Performance Management, Facility and Property Services, HR Technology Systems, Information Services, Internal Audit and Process Improvement, and so on.)
- Philanthropic Programs (Office and mobile workers that do various functions in support of philanthropic programs)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Contractors

- Manufacturer and vendor partners (Onsite and remotely connected via site-to-site VPN providing various non-clinical support functions)

Based on the preceding information, the organization created the following entities. For more information about delivery groups in Citrix Endpoint Management, see Deploy resources in the Citrix Endpoint Management product documentation.

Active Directory Organizational Units (OUs) and Groups

For OU = Citrix Endpoint Management Resources

- OU = Clinical; Groups =
  - XM-Nurses
  - XM-Physicians
  - XM-Specialists
  - XM-Outside Physicians
  - XM-Home Health Services
  - XM-Research Specialist
  - XM-Education and Training
- OU = Non-Clinical; Groups =
  - XM-Shared Services
  - XM-Physician Services
  - XM-Support Services
  - XM-Philanthropic Programs

Citrix Endpoint Management Local Users and Groups

For Group= Contractors, Users =

- Vendor1
- Vendor2
- Vendor 3
- …Vendor 10

Citrix Endpoint Management Delivery Groups

- Clinical-Nurses

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Clinical-Physicians
- Clinical-Specialists
- Clinical-Outside Physicians
- Clinical-Home Health Services
- Clinical-Research Specialist
- Clinical-Education and Training
- Non-Clinical-Shared Services
- Non-Clinical-Physician Services
- Non-Clinical-Support Services
- Non-Clinical-Philanthropic Programs

Delivery Group and User Group mapping

Active Directory Groups	Citrix Endpoint Management Delivery Groups
XM-Nurses	Clinical-Nurses
XM-Physicians	Clinical-Physicians
XM-Specialists	Clinical-Specialists
XM-Outside Physicians	Clinical-Outside Physicians
XM-Home Health Services	Clinical-Home Health Services
XM-Research Specialist	Clinical-Research Specialist
XM-Education and Training	Clinical-Education and Training
XM-Shared Services	Non-Clinical-Shared Services
XM-Physician Services	Non-Clinical-Physician Services
XM-Support Services	Non-Clinical-Support Services
XM-Philanthropic Programs	Non-Clinical-Philanthropic Programs

Delivery Group and Resource mapping of apps

	Secure Mail	Secure Web	Citrix Files	Workspace app	SalesForce1	RSA SecurID	EpicCare Haiku	Epic Hyper-space
Clinical-Nurses	X	X	X					

© 1997–2025 Citrix Systems, Inc. All rights reserved.

	Secure Mail	Secure Web	Citrix Files	Workspace app	SalesForce1	RSA SecurID	EpicCare Haiku	Epic Hyper-space
Clinical-Physicians								
Clinical-Specialists								
Clinical-Outside Physi-cians	X		X					
Clinical-Home Health Services	X		X					
Clinical-Research Special-ist	X		X					
Clinical-Education and Training							X	X
Non-Clinical-Shared Services							X	X
Non-Clinical-Physician Services							X	X
Non-Clinical-Support Services	X		X				X	X

© 1997–2025 Citrix Systems, Inc. All rights reserved.

	Secure Mail	Secure Web	Citrix Files	Workspace app	SalesForce1	RSA SecurID	EpicCare Haiku	Epic Hyper-space
Non-Clinical-Philanthropic Pro-grams	X		X				X	X
Contractors	X		X	X	X		X	X

Delivery Group and Resource mapping of MDM Resources

	MDM: Passcode policy	MDM: Device Restrictions	MDM: Automated Actions	MDM: Network policy
Clinical-Nurses				X
Clinical-Physicians		X		
Clinical-Specialists				
Clinical-Outside Physicians				
Clinical-Home Health Services				
Clinical-Research Specialist				
Clinical-Education and Training				
Non-Clinical-Shared Services				
Non-Clinical-Physician Services				
Non-Clinical-Support Services				

© 1997–2025 Citrix Systems, Inc. All rights reserved.

	MDM: Passcode policy	MDM: Device Restrictions	MDM: Automated Actions	MDM: Network policy
Non-Clinical-Philanthropic Programs Contractors				X

Notes and considerations

- Citrix Endpoint Management creates a default delivery group named All Users during the initial configuration. If you do not disable this Delivery Group, all Active Directory users have the right to enroll into Citrix Endpoint Management.
- Citrix Endpoint Management synchronizes Active Directory users and groups on demand using a dynamic connection to the LDAP server.
- If a user is part of a group that is not mapped in Citrix Endpoint Management, that user cannot enroll. Likewise, if a user is a member of many groups, Citrix Endpoint Management only categorizes the user as being in the groups mapped to Citrix Endpoint Management.

Email strategy

February 23, 2024

Secure access to email from mobile devices is one of the main drivers behind any organization's mobility management initiative. Deciding on the proper email strategy is often a key component of any Citrix Endpoint Management design. Citrix Endpoint Management offers several options to accommodate different use cases, based on security, user experience, and integration requirements. This article covers the typical design decision process and considerations for choosing the right solution, from client selection to mail traffic flow.

Choosing your email clients

Client selection is generally at the top of the list for the overall email strategy design. You can choose from several clients: Citrix Secure Mail, native mail that is included with a particular mobile platform operating system, or other third-party clients available through the public app stores. Depending on your needs, you can possibly support the user communities with a single (standard) client or you might have to use a combination of clients.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The following table outlines some design considerations for the different client options available:

Topic	Citrix Secure Mail	Native (for example, iOS Mail)	Third-party mail
Configuration	Exchange account profiles configured via an MDX policy.	Exchange account profiles configured via an MDM policy. Android support is limited to: Android Enterprise. All other clients are considered third-party clients.	Generally requires manual configuration by the user.
Security	Secure by design, providing the highest security. Uses MDX policies with added data encryption levels. Citrix Secure Mail is a fully managed app via an MDX policy. Added layer of authentication with Citrix PIN.	Based on vendor/app feature set. Provides higher security. Uses device encryption settings. Relies on device-level authentication for access to the app.	Based on vendor/app feature set. Provides high security.
Integration	Allows interaction with managed (MDX) apps by default. Open web URLs with Citrix Secure Web. Save files to and attach files from Citrix Files. Directly join and dial in to GoToMeeting.	Can only interact with other unmanaged (non-MDX) apps by default.	Can only interact with other unmanaged (non-MDX) apps by default.
Deployment/ Licensing	You can push Citrix Secure Mail through MDM, directly from public app stores. Included with Citrix Endpoint Management Advanced and Enterprise licensing.	Client app included with platform operating system. No additional licensing requirements.	You can push via MDM, as an enterprise app or directly from public app stores. Associated licensing model/costs based on app vendor.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Support	Single vendor support for the client and EMM solution (Citrix). Embedded support contact info in Citrix Secure Hub/app debug logging capabilities. One client to support.	Vendor defined support (Apple/Google). Might have to support different clients based on device platform.	Vendor-defined support. One client to support, assuming that the third-party client is supported on all managed device platforms.

Mail traffic flow and filtering considerations

This section discusses the three main scenarios and design considerations about the flow of mail (ActiveSync) traffic in the context of Citrix Endpoint Management.

Scenario 1: Exposed Exchange

Environments that support external clients commonly have Exchange ActiveSync services exposed to the internet. Mobile ActiveSync clients connect through this externally facing path through a reverse proxy (for example, NetScaler Gateway) or through an Edge Server. This option is required for the use of native or third-party mail clients, making these clients the popular choice for this scenario. Although not a common practice, you can also use the Citrix Secure Mail client in this scenario. By doing so, you benefit from the security features offered by the use of MDX policies and management of the app.

Scenario 2: Tunneled via NetScaler Gateway (micro VPN and STA)

This scenario is the default when using the Citrix Secure Mail client, because of its micro VPN capabilities. In this case, the Citrix Secure Mail client establishes a secure connection to ActiveSync via NetScaler Gateway. In essence, you can consider Citrix Secure Mail to be the client connecting directly to ActiveSync from the internal network. Citrix customers often standardize on Citrix Secure Mail as the mobile ActiveSync client of choice. That decision is part of an initiative to avoid exposing ActiveSync services to the internet on an exposed Exchange Server, as described in the first scenario.

Only apps that are MAM SDK enabled or MDX-wrapped can use the micro VPN function. This scenario does not apply to native clients if you use MDX wrapping. Even though it might be possible to wrap third-party clients with the MDX Toolkit, this practice is not common. The use of device-level VPN

© 1997–2025 Citrix Systems, Inc. All rights reserved.

clients to allow tunneled access for native or third-party clients has proven to be cumbersome and not a feasible solution.

Scenario 3: Cloud-hosted Exchange services

Cloud-hosted Exchange services, such as Microsoft Office 365, are becoming more popular. In the context of Citrix Endpoint Management, this scenario might be treated in the same way as the first scenario, because the ActiveSync service is also exposed to the internet. In this case, cloud service provider requirements dictate client choices. The choices generally include support for most ActiveSync clients, such as Citrix Secure Mail and other native or third-party clients.

Citrix Endpoint Management can add value in three areas for this scenario:

- Clients with MDX policies and app management with Citrix Secure Mail
- Client configuration with the use of an MDM policy on supported native email clients
- ActiveSync filtering options with the use of the Citrix Endpoint Management connector for Exchange ActiveSync

Mail traffic filtering considerations

As with most services exposed to the internet, you must secure the path and provide filtering for authorized access. The Citrix Endpoint Management solution includes two components designed specifically to provide ActiveSync filtering capabilities for native and third-party clients: NetScaler Gateway connector for Exchange ActiveSync and Citrix Endpoint Management connector for Exchange ActiveSync.

NetScaler Gateway connector for Exchange ActiveSync

NetScaler Gateway connector for Exchange ActiveSync provides ActiveSync filtering at the perimeter, by using NetScaler Gateway as a proxy for ActiveSync traffic. As a result, the filtering component sits in the path of mail traffic flow, intercepting mail as it enters or leaves the environment. The connector for Exchange ActiveSync acts an intermediary between NetScaler Gateway and Citrix Endpoint Management. When a device communicates with Exchange through the ActiveSync virtual server on the NetScaler Gateway, NetScaler Gateway does an HTTP callout to the connector for the Exchange ActiveSync service. That service then checks the device status with Citrix Endpoint Management. Based on the status of the device, the connector for Exchange ActiveSync replies to NetScaler Gateway to either allow or deny the connection. You might also configure static rules to filter access based on user, agent, and device type or ID.

This setup allows Exchange ActiveSync services to be exposed to the internet with an added layer of security to prevent unauthorized access. Design considerations include the following:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Windows Server:** The connector for the Exchange ActiveSync component requires a Windows Server.
- **Filtering rule set:** The connector for Exchange ActiveSync is designed for filtering based on device state and information, rather than user information. Although you might configure static rules to filter by user ID, no options exist for filtering based on Active Directory group membership, for example. If there is a requirement for Active Directory group filtering, you can use the Citrix Endpoint Management connector for Exchange ActiveSync instead.
- **NetScaler Gateway scalability:** Given the requirement to proxy ActiveSync traffic via NetScaler Gateway: Proper sizing of the NetScaler Gateway instance is critical to support the added workload of all ActiveSync SSL connections.
- **NetScaler Gateway Integrated Caching:** The connector for the Exchange ActiveSync configuration on the NetScaler Gateway uses the Integrated Caching function to cache responses from the connector. Becuase of that configuration, NetScaler Gateway doesn't need to issue a request to the connector for every ActiveSync transaction in a given session. That configuration is also critical for adequate performance and scale. Integrated Caching is available with the NetScaler Gateway Platinum Edition.
- **Custom filtering policies:** You might have to create custom NetScaler Gateway policies to restrict certain ActiveSync clients outside of the standard native mobile clients. This configuration requires knowledge on ActiveSync HTTP requests and NetScaler Gateway responder policy creation.
- **Citrix Secure Mail clients:** Citrix Secure Mail has micro VPN capabilities which eliminate the need for filtering at the perimeter. The Citrix Secure Mail client might generally be treated as an internal (trusted) ActiveSync client when connected through the NetScaler Gateway. If support for both native and third-party (with the connector for Exchange ActiveSync) and Citrix Secure Mail clients is required: Citrix recommends that Citrix Secure Mail traffic does not flow via the NetScaler Gateway virtual server used for the connector. You can accomplish this traffic flow via DNS and keep the connector policy from affecting Citrix Secure Mail clients.

For a diagram of the NetScaler Gateway connector for Exchange ActiveSync in an Citrix Endpoint Management deployment, see Architecture.

Citrix Endpoint Management connector for Exchange ActiveSync

Citrix Endpoint Management connector for Exchange ActiveSync is an Citrix Endpoint Management component that provides ActiveSync filtering at the Exchange service level. As a result, filtering only occurs once the mail reaches the exchange service, rather than when it enters the Citrix Endpoint Management environment. Mail Manager uses PowerShell to query Exchange ActiveSync for device partnership information and control access through device quarantine actions. Those actions take devices in and out of quarantine based on the Citrix Endpoint Management connector for Exchange ActiveSync rule criteria.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Similar to NetScaler Gateway connector for Exchange ActiveSync, the connector for Exchange ActiveSync checks the device status with Citrix Endpoint Management to filter access based on device compliance. You might also configure static rules to filter access based on device type or ID, agent version, and Active Directory group membership.

This solution does not require the use of NetScaler Gateway. You can deploy the connector for Exchange ActiveSync without changes routing for the existing ActiveSync traffic. Design considerations include:

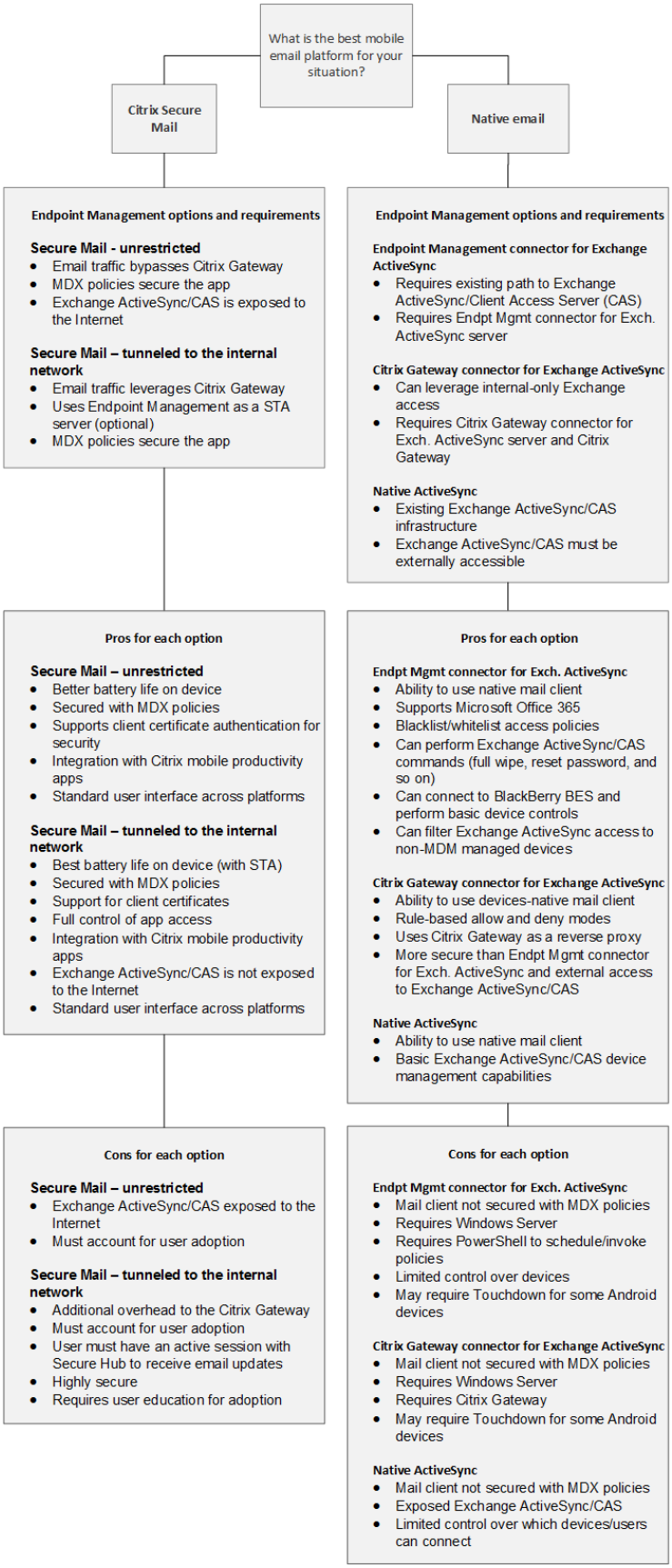
- **Windows Server:** The connector for Exchange ActiveSync requires you to deploy Windows Server.
- **Filtering rule set:** Just like the NetScaler Gateway connector for Exchange ActiveSync, the connector for Exchange ActiveSync includes filtering rules to evaluate device state. Also, the connector for Exchange ActiveSync also supports static rules to filter based on Active Directory group membership.
- **Exchange integration:** The connector for Exchange ActiveSync requires direct access to the Exchange Client Access Server (CAS) hosting the ActiveSync role and control over device quarantine actions. This requirement might present a challenge depending on the environment architecture and security posture. It is critical that you evaluate this technical requirement up front.
- **Other ActiveSync clients:** Because the connector for Exchange ActiveSync is filtering at the ActiveSync service level, consider other ActiveSync clients outside the Citrix Endpoint Management environment. You can configure the connector for Exchange ActiveSync static rules to avoid unintended impact to other ActiveSync clients.
- **Extended Exchange functions:** Through direct integration with Exchange ActiveSync, the connector for Exchange ActiveSync provides the ability for Citrix Endpoint Management to do an Exchange ActiveSync wipe on a mobile device. The connector for Exchange ActiveSync also allows Citrix Endpoint Management to access information about Blackberry devices and to do other control operations.

For a diagram of the Citrix Endpoint Management connector for Exchange ActiveSync in an Citrix Endpoint Management deployment, see Architecture.

Email platform decision tree

The following figure helps you distinguish the pros and cons between using native email or Citrix Secure Mail solutions in your Citrix Endpoint Management deployment. Each choice allows for associated Citrix Endpoint Management options and requirements to enable server, network, and database access. The pros and cons include details on security, policy, and user interface considerations.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management integration

September 6, 2025

This article covers what to consider when planning how Citrix Endpoint Management is to integrate with your existing network and solutions. For example, if you're already using NetScaler Gateway for Citrix Virtual Apps and Desktops:

- Do you want to use the existing NetScaler Gateway instance or a new, dedicated instance?
- Do you want to integrate with Citrix Endpoint Management the HDX apps that are published using StoreFront?
- Do you plan to use Citrix Files with Citrix Endpoint Management?
- Do you have a Network Access Control solution that you want to integrate into Citrix Endpoint Management?

NetScaler Gateway

NetScaler Gateway is required for Citrix Endpoint Management. NetScaler Gateway provides a micro VPN path for access to all corporate resources and provides strong multifactor authentication support.

You can use existing NetScaler Gateway instances or set up new ones for Citrix Endpoint Management. The following sections note the advantages and disadvantages of using existing or new, dedicated NetScaler Gateway instances.

Shared NetScaler Gateway MPX with a NetScaler Gateway VIP created for Citrix Endpoint Management

Advantages:

- Uses a common NetScaler Gateway instance for all Citrix remote connections: Citrix Virtual Apps, full VPN, and clientless VPN.
- Uses the existing NetScaler Gateway configurations, such as for certificate authentication and for accessing services like DNS, LDAP, and NTP.
- Uses a single NetScaler Gateway platform license.

Disadvantages:

- It is more difficult to plan for scale when you handle two different use cases on the same NetScaler Gateway.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Sometimes you need a specific NetScaler Gateway version for a Citrix Virtual Apps use case. That same version might have known issues for Citrix Endpoint Management. Or Citrix Endpoint Management might have known issues for the NetScaler Gateway version.
- If a NetScaler Gateway exists, you cannot run the NetScaler for XenMobile wizard a second time to create the NetScaler Gateway configuration for Citrix Endpoint Management.
- Except when Platinum licenses are used for NetScaler Gateway 11.1 or later: User access licenses installed on NetScaler Gateway and required for VPN connectivity are pooled. Because those licenses are available to all NetScaler Gateway virtual servers, services other than Citrix Endpoint Management can potentially consume them.

Dedicated NetScaler Gateway VPX/MPX instance

Advantages:

Citrix recommends using a dedicated instance of NetScaler Gateway.

- Easier to plan for scale and separate Citrix Endpoint Management traffic from a NetScaler Gateway instance that might already be resource constrained.
- Avoids issues when Citrix Endpoint Management and Citrix Virtual Apps need different NetScaler Gateway software versions. The recommendation generally is to use the latest compatible NetScaler Gateway version and build for Citrix Endpoint Management.
- Allows Citrix Endpoint Management configuration of NetScaler Gateway through the built-in NetScaler for XenMobile wizard.
- Virtual and physical separation of services.

Disadvantages:

- Requires setup of extra services on NetScaler Gateway to support Citrix Endpoint Management configuration.
- Requires another NetScaler Gateway platform license. License each NetScaler Gateway instance for NetScaler Gateway.

For information about what to consider when integrating NetScaler Gateway and Citrix ADC for Citrix Endpoint Management management modes, see Integrating with NetScaler Gateway and Citrix ADC.

StoreFront

If you have a Citrix Virtual Apps and Desktops environment, you can integrate HDX applications with Citrix Endpoint Management using StoreFront. When you integrate HDX apps with Citrix Endpoint Management:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- The apps are available to users who are enrolled with Citrix Endpoint Management.
- The apps display in the app store along with other mobile apps.
- Citrix Endpoint Management uses Citrix Receiver on StoreFront.
- When the Citrix Workspace app is installed on a device, HDX apps start using that app.

StoreFront has a limitation of one service site per StoreFront instance. Suppose that you have many stores and want to segment it from other production usage. In that case, Citrix generally recommends that you consider a new StoreFront Instance and services site for Citrix Endpoint Management.

Considerations include:

- Are there any different authentication requirements for StoreFront? The StoreFront services site requires Active Directory credentials for logon. Customers only using certificate-based authentication cannot enumerate applications through Citrix Endpoint Management using the same NetScaler Gateway.
- Use the same store or create a store?
- Use the same or a different StoreFront server?

The following sections note the advantages and disadvantages of using separate or combined storefronts for Citrix Workspace and Citrix mobile productivity apps.

Integrate your existing StoreFront instance with Citrix Endpoint Management

Advantages:

- Same store: No additional configuration of StoreFront is required for Citrix Endpoint Management, assuming that you use the same NetScaler Gateway VIP for HDX access. Suppose that you choose to use the same store and want to direct Citrix Workspace access to a new NetScaler Gateway VIP. In that case, add the appropriate NetScaler Gateway configuration to StoreFront.
- Same StoreFront server: Uses the existing StoreFront installation and configuration.

Disadvantages:

- Same store: Any reconfiguration of StoreFront to support Citrix Virtual Apps and Desktops workloads might adversely affect Citrix Endpoint Management.
- Same StoreFront server: In large environments, consider the additional load from Citrix Endpoint Management usage of Citrix Receiver for app enumeration and start-up.

Use a new, dedicated StoreFront instance for integration with Citrix Endpoint Management

Advantages:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- New store: Any configuration changes of the StoreFront store for Citrix Endpoint Management don't affect existing Virtual Apps and Desktops workloads.
- New StoreFront server: Server configuration changes don't affect Virtual Apps and Desktops workflows. Also, load outside of Citrix Endpoint Management usage of Citrix Receiver for app enumeration and launch don't affect scalability.

Disadvantages:

- New store: StoreFront store configuration.
- New StoreFront server: Requires a new StoreFront installation and configuration.

For more information, see Citrix Virtual Apps and Desktops through the app store.

ShareFile and Citrix Files

> **Disclaimer:**
>
> This feature will be deprecated if ShareFile (now Progress) discontinues support.

ShareFile enables you to easily and securely exchange documents, send large documents by email, and securely handle document transfers to third parties. The Citrix Files app enables users to access and sync all of their data from any device. With Citrix Files, users can securely share data with people both inside and outside the organization.

Citrix Endpoint Management provides Citrix Files with:

- Single sign-on authentication for mobile productivity app users.
- Active Directory-based user account provisioning.
- Comprehensive access control policies.

