Citrix Endpoint Management
# Contents

- Endpoint Management 3
- What’s new 9
- Third-party notices 18
- System requirements 18
- Endpoint Management compatibility 31
- Supported device operating systems 32
- Language support 34
- About Endpoint Management 37
- Citrix Endpoint Management integration with Microsoft Intune/EMS 46
- Onboarding and resource setup 62
- Prepare to enroll devices and deliver resources 83
- Certificates and authentication 93
- Citrix Gateway and Endpoint Management 105
- Domain or domain plus security token authentication 114
- Client certificate or certificate plus domain authentication 122
- PKI entities 145
- Credential providers 173
- APNs certificates 181
- SAML for single sign-on with Citrix Files 193
- Single sign in with Azure Active Directory 203
- Derived credentials 208
- User accounts, roles, and enrollment 226
- Notifications 242
Configure roles with RBAC  
Device management  
Alexa for Business  
Migrate from device administration to Android Enterprise  
Android Enterprise  
Legacy Android Enterprise for G Suite Customers  
Android OS  
Firebase Cloud Messaging  
Android SafetyNet  
Samsung  
Samsung Knox bulk enrollment  
iOS  
macOS  
Deploy devices through Apple Deployment Program  
Bulk enrollment of Apple devices  
Integrate with Apple Education features  
Network Access Control  
Chrome OS  
Windows Desktop and Tablet  
Windows Phone  
Bulk enrollment of Windows devices  
Workspace hub device management  
Device policies  
AirPlay mirroring device policy
<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirPrint device policy</td>
<td>595</td>
</tr>
<tr>
<td>Android Enterprise app permissions</td>
<td>595</td>
</tr>
<tr>
<td>Android Enterprise managed configurations policy</td>
<td>597</td>
</tr>
<tr>
<td>Android Enterprise permissions</td>
<td>608</td>
</tr>
<tr>
<td>APN device policy</td>
<td>610</td>
</tr>
<tr>
<td>App access device policy</td>
<td>612</td>
</tr>
<tr>
<td>App attributes device policy</td>
<td>612</td>
</tr>
<tr>
<td>App configuration device policy</td>
<td>613</td>
</tr>
<tr>
<td>App inventory device policy</td>
<td>617</td>
</tr>
<tr>
<td>Application Guard device policy</td>
<td>619</td>
</tr>
<tr>
<td>App lock device policy</td>
<td>621</td>
</tr>
<tr>
<td>App network usage device policy</td>
<td>625</td>
</tr>
<tr>
<td>Apps notifications device policy</td>
<td>625</td>
</tr>
<tr>
<td>App restrictions device policy</td>
<td>626</td>
</tr>
<tr>
<td>App tunneling device policy</td>
<td>630</td>
</tr>
<tr>
<td>App uninstall device policy</td>
<td>631</td>
</tr>
<tr>
<td>App uninstall restrictions device policy</td>
<td>632</td>
</tr>
<tr>
<td>BitLocker device policy</td>
<td>633</td>
</tr>
<tr>
<td>Browser device policy</td>
<td>639</td>
</tr>
<tr>
<td>Calendar (CalDav) device policy</td>
<td>640</td>
</tr>
<tr>
<td>Cellular device policy</td>
<td>641</td>
</tr>
<tr>
<td>Connection scheduling device policy</td>
<td>642</td>
</tr>
<tr>
<td>Contacts (CardDAV) device policy</td>
<td>644</td>
</tr>
<tr>
<td>Content device policy</td>
<td>645</td>
</tr>
<tr>
<td>Device Policy</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Copy Apps to Samsung Container device policy</td>
<td>646</td>
</tr>
<tr>
<td>Credentials device policy</td>
<td>647</td>
</tr>
<tr>
<td>Custom XML device policy</td>
<td>654</td>
</tr>
<tr>
<td>Defender device policy</td>
<td>656</td>
</tr>
<tr>
<td>Device Guard device policy</td>
<td>658</td>
</tr>
<tr>
<td>Device Health Attestation device policy</td>
<td>659</td>
</tr>
<tr>
<td>Device name device policy</td>
<td>660</td>
</tr>
<tr>
<td>Education Configuration device policy</td>
<td>661</td>
</tr>
<tr>
<td>Endpoint Management options device policy</td>
<td>664</td>
</tr>
<tr>
<td>Endpoint Management uninstall device policy</td>
<td>665</td>
</tr>
<tr>
<td>Enterprise Hub device policy</td>
<td>666</td>
</tr>
<tr>
<td>Exchange device policy</td>
<td>667</td>
</tr>
<tr>
<td>Files device policy</td>
<td>675</td>
</tr>
<tr>
<td>FileVault device policy</td>
<td>676</td>
</tr>
<tr>
<td>Firewall device policy</td>
<td>679</td>
</tr>
<tr>
<td>Font device policy</td>
<td>681</td>
</tr>
<tr>
<td>Home screen layout device policy</td>
<td>682</td>
</tr>
<tr>
<td>Import Device Configuration device policy</td>
<td>683</td>
</tr>
<tr>
<td>Import iOS &amp; macOS Profile device policy</td>
<td>684</td>
</tr>
<tr>
<td>Keyguard Management device policy</td>
<td>685</td>
</tr>
<tr>
<td>Kiosk device policy</td>
<td>687</td>
</tr>
<tr>
<td>Knox Platform for Enterprise device policy</td>
<td>694</td>
</tr>
<tr>
<td>Launcher configuration device policy for Android</td>
<td>695</td>
</tr>
<tr>
<td>LDAP device policy</td>
<td>697</td>
</tr>
</tbody>
</table>
Location device policy 698
Lock screen message device policy 704
Mail device policy 704
Managed bookmarks device policy 707
Managed domains device policy 707
Maps device policy 710
Maximum resident users device policy 710
MDM options device policy 711
Office device policy 712
Organization information device policy 713
OS Update device policy 714
Passcode device policy 727
Passcode lock grace period device policy 740
Personal hotspot device policy 740
Power management device policy 741
Profile Removal device policy 742
Provisioning profile device policy 743
Provisioning profile removal device policy 744
Proxy device policy 744
Public session device policy 745
Restrictions device policy 749
Roaming device policy 789
Samsung MDM license key device policy 790
SCEP device policy 792
Siri and dictation policies 795
SSO account device policy 797
Storage encryption device policy 798
Store device policy 799
Subscribed calendars device policy 799
Terms and conditions device policy 800
Verified access device policy 801
VPN device policy 802
Wallpaper device policy 850
Web content filter device policy 851
Webclip device policy 853
WiFi device policy 854
Windows Agent device policy 867
Windows Hello for Business device policy 871
Windows GPO Configuration device policy 872
Windows Information Protection device policy 875
Deprecated device policies 879
Add apps 893
App connector types 947
Citrix Launcher 948
iOS Volume Purchase 950
Deploy Microsoft Store for Business apps from Endpoint Management 955
Use Citrix Content Collaboration with Endpoint Management 959
SmartAccess for HDX apps 974
# Citrix Endpoint Management

- Upgrade MDX or enterprise apps 991
- Add media 993
- Deploy resources 997
- Macros 1016
- Automated actions 1051
- Monitor and support 1061
- Connectivity checks 1068
- Mobile Service Provider 1072
- Reports 1073
- Endpoint Management Analyzer 1077
- REST APIs 1087
- ActiveSync Gateway 1088
- Endpoint Management connector for Exchange ActiveSync 1090
- Citrix Gateway connector for Exchange ActiveSync 1142
- Advanced concepts 1158
- Endpoint Management deployment 1158
- Management modes 1160
- Device requirements 1163
- Security and user experience 1163
- Apps 1182
- User communities 1190
- Email strategy 1198
- Endpoint Management integration 1205
- Integrating with Citrix Gateway and Citrix ADC 1212

© 1999-2019 Citrix Systems, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO and proxy considerations for MDX apps</td>
<td>1219</td>
</tr>
<tr>
<td>Authentication</td>
<td>1224</td>
</tr>
<tr>
<td>Server properties</td>
<td>1238</td>
</tr>
<tr>
<td>Device and app policies</td>
<td>1252</td>
</tr>
<tr>
<td>Client properties</td>
<td>1262</td>
</tr>
<tr>
<td>User enrollment options</td>
<td>1273</td>
</tr>
<tr>
<td>App provisioning and deprovisioning</td>
<td>1276</td>
</tr>
<tr>
<td>Dashboard-based operations</td>
<td>1279</td>
</tr>
<tr>
<td>Role-based access control and Endpoint Management support</td>
<td>1280</td>
</tr>
<tr>
<td>Citrix Support process</td>
<td>1282</td>
</tr>
<tr>
<td>Sending group enrollment invitations in Endpoint Management</td>
<td>1283</td>
</tr>
<tr>
<td>Configuring certificate-based authentication with EWS for Secure Mail push notifications</td>
<td>1285</td>
</tr>
<tr>
<td>Configuring an on-premises Device Health Attestation server</td>
<td>1288</td>
</tr>
</tbody>
</table>
Endpoint Management

August 28, 2019

Citrix Endpoint Management is a solution for managing endpoints, offering mobile device management (MDM) and mobile application management (MAM) capabilities. With 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 hosts the Cloud environment in data centers located throughout the world to deliver high performance, rapid response, and support. With Endpoint Management, you pay a subscription fee instead of purchasing and managing licenses.

Integration with Citrix Workspace experience

Endpoint Management customers can opt to integrate Endpoint Management with the Citrix Workspace experience. You make that choice in Citrix Cloud > Workspace Configuration > Service Integrations. By default, Workspace integration is disabled.

Endpoint Management integration with Citrix Workspace differs for new and existing customers.

- For new Endpoint Management customers (as of August 27, 2018):
  During Workspace configuration (Citrix Cloud > Workspace Configuration > Service Integrations), you choose whether to enable Endpoint Management integration with Citrix Workspace. By default, the integration is disabled.

  - If you enable the integration, the Citrix Workspace app aggregates resources from Endpoint Management and other configured sources. Your users access resources from the Citrix Workspace app. Other configured sources might include Citrix Content Collaboration and Citrix Virtual Apps and Desktops.

  - If you leave the integration disabled, Citrix Secure Hub aggregates mobile apps. Your users access apps from Secure Hub.

  Important:
  After you configure your integration choice and enroll users: If you later change your integration choice, re-enrollment is required for all users.

- For customers who onboarded before August 27, 2018:
  You can enable Workspace integration (Citrix Cloud > Workspace Configuration > Service Integrations). Devices that are already enrolled in Secure Hub continue to use Secure Hub.
New devices enroll in Workspace. However, if you prefer to enroll only selected devices in Workspace, you must create a delivery group called Workspace.

- For devices already enrolled in Secure Hub and then added to the Workspace delivery group, a user must re-enroll the device. The user then accesses resources from the Citrix Workspace app.
- For new devices added to the Workspace delivery group, users enroll in Workspace.
- If you move a device from the Workspace delivery group to any other delivery group, a user must re-enroll the device. The user then accesses resources from Secure Hub.
- Citrix will notify you when migration to Workspace is supported without requiring re-enrollment.

To enable Citrix Workspace integration with Citrix Endpoint Management:

1. Sign in to Citrix Cloud.
2. Click Manage on the Endpoint Management tile. You can request a 30-day trial if the Manage tab is unavailable.
3. In the upper-left menu, navigate to Workspace Configuration > Service Integration.
4. Click Enable to integrate Citrix Workspace app with Endpoint Management.

**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:

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

Customer responsibilities:

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

Integration with Microsoft Intune/EMS

Endpoint Management integrates with Microsoft Enterprise Mobility + Security (EMS)/Intune. That integration adds the value of Endpoint Management micro VPN to Microsoft Intune aware apps, such as Microsoft Managed Browser. With the integration, you can:

• 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 Endpoint Management MDM+MAM or Intune MDM to manage devices. For more information, see Endpoint Management integration with Microsoft Intune/EMS.

Cloud Connector and resource locations

You connect to 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 contain the resources required to deliver services to your subscribers. For Endpoint Management, resource locations are your Citrix Gateway, LDAP, DNS, and PKI servers.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
For more information about Cloud Connector and resource locations, see About Endpoint Management.

**Get started with Endpoint Management**

**Tip:** XenMobile Migration Service

If you’re using XenMobile Server on premises, our XenMobile Migration Service can get you started with 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. These blogs discuss the XenMobile Migration Service:

- New XenMobile Migration Service
- Making the Case for XenMobile in the Cloud

When you are evaluating or purchasing Endpoint Management, the Endpoint Management Operations team provides ongoing onboarding help. The Operations team also communicates with you to ensure
that the core Endpoint Management services are running and configured correctly. This figure shows the onboarding steps.

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

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

Want to learn more before starting? Try these resources:

**Endpoint Management documentation:** Provides full 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 release.

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

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

**SalesIQ**: More resources for our Citrix Partners.

**Next steps**

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

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

**Endpoint Management support**

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

Rolling updates to the 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 ensure product quality and to maximize availability.

If you are an Endpoint Management customer, you also receive Endpoint Management updates and communications directly from the 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 Endpoint Management environments with the latest Endpoint Management rolling patches. To obtain 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, Endpoint Management console access, or Secure Mail issues.

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

Examples of changes that you might request are:

- Citrix Files integration with Citrix Gateway in the Cloud
• Change Citrix Gateway authentication type
• Validate connectivity to customer data center resources
• Change split tunnel configuration for micro VPN
• Restart Endpoint Management components due to 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.

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

What’s new

December 10, 2019

A goal of Citrix is to deliver new features and product updates to Endpoint Management customers when they are available. New releases provide more value, so there’s no reason to delay updates. Rolling updates to Endpoint Management release 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. Delivering updates incrementally in waves helps to ensure product quality and to maximize availability.

You also receive Endpoint Management updates and communications directly from the 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 Endpoint Management Service Level Agreement. To monitor service interruptions and scheduled maintenance, see the Service Health Dashboard.

Support for iOS 13

Endpoint Management supports devices upgraded to iOS 13. The upgrade impacts your users as follows:

• During enrollment, a few new iOS Setup Assistant Option screens appear. Apple added new iOS Setup Assistant Option screens to iOS 13. The new options are not included in the Settings
> Apple Deployment Program page in this release. As a result, you can’t configure Endpoint Management to skip those screens. Those pages appear to users on iOS 13 devices.

- Some Restrictions device policy settings available on supervised or unsupervised devices for previous iOS versions are available only on supervised devices for iOS 13+. The current Endpoint Management console tool tips don’t yet indicate that these settings are for supervised devices for iOS 13+ only.
  - Allow hardware controls:
    * FaceTime
    * Installing apps
  - Allow apps:
    * iTunes Store
    * Safari
    * Safari > Autofill
  - Network - Allow iCloud actions:
    * iCloud documents & data
  - Supervised only settings - Allow:
    * Game Center > Add friends
    * Game Center > Multiplayer gaming
  - Media content - Allow:
    * Explicit music, podcasts, and iTunes U material

These restrictions apply as follows:

- If an iOS 12 (or lower) device is already enrolled in Endpoint Management and then upgrades to iOS 13, the preceding restrictions apply to unsupervised and supervised devices.
- If an unsupervised iOS 13+ device enrolls in Endpoint Management, the preceding restrictions apply only to supervised devices.
- If a supervised iOS 13+ device enrolls in Endpoint Management, the preceding restrictions apply only to supervised devices.

Citrix Endpoint Management integration with Citrix Workspace

Endpoint Management integration with Citrix Workspace differs for new and existing customers. See Integration with Citrix Workspace experience.

Mobile SSO to native SaaS apps (preview)

A preview of mobile SSO to native SaaS apps is now available for customers who meet these requirements:
Citrix Endpoint Management

- Citrix Workspace Premium license
- Your identity provider configured in Citrix Cloud
- The following services configured:
  - Workspace service with Endpoint Management enabled. For information about enabling service integration, see Workspace configuration.
  - Citrix Endpoint Management service
  - Citrix Gateway service

Single sign-on to native SaaS apps is available from iOS and Android devices that are enrolled into MDM. For more information, see Configure mobile SSO (preview).

**Citrix Gateway service (preview)**

A preview of Citrix Gateway service is now available for customers who meet these requirements:

- Citrix Workspace experience enabled
- Citrix Gateway service subscription

If you already use on-premises Citrix Gateway and want to switch to Citrix Gateway service, contact your Citrix Support representative. For more information, see Configure Citrix Gateway use with Endpoint Management.

**Endpoint Management 19.12.0**

The following features are now rolling out to commercial customers. Releases to US government customers begin within three months. For feature differences between the commercial and US government offerings, see Endpoint Management service for US Government.

You can now configure delivery groups for Windows devices based on device properties. (Preview) When configuring delivery groups, you can now configure groups based on device properties. This feature is only available for Windows desktops and tablets. To request access to this Preview feature, contact your Citrix sales or support representative. For more information about this feature, see To add a delivery group (Preview).

Import Group Policy Objects (GPOs) into Endpoint Management and deploy them directly to Windows 10 devices. Rather than relying on an AD administrator to deploy GPOs from the Group Policy Management console, you can import and deploy GPOs through the Endpoint Management console. See Windows GPO Configuration device policy.

Install EXE apps for Windows desktops and tablets. You can now upload EXE applications as enterprise apps for Windows Desktops and Tablets. For more information, see Add Win32 apps as Enterprise apps.
Citrix Endpoint Management

Users can no longer remove policies from iOS devices. Some device policies no longer allow users to remove the policy from iOS devices. The setting Allow user to remove policy has been removed for iOS from the following policies: APN policy, Mail policy, Passcode policy, Provisioning Profile policy, Proxy policy, and VPN policy.

Fixed issues in Endpoint Management 19.12.0

If you update an app version number with the Endpoint Management Public REST API and then by using the console: The app version doesn’t update. [CXM-69216]

Sometimes Endpoint Management can’t install EXE apps on Windows devices because the file hash isn’t correct. [CXM-75506]

Endpoint Management 19.11.0

The following features are now rolling out to commercial customers. Releases to US government customers begin within three months. For feature differences between the commercial and US government offerings, see Endpoint Management service for US Government.

Apple Volume Purchase Program migration to Apple Business Manager (ABM) and Apple School Manager (ASM)

Companies and institutions using Apple Volume Purchase Program (VPP) need to migrate to Apps and Books in Apple Business Manager or Apple School Manager before December 1, 2019.

Before migrating VPP accounts in Endpoint Management, see this Apple support article.

If your organization or school only uses the Volume Purchase Program (VPP), you can enroll in ABM/ASM and then invite existing VPP Purchasers to your new ABM/ASM account. For ASM, navigate to https://school.apple.com. For ABM, navigate to https://business.apple.com.

To update your volume purchase (formerly VPP) account on Endpoint Management:

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The Settings page appears.
2. Click Volume Purchase. The Volume Purchase configuration page appears.
3. Ensure that your ABM or ASM account has same app config as your previous VPP account.
4. In the ABM or ASM portal, download an updated token.
5. In the Endpoint Management console, do the following:
   a) Edit the existing volume purchase account with the updated token info for that location.
b) Edit your ABM or ASM credentials. Don’t change the suffix.

c) Click **Save** twice.

For more information, see:

- iOS Volume Purchase
- Deploy devices through Apple Deployment Program
- Bulk enrollment of Apple devices

**Enrollment profiles control enrollment options for Android devices**

Enrollment profiles now control how Android devices are enrolled if Android Enterprise is enabled for your Endpoint Management deployment. Enrollment profiles determine whether Android devices are enrolled in the default Android Enterprise mode (fully managed or work profile) or in legacy (device administrator) mode.

By default, the Global enrollment profile enrolls new and factory reset Android Enterprise devices as fully managed devices and enrolls BYOD Android Enterprise devices as work profile devices. For more information, see **Android Enterprise**.

**Preparing legacy Android devices for Android Enterprise as default enrollment**

Google is deprecating the device administrator mode of device management and encouraging 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 will make Android Enterprise the default enrollment option for Android devices.

This change will mean that if Android Enterprise is enabled for your Endpoint Management deployment, all newly enrolled or re-enrolled Android devices are enrolled as Android Enterprise devices.

To prepare for this change, Endpoint Management now allows you to create enrollment profiles that control how Android devices are enrolled.

Your organization might not be ready to begin managing legacy Android devices in device owner mode or profile owner mode. In that case, you can continue to manage them in device administrator mode. Create an enrollment profile for legacy devices and re-enroll all enrolled legacy devices.

To create an enrollment profile for legacy devices:

1. In the 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. Click **Next** or select **Android** under **Platforms**. The Enrollment Configuration page appears.
4. Set Management to Legacy device administration (not recommended). Click Next.

5. Select Assignment (options). The Delivery Group Assignment screen appears.

6. Choose the delivery group or delivery groups containing the administrators who enroll dedicated devices. Then click Save.

To continue managing legacy device 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 Secure Hub and providing an enrollment server URL.

For more information about Endpoint Management support for the transition to Android Enterprise, see the blog, Android Enterprise as default for Citrix Endpoint Management service.

**Fixed issues in Endpoint Management 19.11.0**

When searching for a Google Play Store app in the Endpoint Management console, the app name is empty. You can enter the name manually to save the app. [CXM-73261]

After uploading an MDX app for Android Enterprise, the managed Google Play store UI might not open in the Endpoint Management console. Until the issue is fixed, go to the managed Google Play store to approve and save the app manually. [CXM-73398]

For iOS, location tracking doesn’t work if you do the following: Configure and deploy a location policy, enable tracking from device security actions, and then delete the deployed location policy and create a new one. [CXM-73470]

Users with apostrophes in their user names can’t enroll their devices when their user name is imported from LDAP. [CXM-73780]
Endpoint Management 19.10.0

The following features are now rolling out to commercial customers. Releases to US government customers begin within three months. For feature differences between the commercial and US government offerings, see Endpoint Management service for US Government.

Expanded support for Zebra OEMConfig. Endpoint Management now supports managing Zebra devices using the Zebra Technologies administrative tool Zebra OEMConfig. (For information, see the Zebra Technologies website.) To manage devices using the Zebra OEMConfig app, publish the app and configure an Android Enterprise managed configurations device policy.

Content delivery network (CDN) availability for Windows apps. You can now deploy Windows apps by using a content delivery network. See Deliver enterprise apps from a CDN.

Group invitation support for users whose names include special characters. When you choose a group to receive enrollment invitations, Endpoint Management now gets the user list from Active Directory. The list includes users whose names contain special characters. See Enrollment invitations.

Fixed issues in Endpoint Management 19.10.0

After you enroll a new device or re-enroll an old device, an error message intermittently displays on Manage > Devices. [CXM-72634, CXM-73077]

When you select a Chrome or Workspace hub device in Manage > Devices > Enrolled Devices and then click Edit, the following message appears: “A configuration error occurred. Please try again.” That message also appears when you mouse over those devices in the devices list and click Show more. In either case, click OK to continue. [CXM-73010]

Current known issues

Known issues in 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]

For sites with Workspace Environment Management (WEM) integrated with Endpoint Management: A Windows GPO configuration device policy created with User Configuration doesn’t deploy to user devices. A policy created with Device Configuration deploys as expected. [CXM-74762, WEM-6319]
Known issues in Endpoint Management 19.9.0

Enterprise apps deployed from Endpoint Management fail to install on macOS devices. This third-party issue is Apple bug #50311461. [CXM-65957]

The Settings > Apple Deployment Program page doesn’t include skip options for the new iOS 13 Setup Assistant screens. During enrollment, users must click through screens for Express Language, Preferred Language, Get Started, and Appearance. [CXM-71370]

The following setting label in the Passcode device policy is incorrect: Lock device after (minutes of inactivity) (0-999). The value range is 1-15. [CXM-73781]

Known issues in Endpoint Management 19.6.1

On the Endpoint Management console, some apps’ status displays as “Pending” even though they are already installed. This limitation is due to macOS and is specific to PKG files with different pkg and app identifiers. [CXM-72203]

Known issues in Endpoint Management 19.5.0

When enrolling a Citrix Ready workspace hub device, the Ethernet (eth0) MAC address needs to be defined in the whitelist or enrollment fails. [CXM-43141]

Known issues in Endpoint Management 19.4.1

The Monitor tab doesn’t appear. [DIR-7483]

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

Known issues in Endpoint Management 19.2.1

If you unenroll an Android Enterprise enterprise by deleting it through the Google admin console: Attempts to re-enroll the enterprise might fail. Always use the Endpoint Management console to unenroll an Android Enterprise enterprise, as described in Unenroll an Android Enterprise enterprise. G Suite customers, follow the instructions in Unenrolling an Android Enterprise enterprise. [CXM-62709] [CXM-62950]
**Known issues in Endpoint Management 19.2.0**

When creating a public store app in 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 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 Endpoint Management 10.18.19**

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

**Known issues in 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]

**Known issues in Endpoint Management 10.18.3**

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

**Known issues in Endpoint Management 10.7.4**

If you configure Endpoint Management for single sign-on using Citrix Identity Platform with Azure Active Directory: When an 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]
Known issues in Endpoint Management 10.7.3

For devices running Windows 10 RS3 Version 1709 build 16299.19: App Configuration device policies created by importing a Citrix Receiver ADMX file might fail when pushed to those devices. This third-party issue is Microsoft bug ID #14280113. [CXM-40521]

Third-party notices

January 28, 2019

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

Citrix Endpoint Management Third-Party Notices

System requirements

November 21, 2019

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

Cloud Connector requirements

Citrix uses Cloud Connector to integrate the Endpoint Management architecture into your existing infrastructure. Cloud Connector integrates the following resource locations to 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 are 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.
Citrix Endpoint Management

Citrix Gateway requirements

Endpoint Management requires a Citrix 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 Citrix Gateway to connect to internal back-end infrastructures.
- You plan to use Citrix mobile productivity apps, such as Citrix Secure Mail.
- You plan to integrate Endpoint Management with Microsoft Intune/EMS.

The requirements:

- Domain (LDAP) authentication
- NetScaler 10.5 build 66.9 or above, with a Platform/Universal license
  
  For information, see the Citrix Support article, [How to License a NetScaler Gateway Appliance](#).
- Public SSL Certificate
  
  For information, see the Citrix Support article, [How to Add an SSL Certificate Bundle on the NetScaler Appliance](#).
- Unused public IP address for Citrix Gateway Virtual Server
- Publicly resolvable Fully Qualified Domain Name (FQDN) for Citrix Gateway Virtual Server
- Cloud-hosted 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 “Citrix Gateway port requirements” later in this article.
- Endpoint Management integration with Microsoft Intune/EMS
- Deploying Citrix NetScaler VPX on Microsoft Azure

For information about NetScaler 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 Endpoint Management Premium Service offering. Storage zones controller extends the Citrix Files software as a service (SaaS) cloud storage by providing your Citrix Files account with private data storage.

Storage zones controller requirements:

- A dedicated physical or virtual machine
Citrix Endpoint Management

- Windows Server 2012 R2 or Windows Server 2016
- 2 vCPUs
- 4 GB RAM
- 50 GB hard disk space
- Server roles for Web Server (IIS):
  - 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 Endpoint Management, you open specific ports in your firewalls. The following diagram shows the traffic flow for Endpoint Management.

The following sections list the ports that you must open.

Citrix Gateway port requirements

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

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

For more information about Citrix Gateway, see Configuration Settings for your Endpoint Management Environment in the Citrix Gateway documentation. For information about IP addresses owned by NetScaler, see How a NetScaler appliance communicates with clients and servers in the NetScaler documentation. That section includes information about the NetScaler IP (NSIP) virtual server IP (VIP) and subnet IP (SNIP) addresses.

<table>
<thead>
<tr>
<th>TCP Port</th>
<th>Description</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>53 (TCP and UDP)</td>
<td>Used for DNS connections.</td>
<td>Citrix Gateway SNIP</td>
<td>DNS server</td>
</tr>
<tr>
<td>80/443</td>
<td>Citrix Gateway passes the micro VPN connection to the internal network resource through the second firewall.</td>
<td>Citrix Gateway SNIP</td>
<td>Intranet websites</td>
</tr>
<tr>
<td>123 (TCP and UDP)</td>
<td>Used for Network Time Protocol (NTP) services.</td>
<td>Citrix Gateway SNIP</td>
<td>NTP server</td>
</tr>
<tr>
<td>389</td>
<td>Used for insecure LDAP connections.</td>
<td>Citrix Gateway NSIP (or, if using a load balancer, SNIP)</td>
<td>LDAP authentication server or Microsoft Active Directory</td>
</tr>
<tr>
<td>443</td>
<td>Used for connections to StoreFront from Citrix Workspace to Citrix Virtual Apps and Desktops.</td>
<td>Internet</td>
<td>Citrix Gateway</td>
</tr>
<tr>
<td>443</td>
<td>Used for connections to Endpoint Management for web, mobile, and SaaS app delivery.</td>
<td>Internet</td>
<td>Citrix Gateway</td>
</tr>
<tr>
<td>TCP Port</td>
<td>Description</td>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>443</td>
<td>Used for Cloud Connector communication – LDAP, DNS, PKI &amp; Citrix Workspace enumeration</td>
<td>Cloud Connector Servers</td>
<td>https://<em>.citrixworkspacesapi.net, https://</em>.cloud.com (commercial), https://<em>.cloud.us (government), https://</em>.blob.core.windows.net /, https://*.servicebus.windows.net</td>
</tr>
<tr>
<td>443</td>
<td>Used for accessing the Endpoint Management Self-Help Portal, if enabled, through the browser.</td>
<td>Access point (browser)</td>
<td>Endpoint Management (https://&lt;sitename&gt;/zdm/shp)</td>
</tr>
<tr>
<td>636</td>
<td>Used for secure LDAP connections.</td>
<td>Citrix Gateway NSIP (or, if using a load balancer, SNIP)</td>
<td>LDAP authentication server or Active Directory</td>
</tr>
<tr>
<td>1494</td>
<td>Used for ICA connections to Windows-based applications in the internal network. Citrix recommends keeping this port open.</td>
<td>Citrix Gateway SNIP</td>
<td>Citrix Virtual Apps and Desktops</td>
</tr>
<tr>
<td>1812</td>
<td>Used for RADIUS connections.</td>
<td>Citrix Gateway NSIP</td>
<td>RADIUS authentication server</td>
</tr>
</tbody>
</table>
### TCP Port Description Source Destination

<table>
<thead>
<tr>
<th>TCP Port</th>
<th>Description</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>2598</td>
<td>Used for connections to Windows-based applications in the internal network using session reliability. Citrix recommends keeping this port open.</td>
<td>Citrix Gateway SNIP</td>
<td>Citrix Virtual Apps and Desktops</td>
</tr>
<tr>
<td>3269</td>
<td>Used for Microsoft Global Catalog secure LDAP connections.</td>
<td>Citrix Gateway NSIP (or, if using a load balancer, SNIP)</td>
<td>LDAP authentication server or Active Directory</td>
</tr>
<tr>
<td>4443</td>
<td>Used for accessing the Endpoint Management console by an administrator through the browser.</td>
<td>Access point (browser)</td>
<td>Endpoint Management</td>
</tr>
<tr>
<td>8443</td>
<td>Used for enrollment, app store, and mobile app management (MAM).</td>
<td>Citrix Gateway SNIP</td>
<td>Endpoint Management</td>
</tr>
<tr>
<td>8443</td>
<td>Secure Ticket Authority (STA) port used for Secure Mail authentication token</td>
<td>Citrix Gateway SNIP</td>
<td>Endpoint Management</td>
</tr>
</tbody>
</table>

### Network and firewall requirements

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

Open ports from the internal network to Citrix Cloud:
<table>
<thead>
<tr>
<th>TCP port</th>
<th>Source IP</th>
<th>Description</th>
<th>Destination</th>
<th>Destination IP</th>
</tr>
</thead>
</table>
## Citrix Endpoint Management

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Source IP</th>
<th>Description</th>
<th>Destination</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td></td>
<td>Endpoint Management Self-Help Portal access through a browser (if the portal is enabled)</td>
<td>Endpoint Management</td>
<td></td>
</tr>
<tr>
<td>4443</td>
<td></td>
<td>Endpoint Management console access through a browser</td>
<td>Endpoint Management</td>
<td></td>
</tr>
</tbody>
</table>

### Open ports from the Internet to the DMZ:

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Source IP</th>
<th>Destination</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Endpoint Management Client Device</td>
<td>Citrix Gateway IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Endpoint Management Client Device</td>
<td>NetScaler VIP</td>
<td>Citrix Files</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Citrix Files Public IP</td>
<td>CTX208318</td>
<td>NetScaler VIP</td>
<td>Citrix Files</td>
</tr>
</tbody>
</table>

### Open ports from the DMZ to the internal network:

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Source IP</th>
<th>Destination</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>389 or 636</td>
<td>NetScaler NSIP</td>
<td></td>
<td>Active Directory</td>
<td>IP</td>
</tr>
<tr>
<td>53 (UDP)</td>
<td>NetScaler NSIP</td>
<td></td>
<td>DNS Server IP</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>NetScaler SNIP</td>
<td></td>
<td>Exchange (EAS)</td>
<td>Server IP</td>
</tr>
</tbody>
</table>
Citrix Endpoint Management

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Source IP</th>
<th>Destination</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>NetScaler SNIP</td>
<td>Internal Web Apps/Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>NetScaler SNIP</td>
<td>Storage zones controller IP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Open ports from the internal network to the DMZ:

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Source IP</th>
<th>Destination</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Admin Client</td>
<td>NetScaler NSIP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Open ports from the internal network to the Internet:

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Source IP</th>
<th>Destination</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Exchange (EAS) Server IP</td>
<td>Endpoint Management Push Notification Listeners (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Storage zones controller IP</td>
<td>Citrix Files Control Plane</td>
<td>CTX208318</td>
<td></td>
</tr>
</tbody>
</table>

(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:

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Source IP</th>
<th>Destination</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>8443 / 443</td>
<td>Endpoint Management Client Device</td>
<td>Endpoint Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5223</td>
<td>Endpoint Management Client Device</td>
<td>Apple APNS Servers</td>
<td>17.0.0.0/8</td>
<td></td>
</tr>
<tr>
<td>TCP port</td>
<td>Description</td>
<td>Source IP</td>
<td>Destination</td>
<td>Destination IP</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>5228</td>
<td>Endpoint Management Client Device</td>
<td>Firebase Cloud Messaging</td>
<td>android.apis.google.com, cm.googleapis.com</td>
<td></td>
</tr>
<tr>
<td>5229</td>
<td>Endpoint Management Client Device</td>
<td>Firebase Cloud Messaging</td>
<td>android.apis.google.com, cm.googleapis.com</td>
<td></td>
</tr>
<tr>
<td>5230</td>
<td>Endpoint Management Client Device</td>
<td>Firebase Cloud Messaging</td>
<td>android.apis.google.com, cm.googleapis.com</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Endpoint Management Client Device</td>
<td>Firebase Cloud Messaging</td>
<td>cm.googleapis.com</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Endpoint Management Client Device</td>
<td>Windows Push Notification Service</td>
<td>*.notify.windows.com</td>
<td></td>
</tr>
<tr>
<td>TCP port</td>
<td>Description</td>
<td>Source IP</td>
<td>Destination</td>
<td>Destination IP</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------</td>
<td>----------------------</td>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>443 / 80</td>
<td>Endpoint Management</td>
<td>Google Play</td>
<td>play.google.com, android.clients.google.com, android.l.google.com, android.com, google.com, google-analytics.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Endpoint Management</td>
<td>Microsoft App Store</td>
<td>login.live.com, *, notify.windows.com</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Endpoint Management AutoDiscovery Service</td>
<td>Endpoint Management</td>
<td>ads.xm.cloud.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Storage zones controller IP</td>
<td>Citrix Files Control Plane</td>
<td>CTX208318</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Endpoint Management</td>
<td>Google Mobile Management, Google APIs, Google Play Store APIs</td>
<td>*googleapis.com</td>
<td></td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
## Port requirement for Auto Discovery Service connectivity

This port configuration ensures that Android devices connecting from Secure Hub for Android can access the 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 Endpoint Management server and NetScaler certificates:** The certificates must be in PEM format and must be a public certificate and not the private key.
- **Contact Citrix Support and place a request to enable certificate pinning:** During this process, you are asked for your certificates.

Certificate pinning requires that devices connect to ADS before the device enrolls. This requirement ensures that the latest security information is available to Secure Hub. For Secure Hub to enroll a

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Source IP</th>
<th>Destination</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Endpoint Management Client Device</td>
<td>Connectivity check prior to CloudDPC v470. Android connectivity check starting with N MR1 requires <code>https://www.google.com/generate_204</code> to be reachable, or for the given Wi-Fi network to point to a reachable PAC file)</td>
<td>connectivitycheck.android.com, <a href="http://www.google.com">www.google.com</a></td>
<td></td>
</tr>
</tbody>
</table>
device, the device must reach the ADS. Therefore, opening ADS access within the internal network is critical to enabling devices to enroll.

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

<table>
<thead>
<tr>
<th>FQDN</th>
<th>IP address</th>
<th>Port</th>
<th>IP and port usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ads.xm.cloud.com</td>
<td>52.5.138.94</td>
<td>443</td>
<td>Secure Hub - ADS Communication</td>
</tr>
<tr>
<td>ads.xm.cloud.com</td>
<td>52.1.30.122</td>
<td>443</td>
<td>Secure Hub - ADS Communication</td>
</tr>
<tr>
<td>ads.xm.cloud.com</td>
<td>34.194.83.188</td>
<td>443</td>
<td>Secure Hub - ADS Communication</td>
</tr>
<tr>
<td>ads.xm.cloud.com</td>
<td>34.193.202.23</td>
<td>443</td>
<td>Secure Hub - ADS Communication</td>
</tr>
</tbody>
</table>

**Android Enterprise network requirements**

There are a number of outbound connections that you should be aware of when setting up network environments for Android Enterprise.

**Port requirements**

If the console is located on-premises, the following destination hosts need to be reachable from the network to create a Managed Google Play Enterprise and to access the Managed Google Play iFrame. Google has made the Managed Play iFrame available to developers to simplify the search and approval of apps.

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Destination host</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Google Play Store, Play Enterprise sign-up</td>
<td>play.google.com</td>
</tr>
<tr>
<td>443</td>
<td>Account authentication</td>
<td>accounts.youtube.com, accounts.google.com</td>
</tr>
<tr>
<td>443</td>
<td>GCM and other Google web services</td>
<td>apis.google.com</td>
</tr>
</tbody>
</table>
| 443      | iFrame UI elements                  | ogs.google.com
Endpoint Management compatibility

November 18, 2019

To use new features, fixes, and policy updates, Citrix recommends that you install the most recent version of the MDX Toolkit and mobile productivity apps (formerly, XenMobile Apps). You can use the MDX Service instead of the MDX Toolkit. For details, see Endpoint Management MDX Service.

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

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

Mobile productivity apps

The latest version of the mobile productivity apps requires the latest version of Secure Hub. The two previous versions of the apps are compatible with the latest Secure Hub.

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

MDX Toolkit and MDX Service

- Citrix supports the latest three releases (n.n.n) of MDX Toolkit. You can also use Endpoint Management MDX Service for wrapping apps. For details, see Endpoint Management MDX Service.
- The latest on-prem toolkit version is MDX Toolkit 19.11.5 (for iOS and Android) for wrapping third-party apps. You can upgrade to MDX Toolkit 19.11.5 from MDX Toolkit 19.9.5 and 19.9.0.

<table>
<thead>
<tr>
<th>TCP port</th>
<th>Description</th>
<th>Destination host</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Desktop and mobile notifications</td>
<td>notifications.google.com</td>
</tr>
<tr>
<td>443</td>
<td>Google Fonts user generated content</td>
<td>fonts.googleapis.com, *.gstatic.com, *.googleusercontent.com</td>
</tr>
<tr>
<td>443</td>
<td>Certificate validation</td>
<td>cri.pki.goog, ocsp.pki.goog</td>
</tr>
</tbody>
</table>
The MDX Toolkit 10.7.10 was the final release that supported the wrapping of mobile productivity apps (formerly, XenMobile Apps). Users access the mobile productivity apps from the public app stores.

**Browser support**

Endpoint Management supports the following browsers:

- Internet Explorer, although not versions 9 or earlier
- Chrome
- Firefox
- Safari on mobile devices for use with the Self-Help Portal

Endpoint Management is compatible with the most current version of the browser and one version before the current version.

**Supported device operating systems**

November 1, 2019

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

For supported device types and operating systems for Citrix mobile productivity apps and MDX, see Support for mobile productivity apps.

**Note:**

Citrix supports, at a minimum, the current and prior version of each major operating system platform. Not all features of the newer version of Endpoint Management work on older platform releases.

**Operating system support list**

Citrix Endpoint Management supports the following operating systems:

- **Android:** 6.x, 7.x, 8.x, 9.x, Android Q
  
  **Note:**

  For Android Q, see Android considerations.

- **Chrome OS:** Chromebook
• **iOS:** 11.x, 12.x, 13.x

• **iPadOS:** 13.x

• **macOS:** 10.11 El Capitan, 10.12 Sierra, 10.13 High Sierra

• **tvOS:** 10.2, 11.x, 12.x, 13.x. Requires 4th generation Apple TV devices enrolled using Apple Deployment Program.

• **Windows 10 Desktops and Tablets:** Windows 10 RS4 and RS5 (MDM only)

• **Windows Phone:** Windows Phone 8.1, Windows Phone 10, Windows 10 RS4, and Windows 10 RS5. MDM only.

• **Windows Mobile/CE:** (MDM only). Starting the second quarter of 2018, support for Windows Mobile/CE devices is no longer available to new customers.

• **Raspberry Pi platform:** Citrix Ready workspace hub, built on the Raspberry Pi 3 platform. For more information about Workspace hub requirements, see [Citrix Ready workspace hub](#).

• **Symbian devices:** Starting the second quarter of 2018, support for Symbian devices is no longer available to new customers. The following list includes some of the Symbian devices that Endpoint Management supports for customers who previously configured these devices.
  - Symbian 3
  - Symbian S60 5th Edition
  - Symbian S60 3rd Edition, Feature Pack 2
  - Symbian S60 3rd Edition, Feature Pack 1
  - Symbian S60 3rd Edition
  - Symbian S60 2nd Edition, Feature Pack 3
  - Symbian S60 2nd Edition, Feature Pack 2

• **Samsung SAFE and Knox:** On compatible Samsung devices, Endpoint Management supports and extends both Samsung for Enterprise (SAFE) and Samsung Knox policies. Endpoint Management requires that you enable the SAFE APIs before you deploy SAFE policies and restrictions. To do that, deploy the built-in Samsung Enterprise License Management (ELM) key to a device. To enable the Samsung Knox API:
  1. Purchase a Samsung Knox license by using the Samsung Knox License Management System (KLMS).
  2. Deploy the Samsung ELM key.

• **HTC:** For HTC-specific policies, HTC API version 0.5.0

• **Sony:** For Sony-specific policies, Sony Enterprise SDK 2.0

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Android considerations

Before upgrading to the Android Q platform: See Migrate from device administration to Android Enterprise for information about how the deprecation of Google Device Administration APIs impacts devices running Android Q. Also see the blog, https://www.citrix.com/blogs/2019/06/26/citrix-endpoint-management-and-android-enterprise-a-season-of-change/.

- Citrix recommends that you avoid enrolling Android Q devices in legacy device administration mode. Google is deprecating Device Administration APIs, which impact devices running Android Q. After the APIs get deprecated, enrollment of Android Q devices in legacy device administration mode will fail.
- Citrix recommends using Android Enterprise for Android Q 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.

Before upgrading to the Android P platform:

- Ensure that your server infrastructure is compliant with security certificates that have a matching host name in the subjectAltName (SAN) extension.
- To verify a host name, the server must present a certificate with a matching SAN. Citrix trusts certificates only if they contain a SAN that matches the host name.
- For details, see the Android Developer site article on Android P behavior changes.

With the release of Android O (version 8):

- SSLv3 is not supported with Android O. Google no longer supports SSLv3 connections. As a result, mobile productivity apps running on Android O devices cannot connect to internal servers that use SSLv3 connections. If you have servers using SSLv3, it’s important to address its limitations before rolling out Android O. Addressing those limitations avoid connectivity failures with users.
- Support ended for Android 4.4x as of the version 10.6.20 public app store release of Citrix mobile productivity apps.
- Citrix mobile productivity apps and MDX-wrapped apps are available on Android devices with ARM-based processors. They are not supported on Intel x86 or x64-based Android devices.

Language support

August 23, 2019
Citrix mobile productivity apps and the 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 is not 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 release of Endpoint Management.

**Endpoint Management console and the Self-Help Portal**

- French
- German
- 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**

<table>
<thead>
<tr>
<th>Language</th>
<th>Secure Hub</th>
<th>Secure Mail</th>
<th>Secure Web</th>
<th>Secure Notes</th>
<th>Secure Tasks</th>
<th>QuickEdit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japanese</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Simplified Chinese</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Traditional Chinese</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>French</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>German</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Spanish</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Korean</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Portuguese</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Dutch</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
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 is not available for Windows devices.

<table>
<thead>
<tr>
<th>Language</th>
<th>Secure Hub</th>
<th>Secure Mail</th>
<th>Secure Web</th>
<th>Secure Notes</th>
<th>Secure Tasks</th>
<th>QuickEdit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Italian</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Danish</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Swedish</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Hebrew</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>iOS only</td>
</tr>
<tr>
<td>Arabic</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Russian</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Turkish</td>
<td>X</td>
<td>X</td>
<td>Android only</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Polish</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**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 is not available for Windows devices.

<table>
<thead>
<tr>
<th>App</th>
<th>iOS</th>
<th>Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Hub</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Secure Mail</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Secure Web</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Secure Tasks</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Secure Notes</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>QuickEdit</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**Note:**

Secure Notes and Secure Tasks reached End of Life (EOL) status on December 31, 2018. For details, see [EOL and deprecated apps](#).  

© 1999-2019 Citrix Systems, Inc. All rights reserved.
About Endpoint Management

November 21, 2019

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

MDM features of 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 Endpoint Management let you:

• Secure apps and data on BYO mobile devices.
• Deliver enterprise mobile apps.
• Lock 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

For more information, see Management modes.

Architecture

The device and app management requirements of your organization determine the Endpoint Management components in your Endpoint Management architecture. The components of Endpoint Management are modular and build on each other. For example, your deployment includes Citrix Gateway to give users remote access to mobile apps and to track user device types. Endpoint Management is where you manage apps and devices, and Citrix Gateway enables users to connect to your network.

The following diagram shows a general architectural overview of an Endpoint Management cloud deployment and its integration with your data center.
The following subsections contain reference architecture diagrams for the core Endpoint Management and for optional components such as an external Certificate Authority and Endpoint Management connector for Exchange ActiveSync.

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

Core reference architecture

For details about port requirements, see System requirements.
Reference architecture with Citrix Virtual Apps and Desktops
Reference architecture with Endpoint Management connector for Exchange ActiveSync
Resource locations

Place resource locations where they best meet your business needs. For example, in a public cloud, in a branch office, 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. Alternatively, 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

Citrix uses Cloud Connector to integrate the Endpoint Management architecture into your existing infrastructure. Cloud Connector authenticates and encrypts all communication between Citrix Cloud and your resource locations. Cloud Connector supports all Endpoint Management authentication types.

The following diagram shows the traffic flow for Cloud Connector.

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

A solution that includes Mobile App Management (MAM) requires a micro VPN that is provided by an on-premises Citrix Gateway. Cloud Connector, Citrix Gateway, and your servers for Exchange, web apps, Active Directory, and PKI reside in your data center. Mobile devices communicate with Endpoint Management and your on-premises Citrix Gateway.

Endpoint Management components

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

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

- The Remote Support client is not available for Endpoint Management.
- Endpoint Management server-side components are not FIPS 140-2 compliant.
- Citrix does not support syslog integration in Endpoint Management with an on-premises syslog server. Instead, you can download the logs from the Troubleshooting and Support page in the Endpoint Management console. When doing so, you must click Download All.

MDX Service. The Endpoint Management MDX Service securely wraps mobile apps created within your organization or outside the company. For more information, see MDX Service.

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

Endpoint Management connector for Exchange ActiveSync. 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 Endpoint Management environment. The connector doesn’t require the use of Citrix Gateway.
You can deploy the connector without changing routing for the existing ActiveSync traffic. For more information, see Endpoint Management connector for Exchange ActiveSync.

**Citrix Gateway connector for Exchange ActiveSync.** Citrix 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, by using Citrix 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 Citrix Gateway and the Endpoint Management server. For more information, see Citrix Gateway connector for Exchange ActiveSync.

**Endpoint Management technical security overview**

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

The following figure illustrates the service and its security boundaries.

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.
Citrix Endpoint Management

- Is not intended to serve as configuration and administration guidance for Citrix Cloud or any of its components or services.

**Data flow**

The control plane has limited read-access to user and group objects from a customer directory and other services such as DNS. The control plane accesses those services over Citrix Cloud Connector, which uses secure HTTPS connections.

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

**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 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 Citrix Gateway within your environments.
Citrix Endpoint Management

More resources

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

Citrix Endpoint Management integration with Microsoft Intune/EMS

December 5, 2019

Endpoint Management integration with Microsoft Enterprise Mobility + Security (EMS)/Intune adds the value of Endpoint Management micro VPN to Microsoft Intune aware apps, such as Microsoft Managed Browser.

Endpoint Management integration with EMS/Intune also allows enterprises to wrap their own line of business apps with Intune and Citrix to provide micro VPN capabilities inside an Intune mobile app management (MAM) container. 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 for ultimate security and productivity.

This release supports the following use cases:

- Intune MAM
- Intune MAM and Intune mobile device management (MDM)
  Secure Mail for iOS supports single sign-on for this use case.
- Intune MAM with Endpoint Management MDM+MAM

Important:

Secure Mail only works in Citrix MAM mode in this use case.

Getting Started Guide

This document is an easy-to-follow, graphical guide to setting up Endpoint Management integration with EMS/Intune.

System requirements

- Citrix Gateway version 12.0.59.x or 12.1.50.x or later. You can download the latest version of Citrix Gateway from the Citrix Gateway download page.
Citrix Endpoint Management

- A Windows desktop running Windows 7 or later (for Android app wrapping only)
- A Mac running macOS 10.10 or later (for iOS or Android app wrapping)
- Mobile platforms:
  - iOS 11.x
  - Android 6.x, 7.x, 8.x

Microsoft

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

Firewall rule

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

Prerequisites

- Intune environment: If you don’t have an Intune environment set up, follow the steps in the Microsoft Intune documentation.

- Intune app wrappers: Microsoft hosts the wrappers in a private GitHub repository that you need an invitation to access. After you receive an invitation, download the wrappers from Microsoft. You can find links to download the wrappers from the Microsoft Intune App SDK documentation on the Microsoft Intune documentation site noted above.

- Managed Browser: The Mobile Apps SDK is integrated within the Intune Managed Browser app for iOS and Android. For more information about the Managed Browser, see the Microsoft Managed Browser page.

- Installations of the Android SDK and the Java JDK: Install these SDKs on the machine you use to wrap apps. For details about the Intune SDK, see the Microsoft Intune App SDK for Android developer guide.

- JDK environment variable: Set the JDK environment variable for the JDK to change the path to match your JDK version and installed location.
  Example: \$env:Path += ”;C:\Program Files\Java\jdk1.8.0_121\bin”

- 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 proceed, 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 certificates 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.

**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 required resources and APIs. Some apps require consent by the Azure AD 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 details, see the Microsoft Graph permissions reference.

- **Sign in and read user profile**: This permission allows users to sign in and connect to Azure AD. Note that Citrix does not view user credentials.

- **Read all users’ basic profiles**: The app reads profile properties on behalf of users in the organization. The properties include 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 enumerated for app and policy assignment.

- **Access directory as the signed-in user**: This permission verifies the Intune subscription and enables Citrix Gateway and VPN configurations.

- **Read and write Microsoft Intune apps**: The app can read and write Microsoft-managed properties, group assignments and the status of apps, app configurations, and app protection policies.

In addition, during the Citrix 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 Citrix Gateway uses to communicate with AAD and Intune.

The global administrator must not have the role of Citrix administrator. Instead, the Citrix administrator assigns Azure AD accounts to users with appropriate Intune application admin privileges.
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 never has access to the password.

**To configure Endpoint Management integration with EMS/Intune**

For a video summary of the integration, watch:

1. Log on to the Citrix Cloud site and request a trial for Endpoint Management.
2. A sales engineer schedules an onboarding meeting with you. Let them know that you want Endpoint Management integration with EMS/Intune. 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**.
4. Follow the link in the first step to the **Identity and Access Management** page.
5. Click **Connect** to connect your Azure AD installation.
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 permissions request.

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

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:**
   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, ensure that you sign out of all other accounts.

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

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

### To configure Citrix Gateway for micro VPN

To use micro VPN with Intune, you must configure Citrix Gateway to authenticate to Azure AD. An existing Citrix 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 ensure that authentication between Intune and Citrix Gateway occurs properly.

1. From the Citrix Cloud console, under **Endpoint Management**, click **Manage**.

2. Next to **Micro VPN**, click **Configure Micro VPN**.

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

   This script configures Citrix 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 is not set up until you run the script on your Citrix Gateway installation.
To configure device management

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

Note:
By default, Intune MDM is selected for the console. To use Intune as your MDM provider, see the Microsoft Intune documentation.

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

2. Enter a unique site name, select the Cloud region closest to you and then click Request a Site. A prompt lets you know that you receive an email when your site is ready.

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 instructions on screen to install the cloud connector. After installation, click Test Connection to verify the connection between Citrix Cloud and the Cloud Connector.

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

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

Wrapping iOS apps

Microsoft has enhanced their Intune App Wrapping Tool to add the optional parameter “-citrix”. As a final step, this parameter invokes the MDX Toolkit command line interface (CLI) CGAppCLPrepTool to wrap the application. To wrap the app with Intune, follow the instructions at Prepare line of business apps for MAM.

Important:
Ensure that you use the wrapping tool supplied for this release and not the one linked to from the article.

Several MDX options exist. See the list below for a description of each MDX Variant.

- **MDX network-only wrapper**: Only Intune MDM, Intune MAM, or Endpoint Management MDM+MAM can manage this wrapper. Wrap the app by using the Intune App Wrapping Tool and specify the “-citrix” option. This wrapper is a minimal version of MDX that only has support for micro VPN without containment or encryption.

- **MDX Wrapper**: Has support for other types of policies, including containment. Does not support encryption. Wrap the app with the Intune App Wrapping tool and then the MDX Toolkit.

- **Citrix Mobile Apps SDK**: Use the Citrix Mobile Apps SDK when developing an app to access all MDX features, including encryption.

You can achieve the same result if, when building your iOS app, you link the Citrix Mobile Apps SDK framework and Intune SDK framework. For more information on the Citrix Mobile Apps SDK and Intune SDK, see [MDX Developer Guide](#) and [Intune App SDK overview](#) respectively.

Customer line of business apps that consume the Intune SDK for containment or networking purposes.

<table>
<thead>
<tr>
<th>Use case example</th>
<th>Intune</th>
<th>Citrix MDX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Line of Business consuming Intune SDK</td>
<td>Intune SDK</td>
<td>MDX network-only wrapper</td>
</tr>
<tr>
<td>needing containment or networking.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citrix mobile productivity apps or Line of Business</td>
<td>Intune SDK</td>
<td>Citrix Mobile Apps SDK</td>
</tr>
<tr>
<td>apps that require containment and networking capabilities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line of Business apps for network-only wrapper.</td>
<td>Intune wrapper</td>
<td>MDX network-only wrapper</td>
</tr>
<tr>
<td>Use of the Microsoft Managed Browser.</td>
<td>Intune SDK already embedded in the app</td>
<td>MDX network-only support already embedded in the app</td>
</tr>
</tbody>
</table>

**Wrapping Android apps**

Wrapping an Android app works similarly to iOS. The tool you use to wrap Android apps is the ManagedAppUtility.jar. You can use the ManagedAppUtility.jar to wrap apps with the full version of MDX or with the network-only version. To use the network-only wrapper, use the “-mVPN” parameter.
See the following table for examples of when to use each wrapping variant.

### Android wrapping scenarios

<table>
<thead>
<tr>
<th>Use case example</th>
<th>Intune</th>
<th>Citrix MDX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft managed browser</td>
<td>Intune SDK</td>
<td>MDX network-only wrapper</td>
</tr>
<tr>
<td>Citrix mobile productivity apps</td>
<td>Intune SDK</td>
<td>MDX for Citrix mobile productivity apps</td>
</tr>
<tr>
<td>Line of business apps for network-only wrapper</td>
<td>Intune wrapper</td>
<td>MDX network-only wrapper</td>
</tr>
</tbody>
</table>

### To add apps to Endpoint Management integration with EMS/Intune console

To add Intune managed apps, follow these steps.

1. From the Citrix Cloud console, click the menu icon and then click **Library**.
2. Click the blue plus sign icon on the upper-right and then click **Add a Mobile app**.
   
   You may need to wait a minute for the options to populate the list.
3. 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 MDX wrapped apps, such as Intune app protection policies and the default MDX policies contained in the package; and 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 is not wrapped with Intune, Intune app protection policies do not apply.
4. If you clicked **Upload my own App**, upload your .mdx or Intune wrapped file.
5. Enter a name and description for the app, choose whether the app is featured or required, and then click **Next**.
6. Set the **Network access** policy to select whether and how to allow micro VPN access. Enabling micro VPN allows the app controlled access to on-premises resources.
- **Unrestricted**: Disables micro VPN access. The app has access to the network with no restrictions, without using the micro VPN. This is the default setting.

  **Note:**
  In version 18.12.0: If you configure unrestricted network access and set the micro VPN session required policy to Yes, the network is unavailable.

- **Tunneled - Full VPN**: Enables micro VPN full tunnel (TCP level) redirection.

- **Tunneled - Web SSO**: Enables HTTP/HTTPS redirection (with SSO) redirection for micro VPN.

- **Tunneled - Full VPN and Web SSO**: Enables micro VPN full tunnel (TCP level) redirection and HTTP/HTTPS redirection (with SSO) redirection.

  This option allows automatic switching between full VPN and Web SSO modes as needed. If a network request fails due to an authentication request that cannot be handled in full VPN mode, the request is retried in the alternate mode. For example, the full VPN can accommodate server challenges for client certificates. Web SSO mode is more likely to service HTTP authentication challenges.

  This setting is the equivalent to the now deprecated policy, PermitVPNModeSwitching.

7. If you enable micro VPN access, set the **micro VPN session required** policy to select whether to require an online session for the app to work. Select **Yes** to require an online session. The default is **No**.

8. If you enable micro VPN access, you can specify an **mVPN tunnel exclusion list**. Enter domains, separated by commas, that you want to exclude from the micro VPN policies.

   For more information on these policies, see MDX Policies.

9. Configure more policies for the app and then click **Next**. For a complete list of app policies, see MDX Policies at a Glance.

   **Note:**
   Not all of these policies are available.

10. Review the summary of the app and then click **Finish**.

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

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

12. In the search box, search for user groups and click to add them. You cannot add individual users.

13. When you have added all groups, you can close the window by clicking the X.
Citrix Endpoint Management

You may encounter an error when adding user groups. This error occurs when the user group has not been synchronized to Local Active Directory.

**MDX policies**

When you wrap an app with MDX technology or you use the Citrix Mobile Apps SDK to build the app, Intune administrators can configure the MDX policies. These policies include a subset of Citrix MDX policies that do not require Secure Hub to manage the app. Citrix recommends that you use the following MDX policies.

The following set of Intune-specific network management policies control the network policy configuration for MDX (full or network only) when managed by Intune. Some of these policies correspond to existing Citrix MDX network containment policies. Others are specific to Intune configuration and control.

**Important:**

The MDX Toolkit version 18.12.0 release included new policies that combined or replaced older policies. The Network Access policy combines Network access, Preferred VPN mode, and Permit VPN mode switching. The Exclusion list policy replaces Split tunnel exclusion list. The micro VPN session required policy replaces micro VPN session required. For details, see What's new in the MDX Toolkit 18.12.0.

Tunneled - Web SSO is the name for Secure Browse in the settings. The behavior is the same.

- **Enable http/https redirection:** Enables or disables HTTP/HTTPS redirection through the Citrix Gateway reverse web proxy endpoint, also known as Tunneled - Web SSO. When **On**, Tunneled - Web SSO is used for web traffic. When using the Tunneled - Web SSO endpoint, the gateway is able to respond to HTTP authentication challenges inline, providing a single-sign-on (SSO) experience. To use Tunneled - Web SSO, set this policy to **On**. Full-tunnel redirection is required for apps that use client certificates for end-to-end SSL with mutual authentication. For those apps, this option needs to be disabled. Default value is **On**.

- **Disable mVPN full tunnel (TCP level) redirection:** Enable or disable TCP level network level redirection through the Citrix Gateway VPN tunneling endpoint. Under normal circumstances, always leave this policy enabled. However, troubleshooting web SSO issues is often easier when preventing TCP level interception of web traffic that standard web interception functions do not catch. Default value is **On**.

- **mVPN session required:** If **On**, the SDK ensures that the configured gateway is reachable and a valid micro VPN session is available before allowing app to become active. If there is no network, the gateway is unreachable or a logon session cannot be established. The app remains blocked until a working micro VPN session can be confirmed. If **Off**, the app opens regardless of network...
condition. A micro VPN session is initialized as needed when an app configured for tunneled access attempts to use one of the redirected network APIs. Default value is Off.

- **mVPN tunnel exclusion list**: Comma-separated list of host or domain names to be excluded from being routed through the Citrix Gateway reverse web proxy. The host or domain names are excluded even though the gateway configured split DNS settings might otherwise select the domain or host.

  **Note:**
  This policy is only enforced for Tunneled - Web SSO connections. If **Enable http/https redirection** is Off, this policy is ignored.

For more information about these policies, see [MDX Policies for iOS Apps](#).

**Deploying policies for line of business apps**

After you’ve uploaded your apps to Intune, follow this procedure to apply policies to those apps.

1. Sign in to [https://portal.azure.com/](https://portal.azure.com/) and then navigate to **Intune > Mobile apps**.
2. Under Manage, click **App configuration policies**.
3. Click **Add** and then enter a name for the policy you want to create. For **Enrollment Type**, select **Not Enrolled with Intune**. This selection is a limitation of the current system.
4. Click **Associated App**, select the apps to which you want to apply the policy, and then click **OK**.
5. Click **Configuration Settings**.
6. In the **Name** field, enter the name of one of the policies noted in the following section in this article.
7. In the **Value** field, enter the value you want to apply for that policy. Click off the field to add the policy to the list. You can add multiple policies.
8. Click **OK** and then click **Add**. The policy is added to your list of policies.
9. You can delete the policy. To do so, select the policy and then click **Delete Policy** on the right.

**Line of business policies**

The following table lists the policies you can deploy for line of business apps. In addition to these policies, you can also use the policies listed earlier in this article for MDX. For more information about these policies, see [MDX Policies at a Glance](#).
<table>
<thead>
<tr>
<th>Name (iOS/Android)</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppLogLevel/DefaultLoggerLevel</td>
<td>Controls default verbosity of the mobile productivity app diagnostic logging facility. Higher-level numbers include more detailed logging.</td>
<td>1–5</td>
</tr>
<tr>
<td>AppLogTarget/DefaultLoggerOut</td>
<td>Determines which output media are used by the mobile productivity app diagnostic logging facilities by default.</td>
<td>File, Console, or Both</td>
</tr>
<tr>
<td>AppLogFileSize/MaxLogFileSize</td>
<td>Limits the size in MB of the log files retained by the mobile productivity app diagnostic logging facility before rolling over. Minimum is 1 MB. Maximum is 5 MB.</td>
<td>1–5</td>
</tr>
<tr>
<td>AppLogFileCount/MaxLogFiles</td>
<td>Limits the number of log files retained by the mobile productivity app diagnostic logging facility before rolling over. Minimum is 2. Maximum is 8.</td>
<td>2–8</td>
</tr>
</tbody>
</table>

**To configure Secure Mail**

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

**Important:**

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

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

1. From your 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
   ```xml
   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 Secure Mail app.

9. In the **Dictionary** content box, type the following text.

   ```xml
   <dict>
   <key>XenMobileUserAttributes</key>
   <dict>
   <key>userPrincipalName</key>
   <string>${ user.userprincipalname }</string>
   <key>email</key>
   <string>${ user.mail }</string>
   <key>displayname</key>
   <string>${ user.displayname }</string>
   <key>sAMAccountName</key>
   </dict>
   </dict>
   ```
<string>${user.samaccountname}</string>

<string>${user.id_token.upn}</string>

<string>${user.id_token.tid}</string>

<string>${user.id_token.upn}</string>

10. Clear the **Windows Phone** and **Windows Desktop/Tablet** check boxes 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:** When wrapping an app, the following error appears:

Failed to **package** app.
com.microsoft.intune.mam.apppackager.utils.AppPackagerException: This app already has the MAM SDK integrated.
com.microsoft.intune.mam.apppackager.PackagerMain.mainInternal(PackagerMain.java:198)
com.microsoft.intune.mam.apppackager.PackagerMain.main(PackagerMain.java:56)

The application could not be wrapped.

Resolution: The app is integrated with the Intune SDK. You do not need to wrap the app with the Intune wrapper.

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

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

Citrix Gateway issues

The following table lists common issues with Citrix 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 shell using tail -f /var/log/ns.log

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The permissions required to be configured for Gateway App on Azure are unavailable.</td>
<td>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.</td>
</tr>
<tr>
<td>Citrix Gateway cannot reach login.microsoftonline.com and graph.windows.net.</td>
<td>From NS Shell, check if you are able to reach the following Microsoft website: curl -v -k <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>. Then, check whether DNS is configured on Citrix Gateway and that the firewall settings are correct (in case DNS requests are firewallled).</td>
</tr>
<tr>
<td>An error appears in ns.log after you configure OAuthAction.</td>
<td>Check if Intune licensing is enabled and the Azure Gateway app has the proper permissions set.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Status</th>
<th>Error Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPLETE</td>
<td>Success</td>
</tr>
<tr>
<td>AADFORGRAPH</td>
<td>Invalid secret, URL not resolved, connection timeout</td>
</tr>
<tr>
<td>MDMINFO</td>
<td>*manage.microsoft.com is down or unreachable</td>
</tr>
<tr>
<td>GRAPH</td>
<td>Graph endpoint is down unreachable</td>
</tr>
<tr>
<td>CERTFETCH</td>
<td>Cannot talk to “Token Endpoint: <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> because of a DNS error. To validate this configuration, go to shell and type curl <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>. This command must validate.</td>
</tr>
</tbody>
</table>

### Limitations

The following items describe some limitations of using Microsoft EMS/Intune 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 Citrix 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 cannot open documents in unmanaged apps until they close and relaunch Secure Mail. [CXM-34990]
- When split tunnel 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, Secure Mail does not function. [CXM-58886]

**Third-party known issues**

On 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 Secure Mail screen when users move the app to the background is not enforced. [CXM-25032]

**Onboarding and resource setup**

December 16, 2019

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

- **Where do I start?**
  - If you haven’t purchased an Endpoint Management subscription, see **For new Citrix customers**.
  - If you have an Endpoint Management subscription, skip to **When the Manage button is available**.
  - If your Endpoint Management site is provisioned, skip to **Configure LDAP**.

- **Does the configuration order matter?** This article follows a recommended configuration sequence. You can work in a different order. The Endpoint Management console lets you know if prerequisites are missing, through messages such as “Set up after provisioning”.

Provide us with your feedback for the new console experience in Endpoint Management using the **Citrix Endpoint Management Console Feedback** link.

**For new Citrix customers**

For Citrix Cloud customers new to Endpoint Management:
If you already purchased an Endpoint Management subscription, skip to When the Manage button is available.

If you already set up a Citrix Cloud account, but haven’t purchased 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 Endpoint Management administrators by default.
- Citrix Cloud administrators created with customer access must have Endpoint Management selected for them to administrate Endpoint Management.

2. On the Citrix Cloud home page, locate the Endpoint Management service tile and click Request Demo. A demo request page appears.

3. Complete and submit the form. The button on the Endpoint Management services tile changes to Demo Requested.

If you click the Endpoint Management services tile before your request is handled, the following screen appears. We advise that you contact your representative or partner. A Citrix sales representative can provide more information and detail about the service.
While waiting for the trial, be sure to prepare for your Endpoint Management deployment by reviewing System requirements. Although Citrix hosts and delivers your Endpoint Management solution, you must handle some communication and port requirements.

Continue with the next section.

**When the Manage button is available**

When your Endpoint Management service is available, the button on the 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 Endpoint Management tile.
3. Type your site name and select a region.

The Endpoint Management console then opens with a provisioning status message.

Note:
To request IP whitelisting, contact the Citrix Support representative.
1. In the **Welcome** screen, click **Start setup**.
2. Select the endpoints you want to manage. 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.
Citrix Endpoint Management

Citrix sends you an email when provisioning completes.

**Resource Center**

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

![Resource Center Icon](image)

**During provisioning**

While we provision 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 Endpoint Management. Resource locations contain 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 Endpoint Management deployment by reviewing System requirements. Although Citrix hosts and delivers your Endpoint Management solution, some communication and port requirements are required. That setup connects the Endpoint Management infrastructure to corporate services, such as Active Directory. The information that you must provide is included in the Onboarding Handbook under “Endpoint Management Trial Sales Engineer engagement.”

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

After your site is provisioned, you can continue with configuration. We recommend that you start with the LDAP authentication to import groups, user accounts, and related properties. As a part of this process, you need to install at least one Cloud Connector.

For a quick overview, watch this 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.

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

Configure Citrix Gateway

When integrated with Endpoint Management, Citrix Gateway provides remote device access to your internal network and resources.
Endpoint Management requires Citrix 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 Citrix Gateway to connect to internal back-end infrastructures.
- You plan to use Endpoint Management to manage apps (MAM or MDM+MAM). Citrix Gateway isn’t required to manage devices only (MDM).
- You plan to integrate Endpoint Management with Microsoft Intune/EMS. (Requires an on-premises Citrix Gateway.)

Citrix offers both cloud-based and on-premises Citrix Gateway solutions. However, only customers with the Citrix Gateway service entitlement can configure the cloud-based service.

For a quick overview, watch this video.

---

**Important:**

After you configure a Citrix Gateway solution, switching to another solution requires that you reenroll devices. If you already use on-premises Citrix Gateway and want to switch to Citrix Gateway service, contact your Citrix Sales representative. For prerequisites, see To use Citrix Gateway service in this article.

The following table summarizes the features supported by the cloud-based and on-premises Citrix Gateway solutions.
**Citrix Endpoint Management**

<table>
<thead>
<tr>
<th>Supported features</th>
<th>Citrix Gateway service</th>
<th>Citrix Gateway on-premises</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Mail (STA)*</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Tunneled - Web SSO (web single sign-on)</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Full VPN</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Per-app VPN</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Mobile single sign-on (access control)</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>High Availability</td>
<td>yes</td>
<td>yes**</td>
</tr>
<tr>
<td>Multi-POP deployment</td>
<td>yes</td>
<td>yes***</td>
</tr>
<tr>
<td>Proxy support</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Split-tunneling</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Split DNS</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

* Citrix Cloud Secure Ticket Authority (STA) service configuration
** On-premises configuration
*** Global Server Load Balancing configuration

**Citrix Gateway service use cases (preview)**

Citrix Gateway service is now in preview. For support during the preview, go to [CGS and Mobile SSO Tech Preview Feedback](#).

Use the cloud-based Citrix Gateway service with Endpoint Management when:

- You want to use the unified authentication experience provided by Citrix Cloud. Citrix Gateway service uses the Citrix Identity provider to manage the identity information for all users in your Citrix Cloud account.
- You plan to use Citrix mobile productivity apps, such as Citrix Secure Mail or Secure Web. Citrix Gateway provides an on-demand application VPN connection that Secure Hub initiates on mobile devices to access corporate network sites or resources.

This variation of a clientless VPN is also known as Tunneled – Web single sign-on (SSO). Connections such as web traffic that tunnel to the internal network use Tunneled - Web SSO. We recommend Tunneled - Web SSO for connections that require single sign-on.
How Citrix Gateway service works

MDM and MAM control traffic go directly to Citrix Endpoint Management, without going through Citrix Gateway service. All traffic sent to Citrix Gateway gets directed to the on-premises Gateway Connector.

Citrix Gateway service isn’t used during device enrollment in Endpoint Management. For Citrix mobile productivity apps:

- Secure Hub uses a certificate for MAM control traffic.
- Secure Mail uses the Citrix Cloud Secure Ticket Authority (STA) service.

**Note:**
Citrix Gateway service uses the primary resource location.

- Citrix Gateway provides an on-demand application VPN connection. Secure Hub initiates that connection on mobile devices to access corporate network sites or resources.

Citrix Gateway service isn’t used during device enrollment in Endpoint Management. After enrollment, MDM control traffic goes directly to Citrix Endpoint Management, without going through Citrix Gateway service. MAM control traffic goes through the Citrix Gateway service. All traffic sent to Citrix Gateway gets directed to the on-premises Gateway Connector.
For a more detailed diagram of the traffic flow, see Support for Citrix Endpoint Management. For Gateway Connector port requirements, see Gateway Connector.

The following authentication types are supported for Citrix Gateway service integration with Endpoint Management:

- Basic, Digest, NTLM
- Kerberos Constrained Delegation (KCD) single sign-on; form-based single sign-on
- SAML single sign-on

**To use Citrix Gateway service:**

**Prerequisites:**

- Citrix Workspace experience enabled
  - With Citrix Workspace enabled, user enrollment starts the Workspace app. When Secure Hub detects the Workspace entitlement, Secure Hub completes enrollment. Secure Hub then opens Citrix Workspace where users can access their apps and other resources.
- Citrix Gateway service subscription
  - If you already use on-premises Citrix Gateway and want to switch to Citrix Gateway service, contact your Citrix Sales representative. Switching from on-premises Citrix Gateway to the Citrix Gateway service requires that you reenroll devices.
  - New Endpoint Management customers: Select the Citrix Gateway service during Endpoint Management onboarding.
- Gateway Connector installed on-premises in a resource location
  - Endpoint Management uses the resource location for Gateway Connector only for STA tickets for Secure Mail. Citrix Gateway sends STA traffic to the Gateway Connector in the resource location.
  - You can install one or more Gateway Connectors in any resource location. Endpoint Management doesn’t support Gateway Connectors installed in multiple resource locations.
  - You can install Gateway Connector in the same or a different resource location than Active Directory. The only role of Active Directory is to use Citrix Cloud authentication to authenticate users to Citrix Gateway service. Citrix Gateway service creates session connections to the Gateway Connector for authenticated users. You can have multiple Active Directories.
  - If the connector isn’t available during Citrix Endpoint Management onboarding, you can install it after onboarding.

For more information, see Citrix Gateway Connector and System requirements.

Citrix recommends that new Endpoint Management customers configure Citrix Gateway service rather than on-premises Citrix Gateway:

**To set up Citrix Gateway service:**
1. On the **Settings** page, scroll to the **Citrix Gateway** tile and then click **Set Up**.
2. Choose **Citrix Gateway service (cloud)** as the type. Only customers with the Citrix Gateway service entitlement can view this setting.
3. Follow the on-screen guidance. For information, see [Configure on-premises Citrix Gateway for use with Endpoint Management](#).

**On-premises Citrix Gateway use cases**

Use one or more on-premises Citrix Gateway appliances with 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.
- You use Citrix Endpoint Management integration with Microsoft Intune/EMS.

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

1. On the **Settings** page, scroll to the **Citrix Gateway** tile and then click **Set Up**.
2. Choose **Citrix Gateway (on-premises)** as the type.
3. Follow the on-screen guidance. For information, see [Configure on-premises Citrix Gateway for use with Endpoint Management](#).

**Configure notification server**

To send notifications, you must configure a gateway and a notification server. A notification server ensures connectivity and the possibility of communication between end users and the administrator. To set up a notification server in Endpoint Management, see [Notifications](#).

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

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

To obtain 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.
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.
APNs Certificate

Create an Apple MDM push certificate to manage Apple devices with Citrix Endpoint Management.

Learn more

Import APNs certificate


   Select a .pfx file

2. Password

   password

3. Click Save to save your APNs certificate information.

Save
Configure Android Enterprise

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, Endpoint Management administration takes place within Citrix Cloud. The combined interface simplifies switching between Citrix Cloud and Endpoint Management.

You can set up Android Enterprise for Endpoint Management with either Google Play or G Suite.

1. **If your organization does not use G Suite:** 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 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 G Suite to provide users access to Google apps:** You can use G Suite to register Citrix as your EMM. If your organization uses G Suite, it has an existing enterprise ID and existing Google Accounts for users. To use Endpoint Management with G Suite, 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. Therefore, each domain can only create one enterprise. To enroll a device in 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 G Suite plan.

For a quick overview, watch this 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 the Re-enroll button, return to the CEM console, and refresh the page.
4. Then follow the on-screen guidance.
Android Enterprise

Android Enterprise is a secure workspace available on Android devices. The workspace isolates business accounts, apps, and data from personal accounts, apps and data.

Set up with

- Google Play
- G Suite

To set up Android Enterprise for your company, you need to bind Citrix Endpoint Management as your enterprise mobile management (EMM) provider through Google Play.

We are taking you out to Google Play to register Citrix as your EMM provider.

When you click on 'Connect' below, you'll see a pop-up window open. If you don't see it, please check your pop-up settings.

Sign in to Google Play with your corporate Google ID. Enter your organization name and confirm that Citrix is your EMM provider.

Connect
See:

1. Managed Google Play or G Suite
2. Create an Android Enterprise Account

Configure Firebase Cloud Messaging

Citrix recommends that you use Firebase Cloud Messaging (FCM) to control how and when Android devices connect to Endpoint Management. 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 Endpoint Management server. See Firebase Cloud Messaging.

Integrate with Microsoft EMS/Intune

Endpoint Management integration with Microsoft Enterprise Mobility + Security (EMS)/Intune adds the value of Endpoint Management micro VPN to Microsoft Intune aware apps, such as Microsoft Managed Browser.

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

In the Endpoint Management console, you can change only the role and membership of a user. To change a role at any time, access the 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 Microsoft EMS/Intune, see Citrix Endpoint Management integration with Microsoft Intune/EMS.

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

If you had a Citrix Content Collaboration 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 Citrix Content Collaboration account. When you’re ready to proceed, go to https://onboarding.cloud.com.

1. After you log in, a screen similar to the following appears.
2. In the **Citrix Content Collaboration** tile, choose **Link Account**.

3. After we confirm your Citrix Content Collaboration account, the following page appears:
4. Click the **Link Account** tab to complete the process. You can immediately manage your Citrix Content Collaboration account from within Citrix Cloud.

**Next steps**

To ensure that everything is set up correctly, you can use the Endpoint Management Analyzer. From the Troubleshooting and Support page, click **Endpoint Management Analyzer** to access this tool. For information on using the Endpoint Management Analyzer, see **Endpoint Management Analyzer**.

After you complete the onboarding and resource configuration described in this article, continue your configuration in the Endpoint Management console. For information about next steps, see **Prepare to enroll devices and deliver resources**.

**Known issues**

- After configuring LDAP, support for nested groups is disabled. [CXM-73722]
Prepare to enroll devices and deliver resources

November 21, 2019

Important:
Before proceeding, be sure to complete all tasks described in Onboarding and resource setup.

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.

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

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

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

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

- To obtain an APNs certificate and import it into Endpoint Management, see APNs certificates.
For more information about Endpoint Management and APNs, see Push Notifications for 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 Endpoint Management service. Any security action or deployment command triggers a push notification. The notification prompts users to reconnect to 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 Endpoint Management AutoDiscovery service**

**Important:**

As of December 31, 2018, the AutoDiscovery service URL discovery.mdm.zenprise.com is replaced with ads.xm.cloud.com. For more information, see the Citrix support article https://support.citrix.com/article/CTX202044.

Autodiscovery is an important part of many Endpoint Management deployments. Autodiscovery simplifies the enrollment process for users. Users:

- Can use their network user names and Active Directory passwords to enroll their devices.
• Don’t need to enter details about Endpoint Management.
• Enter their user name in user principal name (UPN) format. For example, user@mycompany.com.

The Endpoint Management AutoDiscovery service enables you to create or edit an autodiscovery record without assistance from Citrix support.

AutoDiscovery is recommended for high security environments. AutoDiscovery supports certificate pinning, which prevents man-in-the-middle attacks. Certificate pinning ensures that the certificate signed by your enterprise is used when Citrix clients communicate with Endpoint Management. For information about certificate pinning, see Certificate pinning.

To access the Endpoint Management AutoDiscovery service, navigate to https://tools.xm.cloud.com (commercial) or https://tools.cem.cloud.us (government) and then click Request AutoDiscovery.

Request AutoDiscovery

1. On the AutoDiscovery service page, claim a domain. Click Add Domain.
2. In the dialog box that opens, enter the domain name of your Endpoint Management environment and then click **Next**.

![Image of domain entry dialog box]

3. The next screen provides instructions on verifying that you own the domain.

![Image of domain verification screen]

- Copy the DNS token provided in the Endpoint Management Tools portal.
- To create a DNS TXT record in the zone file for your domain in your domain hosting provider portal:
  Log in to the domain hosting provider portal for the domain. You can edit your domain name server records and add a custom TXT record.
Citrix Endpoint Management

- Paste the domain token in your DNS TXT record and save your domain name server record.
- In the Endpoint Management Tools portal, click **Done** to start the DNS check.

The system detects your DNS TXT record. Alternatively, you can click **I’ll update later** to save the record. The DNS check doesn’t start until you select the record that has a status of “Waiting” and then click **DNS Check**.

This check generally takes about an hour. However, it can take up to two days to return a response. The status change might not reflect in the Tools portal until you log out and log in again.

4. After you claim your domain, you provide information about the AutoDiscovery service. Right-click the domain record for which you want to request autodiscovery and then click **Add ADS**.

5. Enter the requested information and then click **Next**. If you are unsure about your instance name, add the default instance of **zdm**.

6. Enter the following information for Secure Hub and then click **Next**.
• **User ID Type:** Select the type of ID with which users sign on as either **E-mail address** or **UPN.**

To prompt users to enter their user name and password, choose **E-mail address.** To prompt users to enter their password, choose **UPN.** Use **UPN** when the User Principal Name matches the email address. Both methods use the domain entered to find the server address.

• **HTTPS Port:** Enter the port used to access Secure Hub over HTTPS. Typically, the HTTPS port is 443.

• **iOS Enrollment Port:** Enter the port used to access Secure Hub for iOS enrollment. Typically, this port is 8443.

• **Required Trusted CA for Endpoint Management:** Indicate whether a trusted certificate is required to access Endpoint Management or not. This option can be **OFF** or **ON.** To use a trusted certificate, contact Citrix Support to upload the certificate. To learn more about certificate pinning, see the section on certificate pinning in **Secure Hub.** To read about the ports required for certificate pinning to work, see the support article on **Endpoint Management Port Requirements for ADS Connectivity.**

7. A summary page displays all the information you entered in the preceding steps. Verify that the data is correct then click **Save.**
At this point, you can enroll all supported devices. Proceed to the next section to prepare to deliver resources to devices.

**Default device policies and mobile productivity apps**

If you onboard starting with 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 device users.

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

- **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 contains 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.

All 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 contains these preconfigured mobile productivity apps:

- SecureMail
- Secure Web
- CitrixFiles

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

For more information, see **About mobile productivity apps** and **MDX policies for mobile productivity apps at a glance**.

**Continue your Endpoint Management configuration**

After you complete the basic setup for device enrollment, how you configure 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 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 Endpoint Management console settings.

**Security and authentication**

Endpoint Management uses certificates to create secure connections and authenticate users. Citrix provides wildcard certificates for your Endpoint Management instance.
**Recommended background reading:**

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 Endpoint Management operations, see *Certificates and authentication.*

You can choose from the following types of authentication. Configuring authentication includes tasks in the Endpoint Management and Citrix 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

For other authentication options, see other articles under *Certificates and authentication.*

**Device enrollment**

Device enrollment modes specify the credential types required for users to enroll their devices in Endpoint Management. Device enrollment modes have varying levels of security and determine the required user enrollment steps.

- For information about Endpoint Management enrollment options, see *Configure enrollment modes.*

Azure Active Directory enrollment is supported for iOS, Android, and Windows 10 devices. For information about configuring Azure as your identity provider (IdP), see *Single sign-in with Azure Active Directory.*

- Other enrollment options:
  - Deploy devices through Apple DEP
  - Bulk enrollment of Apple devices
  - Create an Android Enterprise administrator account. For details, see *Android Enterprise.* Or, see *Legacy Android Enterprise for G Suite Customers.*
  - Samsung Knox Bulk Enrollment
  - Bulk enrollment of Windows devices
  - Configure G Suite for Chrome OS device enrollment from your G Suite account. For details, see *Chrome OS.*
  - Workspace hub device management
You can send notifications for enrollment. For information, see Notifications. You can also use notifications for automated actions and standard messages sent to users.

For more information about enrollment, see Device management and articles under that node.

**Device policies and management**

- Device (MDM) policies
  
  All Endpoint Management device policies are documented under Device policies. For information about some commonly used device policies, see Device Policies and Use Case Behavior.

  You can filter device policy lists in the Endpoint Management console. For example, filter by platform to see a list of policies most often used for that platform. See Device policies.

- Client properties
  
  Client properties contain information that is provided directly to Secure Hub on user devices. See Client properties and Endpoint Management client properties.

- Delivery groups
  
  For a sample use case related to delivery groups, see User Communities and To add a delivery group.

**Prepare apps for deployment**

For information about the apps supported by Endpoint Management, see Add apps.

- You can manage iOS app licensing by using Apple volume purchase. For information, see iOS Volume Purchase.

  You can use Endpoint Management to deploy iBooks that you obtain through Apple volume purchase. For information, see Add media.

- You can connect Citrix Endpoint Management to Microsoft Store for Business. For information, see Deploy Microsoft Store for Business apps from Endpoint Management.

- Citrix provides mobile productivity apps, including Secure Mail and Secure Web. For information, see About mobile productivity apps.

  As an alternative to Secure Mail, you can deliver native mail to devices. See:
  
  - Email strategy
  - Endpoint Management connector for Exchange ActiveSync
  - Citrix Gateway connector for Exchange ActiveSync
Citrix Endpoint Management

- Citrix Secure Mail, Citrix Secure Web, and Citrix Files offer the option of opening the MDX container. That option allows users to transfer docs and data to Microsoft Office 365 apps. You manage this capability for iOS and Android platforms through the open-in policies on the Endpoint Management console. 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 Service and MDX Toolkit are app wrapping technologies that prepare enterprise apps for secure deployment with Endpoint Management.

  For information about Endpoint Management MDX Service, our cloud tool, see Endpoint Management MDX Service.

  For information about Endpoint Management MDX Toolkit, the traditional MDX wrapping process, see MDX Toolkit.

- For more information about apps, see other articles under Add apps.

Other configuration

- The Role-Based Access Control (RBAC) feature in 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 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.

Certificates and authentication

December 10, 2019

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

- **Endpoint Management:** The 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. Through client properties in Endpoint Management, you can enable Citrix PIN authentication and configure the complexity and expiration time of the PIN.
Citrix Endpoint Management

- **Citrix Gateway:** Citrix Gateway provides termination for micro VPN SSL sessions. Citrix Gateway also provides network in-transit security, and lets you define the authentication experience used each time a user accesses an app.

- **Secure Hub:** Secure Hub and Endpoint Management work together in enrollment operations. Secure Hub is the entity on a device that talks to Citrix Gateway: When a session expires, Secure Hub gets an authentication ticket from Citrix Gateway and passes the ticket to the MDX apps. Citrix recommends use of certificate pinning, which prevents man-in-the-middle attacks. For more information, see this section in the Secure Hub article: Certificate pinning.

  Secure Hub also facilitates the MDX security container: Secure Hub pushes policies, creates a session with Citrix Gateway when an app times out, and defines the MDX timeout and authentication experience. 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 Citrix Gateway, enforce offline mode restrictions, and enforce client policies, such as time-outs.

For more information about configuring authentication, including an overview of single-factor and two-factor authentication methods, see the Deployment Handbook article, Authentication.

You use certificates in Endpoint Management to create secure connections and authenticate users. The remainder of this article discusses certificates. For other configuration details, see the following articles:

- Domain or domain plus security token authentication
- Client certificate or certificate plus domain authentication
- PKI entities
- Credential providers
- APNs certificates
- If your site isn’t Workspace enabled: SAML for single sign-on with Citrix Files
- Single sign in with Azure Active Directory
- To send a certificate to devices to authenticate to the WiFi server: WiFi device policy
- To push a unique certificate not used for authentication or a specific policy: Credentials device policy

**Certificates**

Endpoint Management generates a self-signed Secure Sockets Layer (SSL) certificate during installation to secure the communication flows to the server. You must replace the SSL certificate with a trusted SSL certificate from a well-known certificate authority (CA).
Endpoint Management also uses its own Public Key Infrastructure (PKI) service or obtains 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 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 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 Endpoint Management component:

<table>
<thead>
<tr>
<th>Endpoint Management component</th>
<th>Certificate format</th>
<th>Required certificate type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Gateway</td>
<td>PEM (BASE64), PFX (PKCS #12)</td>
<td>SSL, Root (Citrix Gateway converts PFX to PEM automatically.)</td>
</tr>
<tr>
<td>Endpoint Management</td>
<td>.p12 (.pfx on Windows-based computers)</td>
<td>SSL, SAML, APNs (Endpoint Management also generates a full PKI during the installation process.) Important: 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 Endpoint Management.</td>
</tr>
<tr>
<td>StoreFront</td>
<td>PFX (PKCS #12)</td>
<td>SSL, Root</td>
</tr>
</tbody>
</table>

Endpoint Management supports client certificates with bit lengths of 4096, 2048, and 1024. Be aware that 1024-bit certificates are easily compromised.

For Citrix Gateway and Endpoint Management, Citrix recommends obtaining server certificates from a public CA, such as Verisign, DigiCert, or Thawte. You can create a Certificate Signing Request (CSR) from the Citrix Gateway or the 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 Citrix Gateway or Endpoint Management.

**Important: Requirements for trusted certificates in iOS 13 and macOS 15**

Apple has new requirements for TLS server certificates. Verify that all certificates follow the Apple requirements. For details, see the [Apple Support article](#).

### Uploading certificates in Endpoint Management

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, you choose a server certificate that satisfies the context-dependent criteria. For example, you might want to configure Endpoint Management to integrate with your Microsoft CA. The connection to the Microsoft CA must be authenticated by using a client certificate.

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](#).

### Private key requirements

Endpoint Management may or may not possess the private key for a given certificate. Likewise, Endpoint Management may or may not require a private key for certificates you upload.

### Uploading certificates to the console

When uploading certificates to the console, you have two main options:

- You can click to import a keystore. Then, you identify the entry in the keystore repository you want to install, unless you are uploading a PKCS #12 format.
- You can click to 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 Endpoint Management has the private key.

### To import a keystore

By design, keystores, which are repositories of security certificates, can contain multiple entries. When loading from a keystore, therefore, you are prompted to specify the entry alias that identifies
Citrix Endpoint Management

the entry you want to load. If you do not specify an alias, the first entry from the store is loaded. Because PKCS #12 files usually contain only one entry, the alias field does not appear when you select PKCS #12 as the keystore type.

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The Settings page appears.

2. Click Certificates. The Certificates page appears.

3. Click Import. The Import dialog box appears.

4. Configure these settings:

   - **Import**: In the list, click Keystore. The Import dialog box changes to reflect available keystore options.
• **Keystore type:** In the list, click PKCS #12.

• **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 Endpoint Management. You upload server certificates to the Endpoint Management web console. Those certificates include CA certificates, RA certificates, and certificates for client authentication with other components of your infrastructure. In addition, 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 Endpoint Management of SSL cryptographic activity.

• **Keystore file:** Browse to find the keystore you want to import of the file type .p12 (or .pfx on Windows-based computers).

• **Password:** Type the password assigned to the certificate.
- **Description:** Optionally, type a description for the keystore to help you distinguish it from your other keystores.

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

### To import a certificate

When importing a certificate, either from a file or a keystore entry, Endpoint Management attempts to construct a certificate chain from the input. Endpoint Management imports all certificates in that chain to create a server certificate entry for each. This operation only works if the certificates in the file or keystore entry do form a chain. For example, if each subsequent certificate in the chain is 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 Endpoint Management console, click the gear icon in the upper-right corner of the console and then click **Certificates**.

2. On the **Certificates** page, click **Import**. The **Import** dialog box appears.

3. In the **Import** dialog box, in **Import**, if it is not already selected, click **Certificate**.

4. The **Import** dialog box changes to reflect available certificate options. In **Use as**, select how you plan to use the keystore. The available options are:

   - **Server:** Server certificates are certificates used functionally by Endpoint Management. You upload server certificates to the Endpoint Management web console. Those certificates include CA certificates, RA certificates, and certificates for client authentication with other components of your infrastructure. In addition, 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 Endpoint Management of SSL cryptographic activity.

5. Browse to find the keystore you want to import of the file type .p12 (or .pfx on Windows-based computers).

6. Browse to find an optional private key file for the certificate. The private key is used for encryption and decryption along with the certificate.

7. Type a description for the certificate, optionally, to help you identify it from your other certificates.

8. Click **Import**. The certificate is added to the Certificates table.
**Updating a certificate**

Endpoint Management only allows one certificate per public key to exist in the system at a time. If you attempt to import a certificate for the same key pair as an already imported certificate: You can either replace the existing entry or delete the entry.

To most effectively update your certificates, in the Endpoint Management console, do the following. Click the gear icon on the upper-right corner of the console to open the **Settings** page and then click **Certificates**. In the **Import** dialog box, import the new certificate.

When you update a server certificate, components that were 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.

**Endpoint Management Certificate Administration**

We recommend that you list the certificates you use in your Endpoint Management deployment, especially on their expiration dates and associated passwords. This section intends to help you make certificate administration in Endpoint Management easier.

Your environment may include some or all of the following certificates:

- **Endpoint Management server**
  - SSL Certificate for MDM FQDN
  - SAML Certificate (For Citrix Files)
  - Root and Intermediate CA Certificates for the preceding certificates and any other internal resources (StoreFront/Proxy, and so on)
  - APN Certificate for iOS Device Management
  - Internal APNs Certificate for Endpoint Management server Secure Hub Notifications
  - PKI User Certificate for connectivity to PKI

- **MDX Service or MDX Toolkit**
  - Apple Developer Certificate
  - Apple Provisioning Profile (per application)
  - Apple APNs Certificate (for use with Citrix Secure Mail)
  - Android Keystore File
  - Windows Phone – DigiCert Certificate

- **Citrix 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 & Intermediate CA Certificates for the preceding certificates
**Device certificate renewal**

You can now request that Citrix Cloud Operations refresh or regenerate the internal PKI certificate authorities (CAs) in your 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.

For supported iOS, macOS, and Android devices, you can initiate certificate renewal through the security action, Certificate Renewal. You renew device certificates from the Endpoint Management console or the Public REST API. For enrolled Windows devices, users must re-enroll their devices to receive a new device CA.

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

The next time that devices connect back to Endpoint Management, the 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**.

![Certificate Renewal Action](image)

Already enrolled devices continue to work without disruption. 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 if it’s closed.
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.

To renew device certificates by using the REST API

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 Endpoint Management provisioning, the server generates three CAs and gives them the group name “default”.

You can use the following APIs to manage and renew the device certificates that are issued by the CAs. Already enrolled devices continue to work without disruption. 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)

**Endpoint Management Certificate Expiration Policy**

If you allow a certificate to expire, the certificate becomes invalid. You can no longer run secure transactions on your environment and you cannot access Endpoint Management resources.

**Note:**
The Certification Authority (CA) prompts you to renew your SSL certificate before the expiration date.
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 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 Endpoint Management, set up and create an APNs certificate from Apple. If the certificate expires, users cannot enroll in 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. 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.

3. Thank You,

4. Apple Push Notification Service

MDX Service or 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`. 
Citrix Endpoint Management

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 Endpoint Management server certificates are valid, do the following:

1. In the Endpoint Management console, click **Settings > Certificates**.
2. Check that all certificates including APNs, SSL Listener, Root, and Intermediate certificate are valid.

**Android keystore**

The keystore is a file that contains 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.

**Enterprise certificate from DigiCert for Windows phones**

DigiCert is the exclusive provider of code signing certificates for Microsoft App Hub service. Developers and software publishers join App Hub to distribute Windows Phone and Xbox 360 applications for download through the Windows Marketplace. For details, see DigiCert Code Signing Certificates for Windows Phone in the DigiCert documentation.

If the certificate expires, Windows phone users cannot enroll. The users cannot install an app published and signed by the company, or start a company app that was installed on the phone.

**Citrix Gateway**

For details on how to handle certificate expiration for Citrix Gateway, see How to handle certificate expiry on NetScaler in the Citrix Support Knowledge Center.

An expired Citrix Gateway certificate prevents users from enrolling and accessing the Store. The expired certificate also prevents users from connecting to Exchange Server when using Secure Mail. In addition, users cannot enumerate and open HDX apps (depending on which certificate expired).

The Expiry Monitor and Command Center can help you to track your Citrix Gateway certificates. The Center notifies you when the certificate expires. These tools assist to monitor the following Citrix 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)
Citrix Endpoint Management

- SSL Certificate for StoreFront Load Balancing
- Root and Intermediate CA Certificates for the preceding certificates

Citrix Gateway and Endpoint Management

October 23, 2019

When integrated with Endpoint Management, Citrix Gateway provides remote device access to your internal network and resources. Endpoint Management creates a micro VPN from the apps on the device to Citrix Gateway.

You can use the Citrix Gateway service or on-premises Citrix Gateway, also known as NetScaler Gateway. For an overview of the two Citrix Gateway solutions, see Configure Citrix Gateway use with Endpoint Management.

Configure authentication for remote device access to the internal network

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The Settings page appears.

2. Under Server, click Citrix Gateway. The Citrix Gateway page appears. In the following example, a Citrix 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 Endpoint Management to share the authentication certificate with Secure Hub. Sharing the certificate enables Citrix Gateway to handle the client certificate authentication. The default is **OFF**.
   - **Credential Provider**: In the list, click the credential provider to use. For more information, see Credential providers.

4. Click **Save**.

Add a Citrix Gateway instance

After you save the authentication settings, you add a Citrix Gateway instance to Endpoint Management.
1. In the Endpoint Management console, click the gear icon in the upper-right corner. The **Settings** page opens.

2. Under **Server**, click **Citrix Gateway**. The **Citrix Gateway** page appears.

3. You can add Citrix Gateway service or an on-premises Citrix Gateway. To add an on-premises gateway, skip to the next step. To add the Gateway service, click **Add** and then choose **Add Gateway service**. The **Add Citrix Gateway service** page appears. Complete these settings.

   - **External URL**: Type the publicly accessible URL for Citrix Gateway. For example, `https://url.com`.
   - **Set as Default**: Select whether to use this Citrix Gateway as the default. The default is **ON**.
   - **Resource Location**: is required if you use Secure Mail. Specify the resource location for the STA service. The resource location must include a configured Citrix Gateway. If you later want to remove a resource location that’s configured for Gateway service, update this setting.

   When you complete those settings, click **Save**. The new Citrix Gateway is added and appears in the table. To edit or delete an instance, click the name in the list.

4. To add an on-premises gateway, click **Add** and then choose **Add On-Premises Gateway**. The **Add New Citrix Gateway** page appears.
Configure these settings:

- **Name**: Type a name for the Citrix Gateway instance.
- **Alias**: Optionally include an alias name for the Citrix Gateway.
- **External URL**: Type the publicly accessible URL for Citrix Gateway. For example, `https://receiver.com`.
- **Logon Type**: Choose a logon type. Types include **Domain and security token**, **Certificate and domain**, and **Certificate and security token**. The default setting for the **Password Required** field changes based on the **Logon Type** you select. The default is **Domain only**.

If you have multiple domains, use **Certificate and domain**. For more information, see Configure authentication for multiple domains.

Certificate-based authentication at the Citrix 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.

- **Password Required**: Select whether you want to require password authentication. The default varies based on the **Logon Type** chosen.
- **Set as Default**: Select whether to use this Citrix Gateway as the default. The default is **OFF**.
- **Export Configuration Script**: Click the button to export a configuration bundle that you upload to Citrix Gateway to configure it with Endpoint Management settings. For information, see “Configure an on-premises Citrix Gateway for use with Endpoint Management” after these steps.

5. Click **Save**.

The new Citrix Gateway is added and appears in the table. To edit or delete an instance, click the name in the list.

**Configure on-premises Citrix Gateway for use with Endpoint Management**

To configure an on-premises Citrix Gateway for use with Endpoint Management, you perform 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 Endpoint Management console.
3. Run the script on the Citrix Gateway. See the readme file provided with the script for the latest detailed instructions.
4. Test the configuration.
The script configures these Citrix Gateway settings required by Endpoint Management:

- Citrix Gateway virtual servers needed for MDM and MAM
- Session policies for the Citrix Gateway virtual servers
- Endpoint Management server details
- Proxy load balancer for certificate validation
- Authentication Policies and Actions for the NSG virtual server. The script describes the LDAP configuration settings.
- Traffic actions and policies for the proxy server
- Clientless access profile
- Static local DNS record on Citrix Gateway
- Other bindings: Service policy, CA certificate

The script doesn’t handle the following configuration:

- Exchange load balancing
- Citrix Files load balancing
- ICA Proxy configuration
- SSL Offload

**Prerequisites for using the Citrix Gateway configuration script**

**Endpoint Management requirements:**

- Complete the LDAP and Citrix Gateway configuration in Endpoint Management before exporting the script. If you change the settings, export the script again.

**Citrix Gateway requirements:**

- When using certificate-based authentication at the Citrix Gateway, you must create SSL certificates on a Citrix ADC Appliance. See [Create and Use SSL Certificates on a Citrix ADC Appliance](https://support.citrix.com/article/CTX126049).
- Citrix Gateway (minimum version 11.0, Build 70.12).
- Citrix Gateway IP address is configured and has connectivity to the LDAP server, unless LDAP is load balanced.
- Citrix 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.
- Citrix Gateway is licensed with Platform/Universal or Trial licenses. For information, see [https://support.citrix.com/article/CTX126049](https://support.citrix.com/article/CTX126049).

**Install the script in your environment**

The script bundle includes a:
Citrix Endpoint Management

- Readme file with detailed instructions
- Script that contains the NetScaler CLI commands used to configure the required components in NetScaler
- Public Root CA certificate and the Intermediate CA certificate
- Script that contains 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.

The following examples show how to install the root certificate.
Ensure that you install both the root and intermediate certificates.

2. Edit the script (OfflineNSGconfigBundle_CREATESCRIPT) to replace all placeholders with details from your environment.
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/OfflineNSGConfigBundle_CREATESCRIPT.txt"
```

When the script completes, the following lines appear.

```
exec: save ns config
Done
Done
```

**Test the configuration**

To validate the configuration:

1. Validate that Citrix Gateway Virtual Server shows a state of UP.
2. Validate that the Proxy Load Balancing Virtual Server shows a state of **UP**.

3. Open a web browser, connect to the Citrix Gateway URL, and attempt to authenticate. If the authentication succeeds, you are redirected to an “HTTP Status 404 - Not Found” message.

4. Enroll a device and ensure it gets both MDM and MAM enrollment.

**Configure authentication for multiple domains**

If you have multiple Endpoint Management instances, such as for test, development, and production environments, you configure Citrix Gateway for the additional environments manually. (You can use the NetScaler for XenMobile wizard only one time.)

**Citrix Gateway configuration**

To configure Citrix Gateway authentication policies and a session policy for a multi-domain environment:

1. In the Citrix Gateway configuration utility, on the **Configuration** tab, expand **Citrix 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 you want to use for searches. Make a note of the attribute that you specify. You provide it when configuring LDAP settings in the Endpoint Management console.

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 Citrix Gateway virtual server, navigate to **Edit session profile > Published Applications**. Make sure that **Single Sign-On Domain** is blank.

**Endpoint Management configuration**

To configure Endpoint Management LDAP for a multi-domain environment:

1. In the 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
• Ensure that the **User search by** field matches the **Server Logon Name Attribute** specified in the Citrix Gateway LDAP policy.

**Drop inbound connection requests to specific URLs**

If the Citrix 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 whitelist your IP to your on-premises data centers.

**Domain or domain plus security token authentication**

August 26, 2019

Endpoint Management supports domain-based authentication against one or more directories that are compliant with the Lightweight Directory Access Protocol (LDAP). You can configure a connection in Endpoint Management to one or more directories and then use the LDAP configuration to import groups, user accounts, and related properties.

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 multiple 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.

Important:
Endpoint Management doesn’t support changing the authentication mode from domain authentication to a different authentication mode after users enroll devices in Endpoint Management.

To add LDAP connections in Endpoint Management

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The Settings page appears.
2. Under Server, click LDAP. The LDAP page appears. You can add, edit, or delete LDAP-compliant directories, as described in this article.

To add an LDAP-compliant directory

2. Configure these settings:

- **Directory type**: In the list, click the appropriate directory type. 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 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.

• **User base DN:** Type the location of users in 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 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 Active Directory.

• **UserID:** 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.

• **Endpoint Management Lockout Limit:** Type a number between 0 and 999 for the number of failed logon attempts. A value of 0 means that Endpoint Management never locks out the user based on failed logon attempts.

• **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.

• **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 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 username or user ID that Endpoint Management uses to search for users in this directory. Users enter their username or user ID in this format when enrolling.

  If you choose **userPrincipalName**, users enter a user principle 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`

• **Use secure connection:** Select whether to use secure connections. The default is **NO**.

3. Click **Save**.
To edit an LDAP-compliant directory

1. In the LDAP table, select the directory to edit.
   
   When you select the check box next to a directory, the options menu appears above the LDAP list. Click anywhere else in the list and the options menu appears on the right side of the listing.

2. Click Edit. The Edit LDAP page appears.

3. Change the following information as appropriate:
   
   • **Directory type:** In the list, click the appropriate directory type.
   
   • **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, type the IP address or FQDN for the secondary server (if one has been configured).
   
   • **Port:** Type the port number used by the LDAP server. By default, the port number is set to 389 for unsecured LDAP connections. Use port number 636 for secure LDAP connections, use 3268 for Microsoft unsecure LDAP connections, or 3269 for Microsoft secure LDAP connections.
   
   • **Domain name:** You cannot change this field.
   
   • **User base DN:** Type the location of users in Active Directory through a unique identifier. Syntax examples include: `ou=users,dc=example`, or `dc=com`.
   
   • **Group base DN:** Type the group base DN group name specified as `cn=groupName`. For example, `cn=users,dc=servername,dc=net` where `cn=users` is the group name. DN and servername represent the name of the server running 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.

• **Endpoint Management Lockout Limit:** Type a number between 0 and 999 for the number of failed logon attempts. A value of 0 means that Endpoint Management never locks out the user based on failed logon attempts.

• **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.

• **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 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 username or user ID that Endpoint Management uses to search for users in this directory. Users enter their username or user ID in this format when enrolling.

  - If you choose **userPrincipalName**, users enter a user principle 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

• **Use secure connection:** Select whether to use secure connections.

4. Click **Save** to save your changes or **Cancel** to leave the property unchanged.

**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 check box next to each property.

2. Click **Delete**. A confirmation dialog box appears. Click **Delete** again.
Configure domain plus security token authentication

You can configure 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 Endpoint Management. For information, see Uploading certificates in Endpoint Management.

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.
Configure Citrix Gateway settings

The following steps assume that you already have added a Citrix Gateway instance to Endpoint Management. To add a Citrix Gateway instance, see Add a Citrix Gateway instance.

1. In Settings, click Citrix Gateway.
2. Select the Citrix 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 check boxes: Enable Citrix PIN Authentication and Enable User Password Caching. For more information, see Client properties.

Configure Citrix Gateway for domain and security token authentication

Configure Citrix Gateway session profiles and policies for your virtual servers used with Endpoint Management. For information, see the Citrix Gateway documentation.
The default configuration for Endpoint Management is user name and password authentication. To add another layer of security for enrollment and access to Endpoint Management environment, consider using certificate-based authentication. In the 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 security provided by two-factor authentication at Citrix 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:**

Endpoint Management doesn’t support changing the authentication mode from domain authentication to some other authentication mode after users enroll devices in 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 Endpoint Management. Users then enroll using a unique PIN that Endpoint Management generates for them. After a user has access, Endpoint Management then creates and deploys the certificate used to authenticate to the Endpoint Management environment.

You can use the NetScaler for XenMobile wizard to perform the configuration required for Endpoint Management when using Citrix 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 information, see Configuring Endpoint Management for Certificate and Security Token Authentication.

Client certificate authentication is available for Endpoint Management MAM mode and MDM+MAM mode (when users enroll into MDM). Client certificate authentication isn’t available for Endpoint Management MDM+MAM mode when users enroll into legacy MAM mode. To use client certificate authentication for Endpoint Management MDM+MAM and MAM modes, you must configure the Microsoft server, the Endpoint Management server, and then Citrix Gateway. Follow these general steps, as described in this article.

On the Microsoft server:
Add a certificate snap-in to the Microsoft Management Console.

1. Open the console and then click Add/Remove Snap-ins.

Add the template to Certificate Authority (CA).

3. Create a PFX certificate from the CA server.

On the Endpoint Management server:

1. Upload the certificate to Endpoint Management.

2. Create the PKI entity for certificate-based authentication.

3. Configure credentials providers.

4. Configure Citrix Gateway to deliver a user certificate for authentication.

For information about Citrix 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.
- If you use private server certificates to secure the ActiveSync traffic to the Exchange Server, ensure that the mobile devices have all of the Root/Intermediate certificates. Otherwise, certificate-based authentication fails during the mailbox setup in Secure Mail. In the Exchange IIS Console, you must:
  - Add a website for 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.
2. Add the following snap-ins:
   - Certificate Templates
   - Certificates (Local Computer)
   - Certificates - Current User
   - Certificate Authority (Local)

4. Select the User template and Duplicate Template.

![Duplicate Template](image)

5. Provide the Template display name.

   Important:
   Select the Publish certificate in Active Directory check box only if necessary. If this option is selected, all user client certificates are created in Active Directory, which might clutter your Active Directory database.


7. Under Security, click Add and then select the AD user account that Endpoint Management will use 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 will create a user .pfx certificate using the service account. For information, see Creating a PFX certificate from the CA server.
8. Under **Cryptography**, ensure that you provide the key size. You later enter the key size during Endpoint Management configuration.
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**.
2. Right-click in the right pane and then select **New > Certificate Template to Issue**.

3. Select the template you created in the previous step and then click **OK** to add it into the **Certificate Authority**.
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 is uploaded to Endpoint Management, which then requests a user certificate on behalf of 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.

5. Select **Active Directory Enrollment Policy** and then click **Next**.
6. Select the **User** template and then click **Enroll**.
7. Export the .pfx file that you created in the previous step.

8. Click **Yes, export the private key**.
9. Select **Include all certificates in the certification path if possible** and select the **Export all extended properties** check box.
10. Set a password to use when uploading this certificate into Endpoint Management.
11. Save the certificate onto your hard drive.

**Uploading the certificate to Endpoint Management**

1. In the 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 just created.
   - **Password**: Enter the password you created for this certificate.
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)
   - **Authentication type**: Client certificate
• **SSL client certificate:** Select the User Certificate to be used to issue the Endpoint Management client certificate.

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 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:
   - **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:** SHA1withRSA
   • **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 Endpoint Management Client Certificate.
   • **Select distribution mode:** Select **Prefer centralized:** Server-side key generation.
6. For the next two sections, **Revocation Endpoint Management** and **Revocation PKI**, set the parameters as required. In this example, both options are skipped.