Mobile users can benefit from the full Enterprise account feature set.

Alternatively, you can configure Citrix Endpoint Management to integrate only with storage zone connectors. Through storage zone connectors, Citrix Files provides access to:

- Documents and folders
- Network file shares
- In SharePoint sites: Site collections and document libraries.

Connected file shares can include the same network home drives used in Citrix Virtual Apps and Desktops environments. You use the Citrix Endpoint Management console to configure the integration with Enterprise accounts or storage zone connectors. For more information, see Citrix Files for Citrix Endpoint Management.

The following sections note the questions to ask when making design decisions for Citrix Files.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Integrate with Citrix Files or only storage zone connectors

Questions to ask:

- Do you want to store data in Citrix-managed storage zones?
- Do you want to provide users with file sharing and sync capabilities?
- Do you want to enable users to access files on the Citrix Files website? Or to access Office 365 content and Personal Cloud connectors from mobile devices?

Design decision:

- If the answer to any of those questions is "yes,"integrate with an Enterprise account.
- An integration with only storage zone connectors gives iOS users secure mobile access to existing on-premises storage repositories, such as SharePoint sites and network file shares. In this configuration, you don't set up a Citrix Files subdomain, provision users to Citrix Files, or host Citrix Files data. Using storage zone connectors with Citrix Endpoint Management follows security restrictions against leaking user information outside of the corporate network.

Storage zones controller server location

Questions to ask:

- Do you require on-premises storage or features such as storage zone connectors?
- If using on-premises features of Citrix Files, where will the storage zones controllers sit in the network?

Design decision:

- Determine whether to locate the storage zones controller servers in the Citrix Files cloud, in your on-premises single-tenant storage system, or in supported third-party cloud storage.
- Storage zones controllers require some internet access to communicate with the Citrix Files Control Plane. You can connect in several ways, including direct access or NAT/PAT configurations.

Storage zone connectors

Questions to ask:

- What are the CIFS share paths?
- What are the SharePoint URLs?

Design decision:

- Determine if on-premises storage zones controllers are required to access those locations.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Because of storage zone connector communication with internal resources such as file repositories, CIFS shares, and SharePoint: Citrix recommends that the storage zones controllers are in the internal network behind DMZ firewalls and fronted by NetScaler Gateway.

SAML integration with Citrix Endpoint Management

Questions to ask:

- Is Active Directory authentication required for Citrix Files?
- Does first time use of the Citrix Files app for Citrix Endpoint Management require SSO?
- Is there a standard IdP in your current environment?
- How many domains are required to use SAML?
- Are there many email aliases for Active Directory users?
- Are there any Active Directory domain migrations in progress or scheduled soon?

Design decision:

You might choose to use SAML as the authentication mechanism for Citrix Files. The authentication options are:

- Use the Citrix Endpoint Management server as the Identity Provider (IdP) for SAML

  This option can provide excellent user experience, automate Citrix Files account creation, and enable mobile app SSO features.

  The Citrix Endpoint Management server is enhanced for this process: It does not require the synchronization of the Active Directory.

  Use the Citrix Files User Management Tool for user provisioning.

- Use a supported third-party vendor as the IdP for SAML

  If you have an existing and supported IdP and don't require mobile app SSO capabilities, this option might be the best fit for you. This option also requires the use of the Citrix Files User Management Tool for account provisioning.

  Using third-party IdP solutions such as ADFS might also provide SSO capabilities on the Windows client side. Be sure to evaluate use cases before choosing your Citrix Files SAML IdP.

- Or, to satisfy both use cases, see ShareFile single sign-on configuration guide for dual identity providers.

Mobile apps

Questions to ask:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Which Citrix Files mobile app do you plan to use (public, MDM, MDX)?

Design decision:

- You distribute Citrix mobile productivity apps from the Apple App Store and Google Play Store. With that public app store distribution, you get wrapped apps from the Citrix downloads page.
- If your security requirements are low and you don't require containerization, the public Citrix Files app might not be suitable.
- For more information, see Apps and Citrix Files for Citrix Endpoint Management.

Security, policies, and access control

Questions to ask:

- What restrictions do you require for desktop, web, and mobile users?
- What standard access control settings do you want for users?
- What file retention policy do you plan to use?

Design decision:

- Citrix Files lets you manage employee permissions. For information, see Employee Permissions.
- Some Citrix Files device security settings and MDX policies control the same features. In those cases, the Citrix Endpoint Management policies take precedence, followed by the Citrix Files device security settings. Examples: If you disable external apps in Citrix Files, but enable them in Citrix Endpoint Management, the external apps get disabled in Citrix Files. You can configure the apps so that Citrix Endpoint Management doesn't require a PIN/passcode, but the Citrix Files app requires a PIN/passcode.

Standard versus restricted storage zones

Questions to ask:

- Do you require restricted storage zones?

Design decision:

- A standard storage zone is intended for non-sensitive data and enables employees to share data with non-employees. This option supports workflows that involve sharing data outside of your domain.
- A restricted storage zone protects sensitive data: Only authenticated domain users can access the data stored in the zone.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Access control

Enterprises can manage mobile devices inside and outside of networks. Enterprise Mobility Management solutions such as Citrix Endpoint Management are great at providing security and controls for mobile devices, independent of location. However, when you combine them with a Network Access Control (NAC) solution, you can add QoS and more fine-grained control to devices that are internal to your network. That combination enables you to extend the Citrix Endpoint Management device security assessment through your NAC solution. Your NAC solution then can use the Citrix Endpoint Management security assessment to facilitate and handle authentication decisions.

You can use any of these solutions to enforce NAC policies:

- NetScaler Gateway
- ForeScout

Citrix doesn't guarantee integration for other NAC solutions.

Advantages of a NAC solution integration with Citrix Endpoint Management include the following:

- Better security, compliance, and control for all endpoints on an enterprise network.
- A NAC solution can:
  - Detect devices at the instant they try to connect to your network.
  - Query Citrix Endpoint Management for device attributes.
  - Use that device information to determine whether to allow, block, limit, or redirect those devices. Those decisions depend on the security policies that you choose to enforce.
- A NAC solution provides IT administrators with a view of unmanaged and non-compliant devices.

For a description of the NAC compliance filters supported by Citrix Endpoint Management and a configuration overview, see Network Access Control.

Integrating with NetScaler Gateway and Citrix ADC

September 6, 2025

When integrated with Citrix Endpoint Management, NetScaler Gateway provides an authentication mechanism for remote device access to the internal network for MAM devices. The integration enables Citrix mobile productivity apps to connect to corporate servers in the intranet through a micro VPN. Citrix Endpoint Management creates a micro VPN from the apps on the device to NetScaler Gateway. NetScaler Gateway provides a micro VPN path for access to all corporate resources and provides strong multifactor authentication support.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

When a user opts out of MDM enrollment, devices enroll using the NetScaler Gateway FQDN.

Citrix Cloud Operations manages Citrix ADC load balancing.

Design Decisions

The following sections summarize the many design decisions to consider when planning a NetScaler Gateway integration with Citrix Endpoint Management.

Certificates

Decision details:

- Do you require a higher degree of security for enrollment and access to the Citrix Endpoint Management environment?
- Is LDAP not an option?

Design guidance:

The default configuration for Citrix Endpoint Management is user name and password authentication. To add another layer of security for enrollment and access to the Citrix Endpoint Management environment, consider using certificate-based authentication. You can use certificates with LDAP for two-factor authentication, providing a higher degree of security without needing an RSA server.

If you don't allow LDAP and use smart cards or similar methods, configuring certificates allows you to represent a smart card to Citrix Endpoint Management. Users then enroll using a unique PIN that Citrix Endpoint Management generates for them. After a user has access, Citrix Endpoint Management creates and deploys the certificate later used to authenticate to the Citrix Endpoint Management environment.

Citrix Endpoint Management supports Certificate Revocation List (CRL) only for a third party Certificate Authority. If you have a Microsoft CA configured, Citrix Endpoint Management uses NetScaler Gateway to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the NetScaler Gateway Certificate Revocation List (CRL) setting **Enable CRL Auto Refresh**. This step makes sure that the user of a device enrolled in MAM only can't authenticate using an existing certificate on the device. Citrix Endpoint Management reissues a new certificate, because it doesn't restrict a user from generating a user certificate if one is revoked. This setting increases the security of PKI entities when the CRL checks for expired PKI entities.

Dedicated or shared NetScaler Gateway VIPs

Decision details:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Do you currently use NetScaler Gateway for Citrix Virtual Apps and Desktops?
- Will Citrix Endpoint Management use the same NetScaler Gateway as Citrix Virtual Apps and Desktops?
- What are the authentication requirements for both traffic flows?

Design guidance:

When your Citrix environment includes Citrix Endpoint Management, plus Virtual Apps and Desktops, you can use the same NetScaler Gateway virtual server for both. Because of the potential versioning conflicts and environment isolation, a dedicated NetScaler Gateway is recommended for each Citrix Endpoint Management environment.

If you use LDAP authentication, Citrix Secure Hub can authenticate to the same NetScaler Gateway with no issues. If you use certificate-based authentication, Citrix Endpoint Management pushes a certificate in the MDX container and Citrix Secure Hub uses the certificate to authenticate with NetScaler Gateway.

You might consider this work around, which allows you to use the same FQDN for two NetScaler Gateway VIPs. You can create two NetScaler Gateway VIPs with the same IP address. The one for Citrix Secure Hub uses the standard 443 port and the one for Citrix Virtual Apps and Desktops (which deploys the Citrix Workspace app) uses port 444. Then, one FQDN resolves to the same IP address. For this work around, you might need to configure StoreFront to return an ICA file for port 444, instead of the default, port 443. This workaround doesn't require users to enter a port number.

NetScaler Gateway time-outs

Decision details:

- How do you want to configure the NetScaler Gateway time-outs for Citrix Endpoint Management traffic?

Design guidance:

NetScaler Gateway includes the settings Session time-out and Forced time-out. For details, see Recommended configurations. Keep in mind that there are different time-out values for background services, NetScaler Gateway, and for accessing applications while offline.

Enrollment FQDN

> **Important:**
>
> To change the enrollment FQDN requires a new SQL Server database and an Citrix Endpoint Management server rebuild.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Secure Web traffic

Decision details:

- Will you restrict Citrix Secure Web to internal web browsing only?
- Will you enable Citrix Secure Web for both internal and external web browsing?

Design guidance:

If you plan to use Citrix Secure Web for internal web browsing only, the NetScaler Gateway configuration is straightforward. However, if Citrix Secure Web can't reach all internal sites by default, you might need to configure firewalls and proxy servers.

If you plan to use Citrix Secure Web for both internal and external browsing, you must enable the SNIP to have outbound internet access. IT generally views enrolled devices (using the MDX container) as an extension of the corporate network. Thus, IT typically wants Citrix Secure Web connections to come back to NetScaler Gateway, go through a proxy server, and then go out to the Internet. By default, Citrix Secure Web access tunnels to the internal network. Citrix Secure Web uses a per-application VPN tunnel back to the internal network for all network access and NetScaler Gateway uses split tunnel settings.

For a discussion of Citrix Secure Web connections, see Configuring User Connections.

Push Notifications for Citrix Secure Mail

Decision details:

- Will you use push notifications?

Design guidance for iOS:

If your NetScaler Gateway configuration includes Secure Ticket Authority (STA) and split tunneling is off: NetScaler Gateway must allow traffic from Citrix Secure Mail to the Citrix listener service URLs. Those URLs are specified in push notifications for Citrix Secure Mail for iOS.

Design guidance for Android:

Use Firebase Cloud Messaging (FCM) to control how and when Android devices need to connect to Citrix Endpoint Management. With FCM configured, any security action or deploy command triggers a push notification to Citrix Secure Hub to prompt the user to reconnect to the Citrix Endpoint Management server.

HDX™ STAs

Decision details:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- What STAs to use if you integrate HDX application access?

Design guidance:

HDX STAs must match the STAs in StoreFront and must be valid for the Virtual Apps and Desktops site.

Citrix Files and ShareFile

Decision details:

- Will you use a storage zones controller in the environment?
- What Citrix Files VIP URL will you use?

Design guidance:

If you include a storage zones controller in your environment, make sure that you correctly configure the following:

- Citrix Files Content Switch VIP (used by the Citrix Files Control Plane to communicate with the storage zones controller servers)
- Citrix Files Load Balancing VIPs
- All required policies and profiles

For information, see the documentation for Storage zones controller.

SAML IdP

Decision detail:

- If SAML is required for Citrix Files, do you want to use Citrix Endpoint Management as the SAML IdP?

Design guidance:

The recommended best practice is to integrate Citrix Files with Citrix Endpoint Management, a simpler alternative to configuring SAML-based federation. Citrix Endpoint Management provides Citrix Files with:

- Single sign-on (SSO) authentication of Citrix mobile productivity apps users
- User account provisioning based on Active Directory
- Comprehensive access control policies.

The Citrix Endpoint Management console enables you to do Citrix Files configuration and to monitor service levels and license usage.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

There are two types of Citrix Files clients: Citrix Files for Citrix Endpoint Management (also known as wrapped Citrix Files) and Citrix Files mobile clients (also known as unwrapped Citrix Files). To understand the differences, see How Citrix Files for Citrix Endpoint Management Clients differ from Citrix Files mobile clients.

You can configure Citrix Endpoint Management and Citrix Files to use SAML to provide SSO access to:

- Citrix Files apps that are MAM SDK enabled or wrapped by using the MDX Toolkit
- Non-wrapped Citrix Files clients, such as the website, Outlook plug-in, or sync clients

If you want to use Citrix Endpoint Management as the SAML IdP for Citrix Files, make sure that the proper configurations are in place. For details, see SAML for SSO with Citrix Files.

ShareConnect direct connections

Decision detail:

- Will users access a host computer from a computer or mobile device running ShareConnect using direct connections?

Design guidance:

ShareConnect enables users to connect securely to their computers through iPads, Android tablets, and Android phones to access their files and applications. For direct connections, Citrix Endpoint Management uses NetScaler Gateway to provide secure access to resources outside of the local network. For configuration details, see ShareConnect.

Enrollment FQDN for each management mode

Management mode	Enrollment FQDN
MDM+MAM with mandatory MDM enrollment	Citrix Endpoint Management server FQDN
MDM+MAM with optional MDM enrollment	Citrix Endpoint Management server FQDN
MAM-only	Citrix Endpoint Management server FQDN

Deployment Summary

If you have many Citrix Endpoint Management instances, such as for test, development, and production environments, you must configure NetScaler Gateway for the additional environments manually.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

When you have a working environment, take note of the settings before trying to configure NetScaler Gateway manually for Citrix Endpoint Management.

A key decision is whether to use HTTPS or HTTP for communication to the Citrix Endpoint Management server. HTTPS provides secure back-end communication, as traffic between NetScaler Gateway and Citrix Endpoint Management is encrypted. The re-encryption impacts Citrix Endpoint Management server performance. HTTP provides better Citrix Endpoint Management server performance. Traffic between NetScaler Gateway and Citrix Endpoint Management is not encrypted. The following tables show the HTTP and HTTPS port requirements for NetScaler Gateway and Citrix Endpoint Management.

HTTPS

Citrix typically recommends SSL Bridge for NetScaler Gateway MDM virtual server configurations. For NetScaler Gateway SSL Offload use with MDM virtual servers, Citrix Endpoint Management supports only port 80 as the back-end service.

Management mode	NetScaler Gateway load balancing method	SSL re-encryption	Citrix Endpoint Management server port
MAM	SSL Offload	Enabled	8443
MDM+MAM	MDM: SSL Bridge	N/A	443, 8443
MDM+MAM	MAM: SSL Offload	Enabled	8443

HTTP

Management mode	NetScaler Gateway load balancing method	SSL re-encryption	Citrix Endpoint Management server port
MAM	SSL Offload	Enabled	8443
MDM+MAM	MDM: SSL Offload	Not supported	80
MDM+MAM	MAM: SSL Offload	Enabled	8443

For diagrams of NetScaler Gateway in Citrix Endpoint Management deployments, see Architecture.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

SSO and proxy considerations for MDX apps

February 23, 2024

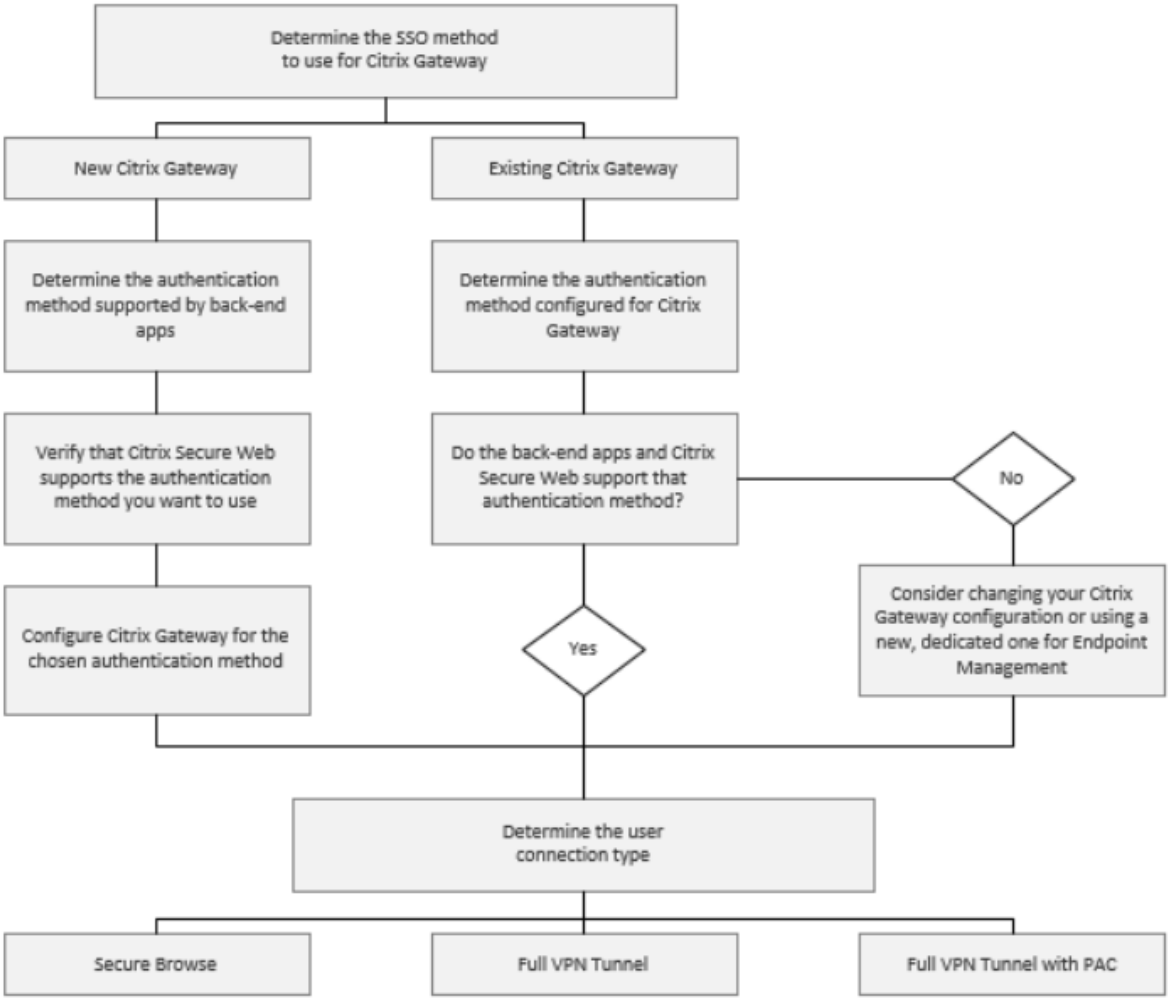
Citrix Endpoint Management integration with NetScaler Gateway enables you to provide users with single sign-on (SSO) to all back end HTTP/HTTPS resources. Depending on your SSO authentication requirements, configure user connections for an MDX app to use Secure Browse (Tunneled - Web SSO), which is a type of clientless VPN.

> **Important:**
>
> Citrix deprecated support for a full VPN tunnel and a Proxy Automatic Configuration (PAC) file with a full VPN tunnel deployment for iOS and Android devices. For more information, see Deprecation.

If NetScaler Gateway isn't the best way to provide SSO in your environment, you can set up an MDX app with policy-based local password caching. This article explores the various SSO and proxy options, with a focus on Citrix Secure Web. The concepts apply to other MDX apps.

The following flow chart summarizes the decision flow for SSO and user connections.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- Recommended
- Provides SSO through Citrix Gateway to HTTP and HTTPS sites.
- Citrix Secure Web does not prompt for credentials.

- Required if end-to-end connections from Citrix Secure Web to an app server is required, such as for certificate authentication to an internal web server.
- Provides SSO through Citrix Gateway to HTTP and HTTPS sites.
- Citrix Secure Web does not prompt for credentials.

Applies only to Citrix Secure Web on iOS and Android devices.

For HTTP sites:

- Provides SSO through Citrix Gateway.
- Citrix Secure Web does not prompt for credentials.

For HTTPS sites:

- Does not support SSO through Citrix Gateway.
- Use Citrix Secure Web MDX policy **Enable web password caching** instead. Citrix Secure Web will prompt for credentials on first access of a website or after a password changes.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway authentication methods

This section provides general information about the authentication methods supported by NetScaler Gateway.

SAML authentication

When you configure NetScaler Gateway for Security Assertion Markup Language (SAML), users can connect to web apps that support the SAML protocol for single sign-on. NetScaler Gateway supports the identity provider (IdP) single sign-on for SAML web apps.

Required configuration:

- Configure SAML SSO in the NetScaler Gateway Traffic profile.
- Configure the SAML IdP for the requested service.

NTLM authentication

If SSO to web apps is enabled in the session profile, NetScaler Gateway does NTLM authentication automatically.

Required configuration:

- Enable SSO in the NetScaler Gateway Session or Traffic profile.

Kerberos impersonation

Citrix Endpoint Management supports Kerberos for Citrix Secure Web only. When you configure NetScaler Gateway for Kerberos SSO, NetScaler Gateway uses impersonation when a user password is available to NetScaler Gateway. Impersonation means that NetScaler Gateway uses user credentials to get the ticket required to gain access to services, such as Citrix Secure Web.

Required configuration:

- Configure the NetScaler Gateway `Worx` Session policy to allow it to identify the Kerberos Realm from your connection.
- Configure a Kerberos Constrained Delegation (KCD) account on NetScaler Gateway. Configure that account with no password and bind it to a traffic policy on your Citrix Endpoint Management gateway.
- For those and other configuration details, see the Citrix blog: WorxWeb and Kerberos Impersonation SSO.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Kerberos Constrained Delegation

Citrix Endpoint Management supports Kerberos for Citrix Secure Web only. When you configure NetScaler Gateway for Kerberos SSO, NetScaler Gateway uses constrained delegation when a user password is not available to NetScaler Gateway.

With constrained delegation, NetScaler Gateway uses a specified administrator account to get tickets for users and services.

Required configuration:

- Configure a KCD account in the Active Directory with the required permissions and a KDC account on NetScaler Gateway.
- Enable SSO in the NetScaler Gateway Traffic profile.
- Configure the back-end website for Kerberos authentication.

Form Fill Authentication

When you configure NetScaler Gateway for Form-based single sign-on, users can log on one time to access all protected apps in your network. This authentication method applies to apps that use the Tunneled - Web SSO mode.

Required configuration:

- Configure a Form-based SSO in the NetScaler Gateway Traffic profile.

Digest HTTP authentication

If you enable SSO to web apps in the session profile, NetScaler Gateway does digest HTTP authentication automatically. This authentication method applies to apps that use Tunneled - Web SSO mode.

Required configuration:

- Enable SSO in the NetScaler Gateway Session or Traffic profile.

Basic HTTP authentication

If you enable SSO to web apps in the session profile, NetScaler Gateway does basic HTTP authentication automatically. This authentication method applies to apps that use Tunneled - Web SSO mode.

Required configuration:

- Enable SSO in the NetScaler Gateway Session or Traffic profile.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Secure Tunneled - Web SSO

This section describes the **Tunneled - Web SSO** user connection types for Citrix Secure Web.