7. Click **Renewal**.

8. For **Renew certificates when they expire**, select **ON**.

9. Leave all other settings as default or change them as required.

10. Click **Save**.

**Configuring Secure Mail to use certificate-based authentication**

When you add Secure Mail to Endpoint Management, be sure to configure the Exchange settings under **App Settings**.
Configuring Citrix Gateway certificate delivery in Endpoint Management

1. Log on to the Endpoint Management console and click the gear icon in the upper-right corner. The **Settings** screen appears.

2. Under **Server**, click **Citrix Gateway**.

3. If Citrix 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 sAMAccount attributes in the user certificates as an alternative to User Principal Name (UPN), configure the LDAP connector in Endpoint Management as follows: Go to **Settings > LDAP**, select the directory and click **Edit**, and select **sAMAccountName** in **User search by**.
Enable Citrix PIN and user password caching

To enable Citrix PIN and user password caching, go to Settings > Client Properties and select these check boxes: Enable Citrix PIN Authentication and Enable User Password Caching. For more information, see Client properties.

Creating an Enterprise Hub policy for Windows Phone

For Windows Phone devices, you must create an Enterprise Hub device policy to deliver the AETX file and the Secure Hub client.

Note:

Ensure that the AETX and Secure Hub files both use the:

- Same enterprise certificate from the certificate provider.
- Same Publisher ID from the Windows Store developer account.

1. In the Endpoint Management console, click Configure > Device Policies.

2. Click Add and then, under More > Endpoint Management Agent, click Enterprise Hub.

3. After naming the policy, be sure to select the correct .AETX file and signed Secure Hub app for the Enterprise Hub.
4. Assign the policy to delivery groups and save it.

**Troubleshooting your client certificate configuration**

After a successful configuration of the preceding configuration plus the Citrix Gateway configuration, the user workflow is as follows:

1. Users enroll their mobile device.
2. Endpoint Management prompts users to create a Citrix PIN.
3. Users are then redirected to the app store.
4. When users start Secure Mail, Endpoint Management doesn't prompt them for user credentials for mailbox configuration. Instead, Secure Mail requests the client certificate from Secure Hub and submits it to Microsoft Exchange Server for authentication. If Endpoint Management prompts for credentials when users start Secure Mail, check your configuration.

If users can download and install Secure Mail, but during the mailbox configuration 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.
2. Verify that the authentication type selected for ActiveSync is **Require client certificates.**
3. On 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.
After selecting **True**, be sure to click **Apply** for the changes take effect.

4. Check the Citrix Gateway settings in the Endpoint Management console: Ensure 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 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:
   
   **Citrix 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:

   ```bash
   netsh http show sslcert
   ```
2. If the value for **Negotiate Client Certificate** is **Disabled**, run the following command to enable it:

```plaintext
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:

```plaintext
netsh http add sslcert ipport=0.0.0.0:443 certhash=23498dfsdfhaf98rhkjqf9823rkjhd appid={123asd456jd-a12b-3c45-d678-123456lkjhgflkjkjdf} certstorename=ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable
```

If you cannot deliver Root/Intermediate certificates to a Windows Phone 8.1 device through Endpoint Management:

- Send Root/Intermediate certificates (.cer) files through email to the Windows Phone 8.1 device and install them directly.

If Secure Mail doesn’t install successfully on Windows Phone 8.1, verify the following:

- The Application Enrollment Token (.AETX file) is delivered through 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 Secure Mail and sign Secure Hub apps.
- The same Publisher ID is used to sign and wrap Secure Hub, Secure Mail, and the Application Enrollment Token.

## PKI entities

December 10, 2019

An Endpoint Management Public Key Infrastructure (PKI) entity configuration represents a component performing actual PKI operations (issuance, revocation, and status information). These components are either internal or external to Endpoint Management. Internal components are referred to as discretionary. External components are part of your corporate infrastructure.

Endpoint Management supports the following types of PKI entities:

- **Generic PKIs (GPKIs)**

  Endpoint Management GPKI support includes DigiCert Managed PKI.
Citrix Endpoint Management

- Microsoft Certificate Services
- Discretionary Certificate Authorities (CAs)

Endpoint Management supports the following CA servers:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

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 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 CAs as part of the PKI entity configuration. To do so, upload the certificates to 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: ! : $ ( )## % + * ~ ? | { } [ ]

Generic PKI

The Generic PKI (GPKI) protocol is a proprietary Endpoint Management protocol running over a SOAP Web Service layer for purposes of uniform interfacing with various PKI solutions. The GPKI protocol defines the following three fundamental PKI operations:

- **Sign**: The adapter can take CSRs, transmit them to the PKI, and return newly signed certificates.
- **Fetch**: The adapter can retrieve (recover) existing certificates and key pairs (depending on input parameters) from the PKI.
• **Revoke:** The adapter can cause the PKI to revoke a given certificate.

The receiving end of the GPKI protocol is the GPKI adapter. The adapter translates the fundamental operations to the specific type of PKI for which it was built. For example, there are GPKI adapters for RSA and Entrust.

The GPKI adapter, as a SOAP Web Services endpoint, publishes a self-describing Web Services Description Language (WSDL) definition. Creating a GPKI PKI entity amounts to providing Endpoint Management with that WSDL definition, either through a URL or by uploading the file itself.

Support for each of the PKI operations in an adapter is optional. If an adapter supports a given operation, the adapter is said to have the corresponding capability (sign, fetch, or revoke). Each of these capabilities may be associated with a set of user parameters.

User parameters are parameters that the GPKI adapter defines for a specific operation and for which you must provide values to Endpoint Management. Endpoint Management parses the WSDL file to determine which operations the adapter has and which parameters the adapter requires for each of those operations. If you choose, use SSL client authentication to secure the connection between Endpoint Management and the GPKI adapter.

**To add a generic PKI**

1. In the Endpoint Management console, click **Settings > PKI Entities**.
2. On the **PKI Entities** page, click **Add**.
   
   A menu of PKI entity types appears.

3. Click **Generic PKI Entity**.
   
   The Generic PKI Entity: General Information page appears.
4. On the **Generic PKI Entity: General Information** page, do the following:
   - **Name**: Type a descriptive name for the PKI entity.
   - **WSDL URL**: Type the location of the WSDL describing the adapter.
   - **Authentication type**: Click the authentication method you want to use.
     - **None**
     - **HTTP Basic**: Provide the user name and password required to connect to the adapter.
     - **Client certificate**: Select the correct SSL client certificate.

5. Click **Next**.
   The Generic PKI Entity: Adapter Capabilities page appears.

6. On the **Generic PKI Entity: Adapter Capabilities** page, review the capabilities and parameters associated with your adapter and then click **Next**.
   The **Generic PKI Entity: Issuing CA Certificates** page appears.

7. On the Generic PKI Entity: Issuing CA Certificates page, select the certificates you want to use for the entity.
   Although entities may return certificates signed by different CAs, the same CA must sign all certificates obtained through a given certificate provider. Thus, when configuring the **Credential Provider** setting, on the **Distribution** page, select one of the certificates configured here.

8. Click **Save**.
   The entity appears on the PKI Entities table.

**DigiCert Managed PKI**

Endpoint Management GPKI support includes DigiCert Managed PKI, also referred to as MPKI. This section describes how to set up Windows Server and Endpoint Management for DigiCert Managed PKI.

**Prerequisites**

- Access to DigiCert Managed PKI Infrastructure
Citrix Endpoint Management

- Windows Server 2012 R2 server with the following components installed, as described in this article:
  - Java
  - Apache Tomcat
  - Symantec PKI Client
  - Portecle
- Access to the Endpoint Management downloads site

Install Java on Windows Server

Download Java for 64-bit Windows from the Java website and then install the application. In the Security Warning dialog box, click Run.

Install Apache Tomcat on Windows Server

Download the Apache Tomcat 32-bit/64-bit Windows Service Installer from https://tomcat.apache.org/download-80.cgi and then install it. In the Security Warning dialog box, click Run. Complete the Apache Tomcat setup, using the following examples as a guide.
Citrix Endpoint Management

Apache Tomcat Setup: Configuration Options

**Configuration**
Tomcat basic configuration.

- **Server Shutdown Port:** 3085
- **HTTP/1.1 Connector Port:** 8080
- **APR/1.3 Connector Port:** 8081
- **Windows Service Name:** Tomcat8
- **Create shortcuts for all users:** [ ]
- **Tomcat Administrator Login** (optional)
  - **User Name:**
  - **Password:**
  - **Roles:** manager-gui

Apache Tomcat Setup: Java Virtual Machine path selection

**Java Virtual Machine**
Java Virtual Machine path selection.

Please select the path of a Java SE 7.0 or later JRE installed on your system.

```
C:\Program Files\Java\jre1.8.0_144
```

© 1999-2019 Citrix Systems, Inc. All rights reserved. 157
Next, go to Windows Services and change *Startup Type* from *Manual* to *Automatic.*
Install Symantec PKI client on Windows Server

Download the installer from the PKI Manager console. If you don’t have access to that console, download the installer from the Symantec support page How to download Symantec PKI Client. Unzip and run the installer.
In the **Security Warning** dialog box, be sure to click **Run**. Follow the instructions in the installer to complete the setup. When the installer completes, it prompts you to restart.

**Install Portecle on Windows Server**

Download the installer from [https://sourceforge.net/projects/portecleinstall/files/](https://sourceforge.net/projects/portecleinstall/files/) and then unzip and run the installer.

**Generate the registration authority (RA) certificate for DigiCert Managed PKI**

The keystore for client certificate authentication is contained in a registration authority (RA) certificate, named RA.jks. The following steps describe how to generate that certificate by using Portecle. You can also generate the RA certificate by using the Java CLI.

This article also describes how to upload the RA and public certificates.

1. In Portecle, go to **Tools > Generate Key Pair**, provide the required information, and generate the key pair.
2. Right-click the key pair and then click **Generate Certification Request**.
3. Copy the CSR.

4. In Symantec PKI Manager, generate an RA certificate: Click Settings, click Get a RA Certificate, paste the CSR, and then click Continue.
5. Click **Download** to download the generated RA certificate.

![Symantec PKI Certificate Service](image)

6. In Portecle, import the RA certificate: Right-click the key pair and then click **Import CA Reply**.
7. In Symantec PKI Manager: Go to Resources > Web Services and then download the CA certificates.
8. In Portecle, import the RA intermediate and root certificates into the keystore: Go to **Tools > Import Trusted Certificates**.
9. After importing the CAs, save the keystore as RA.jks under the C:\Symantec folder on the Windows server.
Configure Symantec PKI adapter on Windows Server

1. Log in to Windows Server as an administrator.

2. Upload the RA.jks file that you generated in the preceding section. Also upload the public certificates (cacerts.jks) for your Symantec MPKI server.

3. From the Citrix XenMobile download page, expand Tools, and download the Symantec PKI Adapter file. The file name is Endpoint Management_Symantec_PKI_Adapter.zip. Unzip the file and copy these files to the Windows Server C: drive:
   - custom_gpki_adapter.properties
   - Symantec.war

4. Open custom_gpki_adapter.properties in Notepad and edit the following values:

   ```plaintext
   Gpki.CaSvc.Url=https://<managed PKI URL>
   # keystore for client-cert auth
   ```
5. Copy Symantec.war under the folder <tomcat_dir>/webapps and then start Tomcat.

6. Verify that the application deployed: Open a web browser and navigate to https://localhost/Symantec. (If you get a certificate error, consider connecting with HTTP instead.)

7. Navigate to the folder <tomcat_dir>/webapps/Symantec/WEB-INF/classes and edit gpki_adapter.properties. Modify the property CustomProperties to point it to the custom_gpki_adapter file under the C:\Symantec folder:

   CustomProperties=C:\Symantec\custom_gpki_adapter.properties

8. Restart Tomcat, navigate to https://localhost/Symantec, and then copy the endpoint address. In the next section, you paste that address when configuring the PKI adapter.

Configure Endpoint Management for DigiCert Managed PKI

Complete the Windows Server setup before performing the following Endpoint Management configuration.

To import the Symantec CA certificates and configure the PKI entity

1. Import the Symantec CA certificates that issue the end-user certificate: In the Endpoint Management console, go to Settings > Certificates and click Import.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
2. Add and configure the PKI Entity: Go to Settings > PKI Entities, click Add, and then choose Generic PKI Entity. In WSDL URL, paste the endpoint address that you copied when configuring the PKI adapter in the previous section, and then append ?wsdl as shown in the following.

3. Click Next. Endpoint Management populates the parameter names from the WSDL.

4. Click Next, select the correct CA certificate, and then click Save.

5. On the Settings > PKI Entities page, verify that the State of the PKI Entity you added is Valid.
To create the credential provider for DigiCert Managed PKI

1. In the Symantec PKI Manager console, copy the Certificate Profile OID from the Certificate Template.

2. In the Endpoint Management console, go to Settings > Credential Providers, click Add, and then configure the settings as follows.
   - **Name**: Type a unique name for the new provider configuration. This name is used to refer to the configuration in other parts of the Endpoint Management console.
   - **Description**: Describe the credential provider. Although this field is optional, a description can be useful when you need details about the credential provider.
   - **Issuing entity**: Choose the certificate issuing entity.
   - **Issuing method**: Choose **Sign** as the method that the system uses to obtain client certificates from the configured entity.
   - **certParams**: Add the following value: `commonName=${user.mail},otherNameUPN=${user.userprincipalname},mail=${user.mail}`
   - **certificateProfileid**: Paste the Certificate Profile OID that you copied in Step 1.
3. Click **Next**. On each of the remaining pages (Certificate Signing Request through Renewal), accept the default settings. When you are finished, click **Save**.

To test and troubleshoot the configuration

1. Create a Credentials device policy: Go to **Configure > Device Policies**, click **Add**, start typing **Credentials**, and then click **Credentials**.

2. Specify a **Policy Name**.

3. Configure the platform settings as follows:

   - **Credential type**: Choose **Credential Provider**.
   - **Credential provider**: Choose the Symantec provider.

4. After you complete the platform settings, continue to the **Assignment** page, assign the policy to delivery groups, and click **Save**.

5. To check whether the policy deployed to the device, go to **Manage > Devices**, select the device, click **Edit**, and click **Assigned Policies**. The following example shows a successful policy deployment.
If the policy didn’t deploy, log in to the Windows Server and check if the WSDL is loading properly.

For more troubleshooting information, check the Tomcat logs in `<tomcat_dir>\logs\catalina .<current_date>`.

**Entrust PKI adapter**

As an alternative to DigiCert Managed PKI, you can install the Entrust PKI adapter. Prior to installing the adapter, see the steps for installing Java and Apache Tomcat on Windows Server in the DigiCert Managed PKI section of this article.
Citrix Endpoint Management

Ensure that the Citrix Cloud Connector is installed as well. For more information on the Cloud Connector, see Citrix Cloud Connector.

Install the Entrust PKI adapter


2. Extract the entrust.war file from the downloaded .zip file and place it in the C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps directory.

3. In C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps\Entrust\WEB-INF\classes, edit entrust_adapter.properties and set CustomProperties to c:\zenprise\custom_entrust_adapter.properties.

4. In your C: drive, create a zenprise directory and a new file called custom_entrust_adapter.properties.

5. Edit the file with the following content, taking care to replace the Entrust.MdmSvc.URL, AdminUserId, and AdminPassword appropriately.

```plaintext
# set the following to the proper URL for AS/IG
Entrust.MdmSvc.Url='https://pki.yourcorp.com:19443/mdmws/services/AdminServiceV8'

# set to 1 or true to force user creation from passed user and
group parameters if using IG and user does not exist
CreateUser=

# set the credentials for the endpoint
AdminUserId='[User ID]'
AdminPassword='[password]'

# keystore for client-cert auth
#keyStore=
#keyStorePassword=
```
Configure Endpoint Management for the Entrust PKI adapter

1. Log in to your Endpoint Management console and navigate to Settings > PKI Entities. Click Add > Generic PKI Entity.
2. Enter the following information:
• **Name:** Enter a name for the PKI Entity.

• **WSDL URL:** If you’re using Citrix Cloud Connector, enter \http://localhost:8080/Entrust/EntrustGpkiAdapter?wsdl. If you aren’t using Citrix Cloud Connector, enter your server’s public URL.

• **Authentication type:** Choose the authentication method 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:** On or Off depending on if you are using the Citrix Cloud Connector or not.

• **Resource Location:** Select My Resource Location.

• **Allowed Relative Paths:** Enter /Entrust/*.

3. Once you’ve finished configuring the PKI Entity, return to the Settings page and add a Credential Provider.

4. On the General tab, select your Entrust entity as the Issuing entity and SIGN as the Issuing method.

5. On the Certificate Signing Request tab, configure the settings as follows:
  - **Key algorithm:** RSA.
  - **Key size:** 2048.
  - **Signature algorithm:** SHA1withRSA.
  - **Subject name:** cd=$user.username
  - **Subject alternative names:** Optional. We recommend the following:
    – **Type:** User Principal name.
    – **Value:** $user.userprincipalname

Note: If you change any settings on the adapter, follow these steps to reconfigure the credential provider.

6. After finishing configuring the credential provider navigate to Configure > Device Policies and add a Credentials policy.

7. Configure the policy for the OSes you plan to use. On each OS configuration page, for Credential Type, select Credential provider. For the Credential provider menu, select the credential provider you configured earlier.

### Microsoft Certificate Services

Endpoint Management interfaces with Microsoft Certificate Services through its web enrollment interface. Endpoint Management only supports the issuing of new certificates through that interface (the equivalent of the GPKI sign capability). If the Microsoft CA generates a Citrix Gateway user certificate, Citrix Gateway supports renewal and revocation for those certificates.
To create a Microsoft CA PKI entity in 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 Endpoint Management and the Certificate Services web interface.

Add a Microsoft Certificate Services entity

1. In the 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/](https://192.0.0.1/certsrv/). The URL may 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 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.
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 ensure 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 templates requirements, see the Microsoft documentation for your Microsoft Server version. 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 you want to add.

8. Click **Next**.

   The **Microsoft Certificate Services Entity: HTTP parameters** page appears. On this page, you specify custom parameters for 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.
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 Endpoint Management of the signers of the certificates that the system obtains through this entity. When your CA certificate is renewed, update it in Endpoint Management. 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.

**Citrix Gateway certificate revocation List (CRL)**

Endpoint Management supports Certificate Revocation List (CRL) only for a third-party Certificate Authority. If you have a Microsoft CA configured, Endpoint Management uses Citrix Gateway to manage revocation.

When you configure client certificate-based authentication, consider whether to configure the Citrix Gateway Certificate Revocation List (CRL) setting, Enable CRL Auto Refresh. This step ensures that the user of a device in MAM-only mode can’t authenticate using an existing certificate on the device.

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 Endpoint Management with a CA certificate and the associated private key. 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, and only 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 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
of your CA private key (recommended): Create a delegate OCSP signing certificate, signed by the CA certificate, and include this extension: \textit{id-kp-OCSPSigning extendedKeyUsage}.

The Endpoint Management OCSP responder service supports basic OCSP responses and the following hashing algorithms in requests:

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Responses are signed with SHA-256 and the signing certificate key algorithm (DSA, RSA, or ECDSA).

\textbf{Add discretionary CAs}

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console and then click \textit{More > PKI Entities}.
2. On the \textit{PKI Entities} page, click \textit{Add}.
   
   A menu of PKI entity types appears.
3. Click \textit{Discretionary CA}.
   
   The \textit{Discretionary CA: General Information} page appears.
4. On the \textit{Discretionary CA: General Information} page, do the following:
   
   - \textbf{Name}: Type a descriptive name for the discretionary CA.
   - \textbf{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 Endpoint Management at \textit{Configure > Settings > Certificates}.
5. Click \textit{Next}.
   
   The \textit{Discretionary CA: Parameters} page appears.
6. On the \textit{Discretionary CA: Parameters} page, do the following:
   
   - \textbf{Serial number generator}: The discretionary CA generates serial numbers for the certificates it issues. From this list, click \textit{Sequential} or \textit{Non-sequential} to determine how the numbers are generated.
   - \textbf{Next serial number}: Type a value to determine the next number issued.
   - \textbf{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 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**.

The **Discretionary CA: Distribution** page appears.

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**.

The **Discretionary CA: Online Certificate Status Protocol (OCSP)** page appears.

On the **Discretionary CA: Online Certificate Status Protocol (OCSP)** page, do 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 OCSP signing CA certificate. This list of certificates is generated from the CA certificates you uploaded to Endpoint Management.

10. Click **Save**.

The discretionary CA appears on the PKI Entities table.

### Credential providers

September 30, 2019

Credential providers are the actual certificate configurations you use in the various parts of the 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, Endpoint Management does not issue certificates before enrollment, although Endpoint Management may issue some certificates as part of
enrollment. In addition, 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 remains.

You may use one credential provider configuration in multiple places, to the effect that one configuration may 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 Endpoint Management determines the following:

- The source of certificates.
- The method in which certificates are obtained: 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.
- Revocation conditions. Although all certificates are revoked in Endpoint Management when the management relationship is severed, the configuration may specify an earlier revocation. For instance, the configuration can specify to revoke a certificate when the associated device configuration is deleted. In addition, under some conditions, the revocation of the associated certificate in Endpoint Management may be sent to the back-end public key infrastructure (PKI). That is, certificate revocation in Endpoint Management may cause certificate revocation on the PKI.
- Renewal settings. Certificates obtained 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.

**Methods of certificate issuance**

You can obtain a certificate, which is known as methods of issuance in two ways:

- **Sign:** 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. Endpoint Management supports the sign method for the three PKI entities (MS Certificate Services Entity, Generic PKI, and Discretionary CA).
Fetch: With this method, the issuance, for the purposes of Endpoint Management, is a recovery of an existing key pair. Endpoint Management supports the fetch method only for Generic PKI. A credential provider uses the sign or fetch method of issuance. The selected method affects the available configuration options. Notably, CSR configuration and distributed delivery are available only if the issuing method is sign. A fetched certificate is always sent to the device as a PKCS #12, the equivalent of centralized delivery mode for the sign method.

Certificate Delivery

Two modes of certificate delivery are available in Endpoint Management: centralized and distributed. Distributed mode uses 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, Endpoint Management acts like a delegate (a registrar) to the actual certificate authority. 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 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.

To configure the credential provider RA certificates, you upload the certificates to 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 Endpoint Management:

<table>
<thead>
<tr>
<th>Context</th>
<th>SCEP supported</th>
<th>SCEP required</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS Profile Service</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Citrix Endpoint Management

<table>
<thead>
<tr>
<th>Context</th>
<th>SCEP supported</th>
<th>SCEP required</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS mobile device management enrollment</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>iOS configuration profiles</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SHTP enrollment</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SHTP configuration</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Windows Phone and Tablet enrollment</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Windows Phone and Tablet config</td>
<td>No, except for the Wifi device policy, which is supported for Windows Phone 8.1 and the latest Windows 10 release</td>
<td>No</td>
</tr>
</tbody>
</table>

**Certificate Revocation**

There are three types of revocation.

- **Internal revocation:** Internal revocation affects the certificate status as maintained by Endpoint Management. 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 Endpoint Management, this type of revocation applies to certificates obtained from an external PKI. The certificate is revoked on the PKI when Endpoint Management internally revokes the certificate, under the conditions defined by the credential provider configuration. The call to perform the revocation requires a revoke-capable General PKI (GPKI) entity.

- **Externally induced revocation:** Also known as Revocation PKI, this type of revocation also only applies to certificates obtained from an external PKI. Whenever Endpoint Management evaluates a given certificate status, Endpoint Management queries the PKI as to that status. If the certificate is revoked, 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.

Endpoint Management first attempts to obtain 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, Endpoint Management attempts 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 Endpoint Management, is an internal entity. The issuing method for a discretionary entity is always sign. Sign means that with each issuing operation, 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 or a GPKI.

For detailed information about setting up DigiCert Managed PKI, including creating the credential provider, see “DigiCert Managed PKI” in PKI entities.

1. In the 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 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 obtain 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 1024 bits. To avoid false negatives, which depends on the underlying hardware and software, 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}
   ```

   For example, for client certificate authentication, use these settings:

   – **Key algorithm:** RSA

   – **Key size:** 2048

   – **Signature algorithm:** SHA1withRSA

   – **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 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 Endpoint Management and is required when using Citrix 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.

8. Click **Next**.

The **Credential Providers: Revocation Endpoint Management** page appears. On this page, you configure the conditions under which Endpoint Management internally flags certificates, issued through this provider configuration, as revoked.

9. On the **Credential Providers: Revocation Endpoint Management** page, do the following:

- In **Revoke issued certificates**, select one of the options indicating when to revoke certificates.

- To direct 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 Endpoint Management: Set **Revoke certificate on PKI** to **On** and, in the **Entity list**, click a template. The Entity list shows all available GPKI entities with revocation capabilities. When the certificate is revoked from 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 Endpoint Management macros for the DN field values. For example:
     
     ```
     CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}
     ```

   • 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 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 Endpoint Management to do the following:
• Renew the certificate. You can optionally send a notification 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. Endpoint Management doesn’t renew certificates after they are internally revoked.

To direct Endpoint Management to send a notification when the certificate has been renewed: Set Send notification to On. To direct 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.

14. Click Save.

The credential provider appears in the Credential Provider table.

APNs certificates

October 7, 2019

To enroll and manage Apple devices in Endpoint Management, you set up an Apple Push Notification service (APNs) certificate from Apple.

Note:

• The APNs certificate from Apple enables mobile device management via the Apple Push Network. 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.

The topics that outline the step-by-step procedures are listed in order in this section. Here’s a summary of the process.

**Step 1:** For Windows, generate a Certificate Signing Request (CSR) by using Microsoft IIS. For Mac, generate a CSR on a Mac computer. Citrix recommends this method.

**Step 2:** Submit the CSR to Citrix. Citrix signs the CSR with its mobile device management signing certificate and returns the signed file in a .plist format.

**Step 3:** Submit the signed CSR to Apple and then download the APNs certificate from Apple.

**Step 4:** Export the APNs certificate as a PKCS #12 (.pfx) certificate (on IIS, Mac, or SSL).

**Step 5:** Import an APNs certificate into Endpoint Management.

### Important:

Note the Apple ID used to create the certificate. In addition, the Apple ID must be a corporate ID and not a personal ID.

### To 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**.
4. Type the appropriate Distinguished Name (DN) information and 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**.

### To create a CSR on a Mac computer

1. On a Mac computer running macOS, under **Applications > Utilities**, start the Keychain Access application.
2. Open the **Keychain Access** menu and then click **Preferences**.
3. Click the **Certificates** tab, change the options for **OCSP** and **CRL** to Off and then close the **Preferences** window.

5. The Certificate Assistant prompts you to enter the following information:
   - **EmailAddress**: Email address of the individual or role account who is responsible for managing the certificate.
   - **Common Name**: Common name of the individual or a role account who is responsible for managing the certificate.
   - **CA Email Address**: Email address of the Certificate Authority.

6. Select the Saved to disk and Let me specify key pair information options and then click Continue.

7. Enter a name for the CSR file, save the file on your computer, and then click Save.

8. 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.

9. Click Done when the Certificate Assistant completes the CSR process.

To create a CSR by using OpenSSL

If you cannot use a Mac computer or Microsoft IIS to generate a CSR: You can use OpenSSL instead.

To use OpenSSL to create a CSR, first download and install OpenSSL from the OpenSSL website.

1. On the computer where you installed OpenSSL, execute 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 ----- Country Name (2 letter code) [AU]:US
   7 State or Province Name (full name) [Some-State]:CA
   8 Locality Name (eg, city) []:RWC
   9 Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer
   ```
3. At the next message, enter a password for the CSR private key.

To sign the CSR

Before you can submit the certificate to Apple, submit the certificate to Citrix for signing so it can be used with Endpoint Management.

1. In your browser, go to the Endpoint Management Tools website and then click Request push notification certificate signature.

2. On the Creating a new certificate page, click Upload the CSR.
3. Browse to and select the certificate.

   The certificate must be in .pem/txt format.

4. On the **Endpoint Management APNs CSR Signing** page, click **Sign**. The CSR is signed and automatically saved to your configured download folder.

**To submit the signed CSR to Apple to obtain the APNs certificate**

After receiving your signed Certificate Signing Request (CSR) from Citrix, submit it to Apple to obtain the APNs certificate.

**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** check box 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 is successful.

5. Click **Download** to retrieve the .pem certificate.

   If you use Internet Explorer and the file name extension is missing, click **Cancel** two times. Then download from the next window.

**To create a .pfx APNs certificate by using Microsoft IIS**

To use the APNs certificate from Apple with Endpoint Management: Complete the certificate request in Microsoft IIS, export the certificate as a PCKS #12 (.pfx) file, and then import the APNs certificate into Endpoint Management.

**Important:**

Use the same IIS server for this task as the server 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 during Endpoint Management installation.

7. Copy the .pfx certificate to the server on which you plan to install Endpoint Management.

8. Sign on to the Endpoint Management console as an administrator.

9. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.
10. Click **Certificates**. The **Certificates** page appears.

11. Click **Import**. The **Import** dialog box appears.
12. From the Import menu, choose Keystore.

13. From Use as, choose APNs.
14. In **Keystore** file, select the keystore file you want to import by clicking **Browse** and navigating to the file’s location.

15. In **Password**, type the password assigned to the certificate.

16. Click **Import**.

**To create a .pfx APNs certificate on a Mac computer**

A .p12 file and .pfx file are the same and can be used interchangeably.

1. On the same Mac computer running macOS that you used to generate the CSR, locate the Production identity (.pem) certificate that you received from Apple.

2. Double-click the certificate file to import the file into the keychain.

3. If you are prompted to add the certificate to a specific keychain, keep the default login keychain selected and then click **OK**. The newly added certificate appears in your list of certificates.

4. Click the certificate and then on the **File** menu, click **Export** to begin exporting the certificate into a PCKS #12 (.pfx) certificate.
5. Give the certificate file a unique name for use with the Endpoint Management server. 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 application prompts you for the login password or selected keychain. Enter the password and then click **OK**. The saved certificate is now ready for use with the Endpoint Management server.

**Note:**

If you don’t plan to keep the computer and user account that you used to generate the CSR and complete the export process: Citrix recommends that you save or export the Personal and Public Keys from the local system. Otherwise, access to the APNs certificates for reuse is voided and you must then repeat the entire CSR and APNs process.

---

**To create a .pfx APNs certificate by using OpenSSL**

After you use OpenSSL to create a Certificate Signing Request (CSR), you can also use OpenSSL to create a .pfx APNs certificate.

1. At a command prompt or shell, execute 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.

   ```bash
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey.pem -out apns_identity.pfx
   ```

2. Enter a password for the .pfx certificate file. Remember this password because you use the password again when you upload the certificate to Endpoint Management.

3. Note the location for the .pfx certificate file. Then, copy the file to the Endpoint Management server so you can use the console to upload the file.

---

**To import an APNs certificate into Endpoint Management**

After you request and receive a new APNs certificate: Import the APNs certificate into Endpoint Management to either add the certificate for the first time or to replace a certificate.

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.

2. Click **Certificates**. The **Certificates** page appears.

3. Click **Import**. The **Import** dialog box appears.
4. From the **Import** menu, choose **Keystore**.
5. From **Use as**, choose **APNs**.
6. Browse to the .pfx or .p12 file on your computer.
7. Enter a password and then click **Import**.

For more information about certificates in Endpoint Management, see **Certificates and authentication**.

### To renew an APNs certificate

To renew an APNs certificate, perform the same steps you would if you were creating a certificate. Then, see the Apple Push Certificates Portal. From that page, upload the new certificate. After logging on, your existing certificate or a certificate imported from your previous Apple Developers account appears.

On 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. When you are renewing your certificate, ensure that you use the same organization name and Apple ID.

To determine when your APNs certificate expires, in the Endpoint Management console, click **Configure > Settings > Certificates**. If the certificate is expired, however, do not revoke the certificate.

**Note:**

Do not use an Internet Explorer browser, or else step 7 outputs a .json file instead of a .pem file.

1. Generate a CSR, using IIS (Microsoft), OpenSSL, or Keychain Access (macOS).
2. In your browser, go to **Endpoint Management Tools**. Then, click **Request push notification certificate signature**.

---

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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 Endpoint Management console, import the .pfx file and complete the configuration as follows:

1. Go to **Settings > Certificate Management**.

2. On the **Certificates** page, click **Import**.

3. From the **Import menu**, choose **Keystore**.

4. From the **Keystore type menu**, choose **PKCS #12**.

5. From **Use as**, choose **APNs**.
6. For Keystore file, click Browse and navigate to the file.

7. In Password, type the certificate password.

8. Type an optional Description.

9. Click Import.

Endpoint Management redirects you back to the Certificates page. The Name, Status, Valid from, and Valid to fields update.

Note:

If you use a different Apple ID for the renewal process, devices need to be re-enrolled.

**SAML for single sign-on with Citrix Files**

December 18, 2019
**Important:**

This article applies only to Endpoint Management environments that aren’t Workspace-enabled.
In a Workspace-enabled environment, Content Collaboration is integrated directly with Citrix Workspace.

You can configure Endpoint Management and Content Collaboration to use 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 wrapped with the MDX Service or MDX Toolkit and 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 Secure Hub for user authentication and to acquire a SAML token. After successful authentication, the Citrix Files mobile app sends the SAML token to Content Collaboration. After the initial logon, users can access the Citrix Files mobile app through SSO. They can also attach documents from Content Collaboration to 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 Endpoint Management. Endpoint Management authenticates the users, who then acquire a SAML token which is sent to Content Collaboration. After the initial logon, users can access Citrix Files clients through SSO without logging on each time.

To use Endpoint Management as a SAML identity provider (IdP) to Content Collaboration, you must configure Endpoint Management for use with Enterprise accounts, as described in this article. Alternatively, you can configure Endpoint Management to work only with storage zone connectors. For more information, see [Content Collaboration use with Endpoint Management](#).

For a detailed reference architecture diagram, see [Architecture](#).

**Prerequisites**

Complete the following prerequisites before you can configure SSO with Endpoint Management and Citrix Files apps:

- The MDX Service or a compatible version of the MDX Toolkit (for Citrix Files mobile apps).
  
  For more information, see [Endpoint Management compatibility](#).

- A compatible version of Citrix Files mobile apps and Secure Hub.

- Content Collaboration administrator account.

- Connectivity verified between Endpoint Management and Content Collaboration.
Configure Content Collaboration access

Before setting up SAML for Content Collaboration, provide Content Collaboration access information as follows:

1. In the Endpoint Management web console, click **Configure > Content Collaboration**. The **Content Collaboration** configuration page appears.

2. Configure these settings:
   - **Domain**: Type your Content Collaboration 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.
   - **Content Collaboration Administrator Account Logon**
     - **User name**: Type the Content Collaboration administrator user name. This user must have administrator privileges.
Citrix Endpoint Management

- **Password**: Type the Content Collaboration administrator password.
- **User account provisioning**: To enable user provisioning in Endpoint Management, enable this setting. To use the Content Collaboration User Management Tool for user provisioning, leave this setting disabled.

**Note:**
If a user without a Content Collaboration account is included in the selected roles and you enable User account provisioning: Endpoint Management automatically provisions a Content Collaboration account for that user. Citrix recommends that you use a role with a small membership for testing the configuration. Doing so avoids the potential of many users without Content Collaboration accounts.

3. Click **Test Connection** to verify that the user name and password for the Content Collaboration administrator account authenticate to the specified Content Collaboration account.

4. Click **Save**.

- Endpoint Management syncs with Content Collaboration and updates the Content Collaboration settings **ShareFile Issuer/Entity ID** and **Login URL**.
- The **Configure > Content Collaboration** page shows the **App internal name**. You need that name to complete the steps described later in **Modify the Citrix Files.com SSO settings**.

**Set up SAML for Wrapped Citrix Files MDX Apps**

The following steps apply to iOS and Android apps and devices.

1. Wrap the Citrix Files mobile app with MDX. For details, see **Endpoint Management MDX Service**.

2. In the Endpoint Management console, upload the wrapped Citrix Files mobile app. For information about uploading MDX apps, see **To add an MDX app to Endpoint Management**.

3. Verify the SAML settings: Log on to Content Collaboration with the administrator user name and password you configured above.

4. Verify that Content Collaboration and Endpoint Management are configured for the same time zone. Ensure that Endpoint Management shows the correct time for the configured time zone. If not, SSO might fail.

**Validate the Citrix Files mobile app**

1. On the user device, install and configure 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 Secure Mail

1. On the user device, if it has not already been done, install and configure Secure Hub.
2. From the app store, download, install, and set up 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 user name or password.

Configure Citrix 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 Citrix Gateway to support the use of 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 Citrix 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 Citrix Gateway virtual server that is used for Endpoint Management logons. In Citrix Gateway, go to **Other Settings** and then clear the check box labeled **Redirect to Home Page**.

2. Under **ShareFile** (now called Content Collaboration), type your Endpoint Management internal server name and port number.
3. Under **Citrix Endpoint Management**, type your Endpoint Management URL.
This configuration authorizes requests to the URL 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:

1. In the Citrix 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.*

Configure these settings:

- **ICA Proxy**: Click **ON**.
- **Web Interface Address**: Type your Endpoint Management server URL.
- **Single Sign-on Domain**: Type your Active Directory domain name.

When configuring the Citrix Gateway Session Profile, the domain suffix for **Single Sign-on Domain** must match the Endpoint Management domain alias defined in LDAP.

5. Click **Create** to define the session profile.

6. Click **Expression Editor**.
Configure these settings:

- **Value**: Type NSC_FSRD.
- **Header Name**: Type COOKIE.

7. Click **Create** and then click **Close**.

### Configure policies on the Citrix Gateway virtual server

Configure these settings on the Citrix Gateway virtual server.

1. In the Citrix Gateway configuration utility, in the left navigation pane, click **NetScaler Gateway > Virtual Servers**.
2. In the **Details** pane, click your Citrix Gateway virtual server.
3. Click **Edit**.
4. Click **Configured policies > Session policies** and then click **Add binding**.
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:

![VPN Virtual Server Session Policy Binding](image)

7. Click **Done** and then save the running Citrix Gateway configuration.

**Modify the Citrix Files.com SSO settings**

Make the following changes for both MDX and non-MDX Citrix Files apps.

**Important:**

Each time you edit or recreate the Citrix Files app or change the Content Collaboration settings in Endpoint Management, a new number is appended the internal application name. As a result, you must also update the Login URL in the Citrix Files website to reflect the updated app name.

Content Collaboration no longer sends a Referrer header on Chrome or FireFox. For information, see [Release Notes, ShareFile Web Application v19.17](#).

1. Log on to your Content Collaboration account ([https://<subdomain>.sharefile.com](https://<subdomain>.sharefile.com)) as a Content Collaboration administrator.

2. In the Content Collaboration 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&amp;app=ShareFile_SAML_SP&amp:reqtype=1](https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&amp;app=ShareFile_SAML_SP&amp:reqtype=1).
- Insert the Citrix Gateway virtual server external FQDN plus /cginfra/https/ in front of the Endpoint Management server FQDN and then add 8443 after the 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 > Content Collaboration page.


- Add &nssso=true to the end of the URL.


4. Under Optional Settings, select the Enable Web Authentication check box.
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 Citrix Gateway logon form. If you are not redirected, verify the preceding configuration settings.

2. Enter the user name and password for the Citrix Gateway and Endpoint Management environment you configured.
   Your Citrix Files folders at <subdomain>.sharefile.com appear. If you do not see your Citrix Files folders, ensure that you entered the proper logon credentials.

Single sign in with Azure Active Directory

December 18, 2019

Endpoint Management supports single sign-in with Azure Active Directory credentials for the following scenarios:

- User enrollment through Citrix Secure Hub (Android or iOS)
- For the RBAC User role, authentication to the Endpoint Management Self-Help Portal
- Administrator authentication to the Endpoint Management console
- For Endpoint Management, administrator authentication to the Public API for REST Services by using a token retrieved through the Citrix Cloud API.
Citrix Endpoint Management

- For more information, see section 3.3.2, Login (Cloud Credentials), in the Public API for REST Services PDF.

Endpoint Management uses the Citrix Cloud service, Citrix Identity Platform, to federate with Azure Active Directory. Citrix Identity Platform is an identity provider (IDP) service.

To set up this service, you configure Citrix Cloud to use Azure Active Directory as your Identity Provider. Then, configure Citrix Identity Platform as the IDP type for Endpoint Management. Users can then log on to Secure Hub with their Azure Active Directory credentials. Secure Hub uses client certificate authentication for MAM devices.

Citrix recommends that you use Citrix Identity Platform instead of a direct connection to Azure Active Directory.

Prerequisites for single sign in with Azure Active Directory

- Citrix Gateway, configured for certificate-based authentication
- Secure Hub 10.7.20 (minimum version)
- Azure Active Directory user credentials
- Citrix Cloud account, with Citrix Cloud Connector installed for directory services synchronization

Configure Citrix Cloud to use Azure Active Directory as your Identity Provider

To configure Azure Active Directory in Citrix Cloud:

1. Go to https://citrix.cloud.com and sign in to your Citrix Cloud account.
2. From the Citrix Cloud menu, go to the Identity and Access Management page and connect to Azure Active Directory.

   ![Identity and Access Management](image)

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.

**Configure Citrix Identity Platform as the IDP type for Endpoint Management**

After you configure Azure Active Directory in Citrix Cloud, configure Endpoint Management as follows.

1. In the Endpoint Management console, go to **Settings > Identity Provider (IDP)** and then click **Add**.

2. In the **Identity Provider (IDP)** page, configure the following:
Citrix Endpoint Management

- **IDP Name**: Type a unique name to identify the IDP connection that you are creating.
- **IDP Type**: Choose Citrix Identity Platform.
- **Auth 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.
- **User Identifier string**: This field is automatically filled.

4. Click Next, review the Summary page, and then click Save.

Secure Hub users, Endpoint Management console, and Self-Help Portal users can now sign in with their Azure Active Directory credentials.

**Endpoint Management administrator and user authentication flow**

The sign-in screen for the Endpoint Management console and the Endpoint Management Self-Help Portal includes the link **Sign in with my company credentials**.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 213
Click that link to enter your Azure Active Directory credentials. After successfully authenticating you, Endpoint Management doesn’t require you to sign in for future access.

If you sign in to the Endpoint Management console or Self-Help Portal from domain-joined devices and click the **Sign in with my company credentials** link: Endpoint Management provides a single sign-on experience. No authentication prompt appears.

**Secure Hub authentication flow**

With Endpoint Management configured to use Citrix Identity Platform as its IDP, the Secure Hub authentication flow is as follows for a device enrolled through Secure Hub:

1. A user starts Secure Hub.
2. Secure Hub passes the authentication request to Citrix Identity Platform, which passes the request to Azure Active Directory.
3. The user types their user name and password.
4. Azure Active Directory validates the user and sends a code to Citrix Identity Platform.
5. Citrix Identity Platform sends the code to Secure Hub, which sends the code to the Endpoint Management server.
6. Endpoint Management obtains an ID token by using the code and secret, and then validates the user information that’s in the ID token. Endpoint Management returns a session ID.

Users of domain-joined devices can use their Azure Active Directory credentials for a single sign-on experience. For Endpoint Management local accounts, single sign-on isn’t available.
Derived credentials

August 28, 2019

Derived credentials provide strong authentication for mobile devices. The credentials, derived from a smart card, reside in a mobile device instead of the card. The smart card is a Personal Identity Verification (PIV) card.

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

Endpoint Management can use derived credentials for device enrollment and authentication. If configured for derived credentials, Endpoint Management doesn’t support enrollment invitations or other enrollment modes. Citrix supports use of a derived credentials app during enrollment of iOS.

Architecture

For enrollment, Endpoint Management connects to the components, as shown in the following diagram.

- During device enrollment, Secure Hub obtains certificates from the derived credentials app.
- The derived credentials app communicates with the credential management server during enrollment.
• You can use the same or different server for the credential management server and a third-party PKI provider.
• Endpoint Management connects to your third-party PKI server to obtain certificates.

Requirements

• Download and install Citrix Secure Hub.
• Based on your derived credential solution, download and configure the app:
  – **For Entrust Datacard:**
    * Download and install the Citrix Derived Credential Manager app on your devices before enrolling in Endpoint Management. The Derived Credentials Manager app is the identity provider app for Citrix. The logo for that app follows.
    
    ![Derived Credential Manager](image)
    
    **Note:**
    Citrix Derived Credential Manager app supports new enrollments only. Device users must re-enroll.
    * Endpoint Management must be configured for MDM+MAM mode.
  – **For other derived credentials providers:** While it’s likely that most other credential solutions are compatible with XenMobile, test the integration before deploying it to production.
  – Must have the root certificate of the authority that issues certificates to the Credentials Provider server. That setup enables Endpoint Management to accept the digitally signed certificates during enrollment. For information about adding the certificates, see Certificates and authentication.
    – If the user email domain differs from the LDAP domain, include the email domain in the Domain alias setting in Settings > LDAP. For example, if the domain for email addresses is citrix.com and the LDAP domain name is sample.com, set Domain alias to sample.com, citrix.com.
- Endpoint Management doesn’t support the use of derived credentials with shared devices.

• User identity certificates:
  - The user name in the Subject alternative name field must be formatted as the otherName, rfc822Name, or dNSName field of the SubjectAltName extension. Other fields are not supported. For more information about Subject alternative name, see the RFC, [https://www.ietf.org/rfc/rfc5280.txt](https://www.ietf.org/rfc/rfc5280.txt).
  - User identity in the Subject field in either Email or CN isn’t supported.

• Citrix Gateway configured for certificate authentication or certificate plus security token authentication

Enable derived credentials

By default, the Endpoint Management console doesn’t include the Settings > Derived Credentials page.

To enable the interface for derived credentials:

  • Go to Settings > Server Properties, add derived.credentials.enable as the server property, and set the property value to true.

Configure derived credentials

The assumption is that you have a working configuration for the derived credentials provider that you plan to integrate with Endpoint Management. You can configure Endpoint Management to communicate with that server. You can also choose a derived credentials CA certificate already added to Endpoint Management or import the certificate.
You can activate Online Certificate Status Protocol (OCSP) support for that CA certificate. For more information about OCSP, see “Discretionary CAs” in PKI entities.

1. In the Endpoint Management console, go to **Settings > Derived Credentials for iOS**.

2. For **Choose derived credentials provider**, choose **Other** for Entrust Datacard. Type `dcapp://mode=SecureHub` in the App URL (iOS).

3. **Optional parameters:** Some derived credential providers might require that you provide parameters for the connection. For example, a vendor might require that you specify the URLs of a back-end server. Click **Add** to provide parameters.

4. Specify a certificate for derived credentials: If the certificate is already uploaded to Endpoint Management, choose that certificate from **Issuer CA**. Otherwise, click **Import** to add a certificate. The **Import Certificate** dialog box appears.

5. In the **Import Certificate** dialog box, click **Browse** to navigate to the certificate. Then click **Browse** to navigate to the private key file.
6. Configure the settings.
   - For Citrix Derived Credential Manager app: The User Identifier field is Subject alternative name, and the User Identifier type is userPrincipalName.
   - Contact other derived credential providers for their information.

7. You can optionally use an OCSP responder for certificate revocation checking. Citrix recommends using an OCSP responder for security purposes. By default, OSP checking is Off.
   - If you activate OCSP support for the CA certificate, choose an option for Use custom OCSP URL. By default, Endpoint Management extracts the OCSP URL from the certificate (the Use certificate definition for revocation option). To specify a responder URL, click Use custom and then type the URL.
   - Responder CA: From Responder CA, choose a certificate. Or, click Import and then use the Import Certificate dialog box to locate the certificate.

8. Click Save. The Enabling Derived Credentials dialog box appears.
To enable the derived credentials configuration, click **Save**. To use derived credentials, you must also configure enrollment settings.

To enable the derived credentials configuration and then go immediately to **Settings > Enrollment**, click **Save and Go to Enrollment**.

9. To enable derived credentials for enrollment: On the **Settings > Enrollment** page, under **Advanced Enrollment**, select **Derived Credentials (iOS only)** and then click **Enable**.

10. A confirmation dialog box appears. To enable derived credentials, select the check box, and click **Enable**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
11. To edit options for derived credentials enrollment, go to Settings > Enrollment, select Derived Credentials (iOS only) and then click Edit.

After you enable derived credentials: In the Devices Enrollment report, the column Enrollment mode shows derived_credentials.

**Configure Endpoint Management for Secure Mail**

To enable Secure Mail to work with derived credentials, add the LDAP Attributes client property. For information about adding a client property, see Client properties.

Use the following information for the client property:

- **Key:** SEND_LDAP_ATTRIBUTES
- **Value:** userPrincipalName=${ user.userprincipalname },sAMAccountName=${ user.samaccountname },displayName=${ user.displayName },mail=${ user.mail }
Activating Entrust Datacard derived credentials on iOS devices

Note:

While using Entrust website:

- Ensure that the Internet Explorer browser is Java-enabled, when you program the PIV card.
- Clear the browser cache when changing the PIV card.

1. To request new smart credentials, use a desktop or any device to log in to the Entrust site. Log in using the Smart Credential Log In button at the bottom of the page. Users insert their smart card into a reader attached to their desktop.
2. From the **Self-Administration Actions**, select the **I’d like to enroll for a derived mobile smart credential** and click **Done**.
3. In the **Derived Mobile Smart Credential** screen, provide the **Identity Name**. The user can choose a unique name such as a user name or ID numbers.

4. Select the **Citrix DCAPP** from the Derived credential app menu, and click **Ok**.
A QR code Activation screen appears and prompts the user to scan the code with their mobile device.

**Note:**

By default, the derived credentials QR code expires in 3 minutes.

5. Scan the QR code using the **Derived Credential Manager** app on the device to complete the activation.

---

**Device enrollment**

After you complete the setup described earlier in this article, users can enroll their devices by using derived credentials.
1. Tap to open Secure Hub. When prompted, type the Endpoint Management server fully qualified domain name and then click Next.

2. Click Yes, Enroll. Device enrollment in Secure Hub starts.

If Endpoint Management is configured for derived credentials, Secure Hub prompts the user to create and confirm the Citrix PIN.
After confirming the Citrix PIN the Derived Credentials setup splash screen appears. Follow the instructions to activate smart credentials.

3. Tap **Scan code**. The mobile phone camera activates.
Note:
To scan the QR code, ensure your camera and microphone is enabled and has required access permissions.

4. In the derived credentials app, scan the QR code that was created in earlier steps.
5. After scanning the QR code, on the **Import New Certificate** screen a password dialog box appears, enter the password and click **OK**.
Import New Certificate screen appears with fields auto-populated.
6. After the certificates are added successfully, in the Derived Credentials screen, click Start Enrollment.
7. In Secure Hub, enter a new PIN when prompted.

After authenticating the PIN, Secure Hub downloads the certificates. Follow the prompts to complete the enrollment.

To view device information in the Endpoint Management console:

- Go to Manage > Devices and then select a device to display a command box. Click Show more.
- Go to Analyze > Dashboard.
You perform user configuration tasks in the 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 mode and invitations**
  - From Settings > Enrollment, configure up to seven enrollment modes and send enrollment invitations. Each enrollment mode has its own level of security and number of steps users must take to enroll their devices.
  - Set up Endpoint Management AutoDiscovery Service

- **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 three different channels: Secure Hub, SMTP, or SMS. For more information, see: Creating and updating Notification Templates.

- **User accounts and groups:**
  - From Manage > Users, you can add user accounts manually or use a .csv provisioning file to import the accounts and to manage local groups. However, most 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 Endpoint Management user account is either for a local, Active Directory, or cloud user.

A cloud user is a special user account that Citrix Cloud creates and manages on the Endpoint Management server. Citrix Cloud creates a cloud user account when an administrator is added to your Citrix Cloud customer account. A cloud user account uses the same user name as the administrator account.
Citrix Endpoint Management

The cloud user account provides single sign-on and performs other administrative functions.

For cloud users:

- You can change the roles and user properties of cloud users through the Endpoint Management console.
- You cannot change cloud user passwords through the Endpoint Management console.
- You can change a cloud user password from Identity and access management in Citrix Cloud.
- You cannot delete cloud users.
- You cannot give cloud users membership in a group.

Configure enrollment modes

You configure device enrollment modes to allow users to enroll their devices in Endpoint Management. Endpoint Management offers seven modes, each with its own level of security and steps users must take to enroll their devices.

You can make some modes available on the Self-Help Portal. From the portal, users generate enrollment links that allow them to enroll their devices. Or users can choose to send themselves an enrollment invitation from the portal. You configure enrollment modes in the Endpoint Management console from the Settings > Enrollment page.

You send enrollment invitations 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 modes. For more information about notification templates, see Creating or Updating Notification Templates.

1. On the 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, containing a table of all available enrollment modes. By default, all enrollment modes are enabled.

3. Select any enrollment mode in the list to edit it. Then, set the mode as the default, disable the mode, or allow users access through the Self-Help Portal.

   Select the check box next to an enrollment 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.
Choose from these enrollment modes:

- User name + Password
- High Security
- Invitation URL
- Invitation URL + PIN
- Invitation URL + Password
- Two Factor
- User name + PIN (not available for Android Enterprise)

You can use enrollment invitations to restrict enrollment to users with an invitation only.

You can use one-time PIN (sometimes referred to as OTP) enrollment invitations as a two-factor authentication solution. One-time PIN enrollment invitations control the number of devices a user can enroll.

For environments with the highest security requirements, you can tie enrollment invitations to a device by SN/UDID/EMEI. A two-factor authentication option is also available to require an Active Directory password and One-time PIN.

To edit an enrollment mode

1. In the Enrollment list, select an enrollment 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**: In the list, click **Days** or **Hours** 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.

- **Numeric**: In the list, click **Numeric** or **Alphanumeric** for the PIN type.

- **Notification templates**:
  - **Template for enrollment URL**: In the list, click a template to use for the enrollment URL. For example, the Enrollment invitation template sends users an email or SMS. The method depends on how you configured the template that lets them enroll their devices in Endpoint Management. For more information on notification templates, see [Create or update notification templates](#).
– **Template for enrollment PIN:** In the list, click a template to use for the enrollment PIN.
– **Template for enrollment confirmation:** In the list, click a template to use to inform a user that they enrolled successfully.

3. Click **Save.**

**To set an enrollment mode as default**

The default enrollment mode is used for all device enrollment requests unless you select a different enrollment mode. If no enrollment mode is set as the default, you must create an enrollment request for each device enrollment.

**Note:**

The only enrollment modes that you can use as a default are **Only Username + Password**, **Two Factor**, or **Username + PIN**.

1. Select the default enrollment mode, either **Username + Password**, **Two Factor**, or **Username + PIN**.

   To use a mode as the default, first enable it.

2. Click **Default**. The selected mode is now the default. If any other enrollment mode was set as the default, the mode is no longer the default.

**To disable an enrollment mode**

Disabling an enrollment 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 mode and enabling another.

1. Select an enrollment mode.

   You cannot disable the default enrollment mode. If you want to disable the default enrollment mode, you must first remove its default status.

2. Click **Disable**. The enrollment mode is no longer enabled.

**To enable an enrollment mode on the Self-Help Portal**

Enabling an enrollment mode on the Self-Help Portal lets users enroll their devices in Endpoint Management individually. The Self-Help Portal can be accessed at the same URL admins access the Endpoint Management console. End users see the Self-Help Portal instead of the admin console.
Note:

- The enrollment mode must be enabled and bound to notification templates to be made available on the Self-Help Portal.
- You can only enable one enrollment mode on the Self-Help Portal at a time.

1. 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.

2. Select an enrollment mode.

3. Click Self-Help Portal. The enrollment mode you selected is now available to users on the Self-Help Portal. Any mode already enabled on the Self-Help Portal is no longer available to users.

Add, edit, or delete local user accounts

You can add local user accounts to 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 are created as Endpoint Management administrators. If you create a Citrix Cloud administrator with custom access, make sure that access includes Endpoint Management. For information on adding Citrix Cloud administrators, see Add administrators.

1. In the Endpoint Management console, click Manage > Users. The Users page appears.

2. Click Show filter to filter the list.

To add a local user account

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.
- **Role:** In the list, click the user role. For more information about roles, see Configure roles with RBAC. Possible options are:
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- **Membership:** In the list, click the group or groups 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:
  - **User Properties:** In the list, click a property 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 containing 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**.

**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**: In the list, click the user role.
   - **Membership**: In the list, click the group or groups to which to add or edit the user account. To remove the user account from a group, clear the check box next to the group name.
   - **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**: In the list, click a property 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 containing 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 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 check box next to each user account.

2. Click **Delete**. A confirmation dialog box appears.

3. Click **Delete** to delete the user account or click **Cancel**.

**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 Endpoint Management, the user cannot enroll by using the corresponding LDAP credentials.

- If importing user accounts to the 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 Endpoint Management.

1. In the Endpoint Management console, click **Manage > Users**. The **Users** page appears.
2. Click Import Local Users. The Import Provisioning File dialog box appears.

   ![Import Provisioning File dialog box](image)

3. Select either User or Property for the format of the provisioning file 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 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 contains 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 sensitive.

Example of user provisioning content

The entry `user01;pwd\;01;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 Endpoint Management console on these pages: **Users, Add Local User,** or **Edit Local User.** There is no group edit command.

To add a local group

1. Do one of the following:
On the Users page, click Manage Local Groups.

![Users page](image)

On either the Add Local User page or the Edit Local User page, click Manage Groups.

![Add Local User page](image)

The Manage Group dialog box appears.
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. However, any other group associations remain intact. If users aren’t associated with any other local groups, they are associated at the top level.

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 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**.
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 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 Endpoint Management:

- In the Settings > Workflows page in the 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 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 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.
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 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 Search. Names originate in Active Directory.
When the name appears in the field, select the check box 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 check box 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 check box 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.

**Notifications**

August 26, 2019

You can use notifications in Endpoint Management for the following purposes:

- To communicate with select groups of users for a number of 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 Endpoint Management, you must configure a gateway and a notification server. You can set up a notification server in Endpoint Management to configure Simple Mail Transfer Protocol (SMTP) and Short Message Service (SMS) gateway servers to send email and text (SMS) notifications to users. You can use notifications to send messages over two different channels: SMTP or SMS.

- **SMTP** is a connection-oriented, text-based protocol in which a mail sender communicates with a mail receiver by issuing command strings and supplying necessary data, typically over a Transmission Control Protocol (TCP) connection. SMTP sessions consist of commands originated by an SMTP client (the person sending the message) and corresponding responses from the SMTP server.
- **SMS** is a text messaging service component of phone, Web, or mobile communication systems. SMS uses standardized communications protocols to enable fixed line or mobile phone devices to exchange short text messages.

You can also set up a Carrier SMS Gateway in Endpoint Management to configure notifications that are sent through an SMS gateway of a carrier. Carriers use SMS gateways to send or receive SMS transmissions to or from a telecommunications network. These text-based messages use standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages.

**Prerequisites**

- Before configuring the SMS gateway, consult your system administrator to determine the server information. It’s important to know whether the SMS server is hosted on an internal corporate server, or whether the server is part of a hosted email service. In that case, you need information from the website of the service provider.
- 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.
- Make sure that only one SMTP server and only one SMS server is active at a time.
- Open port 25 from Endpoint Management located in your network DMZ to point back to the SMTP server on your internal network. That enables Endpoint Management to send notifications successfully.

**Configure an SMTP server and SMS gateway**

1. In the 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 or an SMS gateway.

![Notification Server](image)

- To add an SMTP server, click **SMTP Server** and then see Add an SMTP server for the steps to configure this setting.
- To an SMS gateway, click **SMS Gateway** and then see Add an SMS gateway for the steps to configure this setting.
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. The host name may be a fully qualified domain name (FQDN) or an IP address.
   - **Secure channel protocol**: In the list, click **SSL**, **TLS**, or **None** 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, the port is set to 465.
• **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 is continuously failing because of timeouts. Use caution when decreasing this value; it could increase 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**.
Add an SMS gateway

1. Configure the following settings:

   - **Name**: Type a name for the SMS Gateway configuration. This field is required.
   - **Description**: Optionally, type a description of the configuration.
   - **Key**: Type the numerical identifier provided by the system administrator when activating the account. This field is required.
   - **Secret**: Type a secret provided by the system administrator that is used to access your account in the event that a password is lost or stolen. This field is required.
   - **Virtual Phone Number**: This field is used when sending to North American phone numbers (with the +1 prefix). You must type a Nexmo virtual phone number and you must only use digits in this field. You can purchase virtual phone numbers on the Nexmo website.
   - **HTTPS**: Select whether to use HTTPS to transmit SMS requests to Nexmo. The default is
Important:
Leave HTTPS set to ON unless you have guidance from Citrix Support to turn it to OFF.

- **Country Code:** In the list, click the default SMS country code prefix for recipients in your organization. This field always starts with a + symbol. The default is Afghanistan +93.

2. Click **Test Configuration** to send a test message using the current configuration. Connection errors, such as authentication or virtual phone number errors, are detected and appear immediately. Messages are received in the same time frame as messages sent between mobile phones.

3. Click **Add**.

**Add a carrier SMS gateway**

You can set up a Carrier SMS Gateway in Endpoint Management to configure notifications that are sent through a carrier’s SMS gateway. Carriers use Short Message Service (SMS) gateways to send or receive SMS transmissions to or from a telecommunications network. These text-based messages use standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages.

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.

2. Under **Notifications**, click **Carrier SMS Gateway**. The **Carrier SMS Gateway** page opens.
3. Do one of the following:

- Click **Detect** to automatically discover a gateway. A dialog box appears indicating that there are no new carriers detected or listing the new carriers detected among enrolled devices.
- Click **Add**. The **Add a Carrier SMS Gateway** dialog box appears.

![Carrier SMS Gateway](image)
4. Configure these settings:

- **Carrier**: Type the name of the carrier.
- **Gateway SMTP domain**: Type the domain associated with the SMTP gateway.
- **Country code**: In the list, click the country code for the carrier.
- **Email sending prefix**: Optionally, specify an email sending prefix.

5. Click **Add** to add the new carrier or click **Cancel** to not add the new carrier.
Create and update notification templates

You can create or update notification templates in 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 three different channels: Secure Hub, SMTP, or SMS.

Endpoint Management includes many predefined notification templates that reflect the distinct types of events that Endpoint Management automatically responds to for every device in the system.

**Note:**

If you plan to use SMTP or SMS channels to send notifications to users, you must set up the channels before you can activate them. Endpoint Management prompts you to set up the channels when you add notification templates if they are not already set up.

1. In the 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.

Add a notification template

1. Click **Add**. If no SMS gateway or SMTP server has been set up, a message appears regarding the use of SMS and SMTP notifications. You can choose to set up the SMTP server or SMS gateway...
now or set them up later.

If you choose to set up SMS or SMTP server settings now, you are 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 SMS or SMTP server settings later, you will not be able to activate those channels when you add or edit a notification template, which means those channels will not be 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:** In the list, click the notification type. Only supported channels for the selected type appear. Only one APNS Cert Expiration template is allowed, which is a predefined template. This means you cannot add a new template of this type.

   **Note:**

   For some template types, the phrase Manual sending supported appears below the type. This means that the template is available in the Notifications list on the Dashboard and on the Devices page to let you manually send the notification to users. Manual sending is not 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)}

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 **Secure Hub**, only iOS and Android devices receive the notifications, which appear in the device’s notification tray.
   - If you choose **SMTP**, most users should receive the message because they will have enrolled with their email addresses.
   - If you choose **SMS**, only users using devices with a SIM card receive the notification.

**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 are using 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 contains a pre-built macro for all but Ad Hoc notifications to ensure that notifications are sent to the correct SMTP recipient address. Citrix recommends that you do not modify macros in templates. You can also add recipients (for example, the corporate administrator), in addition to the user by adding their addresses separated by a semi-colon (;). To send Ad Hoc notifications, you can enter specific recipients on this page, 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](#).

**SMS:**

• **Activate:** Click to enable the notification channel.

  You can activate the SMTP notification only after you set up the SMTP server.

• **Recipient:** This field contains a pre-built macro for all but Ad Hoc notifications to ensure that notifications are sent to the correct SMS recipient address. Citrix recommends that you do not modify macros in templates. To send Ad Hoc notifications, you can enter specific recipients, or you can select devices from the **Manage > Devices** page.

• **Message:** Type the message to be sent to the user. This field is required. You can use HTML and macros to draft the message. For information about using macros in a message, see [Macros](#). See the following for an example of using HTML. The `<!DOCTYPE html>` tag is case sensitive.

```html
1   <!DOCTYPE html>
2   <TITLE>Your Title Here</TITLE>
3   <BODY>
4   <HR>
5   6   <HR>
```
4. Click Add. When all channels are correctly configured, they appear in this order on the Notification Templates page: SMTP, SMS, and 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 where you can make changes to all but the Type field, as well as activate or deactivate channels.

2. Click Save.

**Delete a notification template**

You can delete only notification templates that you have added. You cannot 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

November 7, 2019

Each predefined role-based access control (RBAC) role has certain associated access and feature permissions. This article describes what each of those permissions does. For a full list of default permissions for each built-in role, download [Role-Based Access Control Defaults](#).

When you **apply permissions**, you are defining the user groups the RBAC role has the permission to manage. The default administrator cannot change the applied permission settings. By default, the applied permissions apply to all user groups.

When you make an **assignment**, you are assigning the RBAC role to a group, so that the group of users owns the RBAC administrator rights.

### Admin Role

Users with the predefined Admin role have access or do not have access to the following features in Endpoint Management. By default, **Authorized access** (except Self-Help Portal), **Console features**, and **Apply permissions** are enabled.

### Authorized access for administrators

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin console access</td>
<td>Administrators have access to all features on the Endpoint Management console.</td>
</tr>
<tr>
<td>Self-Help Portal access</td>
<td>By default, administrators do not have Self-Help Portal access.</td>
</tr>
<tr>
<td>Shared devices enroller</td>
<td>By default, administrators do not have Shared devices enroller access. This feature is intended for users who require permission to enroll shared devices.</td>
</tr>
<tr>
<td>Remote Support access</td>
<td>Administrators have access to the Remote Support feature.</td>
</tr>
</tbody>
</table>
Public API access

Administrators have access to the public API to perform actions programmatically that are available on the Endpoint Management console. The actions include administering certificates, apps, devices, delivery groups, and local users.

COSU devices enroller

By default, administrators do not have access to enroll Android Enterprise dedicated devices, which are also known as COSU devices, to your Endpoint Management deployment. This feature is intended for users who require permission to enroll dedicated (COSU) devices.

Console features for administrators

Administrators have unrestricted access to the Endpoint Management console.

Dashboard

The Dashboard is the first page that administrators see after logging on to the 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 Endpoint Management.

### Policies

The Configure > Device Policies page is where you manage device policies, such as VPN and WiFi.

### App

The Configure > Apps page is where you manage the various apps that users can install on their devices.

### Media

The Configure > Media page is where you manage the various media that users can install on their devices.

### Smart 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 configure enrollment profiles (modes) to allow users to 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.

### Support

The Troubleshooting and Support page is where you perform 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.
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Wipe device</td>
<td>Erase all data and apps from a device, including memory cards if the device has one.</td>
</tr>
<tr>
<td>Clear Restriction</td>
<td>Remove one or more device restrictions.</td>
</tr>
<tr>
<td>Selective Wipe device</td>
<td>Erase all corporate data and apps from a device, leaving personal data and apps in place.</td>
</tr>
<tr>
<td>View locations</td>
<td>See the location of and set geographic restrictions on a device. Includes: Locate device, Track device.</td>
</tr>
<tr>
<td>Lock device</td>
<td>Remotely lock a device so that users cannot use the device.</td>
</tr>
<tr>
<td>Unlock device</td>
<td>Remotely unlock a device so that users can use the device.</td>
</tr>
<tr>
<td>Lock container</td>
<td>Remotely lock the corporate container on a device.</td>
</tr>
<tr>
<td>Unlock container</td>
<td>Remotely unlock the corporate container on a device.</td>
</tr>
<tr>
<td>Reset container password</td>
<td>Reset the corporate container password.</td>
</tr>
<tr>
<td>Enable ASM DEP/Bypass activation lock</td>
<td>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.</td>
</tr>
<tr>
<td>Get Resident Users</td>
<td>List the users that have active accounts on the current device. This action forces a sync between the device and the Endpoint Management console.</td>
</tr>
<tr>
<td>Logout Resident User</td>
<td>Force a log out of the current user.</td>
</tr>
<tr>
<td>Delete Resident User</td>
<td>Delete the current session for a specific user. The user can sign in again.</td>
</tr>
<tr>
<td>Rings the device</td>
<td>Remotely ring a Windows device at full volume for 5 minutes.</td>
</tr>
<tr>
<td>Reboot the device</td>
<td>Restart Windows devices from the Endpoint Management console.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Deploy to device</td>
<td>Send apps, notifications, restrictions, and other resources to a device.</td>
</tr>
<tr>
<td>Edit device</td>
<td>Change settings on the device.</td>
</tr>
<tr>
<td>Notification to device</td>
<td>Send a notification to a device.</td>
</tr>
<tr>
<td>Add/Delete device</td>
<td>Add or remove devices from Endpoint Management.</td>
</tr>
<tr>
<td>Devices import</td>
<td>Import a group of devices from a file into Endpoint Management.</td>
</tr>
<tr>
<td>Export device table</td>
<td>Collect device information from the Device page and export it to a .csv file.</td>
</tr>
<tr>
<td>Revoke device</td>
<td>Prohibit a device from connecting to Endpoint Management.</td>
</tr>
<tr>
<td>App lock</td>
<td>Deny access to all apps on a device. On Android, this restriction prevents</td>
</tr>
<tr>
<td></td>
<td>users from signing in to Endpoint Management. On iOS, users can sign in, but</td>
</tr>
<tr>
<td></td>
<td>they can't access apps.</td>
</tr>
<tr>
<td>App wipe</td>
<td>On Android, this restriction deletes the user’s Endpoint Management account.</td>
</tr>
<tr>
<td></td>
<td>On iOS, this restriction deletes the encryption key required for users to</td>
</tr>
<tr>
<td></td>
<td>access Endpoint Management features.</td>
</tr>
<tr>
<td>View software inventory</td>
<td>See what software is installed on a device.</td>
</tr>
<tr>
<td>Request AirPlay mirroring</td>
<td>Request to start AirPlay streaming.</td>
</tr>
<tr>
<td>Stop AirPlay mirroring</td>
<td>Stop AirPlay streaming.</td>
</tr>
<tr>
<td>Enable lost mode</td>
<td>On the Manage &gt; Devices page, you can put a supervised device in lost mode</td>
</tr>
<tr>
<td></td>
<td>to block a supervised device on the lock screen. You can then locate the</td>
</tr>
<tr>
<td></td>
<td>device when the device is lost or stolen.</td>
</tr>
<tr>
<td>Disable lost mode</td>
<td>On the Manage &gt; Devices page, you can disable lost mode for a device that</td>
</tr>
<tr>
<td></td>
<td>is set to lost mode.</td>
</tr>
<tr>
<td>OS Update device</td>
<td>You can deploy an OS Update device policy to devices.</td>
</tr>
</tbody>
</table>
Shut down device
Shut down iOS devices from the Endpoint Management console.

Restart device
Restart iOS devices from the 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 Endpoint Management.

Add Local Users
Delete Local Users
Edit Local Users
Import Local Users
Export Local Users
Local User Groups

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

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/Delete policy</td>
<td>Add or remove a device or app policy.</td>
</tr>
<tr>
<td>Edit policy</td>
<td>Change a device or app policy.</td>
</tr>
<tr>
<td>Upload Policy</td>
<td>Upload a device or app policy.</td>
</tr>
<tr>
<td>Clone Policy</td>
<td>Copy a device or app policy.</td>
</tr>
<tr>
<td>Disable Policy</td>
<td>Disable an existing app policy.</td>
</tr>
<tr>
<td>Export Policy</td>
<td>Collect device policy information from the Device Policies page and export it to a .csv file.</td>
</tr>
<tr>
<td>Assign Policy</td>
<td>Assign a device policy to one or more delivery groups.</td>
</tr>
</tbody>
</table>

## App

Administrators manage apps on the **Configure > Apps** page in Endpoint Management.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/Delete app store or enterprise app</td>
<td>Add or remove a public app store app or an app not wrapped with MDX.</td>
</tr>
<tr>
<td>Edit app store or enterprise app</td>
<td>Edit a public app store app or an app not wrapped with MDX.</td>
</tr>
<tr>
<td>Add/Delete MDX, Web, and SaaS app</td>
<td>Add or remove apps. A Web app is an app from your internal network. A SaaS apps is an app from a public network (SaaS).</td>
</tr>
<tr>
<td>Edit MDX, Web, and SaaS app</td>
<td>Edit apps.</td>
</tr>
<tr>
<td>Add/Delete category</td>
<td>Add or delete a category in which apps can appear in the app store.</td>
</tr>
<tr>
<td>Assign public/enterprise app to delivery group</td>
<td>Assign a public app store app or an app not wrapped with MDX to a delivery group for deployment.</td>
</tr>
<tr>
<td>Assign MDX/WebLink/SaaS app to delivery group</td>
<td>Assign apps to a delivery group for deployment to user devices. A WebLink app is an app that does not require single sign-on.</td>
</tr>
</tbody>
</table>
Citrix Endpoint Management

Export app table
Collect app information from the App page and export it to a .csv file.

**Media**
Manage media obtained from a public app store or through a volume purchase license.

<table>
<thead>
<tr>
<th>Add/Delete app store or enterprise books</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign public/enterprise books to delivery group</td>
</tr>
<tr>
<td>Edit app store or enterprise books</td>
</tr>
</tbody>
</table>

**Smart action**

<table>
<thead>
<tr>
<th>Add/delete smart action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or remove an action that is defined by a trigger (event, device or user property, or installed app name) and associated response.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Edit smart action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change an action that is defined by a trigger (event, device or user property, or installed app name) and associated response.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assign smart action to delivery group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign an action to a delivery group for deployment to user devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Export smart action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect action information from the Actions page and export it to a .csv file.</td>
</tr>
</tbody>
</table>

**Delivery group**
Administrators manage delivery groups from the Configure > Delivery Groups page.
## Citrix Endpoint Management

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/delete delivery group</td>
<td>Create or remove a delivery group, which adds specified users and optional policies, apps, and actions.</td>
</tr>
<tr>
<td>Edit delivery group</td>
<td>Change an existing delivery group, which modifies users and optional policies, apps, and actions.</td>
</tr>
<tr>
<td>Deploy delivery group</td>
<td>Make delivery group available for use.</td>
</tr>
<tr>
<td>Export delivery group</td>
<td>Collect delivery group information from the Delivery group page and export it to a .csv file.</td>
</tr>
</tbody>
</table>

## Enrollment profile

Manage enrollment profiles.

- 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.
<table>
<thead>
<tr>
<th>RBAC</th>
<th>RBAC Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Administer one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.</td>
</tr>
<tr>
<td>Enrollment</td>
<td>Enable enrollment modes for users and the Self-Help Portal.</td>
</tr>
<tr>
<td>Release Management</td>
<td>View the current installed release. Includes: Release Management Update</td>
</tr>
<tr>
<td>Certificates</td>
<td>Edit APNS certificate</td>
</tr>
<tr>
<td>Notification Templates</td>
<td>Create notification templates to use in automated actions, enrollment, and standard notification message delivery to users.</td>
</tr>
<tr>
<td>Workflows</td>
<td>Manage the creation, approval, and removal of user accounts for use with app configurations.</td>
</tr>
<tr>
<td>Credential Providers</td>
<td>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.</td>
</tr>
<tr>
<td>PKI Entities</td>
<td>Manage public key infrastructure entities (generic, Microsoft Certificate Services, or discretionary CA).</td>
</tr>
<tr>
<td>Test PKI Connection</td>
<td>Use the Test Connection button on the Settings &gt; PKI Entities page to ensure that the server is accessible.</td>
</tr>
<tr>
<td>Client Properties</td>
<td>Manage various properties on user devices, such as passcode type, strength, and expiration.</td>
</tr>
<tr>
<td>Client Support</td>
<td>Set the ways in which users can contact your support services (email, phone, or support ticket email).</td>
</tr>
<tr>
<td>Client Branding</td>
<td>Create a custom store name and default store views for the app store. Add a custom logo that appears in the app store or Secure Hub.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Carrier SMS Gateway</td>
<td>Set up carrier SMS gateways to configure notifications that Endpoint Management sends through carrier SMS gateways.</td>
</tr>
<tr>
<td>Notification Server</td>
<td>Set up an SMTP gateway server to send email to users.</td>
</tr>
<tr>
<td>ActiveSync Gateway</td>
<td>Manage user access to users and devices through rules and properties.</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Configure Endpoint Management to communicate with your G Suite account.</td>
</tr>
<tr>
<td>Apple Deployment Program</td>
<td>Add an Apple Deployment Program account to Endpoint Management.</td>
</tr>
<tr>
<td>Apple Configurator Device Enrollment</td>
<td>Configure Apple Configurator settings in Endpoint Management.</td>
</tr>
<tr>
<td>iOS/volume purchase Settings</td>
<td>Add Apple volume purchase accounts.</td>
</tr>
<tr>
<td>Mobile Service Provider</td>
<td>Use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and to issue operations.</td>
</tr>
<tr>
<td>NetScaler Gateway</td>
<td>Configure NetScaler Gateway (now renamed Citrix Gateway) settings in Endpoint Management.</td>
</tr>
<tr>
<td>Network Access Control</td>
<td>Set the conditions that determine a device is non-compliant and therefore denied access to the network.</td>
</tr>
<tr>
<td>Samsung Knox</td>
<td>Enable or disable Endpoint Management to query Samsung Knox attestation server REST APIs.</td>
</tr>
<tr>
<td>Server Properties</td>
<td>Add or modify server properties. Requires restarting Endpoint Management on all nodes.</td>
</tr>
<tr>
<td>Virtual Apps and Desktops</td>
<td>Allow users to add Citrix Virtual Apps and Desktops through Citrix Workspace.</td>
</tr>
</tbody>
</table>
Citrix Endpoint Management

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Citrix Files</strong></td>
<td>When using Endpoint Management with Enterprise accounts: Configure settings to connect to the Content Collaboration and administrator service accounts for user account management. Requires existing Citrix Files domain and administrator credentials. When using Endpoint Management with storage zone connectors: Configure Endpoint Management to point to network shares and SharePoint locations defined in storage zone connectors.</td>
</tr>
<tr>
<td><strong>Android Enterprise</strong></td>
<td>Configure Android Enterprise server settings.</td>
</tr>
<tr>
<td><strong>Identity Provider (IdP)</strong></td>
<td>Configure an identity provider.</td>
</tr>
<tr>
<td><strong>Derived Credentials</strong></td>
<td>Configure derived credentials for iOS device enrollment.</td>
</tr>
<tr>
<td><strong>Microsoft Store for Business</strong></td>
<td>Configure Microsoft Store for Business settings in Endpoint Management.</td>
</tr>
<tr>
<td><strong>Endpoint Management Tools</strong></td>
<td>Access Endpoint Management Tools page.</td>
</tr>
<tr>
<td><strong>Windows Bulk Enrollment</strong></td>
<td>Configure Windows bulk enrollment settings.</td>
</tr>
</tbody>
</table>

**Support**

Administrators can perform various support tasks.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NetScaler Gateway Connectivity Checks</strong></td>
<td>Perform various connectivity checks for NetScaler Gateway by IP address. Requires a user name and password.</td>
</tr>
<tr>
<td><strong>Endpoint Management Connectivity Checks</strong></td>
<td>Perform connectivity checks for selected Endpoint Management features, such as database, DNS, and Google Plan.</td>
</tr>
<tr>
<td><strong>Citrix Product Documentation</strong></td>
<td>Access the public Citrix Endpoint Management documentation site.</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Citrix Endpoint Management

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Knowledge Center</td>
<td>Access the Citrix Support site to search for knowledge base articles.</td>
</tr>
<tr>
<td>Logs</td>
<td>View and download log files.</td>
</tr>
<tr>
<td>Macros</td>
<td>Populate user or device property data within 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.</td>
</tr>
<tr>
<td>PKI Configuration</td>
<td>Import and export PKI configuration information.</td>
</tr>
<tr>
<td>APNS Signing Utility</td>
<td>Submit a request for Apple Push Network signing (APNs) certificates, or upload Secure Mail APNs certificate for iOS.</td>
</tr>
<tr>
<td>Citrix Insight Services</td>
<td>Upload logs to Citrix Insight Services (CIS) for assistance with various issues.</td>
</tr>
<tr>
<td>Device Citrix Gateway connector for Exchange ActiveSync Status</td>
<td>Query Endpoint Management for the status of a device as sent to the connector for Exchange ActiveSync based on the device ActiveSync ID.</td>
</tr>
</tbody>
</table>

Restrict Group Access

Admin users can apply permissions to all user groups.

Device Provisioning Role

Important:
The Device Provisioning Role applies only to Windows CE devices.

Users with the predefined Device Provisioning role have limited access to console features. By default, their permission is set to all user groups and they cannot change this setting.

Console features for device provisioning

Device provisioning users have the following restricted access to the Endpoint Management console. By default, each of the following features is enabled.
Device restrictions

<table>
<thead>
<tr>
<th>Edit device</th>
<th>Change settings on the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/Delete device</td>
<td>Add or remove devices from Endpoint Management.</td>
</tr>
</tbody>
</table>

Settings for device provisioning

Device provisioning users can access the Settings page, but do not have the rights to configure the features.

User Role

Users with the User role have the following limited access to Endpoint Management.

Authorized access for users

| Self-Help Portal   | Provide users access only to the Self-Help Portal in Endpoint Management. |

Console features for users

Users have the following restricted access to the Endpoint Management console.

Device restricted access for users

<table>
<thead>
<tr>
<th>Full Wipe device</th>
<th>Erase all data and apps from a device, including memory cards if the device has one.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selective Wipe device</td>
<td>Erase all corporate data and apps from a device, leaving personal data and apps in place.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>View locations</td>
<td>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</td>
</tr>
<tr>
<td>Lock device</td>
<td>Remotely lock a device so that it cannot be used.</td>
</tr>
<tr>
<td>Unlock device</td>
<td>Remotely unlock a device so that it can be used.</td>
</tr>
<tr>
<td>Lock container</td>
<td>Remotely lock the corporate container on a device.</td>
</tr>
<tr>
<td>Unlock container</td>
<td>Remotely unlock the corporate container on a device.</td>
</tr>
<tr>
<td>Reset container password</td>
<td>Reset the corporate container password.</td>
</tr>
<tr>
<td>Enable ASM DEP/Bypass activation lock</td>
<td>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.</td>
</tr>
<tr>
<td>Get Resident Users</td>
<td>List the users that have active accounts on the current device. This action forces a sync between the device and the Endpoint Management console.</td>
</tr>
<tr>
<td>Logout Resident User</td>
<td>Force a log out of the current user.</td>
</tr>
<tr>
<td>Delete Resident User</td>
<td>Delete the current session for a specific user. The user can sign in again.</td>
</tr>
<tr>
<td>Rings the device</td>
<td>Remotely ring a Windows device at full volume for 5 minutes.</td>
</tr>
<tr>
<td>Reboot the device</td>
<td>Restart a Windows device.</td>
</tr>
<tr>
<td>App lock</td>
<td>Deny access to all apps on a device. On Android, users can’t sign in to Endpoint Management. On iOS, users can sign in, but they can’t access apps.</td>
</tr>
</tbody>
</table>
Table: App Wipe and View Software Inventory

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>App wipe</td>
<td>On Android, this restriction deletes the user’s Endpoint Management account. On iOS, this restriction deletes the encryption key required for users to access Endpoint Management features.</td>
</tr>
<tr>
<td>View software inventory</td>
<td>See what software is installed on a device.</td>
</tr>
</tbody>
</table>

**Enrollment restrictions for users**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/Delete enrollment</td>
<td>Add or remove an enrollment invitation to a user or a group of users.</td>
</tr>
<tr>
<td>Notify user</td>
<td>Send and enrollment invitation to a user or group of users.</td>
</tr>
</tbody>
</table>

**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 cannot edit the role.

**To use the RBAC feature**

The Role-Based Access Control (RBAC) feature in 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.

Endpoint Management implements the following default user roles to logically separate access to system functions:

- **Administrator**: Grants full system access.
- **Device Provisioning**: Grants access to basic device administration for Windows CE devices.
- **User**: Used by users who can enroll devices and access the Self-Help Portal.

You can also use the default roles as templates that you customize to create user roles. You can assign to those user roles permissions to access additional system functions.
Citrix Endpoint Management

You can assign roles to local users (at the user level) or to Active Directory groups (all users in that group have the same permissions). If a user belongs to several Active Directory groups, all the permissions merge together to define the permissions for that user. For example, if ADGroupA users can locate manager devices, and ADGroupB users can wipe employee devices: A user who belongs to both groups can locate and wipe devices of managers and employees.

Note:
Local users may have only one role assigned to them.

You can use the RBAC feature in Endpoint Management to do the following:

• Create a role.
• Add groups to a role.
• Associate local users to roles.

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The Settings page appears.

2. Click Role-Based Access Control. The Role-Based Access Control page appears, which displays the default user roles, plus any roles you have previously added.

If you click the plus sign (+) next to a role, the role expands to show all the permissions for that role.

3. Click Add to add a user role. Click the pen icon to the right of an existing role to edit the role. Or, Click the trash can icon to the right of a role that you defined to delete the role. You cannot delete the default user roles.

   • When you click Add or the pen icon, the Add Role or the Edit Role page appears.
   • When you click the trash can icon, a confirmation dialog appears. Click Delete to remove the selected role.

4. Enter the following information to create a user role or to edit a user role:

   • RBAC name: Enter a descriptive name for the new user role. You cannot change the name of an existing role.
   • RBAC template: Optionally, click a template as the starting point for the new role. When editing an existing role, you cannot select a template.
RBAC templates are the default user roles. They define the access to system functions that users associated with that role have. After you select an RBAC template, you can see all of the permissions associated with that role in the **Authorized Access** and **Console Features** fields. Using a template is optional; you can directly select the options you want to assign to a role in the **Authorized Access** and **Console Features** fields.

5. Click **Apply** to the right of the **RBAC template** field to populate the **Authorized access** and **Console features** check boxes. Endpoint Management fills those fields with the pre-defined access and feature permissions for the selected template.

6. Select and clear the check boxes in **Authorized access** and **Console features** to customize the role.

   If you click the triangle next to a Console feature, permissions specific to that feature appear that you can select and clear. Clicking the top-level check box prohibits access to that console part. Select individual options below the top level to enable those options.

7. **Apply permissions**: Select one or more user groups to limit which groups the administrator can manage. If you click **To specific user groups**, a list of groups appears from which you can select one or more groups.

   For example, if an RBAC administrator has permissions to the ActiveDirectory and MSP user groups:
   
   - The administrator can access information only for users who are in the ActiveDirectory group, the MSP group, or both of those groups.
   
   - 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

8. Click **Next**. The **Assignment** page appears.

9. Enter the following information to assign the role to user groups.

- **Select domain**: In the list, click a domain.

- **Include user groups**: Click **Search** to see a list of all available groups. Or, type a full or partial group name to limit the list to only groups with that name.

- In the list that appears, select the user groups to which you want to assign the role. When you select a user group, the group appears in the **Selected user groups** list.
Citrix Endpoint Management

Note:
To remove a user group from the Selected user groups list, click the X next to the user group name.

10. Click Save.

Device management

December 2, 2019

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 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 identities to use to authenticate to devices. Configure how to keep enterprise and personal data separate on devices.

- Deliver any app to end users, regardless of device or operating system. Protect your information at the app level and ensure enterprise-grade mobile application management.

- Use provisioning and configuration controls to set up devices. Those controls include device enrollment, policy application, and access privileges.
Citrix Endpoint Management

- 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 perform general device management tasks.

**Device management workflows**

The workflow diagrams in this section provide a suggested sequence for performing 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.

   ![Recommended before adding devices and apps](image)

   - Add users & groups
   - Add delivery groups
   - Assign roles to users & groups (optional)
   - Prepare notification templates
   - Add workflows for app approvals (optional)

   See:
   - Deploy resources
   - Configure roles with RBAC
   - Create and update notification templates
   - Create and manage workflows

2. **Add devices:**
Citrix Endpoint Management

Add devices

- Upload provisioning file
- Configure device policies
- Deploy policies to delivery groups
- Configure client settings (optional)
- Create automated actions (optional)

See:

Prepare to enroll devices and deliver resources
Device policies
To deploy to delivery groups
Automated actions

3. **Prepare enrollment invitations:** Perform these tasks if you plan to use enrollment invitations.

Prepare enrollment invitations

- Check enrollment modes for invitations
- Send enrollment invitations

See:

Configure enrollment modes
Send a notification to devices

4. **Add apps:**
See:
- MDX Service
- Add apps
- Create app categories
- Create and manage workflows
- To deploy to delivery groups

5. **Perform ongoing device and app management:** In addition to using the Endpoint Management dashboard, we encourage you to review the What’s new content for each release. What’s new provides information about any needed actions, such as configuring new device policies.
Enrollment invitations

To manage user devices remotely and securely, you enroll user devices in Endpoint Management. The Endpoint Management client software is installed on the user device and the user identity is authenticated. Then, Endpoint Management and the user profile are installed. For enrollment details for supported device platforms, see the device articles under this section.

In the Endpoint Management console, you can send an enrollment invitation to users with iOS, macOS, and Android devices. You can also send an installation link to users with iOS or Android devices.

Enrollment invitations are sent as follows:

- If the enrollment invitation is for one local or Active Directory user: The user receives the invitation from SMS at the phone number and carrier name you specify.
- If the enrollment invitation is for a group: The users receive invitations from SMS. If Active Directory users have an email address and mobile phone number in Active Directory, they receive...
the invitation. Local users receive the invitation at the email and phone number specified in user properties.

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 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.
To send an enrollment installation link to a list of recipients over SMTP or SMS, 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.
   • **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**

1. Configure these User settings:
• **User name:** Type a user name. The user must exist in the Endpoint Management server as a local user or as a user in Active Directory. If the user is local, set the email property of the user so you can send that user notifications. If the user is in Active Directory, ensure that LDAP is configured.

• **Device info:** This setting doesn’t appear if you select multiple platforms or if you select only macOS. Choose **Serial number**, **UDID**, or **IMEI**. After you choose an option, a field appears where you can type the corresponding value for the device.

• **Phone number:** This setting doesn’t appear if you select multiple platforms or if you select only macOS. Optionally, type the phone number of the user.

• **Carrier:** This setting doesn’t appear if you select multiple platforms or if you select only macOS. Choose a carrier to associate to the phone number of the user.

• **Enrollment mode:** Choose how you want users to enroll. The default is **User name + Password**. Some of the following options aren’t available for all platforms:
  - User name + Password
  - High Security
  - Invitation URL
  - Invitation URL + PIN
  - Invitation URL + Password
  - Two Factor
  - User name + PIN

Only the enrollment modes that are valid for each of the selected platforms appear. 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 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 Mode and indicates when the enrollment expires. For more information about configuring enrollment modes, see **Configure enrollment modes**.

• **Maximum Attempts:** This field is set when you configure the Enrollment 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 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. Endpoint Management gets the user list from Active Directory. The list includes users whose names contain 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
  - High Security
  - Invitation URL
  - Invitation URL + PIN
  - Invitation URL + Password
- Two Factor
- User name + PIN

Only the enrollment modes that are valid for each of the selected platforms appear.

**Note:**
When you select any enrollment 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 Mode and indicates when the enrollment expires. For more information about configuring enrollment modes, see **Configure enrollment modes**.
- **Maximum Attempts:** This field is set when you configure the Enrollment 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.

To send an installation link

Before you can send an enrollment installation link, you must configure channels (SMTP or SMS) 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 containing 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 containing the listing and 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** or **SMS**. 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:
     - **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.”
• **SMS**: Configure this setting. If you do not type anything in this field, the default value specified in the notification template configured for the platform you selected is used:
  
  – **Message**: Type a message to be sent to the recipients. This field is required for SMS-based notification.

  In North America, SMS messages that exceed 160 characters are delivered in multiple messages.

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.

### Device enrollment limit

Endpoint Management includes a default enrollment profile that allows users to enroll an unlimited number of devices. The default profile is named Global. Create enrollment profiles only if you want to limit the number of devices that users can enroll. You associate enrollment profiles with delivery groups.

The device enrollment limit is available for iOS and Android devices only.

When your Endpoint Management deployment includes dedicated Android Enterprise device (also known as COSU devices), a single Endpoint Management administrator or small group of administrators enroll many devices. To ensure that these administrators can enroll all the devices required, create an enrollment profile for them with unlimited devices allowed per user. For details, see Add a dedicated (COSU) enrollment profile in the Android Enterprise article.

1. Go to **Configure > Enrollment Profiles**. The default Global profile appears.

   ![Enrollment Profiles](image)

2. To add an enrollment profile, click **Add**. In the **Enrollment Info** page, type a name for the enrollment profile and then select the number of devices that members with this profile can enroll.
3. Click Next. The Delivery Group Assignment screen appears.

4. Select the delivery groups for this enrollment profile and then click Save.

The Delivery Groups page appears.

To change the enrollment profiles associated with a delivery group, go to Configure > Delivery Groups and then click Enrollment Profiles.
User experience with a device enrollment limit

When you set the device enrollment limit and users try to enroll a new device, they follow these steps:

1. Sign on to Secure Hub.
2. Enter a server address to enroll.
3. Enter the credentials.
4. If the device limit is reached, an error message informs the user that they have exceeded the device registration limit.

You have exceeded the number of devices that your organization allows you to enroll. Please delete your account in any other device in order to continue.

The Secure Hub enrollment screen appears again.
Security actions

You perform 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 Endpoint Management. On iOS, users can sign in, but they can’t access apps.

- **App wipe**: On Android, an app wipe deletes the user account from Endpoint Management. On iOS, deletes a user account in Secure Hub.

- **ASM Deployment Program Activation Lock**: Creates an Activation Lock bypass code for iOS devices enrolled in Apple School Manager.

- **Certificate renewal**: For supported iOS, macOS, and Android devices, the Certificate Renewal security action initiates certificate renewal. The next time that devices connect back to Endpoint Management, the Endpoint Management server issues new device certificates based on the new CA.

- **Clear restrictions**: On supervised iOS devices, this command allows 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 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 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**.

- **Full wipe**: Immediately erases all data and apps from a device, including from any memory cards.
  - For Android devices, this request can also include the option to wipe memory cards.
  - For iOS, macOS, and tvOS devices, the wipe occurs immediately, even if the device is locked.

  For iOS 11 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 can prevent iOS devices from performing 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 disallow proximity setup on devices that are Endpoint Management managed and have been wiped.
For Windows Phone devices, a full wipe removes all Endpoint Management information and all user data. The user data removed includes personal content such as apps, emails, contacts, and media.

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. 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, this command succeeds only if the devices are in MDM Lost Mode. Locate is a one time action, as opposed to the continuous tracking of Enable tracking. Secure Hub reports its location periodically when it is running.

- **Lock:** Remotely locks a device, which is useful when you lose a device and don’t know if the device is stolen. 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 Endpoint Management console.

- **Lock and Reset Password:** Remotely locks a device and resets the passcode.
  - Not supported for devices enrolled in Android Enterprise in work profile mode that are running Android versions prior to Android 7.0.
  - On devices enrolled in Android Enterprise in work profile mode that are running Android 7.0 or greater:
    * The passcode sent locks the work profile. The device is not locked.
    * If no passcode is sent, or the passcode sent doesn’t meet passcode requirements, and no passcode is already set on the work profile: The device is locked.
    * If no passcode is sent, or the passcode sent doesn’t meet passcode requirements, but a passcode is already set on the work profile: The work profile is locked but device is not locked.

- **Notify (Ring):** Plays a sound on Android devices.

- **Reboot:** Restarts Windows 10 devices. For Windows Tablet and PCs, the message “System will reboot soon” appears and then the reboot occurs in five minutes. For Windows Phone, the reboot occurs after a few minutes, with no warning message to users.

- **Request/Stop AirPlay Mirroring:** Starts and stops AirPlay mirroring on supervised iOS devices.

- **Restart/Shut Down:** Immediately restarts or shuts down supervised devices. tvOS supports Restart but not Shut Down.

- **Revoke:** Prohibits a device from connecting to Endpoint Management.
• **Revoke/Authorize (iOS, macOS, tvOS):** 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.

• **Selective wipe:** Erases all corporate data and apps from a device, leaving personal data and apps in place. After a selective wipe, a user can reenroll the device.
  - 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.
  - If the Samsung Knox API is enabled, selectively wiping the device also removes the Samsung Knox container.
  - 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.
  - Selectively wiping a Windows Phone device removes the enterprise token that allows Endpoint Management to install apps on the device. The wipe also removes all Endpoint Management certificates and configurations deployed to the device. You can’t reenroll a selectively wiped Windows Phone device.
  - Selectively wiping an Android device also revokes the device. You can reenroll the device only after reauthorizing it or deleting it from the console.

• **Unlock:** Clears the passcode sent to the device when it was locked. This command doesn’t unlock 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 Endpoint Management console**

**Important:**

When you remove a device from the Endpoint Management console, managed apps and data remain 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 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 Endpoint Management console.

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.

**Get information about devices**

The Endpoint Management database stores a list of mobile devices. A unique serial number or International Mobile Station Equipment Identity (IMEI)/Mobile Equipment Identifier (MEID) uniquely defines each mobile device. To populate the 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 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.
Citrix Endpoint Management

You can add devices manually, import devices from a device provisioning file, edit device details, perform 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 device attributes. If you apply filters, 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.

**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, elect 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.
3. Configure these settings:

- **Templates**: In the list, click the type of notification you want to send. 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** and **SMS**. Click the tabs to see the message format for each channel.
- **Sender**: Enter an optional sender.
- **Subject**: Enter a subject for an **Ad Hoc** message.
- **Message**: Enter the message for an **Ad Hoc** message.

4. Click **Notify**.
Citrix Endpoint Management

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. 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 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 Endpoint Management console.
2. Add the property named Owned by and choose either Corporate or BYOD (employee-owned).

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
• User Name

You can configure the search scope through a server property, \texttt{include.device.properties.during.search}, which defaults to \texttt{false}. To include all device properties in a device search, go to \texttt{Settings > Server Properties} and change the setting to \texttt{true}.

\section*{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. 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 and use to import devices to Endpoint Management must be in the following format:

\texttt{SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1; propertyName2;propertyValue2; \ldots propertyNameN;propertyValueN}

Keep in mind the following:

- For valid values for each property, see the PDF \texttt{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 contains a semi-colon, escape it with a backslash character (\).

For example, for this property:

\texttt{propertyV;test;1;2}

Escape it as follows:

\texttt{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 \texttt{OperatingSystemFamily} are \texttt{WINDOWS}, \texttt{ANDROID}, or \texttt{iOS}.

Example of a device provisioning file:
Each line in the file describes a device. The first entry in that sample means the following:

- **SerialNumber**: `1050BF3F517301081610065510590391`
- **IMEI**: `15244201625379901`
- **OperatingSystemFamily**: `WINDOWS`
- **PropertyName**: `propertyN`
- **PropertyValue**: `propertyV\test\1\2;prop 2`

### Shared devices

Endpoint Management lets you configure devices that multiple users can share. The shared devices feature lets, for example, clinicians in hospitals use any nearby device to access apps and data rather than having to carry around a specific device. You might also want shift workers in fields like law enforcement, retail, and manufacturing to share devices to reduce equipment costs.

### Key points about shared devices

You can use any of the supported iOS and Android devices as shared devices. For a list of supported devices, see [Supported device operating systems](#).

### MDM mode

- Available on both iOS and Android tablets and phones. Basic Apple Deployment Program enrollment is not supported for an Endpoint Management Enterprise shared device. Use an authorized Apple Deployment Program to enroll a shared device in this mode.
- Authentication types not supported: Client certificate authentication, Citrix PIN, Touch ID, User Entropy, and two-factor authentication.

### MDM+MAM mode

- Available only on iOS and Android tablets.
- Only Active Directory user name and password authentication is supported.
• Client certificate authentication, passcode for Secure Hub, Touch ID, User Entropy, and two-factor authentication are not supported.
• MAM-only mode is not supported. The devices must enroll in MDM.
• Only Secure Mail, Secure Web, and the Citrix Files mobile app are supported. HDX apps are not supported.
• Active Directory users are the only supported users. Local users and groups are not supported.
• Re-enrollment is required for existing MDM-only shared devices to update to MDM+MAM mode.
• Users cannot share native apps on the devices.
• Once downloaded during first-time enrollment, Citrix mobile productivity apps are not downloaded again each time a new user signs on to the device. The new user can pick up the device, sign on, and get going.
• On Android, to isolate each user’s data for security purposes, enable the Disallow rooted devices policy in the Endpoint Management console.

Prerequisites for enrolling shared devices

Before you can enroll shared devices, you must do the following:

• Create a shared device enrollment user role. See Configure roles with RBAC.
• Create a shared device user. See Add, edit, or delete local user accounts.
• Create a delivery group that contains the base policies, apps, and actions that you want to be applied to the shared device enrollment user. See Deploy resources.

Prerequisites for MDM+MAM mode

1. Create an Active Directory group named something like Shared Device Enrollers.
2. Add to this group the Active Directory users who you want to enroll shared devices. If you want a new account for this purpose, create a new Active Directory user (for example, sdenroll) and add that user to the Active Directory group.

Configuring a shared device

Follow these steps to configure a shared device.

1. From the Endpoint Management console, click the gear in the upper-right corner. The Settings page appears.
2. Click Role-Based Access Control, then click Add. The Add Role screen appears.
3. Create a shared-device enrollment user role named Shared Device Enrollment User with Shared devices enroller permissions under Authorized Access. Be sure to expand Devices in
Console features and then select Selective Wipe device. This setting ensures that the apps and policies provisioned through the shared devices enroller account are deleted through Secure Hub, when the device is unenrolled.

For Apply Permissions, keep the default setting, To all user groups, or assign permissions to specific Active Directory user groups with the To specific user groups.

Click Next to move to the Assignment screen. Assign the shared-device enrollment role you created to the Active Directory group you created for shared device enrollment users. In the following image, citrix.lab is the Active Directory domain and Shared Device Enrollers is the Active Directory group.

4. Create a delivery group that contains the base policies, apps, and actions that you want to apply to the device when a user is not signed on. Then, associate that delivery group with the shared device enrollment user Active Directory group.
5. Install Secure Hub on the shared device and enroll it in Endpoint Management using the shared device enrollment user account. You can now view and manage the device through the Endpoint Management console.

6. To apply different policies or to provide more apps for authenticated users, you must create a delivery group associated with those users and deployed to shared devices only. When creating the groups, configure deployment rules to ensure that the packages are deployed to shared devices. For more information, see Deploy Resources.

7. To stop sharing the device, perform a selective wipe to remove the shared device enrollment user account from the device. The selective wipe also removes any apps and policies deployed to the device.

**Shared device user experience**

**MDM mode**

Users see only the resources available to them, and they have the same experience on every shared device. The shared device enrollment policies and apps always remain on the device. When a user who isn’t enrolled in shared devices signs on to Secure Hub, that person’s policies and apps are deployed to the device. When that user signs off, the policies and apps that differ from those of the shared device enrollment are removed. The shared-device enrollment resources remain intact.

**MDM+MAM mode**

Secure Mail and Secure Web are deployed to the device when enrolled by the shared device enrollment user. User data is maintained securely on the device. The data is not exposed to other users when they sign on to Secure Mail or Secure Web.

Only one user at a time can sign on to Secure Hub. The previous user must sign off before the next user can sign on. For security reasons, Secure Hub does not store user credentials on shared devices,
so users must enter their credentials each time they sign on. To ensure that a new user cannot access resources intended for the previous user: Secure Hub does not allow new users to sign on while the policies, apps, and data associated with the previous user are being removed.

Shared device enrollment doesn’t change the process for upgrading apps. You can push upgrades to shared-device users as always, and shared-device users can upgrade apps right on their devices.

**Recommended Secure Mail policies**

- For the best Secure Mail performance, set **Max sync period** based on the number of users to share the device. Allowing unlimited sync is not recommended.

<table>
<thead>
<tr>
<th>Number of users sharing device</th>
<th>Recommended max sync period</th>
</tr>
</thead>
<tbody>
<tr>
<td>21–25</td>
<td>1 week or less</td>
</tr>
<tr>
<td>6–20</td>
<td>2 weeks or less</td>
</tr>
<tr>
<td>5 or fewer</td>
<td>1 month or less</td>
</tr>
</tbody>
</table>

- Block **Enable contact export** to avoid exposing a user’s contacts to other users who share the device.

- On iOS, only the following settings can be set per user. All other settings are common across users who share the device:
  - Notifications
  - Signature
  - Out of Office
  - Sync Mail Period
  - S/MIME
  - Check Spelling

**Alexa for Business**

August 28, 2019

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. Endpoint Management lets you configure and manage these devices in the Endpoint Management console. Endpoint Management doesn’t deploy policies directly to Alexa devices. Instead, Endpoint Management updates AWS services and AWS delivers the configurations to Alexa devices.
Authenticate your AWS account to Endpoint Management

1. To get your AWS account credentials, log in to the AWS console and select My Security Credentials from the user menu.

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.

5. Download the access key ID and secret access key. Save or make a note of them.
6. In the 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**.
Configure Alexa for Business on Endpoint Management

Endpoint Management lets you configure:

- Room profiles of settings that you apply to rooms containing Alexa devices
- Rooms that represent the physical rooms that contain 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 contain Alexa devices. You can add, edit, and delete room profiles.

1. In the 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:

- **Profile Name**: Type the name of the profile.
- **Address**: Type the physical (street) address of the building where the rooms containing 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.
Citrix Endpoint Management

- **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 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.

1. In the Endpoint Management console, select **Configure > Alexa for Business > Rooms**. The list of available rooms appears.

   ![Rooms Configuration](image)

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**.
9. Select the skill groups 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 Endpoint Management console, select **Configure > Alexa for Business > Skill Groups**. The list of available skill groups appears.

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**.
6. Select the skills you want to include in the skill group and click **Add**. The selected skills appear in the **Add skills** page.

7. To add the skill group to Alexa devices in rooms that you specify, click **Add**.
Select the rooms.

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 Endpoint Management console, select Configure > Alexa for Business > Skills. The list
of enabled skills appears.

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 adds more skills.

4. Select the skills you want to add to your organization.
5. Click **Save**.

**Remove skills from your organization**

1. In the Endpoint Management console, select **Configure > Alexa for Business > Skills**. The list of enabled skills appears.
2. Select the skills you want to remove from your organization.
3. Click **Disable**.
**Configure conferencing**

Conferencing features let you configure conferencing providers, like Google Hangout or Amazon Chime, that control how people join conferences in rooms that contain Alexa devices. You can add, edit, and delete conferencing providers. You can also set a default conferencing provider.

1. In the 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:
Citrix Endpoint Management

- **Conferencing provider**: Select a conferencing provider from the list.
- **Name**: Type the name 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 Endpoint Management console, select **Configure > Alexa for Business > Conferencing**. The list of available room profiles appears.
2. Select the conferencing provider you want to set as the default.
3. Click **Set Default**.
Migrate from device administration to Android Enterprise

August 19, 2019

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.

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.

That publication also describes the four phases of device administration migration and includes the following diagram. This article includes recommendations specific to Citrix Endpoint Management for the migration phases.

Diagram from the Android Enterprise Migration Bluebook. Republished with the permission of Google.
Impact of device administration deprecation

Google will deprecate the following Device Administration APIs. These APIs won’t work on devices running Android Q after you upgrade Secure Hub to target the Android Q API level:

- 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.

The deprecated APIs have no impact on devices enrolled in Citrix MAM-only mode.

Recommendations

The following recommendations are for devices already enrolled in the Android legacy device administration mode, unenrolled devices, and devices enrolled in Citrix MAM-only mode.

<table>
<thead>
<tr>
<th>Device enrollment status</th>
<th>Recommended action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing device is enrolled in device administration mode and upgradeable to Android Q.</td>
<td>Before upgrading the device to Android Q, migrate from device administration mode to Android Enterprise.</td>
</tr>
<tr>
<td>Existing device is enrolled in device administration mode. The device can't upgrade to Android Q.</td>
<td>Device can remain in device administration mode. However, plan to move the device to Android Enterprise on device refresh.</td>
</tr>
<tr>
<td>Existing device is enrolled in device administration mode and is upgraded to Android Q.</td>
<td>Migrate from device administration mode to Android Enterprise before Google deprecates the APIs. A warning message for these devices appears in the Endpoint Management console.</td>
</tr>
<tr>
<td>New device delivered with Android Q and enrolled in device administration mode.</td>
<td>Migrate from device administration mode to Android Enterprise before Google deprecates the APIs. A warning message for these devices appears in the Endpoint Management console.</td>
</tr>
<tr>
<td>New device delivered with or upgradeable to Android Q. The device isn't enrolled.</td>
<td>Use Android Enterprise for any new devices.</td>
</tr>
</tbody>
</table>
New or existing device on Android Q gets enrolled in device administration mode after Google deprecates the APIs.

To avoid the impacts of deprecated Google APIs, Citrix recommends migrating to Android Enterprise before Google deprecates the APIs. After that date, enrollments of these devices will fail.

New or existing devices enrolled in Citrix MAM-only mode

No action needed. The deprecated Google APIs have no impact on devices in MAM-only mode.

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 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 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
Citrix Endpoint Management

- 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 G-Suite 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
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 Endpoint Management.
- Option 2: Publish the app from Endpoint Management as an enterprise app. Publish the APK in Endpoint Management and select the platform Android Enterprise for the MDX file.

**Citrix device policy migration**

For policies that are available for both the Android and Android Enterprise platforms: Edit the policy and select the platform Android Enterprise.
For Android Enterprise, consider the enrollment mode. Some policy options are available only for devices in work profile mode or fully managed mode.

**Proof of concept**

After you migrate 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 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.

**Deployment**

You can now deploy your Android Enterprise setup and prepare your users for migration.

**Recommended deployment strategy**

The Citrix recommended 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 due to loss or breakage.
Android Enterprise

December 17, 2019

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 Endpoint Management to manage company-owned Android devices 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 Android operating systems supported for Endpoint Management, see Supported device operating systems.

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.

When you integrate 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 Endpoint Management with Android Enterprise, the complete solution has these components:

- **Citrix Endpoint Management**: The Citrix EMM. Endpoint Management is the unified endpoint management for a secure digital workspace. Endpoint Management provides the means for IT administrators to manage devices and apps for their organizations.
- **Citrix Secure Hub**: The Citrix DPC app. Secure Hub is the launchpad for Endpoint Management. Secure Hub enforces policies on the device.
- **Managed Google Play**: A Google enterprise app platform that integrates with Endpoint Management. The Google Play EMM API sets app policies and distributes app.

This illustration shows how administrators interact with these components and how the components interact with each other:
Using managed Google Play with Endpoint Management

Note:
You can use either managed Google Play or G Suite to register Citrix as your EMM provider. This article discusses using Android Enterprise with managed Google Play. If your organization uses G Suite to provide access to app, you can use it with Android Enterprise. See Legacy Android Enterprise for G Suite customers.

When 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 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 is not 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 to manage separate sets of devices and apps.

For Endpoint Management administrators, managed Google Play combines the user experience and app store features of Google Play with a set of management capabilities 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.
Device deployment scenarios and modes of operation

Device deployment scenario refers to who owns the devices you deploy and how you manage them. Mode of operation refers to how the DPC manages and enforces policies on the device. The mode of operation supports the device deployment scenario.

Work profile: BYOD device deployment, profile owner mode

A BYOD deployment scenario allows employees to bring personally owned devices to work and use those devices to access company information and applications.

The profile owner mode of operation supports BYOD deployments. Through the DPC, the enterprise enables personal devices for work use by adding a work profile to the primary user account on the device. The work profile isolates business accounts, apps, and data from personal accounts, apps, and data. The work profile is associated with the primary user, but as a separate profile. As the profile owner, the DPC manages only the work profile on the device and has limited control outside of the work profile. For more details about work profiles, see the Google Android Enterprise help topic, What is a work profile?

Profile owner mode is enabled when the device is enrolled in Endpoint Management. Because the DPC manages only the work profile, not the whole device, devices enrolled in profile owner mode do not need to be new or factory reset.

A device in profile owner mode is also called a work profile device. Profile owner mode is also called work profile mode or managed profile mode.

Note:

Endpoint Management does not support Zebra devices as in profile owner mode. Endpoint Management supports Zebra devices as fully managed devices and in device legacy mode (also called device admin mode).

Fully managed: Company-owned device deployment, device owner mode

In a company-owned deployment scenario, the enterprise owns and fully controls the devices it uses. Typically, organizations deploy company-owned devices when they need to strictly monitor and manage the whole device.

The device owner mode of operation supports company-owned deployments. In device owner mode, the DPC manages the entire device. As the device owner, the DPC can perform device-wide actions, such as configure device-wide connectivity, configure global settings, and perform a factory reset.

A device in device owner mode is a fully managed device.
Device owner mode is enabled during the initial device setup. Only new or factory reset devices can be enrolled into Endpoint Management in device owner mode.

**Dedicated device: Company-owned device deployment, device owner mode**

A **dedicated device** is a type of fully managed device. Dedicated devices are company-owned devices running in device owner mode. Dedicated devices provide a limited set of apps that serve a dedicated purpose, such as digital signage, ticket printing, or inventory management. When you provision a dedicated device, you provide only the required apps and prevent users from adding other apps.

Dedicated devices are also known as corporate owned single use (COSU) devices or kiosk mode devices.

**Legacy device deployment, legacy mode**

 legacy deployment scenarios are for devices running Android versions earlier than 5.0. Android versions earlier than 5.0 do not support device owner mode or profile owner mode. Android versions 5.1 supports device owner mode but not profile owner mode.

The **legacy** mode of operation, which is also called device admin mode, supports legacy device deployments. In legacy mode, DPC has limited control of a device. The DPC can wipe a device, require a passcode, or enforce some policies. To provide app management on legacy devices, use Google Play and allow users to add a Google Account. You can also have the DPC add a managed Google Play Account to the legacy device.

Legacy mode is discouraged for deployments where you can implement device owner mode or profile owner mode. Google recommends using the highest level of device management possible instead of a lowest common denominator solution across a large fleet. For information on migrating from legacy mode to device owner or profile owner mode, see [Migrate from device administration to Android Enterprise](#).

**Note:**

Citrix also uses the term **legacy** to refer to customers who use Endpoint Management and G Suite, instead of managed Google Play, to manage Android Enterprise devices.

**Authentication methods**

Endpoint Management enrolls Android devices into MDM+MAM or MDM mode, with the option for users to register in MAM-only mode. Endpoint Management supports the following authentication methods for Android devices in MDM+MAM mode. For information, see the articles under [Certificates and authentication](#).
Citrix Endpoint Management

- Domain
- Domain plus security token
- Client certificate
- Client certificate plus domain
- Identity providers:
  - Azure Active Directory
  - Citrix Identity provider

Another rarely used authentication method is 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
  - To deploy private apps (optional), a Google developer account
- For Samsung Knox Mobile Enrollment (optional), Knox premium licenses.

**Connecting 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 Endpoint Management and creates an enterprise for Android Enterprise in Endpoint Management.

You need a corporate Google account to sign in to Google Play.

1. In the 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. On the **Android Enterprise** page in Endpoint Management Settings, click **Connect**. Google Play opens.

4. Sign in to Google Play with your corporate Google account credentials. Enter your organization name and confirm Citrix is your EMM provider.

5. An enterprise ID is added for Android Enterprise. To enable Android Enterprise, slide **Enable Android Enterprise** to **Yes**.
Your Enterprise ID appears in the Endpoint Management console.

Your environment is connected to Google and is ready to manage devices. You can now provide apps for users.

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 these types of apps and providing them to users, see Add apps.

The following section shows how to provide mobile productivity apps.

**Providing Citrix mobile productivity apps to Android Enterprise users**

Providing Citrix mobile productivity apps for Android Enterprise users requires these steps.

1. In your managed Google Play store, approve the apps you want your users to have. See Approve apps in managed Google Play.

2. In the Endpoint Management console, publish the app as a public app store app. See Configure apps as public app store apps.
3. In the Endpoint Management console, publish the same app again as an MDX app so the app can receive MDX policies. See Configure apps as MDX apps.

4. In the Endpoint Management console, configure the rules for the security challenge 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.

Approve apps in managed Google Play

Before you can add apps to Endpoint Management, first approve the app in your managed Google Play store. If you haven’t approved an app in your managed Google Play store, this error appears when you add the app:

Go to the managed Google Play store to determine which apps are already available and approved for use in your enterprise.

1. Log in to https://play.google.com/work with your Google account credentials.
2. Click My managed apps to show all apps that have been approved for your users.

To approve an app in the managed Google Play store:
1. While logged in to managed Google Play, select the app you want to approve. An **Approve** button appears on the app page.

2. Click **Approve**.
3. Click **Approve** again.
4. Select **Keep approved when app requests new permissions**. Click **Save**.
Configure apps as public app store apps

To configure Citrix Files as an Android Enterprise public app store app:

1. In the Endpoint Management console, click Configure > Apps. The Apps page appears.

2. Click Add. The Add App dialog box appears.
3. Click **Public App Store**. The **App Information** page appears.

4. On the **App Information** page, type the following information:
   - **Name**: Type a descriptive name for the app. This name appears under **AppName** 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 [Create app categories](#).

5. Click **Next**. The **App Platforms** page appears.

6. Under **Platforms**, select **Android Enterprise**. Clear the others platforms.

7. Under **Android Enterprise**, enter the bundle ID for the app and click **Search**. The app identifier can be found in the URL for the app in the Google Play store.
8. If the console shows the app is not approved in the Google Play store, click **Yes** to approve it now.

![App is not approved dialog]

9. Select the app to add it. Click **Next**.

![Public App Store and Android Enterprise search]

10. Assign the app to one or more delivery groups.
11. Click **Save**.

Repeat these steps for Citrix Secure Mail and Citrix Secure Web.

**Configure apps as MDX apps**

Mobile productivity apps do not use the native Android manifest. You must add these apps as MDX apps and configure their MDX policies before deploying the apps to users.

Before adding MDX apps, download the latest Android MDX files:


   **Android MDX files v19.5.0 V1**

   **May 8, 2019**

   **2.18 MB - (zip)**

   ![Download File](download_file)

   The MDX files included in this distribution are for use with the Citrix Mobile Productivity Apps distributed through the Google Play.

   **Checksums**

   SHA-256: 9d9d95f90b1ffcedfa1db8099f40127680221b1f470c830371d12a224410ce

2. Decompress the downloaded file and extract its contents.

To add and configure an MDX app:
1. In the Endpoint Management console, click **Configure > Apps**. The **Apps** page appears.

2. Click **Add**. The **Add App** dialog box appears.

3. Click **MDX**. The **MDX App Information** page appears.

4. Name the application and click **Next**.

5. Click **Next** to get to Android platform configuration.
6. Click **Upload**.

![Android MDX App](image)

7. Navigate to the MDX file location and select the MDX file you want to install.

8. Network access in some apps is **Blocked** by default. Enable network access. Click the menu and select **Tunneled - Web SSO**.

![App Network Access](image)

9. Click **Next** through the pages, excepting the defaults, until you reach delivery group assignments page.

10. Assign the app to the same delivery groups you assigned it to when publishing it as a public app store app.

11. Click **Save**.

Repeat the steps to configure an MDX app for each mobile productivity app.

**Configure security challenge policy**

The 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...
Citrix Endpoint Management

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 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.

<table>
<thead>
<tr>
<th>Device Policies</th>
<th>Apps</th>
<th>Media</th>
<th>Actions</th>
<th>ShareFile</th>
<th>Enrollment Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Platform</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>![Check box][1]</td>
<td>IOS</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>![Check box][1]</td>
<td>Windows Desktop/Tablet</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>![Check box][1]</td>
<td>Android</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>![Check box][1]</td>
<td>macOS</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>![Check box][1]</td>
<td>Windows Mobile/CE</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>![Check box][1]</td>
<td>Windows Phone</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>![Check box][1]</td>
<td>Android Enterprise</td>
<td>17</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Enter a Policy Name. Click Next.
6. 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 security challenges.

7. Click **Next**.

8. Assign the policy to one or more delivery groups.

9. Click **Save**.

### Creating enrollment profiles

Enrollment profiles control how Android devices are enrolled if Android Enterprise is enabled for your Endpoint Management deployment. Enrollment profiles determine whether Android devices are enrolled in the default Android Enterprise mode (fully managed or work profile) or in legacy (device administrator) mode.

By default, the Global enrollment profile enrolls new and factory reset Android Enterprise devices as fully managed devices and enrolls BYOD Android Enterprise devices as work profile devices.

### Creating an enrollment profile for legacy devices

Google is deprecating the device administrator mode of device management and encouraging customers 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 will make Android Enterprise the default enrollment option for Android devices.

This change will mean that if Android Enterprise is enabled for your 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 in device owner mode or profile owner mode. In that case, you can continue to manage them in device administrator mode. Create an enrollment profile for legacy devices and re-enroll all enrolled legacy devices.

To create an enrollment profile for legacy devices:

1. In the 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. Click Next or select Android under Platforms. The Enrollment Configuration page appears.
4. Set Management to Legacy device administration (not recommended). Click Next.
5. Select Assignment (options). The Delivery Group Assignment screen appears.
6. Choose the delivery group or delivery groups containing the administrators who enroll dedicated devices. Then click Save.

To continue managing legacy device 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 Secure Hub and providing 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 Endpoint Management. Users download 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.

When enrolling devices in Android Enterprise as work profile devices, always go to Google Play. From there, enable 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 Endpoint Management and downloads 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 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 are first powered on. Zero-touch enrollment is supported on some Android devices running Android 8.0 or later. See Zero-touch enrollment.

- **Google Accounts:** Users enter their Google Account credentials to initiate the provisioning process. This option is for enterprises using G Suite.
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 Secure Hub. Users then follow the Secure Hub set-up prompts to complete the enrollment.

In this enrollment method is recommended for most customers because the latest version of Secure Hub is downloaded from the Google Play store. Unlike with other enrollment methods, you do not provide Secure Hub for download from the Endpoint Management server.

System requirements

- 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.
4. Tap **Install** on the Android Enterprise screen prompting to install Secure Hub.
5. Tap **Install** on the Secure Hub installer screen.
6. Tap **Allow** for all app permission requests.

7. Tap **Accept & Continue** to install Secure Hub and allow it to manage the device.
8. Secure Hub is now installed and on the default enrollment screen. In this example, autodiscovery is not set up. If it was, the user can enter their username/email and a server would be found for them. Instead, enter the enrollment URL for the environment and tap **Next**.
9. The default configuration for 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 name 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 Secure Hub **My Apps** landing screen. Tap **Add apps from Store**.

14. To add Secure Web, tap **Secure Web**.
15. Tap **Add**.

16. Secure Hub directs the user to the Google Play store to install Secure Web. Tap **Install**.

17. After Secure Web is installed, tap **Open**. Enter a URL from an internal site in the address bar and verify that the page loads.
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.
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 Endpoint Management Provisioning Tool.

System requirements and prerequisites

- Supported Android devices.
• 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 Secure Hub or on the Citrix downloads page.

Each device can have only one Android Enterprise profile, managed Secure Hub. Only one profile is allowed on each device. Attempting to add a second DPC app removes the installed 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 initialize Android Enterprise:

• Package name of the DPC app that acts as device owner (in this case, Secure Hub).
• Intranet/Internet location from which the device can download the DPC app.
• SHA1 hash of 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 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 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 text file. The steps in the next procedure describe how to configure the text file and contain 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
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 contain 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=<SHA1 hash>
```