Connections that tunnel to the internal network can use a variation of a clientless VPN, referred to as Tunneled - Web SSO. Tunneled - Web SSO is the default configuration specified for the Citrix Secure Web **Preferred VPN mode** policy. Citrix recommends Tunneled - Web SSO for connections that require single sign-on (SSO).

In Tunneled - Web SSO mode, NetScaler Gateway breaks the HTTPS session into two parts:

- From the client to NetScaler Gateway
- From NetScaler Gateway to the back-end resource server.

In this manner, NetScaler Gateway has full visibility into all transactions between the client and server, enabling it to provide SSO.

You can also configure proxy servers for Citrix Secure Web when used in Tunneled - Web SSO mode. For details, see the blog Citrix Endpoint Management WorxWeb Traffic Through Proxy Server in Secure Browse Mode.

> **Note:**
>
> Citrix announced the deprecation of the Full VPN tunnel with PAC. See Deprecation.

Citrix Endpoint Management supports proxy authentication provided by NetScaler Gateway. A PAC file has rules that define how web browsers select a proxy to access a given URL. PAC file rules can specify handling for both internal and external sites. Citrix Secure Web parses the PAC file rules and sends the proxy server information to NetScaler Gateway. NetScaler Gateway is unaware of the PAC file or proxy server.

For authentication to HTTPS websites: The Citrix Secure Web MDX policy **Enable web password caching** enables Citrix Secure Web to authenticate and provide SSO to the proxy server through MDX.

NetScaler Gateway Split Tunneling

When planning your SSO and proxy configuration, you must also decide whether to use NetScaler Gateway split tunneling. Citrix recommends that you use NetScaler Gateway split tunneling only if needed. This section provides a high-level look at how split tunneling works: NetScaler Gateway determines the traffic path based on its routing table. When NetScaler Gateway split tunneling is on, Citrix Secure Hub distinguishes internal (protected) network traffic from Internet traffic. Citrix Secure Hub makes that determination based on the DNS suffix and Intranet applications. Citrix Secure Hub then tunnels only the internal network traffic through the VPN tunnel. When NetScaler Gateway split tunneling is off, all traffic goes through the VPN tunnel.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

If you prefer to monitor all the traffic because of security considerations, disable NetScaler Gateway split tunneling. As a result, all traffic goes through the VPN tunnel.

NetScaler Gateway also has a micro VPN reverse split tunnel mode. This configuration supports an exclusion list of IP addresses that aren't tunneled to the NetScaler Gateway. Instead, those addresses are sent by using the device internet connection. For more information about reverse split tunneling, see the NetScaler Gateway documentation.

Citrix Endpoint Management includes a **Reverse split tunnel exclusion list**. To prevent certain websites from tunneling through NetScaler Gateway: Add a comma-separated list of fully qualified domain names (FQDN) or DNS suffixes that connect by using the LAN instead. This list applies only to Tunneled - Web SSO mode with NetScaler Gateway configured for reverse split tunneling.

Authentication

September 6, 2025

In an Citrix Endpoint Management deployment, several considerations come into play when deciding how to configure authentication. This section describes the various factors that affect authentication:

- The main MDX policies, Citrix Endpoint Management client properties, and NetScaler Gateway settings involved with authentication.
- The ways these policies, client properties, and settings interact.
- The tradeoffs of each choice.

This article also includes three examples of recommended configurations for increasing degrees of security.

Broadly speaking, stronger security results in a less-optimal user experience, because users have to authenticate more often. How you balance those concerns depends on your organization's needs and priorities. Review the three recommended configurations to understand the interplay of the various authentication options.

Authentication Modes

Online authentication: Allows users into the Citrix Endpoint Management network. Requires an Internet connection.

Offline authentication: Happens on the device. Users unlock the secure vault and have offline access to items, such as downloaded mail, cached websites, and notes.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Methods of Authentication

Single Factor LDAP: You can configure a connection in Citrix Endpoint Management to one or more directories that are compliant with the Lightweight Directory Access Protocol (LDAP). This method is commonly used to provide single sign-on (SSO) for company environments. You might opt for Citrix PIN with Active Directory password caching to improve the user experience with LDAP. At the same time, you can provide the security of complex passwords on enrollment, password expiration, and account lockout.

For more details, see Domain or domain plus security token authentication.

Client certificate: Citrix Endpoint Management can integrate with industry-standard certificate authorities to use certificates as the sole method of online authentication. Citrix Endpoint Management provides this certificate after user enrollment, which requires either a one-time password, invitation URL, or LDAP credentials. When using a client certificate as the primary method of authentication, a Citrix PIN is required in client certificate-only environments to secure the certificate on the device.

Citrix Endpoint Management supports Certificate Revocation List (CRL) only for a third-party Certificate Authority. If you have a Microsoft CA configured, Citrix Endpoint Management uses NetScaler Gateway to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the NetScaler Gateway Certificate Revocation List (CRL) setting, Enable CRL Auto Refresh. This step makes sure that a device enrolled only in MAM can't authenticate using an existing certificate on the device. Citrix Endpoint Management reissues a new certificate, because it doesn't restrict a user from generating a user certificate if one is revoked. This setting increases the security of PKI entities when the CRL checks for expired PKI entities.

For a diagram that shows the deployment needed for certificate-based authentication or the use of your enterprise Certificate Authority (CA) to issue device certificates, see Architecture.

Two-factor authentication LDAP + Client Certificate: This configuration is the best combination of security and user experience for Citrix Endpoint Management. Using both LDAP and client certificate authentication:

- Has the best SSO possibilities coupled with security provided by two-factor authentication at the NetScaler Gateway.
- Provides security with something users know (their Active Directory passwords) and something they have (client certificates on their devices).

Citrix Secure Mail can automatically configure and provide a seamless first-time user experience with client certificate authentication. That feature requires a properly configured Exchange client access server environment.

For optimal usability, you can combine LDAP and client certificate authentication with Citrix PIN and Active Directory password caching.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

LDAP + Token: This configuration allows for the classic configuration of LDAP credentials, plus a one-time password, using the RADIUS protocol. For optimal usability, you can combine this option with Citrix PIN and Active Directory password caching.

Important policies, settings, and client properties for authentication

The following policies, settings, and client properties come into play with the following three recommended configurations:

MDX policies

App passcode: If **On**, a Citrix PIN or passcode is required to unlock the app when it starts or resumes after a period of inactivity. Default is **On**.

To configure the inactivity timer for all apps, set the INACTIVITY_TIMER value in minutes in the Citrix Endpoint Management console in **Client Properties** on the **Settings** tab. The default is 15 minutes. To disable the inactivity timer, so that a PIN or passcode prompt appears only when the app starts, set the value to zero.

micro VPN session required: If **On**, the user must have a connection to the enterprise network and an active session to access the app on the device. If **Off**, an active session isn't required to access the app on the device. Default is **Off**.

Maximum offline period (hours): Defines the maximum period that an app can run without reconfirming app entitlement and refreshing policies from Citrix Endpoint Management. An iOS app retrieves new policies for MDX apps from Citrix Endpoint Management without any interruption to users after meeting the following conditions:

- You set the Maximum offline period and
- Citrix Secure Hub for iOS has a valid NetScaler Gateway token.

If Citrix Secure Hub doesn't have a valid NetScaler Gateway token, users must authenticate through Citrix Secure Hub before app policies can update. The NetScaler Gateway token can become invalid because of NetScaler Gateway session inactivity or a forced session time-out policy. When users sign on to Citrix Secure Hub again, they can continue running the app.

Users are reminded to sign on at 30, 15, and 5 minutes before the period expires. After expiration, the app is locked until users sign on. Default is **72 hours (3 days)**. The minimum period is 1 hour.

> **Note:**
>
> Keep in mind that in a scenario in which users travel often and use international roaming, the default of 72 hours (3 days) might be too short.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Background services ticket expiration: The time period that a background network service ticket stays valid. When Citrix Secure Mail connects through NetScaler Gateway to an Exchange Server running ActiveSync, Citrix Endpoint Management issues a token. Citrix Secure Mail uses that token to connect to the internal Exchange Server. This property setting determines the duration that Citrix Secure Mail can use the token without requiring a new token for authentication and the connection to the Exchange Server. When the time limit expires, users must log on again to generate a new token. Default is **168 hours (7 days)**. When this time-out expires, mail notifications stop.

micro VPN session required grace period: Determines how many minutes a user can use the app offline until the online session is validated. The default is **0** (no grace period).

For information about authentication policies, see:

- If you use the MAM SDK: MAM SDK overview
- If you use the MDX Toolkit: Citrix Endpoint Management MDX Policies for iOS and Citrix Endpoint Management MDX Policies for Android

Citrix Endpoint Management client properties

> **Note:**
>
> Client properties are global settings that apply to all devices that connect to Citrix Endpoint Management.

Citrix PIN: For a simple sign-on experience, you might choose to enable the Citrix PIN. With the PIN, users do not have to enter other credentials repeatedly, such as their Active Directory user names and passwords. You can configure the Citrix PIN as a standalone offline authentication only, or combine the PIN with Active Directory password caching to streamline authentication for optimal usability. You configure the Citrix PIN in **Settings > Client > Client Properties** in the Citrix Endpoint Management console.

The following is a summary of a few important properties. For more information, see Client properties.

ENABLE_PASSCODE_AUTH

Display name: Enable Citrix PIN Authentication

This key allows you to turn on Citrix PIN functionality. With the Citrix PIN or passcode, users are prompted to define a PIN to use instead of their Active Directory password. Enable this setting if **ENABLE_PASSWORD_CACHING** is enabled or if Citrix Endpoint Management is using certificate authentication.

Possible values: true or **false**

Default value: false

© 1997–2025 Citrix Systems, Inc. All rights reserved.

ENABLE_PASSWORD_CACHING

Display name: Enable User Password Caching

This key lets you allow the users' Active Directory password to be cached locally on the mobile device. When you set this key to true, users are prompted to set a Citrix PIN or passcode. The **ENABLE_PASSCODE_AUTH** key must be set to true when you set this key to **true**.

Possible values: true or **false**

Default value: false

PASSCODE_STRENGTH

Display name: PIN Strength Requirement

This key defines the strength of the Citrix PIN or passcode. When you change this setting, users are prompted to set a new Citrix PIN or passcode the next time they're prompted to authenticate.

Possible values: Low, **Medium**, or **Strong**

Default value: Medium

INACTIVITY_TIMER

Display name: Inactivity timer

This key defines the time in minutes that users can leave their devices inactive and then access an app without being prompted for a Citrix PIN or passcode. To enable this setting for an MDX app, you must set the **App Passcode** setting to **On**. If the **App Passcode** setting is set to **Off**, users are redirected to Citrix Secure Hub to do a full authentication. When you change this setting, the value takes effect the next time users are prompted to authenticate. The default is 15 minutes.

ENABLE_TOUCH_ID_AUTH

Display name: Enable Touch ID Authentication

Allows the use of the fingerprint reader (in iOS only) for offline authentication. Online authentication still requires the primary authentication method.

ENCRYPT_SECRETS_USING_PASSCODE

Display name: Encrypt secrets using Passcode

This key lets sensitive data be stored on the mobile device in a secret vault instead of in a platform-based native store, such as the iOS keychain. This configuration key enables strong encryption of key artifacts, but also adds user entropy (a user-generated random PIN code that only the user knows).

Possible values: true or **false**

Default value: false

© 1997–2025 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway Settings

Session time-out: If you enable this setting, NetScaler Gateway disconnects the session if NetScaler Gateway detects no network activity for the specified interval. This setting is enforced for users who connect with the NetScaler Gateway Plug-in, Citrix Secure Hub, or through a web browser. Default is **1440 minutes**. If you set this value to zero, the setting is disabled.

Forced time-out: If you enable this setting, NetScaler Gateway disconnects the session after the time-out interval elapses no matter what the user is doing. When the time-out interval elapses, there's no action the user can take to prevent the disconnection. This setting is enforced for users who connect with the NetScaler Gateway Plug-in, Citrix Secure Hub, or through a web browser. If Citrix Secure Mail is using STA, a special NetScaler Gateway mode, this setting doesn't apply to Citrix Secure Mail sessions. Default is no value, which means sessions are extended for any activity.

For more information about time-out settings for NetScaler Gateway, see the NetScaler Gateway documentation.

For more information on the scenarios that prompt users to authenticate with Citrix Endpoint Management by entering credentials on their devices, see Authentication Prompt Scenarios.

Default configuration settings

These settings are the defaults provided by the:

- NetScaler® for XenMobile wizard
- MAM SDK or MDX Toolkit
- Citrix Endpoint Management console

Setting	Where to Find the Setting	Default Setting
Session time-out	NetScaler Gateway	1440 minutes
Forced time-out	NetScaler Gateway	No value (off)
Maximum offline period	MDX Policies	72 hours
Background services ticket expiration	MDX Policies	168 hours (7 days)
micro VPN session required	MDX Policies	Off
micro VPN session required grace period	MDX Policies	0
App passcode	MDX Policies	On

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	Where to Find the Setting	Default Setting
Encrypt secrets using passcode	Citrix Endpoint Management client properties	false
Enable Citrix PIN Authentication	Citrix Endpoint Management client properties	false
PIN Strength Requirement	Citrix Endpoint Management client properties	Medium
PIN Type	Citrix Endpoint Management client properties	Numeric
Enable User Password Caching	Citrix Endpoint Management client properties	false
Inactivity Timer	Citrix Endpoint Management client properties	15
Enable Touch ID Authentication	Citrix Endpoint Management client properties	false

Recommended Configurations

This section gives examples of three Citrix Endpoint Management configurations that range from the lowest security and optimal user experience to the highest security and more intrusive user experience. These examples provide you with helpful reference points to determine where on the scale you want to place your own configuration. Modifying these settings might require you to alter other settings. For instance, the maximum offline period must not go past the session time-out.

Highest Security

This configuration offers the highest level of security but has significant usability trade-offs.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Session time-out	NetScaler Gateway	1440	Users enter their Citrix Secure Hub credentials only when online authentication is required-every 24 hours.
Forced time-out	NetScaler Gateway	No value	Sessions are extended if there's any activity.
Maximum offline period	MDX Policies	23	Requires policy refresh every day.
Background services ticket expiration	MDX Policies	72 hours	Time out for STA, which allows for long-lived sessions without a NetScaler Gateway session token. For Citrix Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop. In that case, Citrix Secure Mail doesn't prompt the user if they don't open the app before the session expires.
micro VPN session required	MDX Policies	Off	Provides a valid network connection and NetScaler Gateway session to use the apps.
micro VPN session required grace period	MDX Policies	0	No grace period (if you enabled micro VPN session required).
App passcode	MDX Policies	On	Require a passcode for an application.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Encrypt secrets using passcode	Citrix Endpoint Management client properties	true	A key derived from user entropy protects the vault.
Enable Citrix PIN Authentication	Citrix Endpoint Management client properties	true	Enable Citrix PIN for a simplified authentication experience.
PIN Strength Requirement	Citrix Endpoint Management client properties	Strong	High password complexity requirements.
PIN Type	Citrix Endpoint Management client properties	Alphanumeric	PIN is an alphanumeric sequence.
Enable Password Caching	Citrix Endpoint Management client properties	false	Active Directory password isn't cached and a Citrix PIN is used for offline authentications.
Inactivity Timer	Citrix Endpoint Management client properties	15	If a user doesn't use MDX apps or Citrix Secure Hub for this period, prompt for offline authentication.
Enable Touch ID Authentication	Citrix Endpoint Management client properties	false	Disables Touch ID for offline authentication use cases in iOS.

Higher Security

A more middle-of-the-road approach, this configuration requires users to authenticate more often - every 3 days, at most, instead of 7 - and stronger security. The increased number of authentications lock the container more often, providing data security when devices aren't in use.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Session time-out	NetScaler Gateway	4320	Users enter their Citrix Secure Hub credentials only when online authentication is required - every 3 days
Forced time-out	NetScaler Gateway	No value	Sessions are extended if there's any activity.
Maximum offline period	MDX Policies	71	Requires policy refresh every 3 days. The hour difference is to allow for refresh ahead of session time-out.
Background services ticket expiration	MDX Policies	168 hours	Time out for STA, which allows for long-lived sessions without a NetScaler Gateway session token. For Citrix Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop without prompting the user.
micro VPN session required	MDX Policies	Off	Provides a valid network connection and NetScaler Gateway session to use the apps.
micro VPN session required grace period	MDX Policies	0	No grace period (if you enabled micro VPN session required).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App passcode	MDX Policies	On	Require a passcode for an application.
Encrypt secrets using passcode	Citrix Endpoint Management client properties	false	Do not require user entropy to encrypt the vault.
Enable Citrix PIN Authentication	Citrix Endpoint Management client properties	true	Enable Citrix PIN for a simplified authentication experience.
PIN Strength Requirement	Citrix Endpoint Management client properties	Medium	Enforces medium password complexity rules.
PIN Type	Citrix Endpoint Management client properties	Numeric	A PIN is a numeric sequence.
Enable Password Caching	Citrix Endpoint Management client properties	true	The user PIN caches and protects the Active Directory password.
Inactivity Timer	Citrix Endpoint Management client properties	30	If a user doesn't use MDX apps or Citrix Secure Hub for this period, prompt for offline authentication.
Enable Touch ID Authentication	Citrix Endpoint Management client properties	true	Enables Touch ID for offline authentication use cases in iOS.

High Security

This configuration, the most convenient to users, provides base-level security.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Session time-out	NetScaler Gateway	10080	Users enter their Citrix Secure Hub credentials only when online authentication is required - every 7 days
Forced time-out	NetScaler Gateway	No value	Sessions are extended if there's any activity.
Maximum offline period	MDX Policies	167	Requires policy refresh every week (every 7 days). The hour difference is to allow for refresh ahead of session time-out.
Background services ticket expiration	MDX Policies	240	Time out for STA, which allows for long-lived sessions without a NetScaler Gateway session token. For Citrix Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop. In that case, Citrix Secure Mail doesn't prompt the user if they don't open the app before the session expires.
micro VPN session required	MDX Policies	Off	Provides a valid network connection and NetScaler Gateway session to use the apps.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

micro VPN session required grace period	MDX Policies	0	No grace period (if you enabled micro VPN session required).
App passcode	MDX Policies	On	Require a passcode for an application.
Encrypt secrets using passcode	Citrix Endpoint Management client properties	false	Do not require user entropy to encrypt the vault.
Enable Citrix PIN Authentication	Citrix Endpoint Management client properties	true	Enable Citrix PIN for a simplified authentication experience.
PIN Strength Requirement	Citrix Endpoint Management client properties	Low	No password complexity requirements
PIN Type	Citrix Endpoint Management client properties	Numeric	A PIN is a numeric sequence.
Enable Password Caching	Citrix Endpoint Management client properties	true	The user PIN caches and protects the Active Directory password.
Inactivity Timer	Citrix Endpoint Management client properties	90	If a user doesn't use MDX apps or Citrix Secure Hub for this period, prompt for offline authentication.
Enable Touch ID Authentication	Citrix Endpoint Management client properties	true	Enables Touch ID for offline authentication use cases in iOS.

Using Step-Up Authentication

Some apps might require enhanced authentication. For example, a secondary authentication factor, such as a token or aggressive session time-outs. You control this authentication method through an MDX policy. The method also requires a separate virtual server to control the authentication methods (on either the same or on separate NetScaler Gateway appliances).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Alternate NetScaler Gateway	MDX Policies	Requires the FQDN and port of the secondary NetScaler Gateway appliance.	Allows for enhanced authentication controlled by the secondary NetScaler Gateway appliance authentication and session policies.

If a user opens an app that uses the alternate NetScaler Gateway, all other apps use that NetScaler Gateway instance to communicate with the internal network. The session only switches back to the lower security NetScaler Gateway instance when the session times out from the NetScaler Gateway instance with enhanced security.

Using micro VPN session required

For certain applications, such as Citrix Secure Web, you can make sure that users run an app only when they have an authenticated session. This policy enforces that option and allows for a grace period so users can finish their work.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
micro VPN session required	MDX Policies	On	Makes sure that a device is online and has a valid authentication token.
micro VPN session required grace period	MDX Policies	15	Allows a 15-minute grace period before the user can no longer use the apps

Server properties

May 5, 2025

© 1997–2025 Citrix Systems, Inc. All rights reserved.

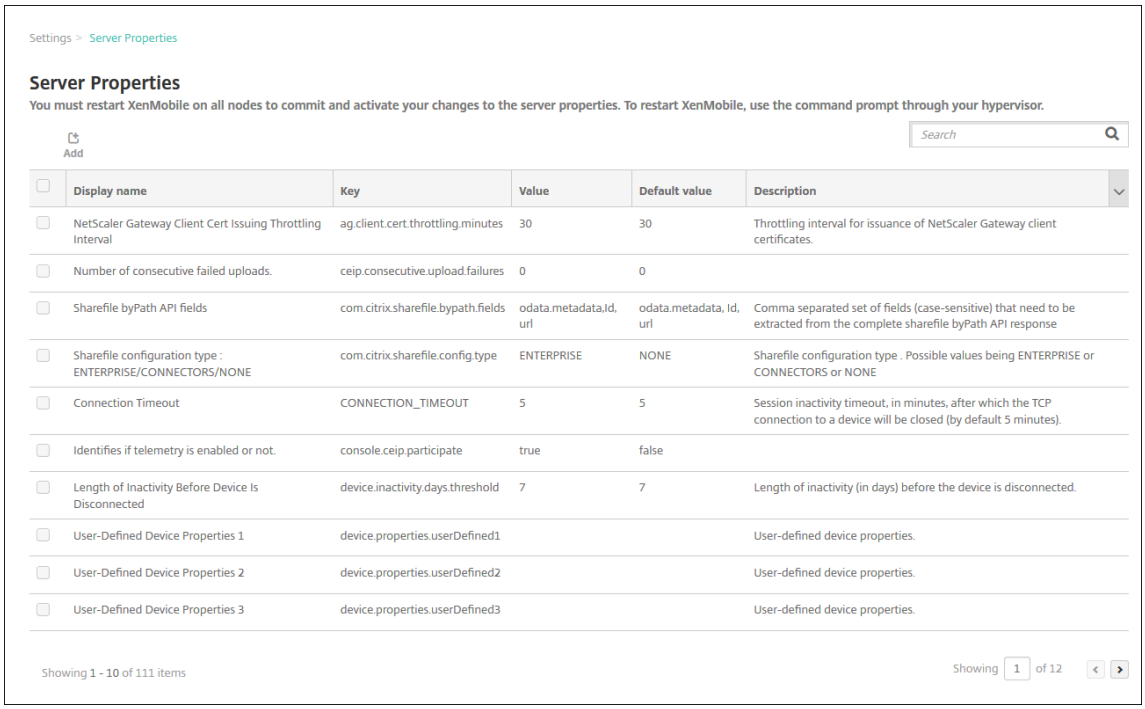
Server properties are global properties that apply to operations, users, and devices across an entire Citrix Endpoint Management instance. Citrix recommends that you evaluate for your environment the server properties covered in this article. Be sure to consult with Citrix before changing other server properties.

To update server properties, go to **Settings > Server Properties**.

Adding, Editing, or Deleting Server Properties

In Citrix Endpoint Management, you can apply properties to the server.

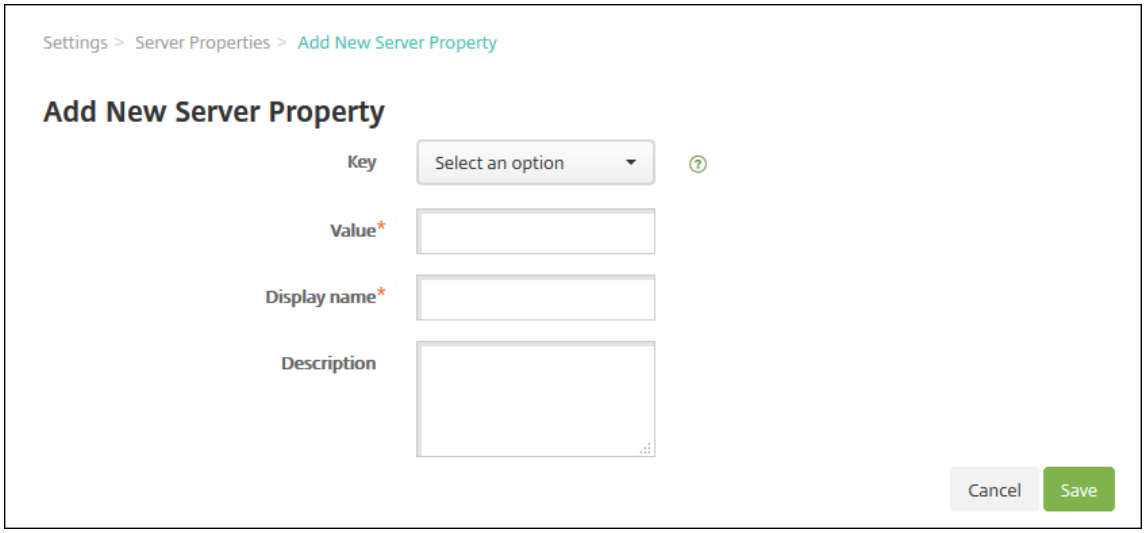
1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Server**, click **Server Properties**. The **Server Properties** page appears. You can add, edit, or delete server properties from this page.