This line is the checksum of the EMM provider app. This checksum is used to verify that the download is successful. Steps to obtain 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 an Olson name of the form area/location. For example, America/Los_Angeles for Pacific time. If you don't enter a name, the time zone is automatically populated.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

This data isn’t required, because the value is hardcoded into the app as Secure Hub. It’s mentioned here only for the sake of completion.
Citrix Endpoint Management

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=ga50TwdCmfdJ72LGRFkke4Crbo\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=ga50TwdCmfdJ72LGRFkke4Crbo\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 Secure Hub checksum**

To get the checksum of any app, add the app as an enterprise app.

1. In the Endpoint Management console, go to **Configure > Apps** and then click **Add**.

   The **Add Apps** window appears.

2. Click **Enterprise**.

   The **App information** page displays.
3. Select the following configuration and then click Next.

The **Android Enterprise Enterprise App** page appears.

4. Provide the path to the .apk and then click **Next** to upload the file.

Once the upload is complete, the details of the uploaded package appear.
5. Click **Next**. Click **Download JSON** to download the JSON file which you then use to upload to Google Play. For Secure Hub, uploading to Google Play is not required, but you need the JSON file to read the SHA1 value from it.

A typical JSON file looks like the following:

6. Copy the **file_sha1_base64 value** and use it in the **Hash** field in the Provisioning Tool.
Note: The hash must be URL safe.

- Convert any + symbols to -
- Convert any / symbols to _
- Replace the trailing \u003d with =

If you store the hash in the nfcpreservation.txt file on the SD card of the device, the app does the safety conversion. However, if you opt to type the hash manually, it’s your responsibility to ensure its URL safety.

Libraries used

The Provisioning Tool uses the following libraries in its source code:

- v7 appcompat library, Design support library, and v7 Palette 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

To enroll a fully managed device 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.

System requirements

- Supported on all Android devices running Android 7.0 and above.

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: qn7oZUtheu3JBAinZRRrrjCQv6LOO6LlI0jcXT3-yKM

Key: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
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.
  
  Enter an Olson name of the form area/location. For example, America/Los_Angeles for Pacific time. If you don’t enter one, the time zone is automatically populated.

- **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:

```json
{
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.example.component",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKER": "true",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://example.com",
    "android.app.extra.PROVISIONING_LOCALE": "en_US",
    "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
    "android.app.extra.PROVISIONING_LOCAL_TIME": 159782841794,
    "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

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, such as https://goqr.me.

This QR code gets scanned by a factory-reset device to enroll the device 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 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 Secure Hub from the download location in the QR code, validate the signing certificate signature, install Secure Hub and sets it as the device owner.
Zero-touch enrollment

Zero-touch enrollment lets you set up devices to provision themselves as fully managed devices when they are 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, you 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 Endpoint Management. The configuration assigned to the device defines its automatic enrollment process.

System requirements

- Supported for zero-touch enrollment begins with Android 8.0.

Devices and account information from your reseller

- Devices eligible for zero-touch enrollment are purchased 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 Endpoint Management server you specify. Substitute the URL of your server for ‘URL’ in this example.

```json
{
    "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 Endpoint Management server and the user name and password that devices using this configuration use to log on to the server.

```json
{
    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
        "serverURL":"URL",
        "xm_username":"username",
        "xm_password":"password"
    }
}
```

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.

2. Click **Configuration**.

3. Click + above the configuration table.
4. Enter your configuration information in the configuration window that appears.
• **Configuration name**: Type the name 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 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
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 the Android Enterprise help topic **Zero-touch enrollment for IT admins**. This Android Enterprise help topic contains more information on how to manage configurations and apply them to devices.
Citrix Endpoint Management

Viewing fully managed devices in the Endpoint Management console

1. In the Endpoint Management console, go to Manage > Devices.

2. Add the **Android enterprise Enabled Device?** column by clicking the menu on the right of the table on this page.

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** is not. That difference is because the device only allows apps from the managed Google Play store. There is not an option for the user to install applications from the public store. Your organization manages all the content on the device.
**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 small set of apps required to perform the tasks needed for this use case. You also prevent users from enabling other apps or performing other actions on the device.

Dedicated devices are enrolled 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.

Dedicated devices are also known as corporate owned single use (COSU) devices.

**Note:**

Unlike other fully managed devices, dedicated devices can only be enrolled by users with Active Directory accounts. Local users can’t enroll dedicated devices.

To provision dedicated devices:

- Add a role-based access control (RBAC) role that allows Endpoint Management administrators to enroll dedicated devices to your Endpoint Management deployment. Assign this role to users whom you want to enroll dedicated devices.
- Add an enrollment profile for Endpoint Management administrators that you allow to enroll dedicated devices to your Endpoint Management deployment.
- Whitelist the app or apps you want the dedicated device to access.
- Optionally, set the whitelisted 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 as a fully managed device.

**System requirements**

- Support for enrolling dedicated devices begins with Android 6.0.

**Add the RBAC role for dedicated devices**

The RBAC role for enrolling dedicated devices enables Endpoint Management to silently provision and activate a managed Google Play account on the device. Unlike managed Google Play user accounts, these device accounts identify a device that is not tied to a user.

You assign this RBAC role to Endpoint Management administrators to enable them to enroll dedicated devices.
To add the RBAC role for enrolling dedicated devices:

1. In the Endpoint Management console, click the gear icon in the upper-right corner of the console. The **Settings** page appears.

2. Click **Role-Based Access Control**. The Role-Based Access Control page appears, which displays the four default user roles, plus any roles you have previously added.

3. Click **Add**. The **Add Role** page appears.

4. Enter the following information.
   - **RBAC name**: Enter “COSU” or other descriptive name for the role. You cannot change the name of a role.
   - **RBAC template**: Choose the ADMIN template.
   - **Authorized access**: Select **Admin console access** and **COSU devices enroller**.
   - **Console features**: Select **Devices**.
   - **Apply permissions**: Select the groups to which you want to apply the COSU role. If you click **To specific user groups**, a list of groups appears from which you can select one or more groups.

5. Click **Next**. The **Assignment** page appears.

6. Enter the following information to assign the role to Active Directory groups.
   - **Select domain**: In the list, click a domain.
   - **Include user groups**: Click **Search** to see a list of all available groups. Or, type a full or partial group name to limit the list to only groups with that name.
   - In the list that appears, select the user groups to which you want to assign the role. When you select a user group, the group appears in the **Selected user groups** list.

7. Click **Save**.

**Add a dedicated (COSU) enrollment profile**

When your Endpoint Management deployment includes dedicated devices, a single Endpoint Management administrator or small group of administrators enroll many dedicated devices.
To ensure that these administrators can enroll all the devices required, create an enrollment profile for them with unlimited devices allowed per user. Assign this profile to a delivery group containing the administrators who enroll dedicated devices. That way, even if the default Global profile has a limited number of devices allowed per user, administrators can enroll an unlimited number of devices. Those administrators must be in the dedicated (COSU) enrollment profile.

1. In the Endpoint Management console, go to **Configure > Enrollment Profiles**. The default Global profile appears.

2. To add an enrollment profile, click **Add**. On the **Enrollment Info** page, type a name for the enrollment profile. Ensure that number of devices that members with this profile can enroll is set to unlimited.

3. On the **Android** page:
   - Set **Management** to **Android Enterprise**.
   - Set **Device owner mode** to **Company-owned device**.

4. On the **Delivery Group Assignment** page, choose the delivery group or delivery groups containing the administrators who enroll dedicated devices. Then click **Save**.

The Enrollment Profile page appears with the profile you added.
Citrix Endpoint Management

**Whitelist apps and set lock task mode**

The Kiosk device policy lets you whitelist apps and set lock task mode. By default, Secure Hub and Google Play services are whitelisted.

To add the Kiosk policy:

1. In the 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.
5. In the Policy Information pane, type the **Policy Name** and an optional **Description**.
6. Click **Next** and then click **Add**.
7. To whitelist an app and allow or deny lock task mode for that app:
   - Select the app you want to whitelist 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 whitelist 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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
To enroll the device

1. Power on a new or factory reset device.
2. Enroll the devices as a fully managed device, assigning it to a user that has the dedicated device RBAC role.

After the device is enrolled, it displays a list of the apps a user can run and lock into this screen.

This example shows that while Gmail is on the device, it is not able to run.

Configure Android Enterprise device policies

Use these policies to configure how Endpoint Management interacts with devices running Android Enterprise. 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.
**Security actions**

Android Enterprise supports the following security actions. For a description of each security action, see Security actions.

<table>
<thead>
<tr>
<th>Security action</th>
<th>Android Enterprise (BYOD)</th>
<th>Android Enterprise (company-owned)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Renewal</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Full Wipe</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Locate</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Lock</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Lock and Reset Password</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Notify (Ring)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Revoke</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Selective Wipe</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Notes:**

The Locate security action fails unless the Location device policy has set the location mode for the device to High Accuracy or Battery Saving.

The Lock and Reset Password command is not supported on work profile devices that are running versions of Android earlier than Android 8.0. On devices work profile devices that are running...
Android 8.0 or greater: The passcode sent locks the work profile but the device is not locked. If no passcode is sent, or the passcode sent doesn’t meet passcode requirements, and no passcode is already set on the work profile: The device is locked. If no passcode is sent, or the passcode sent doesn’t meet passcode requirements, but a passcode is already set on the work profile: The work profile is locked but device is not locked.

**Unenroll an Android Enterprise enterprise**

If you no longer want to use your Android Enterprise enterprise, you can unenroll the enterprise.

**Warning:**

After an enterprise is unenrolled, Android Enterprise apps on devices already enrolled through it are reset to their default states. Google no longer manages the devices. Re-enrolling them in an Android Enterprise enterprise might not restore previous functionality until you perform 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. Android Enterprise Managed Configurations policies previously applied no longer affect operations.
- 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 Android Enterprise Managed Configurations policies. You can apply other policies, such as Scheduling, Password, and Restrictions, to these devices.
- If you attempt to enroll devices in Android Enterprise, they are enrolled as Android devices, not Android Enterprise devices.

Unenroll an Android Enterprise enterprise using the Endpoint Management server console and Endpoint Management Tools.

When you perform this task, the Endpoint Management server opens a popup window for Endpoint Management Tools. Before you begin, ensure that the Endpoint Management server has permission to open popup windows in the browser. Some browsers, such as Google Chrome, require you to disable popup blocking and add the address of the Endpoint Management site to the popup block whitelist.

To unenroll an Android Enterprise enterprise:

1. In the 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**.
Legacy Android Enterprise for G Suite Customers

September 23, 2019

G Suite customers must use the legacy Android Enterprise settings to configure legacy Android Enterprise.

If your organization already uses G Suite to provide users access to Google apps, you can use G Suite to register Citrix as your EMM. If your organization uses G Suite, it has an existing enterprise ID and existing Google Accounts for users. To use Endpoint Management with G Suite, you sync with your LDAP directory and retrieve Google Account 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 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 G Suite 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 legacy Android Enterprise, click legacy Android Enterprise in the Android Enterprise page in 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.

   
   The following page displays where you type your administrator and company information.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
2. Type your administrator user information.

3. Type your company information, in addition to your administrator account information.
The first step in the process is complete and you see the following page.
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**.
3. Google verifies your domain ownership.
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.
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 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 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](https://developers.google.com/identity/protocols/OAuth2ServiceAccount).

1. In a web browser, go to [https://console.cloud.google.com/project](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**.
5. Click Library, in Search, type EMM and then click the search result.

6. On the Overview page, click Enable.
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.
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** check box. Click **P12**, select the **Enable Google Apps Domain-wide Delegation** check box and then click **Create**.
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**.
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 for whitelisting.

14. On the **Library** page, search for **Admin SDK** and then click the search result.

15. On the **Overview** page, click **Enable**.
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.
18. Click **Manage API client access.**
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 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 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 Endpoint Management console to manage your Android devices. Import the P12 certificate 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.
Import the P12 certificate

Follow these steps to import your Android Enterprise P12 certificate:

1. Sign in to the Endpoint Management console.

2. 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.

3. Click Import. The Import dialog box appears.

Configure the following settings:

- **Import**: In the list, click Keystore.
- **Keystore type**: In the list, click PKCS#12.
- **Use as**: In the list, click Server.
Citrix Endpoint Management

- **Keystore file:** Click **Browse** and navigate to the P12 certificate.
- **Password:** Type the certificate password. This is the private key password you created when setting up your Android Enterprise account.
- **Description:** Optionally, type a description of the certificate.

4. Click **Import**.

**Set up Android Enterprise server settings**

1. In the 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.

![Screenshot of Android Enterprise settings](image)

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 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. Sign in to the Endpoint Management console.

2. Click the gear icon in the upper-right corner of the console. The **Settings** page appears.
3. Click **Certificates**. The **Certificates** page appears.

4. In the list of certificates, click the SAML certificate.

5. Click **Export** and save the certificate to your computer.

6. Sign in to the Google Admin portal by using your Android Enterprise administrator credentials. For access to the portal, see [Google Admin portal](#).

7. Click **Security**.

8. Under **Security**, click **Set up single sign-on (SSO)** and then configure the following settings.
• **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 is not available.

• **Verification certificate:** Click **CHOOSE FILE** and then navigate to the SAML certificate exported from Endpoint Management.

9. 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.
The basic steps to setting up any device policy are as follows.

1. Sign on to the Endpoint Management console.
2. Click Configure, and then click Device Policies.
3. Click Add and then 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 Endpoint Management. First, complete Android Enterprise setup tasks on Google to set up a domain administrator and to obtain a service account ID and a binding token.

1. In the Endpoint Management web console, click the gear icon in the upper-right corner. The Settings page displays.
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 G Suite partner access for Endpoint Management**

Some Endpoint Management features for Chrome use Google partner APIs to communicate between Endpoint Management and your G Suite domain. For example, 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 G Suite domain in the Endpoint Management console and then configure your G Suite account.

**Set up your G Suite domain in Endpoint Management**

To enable Endpoint Management to communicate with the APIs in your G Suite domain, go to **Settings > Google Chrome Configuration** and configure the settings.
G Suite domain: The G Suite domain that hosts the APIs needed by Endpoint Management.
G Suite admin account: The administrator account for your G Suite domain.
G Suite client ID: The client ID for Citrix. Use this value to configure partner access for your G Suite domain.
G Suite enterprise ID: The enterprise ID for your account, filled in from your Google enterprise account.

Enable partner access for devices and users in your G Suite 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**.

5. Search for **Chrome Management - Partner Access**.

6. Select the **Enable Chrome Management - Partner Access** check box.

7. Agree that you understand and want to enable partner access. Click **Save**.
8. In the Chrome management page, click **Device Settings**.

9. Search for **Chrome Management - Partner Access**.

10. Select the **Enable Chrome Management - Partner Access** check box.

11. Agree that you understand and want to enable partner access. Click **Save**.

12. Go to the **Security** page and then click **Advanced Settings**.
13. Click **Manage API client Access**.

14. In the 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 Endpoint Management server is configured to search for users by User Principal Name (UPN) or SAM account name.

If the Endpoint Management server is configured to search for users by UPN, users must enter a UPN in the format:

- \textit{username@domain}

If the Endpoint Management server is configured to search for users by SAM users must enter a SAM in one of these formats:

- \textit{username@domain}
- \textit{domain\username}

To determine which type of user name your Endpoint Management server is configured for:

1. In the 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 \textit{User search by} field:
   - If it is set to \textit{userPrincipalName}, Endpoint Management server is set for UPN.
   - If it is set to \textit{sAMAccountName}, Endpoint Management server is set for SAM.
Unenrolling an Android Enterprise enterprise

You can unenroll an Android Enterprise enterprise using the Endpoint Management server console and Endpoint Management Tools.

When you perform this task, the Endpoint Management server opens a popup window for Endpoint Management Tools. Before you begin, ensure that the 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 Endpoint Management site to the popup block whitelist.

Warning:

After an enterprise is unenrolled, Android Enterprise apps on devices already enrolled through it are reset to their default states. The devices will no longer be managed by Google. Re-enrolling them in an Android Enterprise enterprise may 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. Android Enterprise App Permissions and Android Enterprise Managed Configurations policies previously applied no longer have an effect.
- Devices enrolled through the enterprise are managed by Endpoint Management, but are unmanaged from Google perspective. No new Android Enterprise apps can be added. No Android Enterprise App Permissions or Android Enterprise Managed Configurations policies can be applied. Other policies, such as Scheduling, Password, and Restrictions can still be applied to these devices.
- If you attempt to enroll devices in Android Enterprise, they are enrolled as Android devices, not Android Enterprise devices.

To unenroll an Android Enterprise enterprise:

1. In the 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.

5. When the Endpoint Management Tools page opens, enter the password you created in the previous step.
6. Click **Unenroll**.

**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.

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 Endpoint Management and downloads 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 Secure Hub. Users then follow the Secure Hub set-up prompts to complete the enrollment.

In this enrollment method is recommended for most customers because the latest version of Secure Hub is downloaded from the Google Play store. Unlike with other enrollment methods, you do not provide Secure Hub for download from the 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.

**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: qn7oZUtheu3JBAinzZRrrjCQv6LOO6LiOjcT3-yKM

Key: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
Value: https://path/to/securehub.apk

Note:
If Secure Hub is uploaded onto Citrix Endpoint Management server as an enterprise app, it can be downloaded from https://<fqdn>:4443/*instanceName*/worxhome.apk. The path to the Secure Hub APK must be accessible over the Wi-Fi connection that the device connects to during provisioning.

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.

  Enter an Olson name of the form area/location. For example, America/Los_Angeles for Pacific time. If you don’t enter one, the time zone is automatically populated.

- **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:

```json
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "securehub",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "qn7oZUtheu3JBAinzZRrrjCQv6LOO6LiOjcT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://path/to/securehub.apk",
  "android.app.extra.PROVISIONING_LOCAL_TIME": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": "155709284178",
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

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 fully managed devices.
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 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 Secure Hub from the download location in the QR code, validate the signing certificate signature, install 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 Endpoint Management Provisioning Tool.

Prerequisites:

- Supported Android devices
- 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 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 Endpoint Management, Secure Hub is the EMM app. Only one profile is allowed on each device. Attempting 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 Android Enterprise:

- Package name of the EMM provider app that acts as device owner (in this case, Secure Hub).
- Intranet/Internet location from which the device can download the EMM provider app.
- SHA1 hash of EMM provider app to verify if the download is successful.
• 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 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 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 text file. The steps in the next procedure describe how to configure the text file and contain 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
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 contain the following data:

```plaintext
android.app.extra.PROVISIONINGDEVICE_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.

```plaintext
android.app.extra.PROVISIONINGDEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>
```

This line is the checksum of the EMM provider app. This checksum is used to verify that the download is successful. Steps to obtain the checksum are discussed later in this article.

```plaintext
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.

```plaintext
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.

```plaintext
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

If the Wi-Fi is unprotected, this field must be empty.

```plaintext
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.

```plaintext
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

The time zone in which the device is running. Type an Olson name of the form area/location. For example, America/Los_Angeles for Pacific time. If you don't enter a name, the time zone is automatically populated.

```plaintext
android.app.extra.PROVISIONINGDEVICE_ADMIN_PACKAGE_NAME=<package name>
```

This data isn't required, because the value is hardcoded into the app as 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:

```plaintext
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=ga50TwdCmfdJ72LGRFkke4CrbAk
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:

```plaintext
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=ga50TwdCmfdJ72LGRFkke4CrbAk
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 Secure Hub checksum

To get the checksum of any app, add the app as an enterprise app.

1. In the Endpoint Management console, go to **Configure > Apps** and then click **Add**.
   
   The **Add Apps** window appears.

2. Click **Enterprise**.
   
   The **App information** page displays.
3. Select the following configuration and then click Next.

The Android Enterprise Enterprise App page appears.

4. Provide the path to the .apk and then click Next to upload the file.

Once the upload is complete, the details of the uploaded package appear.
5. Click **Next** to open page to download the JSON file, which you then use to upload to Google Play. For Secure Hub, uploading to Google Play is not required, but you need the JSON file to read the SHA1 value from it.

6. Copy the **file_sha1_base64 value** and use it in the **Hash** field in the Provisioning Tool.
Note: The hash must be URL safe.

- Convert any + symbols to -
- Convert any / symbols to _
- Replace the trailing \u003d with =

If you store the hash in the nfcprovisioning.txt file on the SD card of the device, the app does the safety conversion. However, if you opt to type the hash manually, it’s your responsibility to ensure its URL safety.

Libraries used

The Provisioning Tool uses the following libraries in its source code:

- v7 appcompat library, Design support library, and v7 Palette library by Google under Apache license 2.0

  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 Endpoint Management. Users download 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.

Tip:

When enrolling devices in Android Enterprise as work profile devices, always go to Google Play. From there, enable Secure Hub to appear in the user’s personal profile.

Android OS

September 5, 2019
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 Endpoint Management service, use Firebase Cloud Messaging (FCM). For information, see Firebase Cloud Messaging.

Endpoint Management enrolls Android devices into MDM+MAM or MDM mode, with the option for users to register in MAM-only mode. Endpoint Management supports the following authentication types for Android devices in MDM+MAM mode. For information, see the articles under Certificates and authentication.

- Domain
- Domain plus security token
- Client certificate
- Client certificate plus domain
- Identity providers:
  - Azure Active Directory
  - Citrix Identity provider

Another rarely used authentication method is 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.
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 Endpoint Management supports for Android devices:
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 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.

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 you added and then, in the menu that appears, click Edit.

**Note:**
When you select the check box 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 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 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. Endpoint Management deletes the item immediately.

7. The remaining **Device Details** sections contain 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 assigned policies including the number of deployed, pending, and failed policies. Provides the policy name, type and last deployed information for each policy.

• **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.

**Configure Android device policies**

Use these policies to configure how Endpoint Management interacts with devices running Android. This table lists all device policies available for Android devices.

<table>
<thead>
<tr>
<th>APN</th>
<th>App Access</th>
<th>App Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Lock</td>
<td>App Uninstall</td>
<td>Credentials</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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 Secure Hub installs, tap Open.

4. For devices running Android 6.0 and greater, accept the required permissions:
   - Allow Secure Hub to make and manage phone calls? (required)
   - Allow Secure Hub to access photos, media, and files on your device? (required)
   - Allow Secure Hub to access this device's location? (optional)

5. Enter your corporate credentials, such as your Endpoint Management server name, User Principal Name (UPN), or email address. Then, click Next.

6. For devices in MDM+MAM mode, choose how to enroll your device:
   - To enroll in MDM+MAM mode, tap Yes, enroll.
   - To enroll in MAM-only mode, tap No.

7. In the Activate device administrator screen, tap Activate.

8. Enter your corporate password and then tap Sign On.

9. Depending on the way Endpoint Management is configured, you might be asked to create a Citrix PIN. You can use the PIN to sign on to Secure Hub and other Endpoint Management-enabled apps, such as Secure Mail and Citrix Files. You enter your Citrix PIN twice. On the Create Citrix PIN screen, enter a PIN.

10. Reenter the PIN. 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 Endpoint Management to push apps to devices automatically after enrollment, users are prompted to install the apps. In addition, policies that you configure in Endpoint Management are deployed to the device. Tap **Install** to install the apps.

**To unenroll and reenroll an Android device**

Users can unenroll from within Secure Hub. When users unenroll by using the following procedure, the device still appears in the device inventory in the Endpoint Management console. You cannot perform actions on the device, however. For example, you cannot track the device or monitor device compliance.

1. Tap to open the 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**.

   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](#).

<table>
<thead>
<tr>
<th>App Lock</th>
<th>App Wipe</th>
<th>Certificate Renewal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Wipe</td>
<td>Locate</td>
<td>Lock</td>
</tr>
<tr>
<td>Lock and Reset Password</td>
<td>Notify</td>
<td>Revoke</td>
</tr>
<tr>
<td>Selective Wipe</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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, Endpoint Management again requests location permission when sending the Locate command.

**Firebase Cloud Messaging**

August 26, 2019

Note: Firebase Cloud Messaging (FCM) was previously known as Google Cloud Messaging (GCM). Some 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 Endpoint Management. 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 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 Endpoint Management service to your device by using FCM. FCM registration works for new device enrollments and previously enrolled devices.

When Endpoint Management needs to initiate 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.

**Prerequisites**

- Latest Secure Hub client
- Google developer account credentials
- Google Play services installed on FCM-enabled Android devices

**Firewall ports**

- Open port 443 on 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 whitelisting ports 5228 through 5230 with no IP restrictions. However, if you require IP restrictions, FCM recommends whitelisting all the IP addresses in the IPv4 and IPv6 blocks. 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.

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**.

4. Click the **Cloud Messaging** tab. Copy the **Server key** and **Sender ID** values. In the next procedure, you paste those values in the Endpoint Management console. As of October 2016, you must create Server Keys in the Firebase console.
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 Endpoint Management for FCM**

In the Endpoint Management console, go to **Settings > Firebase Cloud Messaging**.

- **Edit API key**, and type the Firebase Cloud Messaging **Server key** that you copied in the last step of Firebase Cloud Messaging configuration.

- **Edit Sender ID**, and type the **Sender ID** value you copied in the previous procedure.

After you complete the setup, you can remove your Scheduling device policy or change that policy to connect less often.

**To test your configuration**

1. Enroll an Android device.
2. Leave the device idle for some time, so that it disconnects from Endpoint Management.
3. Sign in to the Endpoint Management console, click Manage, select the Android device, and then click Secure.


In a successful configuration, selective wipe occurs on the device.

**Android SafetyNet**

September 23, 2019

You can use the Android SafetyNet feature to assess the compatibility and security of Android devices that have 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 Secure Hub has been modified by an unknown source.

When the Android SafetyNet feature is enabled, Secure Hub sends the SafetyNet Attestation API request to Google Play services and the result is reported back to Endpoint Management. 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.
Citrix Endpoint Management

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 Endpoint Management.
- When a 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. 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 Endpoint Management deployment will make more than 10,000 requests per day, fill out this quota request form.

Get the SafetyNet API key

To enable Android SafetyNet in Endpoint Management, you need the SafetyNet API key.

1. Log in to the Google API console with your Google administrator account credentials.
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.
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 Endpoint Management console when you enable the Android SafetyNet.

**Enable Android SafetyNet**

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The Settings page appears.


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.

**View Android SafetyNet results**

To view the results of the SafetyNet Attestation API assessment for a device:

1. In the Endpoint Management console, click Manage > Devices.

2. Select Android devices to see the SafetyNet Attestation API results. Then click Show more.


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 Android Compatibility Test Suite (CTS). If this value is 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 Secure Hub on the device has been modified by an unknown source. If this value is False, Secure Hub on the device has been modified by an unknown source.

- **SafetyNet last known status**: This value shows the last known SafetyNet status of the device:
Citrix Endpoint Management

- **Success:** The SafetyNet Attestation API found no evidence that Secure Hub on the device has been modified by an unknown source.

- **LOCK_BOOTLOADER:** The user should lock the bootloader of the device. Secure Hub on the device has been modified by an unknown source.

- **RESTORE_TO_FACTORY_ROM:** The user should restore the device to a clean factory ROM. Secure Hub on the device has been modified by an unknown source.

**Samsung**

October 1, 2019

Samsung offers several solutions that are compatible with Citrix Endpoint Management.

- Endpoint Management supports and extends both Samsung for Enterprise (SAFE) and Knox policies on compatible Samsung devices.
- Knox includes the SE for Android Management Service (SEAMS). SEAMS provides API-level control of the Samsung security policy engine.
- The Knox Service plug-in (KSP) in an app that supports a subset of Knox Platform for Enterprise features.

To control how and when Android devices connect to the Endpoint Management service, use Firebase Cloud Messaging (FCM). For information, see Firebase Cloud Messaging.

Endpoint Management enrolls Android devices into MDM+MAM or MDM mode, with the option for users to register in MAM-only mode. Endpoint Management supports the following authentication types for Android devices in MDM+MAM mode. For information, see the articles under Certificates and authentication.

- Domain
- Domain plus security token
- Client certificate
- Client certificate plus domain
- Identity providers:
  - Azure Active Directory
  - Citrix Identity provider

Another rarely used authentication method is 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. Deploy Samsung license keys.

4. Enable Knox attestation.

5. Configure Samsung device policies.


For supported operating systems, see Supported device operating systems.

**Supported enrollment methods**

The following table lists the enrollment methods that Endpoint Management supports for Android devices:

<table>
<thead>
<tr>
<th>Method</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulk enrollment</td>
<td>Yes (Knox)</td>
</tr>
<tr>
<td>Manual enrollment</td>
<td>Yes</td>
</tr>
<tr>
<td>Enrollment invitations</td>
<td>Yes</td>
</tr>
</tbody>
</table>

You can use Knox Mobile Enrollment to enroll multiple Knox devices into Endpoint Management (or any mobile device manager) without manually configuring each device. For information, see Knox Bulk Enrollment.

For information about enrolling devices, see Enroll Android devices.

**Deploy Samsung license keys**

Samsung has Enterprise License Management (ELM) keys and Knox License Management (KLM) keys. You purchase Samsung licenses from Samsung.

- **Knox**: The Knox platform requires that you purchase a Knox Workspace license. To enable the Knox APIs and deploy Knox policies and restrictions to devices, first configure the Endpoint Management device policy, Samsung MDM license key. To activate Knox, you must push at least one Restriction device policy specifically for Knox along with the ELM and KLMS key.

  For HTC-specific policies, Endpoint Management supports HTC API version 0.5.0. For Sony-specific policies, Endpoint Management supports Sony Enterprise SDK 2.0.

- **SAFE**: Deploy the built-in Samsung ELM key to a device before deploying SAFE policies and restrictions. To deploy that key, configure the Endpoint Management device policy, Samsung
MDM license key.

**Samsung enterprise Firmware-Over-The-Air (E-FOTA) service**

Endpoint Management also supports the Samsung Enterprise Firmware-Over-The-Air (E-FOTA) service. Samsung E-FOTA lets you determine when devices get updated, determine the firmware version to use, and test updates before deploying them. For information, see [Configure Samsung E-FOTA settings](#).

**Enable Knox attestation**

You can configure Endpoint Management to query the Knox attestation server REST APIs. Knox applies hardware security capabilities that provide multiple levels of protection for the operating system and applications. One level of this security resides at the platform through attestation. An attestation server provides verification of the mobile device core system software (for example, the boot loaders and kernel). The verification occurs at runtime based on data collected during a trusted boot.

1. In the Endpoint Management web console, click the gear icon in the upper-right corner. The **Settings** page appears.
2. Click **Samsung Knox**.

3. Set **Enable Samsung Knox attestation** to **Yes** to enable Knox attestation. The default is **No**.
4. In the **Web service URL** list, do one of the following:
   - Click the appropriate attestation server.
   - Click **Add new** and then enter the Web service URL.
5. Click **Test Connection** to verify the connection. A success or failure message appears.
Configure Samsung device policies

Device policies for Knox:

<table>
<thead>
<tr>
<th>App Restrictions</th>
<th>App Uninstall</th>
<th>Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Apps to Samsung Container</td>
<td>Exchange</td>
<td>Knox Platform for Enterprise key</td>
</tr>
<tr>
<td>Passcode</td>
<td>Restrictions</td>
<td>Samsung MDM License key</td>
</tr>
</tbody>
</table>

Device policies for Samsung SAFE:

<table>
<thead>
<tr>
<th>App Uninstall Restrictions</th>
<th>Browser</th>
<th>Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Kiosk</td>
<td>Knox Platform for Enterprise</td>
</tr>
<tr>
<td>OS update</td>
<td>Restrictions</td>
<td>Samsung MDM License key</td>
</tr>
<tr>
<td>Storage Encryption</td>
<td>VPN</td>
<td></td>
</tr>
</tbody>
</table>

Device policies for Samsung SEAMS:

| Copy Apps to Samsung Container |

Security actions

Android supports the following security actions. For a description of each security action, see Security actions.
Add the Knox service plug-in app

If you plan on using Android Enterprise with Knox, add the Knox service plug-in to Endpoint Management. The KSP app uses AndroidOEMConfig to support features such as security policies, flexible VPN configuration, and biometric authentication controls. AndroidOEMConfig enables OEMs and endpoint mobility managers (EMM) to support custom OEM APIs that cover use cases not supported through Android Enterprise. For more information on KSP, see the Knox Service Plugin Admin Guide.

2. Log in to your Endpoint Management console and add the Knox service plug-in as a public app store app. For more information on adding public app store apps, see Add a public app store app.
3. In your Endpoint Management console, navigate to Configure > Device policies. Click Add.
4. Click **Android Enterprise Managed Configuration**. In the dialog that comes up, select **Knox Service Plugin** from the menu. For more information on the Android Enterprise managed configuration policy, see [Android Enterprise managed configurations policy](#).

5. Type a name for the policy then continue to the platform page.

6. On the platform page, type a **Profile name** for your Knox profile and input the **KPE Premium License key** from Samsung. The policies that appear below these fields come from your Knox deployment. For more information on Knox policies, see the Knox Service Admin Plugin Guide referenced earlier in this section.

7. Click **Next** and configure deployment rules for the policy.

8. Click **Save**.

**Samsung Knox bulk enrollment**

October 1, 2019
To enroll multiple Samsung Knox devices into Endpoint Management (or any mobile device manager) without manually configuring each device, use Knox Mobile Enrollment. The enrollment occurs upon first-time use or after a factory reset. Admins can also pass user names and passwords directly to the device, so users don’t need to enter any information upon enrollment.

**Note:**
The setup for Knox Mobile Enrollment is not related to the Endpoint Management Knox container. For more information on Knox Mobile Enrollment, see the [Knox Mobile Enrollment Admin Guide](#).

**Prerequisites for Knox Mobile Enrollment**

- Endpoint Management must be configured (including licenses and certificates) and running.
- Secure Hub APK file. You upload the file when setting up Knox Mobile Enrollment.
- For a list of KME requirements, see the [Knox Mobile Enrollment Admin Guide](#).

**To download the Secure Hub APK file**

1. Log in to the Citrix download site and go to the [Citrix Endpoint Management downloads](#).
2. Go to [Mobile productivity apps and MDX Toolkit](#) and choose your edition.

**Configure firewall exceptions**

To access Knox Mobile Enrollment, configure the following firewall exceptions. Some of these firewall exceptions are required for all devices and some are specific the device's geographical region.

<table>
<thead>
<tr>
<th>Device Region</th>
<th>URL</th>
<th>Port</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td><a href="https://gslb.secb2b.com">https://gslb.secb2b.com</a></td>
<td>443</td>
<td>Global load balancer for Knox Mobile Enrollment initiation</td>
</tr>
<tr>
<td>All</td>
<td><a href="https://gslb.secb2b.com">https://gslb.secb2b.com</a></td>
<td>80</td>
<td>Global load balancer for Knox Mobile Enrollment initiation on some limited legacy devices</td>
</tr>
<tr>
<td>All</td>
<td>umc-cdn.secb2b.com</td>
<td>443</td>
<td>Samsung agent update servers</td>
</tr>
</tbody>
</table>
### Device Region URL Port Destination

<table>
<thead>
<tr>
<th>Device Region</th>
<th>URL</th>
<th>Port</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>bulkenrollment.s3.amazonaws.com</td>
<td>80</td>
<td>Knox Mobile Enrollment customer EULAs</td>
</tr>
<tr>
<td>All</td>
<td>eula.secb2b.com</td>
<td>443</td>
<td>Knox Mobile Enrollment customer EULAs</td>
</tr>
<tr>
<td>All</td>
<td>us-be-api-mssl.samsungknox.com</td>
<td>443</td>
<td>Samsung servers for IMEI verification</td>
</tr>
<tr>
<td>United States</td>
<td><a href="https://us-segd-api.secb2b.com">https://us-segd-api.secb2b.com</a></td>
<td>443</td>
<td>Samsung Enterprise Gateway for US region</td>
</tr>
<tr>
<td>Europe</td>
<td><a href="https://eu-segd-api.secb2b.com">https://eu-segd-api.secb2b.com</a></td>
<td>443</td>
<td>Samsung Enterprise Gateway for European region</td>
</tr>
<tr>
<td>China</td>
<td><a href="https://china-segd-api.secb2b.com">https://china-segd-api.secb2b.com</a></td>
<td>443</td>
<td>Samsung Enterprise Gateway for China region</td>
</tr>
</tbody>
</table>

**Note:**
You can find a full list of firewall exceptions in the [Knox Mobile Enrollment Admin Guide](#).

### Getting access to Knox Mobile Enrollment

Follow these procedures to get access to Knox Mobile Enrollment.

**If you have a Knox web portal account**

1. Log on to the Knox web portal and go to your Samsung Knox Dashboard. To access your Knox web portal, see the [Samsung Account site](#).
2. Under **Knox Mobile Enrollment**, click **Get Started**.
3. Fill out the applicable fields and then click **Apply**.

After Samsung approves your application, you receive a welcome email with instructions on how to start using the Knox Mobile Enrollment tool. For a faster approval process, provide any essential information, including contact details for your reseller, Samsung sales representative, or any other information that assists in your approval.
Setting up Knox Mobile Enrollment

After you get access to Knox Mobile Enrollment, go to the Knox portal and then click **Launch Mobile Enrollment**.

If Samsung cannot authorize the account to use Bulk Enrollment, you see an error screen.

The enrollment process then follows these general steps, described in detail in the following subsections.

1. Create an MDM profile with your MDM console information and settings.
   
   The MDM profile indicates to your devices how to connect to your MDM.

2. Add devices to your MDM profile.
   
   You can either upload a CSV file with device information or install and use the Knox deployment app from Google Play.

3. Samsung alerts you when device ownership is verified.

4. Provide users with MDM credentials. Instruct them to connect to the Internet using Wi-Fi and to accept the prompt to enroll their device.
To create an MDM profile

Create an MDM profile that defines the Endpoint Management server to use. Create one profile per server.

1. Log on to the Knox Mobile Enrollment website.
2. Click MDM Profiles on the left. Click CREATE PROFILE and then choose from the two options available.
   - **DEVICE OWNER**: For fully managed or dedicated devices. Allows applications to apply policies and restrictions during setup.
   - **DEVICE ADMIN**: A legacy option that has different options from device owner, including the option to skip device setup.

3. Once you’ve selected an option, enter the following information:
   - **Profile Name**: A descriptive name for the profile
   - **Description**: A short description to distinguish the profile.
Citrix Endpoint Management

- **Pick your MDM:** Select Citrix from the menu. Only for device owner profiles.

- **MDM Agent APK:** Only for device owner profiles. Type the Secure Hub APK download URL. For example:

  ```
  https://example.com/zdm/securehub.apk
  https://pmdm.mycorp-inc.net/zdm/securehub.apk
  ```

  The APK file can reside on any server that the devices can access during enrollment. During the enrollment, a device downloads Secure Hub from that URL, installs Secure Hub, and then opens Secure Hub with the custom JSON data described next.

  **Note:**
  The capitalization of the .apk file name must match the URL you enter. For example, if the file name is all lowercase, it must also be all lowercase in the URL.

- **MDM Server URI:** Do not specify an MDM server URI. Endpoint Management does not use the Samsung MDM protocol.

4. Click **Continue** and then configure the following:

- **MDM Agent APK:** Only for device admin profiles. Add any number of MDM apps to download automatically during device enrollment.

- For **Custom JSON Data**, enter the Endpoint Management server address, user name, and password in the format:

  ```
  {
  "serverURL": "URL", "xm_username": "Username", "xm_password": "Password"
  }
  ```

Examples:

```javascript
{
  "serverURL": "https://example.com/zdm", "xm_username": "userN", "xm_password": "password1234"
}
{
  "serverURL": "https://pmdm.mycorp-inc.net/zdm", "xm_username": "james.cork", "xm_password": "aDin20_1fa"
}
```

You can also enter custom JSON for zero-touch enrollment for Android Enterprise.