To add a server property

1. Click **Add**. The **Add New Server Property** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. Configure these settings:

   - Key: In the list, select the appropriate key. Keys are case-sensitive. Contact Citrix Support before you edit property values or to request a special key.
   - Value: Enter a value depending on the key that you selected.
   - Display Name: Enter a name for the new property value that appears in the **Server Properties** table.
   - Description: Optionally, type a description for the new server property.

3. Click **Save**.

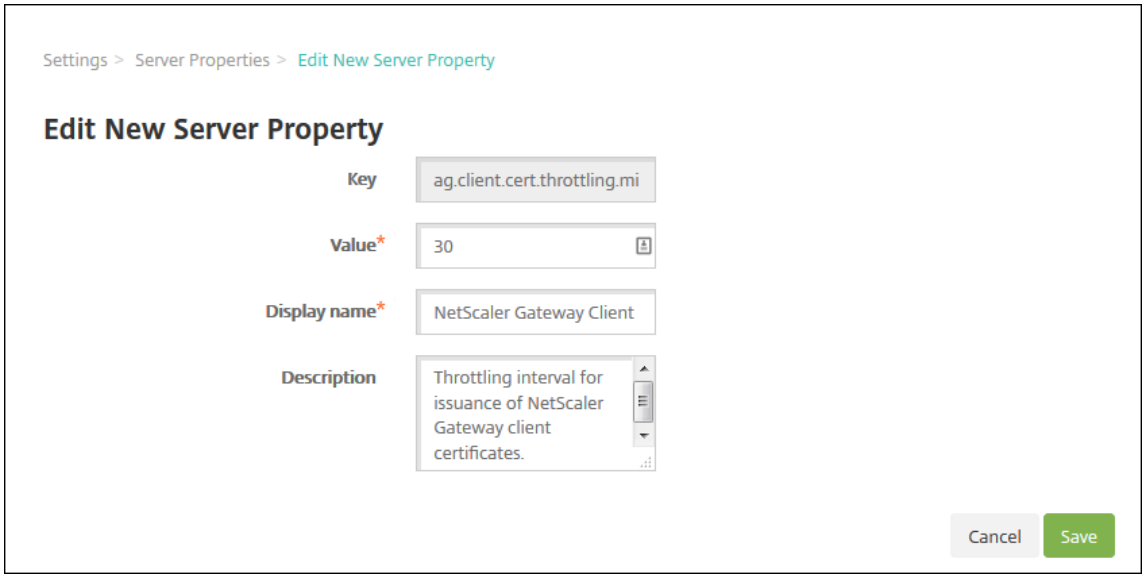
To edit a server property

1. In the **Server Properties** table, select the server property you want to edit.

   When you select the checkbox next to a server property, the options menu appears above the server property list. Click anywhere else in the list to open the options menu on the right side of the listing.

2. Click **Edit**. The **Edit New Server Property** page appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Change the following information as appropriate:
   - Key: You cannot change this field.
   - Value: The property value.
   - Display Name: The property name.
   - Description: The property description.
4. Click **Save** to save your changes or **Cancel** to leave the property unchanged.

To delete a server property

1. In the **Server Properties** table, select the server properties you want to delete.
2. Click **Delete**. A confirmation dialog box appears. Click **Delete** again.

Server Property Definitions

Access all apps in the managed Google Play store

- If **true**, Citrix Endpoint Management makes all apps from the public Google Play store accessible from the managed Google Play store. You can use the Restrictions device policy to control access to these apps. Defaults to **false**.

Add Device Always

- If **true**, Citrix Endpoint Management adds a device to the Citrix Endpoint Management console, even if it fails enrollment. As a result, you can see which devices tried to enroll. Defaults to **false**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

AG Client Cert Issuing Throttling Interval

- The grace period between generating certificates. This interval prevents Citrix Endpoint Management from generating many certificates for a device in a short time period. Citrix recommends that you don't change this value. Defaults to **30** minutes.

Allows The Removal of Devices That Have Been Marked Inactive For A Specified Period Of Time

- If **true**, devices that have been inactive for a specified time (in days) are removed and deleted from Citrix Endpoint Management. The period of activity is set by the **Length of Time Device Can Be Inactive Before Being Automatically Removed From CEM** server property. The default is **true**. To change the value of this property, consult your Citrix representative.

Audit Logger

- If **False**, does not log user interface (UI) events. Defaults to **False**.

Block Enrollment of Rooted Android and Jailbroken iOS Devices

When this property is set as **true**, Citrix Endpoint Management blocks enrollments for rooted Android devices and jailbroken iOS devices. The recommended setting is **true** for all security levels. Defaults to **true**.

cdn.s3.retry.interval and cdn.s3.max.retry

The `cdn.s3.retry.interval` and `cdn.s3.max.retry` server properties work together to set the maximum time limit on every macOS PKG file upload. By default, Citrix Endpoint Management limits file upload times to 100 seconds. If a file upload is over that limit, the upload fails. To change the default, configure the `cdn.s3.retry.interval` and `cdn.s3.max.retry` keys as follows:

- `cdn.s3.retry.interval`. Lets you define the interval, in milliseconds, at which Citrix Endpoint Management verifies whether a file upload completes successfully. The default is `10000`.
- `cdn.s3.max.retry`. Lets you define the maximum number of verification retries after which the upload fails. The default is `10`.

The two keys work together to limit file upload times. By default, the time limit is 100 seconds (10000*10 milliseconds).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Certificate Renewal in Seconds

- The number of seconds before a certificate expires that Citrix Endpoint Management starts to renew certificates. An example is when a certificate expires on December 30 and this property is set to 30 days. If the device connects between December 1 and December 30, Citrix Endpoint Management tries to renew the certificate. Defaults to **2592000** seconds (30 days).

Connection Timeout

- The session inactivity timeout, in minutes, after which Citrix Endpoint Management closes the TCP connection to a device. The session stays open. Applies to Android devices. Defaults to **5** minutes.

Default deployment channel

- Determines how Citrix Endpoint Management deploys a resource to a device: At the user-level (**DEFAULT_TO_USER**) or device-level. Defaults to **DEFAULT_TO_DEVICE**.

Deprecate mobile service provider

- Deprecates support for the mobile service provider interface used to query Blackberry and other Exchange ActiveSync devices. While enabled, the **Mobile Service Provider** interface is hidden from the console. Default is **true**.

Device tagging

- If you set `enable.device.tagging` to **true**, Citrix Endpoint Management tags devices by device type automatically. You can use device tags to deploy policies and apps or configure delivery groups. Citrix Endpoint Management applies tags to devices for the following:
  - BYOD tags
    - iOS User Enrollment
    - Android Enterprise work profile
  - Corporate tags
    - Android Enterprise fully managed corporate devices
    - Bulk enrollment
      - Apple Business Manager devices
      - Apple School Manager devices
      - Windows AutoPilot devices
      - Android Enterprise bulk enrollment

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Disable Hostname Verification

- By default, host name verification is enabled on outgoing connections except for the Microsoft PKI server. When host name verification fails, the server log includes errors such as: "Unable to connect to the Volume Purchase Server: Host name '192.0.2.0'does not match the certificate subject provided by the peer". If host name verification breaks your deployment, change this property to **true**. Defaults to **false**.

Disable SSL Server Verification

- If **True**, disables SSL server certificate validation when all the following conditions are met:
  - You enabled certificate-based authentication on Citrix Endpoint Management
  - The Microsoft CA server is the certificate issuer
  - An internal CA, whose root Citrix Endpoint Management doesn't trust, signed your certificate.

  Defaults to **True**.

Enable Crash Reporting

- If **true**, Citrix collects crash reports and diagnostics to help troubleshoot issues with Citrix Secure Hub for iOS and Android. If **false**, no data is collected. The default value is **true**.

Enable/Disable Hibernate statistics logging for diagnostics

- If **True**, enables Hibernate statistics logging to assist with troubleshooting application performance issues. Hibernate is a component used for Citrix Endpoint Management connections to a Microsoft SQL Server. By default, the logging is disabled because it impacts application performance. Enable logging only for a short duration to avoid creating a huge log file. Citrix Endpoint Management writes the logs to /opt/sas/logs/hibernate_stats.log. Defaults to **False**.

Enable macOS OTAE

- If **false**, prevents the use of an enrollment link for macOS devices, meaning macOS users can enroll only by using an enrollment invitation. Defaults to **true**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Enable Notification Trigger

- Enables or disables Citrix Secure Hub client notifications. The value **true** enables notifications. Defaults to **true**.

Full Pull of ActiveSync Allowed and Denied Users

- The interval in (in seconds) that Citrix Endpoint Management pulls a complete list (baseline) of ActiveSync allowed and denied users. Defaults to **28800** seconds.

Identifies if telemetry is enabled or not

- Identifies if telemetry is enabled. Telemetry is also referred to as the Customer Experience Improvement Program (CEIP). You can opt in to CEIP when you install or upgrade Citrix Endpoint Management. If Citrix Endpoint Management has 15 consecutive failed uploads, it disables telemetry. Defaults to **false**.

Inactivity Timeout in Minutes

- The number of minutes after which Citrix Endpoint Management logs out an inactive user. The user must have used the Citrix Endpoint Management Public API to access the Citrix Endpoint Management console or any third-party app. A time-out value of **0** means that an inactive user stays logged in. For third-party apps that access the API, being logged in is typically necessary. The default value is set as **5**.
- If the **WebServices timeout type** server property is **INACTIVITY_TIMEOUT:** This property defines the number of minutes after which Citrix Endpoint Management logs out an inactive administrator who did the following:
  - Used the Public API for REST Services to access the Citrix Endpoint Management console
  - Used the Public API for REST Services to access any third-party app. A timeout of **0** means that an inactive user stays logged in.

include.device.properties.during.search

- Includes all device properties in a device search. The default is **Off**, which limits the search scope to these device properties, for fast searching:
  - Serial Number
  - IMEI

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Wi-Fi MAC address
- Bluetooth MAC address
- Active Sync ID
- User Name

When this property is set as **On**, device searches can take longer.

ios.delayBeforeDeclareUnreachable; macos.delayBeforeDeclareUnreachable

- Specifies the number of days after which an offline iOS or macOS device is considered unreachable. When an iOS or macOS device reaches the limit specified, they stop checking back with Citrix Endpoint Management. Both properties default to **45** days.

iOS Device Management Enrollment Install Root CA if Required

- The server property **ios.mdm.enrollment.installRootCaIfRequired** is set to **False** for all Citrix Endpoint Management environments. Citrix Endpoint Management uses a publicly trusted certificate chain, so that it isn't necessary to push a root CA to devices. (This property is used only for on-premises environments.)

iOS Device Management Enrollment Last Step Delayed

- During device enrollment, this property value specifies the amount of time to wait between installing the MDM profile and starting the Agent on the device. Citrix recommends that you edit this property only for network latency or speed issues. In that case, don't set to the value to more than 5000 milliseconds (5 seconds). Defaults to **1000** milliseconds (1 second).

iOS Device Management Identity Delivery Mode

- Specifies whether Citrix Endpoint Management distributes the MDM certificate to devices using **SCEP** (recommended for security reasons) or **PKCS12**. In PKCS12 mode, the key pair is generated on the server and no negotiation is done. Defaults to **SCEP**.

iOS Device Management Identity Key Size

- Defines the size of private keys for MDM identities, iOS profile service, and Citrix Endpoint Management iOS agent identities. Defaults to **2048**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

iOS Device Management Identity Renewal Days

- Specifies the number of days before the certificate expiration that Citrix Endpoint Management starts renewing certificates. For example: If a certificate expires in 10 days and this property is **10** days: When a device connects 9 days before expiration, Citrix Endpoint Management issues a new certificate. Defaults to **30** days.

iOS MDM APNS Private Key Password

- This property has the APNs password, which is required for Citrix Endpoint Management to push notifications to Apple servers.

Length of Inactivity Before Device Is Disconnected

- Specifies how long a device can be inactive, including the last authentication, before Citrix Endpoint Management disconnects it. Defaults to **7** days.

Length of Time Device Can Be Inactive Before Being Automatically Removed From CEM

- The length of time (in days) a device can be inactive before being automatically removed from Citrix Endpoint Management. The minimum is **14** days and the default is **30** days. The **Allows The Removal of Devices That Have Been Marked Inactive For A Specified Period Of Time** server property must be set to **true** for this property to take effect.

local.user.account.lockout.time

- Specifies the number of minutes a user must wait after exceeding the lockout limit. Supported values are 0–999. The default is **30** minutes.

local.user.account.lockout.limit

- Specifies the maximum number of consecutive invalid login attempts per user. Supported values are 0–999. The default value is set as **6**.

mac.dep.admin.passwd.rotate

This server property lets you configure administrator password rotation intervals for macOS devices enrolled through the Apple Deployment Program. Citrix Endpoint Management checks whether to rotate the password of the administrator account daily. By default, Citrix Endpoint Management rotates

© 1997–2025 Citrix Systems, Inc. All rights reserved.

the password every 10,080 minutes (7 days). Configure the `mac.dep.admin.passwd.rotate` key as follows:

- Value: *administrator-defined*
  The interval, in minutes, at which Citrix Endpoint Management rotates the password. Type a value equal to or greater than 360 (6 hours). Citrix Endpoint Management ignores values smaller than 360 and rotates the password every 360 minutes (6 hours) instead.
- Display name: *administrator-defined*
- Description: *administrator-defined*

MAM Only Device Max

- This Custom Key limits the number of MAM-only devices that each user can enroll. Configure the key as follows. A **Value** of **0** allows unlimited device enrollment.
- Key = **number.of.mam.devices.per.user**
- Value = **5**
- Display name = **MAM Only Device Max**
- Description = **Limits the number of MAM devices each user can enroll.**

MaxNumberOfWorker

- The number of threads used when importing many Volume Purchase licenses. Defaults to **3**. If you need further optimization, you can increase the number of threads. However, a larger number of threads results in high CPU usage.

NetScaler Gateway (NetScaler) Single Sign-On

- If **False**, disables the Citrix Endpoint Management callback feature during single sign-on from NetScaler Gateway to Citrix Endpoint Management. If the NetScaler Gateway configuration includes a callback URL, Citrix Endpoint Management uses the callback feature to verify the NetScaler Gateway session ID. Defaults to **False**.

Number of consecutive failed uploads

- Displays the number of consecutive failures during Customer Experience Improvement Program (CEIP) uploads. Citrix Endpoint Management increments the value when an upload fails. After 15 upload failures, Citrix Endpoint Management disables CEIP, also called telemetry. For more

© 1997–2025 Citrix Systems, Inc. All rights reserved.

information, see the server property **Identifies if telemetry is enabled or not**. Citrix Endpoint Management resets the value to **0** when an upload succeeds.

Number of Users Per Device

- The maximum number of users who can enroll the same device in MDM. The value **0** means that an unlimited number of users can enroll the same device. Defaults to **0**.

optional.user.identity.attributes

- This server property lets you customize the optional Active Directory user attributes.

  Create the custom key and, in the **Values** field, edit user attributes to define which attributes Citrix Endpoint Management can access to create a user account. For more information, see Customize user properties.

  - Key: **Custom Key**
  - Key: **optional.user.identity.attributes**
  - Value: **commonName, firstName, lastName, displayName, streetAddress, city, state, country, workPhone, homePhone, mobilePhone, company, department, description, employeeID, faxNumber, initials, ipPhone, manager, homePostalAddress, otherMobile, pager, physicalDeliveryOfficeName, postalCode, postOfficeBox, title, organization, preferredLanguage**
  - Display Name: **optional.user.identity.attributes**
  - Description: **Optional Active Directory user attributes**

Organization Name for macOS and iOS/iPadOS Enrollment Profiles

- The value you type for `apple.mdm.enrollment.profile.organization.name` corresponds to the name of the organization that provides the enrollment profile. The name displays when users enroll their device to Citrix Endpoint Management. The default name that displays is **Citrix Workspace**.

Pull of Incremental Change of Allowed and Denied Users

- The number of seconds that Citrix Endpoint Management waits for a response from the domain when running a PowerShell command to get a delta of ActiveSync devices. Defaults to **60** seconds.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Read Timeout to Microsoft Certification Server

- The number of seconds that Citrix Endpoint Management waits for a response from the certificate server when doing a read. If the certificate server is slow and has much traffic, you can increase this value to 60 seconds or more. A certificate server that doesn't respond after 120 seconds requires maintenance. Defaults to **15000** milliseconds (15 seconds).

REST Web Services

- Enables the REST Web Service. Defaults to **true**.

Retrieves devices information in chunks of specified size

- This value is used internally for multithreading during device exports. If the value is higher, a single thread parses more devices. If the value is lower, more threads fetch the devices. Reducing the value might increase the performance of exports and device list fetches, yet might reduce available memory. Defaults to **1000**.

shp.console.enable

- If **False**, prevents access to the Self-Help Portal. Users who navigate to the portal on port 4443 get an "Access Denied"message. If **True**, provides access to the Self-Help Portal over port 443.

  Defaults to **False**.

enable.new.shp

- If **False**, prevents users from enabling their devices from the Self-Help Portal. If **True**, users can enable their devices from the Self-Help Portal.

  The BitLocker recovery key feature requires that you set this property to **False** and the `shp.console.enable` property to **True**.

  Defaults to **False**.

Session Log Cleanup (in Days)

- The number of days that Citrix Endpoint Management keeps the session log. Defaults to **7**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

ShareFile configuration type

- Specifies the Citrix Files storage type. **ENTERPRISE** enables Citrix Files Enterprise mode. **CONNECTORS** provides access only to storage zone connectors that you create through the Citrix Endpoint Management console. Defaults to **NONE**, which shows the initial view of the **Configure > Citrix Files** screen where you choose between Citrix Files Enterprise and Connectors. Defaults to **NONE**.

Static Timeout in Minutes

- If the **WebServices timeout type** server property is **STATIC_TIMEOUT:** This property defines the number of minutes after which Citrix Endpoint Management logs out an administrator after using the following:
  - The Public API for REST Services to access the Citrix Endpoint Management console.
  - The Public API for REST Services to access any third-party app.

  Defaults to **60**.

Trigger Agent Message Suppression

- Enables or disables Citrix Secure Hub client messaging. The value **false** enables messaging. Defaults to **true**.

Trigger Agent Sound Suppression

- Enables or disables Citrix Secure Hub client sounds. The value **false** enables sounds. Defaults to **true**.

Unauthenticated App Download for Android Devices

- If **True**, you can download self-hosted apps to Android devices running Android Enterprise. Citrix Endpoint Management needs this property if the Android Enterprise option to provide a download URL in the Google Play Store statically is enabled. In that case, download URLs can't include a one-time ticket (defined by the **XAM One-Time Ticket server** property) which has the authentication token. Defaults to **False**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Unauthenticated App Download for Windows Devices

- Used only for older Citrix Secure Hub versions which don't validate one-time tickets. If **False**, you can download unauthenticated apps from Citrix Endpoint Management to Windows devices. Defaults to **False**.

Use ActiveSync ID to Conduct an ActiveSync Wipe Device

- If **true**, the Citrix Endpoint Management connector for Exchange ActiveSync uses the ActiveSync identifier as an argument for the **asWipeDevice** method. Defaults to **false**.

Users only from Exchange

- If **true**, disables user authentication for ActiveSync Exchange users. Defaults to **false**.

Volume Purchase baseline interval

- The minimum interval that Citrix Endpoint Management reimports Volume Purchase licenses from Apple. Refreshing license information makes sure that the Citrix Endpoint Management reflects all changes, such as when you manually delete an imported app from Volume Purchase. By default, Citrix Endpoint Management refreshes the Volume Purchase license baseline a minimum of every **1440** minutes.
  - If you have many Volume Purchase licenses installed (for example, more than 50,000): Citrix recommends that you increase the baseline interval to reduce the frequency and overhead of importing licenses.
  - If you expect frequent Volume Purchase license changes from Apple: Citrix recommends that you lower the value to keep Citrix Endpoint Management updated with the changes.
  - The minimum interval between the two baselines is 60 minutes. Also, the Citrix Endpoint Management does a delta import every 60 minutes, to capture the changes since the last import. So, if the Volume Purchase baseline interval is 60 minutes, the interval between baselines might be delayed up to 119 minutes.

WebServices Timeout Type

- Specifies how to expire an authentication token retrieved from the public API.
  - If **STATIC_TIMEOUT:** Citrix Endpoint Management considers a token expired, based on the value of the server property **Static Timeout in Minutes**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - If **INACTIVITY_TIMEOUT:** Citrix Endpoint Management considers a token expired, based on the value of the server property **Inactivity Timeout in Minutes**. Defaults to **STATIC_TIMEOUT**.

Windows Tablet MDM Certificate Extended Validity (5y)

- The validity period of the device certificate issued by MDM for the Windows Tablet. Devices use a device certificate to authenticate to the MDM server during device management. If **true**, the validity period is five years. If **false**, the validity period is two years. Defaults to **true**.

Windows WNS Channel - Number of Days Before Renewal

- The renewal frequency for the ChannelURI. Defaults to **10** days.

Windows WNS Heartbeat Interval

- How long Citrix Endpoint Management waits before connecting to a device after connecting to it every three minutes five times. Defaults to **6** hours.

XAM One-Time Ticket

- The number of milliseconds that a one-time authentication token (OTT) is valid for downloading an app. This property and the properties **Unauthenticated App download for Android** and **Unauthenticated App download for Windows** work together. Those properties specify whether to allow unauthenticated app downloads. Defaults to **3600000**.

Citrix Endpoint Management MDM Self-Help Portal console max inactive interval (minutes)

- This property name reflects the older Citrix Endpoint Management versions. The property controls the Citrix Endpoint Management console max inactive interval. That interval is the number of minutes after which Citrix Endpoint Management logs an inactive user out of the Citrix Endpoint Management console. A time-out of **0** means that an inactive user stays logged in. Default is **30**.

Remove ABM devices from CEM when unassigned from ABM MDM server

- If `remove.unassigned.abm.devices` is **true**, CEM removes devices that are no longer assigned to this server. Default to **false**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Device and app policies

September 6, 2025

Citrix Endpoint Management device and app policies enable you to optimize a balance between factors, such as:

- Enterprise security
- Corporate data and asset protection
- User privacy
- Productive and positive user experiences

The optimum balance between those factors can vary. For example, highly regulated organizations, such as finance, require stricter security controls than other industries, such as education and retail, in which user productivity is a primary consideration.

You can centrally control and configure policies based on users' identity, device, location, and connectivity type to restrict malicious usage of corporate content. If a device is lost or stolen, you can disable, lock, or wipe business applications and data remotely. The overall result is a solution that increases employee satisfaction and productivity, while making sure of the security and administrative control.

The primary focus of this article is the many device and app policies related to security.

Policies that address security risks

Citrix Endpoint Management device and app policies address many situations that might pose a security risk, such as when:

- Users try to access apps and data from untrusted devices and unpredictable locations
- Users pass data between devices
- An unauthorized user tries to access data
- A user who has left the company used their own device (BYOD)
- A user misplaces a device
- Users must access the network securely always
- Users have their own device managed and you must separate work data from personal data
- A device is idle and requires verification of user credentials again
- Users copy and paste sensitive content into unprotected email systems
- Users receive email attachments or web links with sensitive data on a device that holds both personal and company accounts

Those situations relate to two main areas of concern when protecting company data, which are when data is:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- At rest
- In transit

How Citrix Endpoint Management protects data at rest

Data stored on mobile devices is referred to as data at rest. Citrix Endpoint Management uses the device encryption provided by the iOS and Android platforms. Citrix Endpoint Management supplements platform-based encryption with features such as compliance checking, available through the Citrix MAM SDK.