```json
{
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
    "serverURL": "URL", "xm_username": "username", "xm_password": "password"
  }
}
```
Note:
The Secure Hub APK file must be uploaded on the specified server (example: https://pmdm.mycorp-inc.net:4443) under the Apps section. This process is similar to uploading enterprise apps.

- **Dual DAR**: Optionally enable Dual DAR to apply extra layers of encryption on device owner profiles. You can also use a third party crypto app.

- **System apps**: For device owner profiles only. Select **Disable system apps** to disable all apps except for a limited set. Select **Leave all system apps enabled** to ensure that the device owner profile can access all apps.

- **Enrollment settings**: For device admin profiles only. Mark the checkboxes for **Skip Setup Wizard** or **Allow end user to cancel enrollment** if you want to allow those options.
• **Privacy Policy, EULAs and Terms of Service:** Click **ADD LEGAL AGREEMENT** to enter a title and text for any sort of policy you want to display during enrollment.

• **Company Name:** For device owner profiles only. Type the organization name to display during enrollment.

• **Support contact details:** On device admin profiles, edit the following information shown upon successful enrollment:
  
  – **Company Name**
  – **Company Address**
  – **Support Phone Number**
  – **Support Email Address**

  You can also select **Save as default support contact details** to use the same information for other profiles.

• **Associate a Knox license with this profile:** On device admin profiles, select this option to pass the Knox license key directly to the device. This allows for easier Knox profile configuration.

  ![Device Owner profile settings](image)

5. Click **CREATE** to finalize the profile.

When a device starts bulk enrollment, the device uses the profile data. First, the device downloads Secure Hub from the given URL, installs Secure Hub, and opens Secure Hub with the custom JSON
data as parameter. Secure Hub already has the Endpoint Management address, so Secure Hub doesn’t need to prompt for it. Enrollment occurs automatically, since the JSON file provides credentials as well.

For more information on creating profiles, see Samsung’s documentation at https://docs.samsungknox.com/KME-Getting-Started/Content/create-profiles.htm.

**To add devices by using a .csv file**

To add devices, upload device IDs and associate them to one of the previously created MDM profiles. Upload a .csv file. The different ways of building the file are documented on the Knox website. The simplest way is to enter one IMEI per line, as follows.

**Note:**

You can alternatively add devices by scanning them, as described in the next section.

1. From the Knox Mobile Enrollment site, go to Devices > All Devices and then click Upload Devices.
2. Under CSV File Format, click Download file template.
3. Enter information in corresponding columns in the template:
   - **Device info:** IMEI, MEID, or serial number.
   - **Other info:** (optional) Any other information that you want to include about the device.

**Note:**

The template includes Username and Password columns. If you are using legacy Android Enterprise and users’ Samsung devices are running versions earlier than Knox 3.0, they cannot sign on with their user name and password in Secure Hub. Therefore, you can leave these columns blank.

If you are using Android Enterprise and users’ Samsung devices are running Knox 3.0 or later, optionally you can enter a user name and password. The user name and password would have been provisioned to users for the enterprise MDM setup.

4. Highlight all the cells in the spreadsheet.
5. Right-click the highlighted cells and then select Format cells.
6. On the Number tab, under Category, click Text and then click OK.
7. Save the spreadsheet as a .csv file.

**To enroll devices by using a .csv file**

1. Click the Devices tab.
2. Click **Upload Devices**.

3. In the **Add Devices** dialog box, click **Browse**, select your .csv file and then click **Upload**.

4. Enter your purchase details. The Knox Mobile Enrollment tool verifies your purchase details to ensure that each device is enrolled in the proper enterprise.

5. Under **Assign to Profile**, select the MDM profile that you added.

6. Click **Submit**.

The **All Devices** list displays the enrollment status and profile of all the devices that you attempted to enroll.

For a device to successfully enroll in the enterprise, the device must connect to Wi-Fi and users must agree to download and install Secure Hub.

**To add devices by using scan**

1. Download and install the Knox Mobile Enrollment app from Google Play.

2. Enter your Samsung Portal credentials and then tap **SIGN IN**.

3. Tap **Scan Devices**.

4. Tap **Scan new devices**.

5. Align the barcode of your device with the red line to scan.

6. If the scan succeeds, the device IMEI appears. Tap **Save**.
7. Your scanned devices are shown in the scan queue. Tap **Upload**.

**To enroll scanned devices**

1. Log on to your Knox Web Portal account and click **Launch Mobile Enrollment**.
2. Tap **Scanned** to view all added devices.
3. Select the devices that you want to enroll and then tap **Submit selected**. To submit all scanned devices, tap **Submit all**.
4. In the **Submit scanned devices** pop-up, enter your **Purchase details** to confirm device ownership.
5. In the **Assign MDM profile** menu, select the profile to use for device enrollment and then click **Submit**.

You receive a confirmation email when the device information is verified.

For security reasons, devices are not immediately assigned to this bulk enrollment account. Samsung first must verify that the devices belong to the entity that is setting up the bulk enrollment account.

For that purpose, the next screen prompts for the identity of the reseller and for matching invoices.

---

**Add Devices**

**Device details**

File uploaded: (3 devices)

**Purchase details**

To prevent devices from being incorrectly enrolled with MDMs, Samsung verifies device ownership using your purchase information.

Provide contact details of either a Samsung B2B sales representative or a KNOX reseller who can verify the purchase/ownership of the devices you want to enroll.

- Name of reseller
- Email Address
- Phone Number
- Address
- Customer ID

**Device Information**

**Assign MDM profile**

* MyKXS

**Tags**

Add a tag

Create tags to group and label devices and make them easier to locate.

**Note**

0/200 Characters

---

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Important:
For legal reasons, Samsung maintains two distinct server groups: Americas and EU. U.S. devices must register with a Knox account for the U.S. region. EU devices, as well as devices from any other region except China, which is not supported, must register with a Knox account for the EU region.

A device from the wrong region is accepted into the account, but bulk enrollment fails on the device with a cryptic error. To check whether the device country code or origin is a non-U.S. country, download the simple Phone Info Samsung app from Google Play.

Enrollment experience for users
After the preceding configuration is completed, the first time a user starts a device and connects to the Internet using Wi-Fi, the following sequence of screens appears. The enrollment process starts automatically and users needs to download and install Secure Hub and then enter valid credentials on the Secure Hub screen to complete the enrollment.

Note:
Enrollment doesn’t use a cellular connection to avoid any network costs for the user.

To enroll devices running a Knox API earlier than version 2.4
On devices that have Knox API earlier than version 2.4, bulk enrollment does not work out of the box. Therefore, users must initiate enrollment by going to a Samsung site to download the new Mobile Enrollment client and start the enrollment.

The downloaded enrollment client uses the same MDM profile and APKs configured in the Knox Bulk enrollment portal for the Knox 2.4/2.4.1 devices.

Users typically follow these steps:

1. Turn on the device and connect to Wi-Fi. If the Mobile Enrollment doesn’t start or Wi-Fi is not available, do the following:
   a) Go to Samsung Knox Mobile Enrollment.
   b) Tap the Enroll button to enroll devices with mobile data.

2. When the prompt Enroll with Knox appears, tap Continue.

3. Read the EULAs (if available). Tap Next.

4. If prompted, enter the User ID and Password provided by the IT administrator.

At this point, the user credentials are validated and their device is enrolled in your organization’s enterprise IT environment.
Enable and disable biometric authentication for Samsung devices

 Endpoint Management allows you to enable and disable biometric authentication (fingerprint and iris scan authentication) for Samsung devices without requiring any action from users. If you disable biometric authentication in Endpoint Management, users and third-party apps cannot enable the feature.

1. In the Endpoint Management console, click **Configure > Device Policies**. The **Device Policies** page appears.

2. Click **Add**. The **Add New Policy** page appears.

3. Click **Passcode**. The **Passcode Policy Information** page appears.

4. In the **Policy Information** pane, enter the following information:
   - **Policy Name**: Type a descriptive name for the policy.
   - **Description**: Optionally, type a description of the policy.

5. Click **Next**. The **Platforms** page appears.

6. Under **Platforms**, select **Android** or **Samsung Knox**.

7. Set **Configure biometric authentication** to **ON**.

8. If you selected **Android**, under **Samsung SAFE**, select **Allow fingerprint** or **Allow Iris** or both.

### iOS

November 7, 2019

To manage iOS devices in Endpoint Management, you set up an Apple Push Notification service (APNs) certificate from Apple. For information, see APNs certificates.
Endpoint Management enrolls iOS devices into MDM+MAM mode, with the option for users to register in MAM-only mode. Endpoint Management supports the following authentication types for iOS devices in MDM+MAM mode. For information, see the articles under Certificates and authentication.

- Domain
- Domain plus security token
- Client certificate
- Client certificate plus domain
- Derived credentials
- Identity providers:
  - Azure Active Directory
  - Citrix Identity provider

**Requirements for trusted certificates in iOS 13:**


For help with managing certificates, see [Uploading certificates in Endpoint Management](#).

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](#).

**Apple host names that must remain open**

Some Apple host names must remain open to ensure proper operation of iOS, macOS, and iTunes. 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](https://support.apple.com/en-us/HT201999).

**Supported enrollment methods**

The following table lists the enrollment methods that Endpoint Management supports for iOS devices:
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 Endpoint Management. That program is for iOS, macOS, and Apple TV devices. See Deploy devices through Apple DEP.

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 bulk enroll iOS, macOS, and Apple TV devices. You can purchase those devices directly from Apple, a participating Apple Authorized Reseller, or a carrier. Whether you purchase iOS devices directly from Apple, you can use the Apple Configurator to enroll those devices. See Bulk enrollment of Apple devices.

**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 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 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 you added and then, in the menu that appears, click **Edit**.

   **Note:**
   When you select the check box 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 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 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. Endpoint Management deletes the item immediately.

7. The remaining Device Details sections contain summary information 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 assigned policies including the number of deployed, pending, and failed policies. Provides the policy name, type and last deployed information for each policy.
- 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.

**Configure iOS device policies**

Use these policies to configure how Endpoint Management interacts with devices running iOS. This table lists all device policies available for iOS devices.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirPlay Mirroring</td>
<td>AirPrint</td>
<td>APN</td>
</tr>
<tr>
<td>App Access</td>
<td>App Attributes</td>
<td>App Configuration</td>
</tr>
<tr>
<td>App Inventory</td>
<td>App Lock</td>
<td>App Network Usage</td>
</tr>
<tr>
<td>App Uninstall</td>
<td>Apps Notifications</td>
<td>Calendar (CalDAV)</td>
</tr>
<tr>
<td>Cellular</td>
<td>Contacts (CardDAV)</td>
<td>Control OS Update</td>
</tr>
<tr>
<td>Credentials</td>
<td>Device Name</td>
<td>Education Configuration</td>
</tr>
<tr>
<td>Exchange</td>
<td>Font</td>
<td>Home Screen Layout</td>
</tr>
<tr>
<td>Import iOS &amp; macOS Profile</td>
<td>LDAP</td>
<td>Location</td>
</tr>
<tr>
<td>Lock Screen Message</td>
<td>Mail</td>
<td>Managed Domains</td>
</tr>
<tr>
<td>MDM Options</td>
<td>Organization Info</td>
<td>Passcode</td>
</tr>
<tr>
<td>Personal Hotspot</td>
<td>Profile Removal</td>
<td>Provisioning Profile</td>
</tr>
<tr>
<td>Provisioning Profile Removal</td>
<td>Proxy</td>
<td>Restrictions</td>
</tr>
<tr>
<td>Roaming</td>
<td>SCEP</td>
<td>Shared iPad - Maximum Resident Users</td>
</tr>
<tr>
<td>Shared iPad - Passcode Lock Grace Period</td>
<td>SSO Account</td>
<td>Store</td>
</tr>
<tr>
<td>Subscribed Calendars</td>
<td>Terms &amp; Conditions</td>
<td>VPN</td>
</tr>
<tr>
<td>Wallpaper</td>
<td>Web Content Filter</td>
<td>Webclip</td>
</tr>
<tr>
<td>WiFi</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enroll iOS devices

This section shows how users enroll iOS devices (12.2 or later) into Endpoint Management. For more information about the iOS enrollment, open the following video:

For information about enrollment when using derived credentials, see Device enrollment.

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 Secure Hub installs, tap Open.
4. Enter your corporate credentials, such as your Endpoint Management server name, User Principal Name (UPN), or email address. Then, click Next.
5. Tap Yes, Enroll to enroll your iOS device.
6. After you type your credentials, tap **Allow** when prompted, to download the configuration profile.

   **This website is trying to download a configuration profile. Do you want to allow this?**

   ![Yes, Enroll](image1)
   ![No](image2)

7. After you download the configuration profile, tap **Close**.

   **Profile Downloaded**
   Review the profile in Settings app if you want to install it.

   ![Close](image3)

8. In your device settings, install the iOS certificate and add the device to the trusted list.
   - 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.
9. Sign in to Secure Hub. If you are 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**

iOS supports the following security actions. For a description of each security action, see Security actions.

<table>
<thead>
<tr>
<th>Activation Lock Bypass</th>
<th>App Lock</th>
<th>App Wipe</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASM Activation Lock</td>
<td>Certificate Renewal</td>
<td>Clear Restrictions</td>
</tr>
<tr>
<td>Enable/Disable Lost Mode</td>
<td>Enable/Disable Tracking</td>
<td>Full Wipe</td>
</tr>
<tr>
<td>Locate</td>
<td>Lock</td>
<td>Ring</td>
</tr>
<tr>
<td>Request/Stop AirPlay Mirroring</td>
<td>Restart/Shut Down</td>
<td>Revoke/Authorize</td>
</tr>
<tr>
<td>Selective Wipe</td>
<td>Unlock</td>
<td></td>
</tr>
</tbody>
</table>

**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 Endpoint Management console. Alternatively, users can enable the passcode on the device manually.

1. Click Manage > Devices. The Devices page appears.
2. Select the iOS device you want to lock.

Select the check box 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.

3. In the options menu, click Secure. The Security Actions dialog box appears.
4. Click **Lock**. The **Security Actions** confirmation dialog box displays.

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 Endpoint Management Lost Mode device property puts an iOS device in Lost Mode. Unlike Apple Managed Lost Mode, Endpoint Management Lost Mode doesn’t require a user to perform 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 Endpoint Management Lost Mode, only Endpoint Management can unlock the device. (In contrast, if you use the 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.
If you click **Enable Lost Mode**, type information to appear on the device when it's in lost mode.
Use any of the following methods to check Lost Mode status:

- In the Security Actions window, verify if the button is **Disable Lost Mode**.
- From Manage > Devices, on the General tab under Security, see the last Enable Lost Mode or Disable Lost Mode action.

- From Manage > Devices, on the Properties tab, verify that the value of the **MDM lost mode enabled** setting is correct.
If you enable Endpoint Management Lost Mode on an iOS device, the Endpoint Management console also changes as follows:

- 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 perform 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 perform 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 Endpoint Management MDM Options device policy. You can then manage a device from the 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 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 iTunes account credential, you can bypass that step by issuing the Activation Lock Bypass security action from the Endpoint Management console.

**Device requirements for activation lock bypass**

- Supervised through Apple Configurator or Apple DEP
- Configured with an iCloud account
- Find My iPhone/iPad enabled
- Enrolled in 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**.
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 perform 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 with a generated Activation lock bypass code and with the Activation lock enabled: If you can’t bypass the Activate iPhone/iPad page after a Full Wipe, there is no need to delete the device from Endpoint Management. Either you or the user can contact Apple support to unblock the device directly.
- During a hardware inventory, Endpoint Management queries a device for an Activation lock bypass code. If a bypass code is available, the device sends it to Endpoint Management. Then, to remove the bypass code from the device, send the Activation Lock Bypass security action from the Endpoint Management console. At that point, 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 as follows. On the device, manually enter the credentials of the iCloud account. Or, 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

November 7, 2019

To manage macOS devices in Endpoint Management, you set up an Apple Push Notification service (APNs) certificate from Apple. For information, see APNs certificates.

Endpoint Management enrolls macOS devices into MDM mode.

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 Uploading certificates in Endpoint Management.

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.

Supported enrollment methods

The following table lists the enrollment methods that Endpoint Management supports for macOS devices:

<table>
<thead>
<tr>
<th>Method</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple Deployment Program</td>
<td>Yes</td>
</tr>
<tr>
<td>Apple School Manager</td>
<td>Yes</td>
</tr>
<tr>
<td>Apple Configurator</td>
<td>No</td>
</tr>
<tr>
<td>Manual enrollment</td>
<td>Yes</td>
</tr>
<tr>
<td>Enrollment invitations</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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 Endpoint Management. That program is for iOS, macOS, and Apple TV devices. See Deploy devices through Apple DEP.

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 bulk enroll iOS, macOS, and Apple TV devices. You can purchase those devices directly from Apple, a participating Apple Authorized Reseller, or a carrier.

Configure macOS device policies

Use these policies to configure how Endpoint Management interacts with devices running macOS. This table lists all device policies available for macOS devices.

<table>
<thead>
<tr>
<th>AirPlay Mirroring</th>
<th>App Inventory</th>
<th>Calendar (CalDAV)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts (CardDAV)</td>
<td>Control OS Update</td>
<td>Credentials</td>
</tr>
<tr>
<td>Device Name</td>
<td>Exchange</td>
<td>FileVault</td>
</tr>
<tr>
<td>Firewall</td>
<td>Font</td>
<td>Import iOS &amp; macOS Profile</td>
</tr>
<tr>
<td>LDAP</td>
<td>Mail</td>
<td>Passcode</td>
</tr>
<tr>
<td>Profile Removal</td>
<td>Restrictions</td>
<td>SCEP</td>
</tr>
<tr>
<td>VPN</td>
<td>Webclip</td>
<td>WiFi</td>
</tr>
</tbody>
</table>

Enroll macOS devices

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 modes for macOS devices:
  - User name + password
  - User name + PIN
  - Two Factor

  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. Endpoint Management fills in the user name. If you chose **Two Factor** for the enrollment 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 Macs with Endpoint Management just as you manage mobile devices.
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 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 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 Macs with 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.

<table>
<thead>
<tr>
<th>Certificate renewal</th>
<th>Full Wipe</th>
<th>Lock</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify</td>
<td>Revoke/Authorize</td>
<td>Selective Wipe</td>
</tr>
</tbody>
</table>

Deploy devices through Apple Deployment Program

November 1, 2019

Apple has device enrollment programs for business and education accounts. For business accounts, you enroll in the Apple Deployment Program to use the Apple Business Manager (ABM) or Apple School Manager (ASM) for device enrollment and management in Endpoint Management. That program is for iOS, macOS, and Apple TV devices.

Be aware that the Apple Deployment Program is available for organizations and not individuals. You
Citrix Endpoint Management

must provide a considerable amount of corporate details and information to create an Apple Deployment Program account. Thus, it could take time to request and receive approval for accounts.

For education accounts, you create an Apple School Manager account. ASM unifies the Apple Deployment Program and Apple volume purchase. To create an Apple School Manager account, go to the Apple School site.

If Endpoint Management is integrated with Citrix Workspace, the Workspace App is included in the ABM or ASM deployment package as a required app. To support that feature, Endpoint Management requires that you configure your ABM or ASM account settings for iOS with required credentials set to off.

**Enroll in the Apple Deployment Program**

Go to [deploy.apple.com](http://deploy.apple.com) to apply for an Apple Deployment Program account. When applying for an account, the best practice is to use an email address for the organization, such as deployment@company.com. Follow the steps provided there to enroll for an account.

**Note:**

For education accounts, go to the Apple School site noted in the preceding section.

After you receive your logon credentials from Apple, log in to the Apple Deployment Program Portal.
To connect your account to Endpoint Management, see “Integrate your Apple Deployment Program account with Endpoint Management” in Bulk enrollment of Apple devices.

Order Deployment Program enabled devices

You can order Deployment Program enabled devices directly from Apple or Deployment Program enabled authorized resellers or carriers. To order from Apple, provide your Apple Customer ID in the Apple Deployment Program Portal. Your Customer ID enables Apple to associate your purchased devices with your Apple Deployment Program account.

To order from your reseller or carrier, contact your Apple reseller or carrier to check if they participate in the Apple Deployment Program. Ask for the Apple Deployment Program ID of the reseller when purchasing devices. Apple requires that information when you add your Apple Deployment Program reseller to your Apple Deployment Program account. After you add the Apple Deployment Program ID for the reseller, you receive a Deployment Program customer ID. Provide the Deployment Program customer ID to the reseller, who uses the ID to submit information about your device purchases to Apple. For more information, see this Apple Use Device Enrollment site.

Manage Deployment Program enabled devices

Follow these steps to associate devices with your Endpoint Management server by using the Apple Deployment Program Portal to update your Apple Deployment Program account.

1. Log on to the Apple Deployment Program Portal.

2. Click Device Enrollment Program and then click Device Assignments. In Choose Devices, choose the option for which you want to upload and define your Apple Deployment Program enabled devices: Serial Number, Order Number, or Upload CSV File.
3. To assign your devices to an Endpoint Management server, under **Choose Action**, choose **Assign to Server**. Then, in the list, choose the name of your Endpoint Management server. Click **OK**.
Your Apple Deployment Program devices are now associated with the selected Endpoint Management server.

Endpoint Management displays a **License Expiration Warning** when Apple volume purchase has expired.
Bulk enrollment of Apple devices

You can enroll large numbers of iOS, macOS, and Apple TV devices in Endpoint Management in two ways.

- You can use the Apple Deployment Program to enroll the iOS, macOS, and Apple TV devices that you buy directly from Apple, a participating Apple Authorized Reseller, or a carrier. That support includes Shared iPads. Endpoint Management supports the Apple Deployment Program for Apple Business Manager (ABM) and Apple School Manager (ASM) for Education. This article describes integrating with ABM accounts. For information about Apple School Manager accounts, see Integrate with Apple Education features.

For enrollment of macOS devices, Endpoint Management requires that the devices run macOS 10.10 or later.

- You can also use the Apple Configurator to enroll iOS devices whether you purchased them directly from Apple or not.

**With ABM:**

- You do not have to touch or prepare the devices. Instead, you submit device serial numbers or purchase order numbers through ABM to configure and enroll the devices.
- After Endpoint Management enrolls the devices, you can give them to users who can start using them right out of the box. In addition, when you set up devices with ABM, you can eliminate some of the Setup Assistant steps that users would otherwise have to complete when they first start their devices.
- For more information on setting up ABM, see the documentation available from Apple Business Manager.

**With the Apple Configurator:**

- You attach iOS devices to an Apple computer 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.
- After you provision the devices with the required policies, the first time the devices connect to Endpoint Management, the devices receive policies from Endpoint Management. You can then start managing the devices.
- For more information about using Apple Configurator, see the Apple Configurator Help.
Prerequisites

Open required ports for connectivity between Endpoint Management and Apple. For more information, see Port requirements.

Integrate your Apple Business Manager account with Endpoint Management

If you do not have an ABM account, see Deploy devices through Apple Deployment Program.

To connect your Apple Business Manager account with your Endpoint Management server deployment, you enter information in the Endpoint Management console and the Apple Deployment Program Portal, as described in the following steps.

Step 1: Download a public key from your Endpoint Management server

1. Log on to the Endpoint Management console and go to Settings > Apple Deployment Program.

2. Under Download Public Key, click Download.

Step 2: Create and download a server token file from your Apple account

1. Using your corporate Apple ID, log on to the Apple Deployment Program Portal.
2. In the Apple Deployment Program portal, click Settings, then Device Management Settings. Click Add MDM Server.

3. Type a name for Endpoint Management. The server name that you type is for your reference and is not the server URL or name. Under Upload Public Key, click Choose File.
4. Upload the server key that you downloaded from Endpoint Management and then click **Save**.

5. Generate a server token: Click **Download Token** and then download the server token file to your computer.

6. Under **Default Device Assignment** click **Change**. Choose how you want to assign devices and then provide the information requested. For information, see the ABM User Guide.
Your ABM token information appears in the Endpoint Management console after you import the token file. You upload the server token file when adding the ABM account to Endpoint Management.

**Step 3: Add an ABM account to Endpoint Management**

You can add multiple ABM accounts to 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 accounts with different device policies.

For example, you might centralize all of your ABM accounts from different countries on the same Endpoint Management server, to import and supervise all ABM devices. By customizing enrollment settings and setup assistant options per department, organizational hierarchy, or other structure, you can ensure that policies provide appropriate functionality across your organization and that device users receive the appropriate setup assistance.

1. In Endpoint Management console, go to **Settings > Apple Deployment Program** and, under **Add Apple Deployment Program Account**, click **Add**.

2. In the **Server Tokens** page, specify your server token file and then click **Upload**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Your server token information appears.

3. In the **Account Info** page, specify these settings:
- **Apple Deployment Program account name**: A unique name for this Apple Deployment Program account. Use names that reflect how you organize Apple Deployment Program 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.

4. In **iOS Settings**, specify these settings:

   [Image of iOS Settings settings]

   **Enrollment settings**:

   - **Require device enrollment**: Whether to require users to enroll their devices. The default is *Yes*.

   - **Require credentials for device enrollment**: Whether to require users to enter their credentials during ABM setup. Citrix recommends that you require all users to enter their credentials during device enrollment, thus allowing only authorized users to enroll devices. The default is *Yes*.

     When ABM is on for the first time setup and you don’t select this option, the ABM components, such as ABM user, Secure Hub, software inventory, and ABM deployment group, are created. If you do select this option, 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 perform the ABM enrollment because these ABM components do not exist. To add ABM components, in that case, you should disable and enable the ABM account.

   - **Wait for configuration to complete setup**: Whether to require users’ devices to remain
in Setup Assistant mode until all MDM resources deploy to the device. This is available for devices in supervised mode. The default is **No**.

- Apple documentation states that the following commands may not work while a device is in Setup Assistant mode:
  - `InviteToProgram`
  - `InstallApplication`
  - `ApplyRedemptionCode`
  - `InstallMedia`
  - `RequestMirroring`
  - `DeviceLock`

Device settings:

- **Supervised mode**: Must be set to **Yes** if you are using the Apple Configurator to manage ABM enrolled devices or when **Wait for configuration to complete setup** is enabled. The default is **Yes**. For details on placing an iOS device in supervised mode, see [To place an iOS device in Supervised mode by using the Apple Configurator](#).

- **Allow enrollment profile removal**: Whether to allow devices to use a profile that you can remove remotely. The default is **No**.

- **Allow device pairing**: For devices enrolled through ABM, whether you can manage them through iTunes and the Apple Configurator. The default is **No**.

Supervision Identities

- Add a certificate to support the use of GroundControl. With this certificate, you can do the following:
  - Override pairing restrictions to avoid the “Trust this host” prompt.
  - Escalate managed device actions over USB to perform activities such as profile installation without user interaction. This allows GroundControl to enable single app mode and device lock for checkout.
  - Restore a backup to ABM devices.

For more information on GroundControl, see [The GroundControl website](#).

5. In **macOS Settings**, specify these settings:
Enrollment settings:

- **Require device enrollment**: Whether to require users to enroll their devices. The default is **Yes**.
- **Wait for configuration to complete setup**: If **Yes**, 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 is available for macOS 10.11 and higher devices. The default is **No**.

Device settings:

- **Allow enrollment profile removal**: Whether to allow devices to use a profile that you can remove remotely. The default is **No**.

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 iTunes and the Apple Configurator.
7. In **iOS Setup Assistant Options**, select the iOS Setup Assistant steps that your users will skip when they start their devices the first time. The default for all items is unchecked.

<table>
<thead>
<tr>
<th>Apple deployment program Account</th>
<th>iOS Setup Assistant Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Server Tokens</td>
<td>![Skip setup options]</td>
</tr>
<tr>
<td>2 Account Info</td>
<td>![Skip setup options]</td>
</tr>
<tr>
<td>3 Settings</td>
<td>![Skip setup options]</td>
</tr>
<tr>
<td><strong>iOS</strong></td>
<td>![Skip setup options]</td>
</tr>
<tr>
<td>macOS</td>
<td>![Skip setup options]</td>
</tr>
<tr>
<td>Apple TV</td>
<td>![Skip setup options]</td>
</tr>
<tr>
<td>4 Setup Assistant Options</td>
<td>![Skip setup options]</td>
</tr>
<tr>
<td><strong>iOS</strong></td>
<td>![Skip setup options]</td>
</tr>
<tr>
<td>macOS</td>
<td>![Skip setup options]</td>
</tr>
<tr>
<td>Apple TV</td>
<td>![Skip setup options]</td>
</tr>
</tbody>
</table>

- **Location services**: Set up the location service on the device.
- **Touch ID**: Set up Touch ID on iOS devices.
- **Passcode lock**: Create a passcode for the device.
- **Set up as New or Restore**: Set up the device as new or from an iCloud or iTunes backup.
- **Move from Android**: Enable 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**: Set up an Apple ID account for the device.
- **Terms and conditions**: Require users to accept terms and conditions for use of the device.
- **Apple Pay**: Set up Apple Pay on iOS devices.
Citrix Endpoint Management

- **Siri**: Use or not use Siri on the device.
- **App analytics**: Set up whether to share crash data and usage statistics with Apple.
- **Display zoom**: Set up the display resolution (either standard or zoomed) on iOS devices.
- **True Tone**: Set up the True Tone Display on iOS devices.
- **Home Button**: Set up the Home Button screen sensitivity on iOS devices.
- **New feature highlights**: Set up the onboarding informational screens, Access the Dock from Anywhere and Switch Between Recent Apps on iOS 11.0 devices (minimum version).
- **Privacy**: Prevent users from seeing the data and privacy pane during setup of ABM devices. For iOS 11.3 and later.
- **SoftwareUpdate**: Prevents the user from seeing the mandatory software update screen during setup of the ABM devices. For iOS 12.0 and later.
- **ScreenTime**: Prevents the user from seeing the Screen Time screen during setup of the ABM devices. For iOS 12.0 and later.
- **SIM Setup**: Prevents the user from seeing the Add Cellular Plan screen during setup of the ABM devices. For iOS 12.0 and later.
- **iMessage & FaceTime**: Prevents the user from seeing the iMessage and FaceTime screen during setup of the ABM devices. For iOS 12.0 and later.

The ABM account appears on **Settings > Apple Deployment Program**.

8. In **macOS Setup Assistant Options**, select the macOS Setup Assistant steps that your users skip when they start their devices the first time. The default for all items is unchecked.

- **Set up as New or Restore**: Set up the device as new or from an iCloud or iTunes backup.
- **Location services**: Set up the location service on the device.
- **Apple ID**: Set up an Apple ID account for the device.
- **Terms and conditions**: Require users to accept terms and conditions for use of the device.
Siri: Use or not use Siri on the device.

FileVault: Use FileVault to encrypt the startup disk. Endpoint Management applies the FileVault setting only 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: Set up whether to share crash data and usage statistics with Apple.

Registration: Require users to register their device.

Registration information setup was available through OS X 10.9. The registration process allowed you to send system registration information to Apple. This information associated your contact information with the Mac hardware. Apple primarily used the information to facilitate AppleCare support. If you previously entered an Apple ID, Setup Assistant optionally submitted the registration based on your Apple ID account. If you didn’t enter an Apple ID, you could manually enter your contact information.

Under Local account setup options, specify the settings to create an administrator account, which is required for macOS. Endpoint Management creates the account, using the specified information.

Privacy: Prevent users from seeing the Data and privacy pane during setup of ABM devices. For macOS 10.13 and later.

iCloud Analytics: Prevent users from seeing the iCloud analytics screen during setup of ABM devices. For macOS 10.13 and later.

iCloud Documents and Desktop: Prevent users from seeing the iCloud documents and desktop screen during setup of ABM devices. For macOS 10.13 and later.

Appearance: Prevents the user from seeing the Choose Your Look screen during setup of the ABM devices. For macOS 10.14 and later.

9. In Apple TV Setup Assistant Options, select the Apple TV Setup Assistant steps that your users will skip when they start their devices the first time. The default for all items is unchecked.
10. To test connectivity between Endpoint Management and Apple, select the account and click **Test Connectivity**.
Renew your connection between the Apple Deployment Program and Endpoint Management

If your Automated Device Enrollment server token expires, replace the token from Apple School Manager/Apple Business Manager.

**Step 1: Download a public key from your Endpoint Management server**

1. In the 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 the **Apple Deployment Program Portal** to download the token.
2. Open **Settings** and select the server from which you need a token. Click **Edit**.
3. Upload the new public key you downloaded from Endpoint Management, and save the changes.
4. Click **Download Token** to download the new token.
Step 3: Upload a server token file in Endpoint Management

1. In Citrix Endpoint Management, go to Settings > Apple Deployment Program. Select the Deployment Program account, click Edit, and upload your server token file.
2. Click Next and save the changes.

User experience when enrolling an Apple Deployment Program enabled device

When users enroll an Apple Deployment Program enabled device, their experience is as follows.

1. Users start their Apple Deployment Program enabled device.
2. Endpoint Management delivers the Apple Deployment Program configuration that you configured in the Endpoint Management console to the Apple Deployment Program enabled device.
3. Users configure the initial settings on their device.
4. The device automatically starts the Endpoint Management device enrollment process.
5. If Endpoint Management is integrated with Citrix Workspace, the Workspace App is included in the Deployment Program deployment package as a required app. In that case, Secure Hub prompts users to enroll the device in Citrix Workspace before enrolling in Endpoint Management.
6. Users continue to configure the other initial settings on their device.
7. In the home screen, users might be prompted to sign in to iTunes so that they can download Citrix Secure Hub.

Note:

This step is optional if Endpoint Management is configured to deploy the Secure Hub app using the device-based volume purchase app assignment. In this case, you don’t need to create an iTunes account or use an existing account.
8. Users open Secure Hub and type their credentials. If required by the policy, users might be prompted to create and verify a Citrix PIN.

Endpoint Management deploys any remaining required apps to the device.

**Configure deployment rules of device policies and apps for ABM accounts**

You can associate ABM accounts with different device policies and apps by using the Deployment Rules section under Configure > Device Policies and Configure > Apps. You can specify that a policy or app either:

- Deploys only for a particular ABM account.
- Deploys 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. Therefore, Endpoint Management
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”.

Configure Apple Configurator settings

1. In the Endpoint Management console, go to Settings > Apple Configurator Device Enrollment.

2. Set Enable Apple Configurator device enrollment to Yes.

3. The Enrollment URL to enter in Apple Configurator is a read-only field. This is the URL for the Endpoint Management server that communicates with Apple. Later in these steps, you copy and paste the URL into the Apple Configurator. In Apple Configurator 2, the enrollment URL is
the 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 **Yes**, you must add the configured devices to **Manage > Devices** in 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 not to require credentials for enrollment.

6. Note: If the Endpoint Management server is using a trusted SSL certificate, skip this step. Click **Export anchor certs** and save the certchain.pem file to the macOS keychain (login or System).

7. Start the Apple Configurator and go to **Prepare > Setup > Configure Settings**.

8. In the **Device Enrollment** setting, paste the MDM server URL from step 4 into the **MDM server URL** box in the Configurator.

9. In the **Device Enrollment** setting, copy the Root Certificate Authority and SSL Servers Certificate Authority to the **Anchor** certificates, if Endpoint Management isn’t using a trusted SSL certificate.

10. Use a Dock Connector-to-USB cable to connect devices to the Mac running the Apple Configurator to 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.
11. Click **Prepare**. For more information on preparing devices with the Apple Configurator, see the Apple Configurator help page, **Prepare devices**.

12. In the Apple Configurator, configure the device policies you require.

13. As each device is prepared, turn it on to start the iOS Setup Assistant, which prepares the device for first-time use.

### Renew or update certificates when using the Apple Deployment Program

When the Endpoint Management Secure Sockets Layer (SSL) certificate is renewed, you upload a new certificate in the Endpoint Management console in **Settings > Certificates**. In the **Import** dialog box, in **Use as**, be sure to click **SSL Listener** so that the certificate is used for SSL. After you restart the server, Endpoint Management uses the new SSL certificate. For more information about certificates in Endpoint Management, see **Uploading Certificates in Endpoint Management**.

It is not necessary to reestablish the trust relationship between Apple Deployment Program and Endpoint Management when you renew or update the SSL certificate. You can, however, reconfigure your **DEP** settings at any time by following the preceding steps in this article.

For more information about Apple Deployment Program, see the **Apple documentation**.

### To place an iOS device in Supervised mode by using the Apple Configurator

**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.

1. Install the Apple Configurator from App Store.

2. Connect the iOS device to your Apple computer.

3. Start Apple Configurator. The Configurator shows that you have a device to prepare for supervision.

4. To prepare the device for supervision:
   - Set the **Supervision control** to **On**. Citrix recommends that you choose this setting if you intend to maintain control of the device by reapplying a configuration regularly.
   - Optionally, provide a name for the device.
   - In iOS, click **Latest** for the latest version of iOS that you want to install.

5. When you are ready to prepare the device for supervision, click **Prepare**.
Integrate with Apple Education features

November 1, 2019

You can use Endpoint Management as your mobile device management (MDM) solution in an environment that uses Apple Education. Endpoint Management support includes Apple School Manager (ASM) and Classroom app for iPad. The 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 Endpoint Management, a Managed Apple ID account configured with a new password, and required volume purchase apps and iBooks.

The following video provides a quick tour of the changes you make to ASM and Endpoint Management.

Here are highlights of Endpoint Management support for Apple Education features.
Apple School Manager

ASM is a service that lets you set up, deploy, and manage iOS devices and macOS laptops used in educational institutions. ASM includes a web-based portal that lets IT administrators:

- Assign Apple Deployment Program devices to different MDM servers.
- Purchase volume purchase licenses for apps and iBooks
- Create Managed Apple IDs in bulk. These customized Apple IDs provide access to Apple services such as storing documents in iCloud Drive and enrolling in iTunes courses.

You can add multiple ASM accounts to Endpoint Management. For example, this feature enables you to use different enrollment settings and Setup Assistant options by Education unit or department. You then associate ASM accounts with different device policies.

After you add an ASM account to the Endpoint Management console, Endpoint Management retrieves class and roster information. During device setup, Endpoint Management:

- Enrolls the devices.
- Installs the resources you configured for deployment, such as device policies (Education Configuration, Home screen layout, and so on).
- Also installs both apps and iBooks purchased through volume purchase.

You then provide the preconfigured devices to instructors and students. If a device is lost or stolen, you can use MDM Lost Mode feature to lock and locate 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 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 about Apple Education features, see the Apple Education site and the Apple Education Deployment Guide from the same site.

Prerequisites

- Citrix Gateway
- Endpoint Management configured in MDM+MAM mode. If you already have an Endpoint Management configured in MDM+MAM, you can use it with ASM.
Citrix Endpoint Management

- Apple iPad 3rd generation (minimum version) or iPad Mini, with iOS 9.3 (minimum version)

**Note:**

Endpoint Management doesn’t validate ASM user accounts against LDAP or Active Directory. However, you can connect Endpoint Management to 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 Secure Mail and 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 Citrix Gateway authentication doesn’t support local users (only Active Directory users). Therefore, Endpoint Management deploys only required volume purchase apps and iBooks to instructor and student devices.

**Prerequisites for Shared iPads**

- Any iPad Pro, iPad 5th generation, iPad Air 2 or later, and iPad mini 4 or later
- At least 32 GB of storage
- Supervised

**Configure Apple School Manager and Endpoint Management**

After you purchase iPads from Apple or from Apple Authorized Resellers or carriers: Follow the workflow in this section to set up your ASM account and devices. This workflow includes steps that you perform in the ASM portal and in the Endpoint Management console.

Follow these instructions to configure your integration for any iPads that you use in a one-to-one model (one iPad per student) or for instructor iPads (unshared). To configure Shared iPads, see Configure Shared iPads.

**Step 1: Create your Apple School Manager account and complete the Setup Assistant**

If you plan to upgrade from Apple Deployment Program, see the Apple Support article, Upgrade your institution to ASM. To create your ASM account, go to https://school.apple.com/ 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, 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 ASM User Guide, referenced earlier.

You can customize the Managed Apple ID format for your institution, as described in the ASM User Guide, referenced earlier.

**Important:**

Don’t change Managed Apple IDs after you import ASM information into Endpoint Management.

If you purchased devices through resellers or carriers, link those devices to ASM. For information, see the ASM User Guide, referenced earlier.

### Step 2: Configure Endpoint Management as the MDM Server for Apple School Manager and configure device assignments

The ASM portal includes an MDM Servers tab. You need the public key file from Endpoint Management to complete that setup.

1. **Download the public key for your Endpoint Management to your local computer:** Log on to the Endpoint Management console and go to **Settings > Apple Deployment Program**.

2. **Under Download Public Key,** click **Download** and then save the PEM file.

3. **In the Apple Deployment Program portal,** click **Settings,** then **Device Management Settings.** Click **Add MDM Server.**
4. Type a name for Endpoint Management. The server name that you type is for your reference and is not the server URL or name. Under **Upload Public Key**, click **Choose File**.

5. Upload the server key that you downloaded from Endpoint Management and then click **Save**.

6. Generate a server token: Click **Download Token** and then download the server token file to your computer.
7. Under **Default Device Assignment** click **Change**. Choose how you want to assign devices and then provide the information requested. For information, see the [ASM User Guide](#).

**Step 3: Add the Apple School Manager account to Endpoint Management**

1. In Endpoint Management console, go to **Settings > Apple Deployment Program** and under **Add Apple Deployment Program Account**, click Add.

2. In the **Server Tokens** page, click **Upload** and choose the server token (.p7m) file that you downloaded from the ASM portal. The token information appears.
Notes:

- **Organization ID** is your customer ID for Apple Deployment Program.

- ASM accounts have an **Organization type** of Education and an **Organization version** of v2.

3. In the **Account Info** page, specify the following settings.
- **Apple Deployment Program account name**: A unique name for this Apple Deployment Program account. Use names that reflect how you organize Apple Deployment Program accounts, such as by country or organizational hierarchy.
- **Business/Education unit**: The Education unit or department for device assignment. 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 can call for help during setup. This field is required.
- **Support email address**: An optional support email address available to end users.
- **Education suffix**: Flags the classes for a given ASM Deployment Program account. (The volume purchase suffix flags apps and iBooks for a given volume purchase account.) The recommendation is to use the same suffix for both accounts, ASM Deployment Program and ASM volume purchase.

4. Click **Next**. In **iOS Settings**, specify the following settings.
• **Enrollment settings**
  
  − **Require device enrollment**: Require users to enroll their devices. Change this setting to **No**.
  
  − **Require credentials for device enrollment**: Require users to enter their credentials during Apple Deployment Program setup. For ASM integration with Endpoint Management, this setting is **Yes** by default and can’t be changed. Apple Deployment Program requires credentials for device enrollment.
  
  − **Wait for configuration to complete setup**: Whether to require user devices to remain in Setup Assistant mode until all MDM resources deploy to the device. For ASM integration with Endpoint Management, this setting is **No** by default. According to Apple documentation, the following commands might not work while a device is in Setup Assistant mode:
    * InviteToProgram
    * InstallApplication
    * InstallMedia
    * ApplyRedemptionCode

• **Device settings**
  
  − **Supervised mode**: Place iOS devices in supervised mode. Don’t change the default, **Yes**. For details on placing an iOS device in supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator.
  
  − **Shared mode**: Enable shared mode on iPads. Devices that don’t meet the minimum requirements can’t share.
  
  − **Allow enrollment profile removal**: For ASM integration, allow user to remove the
Citrix Endpoint Management

enrollment profile from the device. Change this setting to **Yes**.

- **Allow device pairing:** For ASM integration, allow device pairing so you can manage them through iTunes and the Apple Configurator. Change this setting to **Yes**.

5. In **iOS Setup Assistant Options**, select the iOS Setup Assistant steps to skip when users start their devices the first time. By default, the Setup Assistant includes all steps. Consider that removing steps from the Setup Assistant simplifies the user experience.

**Important:**

Citrix strongly recommends that you include the **Apple ID** and **Terms & Conditions** steps. Those steps enable instructors and students to provide their new Managed Apple ID passwords and accept the required terms and conditions.

- **Location services:** Set up the location service on the device.
- **Touch ID:** Set up Touch ID on iOS devices.
- **Passcode lock:** Create a passcode for the device.
- **Set up as New or Restore:** Set up the device as new or from an iCloud or iTunes backup.
- **Move from Android:** Enable 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:** Set up an Apple ID account for the device. Citrix recommends that you select the check box to include this step.
- **Terms and conditions:** Require users to accept terms and conditions for use of the device. Citrix recommends that you select the check box to include this step.
- **Apple Pay:** Set up Apple Pay on iOS devices.
- **Siri:** Use or not use Siri on the device.
- **App analytics:** Set up whether to share crash data and usage statistics with Apple.
- **Display zoom**: Set up the display resolution (either standard or zoomed) on iOS devices.
- **True Tone**: Set up the True Tone Display on iOS devices.
- **Home Button**: Set up the Home Button screen sensitivity.
- **New feature highlights**: Set up the onboarding informational screens, Access the Dock from Anywhere and Switch Between Recent Apps on iOS 11.0 devices (minimum version).
- **Privacy**: Prevent users from seeing the data and privacy pane during setup of Apple Deployment Program devices. For iOS 11.3 and later.
- **SoftwareUpdate**: Prevents the user from seeing the mandatory software update screen during setup of the Apple Deployment Program devices. For iOS 12.0 and later.
- **ScreenTime**: Prevents the user from seeing the Screen Time screen during setup of the Apple Deployment Program devices. For iOS 12.0 and later.
- **SIM Setup**: Prevents the user from seeing the Add Cellular Plan screen during setup of the Apple Deployment Program devices. For iOS 12.0 and later.
- **iMessage & FaceTime**: Prevents the user from seeing the iMessage and FaceTime screen during setup of the Apple Deployment Program devices. For iOS 12.0 and later.

6. The account appears on **Settings > Apple Deployment Program**. To test connectivity between Endpoint Management and your ASM account, select the account and click **Test Connectivity**.

A status message appears.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 509
After a few minutes, the user accounts from ASM appear on **Manage > Users** page. Endpoint Management creates local user accounts based on the imported Managed Apple ID for each user. In the following example, the domain name prefix of customized Apple IDs for user accounts is **appleid**.

To find all users for a given ASM account, type the account name in the user search filter.

**Step 4: Configure an Education volume purchase account for Apple School Manager**

In this section, you point Endpoint Management to the volume purchase account that you use to purchase volume purchase licenses for apps and iBooks.

1. To configure an Education volume purchase account for ASM, follow the instructions in **iOS Volume Purchase**. The Add a volume purchase account screen requires that you supply a Company Token. Download your token directly from your Education volume purchase account and paste it into the **Add a Volume purchase account** screen.
2. Wait a few minutes for the volume purchase licenses to import into Endpoint Management.

**Step 5: Add passwords for Apple School Manager users**

After you add an ASM account, Endpoint Management imports classes and users from ASM. Endpoint Management treats classes as local groups and uses the term “group” in the console. If a class has a group name in ASM, Endpoint Management assigns the group name to the class. Otherwise, Endpoint Management uses the source system ID for the group name. Endpoint Management doesn't use the course name for the class name because course names in ASM aren't unique.

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, Endpoint Management doesn’t use a directory server to authenticate these new users.

ASM doesn’t send temporary user passwords to Endpoint Management. You can import them from a CSV file or add them manually. To import temporary user passwords:

1. Obtain 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 Endpoint Management. There is 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 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.
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:
Citrix Endpoint Management

- **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. Endpoint Management requires a Managed Apple ID for authentication.
- **ASM org name**: The name you gave the account in 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).

**Step 6: Optionally add photos of students**

You can add a photo of each student. If the instructors use the Apple Classroom app, the photos appear in this app.

Recommended for photos:

- Resolution: 256 x 256 pixels (512 x 512 pixels on a 2x device)
- Format: JPEG, PNG, or TIFF

To add a photo, go to Manage > Users, select a user, click Edit, and then click Choose image.
Step 7: Plan and add resources and delivery groups to 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:**
  
  Endpoint Management requires that you deploy volume purchase apps as required apps for education users. 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 Citrix Secure Hub app, so there’s no need to deploy it to instructors or students.

- Volume purchase iBooks:

  After Endpoint Management connects to your ASM account, your purchased iBooks appear in the Endpoint Management console, in Configure > Media. The iBooks listed on that page are available to add to delivery groups. 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 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, 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.
To deploy an app only to instructors, select a delivery group that includes only instructors or use the following deployment rule:

1. Deploy this resource by ASM device type only
2. 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.
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:

1. **Limit by user property**
2. **ASM person title**
3. **is equal to**
4. **Instructor**
The following user assignments are for students. The deployment rule is:

1. Limit by user property
2. ASM person title
3. is equal to
4. Student
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 contained in a delivery group.
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**.

**Step 8: 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 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, Endpoint Management sends device policies, apps, and media to the devices.
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 performing 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.

Step 9: Distribute devices

Apple recommends that you host an event so you can distribute devices to instructors and students.
If you don’t distribute pre-enrolled devices, also provide the following to these users:

- 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, Endpoint Management prompts them in the enrollment screen to enroll their device.
2. The user provides their Managed Apple ID and Endpoint Management password used to authenticate to 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, 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).

**Configure Shared iPads**

Multiple students in a classroom can share an iPad for different subjects taught by one or several instructors.

Either you or instructors enroll Shared iPads and then deploy device policies, apps, and media to the devices. After that, students provide their managed Apple ID credentials to sign in to a Shared iPad. If you previously deployed an Education Configuration policy to students, they no longer sign in as an “Other User” to share devices.

Endpoint Management uses two communications channels for Shared iPads: The system channel for the device owner (instructor) and the user channel for the current resident user (student). 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.
Citrix Endpoint Management

- 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, and Restrictions
  Endpoint Management supports only those device policies over the user channel.

When configuring device policies, you specify the deployment channel in the policy setting **Profile scope**.

![Policy Settings](image)

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 instructors. The instructors then distribute the devices to students. If you don't distribute pre-enrolled Shared iPads to instructors: Be sure to provide the instructors with their 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 Endpoint Management server console to add ASM accounts (**Settings > Apple Deployment Program**) with **Shared mode** enabled. For more information, see “Manage ASM accounts for Shared iPads” next.
2. As described in this section, add the required device policies, apps, and media to Endpoint Management. Assign those resources to delivery groups.
3. Have the instructors perform a hard reset on the Shared iPads. The Remote Management screen for enrollment appears.
4. The instructors enroll the Shared iPads. Endpoint Management deploys configured resources to each enrolled Shared iPad. After an automatic restart, instructors can share the devices with students. A sign in page appears on the iPad.
5. A student chooses the class and then enters their Managed Apple ID and temporary ASM (ASM) password. The Shared iPad authenticates to ASM and prompts the student to create an ASM password. For the next sign into the Shared iPad, the student provides the new ASM password.

6. Another student who is sharing the iPad can then sign in by repeating the previous step.

**Manage ASM accounts for Shared iPads**

If you already use Endpoint Management with Apple Education: You have an existing ASM account configured in Endpoint Management for devices that aren’t shared, such as the devices used by instructors. You can use the same ASM and the same Endpoint Management server for both shared and non-shared devices.

Endpoint Management supports these deployment scenarios:

- **A group of Shared iPads per class**
  
  In this scenario, you assign the Shared iPads to a class of students. The iPads stay in the classroom. Instructors who teach different subjects in that class use the same set of iPads.

- **A group of Shared iPads per instructor**
  
  In this scenario, you assign the Shared iPads to an instructor, who uses those iPads for the various classes that they teach.

**Organize Shared iPads into device groups**

ASM 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, per class or per instructor:

- 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 accounts from the Endpoint Management server console, you automatically import groups of Shared iPads (one for each class or instructor):

- 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
Citrix Endpoint Management

Requirements specific to Shared iPads are as follows:

- One ASM 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.

To add an account, go to Settings > Apple Deployment Program.

**Apps for Shared iPads**

Shared iPads support assignment of device-based volume purchase apps. Before deploying an app on a Shared iPad, Endpoint Management sends a request to the Apple volume purchase server to assign volume purchase licenses to 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, Endpoint Management sends a request to the Apple volume purchase server to assign volume purchase licenses to students. To check the volume purchase assignments, go to Configure > Media > iPad and expand Volume Purchase.
Deployment rules forShared 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:

  1. Apple Deployment Program account name
  2. Only
  3. Device Group 1 account

- For the Device Group 2 account, set this deployment rule:

  1. Apple Deployment Program account name
  2. Only
  3. Device Group 2 account

- For the Device Group N account, set this deployment rule:

  1. Apple Deployment Program account name
  2. Only
  3. Device Group N account
To deploy the Apple Classroom app only to instructors (using unshared iPads), filter the resources by ASM shared status with these deployment rules:

1. Deploy this resource regarding ASM shared mode
2. only
3. unshared

Or:

1. Deploy this resource regarding ASM shared mode
2. except
3. shareable
Delivery groups for Shared iPads

For the device group for each instructor:

- Configure one delivery group. For the instructor, assign all the classes that the Education Configuration policy defines.

- That delivery group must include these MDM resources:
Citrix Endpoint Management

- Device policies:
  * Education Configuration
  * 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 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.
After you click **Delete Resident User**, you can specify the user name.
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 shared)
  - Who is logged in to the shared device (ASM logged-in user)
  - All users assigned to the shared device (ASM resident users)

- Filter the device list by its ASM Device Status:

- View details about the user logged in to a Shared iPad, on the Manage > Devices > Logged-in User Properties page.
• See the channel used to deploy resources to instructors 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 (instructor or student).
• 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.

• View the push status for both channels.
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 Endpoint Management. Endpoint Management also uses ASM user identifiers to identify users.

- If you add or change class data in 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 ensure it updates in the Endpoint Management console and then redeploy the policy.

- If you update user properties in the ASM portal, Endpoint Management also updates those properties in the console. However, 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 ASM, complete the following steps to reflect that change in Endpoint Management.

To manage the data:

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 End-
point 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, Endpoint Management also deletes that user from the Endpoint Management console after a fetch.

   You can reduce the interval between 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 that’s enrolled in Apple School Manager DEP**

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 Apple Deployment Program.

Endpoint Management includes an **ASM Activation Lock** security action that enables you to send a lock code to an ASM DEP-enrolled device.

When you use the **ASM Activation Lock** security action, 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 also can 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**.
The properties **ASM escrow key** and **ASM activation lock bypass code** appear in **Device details**.

<table>
<thead>
<tr>
<th>Device details</th>
<th>Security Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 General</td>
<td></td>
</tr>
<tr>
<td>2 Properties</td>
<td>Activation lock bypass code</td>
</tr>
<tr>
<td>3 User Properties</td>
<td>ASM Automated Device Enrollment escrow key</td>
</tr>
<tr>
<td>4 Assigned Policies</td>
<td>ASM Automated Device Enrollment activation lock bypass code</td>
</tr>
<tr>
<td>5 Apps</td>
<td>Activation lock enabled</td>
</tr>
<tr>
<td>6 Media</td>
<td>Hardware encryption capabilities</td>
</tr>
<tr>
<td>7 Actions</td>
<td>Internal storage encrypted</td>
</tr>
<tr>
<td>8 Delivery Groups</td>
<td>Jailbroken/Rooted</td>
</tr>
<tr>
<td>9 iOS Profiles</td>
<td>MDM lock mode enabled</td>
</tr>
<tr>
<td>10 iOS Provisioning Profiles</td>
<td>Passcode compliant</td>
</tr>
<tr>
<td>11 Certificates</td>
<td>Passcode compliant with configuration</td>
</tr>
<tr>
<td>12 Connections</td>
<td>Passcode present</td>
</tr>
<tr>
<td>13 MDM Status</td>
<td>Supervised</td>
</tr>
</tbody>
</table>

The RBAC permission for an ASM Activation Lock is **Devices > Enable ASM Bypass activation lock**.
If you have a Network Access Control (NAC) appliance, such as a Cisco ISE, in your network: You can enable filters in Endpoint Management to set devices as compliant or not compliant for NAC, based on rules or properties. If a managed device in Endpoint Management does not meet the specified criteria, Endpoint Management marks the device as Not Compliant. A NAC appliance blocks non-compliant devices on your network.

For iOS devices, you can deploy the VPN policy and enable a NAC filter to block a VPN connection for devices that have non-compliant apps installed. For details, see iOS NAC configuration, in this article.

In the Endpoint Management console, you select one or more criteria in the list to set a device as not compliant.

Endpoint Management supports the following NAC compliance filters:

**Anonymous Devices:** Checks if a device is in anonymous mode. This check is available if Endpoint Management can’t reauthenticate the user when a device attempts to reconnect.

**Failed Samsung Knox attestation:** Checks if a device failed a query of the Samsung Knox attestation server.

**Forbidden Apps:** Checks if a device has forbidden apps, as defined in an App Access policy. For more information about the App access 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 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, 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 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 a third party using Endpoint Management APIs typically change that property.

Revoked Status: Checks whether the device certificate was 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 a device is still in a managed state, under Endpoint Management control. For example, a device running in MAM mode or an unenrolled device is not managed.

Note:

The Implicit Compliant/Not Compliant filter sets the default value only on devices that Endpoint Management manages. For example, the NAC appliance marks as Not-Compliant any devices that have a blacklisted app installed or are not enrolled. Your network blocks those devices.

iOS NAC configuration

Through policy settings in Citrix Gateway, Endpoint Management supports Network Access Control (NAC) as an endpoint security feature for iOS devices. When you enable NAC, split tunneling becomes possible. You can also enable a NAC filter to block a VPN connection for devices that have non-compliant apps installed. When the VPN connection is blocked, the user cannot access any apps or websites through VPN.

For example, in the App Access Policy, you identify a particular app as Forbidden, or blacklisted. A user installs that app. When the user opens Citrix SSO and tries to connect to the VPN, the connection is blocked. The following error appears: Error while processing request. Contact your administrator.

The configuration requires that you update Citrix Gateway policies to support NAC. In the Endpoint Management console, you enable NAC filters and deploy the VPN device policy. For this feature to
work on devices, users install the Citrix SSO VPN client from the Apple store. For more information on split tunneling, see Configuring Split Tunneling.

The NAC filters supported are:

- Anonymous Devices
- Forbidden Apps
- Inactive Devices
- Missing Required Apps
- Non-Suggested Apps
- Noncompliant Password
- Out of Compliance Devices
- Revoked Status
- Rooted Android and Jailbroken iOS Devices
- Unmanaged Devices

**Prerequisites**

- Citrix Gateway
- Citrix SSO installed on devices

**To update the Citrix Gateway policies to support NAC**

The authentication and VPN sessions policies you configure must be advanced. On your virtual VPN server from a console window, do the following. The IP addresses in the commands and examples are fictitious.

These steps update a Citrix Gateway that’s integrated with an Endpoint Management environment. If you have a Citrix Gateway that’s setup for VPN and not part of the Endpoint Management environment, but can reach Endpoint Management: You can also use these steps.

1. Remove and unbind all classic policies if you are using classic policies on your VPN virtual server.
   To check, type:
   ```bash
   show vpn vserver <VPN_VServer>
   ```
   Remove any result that contains the word Classic. For example: **VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0**
   To remove the policy, type:
   ```bash
   unbind vpn vserver <VPN_VServer> -policy <policy_name>
   ```

2. Create the corresponding advanced session policy by typing the following.
   ```bash
   add vpn sessionPolicy <policy_name> <rule> <session action>
   ```
For example:

```
add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1
```

3. Bind the policy to your VPN virtual server by typing the following.

```
bind vpn vserver _XM_Endpoint ManagementGateway -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_Endpoint ManagementGateway -authnProfile xm_nac_prof
```

8. Check the connection from Citrix 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 obtaining 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"

You should see a similar command as the following example.

```
HTTP/1.1 200 OK
< Server: Apache-Coyote/1.1
< X-Citrix-Device-State: Non Compliant
< Set-Cookie: ACNODEID=181311111; Path=/; HttpOnly; Secure
```

9. When the preceding step is successful, create the web authentication action to Endpoint Management. First, create a policy expression to extract the device ID from the iOS VPN plug-in.

```
add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\',\'&\').VALUE("deviceidvalue")"
```

10. Send the request to Endpoint Management by typing the following. In this example, the Endpoint Management IP is 10.207.87.82.