The mobile application management (MAM) capabilities in Citrix Endpoint Management enable complete management, security, and control over Citrix mobile productivity apps, MDX-enabled apps, and their associated data.

The Mobile Apps SDK enables apps for Citrix Endpoint Management deployment through use of the Citrix MDX app container technology. The container technology separates corporate apps and data from personal apps and data on a user device. The data separation allows you to secure any custom-developed, third-party, or BYO mobile app with comprehensive policy-based controls.

Citrix Endpoint Management also includes app-level encryption. Citrix Endpoint Management separately encrypts data stored within any MDX-enabled app without requiring a device passcode and without requiring that you manage the device to enforce the policy.

- On iOS devices, Citrix Endpoint Management uses strong FIPS-validated cryptographic services and libraries such as keychain.
- OpenSSL provides FIPS-validated modules for various device platforms. OpenSSL further secures data in motion and the certificates required to manage and enroll devices.
- Citrix Endpoint Management uses the MAM SDK shared vault API to share managed content between apps that have the same keychain access group. For example, you can share user certificates through an enrolled app so that apps can get a certificate from the secure vault.
- Citrix Endpoint Management uses the device encryption provided by the platforms.
- Citrix Endpoint Management MAM controls at the app level do a compliance check to validate that device encryption is enabled at every app launch.

How Citrix Endpoint Management protects data in transit

Data on the move between your user's mobile devices and your internal network is referred to as data in transit. MDX app container technology provides application-specific VPN access to your internal network through NetScaler Gateway.

Consider the situation where an employee wants to access the following resources that are in the secure enterprise network from a mobile device:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- The corporate email server
- An SSL-enabled web application hosted on the corporate intranet
- Documents stored on a file server or Microsoft SharePoint

MDX enables access to all these enterprise resources from mobile devices through an application-specific micro VPN. Each device has its own dedicated micro VPN tunnel.

Micro VPN functionality does not require a device-wide VPN, which can compromise security on untrusted mobile devices. As a result, the internal network is not exposed to malware or attacks that can infect the entire corporate system. Corporate mobile apps and personal mobile apps can coexist on one device.

To offer even stronger levels of security, you can configure MDX-enabled apps with an Alternate NetScaler Gateway policy. The policy is used for authentication and for micro VPN sessions with an app. You can use an Alternate NetScaler Gateway with the micro VPN session-required policy to force apps to reauthenticate to the specific gateway. Such gateways might typically have different (higher assurance) authentication requirements and traffic management policies.

In addition to security features, the micro VPN feature also offers data optimization techniques, including compression algorithms. Compression algorithms make sure that:

- Only minimal data is transferred
- The transfer is done in the quickest time possible. Speed improves user experience, which is a key success factor in mobile device adoption.

Reevaluate your device policies periodically, such as in these situations:

- When a new version of Citrix Endpoint Management includes new or updated policies because of the release of device operating system updates
- When you add a device type:

  Although many policies are common to all devices, each device has a set of policies specific to its operating system. As a result, you might find differences between iOS, Android, and Windows devices, and even between Android devices from different manufacturers.
- To keep Citrix Endpoint Management operation in sync with enterprise or industry changes, such as new corporate security policies or compliance regulations
- When a new version of the MAM SDK includes new or updated policies
- When you add or update an app
- To integrate new workflows for your users because of new apps or new requirements

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App policies and Use case scenarios

Although you can choose which apps are available through Citrix Secure Hub, you might also want to define how those apps interact with Citrix Endpoint Management. Use app policies:

- If you want users to authenticate after a certain time period passes.
- If you want to provide users offline access to their information.

The following sections include some of the policies and example usage.

- For a list of the third-party policies you can integrate in your iOS and Android app by using the MAM SDK, see MAM SDK overview.
- For a list of all MDX policies per platform, see MDX Policies at a Glance.

Authentication policies

- **Device passcode**

  Why use this policy: Enable the Device passcode policy to enforce that a user can access an MDX app only if the device has a device passcode enabled. This feature makes sure that the use of iOS encryption at the device level.

  User example: Enabling this policy means that the user must set a passcode on their iOS device before they can access the MDX app.

- **App passcode**

  Why use this policy: Enable the App passcode policy to have Citrix Secure Hub prompt a user to authenticate to the managed app before they can open the app and access data. The user might authenticate with their Active Directory password, Citrix PIN, or iOS TouchID, depending what you configure under **Settings > Client Properties** in the Citrix Endpoint Management console. You can set an inactivity timer in Client Properties so that Citrix Secure Hub doesn't prompt the user to reauthenticate to the managed app until the timer expires.

  The app passcode differs from a device passcode. With a device passcode policy pushed to a device, Citrix Secure Hub prompts the user to configure a passcode or PIN. The user must unlock their device when they turn on the device or when the inactivity timer expires. For more information, see Authentication in Citrix Endpoint Management.

  User example: When opening the Citrix Secure Web application on the device, the user must enter their Citrix PIN before they can browse websites if the inactivity period is expired.

- **micro VPN session required**

  Why use this policy: If an application requires access to a web app (web service) to run, enable this policy. Citrix Endpoint Management then prompts the user to connect to the enterprise network or have an active session before using the app.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

User example: When a user tries to open an MDX app that has the micro VPN session-required policy enabled: They can't use the app until they connect to the network. The connection must use a cellular or Wi-Fi service.

- **Maximum offline period**

  Why use this policy: Use this policy as an extra security option. The policy makes sure that users who run an app offline for a specified duration must reconfirm app entitlement and refresh policies.

  User example: If you configure an MDX app with a Maximum offline period, the user can open and use the app offline until the offline timer period expires. At that point, the user must connect back to the network via cellular or Wi-Fi service and reauthenticate, if prompted.

Miscellaneous access policies

- **App update grace period (hours)**

  Why use this policy: The app update grace period is the time available to the user before they must update an app that has a newer version available in the app store. At the point of expiry, the user must update the app before they can gain access to the data in the app. When setting this value, keep in mind the needs of your mobile workforce, particularly users who might experience long periods offline when traveling internationally.

  User example: You load a new version of Citrix Secure Mail in the app store and then set an app update grace period of 6 hours. Citrix Secure Hub users then have 6 hours to upgrade Citrix Secure Mail before they are routed to the app store.

- **Active poll period (minutes)**

  Why use this policy: The active poll period is the interval at which Citrix Endpoint Management checks apps for when to do security actions, such as App Lock and App Wipe.

  User example: If you set the Active poll period policy to 60 minutes and then send the App Lock command, the lock occurs within 60 minutes of the last poll.

Non-compliant device behavior policies

When a device falls below the minimum compliance requirements, the Non-compliant device behavior policy allows you to select the action to take. For information, see Non-compliant device behavior.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App interaction policies

Why use these policies: Use App Interaction policies to control the flow of documents and data from MDX apps to other apps on the device. For example, you can prevent a user from:

- moving data to their personal apps outside of the container
- pasting data from outside the container into the containerized apps

User example: You set an App interaction policy to Restricted, which means a user can copy text from Citrix Secure Mail to Citrix Secure Web. The user can't copy that data to their personal Safari or Chrome browser that is outside the container. Also, a user can open an attached document from Citrix Secure Mail into Citrix Files or QuickEdit. The user can't open the attached document in their own personal file viewing apps that are outside the container.

App Restrictions policies

Why use these policies: Use App Restriction policies to control what features users can access from an MDX app while it is open. The restrictions help to make sure that no malicious activity can take place while the app is running. The App Restriction policies vary slightly between iOS and Android. For example, in iOS you can block access to iCloud while the MDX app is running. In Android, you can stop NFC use while the MDX app is running.

User example: Suppose that you enable the App Restriction policy to block dictation on iOS in an MDX app. As a result, the user can't use the dictate function on the iOS keyboard while the MDX app is running. So, the data that users dictate isn't passed to the unsecure third-party cloud dictation service. When the user opens their personal app outside of the container, the dictate option stays available to the user for their personal communications.

App Network Access policies

Why use these policies: Use the App Network Access policies to provide access from an MDX app in the container on the device to data sitting inside your corporate network. The Tunneled - Web SSO option allows only the tunneling of HTTP and HTTPS traffic. That option provides single sign-on (SSO) for HTTP and HTTPS traffic and PKINIT authentication.

User example: When a user opens an MDX app that has tunneling enabled, the browser opens an intranet site without requiring the user to start a VPN. The app automatically accesses the internal site using the micro VPN technology.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App Geolocation and Geofencing policies

Why use these policies: The policies that control app geolocation and geofencing include center point longitude, center point latitude, and radius. Those policies have access to the data in the MDX apps to a specific geographical area. The policies define a geographic area by a radius of latitude and longitude coordinates. If a user tries to use an app outside of the defined radius, the app stays locked and the user can't access the app data.

User example: A user can access merger and acquisition data while they are in their office location. When they move outside of their office location, this sensitive data becomes inaccessible.

Citrix Secure Mail App policies

- **Background network services**

  Why use this policy: Background network services in Citrix Secure Mail use the Secure Ticket Authority (STA), which is effectively a SOCKS5 proxy to connect through NetScaler Gateway. STA supports long-lived connections and provides better battery life compared to micro VPN. So, STA is ideal for mail that connects constantly. Citrix recommends that you configure these settings for Citrix Secure Mail. The NetScaler for XenMobile wizard automatically sets up STA for Citrix Secure Mail.

  User example: When STA isn't enabled and an Android user opens Citrix Secure Mail, they are prompted to open a VPN, which stays open on the device. When STA is enabled and the Android user opens Citrix Secure Mail, Citrix Secure Mail connects seamlessly with no VPN required.

- **Default sync interval**

  Why use this policy: This setting specifies the default days of email that synchronize to Citrix Secure Mail when the user accesses Citrix Secure Mail for the first time. Two weeks of email take longer to sync than three days of email. More data to sync prolongs the setup process for the user.

  User example: Suppose that the default sync interval is set to three days when the user first sets up Citrix Secure Mail. The user can see any emails in their Inbox that they received from the present to three days in the past. If a user wants to see emails that are older than three days, they can do a search. Citrix Secure Mail then shows the older emails stored on the server. After installing Citrix Secure Mail, each user can change this setting to better suit their needs.

Device policies and use case behavior

Device policies, sometimes referred to as MDM policies, determine how Citrix Endpoint Management manages devices. Although many policies are common to all devices, each device has a set of policies

© 1997–2025 Citrix Systems, Inc. All rights reserved.

specific to its operating system. The following list includes some of the device policies and discusses how you might use them. For a list of all device policies, see the article under Device policies.

- **App inventory policy**

  Why use this policy: To see the apps installed by a user, deploy the App inventory policy to a device. If you don't deploy the policy, you can see only the apps that a user installed from the app store, not personally installed apps. Use the App inventory policy to block certain apps from running on corporate devices.

  User example: A user with an MDM-managed device cannot disable this functionality. The user's personally installed applications are visible to Citrix Endpoint Management administrators.

- **App lock policy**

  Why use this policy: The App Lock policy, for Android, allows you to place apps on an allow list or block list. For example, for allowed apps you can configure a kiosk device. Typically, you deploy the App lock policy only to corporate-owned devices, because it limits the apps that users can install. You can set an override password to provide user access to blocked apps.

  User example: Suppose that you deploy an App lock policy that blocks the Angry Birds app. The user can install the Angry Birds app from Google Play, yet when they open the app a message advises them that their administrator blocked the app.

- **Connection scheduling policy**

  Why use this policy: The Connection scheduling policy enables Windows Mobile devices to connect back to Citrix Endpoint Management for MDM management, app push, and policy deployment. For Android and Android Enterprise devices, use Google Firebase Cloud Messaging (FCM) instead. FCM controls connections to Citrix Endpoint Management. The Scheduling options are as follows:

  - **Never:** Connect manually. Users must start the connection from Citrix Endpoint Management on their devices. Citrix doesn't recommend this option for production deployments because it prevents you from deploying security policies to devices. As a result, users don't receive new apps or policies. The **Never** option is enabled by default.
  - **Every:** Connects at the chosen interval. When you send a security policy, such as a lock or a wipe, Citrix Endpoint Management processes the policy on the device the next time the device connects.
  - **Define schedule:** Citrix Endpoint Management tries to reconnect the user's device to the Citrix Endpoint Management server after a network connection loss. Citrix Endpoint Management monitors the connection by transmitting control packets at regular intervals within the timeframe that you define.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

User example: You want to deploy a passcode policy to enrolled devices. The scheduling policy makes sure that the devices connect back to the server at a regular interval to collect the new policy.

- **Credentials Policy**

  Why use this policy: Often used with a network policy, the Credentials policy lets you deploy certificates for authentication to internal resources that require certificate authentication.

  User example: You deploy a network policy that configures a wireless network on the device. The Wi-Fi network requires a certificate for authentication. The Credentials policy deploys a certificate that is then stored in the operating system keystore. The user can then select the certificate when connected to the internal resource.

- **Exchange policy**

  Why use this policy: With Citrix Endpoint Management, you have two options to deliver Microsoft Exchange ActiveSync email.

  - **Citrix Secure Mail app:** Deliver email by using the Citrix Secure Mail app that you distribute from the public app store or the app store.
  - **Native email app:** Enable ActiveSync email for the native email client on the device. You can use macros to populate the user data from their Active Directory attributes, such as `${ user.username }` to populate the user name and `${ user.domain }` to populate the user domain.

  User example: When you push the Exchange policy, you send Exchange Server details to the device. Citrix Secure Hub then prompts the user to authenticate and their email begins to sync.

- **Location policy**

  Why use this policy: The Location policy lets you geolocate devices on a map, if the device has GPS enabled for Citrix Secure Hub. After you deploy this policy and then send a locate command from Citrix Endpoint Management, the device responds back with the location coordinates.

  User example: When you deploy the Location policy and GPS is enabled on the device: If users misplace their device, they can log on to the Citrix Endpoint Management Self-Help Portal and choose the locate option to see their device location on a map. A user chooses whether to allow Citrix Secure Hub to use location services. You cannot enforce the use of location services when users enroll a device themselves. Another consideration for using this policy is the effect on battery life.

- **Passcode policy**

  Why use this policy: The passcode policy allows you to enforce a PIN code or password on a managed device. This passcode policy allows you to set the complexity and time-outs for the passcode on the device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

User example: When you deploy a passcode policy to a managed device, Citrix Secure Hub prompts the user to configure a passcode or PIN. The passcode or PIN gives the user access to their device during start-up or when the inactivity timer expires.

- **Profile removal policy**

  Why use this policy: Suppose that you deploy a policy to a group of users and later must remove that policy from a subset of the users. You can remove the policy for selected users by creating a Profile removal policy. Then, use the deployment rules to deploy the Profile removal policy only to specified users.

  User example: When you deploy a Profile removal policy to user devices, users might not notice the change. For example, if the Profile removal policy removes a restriction that disabled the device camera, the user doesn't know about the change. Consider letting users know when changes affect their user experience.

- **Restrictions policy**

  Why use this policy: The restriction policy gives you many options to lock down and control features and functionality on the managed device. You can enable hundreds of restriction options for supported devices. For example, you can: disable the camera or microphone on a device, enforce roaming rules, and enforce access to third-party services like app stores.

  User example: If you deploy a restriction to an iOS device, the user might not be able to access iCloud or the Apple App Store.

- **Terms and conditions policy**

  Why use this policy: It might be necessary to advise users of the legal implications of having their device managed. Also, you might want to make sure that users are aware of the security risks when corporate data is pushed to the device. The Terms and Conditions document allows you to publish rules and notices before the user enrolls.

  User example: A user sees the Terms and Conditions information during the enrollment process. If they decline to accept the conditions stated, the enrollment process ends and they cannot access corporate data. You can generate a report to provide to HR/Legal/Compliance teams to show who accepted or declined the terms.

- **VPN policy**

  Why use this policy: Use the VPN policy to provide access to back-end systems using older VPN Gateway technology. The policy supports various VPN providers, including Cisco AnyConnect, Juniper, and Citrix VPN. It is also possible to link this policy to a CA and enabled VPN on-demand, if the VPN gateway supports this option.

  User example: With the VPN policy enabled, a user's device opens a VPN connection when the user accesses an internal domain.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Web clip policy**

  Why use this policy: Use the Web clip policy if you want to push to devices an icon that opens directly to a website. A web clip has a link to a website and can include a custom icon. On a device a web clip looks like an app icon.

  User example: A user can click a web clip icon to open an internet site to gain access to needed services. Using a web link is more convenient than typing a link address in a browser.

- **Network policy**

  Why use this policy: The network policy lets you deploy Wi-Fi network details, such as the SSID, authentication data, and configuration data, to a managed device.

  User example: When you deploy the network policy, the device automatically connects to the Wi-Fi network and authenticates the user so they can gain access to the network.

- **Endpoint Management Store policy**

  Why use this policy: The app store is a unified app store where administrators can publish all the corporate apps and data resources needed by their users. An administrator can add:

  - Web apps, SaaS apps, and MAM SDK enabled apps or MDX-wrapped apps
  - Citrix mobile productivity apps
  - Native mobile apps such as .ipa or .apk files
  - Apple App Store and Google Play apps
  - Web links
  - Citrix Virtual Apps published using Citrix StoreFront

  User example: After a user enrolls their device into Citrix Endpoint Management, they access the app store through the Citrix Secure Hub app. The user can then see all the corporate apps and services available to them. Users can click an app to install it, access the data, rate and review the app, and download app updates from the app store.

Client properties

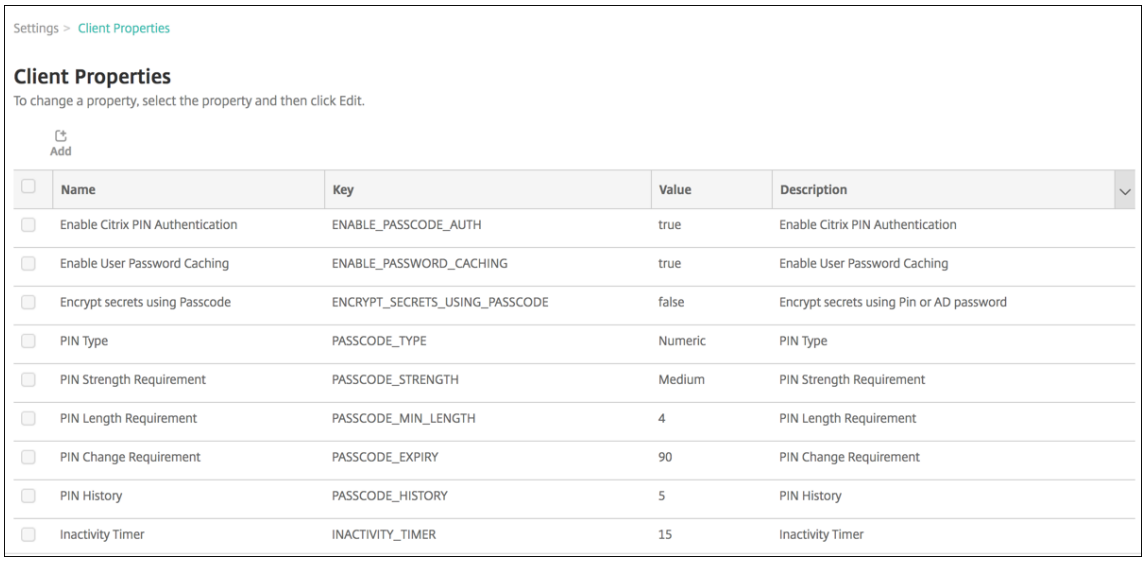
September 6, 2025

Client properties have information that is provided directly to Citrix Secure Hub on user devices. You can use these properties to configure advanced settings, such as the Citrix PIN. You can get client properties from Citrix support.

Client properties are subject to change with every release of Citrix Secure Hub and occasionally for client apps. For details about more commonly configured client properties, see Client property reference, later in this article.

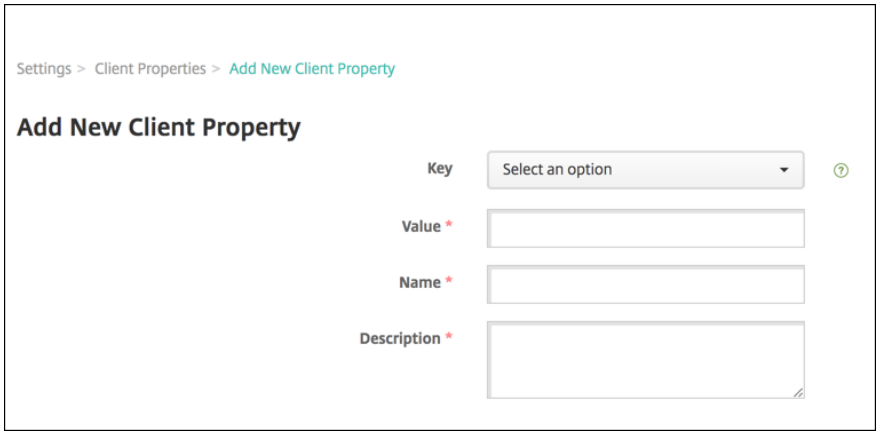
© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. In the Citrix Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Under **Client**, click **Client Properties**. The **Client Properties** page appears. You can add, edit, and delete client properties from this page.



To add a client property

1. Click **Add**. The **Add New Client Property** page appears.



2. Configure these settings:

   - **Key:** Click the property key that you want to add from the drop-down list. **Important:** Contact Citrix Support before updating the settings. You can request a special key.
   - **Value:** The value of the selected property.
   - **Name:** A name for the property.
   - **Description:** A description of the property.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

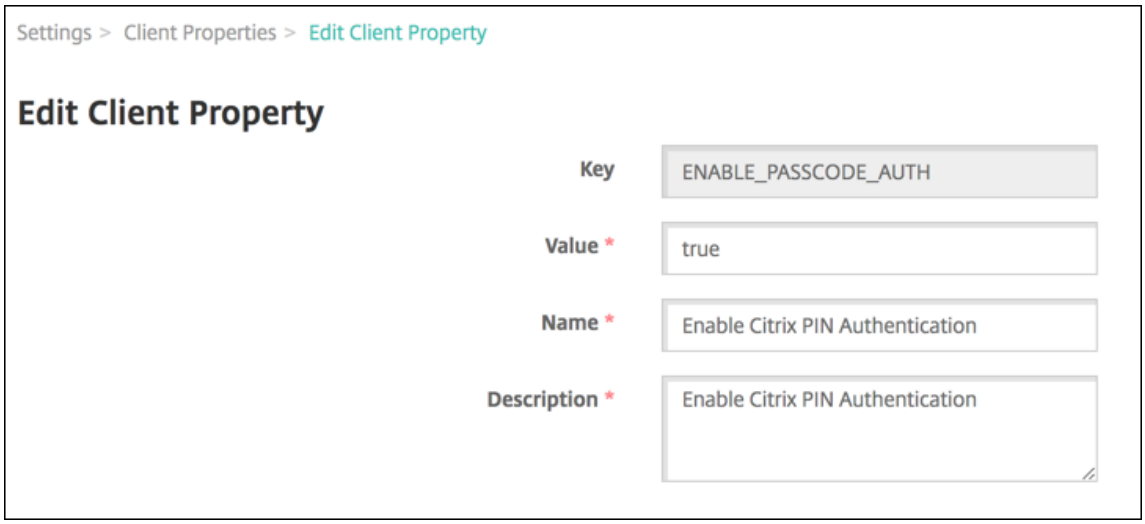
3. Click **Save**.

To edit a client property

1. In the **Client Properties** table, select the client property you want to edit.

   Select the checkbox next to a client property to open the options menu above the client property list. Click anywhere else in the list to open the options menu on the right side of the listing.

2. Click **Edit**. The **Edit Client Property** page appears.



3. Change the following information as appropriate:

   - **Key:** You cannot change this field.
   - **Value:** The property value.
   - **Name:** The property name.
   - **Description:** The property description.

4. Click **Save** to save your changes or **Cancel** to leave the property unchanged.

To delete a client property

1. In the **Client Properties** table, select the client property you want to delete.

   You can select more than one property to delete by selecting the checkbox next to each property.

2. Click **Delete**. A confirmation dialog box appears. Click **Delete** again.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Client property reference

The predefined client properties and their default settings for Citrix Endpoint Management are as follows:

- **ALLOW_CLIENTSIDE_PROXY**
  - Display name: ALLOW_CLIENTSIDE_PROXY
  - If your users want to use a proxy they've configured on their iOS phones, leave this custom policy set to the default value **true**.