```
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: 10.207.87.82:4443\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 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 auth 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.

```
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 <webauth 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 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

19. Configure the VPN device policy. For more information on configuring the VPN device policy, see VPN Device Policy

Configure Network Access Control

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The Settings page appears.

3. Select the check boxes for the **Set as not compliant** filters you want to enable.

4. Click **Save**.

**Chrome OS**

August 28, 2019

Endpoint Management support for Chrome OS devices includes the ability to run Chrome OS devices in a public session. A public session doesn’t require a user to sign on and doesn’t have permanent data. Public sessions are useful for libraries, public schools, and other situations where session data isn’t permanent. You can also configure a Chrome OS device in kiosk mode. Kiosk mode locks down a device per user.

To manage Chrome OS devices, Endpoint Management uses a Secure Hub extension installed in the Chrome device browser. Before enrolling Chrome OS devices in Endpoint Management, you configure G Suite to install the Secure Hub extension on the device. Then, you connect G Suite to Endpoint Management.
Endpoint Management enrolls Chrome OS devices into MDM. Endpoint Management doesn’t support MAM-only registration for Chrome OS devices. Endpoint Management supports user name and password authentication on Chrome OS devices.

A general workflow for starting Chrome OS 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 G Suite to install Secure Hub on the Chrome OS device.
5. Configure Chrome OS device policies.
6. Enroll Chrome OS devices in G Suite and then Enroll Chrome devices in Endpoint Management.

For supported operating systems, see [Supported device operating systems](#).

**Supported enrollment methods**

The following table indicates the enrollment methods that Endpoint Management supports for Chrome OS devices:

<table>
<thead>
<tr>
<th>Method</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulk enrollment</td>
<td>No</td>
</tr>
<tr>
<td>Manual enrollment</td>
<td>Yes (user name + password only)</td>
</tr>
<tr>
<td>Enrollment invitations</td>
<td>No</td>
</tr>
</tbody>
</table>

For more information, see the G Suite configuration sections in this article.

**Configure G Suite to install Secure Hub on the Chrome OS device**

You configure forced installation of the Secure Hub extension on the Chrome OS device and prevent the extension from being disabled or deleted.

1. Go to [https://admin.google.com](https://admin.google.com) and log in to your G Suite account.
2. Verify that you have completed the configuration that’s described in [Enable partner access for devices and users in your G Suite domain](#).
3. In the Google administrator console, click **Device Management**.
4. Click **Chrome management**.

5. In the Chrome device management page, click **User Settings**.
6. In the User settings page, search for **Client certificates**. Add this pattern:

   ```json
   { "pattern": "https://[*.]xm.cloud.com", "filter": { } }
   ```

   When you add this pattern to Client certificates, device certificates pushed from Endpoint Management to the device are auto-selected. The user isn't prompted to select certificates.

7. Click **Save**.

8. Search for **Force-installed Apps and Extensions** and then click **Manage force-installed apps**.
9. Click **Specify a Custom App**.

10. Click the **ID** field, type `cnkimbkgdakemjcipljhmoplehfcjban`.

11. Click the **URL** field, type `https://chrome.google.com/webstore/detail/cnkimbkgdakemjcipljhmoplehfcjban`.
12. Click Add.

13. Click Save in the Force-installed Apps and Extensions dialog window.

14. Click Save in the User Settings page.

**Connect Endpoint Management to G Suite**

1. In the Endpoint Management console, click the gear icon in the upper-right corner and then click Settings > Google Chrome.

2. Click Connect. A Google account sign-in window appears.
3. Sign in with your Google account credentials and click Next.

4. Endpoint Management fills in your G Suite domain and G Suite account administrator name. The Connect button has changed to Disconnect. Endpoint Management is connected to G Suite.
Configure Chrome OS device policies

Use these policies to configure how Endpoint Management interacts with devices running Chrome OS. This table lists all device policies available for Chrome OS devices.

<table>
<thead>
<tr>
<th>App Restrictions</th>
<th>Scheduling</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control OS Update</td>
<td>Kiosk</td>
<td>Managed Bookmarks</td>
</tr>
<tr>
<td>Power Management</td>
<td>Public Session</td>
<td>Restrictions</td>
</tr>
<tr>
<td>Verified Access</td>
<td>VPN</td>
<td>WiFi</td>
</tr>
</tbody>
</table>

Enroll Chrome OS devices in G Suite

Device enrollment in your G Suite domain is a pre-requisite for enrolling a Chrome OS device in Endpoint Management. For information on G Suite domain enrollment, see the Google article, Enroll Chrome devices.

Enroll Chrome devices in Endpoint Management

A Citrix PIN must be created when a Chrome OS device is enrolled in Endpoint Management. The Citrix PIN is separate from the Endpoint Management passcode. The Citrix PIN secures a certificate from the Endpoint Management server. This PIN cannot be reset. If a user forgets this PIN, the Chrome OS device must be unenrolled and re-enrolled.

1. Sign in to your Chrome OS device by using your G Suite credentials.
2. Click the Secure Hub extension in Chrome. The Secure Hub extension appears next to your browser address bar, is grayed out, and looks like the following image:

![Secure Hub Extension](image)

3. The Secure Hub enrollment window appears. Click **Enroll**.

![Secure Hub Enrollment Window](image)

4. Type your corporate credentials, such as your Endpoint Management server name, User Principal Name (UPN), or email address. Then, click **Next**.
5. If prompted, type your corporate user name. Type your corporate password. Then, click **Sign In**.
6. Create a Citrix PIN. This PIN must be 6 characters long. It can contain only letters and numbers. Type your Citrix PIN twice and then click Finish.
When the enrollment is complete, the Secure Hub extension icon is active.

**Sign in to an enrolled Chrome OS device**

To sign in to a Chrome OS device that is enrolled in Endpoint Management:

2. When prompted, enter your Citrix PIN. This PIN was created when the device was enrolled in Endpoint Management.

If you do not type your Citrix PIN:

- You are prompted to type your Citrix PIN every minute until you type the PIN.
- After five minutes, access is blocked to all websites except google.com, citrix.com, gotomeeting.com, cloud.com.
- If you try to access any other website, an error message appears and you are prompted to sign in using your Citrix PIN.
Unenroll and reenroll a Chrome OS device

To unenroll a Chrome OS device from Endpoint Management, users delete their account.

1. In the Chrome browser, click the Secure Hub extension icon.
2. In the Secure Hub enrollment window, click Delete.
3. Click Yes, Delete to confirm the deletion.

The Secure Hub enrollment window closes and the Secure Hub extension icon is grayed out.

To re-enroll:

1. Log out of your Chrome OS device and log back in using your G Suite credentials.
2. Click Enroll and follow the prompts to re-enroll.

Security actions

Chrome OS doesn’t support security actions.

Windows Desktop and Tablet

December 17, 2019

To manage Windows 10 Desktop and Tablet devices in Endpoint Management, you must configure the Citrix AutoDiscovery Service. See Prepare to enroll devices and deliver resources.

Endpoint Management enrolls Windows 10 Desktop and Tablet devices into MDM mode. Endpoint Management supports the following authentication types for Windows Desktop and Tablet devices in MDM+MAM mode. For information, see the articles in the section, Certificates and authentication.

- Domain
- Domain plus security token
- Client certificate
- Client certificate plus domain
- Identity providers:
  - Azure Active Directory
  - Citrix Identity provider

A general workflow for starting Windows 10 Desktop and Tablet 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 Windows Desktop and Tablet 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 Endpoint Management supports for Windows Desktop and Tablet devices:

<table>
<thead>
<tr>
<th>Method</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Active Directory enrollment</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows bulk enrollment</td>
<td>Yes</td>
</tr>
<tr>
<td>Manual enrollment</td>
<td>Yes</td>
</tr>
<tr>
<td>Enrollment invitations</td>
<td>No</td>
</tr>
</tbody>
</table>

**Azure enrollment**

Devices running Windows 10 Enterprise can enroll with Azure as a federated means of Active Directory authentication. This setup requires an Azure Active Directory Premium subscription.

You can join Windows 10 devices to Microsoft Azure AD in any of the following ways:

- Enroll in MDM as part of Azure AD Join setup the first time the device is powered on.
- Enroll in MDM as part of Azure AD Join from the Windows Settings page after configuring the device.
- Enroll in MDM as part of Azure AD Join when you add a work account on a personal device.

Before Windows device users can enroll by using Azure, you must configure the Microsoft Azure server settings in Endpoint Management. For details, see Single sign in with Azure Active Directory.

For Windows devices that you enroll with Azure, you can use Windows AutoPilot to set up and pre-configure the devices. See Use Windows AutoPilot to set up and configure devices.
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 Desktop and Laptop devices. For information, see Bulk enrollment of Windows devices.

Device management when integrated with Workspace Environment Management

With Workspace Environment Management (WEM) alone, MDM deployments aren’t possible. With Endpoint Management alone, you’re limited to managing Windows 10 devices. By integrating the two, WEM has access to MDM features and you can manage a wider spectrum of Windows operating systems through 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 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 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 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.

Configure Windows Desktop and Tablet device policies

Use these policies to configure how Endpoint Management interacts with desktop and tablet devices running Windows 10. This table lists all device policies available for Windows desktop and tablet devices.

<table>
<thead>
<tr>
<th>App Configuration</th>
<th>App Inventory</th>
<th>App Lock</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Uninstall</td>
<td>Application Guard</td>
<td>BitLocker</td>
</tr>
<tr>
<td>Control OS Update</td>
<td>Credentials</td>
<td>Custom XML</td>
</tr>
<tr>
<td>Defender</td>
<td>Device Guard</td>
<td>Device Health Attestation</td>
</tr>
<tr>
<td>Exchange</td>
<td>Firewall</td>
<td>Kiosk</td>
</tr>
</tbody>
</table>
Enroll Windows desktop and tablet devices by using Azure Active Directory

1. Sign on to a Windows Enterprise edition computer. Open Settings > Accounts > Access work or school and then click Connect.
2. From Set up a work or school account, under Alternative actions, click Join this device to Azure Active Directory.
3. Provide your Azure Active Directory credentials and then click Sign in.
4. Accept the Terms and Conditions set by your organization.
5. Click Join to proceed with the enrollment process.
6. Click Done to complete the enrollment process.

Enroll Windows devices by using the AutoDiscovery service

Note:
For Windows devices to enroll, the SSL listener certificate must be a public certificate. Enrollment fails for self-signed SSL certificates.

1. On the device, check for and install all available Windows Updates.
2. In the charms menu, tap Settings and then tap Accounts > Access work or school > Connect to work or school.
3. Enter your corporate email address and then tap Continue.

To enroll as a local user, enter a nonexistent email address with the correct domain name (for example, foo@mydomain.com). That step lets you bypass a known Microsoft limitation where the built-in Device Management on Windows performs enrollment. In the Connecting to a service dialog box, enter the user name and password associated with the local user. The device then discovers an Endpoint Management server and starts the enrollment process.
4. Enter your password. Use the password associated with an account that is part of a user group in Endpoint Management.

5. In the Terms of use dialog box, indicate that you agree to have your device managed and then tap Accept.

To enroll Windows devices without self-discovery (for test environments only)

A best practice for production deployments is to enroll Windows devices by using the AutoDiscovery service. Citrix recommends enrolling Windows devices without self-discovery only in test environments and proof of concept deployments. Enrollment without the AutoDiscovery service results in a call to port 80 when connecting.

1. On the device, check for and install all available Windows Updates.

2. In the charms menu, tap Settings and then tap Accounts > Access work or school > Connect to work or school.

3. Enter your corporate email address.

4. In the Enter server address field, type the address:
   - For commercial: https://url.xm.cloud.com:8443/zdm/wpe
   - For government: https://url.cem.cloud.us:8443/zdm/wpe

   If a port other than 8443 is used for unauthenticated SSL connections, use that port number in place of 8443 in this address.

5. Type your password.

6. In the Terms of use dialog box, indicate that you agree to have your device managed and then tap Accept.

Security actions

Windows 10 Desktops and Tablets support the following security actions. For a description of each security action, see Security actions.

<table>
<thead>
<tr>
<th>Locate</th>
<th>Lock</th>
<th>Reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revoke</td>
<td>Selective Wipe</td>
<td>Wipe</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
**BitLocker recovery key**

Encrypting disks using BitLocker is a useful security feature, but unlocking devices can be a challenge if the user loses their BitLocker recovery key. 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 Endpoint Management console, navigate to Settings > Server Properties.
2. Search for `shp` and enable the `shp.console.enable` feature. Ensure that `enable.new.shp` remains disabled. For more information on enabling the Self-Help Portal, see *Configure Enrollment Modes*.
3. Navigate to Configure > Device policies. Find your BitLocker policy or create one and enable the **BitLocker Recovery backup to 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.
   - **Recovery key**: The key the 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.

Windows Phone

September 30, 2019

Note:

If you use Microsoft Intune/EMS, this article doesn’t apply to your setup. See Citrix Endpoint Management integration with Microsoft Intune/EMS.

Microsoft moved Windows Phone 8.1 devices to End of Support on July 11, 2017. Endpoint Management supports Windows Phone 8.1 devices for MDM enrollment only.

To manage Windows 10 Phone devices in Endpoint Management, you can configure the Citrix AutoDiscovery Service. See Prepare to enroll devices and deliver resources.

Endpoint Management enrolls Windows 10 Phone devices into MDM mode. Endpoint Management supports the following authentication types for Windows Phone devices in MDM+MAM mode. For information, see the articles in the section, Certificates and authentication.

- Domain
- Domain plus security token
- Client certificate
- Client certificate plus domain
- Identity providers:
  - Azure Active Directory
  - Citrix Identity provider

A general workflow for starting Windows 10 Phone 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 Windows Phone device policies.
4. Enroll Windows Phone devices.
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 Endpoint Management supports for Windows Phone devices:

<table>
<thead>
<tr>
<th>Method</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Active Directory enrollment</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows bulk enrollment</td>
<td>No</td>
</tr>
<tr>
<td>Manual enrollment</td>
<td>Yes</td>
</tr>
<tr>
<td>Enrollment invitations</td>
<td>No</td>
</tr>
</tbody>
</table>

**Azure enrollment**

Devices running Windows 10 Enterprise can enroll with Azure as a federated means of Active Directory authentication. This setup requires an Azure Active Directory Premium subscription.

You can join Windows 10 devices to Microsoft Azure AD in any of the following ways:

- Enroll in MDM as part of Azure AD Join setup the first time the device is powered on.
- Enroll in MDM as part of Azure AD Join from the Windows Settings page after configuring the device.
- Enroll in MDM as part of Azure AD Join when you add a work account on a personal device.

Before Windows device users can enroll by using Azure, you must configure the Microsoft Azure server settings in Endpoint Management. For details, see Single sign in with Azure Active Directory.

**Configure Windows Phone device policies**

Use these policies to configure how Endpoint Management interacts with phone devices running Windows 10. This table lists all device policies available for Windows 10 Phone devices.
Enroll Windows Phone devices by using Azure Active Directory

1. Sign on to a Windows Enterprise edition computer. Open Settings > Accounts > Access work or school and then click Connect.
2. From Set up a work or school account, under Alternative actions, click Join this device to Azure Active Directory.
3. Provide your Azure Active Directory credentials and then click Sign in.
4. Accept the Terms and Conditions set by your organization.
5. Click Join to proceed with the enrollment process.
6. Click Done to complete the enrollment process.

Enroll Windows Phone devices

To enroll Windows Phone devices in Endpoint Management, users need their Active Directory or internal network email address, and password. If AutoDiscovery is not set up, users also need the server web address for the Endpoint Management server. Then, they follow this procedure on their devices to enroll.

Note:

If you plan to deploy apps through the Windows Phone company store: Before your users enroll, configure an Enterprise Hub device policy. In that policy, you upload a signing certificate from DigiCert and a signed Citrix Company Hub app.

1. On the main screen of the Windows phone, tap the Settings icon.
2. Depending on your version, either tap Accounts > Access work or school > Connect to work or school or tap Accounts > Work access > Enroll in to device management.
3. On the next screen, enter an email address and password and then tap **sign in**.

   If AutoDiscovery is configured for your domain, the information requested in the next several steps is automatically populated. Proceed to the last step in this procedure.

   If AutoDiscovery is not configured for your domain, continue with the next step. To enroll as a local user, enter a non-existent email address with the correct domain name (for example, `foo@mydomain.com`). Using a non-existent address permits you to bypass a known Microsoft limitation. In the **Connecting to a service** screen, enter the user name and password associated with the local user.

4. On the next screen, type the web address of the Endpoint Management server, such as: `https://<xenmobile_server_fqdn>:<enrollment_port>/<instance_name>/wpe`. For example, `https://mycompany.mdm.com:8443/zdm/wpe`.

   **Note:**
   The port number must be the same port that you used for an iOS enrollment.

5. If authentication is validated through a user name and domain, type the user name and domain and then tap **sign in**.

6. If a message indicates a problem with the certificate, the error is the result of using a self-signed certificate. If the server is trusted, tap **continue**. Otherwise, tap **Cancel**.

7. To force a connection to the server, tap the refresh icon. If the device does not manually connect to the server, Endpoint Management attempts to reconnect.

   Endpoint Management connects to the device every three minutes for five successive times, then every two hours afterward. You can alter this connection rate in the **Windows WNS Heartbeat Interval** located in **Server properties**.

   Once enrollment is complete, Secure Hub enrolls in the background. No indicator appears when the installation is complete. Tap Secure Hub from the **All Apps** screen.

### Security actions

Windows 10 Phone devices support the following security actions. For a description of each security action, see Security actions.

<table>
<thead>
<tr>
<th>Locate</th>
<th>Lock</th>
<th>Lock and Reset Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot</td>
<td>Revoke</td>
<td>Ring</td>
</tr>
<tr>
<td>Selective Wipe</td>
<td>Wipe</td>
<td></td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Bulk enrollment of Windows devices

August 26, 2019

Endpoint Management supports bulk enrollment of Windows 10 devices. With bulk enrollment, you can set up many devices for an MDM server to manage without the need to reimage devices. You can use the provisioning package for bulk enrollment for Windows 10 desktop devices. Follow steps in this article to set up and perform bulk enrollment.

Before running bulk enrollment, ensure that all devices are assigned to the correct end-user. Perform this assignment by registering the devices per user or by performing a bulk import of devices.

Note:
For information on configuring the tool, building a provisioning package, and installing a provisioning package, see https://docs.microsoft.com/en-us/windows/client-management/mdm/bulk-enrollment-using-windows-provisioning-tool. For information on including Endpoint Management bulk enrollment configuration settings, see the section Create and apply a provisioning package for on-premises authentication in that document.

Assign devices

If you prefer to assign devices in bulk, skip to Add devices in bulk.

1. In the Endpoint Management console, navigate to Manage > Device Whitelist.
2. To add each device manually, click **Add**.

3. Type the following information:
   - **Device platform**: Select **Windows**.
   - **Device ID Type**: Select an ID to use to identify the device. Endpoint Management supports **Hardware ID** and **Device Name** for Windows devices.
   - **Device ID**: Type the identification selected previously for the device.
   - **Associated User**: Displays the associated user for this device.
   - **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 Endpoint Management console, navigate to **Manage > Device Whitelist**.
2. Click **Import**.

   ![Import Whitelist Devices](image)

   3. Click **Download** to download a template for the device whitelist. Fill out that template using the previous descriptions, and then upload the file using **Choose File** and **Import**.

**Bulk enroll devices**

1. In the Endpoint Management console, navigate to **Settings > Windows Bulk Enrollment**.
2. In the **UPN** box, type a valid user name to use to deploy all devices.
3. Click **Save**.

4. 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 Endpoint Management bulk enrollment configuration settings so that devices automatically enroll into Endpoint Management.

**Workspace hub device management**

October 8, 2019

Citrix Ready workspace hub devices let users move virtual app and desktop sessions from a mobile device running Citrix Workspace app to a Citrix Ready workspace hub. The Citrix Ready workspace hub is a Raspberry Pi device that has a keyboard, mouse, monitor, and any other accessory attached to it. You can manage Citrix Ready workspace hub devices from your Endpoint Management console. For more information about Citrix Ready workspace hub, see [Citrix Ready workspace hub](#) and this [Citrix blog post](#).

By using Endpoint Management to manage Citrix Ready workspace hub, you can keep your devices updated with the latest features and security patches. You can also perform security actions, such as full wipes or restarts. For more details about the unified endpoint management (UEM) and data protection benefits of Endpoint Management, see this [use case on the Citrix website](#).
A general workflow for the workspace hub device management is as follows:

1. Complete the onboarding process. See Onboarding and resource setup and Prepare to enroll devices and deliver resources.

2. Add Citrix Ready workspace hubs to the Device Whitelist table in the Endpoint Management Console, using either of the following methods:
   - To add Citrix Ready workspace hubs to Endpoint Management manually
   - To import or export Citrix Ready workspace hub devices in bulk

3. Configure a Citrix Ready workspace hub.

4. Deploy custom configurations to Citrix Ready workspace hub devices.

5. Deploy the Citrix Workspace configuration to Citrix Ready workspace hub devices.

6. Configure Citrix Ready workspace hub device policies.

7. Deploy and update apps for Citrix Ready workspace hub.


For supported operating systems, see Supported device operating systems.

To add Citrix Ready workspace hubs to Endpoint Management manually

To enroll a Citrix Ready workspace hub in Endpoint Management, you can manually add the device to the Device Whitelist table in the Endpoint Management console.

A workspace hub device must enroll from the same region where Citrix Endpoint Management is located. For example, if your home region is European Union, the device must enroll while in that region. After a workspace hub device enrolls from your home region and the device roams to a different geographical region, workspace hub works as usual.

If a workspace hub device has to enroll when outside of the home region, the Service URL will contain an incorrect home region. You can change the Service URL in the Stratodesk configuration to point to the correct home region, as follows.

1. On the Stratodesk system: Go to Services > NoTouch Center > Central Management URL.

2. Change the Management URL to include the URL for your home region.
   - Asia Pacific South (Asia, Australia/Pacific, Middle East): manageiot-apse.xm.cloud.com
   - European Union: manageiot-eu.xm.cloud.com
   - United States (Africa, Antarctica, Caribbean, Central America, North America, South America): manageiot-us.xm.cloud.com

3. Save the configuration.
4. Go to **Information > NoTouch Center** and then click **Announce**.

For example, if your home region is in the U.S. and the Workspace hub device has to enroll while in the U.K.: Change the Service URL in Stratodesk from https://manageiot-eu.xm.cloud.com:443/easyadmin/servlet/XmlRPC to https://manageiot-us.xm.cloud.com:443/easyadmin/servlet/XmlRPC.

**Prerequisite**

The configuration steps in this section include specifying a domain for Citrix Ready workspace hub users. Workspace hub uses email-based management server lookup. The lookup requires that you create a DNS SRV record named \_tcmgr\_tcp.mycompany.com, where mycompany.com is your domain name.

For more information, see the NComputing documentation article, *E-mail based management server lookup*.

**To add a device to the Device Whitelist table**

1. In the Endpoint Management console, navigate to **Manage > Devices**.

![Endpoint Management console](image)

2. Click **Device Whitelist** at the top.
3. Click Add. On the page that opens, type the following information.

- **Device platform**: Select Workspace Hub.
- **Device ID Type**: Select the method to identify devices. Citrix Ready workspace hub only supports **MAC address**. For the device registration process, the eth0 MAC address is used, regardless of which connection type you choose.
- **Device ID**: Type the appropriate identifier you selected previously.
- **Associated User**: User to associate with the Citrix Ready workspace hub. The user associated with the device can be a pseudo user, such as a service account. The selected user is used for enrollment, policy pushing, and applying security actions. A single user can associate with multiple devices. This user can be a Local user or LDAP user already configured in your Endpoint Management console. If you want to associate the Citrix Ready workspace hub with a local user, choose **Local** from **Select domain**. Enter the user name in **Search for user** and select the user. If you want to associate the Citrix Ready workspace hub with an LDAP user, choose the appropriate domain from **Select domain**. Search for a user in **Search for user** and select the user.
- **Select domain**: Select the domain to use when searching for users.
- **Search for user**: Type the user name you want to associate with this device and click **Search**. Select the user from the result box. The user appears in the **Associated User** box.
4. Click **Save**. The device is added to the table.

**To import or export Citrix Ready workspace hub devices in bulk**

To enroll a Citrix Ready workspace hub in Endpoint Management, you can import or export the devices in bulk to the Device Whitelist table.

1. In the Endpoint Management console, navigate to **Manage > Devices**. Click **Device Whitelist** and then click **Import**.

2. Click **Download** to download a .csv template for importing devices. The columns in the file are the same as the fields in the previous workflow.

3. Fill out the form and save it. When finished, click **Choose File** and select the template.
4. Click **Import**. All Citrix Ready workspace hubs in the template file are added to the table.

5. To export the list of Citrix Ready workspace hubs for editing, click **Export**.

**Configure a Citrix Ready workspace hub**

After configuring Endpoint Management to enroll your Citrix Ready workspace hub devices, configure the workspace hub device itself. For more information on configuring the device, see the Stratodesk Knowledge Base.

For first-time device use, configure Central Management during the first time wizard. Enter https://manageiot.xm.cloud.com:443/easyadmin/servlet/XmlRPC as the **Management URL** and then click **Finish**. The device performs an Announce and enrolls in Endpoint Management.
If the device was configured, or if you don't want to use the wizard, navigate to Services > No Touch Center. Configure the Management URL as you did previously and Save. Do a manual Announce by navigating to Information on the left pane and clicking Announce.
Deploy custom configurations to Citrix Ready workspace hub devices

You can deploy custom configurations to Citrix Ready workspace hub devices. After manually configuring your first workspace hub device, you then download the configuration from the device and deploy the configuration to all other devices.

Requirements:

- Workspace hub device running Stratodesk NoTouch OS v2.40.3512 (minimum version)

To set up and deploy custom configurations:

1. Configure your Citrix Ready workspace hub device and download the configuration file.
   a) Log in to the Workspace Hub console from a remote machine.
   b) Set up network shares, printer configuration, and any other settings you want shared across devices on your Citrix Ready workspace hub device.
   c) In the left pane of your workspace hub console, click **Download config**.
   d) The .config file downloads to the remote machine where you’re logged in.

2. Host the configuration file on a file sharing web server. Ensure that the file share isn’t protected with any authentication.

3. On your Endpoint Management console, navigate to **Configure > Device Policies** and select **Import Device Configuration**.
4. Type a **Policy Name** and, optionally, a **Description**. Click **Next**.

5. Paste the URL for the configuration file and click **Next**.

6. Configure your deployment rules. For information on configuring those rules, see **Device policies**. Click **Save**.

7. Within a few minutes after the policy pushes to devices, enrolled devices show the configured settings. Those settings include network shares, desktop wallpapers, and connections.

   If the device doesn’t reflect the configuration, check the configuration URL in your Citrix Ready workspace hub device console. Navigate to **Services > NoTouch Center**. Then confirm that the **Configuration archive URL** is the URL where you hosted the configuration file.

**To manage Citrix Ready workspace hub devices**

1. To view and manage Citrix Ready workspace hubs in Endpoint Management after enrollment, navigate to **Manage > Devices**. The **Devices** table appears. Select **Workspace Hub** on the left to see the newly enrolled device. Choose the Citrix Ready workspace hub you want to manage, and then click **Edit** to view and confirm the device details.

   When you select the check box 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.
2. The **General** page lists device **Identifiers** for the platform type, such as the serial number, ActiveSync ID, and other information. 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.

3. The remaining **Device Details** sections contain summary information for the device.

   - **Assigned Policies**: Displays the number of assigned policies including the number of deployed, pending, and failed policies. Provides the policy name, type and last deployed information for each policy.
   - **Apps**: Displays the apps that are installed, pending, or failed.
   - **Delivery Groups**: Displays the number of successful, pending, and failed delivery groups. For each deployment, provides the delivery group name and deployment time.

You can also perform security actions, such as full wipe or restart. For more information on security actions, see **Security actions**.

**Deploy the Citrix Workspace configuration to Citrix Ready workspace hub devices**

Use the App Configuration device policy to deploy the Citrix Workspace configuration to Citrix Ready workspace hub devices. Go to **Configure > Device Policies**, add the **App Configuration** policy, and, under **Platforms**, select **Workspace Hub**. Configure the following Workspace Hub settings:

   - **Connection Mode**: Select **Citrix Receiver**.
   - **Connection Name**: Type a descriptive name for your connection.
   - **Connection Target**: Type a URL to load upon connection.
Some apps might require extra parameters to function. For each configuration parameter you want to add, click **Add** and then do the following:

- **Parameter name**: Type the key name of an application setting for the Citrix Ready workspace hub device.
- **Value**: Type the value for the specified parameter.

After you complete the configuration, choose delivery groups. For more information, see **Device policies**.

### Configure Citrix Ready workspace hub device policies

Use these policies to configure how Endpoint Management interacts with the workspace hub devices. This table lists all device policies available for Citrix Ready workspace hub devices.

<table>
<thead>
<tr>
<th>App Configuration Policy</th>
<th>Credentials</th>
<th>Import Device Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control OS Update</td>
<td>WiFi</td>
<td></td>
</tr>
</tbody>
</table>

### Deploy and update apps for Citrix Ready workspace hub

1. Because Citrix Ready workspace hub devices only allow for deploying and updating a single file, first package all of your apps into a Squash FS file.

   For more information on creating a Squash FS file, see the Squash FS documentation.
Note: When creating the file, ensure that you output an .img file.

2. In the Endpoint Management console, navigate to Configure > Apps and click Add. Click Enterprise.

3. Type a name and description for your app, and then deselect all platforms except Workspace Hub. Click Next.

4. On the Workspace Hub Enterprise App page, click Upload. Navigate to the .img file you created previously and click Open.

5. Click Next. The Approvals page does not function for Citrix Ready workspace hub.

6. Click Next. The Delivery Group Assignment page appears.

7. 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.

Note: Apps are always delivered to the device assigned to the delivery group. It doesn’t matter whether the app is optional or required because there is no store for Citrix Ready workspace hub devices.

8. Click Save.

After the apps upload to Endpoint Management, the workspace hub devices receive the update when restarted.
Security actions

Workspace hub supports Full Wipe and Restart security actions. For a description of each security action, see Security actions.

Device policies

September 4, 2019

You can configure how 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 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): When you configure Endpoint Management device policies for Windows 10, keep the following
Citrix Endpoint Management

Keep this rule in mind. If a policy on one or more enrolled Windows 10 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 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.
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.

To add a policy:

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 remains in the results. Click it to open the **Policy Information** page for that policy.

3. Select the platforms 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.

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 containing 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 containing 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 **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 would like.

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.

![Delivery groups to receive app assignment](image)

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 **On**.

   • Next to **Deployment schedule**, **click Now** or **Later**. The default option is **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 **On every connection**.

   • Next to **Deploy for always-on connection**, **click On** or **Off**. The default option is **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, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with version 10.18.19 or later
   - Is not recommended for Android, Android Enterprise, and Chrome OS to
customers who began using Endpoint Management with before version 10.18.19

The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

7. Click **Save**.

The policy appears in the **Device Policies** table.

**Edit or delete a device policy**

To edit or delete a policy, select the check box 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.
Check policy deployment status

Click a policy row on the Configure > Device Policies page to check its deployment status.

When a policy deployment is pending, users can refresh the policy from Secure Hub by tapping Preferences > Device Information > Refresh policy.

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 Endpoint Management Uninstall device policy. For information, see 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. Thus, 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 remain on the device. For information, see Profile Removal device policy.

- **Windows 10**
  You can’t directly remove a device policy from a Windows 10 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 contains just that device and push the delivery group to the device. Users then re-enroll to continue.

- Chrome OS

To remove a device policy from a Chrome OS device, you can remove the device policy from a delivery group that contains just that device. You then push the delivery group to the device.

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 check boxes for the items you want to see.

![Device Policies](image)

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
<table>
<thead>
<tr>
<th>Device Policy Name</th>
<th>Device Policy Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirPlay Mirroring</td>
<td>Adds specific AirPlay devices (such as Apple TV or another Mac computer) to iOS devices. You also have the option of adding devices to a whitelist for supervised devices. That option limits users to only the AirPlay devices on the whitelist.</td>
</tr>
<tr>
<td>AirPrint</td>
<td>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.</td>
</tr>
<tr>
<td>Android Enterprise App Permissions</td>
<td>Configures how requests to Android Enterprise apps within work profiles handle what Google calls “dangerous” permissions.</td>
</tr>
<tr>
<td>Android Enterprise Managed Configurations</td>
<td>Controls various app configuration options and app restrictions for Android Enterprise devices.</td>
</tr>
<tr>
<td>APN</td>
<td>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.</td>
</tr>
<tr>
<td>App Access</td>
<td>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.</td>
</tr>
<tr>
<td>App Attributes</td>
<td>Specifies attributes, such as a managed app bundle ID or per-app VPN identifier, for iOS devices.</td>
</tr>
<tr>
<td>App Configuration</td>
<td>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 phone, desktop, or tablet devices.</td>
</tr>
<tr>
<td>Device Policy Name</td>
<td>Device Policy Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>App Inventory</td>
<td>Collects an inventory of the apps on managed devices. 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 app access blacklist or whitelist and then act accordingly.</td>
</tr>
<tr>
<td>App Lock</td>
<td>Defines a list of apps that users either can or can't run on iOS or certain Android devices.</td>
</tr>
<tr>
<td>App Network Usage</td>
<td>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 Endpoint Management.</td>
</tr>
<tr>
<td>App Restrictions</td>
<td>Creates blacklists for apps you want to prevent users from installing on Samsung Knox devices. You can also create whitelists for apps you want to allow users to install.</td>
</tr>
<tr>
<td>App Uninstall</td>
<td>Remove apps from user devices.</td>
</tr>
<tr>
<td>App Uninstall Restrictions</td>
<td>Specifies the apps that users can or can't uninstall.</td>
</tr>
<tr>
<td>Application Guard</td>
<td>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.</td>
</tr>
<tr>
<td>Apps Notifications</td>
<td>Controls how iOS users receive notifications from specified apps.</td>
</tr>
<tr>
<td>BitLocker</td>
<td>Configures the settings available in the BitLocker interface on Windows 10 devices.</td>
</tr>
<tr>
<td>Browser</td>
<td>Defines whether user devices can use the browser or which browser functions the devices can use.</td>
</tr>
<tr>
<td>Device Policy Name</td>
<td>Device Policy Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Calendar (CalDav)</td>
<td>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.</td>
</tr>
<tr>
<td>Cellular</td>
<td>Configures cellular network settings.</td>
</tr>
<tr>
<td>Configure Windows Agent</td>
<td>Allows you to configure, schedule, and run various PowerShell scripts on MDM-managed devices.</td>
</tr>
<tr>
<td>Connection Manager</td>
<td>Specifies the connection settings for apps that connect automatically to the internet and to private networks. This policy is only available on Windows Pocket PCs.</td>
</tr>
<tr>
<td>Contacts (CardDAV)</td>
<td>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.</td>
</tr>
<tr>
<td>Content</td>
<td>Controls various web content options for Chrome OS, including what home page to show and how popups are handled.</td>
</tr>
<tr>
<td>Copy apps to Samsung Container</td>
<td>Copies the apps already installed on a device to a SEAMS or Knox container on supported Samsung devices. Apps copied to the SEAMS container are available on the device home screen. Apps copied to the Knox container are available only when users sign in to the Knox container.</td>
</tr>
<tr>
<td>Control OS Update</td>
<td>Deploys the latest OS updates to supported, supervised devices.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Enables integrated authentication with your PKI configuration in Endpoint Management. For example, with a PKI entity, a keystore, a credential provider, or a server certificate.</td>
</tr>
<tr>
<td>Custom XML</td>
<td>Customizes features such as provisioning devices, enabling device features, configuring devices, and managing faults.</td>
</tr>
<tr>
<td>Device Policy Name</td>
<td>Device Policy Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Defender</td>
<td>Configures Windows Defender settings for Windows 10 for desktop and tablet.</td>
</tr>
<tr>
<td>Device Guard</td>
<td>Enable security features such as secure boot, UEFI lock, and virtualization.</td>
</tr>
<tr>
<td>Device Health Attestation</td>
<td>Requires that Windows 10 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 Endpoint Management. When Endpoint Management receives the Health Attestation Certificate, based on the contents of that certificate, it can deploy automatic actions that you configured.</td>
</tr>
<tr>
<td>Device Name</td>
<td>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.</td>
</tr>
<tr>
<td>Education Configuration</td>
<td>Configures instructor and student devices for use with Apple Education. If instructors use the Classroom app, the Education Configuration device policy is required.</td>
</tr>
<tr>
<td>Endpoint Management Options</td>
<td>Configures the Secure Hub behavior when connecting to Endpoint Management from Android devices.</td>
</tr>
<tr>
<td>Endpoint Management Uninstall</td>
<td>Uninstalls Endpoint Management from Android devices. When deployed, this policy removes Endpoint Management from all devices in the deployment group.</td>
</tr>
</tbody>
</table>
### Device Policy Name

<table>
<thead>
<tr>
<th>Device Policy Name</th>
<th>Device Policy Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Hub</td>
<td>Distributes apps to Windows Phones through the Enterprise Hub Company store. Endpoint Management supports only one Enterprise Hub policy for one mode of Windows Phone Secure Hub. For example, don’t create multiple Enterprise Hub policies with different versions of Secure Home for Endpoint Management. You can deploy the initial Enterprise Hub policy only during device enrollment.</td>
</tr>
<tr>
<td>Exchange</td>
<td>Enables ActiveSync email for the native email client on the device.</td>
</tr>
<tr>
<td>Files</td>
<td>Adds script files to Endpoint Management that perform certain functions for users. Or, you can add document files that you want Android device users to be able 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.</td>
</tr>
<tr>
<td>FileVault</td>
<td>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.</td>
</tr>
<tr>
<td>Firewall</td>
<td>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.</td>
</tr>
<tr>
<td>Font</td>
<td>Adds fonts to iOS and macOS devices. Fonts must be TrueType (.TTF) or OpenType (.OFT) fonts. Endpoint Management doesn’t support font collections (.TTC or .OTC).</td>
</tr>
<tr>
<td>Home screen layout</td>
<td>Specifies the layout of apps and folders for the iOS Home screen on supervised iOS devices.</td>
</tr>
<tr>
<td>Import Device Configuration</td>
<td>Imports a template configuration file from Workspace Hub devices.</td>
</tr>
<tr>
<td>Device Policy Name</td>
<td>Device Policy Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Import iOS &amp; macOS Profile</td>
<td>Imports device configuration XML files for iOS and macOS devices into Endpoint Management. The file contains device security policies and restrictions that you prepare by using the Apple Configurator.</td>
</tr>
<tr>
<td>Keyguard Management</td>
<td>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.</td>
</tr>
<tr>
<td>Kiosk</td>
<td>Restricts app usage on Samsung SAFE devices. You can limit available apps to a specific app or apps. This policy is useful for corporate devices that are intended to run only a specific type or class of apps. This policy also lets you choose custom images for the device home screen and lock screen wallpapers for kiosk mode.</td>
</tr>
<tr>
<td>Knox Platform for Enterprise</td>
<td>Specifies the Knox Platform for Enterprise (KPE) Premium license key.</td>
</tr>
<tr>
<td>Launcher Configuration</td>
<td>Specifies settings for Citrix Launcher on Android devices, such as the apps allowed and a custom logo image for the Launcher icon.</td>
</tr>
<tr>
<td>LDAP</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Device Policy Name** | **Device Policy Description**
--- | ---
Location | Lets you geo-locate devices on a map, assuming that the device has GPS enabled for Secure Hub. After deploying this policy to the device, you can send a locate command from Endpoint Management. The device then responds with its location coordinates. 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.
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.
Managed Bookmarks | Deploys a folder of bookmarks to Chrome OS devices.
Maps | Specifies which maps to download to supervised Windows 10 phone devices. The Microsoft Maps configuration service provider (CSP) only supports maps of Germany, the United Kingdom, and the United States.
Maximum resident users | Specifies the maximum number of users for a Shared iPad.
MDM Options | Manages Find My Phone and iPad Activation Lock on supervised iOS devices.
<table>
<thead>
<tr>
<th>Device Policy Name</th>
<th>Device Policy Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Info</td>
<td>Specifies organization information for alert messages that Endpoint Management deploys to iOS devices.</td>
</tr>
<tr>
<td>Passcode</td>
<td>Enforces a PIN code or password on a managed device. You can set the complexity and timeouts for the passcode on the device.</td>
</tr>
<tr>
<td>Passcode lock grace period</td>
<td>Specifies the number of minutes that a Shared iPad screen stays locked before the user must enter a passcode to unlock the screen.</td>
</tr>
<tr>
<td>Personal Hotspot</td>
<td>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.</td>
</tr>
<tr>
<td>Profile Removal</td>
<td>Removes the app profile from iOS or macOS devices.</td>
</tr>
<tr>
<td>Provisioning Profile</td>
<td>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.</td>
</tr>
<tr>
<td>Provisioning Profile Removal</td>
<td>Removes iOS provisioning profiles.</td>
</tr>
<tr>
<td>Power management</td>
<td>Controls how Chrome OS devices respond to idle periods when using AC or battery power.</td>
</tr>
<tr>
<td>Proxy</td>
<td>Specifies global HTTP proxy settings for devices running iOS. You can deploy only one global HTTP proxy policy per device.</td>
</tr>
<tr>
<td>Public Session</td>
<td>Configure a Chrome OS device to act as a public device in guest mode.</td>
</tr>
<tr>
<td>Device Policy Name</td>
<td>Device Policy Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Restrictions</td>
<td>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.</td>
</tr>
<tr>
<td>Roaming</td>
<td>Configures whether to allow voice and data roaming on iOS devices. If voice roaming is disabled, data roaming is automatically disabled.</td>
</tr>
<tr>
<td>Samsung MDM License Key</td>
<td>Specifies the built-in Samsung Enterprise License Management (ELM) key that you must deploy to a device before you can deploy SAFE policies and restrictions. Endpoint Management also supports the Samsung Enterprise Firmware-Over-The-Air (E-FOTA) service. Endpoint Management supports and extends both Samsung for Enterprise (SAFE) and Samsung Knox policies.</td>
</tr>
<tr>
<td>Scheduling</td>
<td>Required for Android devices to connect back in to 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.</td>
</tr>
<tr>
<td>SCEP</td>
<td>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 Endpoint Management. To do that, create a PKI entity and a PKI provider in distributed mode.</td>
</tr>
<tr>
<td>Device Policy Name</td>
<td>Device Policy Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>SSO Account</td>
<td>Creates single sign-on (SSO) accounts so users sign on one-time only to access Endpoint Management and your internal company resources. Users do not need to store any credentials on the device. 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.</td>
</tr>
<tr>
<td>Storage Encryption</td>
<td>Encrypts internal and external storage. For some devices, this policy prevents users from using a storage card on their devices.</td>
</tr>
<tr>
<td>Store</td>
<td>Specifies whether an app store web clip appears on the home screen of user devices.</td>
</tr>
<tr>
<td>Subscribed Calendars</td>
<td>Adds a subscribed calendar to the calendars list on iOS devices. Ensure that you subscribe to a calendar before you add it to the subscribed calendars list on user devices.</td>
</tr>
<tr>
<td>Terms and Conditions</td>
<td>Requires that users accept the specific policies of your company that govern connections to the corporate network. When users enroll their devices with Endpoint Management, they must accept the terms and conditions to enroll their devices. Declining the terms and conditions cancels the enrollment process.</td>
</tr>
<tr>
<td>Verified Access</td>
<td>With verified access enabled, devices can access the network only when they are unmodified and policy-compliant.</td>
</tr>
<tr>
<td>Device Policy Name</td>
<td>Device Policy Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VPN</td>
<td>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. 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.</td>
</tr>
<tr>
<td>Wallpaper</td>
<td>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.</td>
</tr>
<tr>
<td>Web Content Filter</td>
<td>Filters web content on iOS devices. Endpoint Management uses the Apple auto-filter function and the sites that you add to whitelists and blacklists. Available only for iOS supervised devices.</td>
</tr>
<tr>
<td>Webclip</td>
<td>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.</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Allows administrators to deploy Wi-Fi router details to managed devices. The router details include SSID, authentication data, and configuration data.</td>
</tr>
<tr>
<td>Windows Agent</td>
<td>Enable this policy to run uploaded PowerShell scripts on Windows desktops and tablets.</td>
</tr>
<tr>
<td>Windows Hello for Business</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Device Policy Name | Device Policy Description
---|---
Windows GPO configuration | Configure Group Policy Objects (GPOs) for any Windows device supported by Citrix Workspace Environment Management.
Windows Information Protection | Specifies the apps that require Windows Information Protection at the enforcement level you set for the policy. The policy is for Windows 10 version 1607 and later supervised devices.

### AirPlay mirroring device policy

August 26, 2019

The Apple AirPlay feature allows users to wirelessly stream content 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 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 a whitelist for supervised devices, which limits users to only the AirPlay devices on the whitelist. For information about placing a device into Supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator.

**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 ID**: Enter the hardware address (Mac address) in xx:xx:xx:xx:xx:xx format. This field is not case-sensitive.
  - **Password**: Enter an optional password for the device.
  - Click **Add** to add the device or click **Cancel** to cancel adding the device.

- **Whitelist 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 xx:xx:xx:xx:xx:xx format. This field is not case-sensitive.
  - Click **Add** to add the device or click **Cancel** to cancel adding the device.

macOS settings

- **AirPlay Password**: For each device you want to add, click **Add** and then do the following:
Citrix Endpoint Management

- **Device ID**: Enter the hardware address (Mac address) in xx:xx:xx:xx:xx:xx format. This field is not case-sensitive.
- **Password**: Enter an optional password for the device.
- Click **Add** to add the device or click **Cancel** to cancel adding the device.

**Whitelist 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 xx:xx:xx:xx:xx:xx format. This field is not case-sensitive.
- Click **Add** to add the device or click **Cancel** to cancel adding the device.

### AirPrint device policy

April 25, 2019

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.

### Android Enterprise app permissions

November 13, 2019
For Android Enterprise (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 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 or deny dangerous permission requests.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.

### 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 is not prompted.
- **Deny**: All dangerous permission requests are denied. The user is not 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** and 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 is not prompted.
  - **Deny**: Dangerous permission requests from this permission group for this app are denied. The user is not 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**.

**Android Enterprise managed configurations policy**

November 21, 2019

The Android Enterprise managed configurations device policy controls various app configuration options and app restrictions. The app developer defines the options and tooltips available for an app. If a tooltip mentions using a “templated value,” use the corresponding 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:

- App email settings
- Whitelist or blacklist 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.
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 Endpoint Management. For more information, see Adding Apps to Endpoint Management.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.

Android Enterprise settings

After you choose to add an Android Enterprise managed configurations device policy, a prompt to select an app appears. If there are no Android Enterprise apps added to Endpoint Management, you cannot proceed.

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 Android Enterprise managed configuration device policy.

Start by adding Citrix SSO to the Endpoint Management console as a Google Play store app. See Add a public app store app.
Create an Android Enterprise managed configuration for Citrix SSO

Configure the Android Enterprise managed configurations device policy for Citrix SSO to create VPN profiles. Devices that have the Citrix SSO app installed and the policy deployed have access to the VPN profiles you create.

You need your Citrix Gateway FQDN and port.

1. In the Endpoint Management console, click **Configure > Device Policies**. Click **Add**.

2. Select **Android Enterprise**. Click **Android Enterprise 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**.

5. Configure VPN profile parameters.
   - **VPN Profile Name:** Type a name for the VPN profile. If you are 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 Citrix Gateway FQDN. If your Citrix Gateway port is not 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 Citrix Gateway. You can use the 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 Citrix Gateway.

- **Password (optional):** Provide the password that end users use to authenticate to the Citrix Gateway. If you don’t provide a password, users are prompted to provide a password when the connect to Citrix Gateway.

- **Certificate Alias (optional):** Provide a certificate alias in Android KeyStore to be used for client certificate authentication. This certificate is pre-selected for users if you are using certificate-based authentication.

- **Per-App VPN Type (optional):** If you are using per-app VPN to restrict which apps use this VPN, you can configure this setting. If you select **Allow**, network traffic for 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 app 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 disallowed 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 user interface of the Citrix SSO app instead of tapping a specific profile. If this field is left empty, the main profile is used for connection. If only one profile is configured, it is marked as default profile. For always-on VPN, this field must be set to the name of the VPN profile to be used for establishing 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 when using a self-signed certificate for Citrix Gateway or when the root certificate for the CA issuing the Citrix Gateway certificate is not in the system CA list. If this setting is ON, the Android operating system validates the Citrix
Citrix Endpoint Management

Gateway certificate. If the validation fails, the connection is not allowed. 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.

   a) Create a custom parameter:

   - **Parameter name**: Type `XenMobileDeviceId`. This field is the device ID to use for Network Access Check based on device enrollment in Endpoint Management. If Endpoint Management enrolls and manages the device, the VPN connection is allowed. Otherwise, authentication is denied at the time of VPN establishment.

   - **Parameter value**: For Endpoint Management to determine the enrollment and management state of the devices, the value of `XenMobileDeviceId` set to `DeviceID_${device.id}`.
a) To create another custom parameter, click Add again. Create this custom parameter.

- **Parameter name:** Type **UserAgent**. This text appended to the User-Agent HTTP header for performing an extra check on Citrix Gateway. Value of this text is appended to the User-Agent HTTP header by the Citrix SSO app while communicating with the Citrix Gateway.

- **Parameter value:** Type the text you want to append to the User-Agent HTTP header. This text must conform to the HTTP User-Agent specifications.

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 have 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 **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 Google Play store.

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 icon indicates 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.

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.

Start by adding the Zebra OEMConfig app to the Endpoint Management console 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 Android Enterprise 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 Endpoint Management console, click Configure > Device Policies. Click Add.

2. Select Android Enterprise. Click Android Enterprise Managed Configurations.

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** for 12-hour format or **24** for 24-hours format.

For a list and descriptions of all available configuration, 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 have created all the Zebra OEMConfig configurations you want, click **Next**.

3. Configure deployment rules for this managed configuration for Zebra OEMConfig.

4. Click **Save**.

### Android Enterprise permissions

**August 26, 2019**

You can configure how requests to Android Enterprise (Android enterprise) apps, that are within work profiles, 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 could potentially affect the user’s stored data or the operation of other apps. For example, the ability to read the user’s contacts is a dangerous permission.

You can configure a global state that controls the behavior of all dangerous permission requests to Android Enterprise apps within work profiles. You can also control the behavior of dangerous permission request for individual permission groups, as defined by Google, for each app. These individual settings override the global state.

For information on how Google defines permission groups, see the **Android developers guide**.

By default, users are prompted to grant or deny dangerous permission requests.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see **Device policies**.
**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 is not prompted.
  - **Deny**: All dangerous permission requests are denied. The user is not 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** and then under **App**, choose an app from the list. Under Grant State, choose **Prompt, Grant, or Deny**. This grant state overrides the global state.
  - **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 is not prompted.
  - **Deny**: Dangerous permission requests from this permission group for this app are denied. The user is not prompted.

Default is **Prompt**.

- Click **Save** next to the app and grant state.

- To add more apps for the permission group, click **Add** again and repeat these steps.

- When you have finished setting grant states for all permission groups you want to, click **Next**.
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

- **APN**: Type the name of the access point. This must match an accepted iOS APN or the policy will fail.
- **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. This 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)**.
  - If you click **Select date**, click the calendar to select the specific date for removal.
– If you click **Password required**, next to **Removal password**, type the necessary password.

### Android settings

- **APN**: Type the name of the access point. This must match an accepted Android APN or the policy will fail.
- **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 could not access or render standard-web sites.
- **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 should rarely be used.
  - `hipri`: High priority networking.
  - `fota`: Firmware over the air is used for receiving firmware updates.
- **Authentication type**: In the list, click the type of authentication to be used. 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. This 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**: This is 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

August 21, 2018

The app access device policy in Endpoint Management allows you to define a list of apps that are either required to be installed on the device, can be installed on the device, or must not be installed on the device. You can then create an automated action to react to the device compliance with that list of apps.

You can only configure one type of access policy at a time. You can add a policy for either 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, we recommend that you name each policy carefully, so you know which policy in Endpoint Management 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 settings

- **Access policy**: Click **Required**, **Suggested**, or **Forbidden**. The default is **Required**.

- To add one or more apps to the list, click **Add** and then do the following:
  - **App name**: Enter an app name.
  - **App Identifier**: Enter an optional app identifier.
  - Click **Save** or **Cancel**.
  - Repeat these steps for each app you want to add.

### App attributes device policy

August 26, 2019
Citrix Endpoint Management

The App attributes device policy lets you specify attributes, such as a managed app bundle ID or per-app VPN identifier, for iOS devices.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see **Device policies**.

**iOS settings**

- **Managed app bundle ID**: In the list, click an app bundle ID or click **Add new**.
  - If you click **Add new**, type the app bundle ID in the field that appears.
- **Per-app VPN identifier**: In the list, click per-app VPN identifier.

**App configuration device policy**

November 21, 2019

You can remotely configure apps that support managed configuration by deploying:

- An XML configuration file (called a property list, or plist) to iOS devices
- Key/value pairs for Windows 10 Phone, Desktop, or Tablet devices
- Citrix Workspace connection information to Workspace hub devices

The configuration specifies various settings and behaviors in the app. 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**.
iOS settings

• **Identifier**: In the list, click the app you want to configure or click **Add new** to add a new 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**. 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 Phone settings
• In the **Make a selection** list, click the app you want to configure or click **Add new** to add a new app to the list.
  – 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.

**Windows Desktop/Tablet settings**

You can configure either Universal Windows Platform (UWP) apps or Win32 apps. To import Microsoft Administrative Template (ADMX) policy settings, configure Win32 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 a new app to the list.

  – 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.

- Choose a policy path. If you choose the same path more than once, the configuration associated with the most recently version is enforced.

- Set **Enable** to **On**.

- Input any required list element values as key-value pairs. Use the text string `&#x00F000` 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.
Workspace Hub settings

Use the App Configuration device policy to deploy the Citrix Workspace configuration to Citrix Ready workspace hub devices. Configure the following settings:

- **Connection Mode**: Select **Citrix Receiver**.
- **Connection Name**: Type a descriptive name for your connection.
- **Connection Target**: Type a URL to load upon connection.

Some apps might require extra parameters to function. For each configuration parameter you want to add, click **Add** and then configure the following:

- **Parameter name**: Type the key name of an application setting for the Citrix Ready workspace hub device.
- **Value**: Type the value for the specified parameter.

For more information about configuring Citrix Ready workspace hub devices, see **Workspace hub device management**.

App inventory device policy

August 26, 2019

The App inventory policy lets you collect an inventory of the apps on managed devices. 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 blacklist (forbidden in an app access policy) or whitelist (required in an app access policy) and take action accordingly.
To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.

**iOS, macOS, Android, Android Enterprise, Windows Desktop/Tablet, and Windows Phone**

- 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 comply with your App access device policy. To view an inventory of Win32 apps on managed Windows 10 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 device that you want to view, click Edit, and then click the Apps tab.
   
   The results of the inventory appear.
Citrix Endpoint Management

3. Compare the app inventory to your App access device policy. If the device has blacklisted apps installed, you can delete them from devices as follows.

**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 Endpoint Management. As a result:

- The App Uninstall device policy doesn’t uninstall the app.
- 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 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**

August 26, 2019

The Application Guard policy specifies Windows Defender Application Guard settings. The settings include whether to enable Application Guard and controls for clipboard behavior.
Citrix Endpoint Management

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

• Windows 10 (64-bit) enterprise devices running OS version 1709. A device restart is required to install the Windows Defender Application Guard.

• Microsoft Edge browser

Windows Desktop and Tablet settings

![Image of 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 from browser to PC only**: Allows users to copy and paste content only from their browser to their PC.
- **Allow copy and paste from PC to browser only**: 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:
  - **Not configured**
  - **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, Windows Defender Application Guard prevents content from unapproved sites from loading on enterprise sites. Default is Off.

- **Retain user-generated browser data**: If On, 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

October 16, 2019

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 the policy works differs for each supported platform. For example, you cannot block multiple apps on an iOS device.

Likewise, for iOS devices, you can select only one iOS app per policy. This means that users are only able to use their device to run a single app. They cannot do any other activities on the device except for the options you specifically allow when the app lock policy is enforced.

In addition, iOS devices must be supervised to push App Lock policies.

Although the device policy works on most Android L and M devices, app lock does not function on Android N or later devices because Google deprecated the required API.
For managed Windows Desktops and Tablets, you can create an App Lock device policy that defines the list of blacklisted and whitelisted apps. 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**: In the list, click the app to which this policy applies or click Add new to add a new 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
  - Enable invert colors
  - Enable AssistiveTouch
  - Enable speak selection
  - Enable mono audio
• **User Enabled Options:** For each option, the default is **Off**.
  – Allow VoiceOver adjustment
  – Allow zoom adjustment
  – Allow invert colors adjustment
  – Allow AssistiveTouch adjustment

**Android settings**

**Note:**
You can’t block the Android Settings app by using the App Lock device policy.

**App Lock parameters**
  – **Lock message:** Type a message that users see when they attempt 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 either **Blacklist** to create a list of apps that are not allowed to run on devices or click **Whitelist** to create a list of apps that are allowed to run on devices.

**Apps:** Click **Add** and then do the following:
  – **App name:** In the list, click the name of the app to add to the whitelist or blacklist, or click **Add new** to add a new 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 you want to add to the whitelist or blacklist.
Windows Desktop and Tablet settings

Prerequisites for App lock

- In Windows, configure rules in the Local Security Policy editor on a Windows 10 Desktop running Windows 10 Enterprise or Pro.
- 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 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, click Computer Configuration > Windows Settings > Security Settings and then expand Application Control Policies.
3. Click AppLocker and then in the center pane, click Configure rule enforcement.
4. Select Enforcerules. When you enable a rule, Enforcerules is the default.
5. 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.
6. Right-click AppLocker, click Export Policy, and then save the XML file.

To import the policy XML file into 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 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 are not affected. Devices receiving the policy for the first time do not have the App Lock policy in place.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
App network usage device policy

August 21, 2018

You can set 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 those that you deploy to users’ devices through Endpoint Management. They do not include apps that users have downloaded directly to their devices without being deployed through Endpoint Management or those already installed on the devices when the devices were enrolled in Endpoint Management.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.

iOS settings

- **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 do the following:
  - **App Identifier**: Enter an app identifier.
  - Click **Save** to save the app to the list or **Cancel** to not save the app to the list.

Apps notifications device policy

August 26, 2019

The Apps notifications policy lets you control how iOS users receive notifications from specified apps.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.
iOS settings

- **App Bundle identifier**: Specify the apps you want to apply this policy to.
- **Allow Notifications**: Select On to allow notifications.
- **Show in Notification Center**: Select On to show notifications in the notification center of the user devices.
- **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**: If On, notifications display in Apple CarPlay. Available in iOS 12 and later. Default is On.
- **Enable Critical Alert**: If On, an app can mark a notification as a critical notification that ignores Do Not Disturb and ringer settings. Available in iOS 12 and later. Default is Off.
- **Unlocked Alert Style**: In the list, select None, Banner, or Alerts to configure the appearance of unlocked alerts.

App restrictions device policy

November 13, 2019

You use the App Restrictions device policy to specify allowed or blocked Chrome apps, Android apps running on Chrome OS, and Samsung Knox apps. If you enable App Runtime for Chrome (ARC) in the Restrictions device policy, you configure Android app restrictions under **Android apps** in the App Restrictions device policy.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.
Samsung Knox settings

For each app you want to add to the Allow/Deny list, click **Add** and then do the following:

- **Allow/Deny**: Select whether users are allowed to install the app.
- **New app restriction**: Type the app package ID; for example, com.kmdm.af.crackle.
- Click **Save** to save the app to the Allow/Deny list or click **Cancel** to not save the app to the Allow/Deny list.

Chrome app settings

Chrome apps are both apps and extensions.
• **App install allowed**: A global setting to allow or block the installation of all Chrome apps on Chrome OS devices. If you choose **Allowed**, you can create a list of specific blocked apps. If you choose **Not allowed**, you can create a list of specific allowed apps. To do that, click **Add** under **Chrome apps**. To use the settings specified in your Chrome account, select **Unspecified**. Default is **Allowed**.

• **Chrome apps**: To add Chrome apps that are exceptions to your selection for the **App install allowed** setting, click **Add** and then specify these settings:
  - **App name**: A name used to identify an app in the Endpoint Management console.
  - **App ID**: The unique identifier for a Chrome app. Don’t include the prefix “app:”.

To look up a Chrome app ID: Go to the Chrome web store. Then, search for the app. Click the app to view the URL and app ID in the address bar. The last portion of the address is the app ID. For example, if the URL is `https://chrome.google.com/webstore/detail/citrix-intranet/hjacpdaecmilhndcbllidcgaaicdlpff`, the app id is “hjacpdaecmilhndcbllidcgaaicdlpff”.

You can look up Chrome apps only from Chromebook. You can look up Chrome extensions from any platform.

  - **App install allowed**: Creates an exception to the global setting above. This setting allows or blocks the specified Chrome app.
  - **Installed**: If **On**, forces the Chrome app to install for enrolled Chrome OS device users. If **Off** and an app is installed, the app is uninstalled. If **Off** and the app is no longer configured by the policy, the app remains installed. Default is **Off**.
  - **Pinned**: If **On**, pins the app to the Chromebook task bar. Default is **Off**.
  - **URL**: Specifies the URL from which users can download an app that isn’t hosted in the Chrome Web Store.
  - **Extension policy**: Defines, in JSON format, the app-specific policy defined by this app. For information, see **Manifest for storage areas**.

**Android app settings**

To enable enrolled Chrome OS device users to run Android apps, configure the Restrictions device policy as noted in the next section “Enable enrolled Chrome OS device users to run Android apps.” To configure ARC app restrictions, click **Add** under Android apps and then specify these settings.
Citrix Endpoint Management

- **App ID**: A unique app identifier for an Android app running on Chrome OS. For example: com.android.camera. Don’t include the prefix “app:”.

  To look up an Android app ID: Go to the Google Play store. Then, search for the app. Click the app to view the app ID in the address bar. The portion after `id=` is the app ID. For example, if the URL is `https://play.google.com/store/apps/details?id=com.citrix.mail`, the app id is `id=com.citrix.mail`.

- **Installed**: Specifies whether to force the Android app to install for enrolled Chrome OS device users. If Off and an app is installed, the app is uninstalled. If Off and the app is no longer configured by the policy, the app remains installed. Default is Off.

- **Pinned**: If On, pins the Android app to the Chromebook task bar. Default is Off.

**Enable enrolled Chrome OS device users to run Android apps**

To enable enrolled Chrome OS device users to run Android apps: Go to Configure > Device Policies and add a Restrictions device policy for Chrome OS with the setting Enable App Runtime for Chrome (ARC) enabled.

- **Enable App Runtime for Chrome (ARC)**: If On, allows enrolled Chrome OS device users to run Android apps. Specify ARC apps in the App Restrictions device policy. Requires G Suite Chrome configuration. ARC isn’t available if either Ephemeral mode or multiple sign-on is enabled in the current user session. If Off, enterprise Chrome OS device users can’t run Android apps. The default is On.
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 mobile device app and the app server component. You can configure the app Tunneling policy for Android devices.

Any app traffic sent through a tunnel that you define in this policy goes through 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 initiating 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. WiFi and USB connections aren’t blocked.

• **Client port**: Type the client port number. In most cases, this value is the same as for the server port.

• **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.

## App uninstall device policy

August 26, 2019

The App uninstall policy lets you remove apps from user devices for any number of reasons. It may be that you no longer want to support certain apps, your company may want to replace existing apps with similar apps from different vendors, and so on.

The apps are removed when this policy is deployed to user devices. With the exception of Samsung Knox devices, users receive a prompt to uninstall the app. Samsung Knox device users do not receive a prompt to uninstall the app.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

## iOS settings

![iOS settings configuration](image-url)
• **Managed app bundle ID:** in the list, click an existing app or click **Add new**. If there are no apps configured for this platform, the list will be empty and you must add a new app.  
  – When you click **Add**, a field appears where you can type an app name.

### Android, Samsung Knox, Android Enterprise, Windows Phone, and Windows Desktop/Tablet settings

• **Apps to uninstall:** For each app you want to add, click **Add** and then do the following:  
  – **App name:** In the list, click an existing app 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 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 identical app icons after the public app store version installs.

A deployment condition for the App Uninstall device policy triggers Endpoint Management to remove older apps from user devices upon installation of the new version. This feature is available only for managed iOS devices connected to an 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, Endpoint Management removes the Enterprise version (com.citrix.mail).

### App uninstall restrictions device policy

August 21, 2018

You can specify the apps users can or cannot uninstall on a Samsung SAFE or Amazon device.
To add or configure this policy, go to **Configure > Device Policies**. For more information, see **Device policies**.

**Samsung SAFE or Amazon settings**

- **App Uninstall Restrictions Settings**: For each app rule you want to adds, click **Add** and then do the following:
  - **AppName**: In the list, click an app or **Add new** to add a new app.
  - **Rule**: Select whether users can uninstall the app. The default is to allow uninstallation.
  - Click **Save** or **Cancel**.

**BitLocker device policy**

November 13, 2019

Windows 10 includes 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 Endpoint Management to configure the settings available in the BitLocker wizard on Windows 10 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 setting 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 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.

Windows Phone settings

- **Require device to be encrypted:** Determines whether to prompt users to enable BitLocker encryption on a Windows Phone system card. If **On**, devices show a message after enrollment completes, indicating that the enterprise requires device encryption. If the user opts out of device encryption, the user isn’t granted write access to the system card. If **Off**, the user isn’t prompted and the BitLocker policy determines whether the device is encrypted. Defaults to **Off**.

- **Require storage card encryption:** Determines whether to prompt users to enable BitLocker encryption on a Windows Phone storage card. If **On**, storage card encryption is required to gain write permission on the card. Defaults to **Off**.
Windows Desktop and Tablet settings

BitLocker policy
This policy lets you enable BitLocker on an enrolled machine and specify the encryption mechanism to use.

BitLocker settings
- Require device to be encrypted

Encryption settings
- Configure encryption methods
  - Operating system drive
  - Fixed drive
  - Removable drive

OS drive settings
- Require additional authentication at startup
- Block BitLocker on devices without TPM chip
- TPM status
  - Allow TPM
  - Allow startup PIN
  - Allow TPM key at startup
  - Allow startup key and PIN

PIN length
- Minimum PIN length
  - 8

BitLocker password recovery settings
- BitLocker Recovery backup to Endpoint Management
- The text here should display the recovery key on the Device page. Enable the server policies to display the recovery key on the device policy to properly guide end users on how to back up the recovery key.

OS drive recovery settings
- Enable OS drive recovery
- Allow certificate based data recovery agent
- 40-bit recovery password
- 256-bit recovery key
- Allow 256-bit recovery key

Fixed drive settings
- Semi-recovery info in Active Directory Domain Services
- Recovery info stored in Active Directory Domain Services
- Use default recovery message and URL

Deployment Rules
• **Bitlocker settings**
  
  **Require device to be encrypted**: Determines whether to prompt users to enable BitLocker encryption on the Windows Desktop or Tablet. If **On**, devices show a message after enrollment completes, indicating that 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 store 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.

  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 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 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 located 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 devices 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 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 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 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 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.

Browser device policy

March 21, 2019

You can create browser device polices for Samsung SAFE or Samsung Knox devices to define whether user devices can use the browser or to limit the browser functions that the devices can use.
On Samsung devices, you can completely disable the browser, or you can enable or disable pop-ups, JavaScript, cookies, autofill, and whether to force fraud warnings.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.

**Samsung SAFE and Samsung Knox settings**

- **Disable browser**: Select whether to completely disable the Samsung browser on users’ devices. The default is Off, which lets users use the browser. When you disable the browser, the following options disappear.
- **Disable pop-up**: Select whether to allow pop-up messages on the browser.
- **Disable Javascript**: Select whether to allow JavaScript to run on the browser.
- **Disable cookies**: Select whether to allow cookies.
- **Disable autofill**: Select whether to allow users to turn on the browser’s autofill function.
- **Force fraud warning**: Select whether to display a warning when users visit a fraudulent or compromised website.

**Calendar (CalDav) device policy**

August 21, 2018

You can add a device policy in 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.

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**.

**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.
- **Username**: 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**.

**Cellular device policy**

August 21, 2018

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 Endpoint Management by using the Import iOS & macOS Profile device policy.

- **Attach APN**
  - **Name**: A name for this configuration.
  - **Authentication type**: In the list, click Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP). 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**: In the list, click **CHAP** or **PAP**. The default is **PAP**.
- **User name** and **Password**: The user name and password to use for authentication.
- **Proxy server**: The proxy server network address.
- **Proxy server port**: The proxy server port.

**Connection scheduling device policy**

August 26, 2019

**Important:**

Citrix recommends that you use Firebase Cloud Messaging (FCM) to control connections from Android, Android Enterprise, and Chrome OS devices to 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 Endpoint Management.

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 you want to set for this schedule.
  - **Never**: Connect manually. Users must initiate the connection from 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, Endpoint Management processes the action on the device the next time the device connects. When you select this option, the **Connect 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**: Endpoint Management on the user device attempts to reconnect to the Endpoint Management server after a network connection loss. Endpoint Management and monitors the connection by transmitting control packets at regular intervals within the time frame 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
Chrome OS settings

- **Require devices to connect**: Specify the connection frequency in **Connect every N minutes**. Default is **120** minutes (2 hours).

Contacts (CardDAV) device policy

August 21, 2018

You can add a device policy in 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.
- **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.
- **Username**: 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**.

**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.
- **Username**: 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**.

**Content device policy**

August 26, 2019

You can control various web content options for Chrome OS, including what homepage to show and how popups are handled.

To add or configure this policy, go to **Configure > Device Policies.** For more information, see [Device policies](#).
Chrome OS Settings

- **HomePage Settings**: Select whether the home page should be a new tab or a specified URL.
- **Homepage URL**: If you selected a Homepage URL for the Homepage settings, type the URL here.
- **Pop-up default settings**: Select whether to allow or disallow popups by default. You can then disallow or allow specific URLs from opening popups.
- **Pop-ups allowed from these sites**: Specify a list of URLs allowed to open popups.
- **Pop-up not allowed from these sites**: Specify a list of URLs blocked from opening popups.
- **Pages to load on startup**: Specify a list of URLs to be opened on browser startup.

Copy Apps to Samsung Container device policy

May 17, 2019

For apps that are already installed on a device, you can specify to copy the apps to a SEAMS container or to a Knox container on supported Samsung devices. For information about supported devices, see the Samsung article, [Samsung Knox Supported Devices](#).

Apps copied to the SEAMS container are available on users’ home screens. Apps copied to the Knox container are only available when users sign in to the Knox container.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

**Prerequisites**

- Enroll the device in Endpoint Management.
Citrix Endpoint Management

- Deploy the Samsung MDM keys (ELM and KLM). For how to do this, see Samsung MDM License Key device policy.
- Install apps on the device.
- Initialize Knox on the device to copy apps to the Knox container.

**Samsung SEAMS and Samsung Knox settings**

- **New app:** For each app you want to add to the list, click Add and then do the following:
  - Type a package ID; for example, com.mobiwolf.lacingart for the LacingArt app.
  - Click Save or Cancel.

**Credentials device policy**

November 21, 2019

Credentials device policies point to a PKI configured in Endpoint Management. For example, your PKI configuration might include a PKI entity, a keystore, a credential provider, or a server certificate. For more information about credentials, see Certificates and authentication.

Each supported platform requires a different set of values, which are described in this article.

**Note:**

Before you can create this policy, you need the credential information you plan to use for each platform, plus any certificates and passwords.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.
iOS and tvOS settings

Configure the following settings:

- **Credential type**: In the list, click the type of credential to use with this policy and then enter the following information for the selected credential:
  - **Certificate**
    - **Credential name**: Enter a unique name for the credential.
    - **The credential file path**: Select the credential file by clicking Browse and navigating to the file’s location.
  - **Keystore**
    - **Credential name**: Enter a unique name for the credential.
    - **The credential file path**: Select the credential file by clicking Browse and navigating to the file’s location.
    - **Password**: Enter the keystore password for the credential.
  - **Server certificate**
    - **Server certificate**: In the list, click the certificate to use.
  - **Credential provider**
    - **Credential provider**: In the list, click the name of the credential provider.
Configure the following settings:

- **Credential type**: In the list, click the type of credential to use with this policy and then enter the following information for the selected credential:
  - **Certificate**
    - **Credential name**: Enter a unique name for the credential.
    - **The credential file path**: Select the credential file by clicking **Browse** and navigating to the file’s location.
  - **Keystore**
    - **Credential name**: Enter a unique name for the credential.
    - **The credential file path**: Select the credential file by clicking **Browse** and navigating to the file’s location.
    - **Password**: Enter the keystore password for the credential.
  - **Server certificate**
    - **Server certificate**: In the list, click the certificate to use.
  - **Credential provider**
    - **Credential provider**: In the list, click the name of the credential provider.
Configure the following settings:

- **Credential type**: In the list, click the type of credential to use with this policy and then, enter the following information for the selected credential:
  - **Certificate**
    - **Credential name**: Type a unique name for the credential.
    - **The credential file path**: Select the credential file by clicking Browse and then navigating to the file’s location.
  - **Keystore**
    - **Credential name**: Type a unique name for the credential.
    - **The credential file path**: Select the credential file by clicking Browse and then navigating to the file location.
    - **Password**: Type the keystore password for the credential.
  - **Server certificate**
    - **Server certificate**: In the list, click the certificate to use.
  - **Credential provider**
    - **Credential provider**: In the list, click the name of the credential provider.
Configure the credential settings:

- **Credential type:** In the list, click the type of credential to use with this policy and then enter the following information for the selected credential:
  
  - **Certificate**
    - **Credential name:** Type a unique name for the credential.
    - **The credential file path:** Select the credential file by clicking **Browse** and then navigating to the file location.
  
  - **Keystore**
    - **Credential name:** Type a unique name for the credential.
    - **The credential file path:** Select the credential file by clicking **Browse** and then navigating to the file location.
    - **Password:** Type the keystore password for the credential.
  
  - **Server certificate**
    - **Server certificate:** In the list, click the certificate to use.
  
  - **Credential provider**
    - **Credential provider:** In the list, click the name of the credential provider.
    - **Apps to use certificates:** To specify apps that have silent access to the credentials from this provider: Click **Add**, select an app, and click **Save**.
Windows Desktop/Tablet settings

- **Certificate Type:** In the list, click either ROOT or CLIENT.
- If you click **ROOT**, configure these settings:
  - **Store device:** In the list, click root, My, or CA for the location of the certificate store for the credential. My stores the certificate in users’ certificate stores.
  - **Location:** For Windows 10 tablets, System is the only location.
  - **Credential type:** For Windows 10 tablets, Certificate is the only credential type.
  - **Credential file path:** Select the certificate file by clicking **Browse** and navigating to the file's location.
- If you click **CLIENT**, configure these settings:
  - **Location:** For Windows 10 tablets, System is the only location.
  - **Credential type:** For Windows 10 tablets, Keystore is the only credential type.
  - **Credential name:** Type the name of the credential. This field is required.
  - **Credential file path:** Select the certificate file by clicking **Browse** and navigating to the file's location.
  - **Password:** Type the password associated with the credential. This field is required.
Windows Phone settings

- **Certificate Type**: In the list, click either **ROOT** or **CLIENT**.
  - If you click **ROOT**, configure these settings:
    - **Store device**: In the list, click **root**, **My**, or **CA** for the location of the certificate store for the credential. **My** stores the certificate in users’ certificate stores.
    - **Location**: The **System** value is the only location for Windows phones.
    - **Credential type**: Certificate is the only credential type for Windows phones.
    - **Credential file path**: Select the certificate file by clicking **Browse** and navigating to the file's location.
  - If you click **CLIENT**, configure these settings:
    - **Location**: For Windows phones, **System** is the only location.
    - **Credential type**: For Windows phones, **Keystore** is the only credential type.
    - **Credential name**: Type the name of the credential. This field is required.
    - **Credential file path**: Select the certificate file by clicking **Browse** and navigating to the file's location.
    - **Password**: Type the password associated with the credential. This field is required.
WorkSpace Hub settings

The credential file path: Browse for the CA certificate file or .zip file containing the certificates to upload. This policy supports .cer, .crt, .pem, and .der certificate files.

Custom XML device policy

December 9, 2019

You can create custom XML policies in Endpoint Management to customize the following features on supported Windows, Zebra Android, and Android Enterprise 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

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 Device Management on the Microsoft Developer Network site.

Note:

For Windows 10 RS2 Phone: After a Custom XML policy or Restrictions policy that disables Internet Explorer deploys to the phone, the browser remains enabled. To work around this issue, restart the phone. This is a third-party issue.

For Zebra Android and 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. For more information about using MXMS, see the Zebra product documentation.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.
Windows Phone, Windows Desktop/Tablet, Zebra Android, and Android Enterprise settings

XML content: Type, or cut and paste, the custom XML code you want to add to the policy.

1. After you click **Next**, Endpoint Management checks the XML content syntax. Any syntax errors appear below the content box. Fix any errors before you continue.

2. 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.

Prerequisites

- Devices registered to the organization in Microsoft Store for Business portal.
- Company branding configured in Azure Active Directory portal.
- Company has an Azure Active Directory Premium P1 or P2 subscription.
- Configure Citrix Identity Platform as the IDP type for Endpoint Management: In the Endpoint Management console, go to Settings > Identity Provider (IDP). For more information, see Single sign in with Azure Active Directory.
- Network connectivity to cloud services used by Windows AutoPilot.
- Devices pre-installed with Windows 10 Professional, Enterprise or Education, version 1703 or later.
- Devices have access to the internet.

For more information on configuring prerequisites, see the Microsoft Windows documentation on AutoPilot.

To configure Windows Automatic Redeployment in Endpoint Management for AutoPilot devices

1. Follow the steps to add a custom XML policy at Custom XML Device Policy. Add the following in XML Content:
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 rights to redeploy the device. The device then redeployes.

5. After the device updates with the AutoPilot configuration, the user can then log into the freshly configured device.

**Defender device policy**

August 26, 2019

Windows Defender is malware protection included with Windows 10. You can use the Endpoint Management device policy, Defender, to configure the Microsoft Defender policy for Windows 10 for desktop and tablet.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.
Windows Desktop and Tablet settings

- **Allows scanning of archives:** Allows or disallows Defender to scan archived files. Defaults to Off.
- **Allows cloud protection:** Allows or disallows Defender to send information to Microsoft about malware activity. Defaults to On.
- **Allows a full scan of removable drives:** Allows or disallows Defender to scan removable drives such as USB sticks. Defaults to On.
- **Allows Windows Defender Real-time Monitoring functionality:** Defaults to On.
- **Allows scanning of network files:** Allows or disallows Defender to scan network files. Defaults to On.
- **Allows user 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 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 consent:** Controls whether to send to Microsoft files that might require further analysis to determine if they are malicious. Options: Always prompt, Send safe samples, Never send, Send all samples. Defaults to Send safe samples.
Device Guard device policy

August 26, 2019

Device Guard is a Windows 10 security feature that 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 Desktops and Tablets with an Enterprise or Education license on version 1709 (RS3)
- 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.
- **LSA Configuration Flags**: Allows you to configure Credential Guard. This setting lets users turn on Credential Guard with virtualization-based security to help protect credentials at next reboot. Options are Off, On with UEFI Lock, and On without UEFI Lock. Default is Off.
- **Require Platform Security Features**: Specifies the platform security level at the next reboot. Options are Off, VBS with Secure Boot, and VBS with Secure Boot and direct memory access (DMA). Default is Off.
Endpoint Management queries a device to determine if the virtualization based security settings match the settings on the server. If the security settings match, Endpoint Management doesn't deploy this policy to the device. If the security settings don't match, Endpoint Management deploys the policy.

**Device Health Attestation device policy**

November 7, 2019

In Endpoint Management, you can require Windows 10 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 Endpoint Management. 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
- Bit Locker 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
- WinPE Enabled

For more information, refer to the Microsoft 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 Phone and 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 you set up.
- **On-prem DHA API version**: Select the version of the DHA service installed on the DHA server.

Device name device policy

August 26, 2019

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, to set the device name as the serial number of the device, you would use ${device.serialnumber}. To set the device name as a combination of the user’s name and your domain, you would use ${user.username}@example.com. For more information about macros, see Macros in 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 name in the device name.

### Education Configuration device policy

**August 26, 2019**

The Education Configuration device policy defines:

- The Apple Classroom app settings for instructor devices.
- The certificates used to perform client authentication between instructor and student devices.

When you choose a class in this policy, the 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.

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 obtained from your connected Apple School Manager account appears.

When you choose a class from **Display Name**, Endpoint Management fills in the instructors and students. Continue adding classes.
• **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.

**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. 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.

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

November 21, 2019

You add an Endpoint Management options policy to configure Secure Hub behavior when connecting to Endpoint Management from Android devices.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.

Android settings

- **Traybar notification - hide traybar icon**: Select whether the traybar icon is hidden or visible. The default is Off.
- **Connection: time-out(s)**: 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 interval(s)**: 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**: In the list, click whether to warn the user about a file transfer or whether to ask the user for permission. Available values: Do not warn the user, Warn the user, and Ask for user permission. The default is Do not warn the user.
**Android Enterprise settings**

Supported starting with Android version 7.

- **Enable Always On VPN**: Select whether the always-on VPN is enabled. When this setting is **On**, the VPN service starts when the device is powered on and continues to run while the device is on. Default is **Off**.
- **VPN Package**: Type the package name of the VPN app the device uses. By default, the package name of the Citrix SSO app, `com.citrix.CitrixVPN`, is autopopulated in this field.

**Endpoint Management uninstall device policy**

August 21, 2018

You can add a device policy in Endpoint Management to uninstall Endpoint Management from Android devices. When deployed, this policy removes 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 Endpoint Management from devices**: Select whether to uninstall Endpoint Management from every device to which you deploy this policy. The default is **Off**.
An Enterprise Hub device policy for Windows Phone lets you distribute apps through the Enterprise Hub Company store.

Before you can create the policy, you need the following:

- An AET (.aetx) signing certificate from DigiCert
- The Citrix Company Hub app signed by using the Microsoft app signing tool (XapSignTool.exe)

Note:
Endpoint Management supports only one Enterprise Hub policy for one mode of Windows Phone Secure Hub. For example, to upload Windows Phone Secure Hub for Endpoint Management, you should not create multiple Enterprise Hub policies with different versions of Secure Hub for Endpoint Management. You can only deploy the initial Enterprise Hub policy during device enrollment.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).

### Windows Phone settings

- **Upload .aetx file**: Select the .aetx file by clicking **Browse** and navigating to the file location.
- **Upload signed Enterprise Hub app**: Select the Enterprise Hub app by clicking **Browse** and navigating to the app location.
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. You can create policies for iOS, macOS, Android HTC, Android Enterprise, Samsung SAFE, Samsung Knox, Windows Phone, and Windows Tablet. 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 resides. You can use the system macro $user.domainname in this field to automatically look up user domain names.
- **User**: Specify the user name for the Exchange user account. You can use the system macro $user.username in this field to automatically look up user names.
• **Email address:** Specify the full email address. You can use the system macro \$user.mail in this field to automatically look up 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 email is synced with the Exchange Server. The default is 3 days.

• **Identity credential (keystore or PKI):** In the list, click an optional identity credential if you have configured an identity provider for Endpoint Management. This field is only required when Exchange requires a client certificate authentication. The default is None.

• **Authorize email move between accounts:** Select whether to allow users to move email out of this account into another account and to forward and reply from a different account. The default is Off.

• **Send email only from email app:** Select whether to restrict users to the iOS mail app for sending email. The default is Off.

• **Disable email recent syncing:** Select whether to prevent users from syncing recent addresses. 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 Overrideable:** 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 Overrideable:** 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.
  - **S/MIME Encrypt By Default User Overrideable:** 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 Overrideable:** 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.
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 look up user names.
- **Email address**: Specify the full email address. You can use the system macro $user.mail in this field to automatically look up 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 SignIn URL**: Specifies the URL to load into a webview to authenticate using OAuth when AutoDiscovery Service is not used. 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.
- **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 differ-
ent, 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**.

### Android HTC settings

![Android HTC settings](image)

- **Configuration display name**: Type the name for this policy that appears on user devices.
- **Server address**: Type the Exchange Server host name or IP address.
- **User ID**: Specify the user name for the Exchange user account. You can use the system macro $user.username in this field to automatically look up user names.
- **Password**: Enter an optional password for the Exchange user account.
- **Domain**: Enter the domain in which the Exchange Server resides. You can use the system macro $user.domainname in this field to automatically look up user domain names.
- **Email address**: Specify the full email address. You can use the system macro $user.mail in this field to automatically look up user email accounts.
- **Use SSL**: Select whether to secure connections between user devices and the Exchange Server. The default is **On**.

### Android TouchDown settings

**Note:**

DigiCert stopped supporting Android TouchDown on July 2, 2018. Citrix recommends that you use Citrix Secure Mail.
• **Server name or IP address**: Type the Exchange Server host name or IP address.

• **Domain**: Type the domain in which the Exchange Server resides. You can use the system macro $user.domainname in this field to automatically look up user domain names.

• **User ID**: Specify the user name for the Exchange user account. You can use the system macro $user.username in this field to automatically look up user names.

• **Password**: Type an optional password for the Exchange user account.

• **Email address**: Specify the full email address. You can use the system macro $user.mail in this field to automatically look up user email accounts.

• **Identity credential (keystore or PKI)**: In the list, click an optional identity credential if you have configured an identity provider for Endpoint Management. This field is only required when Exchange requires a client certificate authentication. The default is **None**.

• **App Setting**: Optionally, add TouchDown app settings for this policy.

• **Policy**: Optionally, add TouchDown policies for this policy.
Android Enterprise

- **Server name or IP address**: Type the Exchange Server host name or IP address.
- **Domain**: Type the domain in which the Exchange Server resides. You can use the system macro $user.domainname in this field to automatically look up user domain names.
- **User ID**: Specify the user name for the Exchange user account. You can use the system macro $user.username in this field to automatically look up user names.
- **Password**: Type an optional password for the Exchange user account.
- **Email address**: Specify the full email address. You can use the system macro $user.mail in this field to automatically look up user email accounts.
- **Identity credential (keystore or PKI)**: In the list, click an optional identity credential if you have configured an identity provider for Endpoint Management. This field is only required when Exchange requires a client certificate authentication. The default is **None**.
Samsung SAFE and Samsung Knox settings

<table>
<thead>
<tr>
<th>Device Policies</th>
<th>Apps</th>
<th>Media</th>
<th>Actions</th>
<th>Share/Files</th>
<th>Enrollment Profiles</th>
<th>Delivery Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Server name or IP address**: Type the Exchange Server host name or IP address.
- **Domain**: Type the domain in which the Exchange Server resides. You can use the system macro $user.domainname in this field to automatically look up user domain names.
- **User ID**: Specify the user name for the Exchange user account. You can use the system macro $user.username in this field to automatically look up user names.
- **Password**: Type an optional password for the Exchange user account.
- **Email address**: Specify the full email address. You can use the system macro $user.mail in this field to automatically look up user email accounts.
- **Identity credential (keystore or PKI)**: In the list, click an optional identity credential if you have configured an identity provider for Endpoint Management. This field is only required when Exchange requires a client certificate authentication.
- **Use SSL connection**: Select whether to secure connections between user devices and the Exchange Server. The default is **On**.
- **Sync contacts**: Select whether to enable synchronization for user contacts between devices and the Exchange Server. The default is **On**.
- **Sync calendar**: Select whether to enable synchronization for user calendars between devices and the Exchange Server. The default is **On**.
- **Default account**: Select whether to make user Exchange accounts the default for sending email from their devices. The default is **On**.
Windows Phone and Windows Desktop/Tablet settings

<table>
<thead>
<tr>
<th>Exchange Policy</th>
<th>Exchange Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Policy Info</td>
<td>2 Platforms</td>
</tr>
<tr>
<td></td>
<td>Windows Phone</td>
</tr>
</tbody>
</table>

**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 resides. You can use the system macro $user.domainname in this field to automatically look up 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 look up user names.
- **Email address:** Specify the full email address. You can use the system macro $user.mail in this field to automatically look up 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:** In the list, click the schedule to use when syncing data that is sent to the device from the Exchange Server. The default is **When item arrives**.
- **Logging level:** In the list, click **Disabled**, **Basic**, or **Advanced** to specify the level of detail when logging Exchange activity. The default is **Disabled**.
You can add script files to Endpoint Management that perform certain functions for users, or you can add document files that you want Android 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. For example, if you want Android users to receive a company document or .pdf file, you can deploy the file to the device and let users know where the file is located.

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.
- **File type**: Select either File or Script. When you select Script, Execute immediately appears. Select whether to run the script as soon as the file uploads. The Execute immediately default is Off.
Citrix Endpoint Management

- **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 in which to store the uploaded file or click **Add new** to choose an unlisted file location. You can use the macros `%XenMobile Folder%` or `%Flash Storage%` as the start of any path identifier.
- **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**.

**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**. When you select **Script**, **Execute immediately** appears. Select whether to run the script as soon as the file uploads. The **Execute immediately** default is **Off**.
- **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 in which to store the uploaded file or click **Add new** to choose an unlisted file location. You can use the macros `%XenMobile Folder%` or `%Flash Storage%` as the start of any path identifier.
- **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**

December 9, 2019

The macOS FileVault Disk Encryption feature protects the system volume by encrypting its contents. With FileVault enabled on a macOS device, a user logs in with their account password each time that the device starts. If the user loses their password, a recovery key enables them to unlock the disk and reset their password.

The Endpoint Management device policy, FileVault, 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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
macOS settings

- **Prompt for FileVault setup during logout**: If ON, prompts the user to enable FileVault during the next N logouts, as specified by the option, **Maximum times to skip FileVault setup**. If OFF, the FileVault password prompt doesn’t appear.

After you deploy the FileVault policy with this setting on, the following screen appears when a user signs off the device. The screen gives the user the option to enable FileVault before signing off.

![FileVault prompt screenshot](image)

If the **Maximum times to skip FileVault setup** value isn’t **0**: After you deploy the FileVault policy with this setting off and then the user signs on, the following screen appears.

![FileVault prompt screenshot](image)

If the **Maximum times to skip FileVault setup** value is **0** or the user has skipped setup the maximum number of times, the following screen appears.
• **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 future use. For information about recovery key management, see the Apple support site.
  
  – **Institutional recovery key:** You can create an institutional (or master) recovery key and FileVault certificate, which you then use to unlock devices. For information, see the Apple support site. Use 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.

• **Show personal recovery key:** If ON, shows the personal recovery key to the user after enabling FileVault on the device. Defaults to ON.
Firewall device policy

August 26, 2019

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.

Samsung SAFE settings

- **Allow/Deny host**: For each host to which you want to allow or deny access, click Add and configure the following:
  - **Host name/IP range**: The host name or IP address range of the site you want to affect.
  - **Port/port range**: The port or port range.
  - **Allow/deny rule filter**: Click Whitelist to allow access or click Blacklist to deny access to the site.

- **Reroute configuration**: For each proxy you want to configure, click Add and configure the following:
  - **Host name/IP range**: The host name or IP address range for the proxy reroute.
  - **Port/port range**: The port or port range for the proxy reroute.
  - **Proxy IP**: The proxy IP address for the proxy reroute.
  - **Proxy port**: The proxy port for the proxy reroute.

- **Proxy Configuration**
  - **Proxy IP**: The IP address of the proxy server.
  - **Port**: The proxy server port.

macOS settings

Requires macOS 10.12 and later.
**Citrix Endpoint Management**

- **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 10 Desktop and Tablet devices running Windows 10 RS3 and later.
### Windows Firewall

<table>
<thead>
<tr>
<th>Policy</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Feature</td>
<td>On</td>
</tr>
<tr>
<td>Public Profile</td>
<td>On</td>
</tr>
<tr>
<td>Private Profile</td>
<td>On</td>
</tr>
<tr>
<td>Domain Profile</td>
<td>On</td>
</tr>
<tr>
<td>Block all incoming connections, including those in the list of allowed programs</td>
<td>Off</td>
</tr>
<tr>
<td>Disable notifications to user when Firewall blocks a new program</td>
<td>Off</td>
</tr>
</tbody>
</table>

- **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

December 17, 2018

You can add a device policy in Endpoint Management to add additional fonts to iOS and macOS devices. Fonts must be TrueType (.ttf) or OpenType (.oft) fonts. Font collections (.ttc or .otc) are not supported.
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.

### 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.

### Home screen layout device policy

August 26, 2019

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 polices to a device results in an iOS error on the device. This limitation applies whether you define the home screen through this 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**.
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**.

- **Display Name:** The name to appear on the home screen for the app or folder.
- **Value:** For apps, the bundle identifier. For folders, a list of bundle identifiers, separated by commas. For web clips, the URL for the web clip. If more than one Web Clip value exists with the same URL, the behavior is undefined on iOS 11.3 and later devices.

**Import Device Configuration device policy**

August 21, 2018

The Import Device Configuration device policy lets you deploy custom configurations to Citrix workspace hub devices. The general steps are:

1. Manually configure your first Citrix workspace hub device.
2. Download the configuration file from the device.
3. Configure the Import Device Configuration policy and deploy the policy to push the configuration to all other devices.

For more information, see Workspace hub device management.

**Worspace Hub settings**

- **URL:** The URL for the configuration file hosted on a file sharing web server.

**Import iOS & macOS Profile device policy**

August 26, 2019

You can import device configuration XML files for iOS and macOS devices into Endpoint Management. The file contains device security policies and restrictions that you prepare with the Apple Configurator. The configuration XML file can contain macros. For more information, see Macros.

You can place an iOS device in Supervised mode with the Apple Configurator, as described later in this article. For more information about using the Apple Configurator to create a configuration file, see the Apple Configurator Help page.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.

**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.
**Place an iOS device in Supervised mode with the Apple Configurator**

To use the Apple Configurator, you need an Apple computer running macOS 10.7.2 or later.

**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.

1. Install the Apple Configurator from iTunes.
2. Connect the iOS device to your Apple computer.
3. Start the Apple Configurator. The Configurator shows that you have a device to prepare for supervision.
4. To prepare the device for supervision:
   a) Switch the **Supervision** control to **On**. Citrix recommends that you choose this setting if you intend to maintain control of the device on an ongoing basis by reapplying a configuration regularly.
   b) Optionally, provide a name for the device.
   c) In iOS, click **Latest** for the latest version of iOS you want to install.
5. When you are ready to prepare the device for supervision, click **Prepare**.

**Keyguard Management device policy**

November 21, 2019

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:

- 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.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see **Device policies**.
Android Enterprise settings

- **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 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 unredacted notifications**: If Off, unredacted notifications appear on secure keyguard screens. Set to On to show unredacted notifications. Default is Off, which means only redacted notifications on secure keyguard screens are allowed.

- **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 fingerprint lock**: If Off, the fingerprint lock feature is available on secure keyguard screens. Set to On to disable the fingerprint lock feature. Default is Off.
- **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, unredacted notifications appear on secure keyguard screens. If you disable unredacted notifications, only redacted notifications are allowed on secure keyguard screens. Set to On to include unredacted notifications. Default is Off.
- **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**

August 26, 2019

The Kiosk policy lets you restrict devices to Kiosk mode by limiting the apps that can run, as follows:

- For Samsung SAFE devices: You can specify that only a specific app or apps can be used. This policy is useful for corporate devices that are designed to run only a specific type or class of apps. This policy also lets you choose custom images for the device home screen and lock screen wallpapers for when the device is in Kiosk mode.
- For for dedicated Android Enterprise devices, which are also known as corporate owned single use (COSU) devices: You can whitelist apps and set lock task mode. By default, Secure Hub and Google Play services are whitelisted.
- For Windows 10 Desktop and Tablet devices: You can enable or disable Kiosk mode for one or more applications.

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**.

**Samsung SAFE settings**

**To put a Samsung SAFE device into Kiosk mode**

1. Enable the Samsung SAFE API key on the mobile device, as described in Samsung MDM license key device policies. This step lets you enable policies on Samsung SAFE devices.
2. Enable Firebase Cloud Messaging for Android devices, as described in Firebase Cloud Messaging. This step enables Android devices connect back to Endpoint Management.
3. Add a Kiosk device policy, as described in the next section.

4. Assign those three device policies to the appropriate delivery groups. Consider whether you want to include other policies, such as App inventory, in those delivery groups.

To remove the devices from Kiosk mode, create a Kiosk device policy that has Kiosk mode set to Disable. Update the delivery groups to remove the Kiosk policy that enabled Kiosk mode and to add the Kiosk policy that disables Kiosk mode.

To add a Kiosk device policy for Samsung SAFE

All apps that you specify for Kiosk mode must already be installed on the user devices.

Some options apply only to the Samsung Mobile Device Management (MDM) API 4.0 and later.

- **Kiosk mode:** Click Enable or Disable. The default is Enable. When you click Disable, all the following options disappear.
- **Launcher package:** Citrix recommends that you leave this field blank unless you have developed an in-house launcher to enable users to open the Kiosk app or apps. If you use an in-house launcher, enter the full name of the launcher application package.
- **Emergency phone number:** Enter an optional phone number. Anyone can use this number to contact your company to find a lost device. Applies only to MDM 4.0 and later.
- **Allow navigation bar:** Select whether to let users see and use the navigation bar while in Kiosk mode. Applies only to MDM 4.0 and later. The default is On.
- **Allow multi-window mode:** Select whether to let users use multiple windows while in Kiosk mode. Applies only to MDM 4.0 and later. The default is On.
- **Allow status bar:** Select whether to let users see the status bar while in Kiosk mode. Applies only to MDM 4.0 and later. The default is On.
- **Allow system bar:** Select whether to let users see the system bar while in Kiosk mode. The default is On.
- **Allow task manager:** Select whether to let users see and use the task manager while in Kiosk mode. The default is On.
- **Change Common SAFE passcode:** This setting helps protect against inadvertent changes to the Common SAFE passcode field. When this setting is Off, you can’t change the Common SAFE passcode field. The default is Off.
- **Common SAFE passcode:** If you set a general passcode policy for all Samsung SAFE devices, enter that optional passcode in this field.
- **Wallpapers**
  - **Define a home wallpaper:** Select whether to use a custom image for the home screen while in Kiosk mode. The default is Off.
    - **Home image:** When you enable Define a home wallpaper, select the image file by clicking Browse and navigating to the file location.
- **Define a lock wallpaper**: Select whether to use a custom image for the lock screen while in Kiosk mode. The default is **Off**. Applies only to MDM 4.0 and later.
  - **Lock image**: When you enable **Define a lock wallpaper**, select the image file by clicking **Browse** and navigating to the file location.
- **Apps**: For each app that you want to add to Kiosk mode, 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 lets users use the Android calendar app.
  - Click **Save** to add the app or click **Cancel** to cancel adding the app.

### Windows Desktop and Tablet settings

For Windows tablets we support multiple app kiosk configuration (AssignedAccess) starting from Windows 10, version 1803.
We also support single app kiosk configuration (AssignedAccess) starting from Windows 10, version 1709.

**Prerequisites:**
Kiosk policy for Windows Desktop and Tablet only applies to local users and users enrolled in Azure Active Directory.

**Note:**
The upgrade to Citrix Endpoint Management 10.19.1 removes your previous Kiosk device policies for Windows Desktop and Tablet. Be sure to add a Kiosk policy for one or more applications.

- **Kiosk mode**: Enables or disables Kiosk mode.
Citrix Endpoint Management

- **Application user model ID (AUMID):** The ID of the app that you want to allow in Kiosk mode. To get a list of the AUMIDs for all Microsoft Store apps installed for the current device user: Run the following PowerShell command.