    Some users might already have a proxy configured in **Settings > Wi-Fi > Configure Proxy** on their devices. If Citrix Secure Hub doesn't open for those users, do one of the following actions:

    * Remove the proxy configuration from the device and then restart Citrix Secure Hub.
    * Connect the device to another Wi-Fi network. After Citrix Secure Hub re-authenticates, it gets the **ALLOW_CLIENTSIDE_PROXY** property and opens.
  - If **ALLOW_CLIENTSIDE_PROXY** is **false** and users configure a proxy on their device, Citrix Endpoint Management detects the proxy. However, Citrix Secure Hub doesn't use the proxy and displays an error message. If a device connects to an access point or router that has a proxy enabled, Citrix Endpoint Management doesn't detect the proxy. For the highest security, we recommend that you use certificate pinning. For information about enabling certificate pinning for Citrix Secure Hub, see Certificate pinning.
  - To configure this custom client policy, go to **Settings > Client Properties**, add the custom key **ALLOW_CLIENTSIDE_PROXY**, and set the **Value**.
- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - Display name: MDX Container Self-Destruct Period
  - Self-destruct prevents access to Citrix Secure Hub and managed apps, after a specified number of days of inactivity. After the time limit, apps are no longer usable. Wiping the data includes clearing the app data for each installed app, including the app cache and user data.

    The inactivity time is when the server doesn't receive an authentication request to validate the user over a specific length of time. Suppose that this property is 30 days. If the user doesn't use the app for more than 30 days, the policy takes effect.

    This global security policy applies to iOS and Android platforms and is an enhancement of the existing app lock and wipe policies.
  - To configure this global policy, go to **Settings > Client Properties** and add the custom key **CONTAINER_SELF_DESTRUCT_PERIOD**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - Value: Number of days

- **DEVICE_LOGS_TO_IT_HELP_DESK**

  - Display name: Send device logs to IT help desk
  - This property enables or disables the ability to send logs to the IT help desk.
  - Possible values: **true** or **false**
  - Default value: **false**

- **DISABLE_LOGGING**

  - Display name: Disable Logging

  - Use this property to prevent users from collecting and uploading logs from their devices. This property disables logging for Citrix Secure Hub and for all installed MDX apps. Users can't send logs for any app from the Support page. Even though the mail composition dialog box appears, the logs aren't attached. A message indicates that logging is disabled. This setting also prevents you from updating log settings in the Citrix Endpoint Management console for Citrix Secure Hub and MDX apps.

    When this property is set to **true**, Citrix Secure Hub sets **Block application logs** to **true**. As a result, MDX apps stop logging when the new policy is applied.

  - Possible values: **true** or **false**

  - Default value: **false** (logging is not disabled)

- **ENABLE_CRASH_REPORTING**

  - Display name: Enable Crash Reporting
  - If **true**, Citrix collects crash reports and diagnostics to help troubleshoot issues with Citrix Secure Hub for iOS and Android. If **false**, no data is collected.
  - Possible values: **true** or **false**
  - Default value: **true**

- **ENABLE_CREDENTIAL_STORE**

  - Display name: Enable Credential Store
  - Enabling the credential store means that Android or iOS users enter their password one time when accessing Citrix mobile productivity apps. You can use the credential store whether you enable Citrix PIN. If you don't enable Citrix PIN, users enter their Active Directory password. Citrix Endpoint Management supports the use of Active Directory passwords with the credential store only for Citrix Secure Hub and public store apps. If you use Active Directory passwords with the credential store, Citrix Endpoint Management doesn't support PKI authentication.
  - Automatic enrollment in Citrix Secure Mail requires that you set this property to **true**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - To configure this custom client policy, go to **Settings > Client Properties**, add the custom key **ENABLE_CREDENTIAL_STORE**, and set the **Value** to **true**.

- **ENABLE_PASSCODE_AUTH**
  - Display name: Enable Citrix PIN Authentication
  - This property allows you to turn on Citrix PIN functionality. With the Citrix PIN or passcode, users are prompted to define a PIN to use instead of their Active Directory password. This setting is automatically enabled when ENABLE_PASSWORD_CACHING is enabled or when Citrix Endpoint Management is using certificate authentication.

    For offline authentication, the Citrix PIN is validated locally and users are allowed to access the app or content they requested. For online authentication, the Citrix PIN or passcode unlocks the Active Directory password or certificate, which is then sent to authenticate with Citrix Endpoint Management.

    If ENABLE_PASSCODE_AUTH is true and ENABLE_PASSWORD_CACHING is false, online authentication always prompts for the password because Citrix Secure Hub doesn't save it.
  - Possible values: **true** or **false**
  - Default value: **false**

- **ENABLE_PASSWORD_CACHING**
  - Display name: Enable User Password Caching
  - This property enables Active Directory passwords to cache locally on the mobile device. When you set this property to **true**, you must also set the **ENABLE_PASSCODE_AUTH** property to **true**. With user password caching enabled, Citrix Endpoint Management prompts users to set a Citrix PIN or passcode.
  - Possible values: **true** or **false**
  - Default value: **false**

- **ENABLE_TOUCH_ID_AUTH**
  - Display name: Enable Touch ID Authentication
  - For devices that support Touch ID authentication, this property enables or disables Touch ID authentication on the device. Requirements:

    User devices must have Citrix PIN or LDAP enabled. If LDAP authentication is off (for example, because only certificate-based authentication is used), users must set a Citrix PIN. In this case, Citrix Endpoint Management requires the Citrix PIN even if the client property **ENABLE_PASSCODE_AUTH** is **false**.

    Set **ENABLE_PASSCODE_AUTH** to **false** so that when users launch an app, they must respond to a prompt to use Touch ID.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - Possible values: **true** or **false**
  - Default value: **false**

- **ENABLE_WORXHOME_CEIP**
  - Display name: Enable Citrix Secure Hub CEIP
  - This property turns on the Customer Experience Improvement Program. That feature sends anonymous configuration and usage data to Citrix periodically. The data helps Citrix improve the quality, reliability, and performance of Citrix Endpoint Management.
  - Value: **true** or **false**
  - Default value: **false**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - Display name: Encrypt secrets using Passcode
  - This property stores sensitive data on the device in a secret vault instead of in a platform-based native store, such as the iOS keychain. This property enables strong encryption of key artifacts and adds user entropy. User entropy is a user-generated random PIN code that only the user knows.

    Citrix recommends that you enable this property to help provide higher security on user devices. As a result, users experience more authentication prompts for the Citrix PIN.
  - Possible values: **true** or **false**
  - Default value: **false**

- **INACTIVITY_TIMER**
  - Display name: Inactivity Timer
  - This property defines how long users can leave their device inactive and then access an app without a prompt for a Citrix PIN or passcode. To enable this setting for an MDX app, set the App Passcode setting to On. If the App Passcode setting is set to Off, users are redirected to Citrix Secure Hub to do a full authentication. When you change this setting, the value takes effect the next time that users are prompted to authenticate.

    On iOS, the Inactivity Timer also governs access to Citrix Secure Hub for MDX and non-MDX apps.
  - Possible values: Any positive integer
  - Default value: **15** (minutes)

- **ON_FAILURE_USE_EMAIL**
  - Display name: On failure Use Email to Send device logs to the IT help desk

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - This property enables or disables the ability to use email to send device logs to IT.
  - Possible values: **true** or **false**
  - Default value: **true**

- **PASSCODE_EXPIRY**

  - Display name: PIN Change Requirement
  - This property defines how long the Citrix PIN or passcode is valid, after which the user is forced to change their Citrix PIN or passcode. When you change this setting, the new value is set only when the current Citrix PIN or passcode expires.
  - Possible values: **1** through **99** recommended. To eliminate PIN resets, set the value to a high number (for example, 100,000,000,000). If you originally set the expiry period to between 1 and 99 days and then change to the large number during that period: PINs still expire at the end of the initial period, but never again afterward.
  - Default value: **90** (days)

- **PASSCODE_HISTORY**

  - Display name: PIN History
  - This property defines the number of previously used Citrix PINs or passcodes that users cannot reuse when changing their Citrix PIN or passcode. When you change this setting, the new value is set the next time that users reset their Citrix PIN or passcode.
  - Possible values: **1** through **99**
  - Default value: **5**

- **PASSCODE_MAX_ATTEMPTS**

  - Display name: PIN Attempts
  - This property defines how many wrong Citrix PIN or passcode attempts users can make before being prompted for full authentication. After users successfully do a full authentication, they are prompted to create a Citrix PIN or passcode.
  - Possible values: Any positive integer
  - Default value: **15**

- **PASSCODE_MIN_LENGTH**

  - Display name: PIN Length Requirement
  - This property defines the minimum length of Citrix PINs.
  - Possible values: **4** through **10**
  - Default value: **6**

- **PASSCODE_STRENGTH**

  - Display name: PIN Strength Requirement

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- This property defines the strength of a Citrix PIN or passcode. When you change this setting, users are prompted to create a Citrix PIN or passcode the next time they are prompted to authenticate.
- Possible values: **Low**, **Medium**, **High**, or **Strong**
- Default value: **Medium**
- The password rules for each strength setting based on the PASSCODE_TYPE setting are as follows:

Rules for numeric passcodes:

Passcode strength	Rules for numeric passcode type	Allowed	Not allowed
Low	All numbers, any sequences allowed	444444, 123456, 654321	
Medium (default setting)	All numbers cannot be the same or consecutive.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
High	Adjacent numbers cannot be the same.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
Strong	Do not use the same number more than twice. Do not use three or more consecutive numbers in a row. Do not use three or more consecutive numbers in the reverse order.	102983, 085085, 824673, 132312	132132, 131313, 902030

Rules for alphanumeric passcodes:

Passcode strength	Rules for alphanumeric passcode type	Allowed	Not allowed
Low	Must have at least one number and one letter	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Passcode strength	Rules for alphanumeric passcode type	Allowed	Not allowed
Medium (default setting)	In addition to the rules for Low passcode strength, letters and all numbers cannot be the same. Letters cannot be consecutive and numbers cannot be consecutive.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, or aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, or cba123
High	Include at least one capital letter and one small letter.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Strong	Include at least one number, one special symbol, one capital letter, and one small letter.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

- **PASSCODE_TYPE**
  - Display name: PIN Type
  - This property defines whether users can define a numerical Citrix PIN or an alphanumeric passcode. When you select **Numeric**, users can use numbers only (Citrix PIN). When you select **Alphanumeric**, users can use a combination of letters and numbers (passcode).

    If you change this setting, users must set a new Citrix PIN or passcode the next time that they are prompted to authenticate.
  - Possible values: **Numeric** or **Alphanumeric**
  - Default value: **Numeric**
- **REFRESHINTERVAL**
  - Display name: REFRESHINTERVAL
  - By default, Citrix Endpoint Management pings the AutoDiscovery Server (ADS) for pinned certificates every 3 days. To change the refresh interval, go to **Settings > Client Properties**, add the custom key **REFRESHINTERVAL**, and set the **Value** to the number of hours.
  - Default value: **72** hours (3 days)
- **SEND_LDAP_ATTRIBUTES**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - For MAM-only deployments of Android, iOS, or macOS devices: You can configure Citrix Endpoint Management so that users who enroll in Citrix Secure Hub with email credentials are automatically enrolled in Citrix Secure Mail. As a result, users don't provide extra information or take extra steps to enroll in Citrix Secure Mail.
  - To configure this global client policy, go to **Settings > Client Properties**, add the custom key **SEND_LDAP_ATTRIBUTES**, and set the **Value** as follows.
  - Value: `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme =${ user.samaccountname } , displayName=${ user.displayName } ,mail=${ user.mail }`
  - The attribute values are specified as macros, similar to MDM policies.
  - Here is a sample account service response for this property:

    ```
    <property value="userPrincipalName=user@site.com,sAMAccountName
    =eng1,displayName=user\,test1,email=user@site.com\,user@site.
    com"name="SEND_LDAP_ATTRIBUTES"/>
    ```

  - For this property, Citrix Endpoint Management treats comma characters as string terminators. So, if an attribute value includes a comma, precede it with a backslash. The backslash prevents the client from interpreting the embedded comma as the end of the attribute value. Represent backslash characters with `"\\"`.

- **HIDE_THREE_FINGER_TAP_MENU**
  - When this property is not set or is set to **false**, users can access the hidden features menu by doing a three-finger tap on their devices. The hidden features menu allowed users to reset application data. Setting this property to **true** disables users access to the hidden features menu.
  - To configure this global client policy, go to **Settings > Client Properties**, add the custom key **HIDE_THREE_FINGER_TAP_MENU** and set the **Value**.

- **TUNNEL_EXCLUDE_DOMAINS**
  - Display name: Tunnel Exclude Domains
  - By default, MDX excludes from micro VPN tunneling some service endpoints that Mobile Apps SDKs and apps use for various features. For example, those endpoints include services that don't require routing through enterprise networks, such as Google Analytics, Citrix Cloud™ services, and Active Directory services. Use this client property to add additional domains to the list of domains excluded.
  - To configure this global client policy, go to **Settings > Client Properties**, add the custom key **TUNNEL_EXCLUDE_DOMAINS**, and set the **Value**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - Value: The additional domains that you want to exclude from tunneling, type a comma-separated list of domain suffixes. For example:

    ```
    app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,
    cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics
    .com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.
    com, hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.
    com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.
    com,ssl.google-analytics.com,stream.launchdarkly.com,features
    .netscalergatewaystaging.net,features.netscalergateway.net
    ```

The custom client properties for Citrix Endpoint Management are as follows:

ENABLE_MAM_NFACTOR_SSO:

- This property allows you to enable or disable the MAM nFactor SSO during the MAM enrollment or login for Secure Hub while using the advanced authentication policy in the NetScaler® Gateway. If the value is set to **true**, then the MAM nFactor SSO is enabled during the MAM enrollment or login for Secure Hub.
- To configure this property, go to **Settings > Client Properties** and click **Add**. Select **Custom Key** in the **Key** drop-down menu and update the following information as appropriate:
  - Key - ENABLE_MAM_NFACTOR_SSO
  - Value - true or false
  - Name - ENABLE_MAM_NFACTOR_SSO
  - Description - Add the relevant description

User enrollment options

September 6, 2025

You can have users enroll their devices in Citrix Endpoint Management in several ways. Before considering the specifics, decide which devices you want to enroll in MDM+MAM, MDM, or MAM. For more information about those management modes, see Management modes.

At the highest level, there are four enrollment options:

- **Enrollment Invitation:** Send an enrollment invitation or invitation URL to users. Enrollment invitations and URLs aren't available for Windows devices.
- **Self-Help Portal:** Set up a portal that users can visit to download Citrix Secure Hub, request enrollment, and view device information.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Manual Enrollment:** Send out an email, handbook, or some other communication letting users know that the system is up and that they can enroll. Users then download Citrix Secure Hub and enroll their devices manually.
- **Enterprise:** Another option for device enrollment is through an Apple Deployment Program and Google Android Enterprise. Through each of these programs, you can buy devices that are pre-configured and ready for employees to use. For more information, see Apple Deployment Program articles in Apple Support and Google Android Enterprise documentation on the Android Enterprise website.

Enrollment Invitation

You can email an enrollment invitation to users with iOS, macOS, Android Enterprise, and legacy Android devices. Enrollment invitations aren't available for Windows devices.

You can also send an installation link through SMTP to users with iOS, macOS, Android Enterprise, Android, or Windows devices. For more information, see Enroll devices.

If you choose to use the enrollment invitation method, you can:

- Choose **Invitation URL**, **Invitation URL + PIN**, or **Invitation URL + Password** enrollment security modes.
- Use any combination of the modes.
- Enable or disable the modes from the Citrix Endpoint Management **Settings** page.

For information on each enrollment security mode, see Configure enrollment security modes.

Invitations serve many purposes. The most common use of invitations is to notify users that the system is available, and that they can enroll. Invitation URLs are unique. After a user uses an invitation URL, the URL is no longer available. You can use this property to limit the users or devices enrolling to your system.

When configuring an enrollment profile, you can control the number of devices specific users can enroll, based on Active Directory groups. For example, you might allow your Finance division only one device per user.

Be aware of the extra costs and pitfalls of certain enrollment options. To send invitations using SMTP requires extra infrastructure. For more information on this option, see Notifications.

Also, to send invitations by email, male sure that users have a way of accessing email outside of Citrix Secure Hub. You can use one-time password (OTP) enrollment security modes as an alternative to Active Directory passwords for MDM enrollment.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Self-Help Portal

The Self-Help Portal can be accessed at the same URL that admins use to access the Citrix Endpoint Management console. End users see the Self-Help Portal instead of the admin console. Users can download Citrix Secure Hub, request enrollment, and view device information in the Self-Help Portal.

To set up a portal, update these server properties in **Settings > Server Properties**:

- `shp.console.enable`: Set to **True** to provide access to the Self-Help Portal.
- `enable.new.shp`: Set to **True** to allow users to enable their devices from the Self-Help Portal.

Manual Enrollment

With manual enrollment, users connect to Citrix Endpoint Management either through AutoDiscovery or by entering the server information. With AutoDiscovery, users log on with only their email address or Active Directory credentials in User Principal Name format. Without AutoDiscovery, they must enter the server address and their Active Directory credentials. For more information about setting up AutoDiscovery, see Setup Citrix Endpoint Management AutoDiscovery service.

You can facilitate manual enrollment in several ways. You can create a guide, distribute it to users, and have them enroll themselves. You can have your IT department manually enroll groups of users in certain time slots. You can use any similar method where users must enter their credentials or server information.

User Onboarding

After you have your environment set up, you need to decide how to get users into your environment. An earlier section in this article discusses the specifics of user enrollment security modes. This section discusses the way that you reach out to users.

Open Enrollment versus Selective Invitation

When onboarding users, you can allow enrollment through two basic methods:

- Open enrollment. By default, any user with LDAP credentials and the Citrix Endpoint Management environment information can enroll.
- Limited enrollment. You can limit the number of users by only allowing users with invitations to enroll. You can also limit open enrollment by an Active Directory group.

With the invitation method, you can also limit the number of devices a user can enroll. In most situations, open enrollment is acceptable, but there are a few things to consider:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- For MAM enrollment, you can easily limit open enrollment through Active Directory group membership.
- For MDM enrollment, you can limit the number of devices that can enroll based on Active Directory group membership. If you only allow corporate devices in your environment, that limitation typically isn't an issue. You might want to consider this method, however, in a BYOD workplace if you want to limit the number of devices in your environment.

Selective invitation is typically done less often because it requires a bit more work than open enrollment. For users to enroll their devices in your environment, you must send an invitation unique to each user. For information on how to send an enrollment invitation, see Enrollment invitations.

Send an invitation for each user or group whom you want enrolled in your environment. That process can take a long time depending on the size of your organization. It is possible to use Active Directory groups to create invitations in batches, but you must carry out this approach in waves.

First Contact with Users

After deciding whether to use open enrollment or selective invitation and you set up those environments, inform users about their enrollment options.

If you use the selective invitation method, email messages are a part of the process. You can send emails through the Citrix Endpoint Management console for open enrollment as well. For details, see Enrollment invitations.

In either case, keep in mind that for email, you need an SMTP server. Those servers might be an extra cost to consider when making your decision. Consider how you expect new users to access information. If you want all users to access their email through Citrix Endpoint Management, sending them an invitation email might be problematic.

You can also send communications by another means outside of Citrix Endpoint Management for an open enrollment environment. For that option, be sure to include all the relevant information. Let users know where they can get the Citrix Secure Hub app and what method to use to enroll. If you have discovery turned off, also provide users the Citrix Endpoint Management server address. To learn more about discovery, see Setup Citrix Endpoint Management AutoDiscovery service.

App provisioning and deprovisioning

September 6, 2025

Application provisioning revolves around mobile app lifecycle management: Preparing, configuring, delivering, and managing mobile apps within the Citrix Endpoint Management environment. Sometimes, developing or modifying application code might also be part of the provisioning process. Citrix

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Endpoint Management is equipped with various tools and processes that you can use for app provisioning.

Before reading this article on app provisioning, we recommend you read Apps and User communities. When you have finalized the type of apps your organization plans to deliver to users, you can then outline the process for managing the apps throughout their lifecycle.

Consider the following points when defining your app provisioning process:

- **App profiling:** Your organization might start with a limited number of apps. However, the number of apps you manage can rapidly increase as user adoption rates increase and your environment grows. Define specific app profiles up front to make app provisioning easy to manage. App profiling helps you categorize apps into logical groups from a nontechnical perspective. For example, you can create app profiles based on the following factors:
  - Version: App version for tracking
  - Instances: Many instances that are deployed for different sets of users, for example, with different levels of access
  - Platform: iOS, Android, or Windows
  - Target Audience: Standard users, departments, C-level executives
  - Ownership: Department that owns the app
  - Type: MDX, Public, Web and SaaS, or Web links
  - Upgrade Cycle: How often the app is upgraded
  - Licensing: Licensing requirements and ownership
  - MAM SDK or MDX policies: To apply MDX capabilities to your mobile apps
  - Network Access: Type of access, such as tunneling HTTP and HTTPS traffic with single sign-on (Tunneled - Web SSO).

Example:

Factor	Citrix Secure Mail	Mail	In-House	Epic Rover
Version	10.1	10.1	X.x	X.x
Instance	VIP	Physicians	Clinical	Clinical
Platform	iOS	iOS	iOS	iOS
Target Users	VIP Users	Physicians	Clinical Users	Clinical Users
Ownership	IT	IT	IT	IT
Type	MDX	MDX	Native	Public
Upgrade Cycle	Quarterly	Quarterly	Yearly	N/A
Licensing	N/A	N/A	N/A	Volume Purchase

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Factor	Citrix Secure Mail	Mail	In-House	Epic Rover
MDX Policies	Yes	Yes	Yes	No
Network Access	VPN	VPN	VPN	Public

- **App versioning:** Maintaining and tracking app versions is a critical part of the provisioning process. Versioning is typically transparent to users. They only receive notifications when a new version of the app is available for download. From your perspective, reviewing and testing each app version in a non-production capacity is also critical to avoid impacting a production site.

  It is also important to evaluate if a specific upgrade is required. App upgrades are usually of two types: A minor upgrade, such as a fix to a specific bug, or a major release, which introduces significant changes. In either case, carefully review the Release Notes of the app to evaluate if the upgrade is necessary.

- **App development:** When you integrate the MAM SDK in the mobile apps that you develop, you apply MDX capabilities to those apps. See MAM SDK overview.

  The MAM SDK replaces the MDX Toolkit, which is scheduled for deprecation in July 2023. For information about app wrapping, see MDX Toolkit. The app provisioning process for a wrapped app differs from the provisioning process for a standard non-wrapped app.

- **App security:** You define the security requirements of individual apps or app profiles as part of the provisioning process. You can map security requirements to specific MDM or MAM policies before deploying the apps. That planning simplifies and speeds up app deployment. For example:

  - You might deploy certain apps differently.
  - You might want to make architectural changes to your Citrix Endpoint Management environment. The changes depend on the type of security compliance that the apps require. For example, a particular app might require end-to-end SSL encryption or geofencing.

- **App delivery:** Citrix Endpoint Management allows you to deliver apps as MDM apps or as MAM apps. The MDM apps appear in the app store. This store allows you to conveniently deliver public or native apps to users. Other than enforcing device level restrictions, no other app controls are needed. However, delivering apps by using MAM allows full control over app delivery and over the app itself. Delivering the apps through MAM is typically more suitable.

- **Application maintenance:**

  - Do an initial audit: Track the app version that is present in your production environment, and the last upgrade cycle. Make note of specific features or bug fixes that required the upgrade to take place.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - Establish baselines: Maintain a list of the latest stable releases of each app. Be ready to fall back to an earlier app version if unexpected issues occur after an upgrade. Develop a rollback plan. Test app upgrades in a test environment before deploying to production. If possible, deploy the upgrade to a subset of production users first and then to the entire user base.
  - Subscribe to Citrix® software update notifications and any third-party software vendor notifications: Keeping up to date with the latest releases of the apps is critical. An Early Access Release (EAR) build might be available for testing ahead of time.
  - Devise a strategy to notify users: Define a strategy to notify users when app upgrades are available. Prepare users with training before deployment. Consider sending multiple notifications before updating the app. Depending on the app, the best notification method might be email notifications or websites.

App lifecycle management involves the complete lifecycle of an app from its initial deployment through retirement. The lifecycle of an app has these phases:

1. Requirements for specifications: Start with business case and user requirements.
2. Development: Validate that the app meets business needs.
3. Testing: Identify test users, issues, and bugs.
4. Deployment: Deploy the app to production users.
5. Maintenance: Update app version. Deploy the app in a test environment before updating the app in a production environment.

Dashboard-based operations

February 23, 2024

You can view information at a glance by accessing your Citrix Endpoint Management console dashboard. With this information, you can see issues and successes quickly by using widgets.

The dashboard is usually the screen that appears when you first sign on to the Citrix Endpoint Management console. To access the dashboard from elsewhere in the console, click **Analyze**. Click **Customize** on the dashboard to edit the layout of the page and to edit the widgets that appear.

- **My Dashboards:** You can save up to four dashboards. You can edit these dashboards separately and view each one by selecting the saved dashboard.
- **Layout Style:** In this row, you can select how many widgets appear on your dashboard and how the widgets are laid out.
- **Widget Selection:** You can choose which information appears on your dashboard.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Notifications:** Mark the checkbox above the numbers on the left to add a Notifications bar above your widgets. This bar shows the number of compliant devices, inactive devices, and devices wiped or enrolled in the last 24 hours.
- **Devices By Platform:** Displays the number of managed and unmanaged devices by platform.
- **Devices By Carrier:** Displays the number of managed and unmanaged devices by carrier. Click each bar to see a breakdown by platform.
- **Managed Devices By Platform:** Displays the number of managed devices by platform.
- **Unmanaged Devices By Platform:** Displays the number of unmanaged devices by platform. Devices that appear in this chart might have an agent installed on them, but have had their privileges revoked or have been wiped.
- **Devices By ActiveSync Gateway Status:** Displays the number of devices grouped by ActiveSync Gateway status. The information shows Blocked, Allowed, or Unknown status. You can click each bar to break down the data by platform.
- **Devices By Ownership:** Displays the number of devices grouped by ownership status. The information shows corporate-owned, employee-owned, or unknown ownership status.
- **Failed Delivery Group Deployments:** Displays the total number of failed deployments per package. Only packages that have failed deployments appear.
- **Devices By Blocked Reason:** Displays the number of devices blocked by ActiveSync
- **Installed Apps:** By using this widget, you can type an app name, and a graph displays information about that app.
- **Volume Purchase Apps License Usage:** Displays license usage statistics for Apple Volume Purchase apps.

Use cases

Some examples for the many ways you can use dashboard widgets to monitor your environment are as follows.

- You have deployed Citrix mobile productivity apps and are receiving support tickets about mobile productivity apps failing to install on devices. Use the **Out of Compliance Devices** and **Installed Apps** widgets to see the devices that do not have Citrix mobile productivity apps installed.
- You want to monitor inactive devices so that you can remove the devices from your environment and reclaim licenses. Use the **Inactive Devices** widget to track this statistic.
- You are receiving support tickets concerning data not being synced properly. You might want to use the **Devices by ActiveSync Gateway Status** and **Devices By Blocked Reason** widgets to determine whether the issue is ActiveSync related.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Reporting

After your environment is set up and users enroll, you can run reports to learn about your deployment. Citrix Endpoint Management comes with various reports built in to help you get a better picture of the devices running on your environment. For details, see Reports.

Role-based access control and Citrix Endpoint Management support

February 23, 2024

Citrix Endpoint Management uses role-based access control (RBAC) to restrict user and group access to Citrix Endpoint Management system functions such as the Citrix Endpoint Management console, Self-Help Portal, and public API. This article describes the roles built in to Citrix Endpoint Management and includes considerations for deciding on a support model for Citrix Endpoint Management that uses RBAC.

Built-In roles

You can change the access granted to the following built-in roles and you can add roles. For the full set of access and feature permissions associated with each role and their default settings, download Role-Based Access Control Defaults. For a definition of each feature, see Configure roles with RBAC.

Admin role

Default access granted:

- Full system access except to the Self-Help Portal.
- By default, administrators can do some support tasks, such as check connectivity and create support bundles.

Considerations:

- Do some or all of your administrators need access to the Self-Help Portal? If so, you can edit the Admin role or add Admin roles.
- To restrict access further for some administrators or administrator groups, add roles based on the Admin template and edit the permissions.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

User

Default access granted:

- Access to the Self-Help Portal, which lets authenticated users generate enrollment links. The links allow them to enroll their devices or send themselves an enrollment invitation.
- Restricted access to the Citrix Endpoint Management console: device features (such as wipe, lock/unlock device; lock/unlock container; see location and set geographic restrictions; ring the device; reset container password); add, remove, and send enrollment invitations.

Considerations:

- The User role enables you to enable users to help themselves.
- To support shared devices, create a user role for shared device enrollment.

Considerations for a Citrix Endpoint Management support model

The support models that you can adopt can vary widely and might involve third parties who handle level 1 and 2 support while employees handle level 3 and 4 support. Regardless of how you distribute the support load, keep in mind the considerations in this section specific to your Citrix Endpoint Management deployment and user base.

Do users have corporate-owned or BYO devices?
The primary question that influences support is who owns the user devices in your Citrix Endpoint Management environment. If your users have corporate-owned devices, you might offer a lower level of support, as a way to lock down the devices. In that case, you might provide a help desk that assists users with device issues and how to use the devices. Depending on the types of devices you need to support, consider how you might use the RBAC Device Provisioning and Support roles for your help desk.

If your users have BYO devices, your organization might expect users to find their own sources for device support. In that case, the support your organization provides is more of an administrative role focused around Citrix Endpoint Management-specific issues.

What is your support model for desktops?
Consider whether your support model for desktops is appropriate for other corporate-owned devices. Can you use the same support organization? What extra training might they need?

Do you want to give users access to the Citrix Endpoint Management Self-Help Portal?
Although some organizations prefer not to grant users access to Citrix Endpoint Management, giving users some self-support capabilities can ease the load on your support organization. If the default User role for RBAC includes permissions that you don't want to grant, consider creating a role with only the permissions you want to include. You can create as many roles as needed to meet your requirements.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Support process

September 6, 2025

You can turn Citrix Technical Support Services to help with issues related to Citrix products. The group offers workarounds and resolutions and works hand in hand with development teams to offer solutions.

Citrix ConsultingSM Services or Citrix Education Services offer help related to product training, advising on product usage, configuration, installation, or environment design and architecture.

Citrix Consulting helps with the Citrix product-related projects including the following:

- Proof of concepts
- Economic impact assessment
- Infrastructure health checks
- Design requirements analysis
- Architecture design verification
- Integration
- Operational process development

Citrix EducationSM offers best-in-class IT training and certification on Citrix Virtualization, Cloud, and networking technologies.

Citrix recommends that you take full advantage of the Citrix Self-Help Resources and recommendations before creating a support case. For instance, there are several places where you can access articles and bulletins written by Citrix technical experts, see product documentation for Citrix solutions and technologies, or read straight talk from Citrix executives, product teams, and technical experts. See the Knowledge Center, Product documentation, and Blogs pages respectively.

For more interactive assistance, you can participate in discussion forums where you can ask questions and get real-world answers from other customers, share ideas, opinions, technical information, and best practices within user groups and interest groups, or interact with Citrix Support engineers who monitor Citrix Support social networking sites. See the Support Forums and Citrix Community pages respectively.

You also have access to training and certification courses to build your skills. See Citrix Education.

Citrix Insight Services provides a simple, online troubleshooting platform and health-checker for your Citrix environment. Available for Citrix Endpoint Management, Citrix Virtual Apps and Desktops, Citrix Hypervisor, and NetScaler Gateway. See Analysis Tool.

To seek technical support, you can create a support case either by phone or via the web. You can use the web for low- and medium-severity issues and use the phone option for high-severity issues. To contact support for Citrix Endpoint Management issues, see Citrix Support Services.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

If you seek a highly trained single point of contact with extensive experience delivering Citrix solutions, Citrix Services offers a Technical Relationship Manager. For more information about Citrix services offerings and benefits, see Citrix Worldwide Services.

Sending group enrollment invitations in Citrix Endpoint Management

September 6, 2025

Author:
John Bartel III

You can send enrollment invitations to groups and nested groups in Citrix Endpoint Management. Enrollment invitations aren't available for Windows devices.

When setting up the group invitation, you can specify one or more device platforms. You can also tag devices so that you can, for example, differentiate corporate-owned devices from employee-owned devices. Then, you set the authentication type for user devices.

> **Note:**
>
> If you plan to use custom notification templates, you must set up the templates before you configure enrollment security modes. For more information about notification templates, see Create and update notification templates.

For more information on basic configurations on user accounts, roles, and enrollment security modes and invitations, see User accounts, roles, and enrollment.

General steps

1. Within the Citrix Endpoint Management console, navigate to **Manage > Enrollment Invitations**.
2. Click **Add** toward the upper left of the screen and then click **Add Invitation**.
3. Click **Group** from the **Recipient** menu.

   This step lets you choose one or more platforms. If you have a mix of different operating system platforms within your company, choose all platforms. Only clear the platform selection if you are sure that no users are using the particular platform.
4. You can choose to tag devices during the invite process. Choose **Corporate** or **Employee**.

   Tagging makes it easy to separate corporate-owned devices and employee-owned devices.
5. In the **Domain** list, choose the domain in which the group exists.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

6. In the **Group** list, select the Active Directory group you want to send the invites to.
7. The **Enrollment mode** allows you to set the type of enrollment security that you prefer for users.
    - User name + Password
    - High Security
    - Invitation URL
    - Invitation URL + PIN
    - Invitation URL + Password
    - Two Factors
    - User name + PIN

    > **Note:**
    >
    > We deprecated the **High Security** enrollment security mode. To send enrollment invitations, you can use only **Invitation URL**, **Invitation URL + PIN**, or **Invitation URL + Password** enrollment security modes. For devices enrolling with **User name + Password**, **Two Factor**, or **User name + PIN**, users must download Citrix Secure Hub and manually enter their credentials.

8. For the **Agent Download**, **Enrollment URL**, **Enrollment PIN**, and **Enrollment Confirmation** templates, choose the custom notification template that you have created in the past. Or, choose the default that is listed.

    For these notification templates, use your configured SMTP server setup within Citrix Endpoint Management. Set your SMTP information first before proceeding.

    > **Note:**
    >
    > The **Expire after** and **Maximum Attempts** options change based on the **Enrollment mode** option that you choose. You cannot change these options.

9. Select On for **Send invitation** and then click **Save and Send** to complete the process.

Nested group support

You can use nested groups to send invites. Typically, nested groups are used in large-scale environments where groups with similar permissions are bound to each other.

Navigate to **Settings > LDAP** and then enable the **Support nested group** option.

Troubleshooting and known limitations

Issue: Invites are being sent out to users even though they have been removed from an Active Directory group.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Solution: Depending on how large your Active Directory environment is, it can take up to six hours for changes to propagate to all servers. If a user or nested group is removed recently, Citrix Endpoint Management might still consider those users as a part of the group.

So, it's best to wait up to six hours before sending out another group invite to your users.

Configuring certificate-based authentication with EWS for Citrix Secure Mail push notifications

September 6, 2025

For Citrix Secure Mail push notifications to work, you must do the following:

- Configure Exchange Server for certificate-based authentication. This requirement is especially necessary when Citrix Secure Hub is enrolled in Citrix Endpoint Management with certificate-based authentication.
- Configure the Active Sync and Exchange Web Services (EWS) virtual directory on the Exchange Mail Server with certificate-based authentication.

Unless you complete these configurations, the subscription to Citrix Secure Mail push notifications fails and no badge updates occur in Citrix Secure Mail.

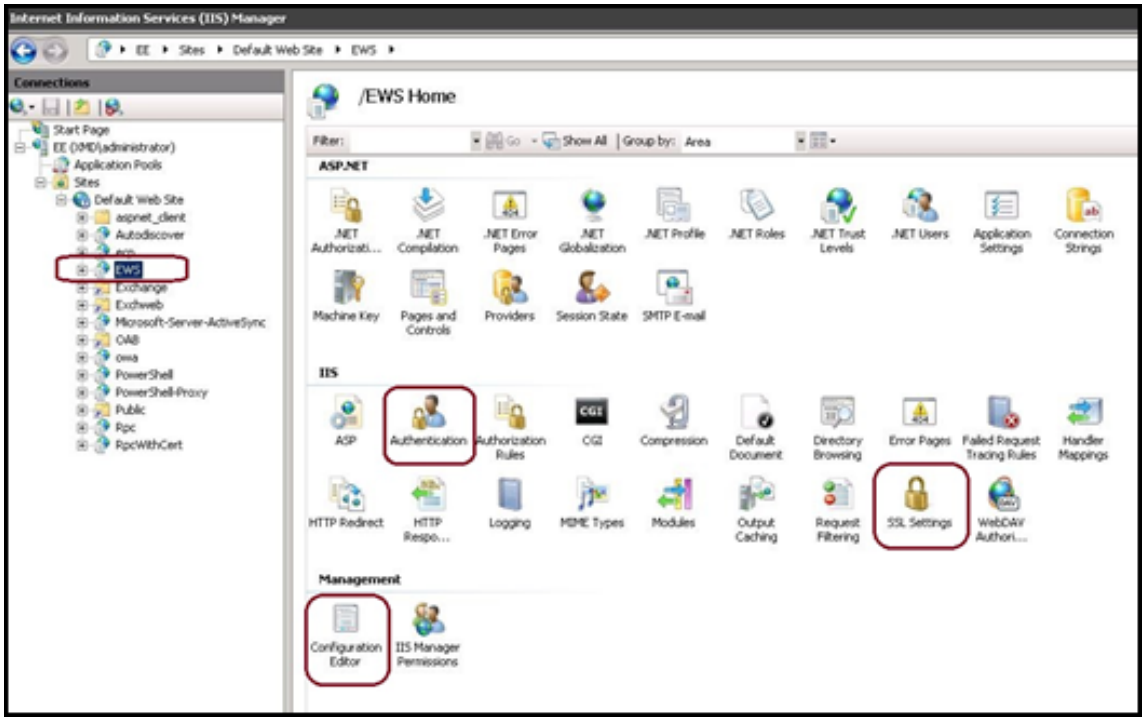
This article describes the steps to configure certificate-based authentication. The configurations are specifically against the EWS virtual directory on the Exchange Server.

To get started with the configuration, do the following:

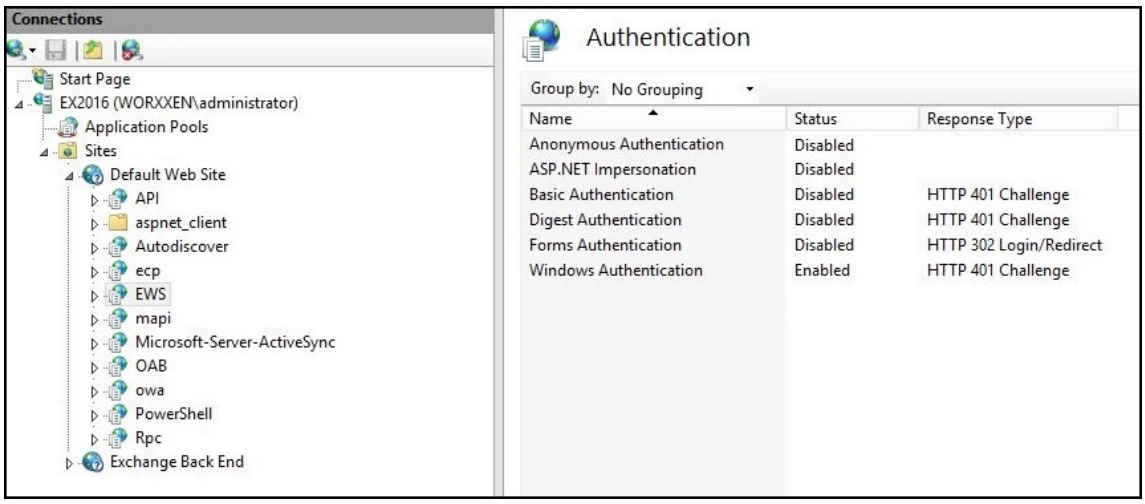
1. Log on to the server or servers where the EWS virtual directory is installed.
2. Open the IIS Manager Console.
3. Under the **Default Web Site**, click the EWS virtual directory.

   The Authentication, SSL, Configuration Editor snap-ins are on the right side of the IIS Manager Console

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Make sure that the **Authentication** settings for EWS are configured as shown in the following figure.

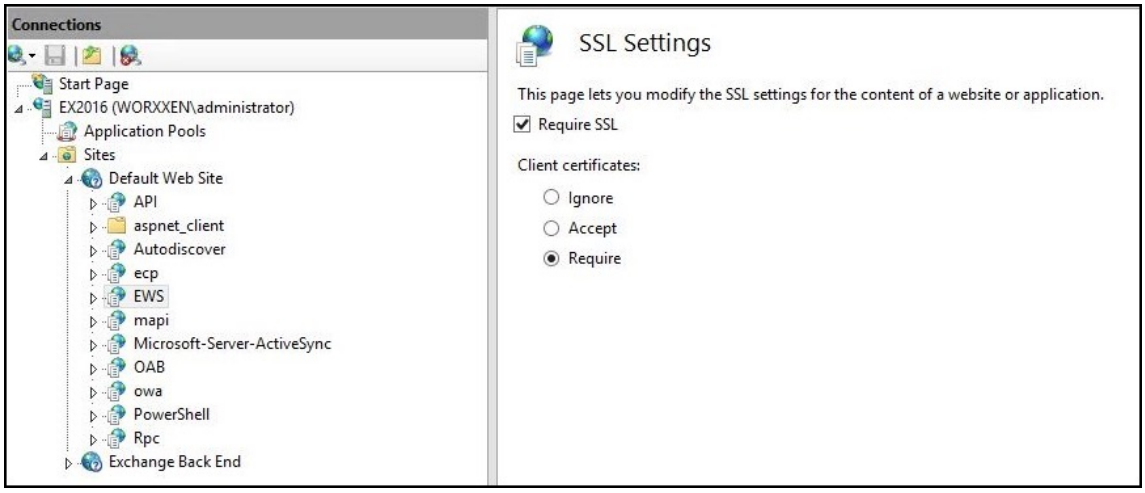


5. Configure the **SSL Settings** for the EWS virtual directory.

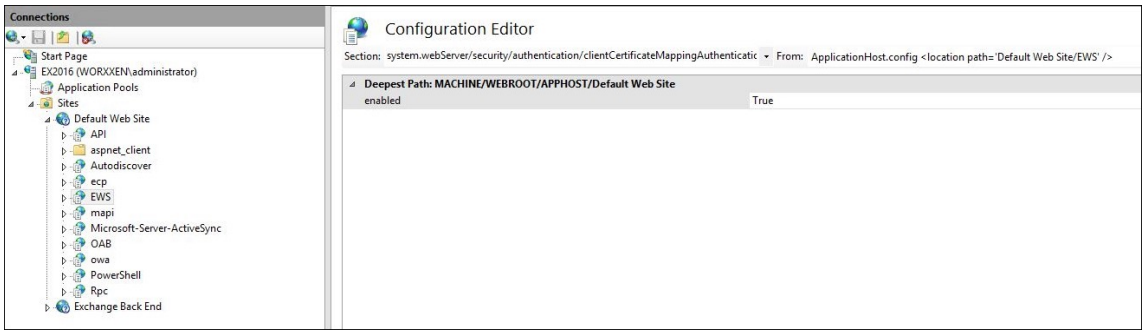
   a) Select the **Require SSL** checkbox.

   b) Under **Client Certificates**, click **Require**. Or, if other EWS mail clients use a user name and password to authenticate to the Exchange Server, click **Accept**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. Click **Configuration Editor**. Go to the following section in the **Section** drop-down list:
   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**
7. Set the **enabled** value to **True**.

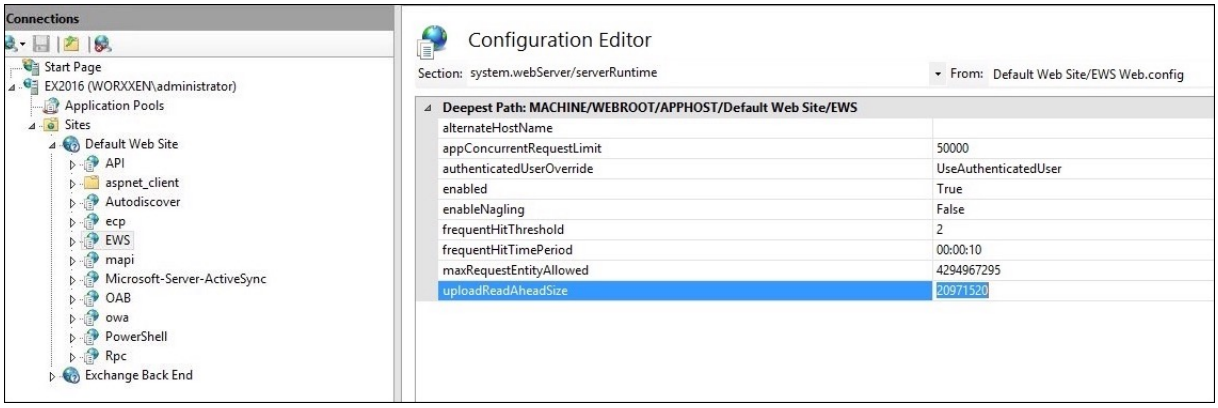


8. Click **Configuration Editor**. Go to the following section in the **Section** drop-down list:
   - **system.webServer/serverRuntime**
9. Set the **uploadReadAheadSize** value to **10485760** (10 MB) or **20971520** (20 MB) or to a value as required by your organization.

   > **Important:**
   >
   > If you don't set this value correctly, certificate-based authentication while subscribing to EWS push notifications can fail with an error code of 413.
   >
   > Do not set this value to **0**.

For more information, see the Microsoft article, Microsoft IIS server runtime.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



For more information about troubleshooting Citrix Secure Mail issues with iOS push notifications, see this Citrix Support Knowledge Center article.

Related information

Push notifications for Citrix Secure Mail for iOS

Configuring an on-premises Device Health Attestation server

September 6, 2025

You can enable Device Health Attestation (DHA) for Windows 10 and Windows 11 mobile devices through an on-premises Windows server. To enable DHA on-premises, you first configure a DHA server.

After you configure the DHA server, you create an Citrix Endpoint Management policy to enable the on-premises DHA service. For information, see Device Health Attestation device policy.

Prerequisites for a DHA server

- A server running Windows Server Technical Preview 5 or later, installed using the Desktop Experience installation option.
- One or more Windows 10 and Windows 11 client devices. These devices must have TPM 1.2 or 2.0 running the latest version of Windows.
- These certificates:
  - **DHA SSL certificate:** An x.509 SSL certificate that chains to an enterprise trusted root with an exportable private key. This certificate protects DHA data communications in transit including:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

    * server to server (DHA service and MDM server) communications
    * server to client (DHA service and a Windows 10 or Windows 11 device) communications
  - **DHA signing certificate:** An x.509 certificate that chains to an enterprise trusted root with an exportable private key. The DHA service uses this certificate for digital signing.
  - **DHA encryption certificate:** An x.509 certificate that chains to an enterprise trusted root with an exportable private key. The DHA service also uses this certificate for encryption.

- Choose one of these certificate validation modes:

  - **EKCert:** EKCert validation mode is optimized for devices in organizations that are not connected to the Internet. Devices connecting to a DHA service running in EKCert validation mode do not have direct access to the Internet.
  - **AIKCert:** AIKCert Validation Mode is optimized for operational environments that do have access to the Internet. Devices connecting to a DHA service running in AIKCert validation mode must have direct access to the Internet and can get an AIK certificate from Microsoft.

Add the DHA server role to the Windows server

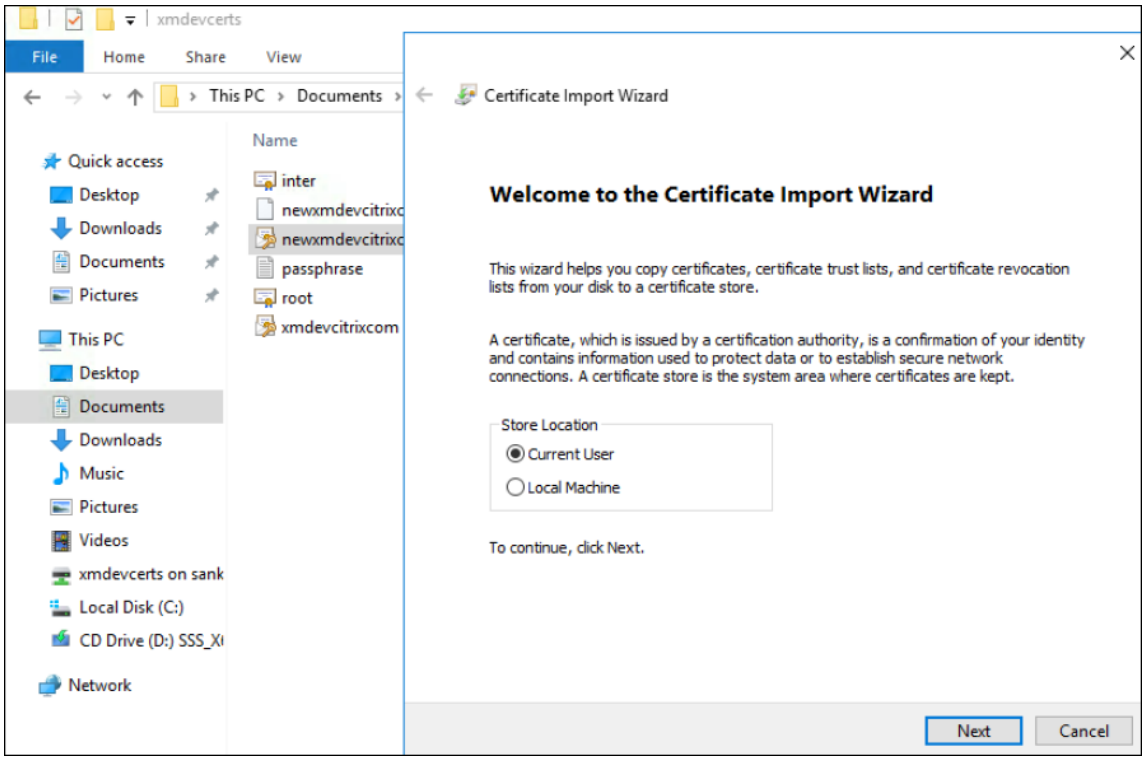
1. On the Windows server, if the Server Manager is not already open, click **Start** and then click **Server Manager**.
2. Click **Add roles and features**.
3. On the **Before you begin** page, click **Next**.
4. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
5. On the **Select destination server** page, click **Select a server from the server pool**, select the server, and then click **Next**.
6. On the **Select server role**s page, select the **Device Health Attestation** checkbox.
7. Optional: Click **Add Features** to install other required role services and features.
8. Click **Next**.
9. On the **Select feature**s page, click **Next**.
10. On the **Web Server Role (IIS)** page, click **Next**.
11. On the **Select role services** page, click **Next**.
12. On the **Device Health Attestation Service** page, click **Next**.
13. On the **Confirm installation selections** page, click **Install**.
14. When the installation is done, click **Close**.

Add the SSL certificate to the certificate store of the server

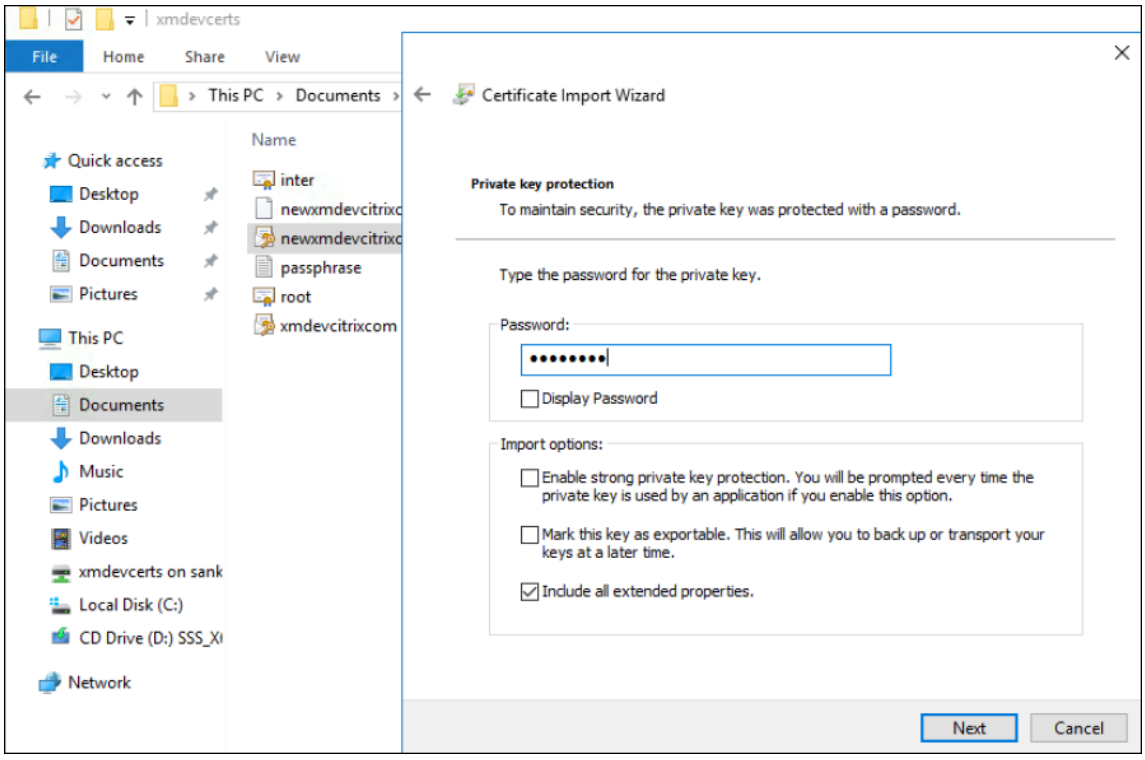
1. Go to the SSL certificate file and select it.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. For the store location, select **Current user** and then click **Next**.



3. Type the password for the private key.
4. Make sure that the import option **Include all extended properties** is selected. Click **Next**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. When this window appears, click **Yes**.

6. Confirm that the certificate is installed:

   a) Open a Command Prompt window.

   b) Type `mmc` and press the **Enter** key. To view certificates in the local machine store, you must be in the Administrator role.

   c) On the File menu, click **Add/Remove Snap In**.

   d) Click **Add**.

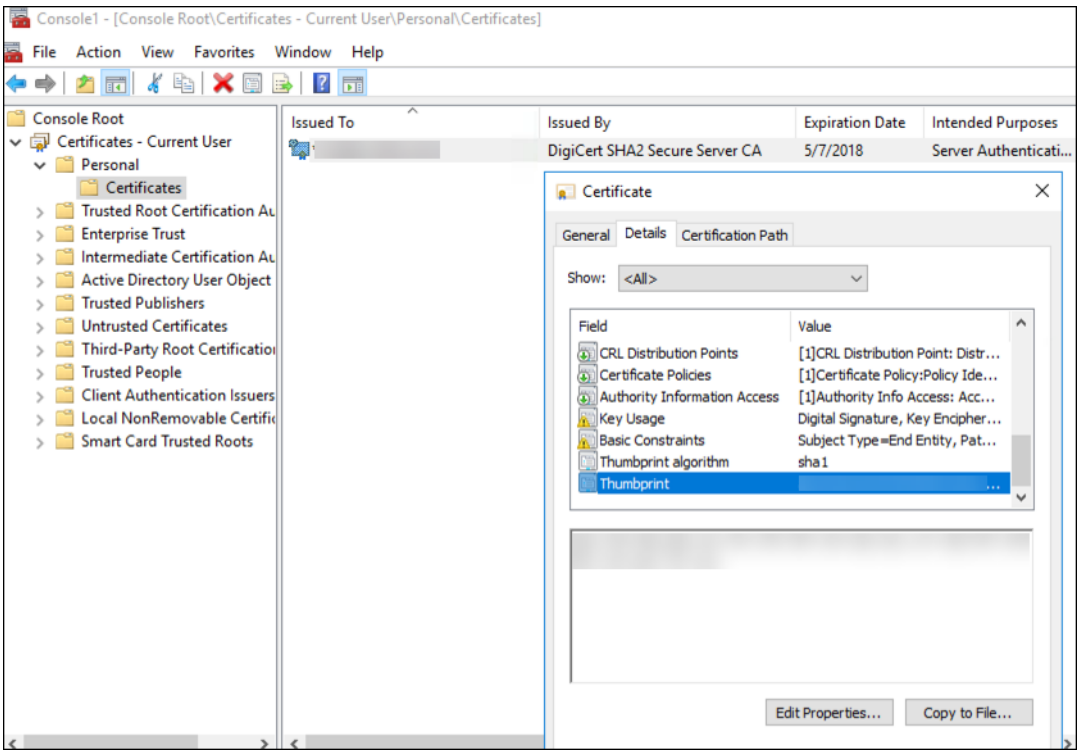
   e) In the Add Standalone Snap-in dialog box, select **Certificates**.

   f) Click **Add**.

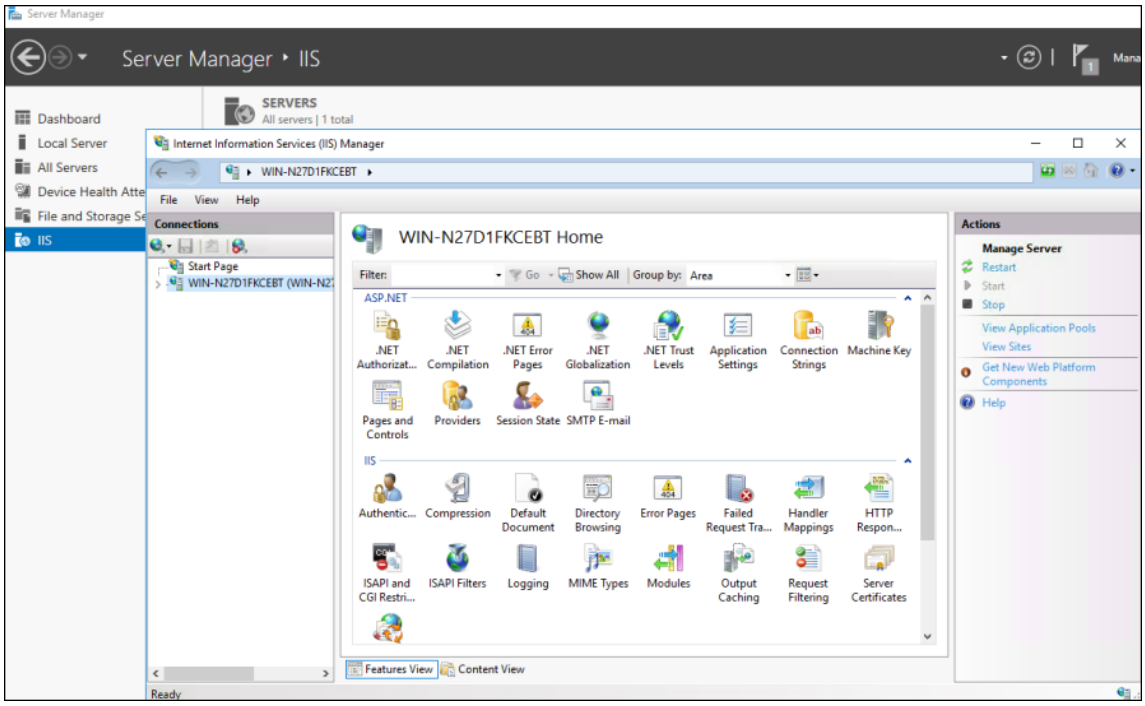
   g) In the Certificates snap-in dialog box, select **My User account**. (If you are signed in as a service account holder, select **Service account**.)

   h) In the Select Computer dialog box, click **Finish**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

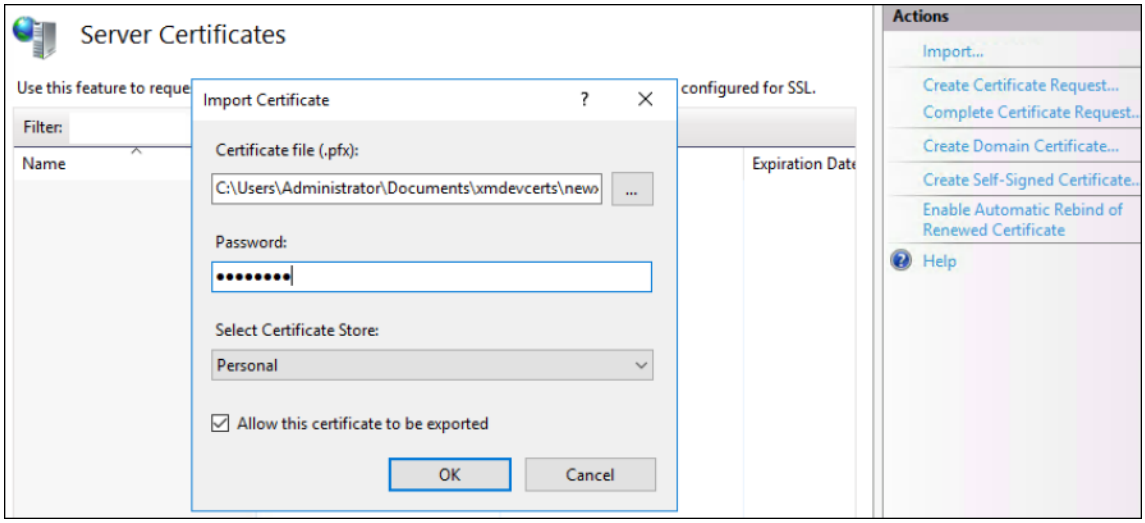


7. Go to **Server Manager > IIS** and select **Server Certificates** from the list of icons.



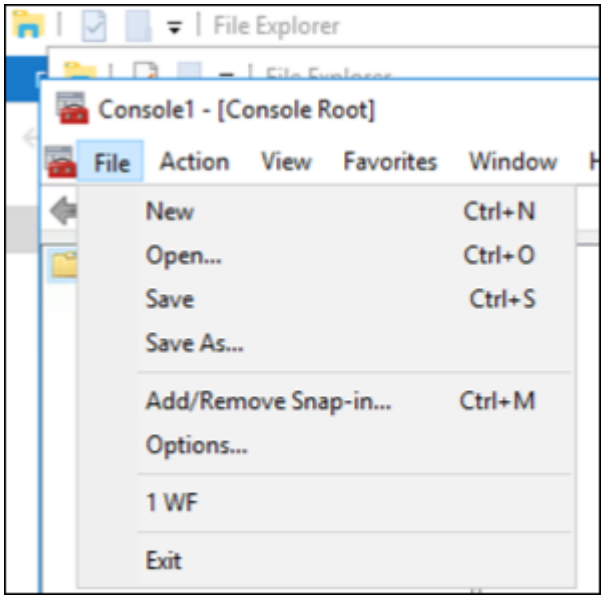
8. From the Action menu, select **Import...** to import the SSL certificate.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



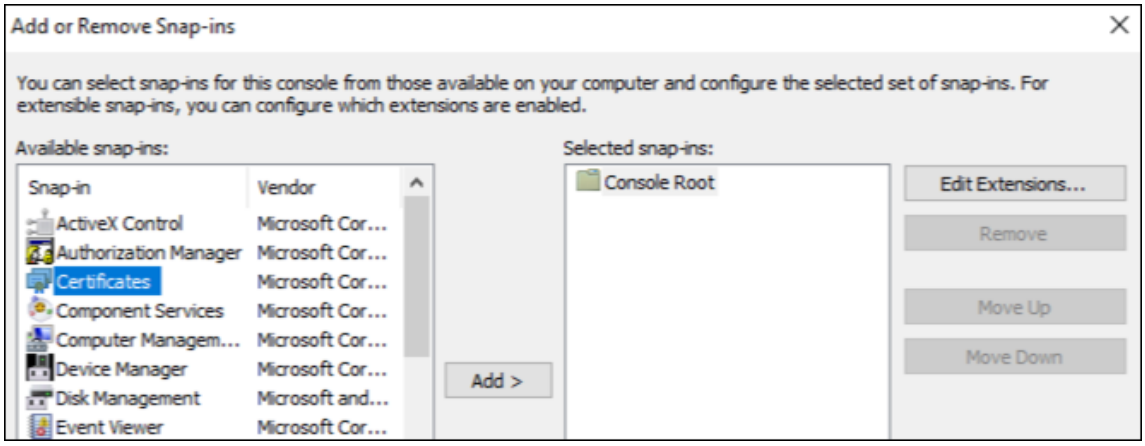
Retrieve and save the thumbprint of the certificate

1. In the File Explorer search bar, type `mmc`.
2. In the Console Root window, click **File > Add/Remove Snap-in**.

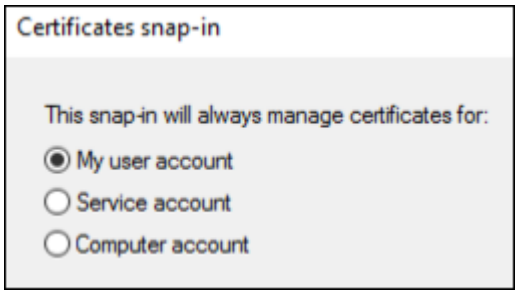


3. Select the certificate from an available snap-in and add it to the selected snap-ins.

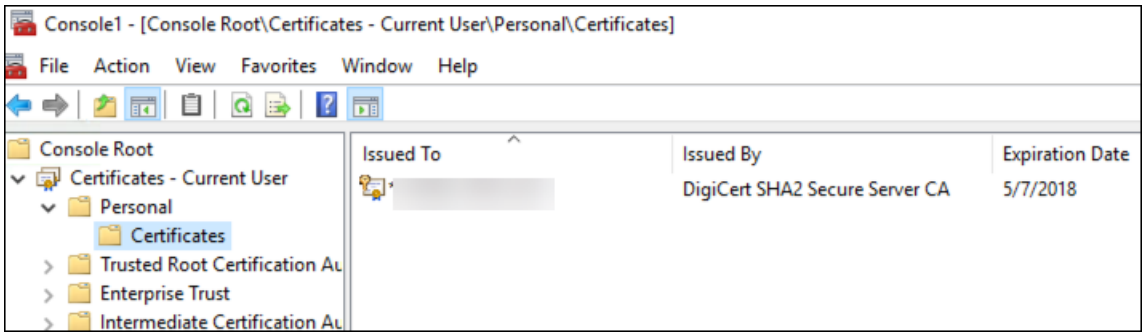
© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Select **My user account**.

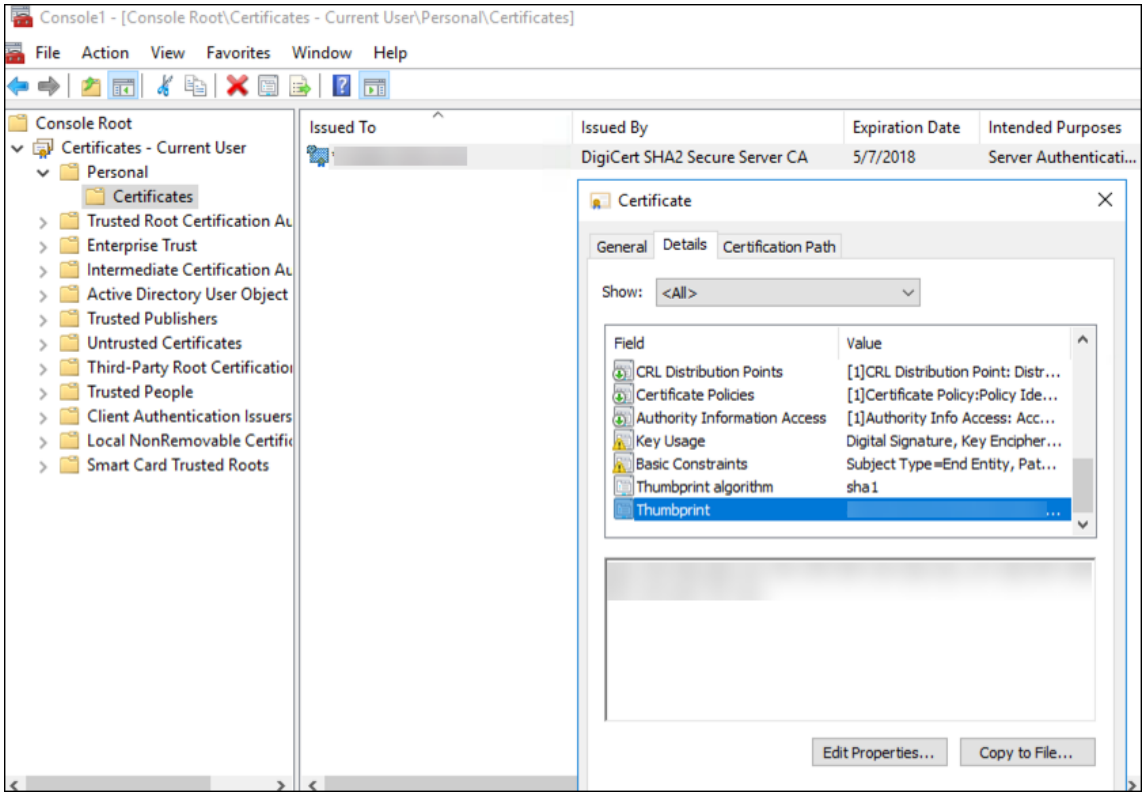


5. Select the certificate and click **OK**.



6. Double-click on the certificate and select the **Details** tab. Scroll down to see the certificate thumbprint.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



7. Copy the thumbprint to a file. Remove the spaces when using the thumbprint in PowerShell commands.

Install the signing and encryption certificates

Run these PowerShell commands on the Windows server to install the signing and encryption certificates.

Replace the placeholder ReplaceWithThumbprint and enclose it inside double-quotation marks as shown.

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
 $_.Thumbprint -like "ReplaceWithThumbprint" }


$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys\" +
   $keyname icacls $keypath /grant IIS_IUSRS`:R
```

Extract the TPM roots certificate and install the trusted certificate package

Run these commands on the Windows server:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
mkdir .\TrustedTpm

expand -F:\* .\TrustedTpm.cab .\TrustedTpm

cd .\TrustedTpm

.\setup.cmd
```

Configure the DHA service

Run this command on the Windows server to configure the DHA service.

Replace the placeholder ReplaceWithThumbprint.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
   ReplaceWithThumbprint

-SigningCertificateThumbprint ReplaceWithThumbprint

-SslCertificateStoreName My -SslCertificateThumbprint
   ReplaceWithThumbprint

-SupportedAuthenticationSchema "AikCertificate"
```

Run these commands on the Windows server to set up the certificate chain policy for the DHA service:

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

Respond to these prompts as follows:

```
  Confirm

    Are you sure you want to perform this action?

    Performing the operation "Install-DeviceHealthAttestation" on
       target "[Machine Name]".

    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?]
       Help (default is "Y"): A

    Adding SSL binding to website 'Default Web Site'.

    Add SSL binding?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
14
15      Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17      Add application pool?
18
19      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
20
21      Adding web application 'DeviceHealthAttestation' to website '
           Default Web Site'.
22
23      Add web application?
24
25      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
26
27      Adding firewall rule 'Device Health Attestation Service' to allow
           inbound connections on port(s) '443'.
28
29      Add firewall rule?
30
31      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
32
33      Setting initial configuration for Device Health Attestation Service
           .
34
35      Set initial configuration?
36
37      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
38
39      Registering User Access Logging.
40
41      Register User Access Logging?
42
43      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

Check the configuration

To check whether the DHASActiveSigningCertificate is active, run this command on the server:

```
Get-DHASActiveSigningCertificate
```

If the certificate is active, the certificate type (Signing) and thumbprint are displayed.

To check whether the DHASActiveSigningCertificate is active, run these commands on the server

Replace the placeholder ReplaceWithThumbprint and enclose it inside double-quotation marks as shown.

```
1  Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
       -Force
2
3  Get-DHASActiveEncryptionCertificate
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

If the certificate is active, the thumbprint appears.

To do a final check, go to this URL:

`https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate/v1`

If the DHA service is running, “Method not allowed”appears.

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.