```powershell
installerapps = get-AppxPackage
$aumidList = @()
foreach ($app in $installedapps)
{
    foreach ($id in (Get-AppxPackageManifest $app).package.applications.application.id)
    {
        $aumidList += $app.packagefamilyname + ";" + $id
    }
}
$aumidList
```

**Run multiple apps in Kiosk mode**

**Windows OS support:** Windows 10 Enterprise or Education; Windows 10 Pro or Windows 10 S, minimum version 1803. CEM supports users enrolled in Azure AD. To add the Azure AD device, join the device to the domain.
• **UWP and Win32 apps**: Click **Add** and select the Universal Windows Platform (UWP) apps or Windows desktop app (Win32).

• **UWP AUMID or Win32 path**: Provide the AUMID for each UWP app and the path for each Win32 app. For example,
  - **UWP AUMID**: `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`
  - **Win32 path**: `%windir%\system32\mspaint.exe` or `C:\Windows\System32\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**: CEM creates a new user for the target device or adds an existing user.
  - **Azure AD**: CEM 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, type the name. Ensure your local user name doesn’t contain the domain. If you enter an existing name, CEM doesn’t create a new user or change the current password.
  - To add an Azure AD user, enter the name in the format `azuread\user`. The **user** portion can either be the **Name** entered when creating a new user in Azure AD, or the **User name** entered when creating a new user in Azure AD. The assigned user can not be an Azure AD administrator.

• **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 ap-
applications. The default is **Off**.

- Click **Next** and save the changes.

### Chrome OS settings

Assign the Kiosk policy to a specific delivery group rather than the **All Users** group. After successfully enrolling the device and signing out, Kiosk mode launches on the device.

To remove the device from Kiosk mode, select the device and delete it from the administrator console. This removes all of the policies pushed from the Endpoint Management console to the device.

- **Heartbeat setting**: Monitor the status of the device. The default is **On**.
- **Device log upload enabled**: Store the record of events from the Chrome device. You can locate the .log file in the G Suite domain. The default is **On**.
- **Device status alert delivery**: Send alert notifications via email or text messages. Only configured emails and mobile numbers get notifications.
  - **Email addresses**: If you select the **Email** box, specify the email addresses to receive the alerts. Save the changes.
  - **Mobile numbers**: If you select the **SMS** box, specify the phone numbers to receive the alerts. Save the changes.

### Configure multiple kiosk apps

© 1999-2019 Citrix Systems, Inc. All rights reserved.
To add multiple apps, click **Add**.

- **App name**: Enter the full name of the app to add.
- **App ID**: Specify the ID of the app that you want to allow in Kiosk mode.
- **URL**: Specify the URL to download the app. You can enter a specific URL or download the app from the App Store.
- **Extension policy**: Customize the browsing experience by adjusting Chrome functionality and behavior. Enter a configuration code that contains a valid JSON object.
- **Click Next** and save the changes. Users can start the apps in Kiosk mode after you deploy the policy.

**Auto launch apps in Kiosk mode**

**Prerequisite:**

Before configuring auto launch, add the apps to the Kiosk policy.

- **Auto launch kiosk app**: Launches the Kiosk policy when users start the device.
  - **App name**: Enter the full name of the app to auto launch.
  - **App ID**: Specify the ID of the app that you want to allow in Kiosk mode.
  - **Enable auto login cancel**: When the device starts, provide users with the option to sign in using the regular sign-in screen. The default is **On**.
  - **Prompt for network when offline**: Let users select a network when the device enters Kiosk mode. The default is **On**.

**Android Enterprise settings**

To whitelist an app, click **Add**. You can whitelist multiple apps. For more information, see **Android Enterprise**.

- **Apps to whitelist**: Enter the package name of the app you want to whitelist or select the app from the list.
  - **Click Add new** to enter the package name of the app approved to show in the list.
Select the existing app from the list. The list shows apps that are uploaded in Endpoint Management. By default, Secure Hub and Google Play services are whitelisted.

- **Lock task mode:** 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**.

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 device policy**

August 26, 2019

Samsung upgraded the Knox License (KLM) and renamed it to the Knox Platform for Enterprise (KPE) Premium license key. You can replace existing Enterprise Licenses (ELM) and KLM keys with a new KPE Premium license key or continue to use the legacy keys in Citrix Endpoint Management.

- You purchase a Samsung Knox Platform for Enterprise License and obtain the KPE Premium key from Samsung. For more information, see the [KPE Premium key](#) article.
- To use a KPE key, create a Knox Platform for Enterprise device policy. If you are replacing legacy keys with a KPE key, remove the old Samsung MDM license key device policy.
- For information about using existing ELM and KLM keys, see [Samsung MDM license key device policy](#).
Citrix Endpoint Management

Samsung SAFE settings

- **Knox Platform for Enterprise Key**: The KPE key that you received from Samsung.
- **Backwards-Compatible Key**: If you support Samsung devices running Knox 2.7.1 or earlier, specify the backwards-compatible key that is provided with your entitlement-based Samsung Knox License key.

Android Enterprise settings

- **Knox Platform for Enterprise Key**: The KPE key that you received from Samsung for devices running Knox version 3.0 or later.

After you submit the changes, Endpoint Management then validates and registers the information.

Launcher configuration device policy for Android

August 26, 2019

Citrix Launcher lets you customize the user experience for Android devices deployed by Endpoint Management. Citrix Launcher and the Launcher Configuration device policy are not compatible with Android Enterprise.

You can add a Launcher Configuration policy to control these Citrix Launcher features:
Citrix Endpoint Management

- Manage 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 enter to exit the launcher.

While Citrix Launcher enables you to apply those device-level restrictions, the launcher grants users the operational flexibility they need through built-in access to device settings such as WiFi settings, Bluetooth settings, and device passcode settings. Citrix Launcher isn't intended as an extra layer of security over what the device platform already provides.

After you deploy Citrix Launcher, Endpoint Management installs it, replacing the default Android launcher.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.

Android settings

- **Define a logo image**: Select whether to use a custom logo image for 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.
- **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

August 21, 2018

You create an LDAP policy for iOS devices in 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 should 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.
    - **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.
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 should 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.
    - **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 you want to add.

Location device policy

November 8, 2019

You create location device policies in Endpoint Management to enforce geographic boundaries. When users breach the defined boundary, also called a **geofence**, Endpoint Management can perform 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**.
• **Location timeout**: Type a numeral and then click **Seconds** or **Minutes** to set how often Endpoint Management attempts to fix the device’s location. Valid values are 60–900 seconds or 1–15 minutes. The default is **1 minute**.

• **Tracking duration**: Type a numeral and then click **Hours** or **Minutes** to set how long Endpoint Management tracks the device. Valid values are 1–6 hours or 10–360 minutes. The default is **6 hours**.

• **Accuracy**: Type a numeral and then click **Meters**, **Feet**, or **Yards** to set how close to a device 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 Endpoint Management when the user turns off 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 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 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 Endpoint Management selectively wipes their devices. The default is **0 seconds**.

**Android settings**

Android location tracking requires Android 8.5 and higher.

- **Poll interval**: Type a numeral and then click **Minutes** or **Hours**, or **Days** to set how often 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 Endpoint Management when the user turns off 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
  - 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 Endpoint Management is required to display the warning message.

- **Device connects to 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 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
Citrix Endpoint Management

allowed location before 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

Android location tracking requires Android 8.5 and higher.

Managed device

- **Location Mode**: Specify the degree of location detection to enable. You can use the Locate security action only when 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.
  - **Off**: Disables location detection.

- **Geofencing**: 

  ![Geofencing settings](image)

  When you enable Geofencing, configure these settings:
- **Poll interval:** Type a numeral and then click **Minutes** or **Hours**, or **Days** to set how often 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, 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.

- **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 Endpoint Management is required to display the warning message.

- **Device connects to 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 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 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 Endpoint Management when the user turns off GPS. The default is **Off**.
- **Geofencing**: See the settings in this article under Managed device.

Lock screen message device policy

December 17, 2018

The Lock screen message policy lets you set messages to appear on the following iOS devices when they are 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**.

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. 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. String length depends on the Apple device model and Apple settings, which can change.

Mail device policy

December 17, 2019

You can add a mail device policy in 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**.
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.
  - **Username**: 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 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 and to forward and 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 Overrideable:** 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 Overrideable:** 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*.
  * **S/MIME Encrypt By Default User Overrideable:** 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 Overrideable:** 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**
Citrix Endpoint Management

- **Remove policy:** To remove the policy at a later time, you can 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 bookmarks device policy**

August 26, 2019

With the Managed bookmarks device policy, you can deploy a folder of bookmarks to Chrome OS devices.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.

**Chrome OS settings**

- **Folder name:** The name of a bookmark folder to deploy to Chrome OS devices.
- **Name:** The name of a bookmark.
- **Bookmark:** The URL for the bookmark.

**Managed domains device policy**

December 17, 2018

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 To place an iOS device in Supervised mode by using the Apple Configurator.

When a user sends email to a recipient whose domain is not on the managed email domains list, the message is flagged on the user’s device to warn them that they are 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 the item. If the item is not from a web domain on the managed web domains list, the user cannot open the item with a corporate app. They must use a personal, unmanaged app.

For supervised devices, even if you do not specify Safari password autofill domains: If the device is configured as ephemeral multi-user, users can’t save passwords. However, if the device isn’t configured as 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:

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>Treat any path under example.com as managed, but not site.example.com/.</td>
</tr>
<tr>
<td>foo.example.com</td>
<td>Treat any path under foo.example.com as managed, but not example.com/ or bar.example.com/.</td>
</tr>
<tr>
<td>*.example.com</td>
<td>Treat any path under foo.example.com or bar.example.com as managed, but not example.com/.</td>
</tr>
<tr>
<td>example.com/sub</td>
<td>Treat example.com/sub and any path under it as managed, but not example.com/.</td>
</tr>
</tbody>
</table>
Format Description

<table>
<thead>
<tr>
<th>foo.example.com/sub</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.example.com/sub</td>
<td>Treat any path under foo.example.com/sub or bar.example.com/sub as managed, but not example.com or foo.example.com/.</td>
</tr>
</tbody>
</table>

Rules:

- Leading “www.” and trailing slashes in URLs are ignored when domains are compared.
- If an entry contains 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 https://site.example.com:8080/page.html, but not https://site.example.com/page.html, whereas 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.
Maps device policy

June 28, 2019

Windows 10 phone devices support offline maps. Use the Maps device policy to specify which maps to download to devices. The Microsoft Maps configuration service provider (CSP) only supports maps of Germany, the United Kingdom, and the United States.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.

Windows Phone settings

To add a map, click Add and then select the Country and State. Repeat those steps to add more maps.

Maximum resident users device policy

August 26, 2019

The Maximum resident users device policy is for Shared iPads. 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.

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: 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. In addition, 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

August 26, 2019

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 To place an iOS device in Supervised mode by using the Apple Configurator.

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 Endpoint Management MDM Options device policy. You can then manage a device from the 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 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 iTunes account credential, you can bypass that step by issuing the Activation Lock Bypass security action from the 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 prior to 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](#).

Office device policy

August 26, 2019

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 Windows 10 Desktop or Tablet running update 1709 or later.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](#).
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.

Organization information device policy

December 17, 2018
The Organization information device policy specifies your organization information for alert messages that are pushed from 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 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

November 21, 2019

The OS Update device policy lets you deploy:

- The latest OS updates to supervised iOS devices.
  The OS Update device policy doesn’t support devices that are both supervised and DEP-enrolled.
- The latest OS and app updates to DEP-enrolled macOS devices running macOS 10.11.5 and later.
- The latest OS updates to supervised Samsung SAFE devices.
  For Samsung SAFE devices, Endpoint Management sends the OS Update policy to Secure Hub, which then applies the policy to the device. The Manage > Devices page shows when Endpoint Management sends the policy and when the device receives the policy.
- The latest OS updates to supervised Windows 10 Desktop and Tablet devices.
  You can also use the OS Update policy to manage delivery optimization settings for desktops and tablets running Windows 10 version 1607. Delivery optimization is a peer-to-peer client update service provided by Microsoft for Windows 10 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).
  - The latest OS updates to Chrome OS devices.
• The specified OS update file to Citrix Ready workspace hub devices.

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 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.
  - **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

© 1999-2019 Citrix Systems, Inc. All rights reserved.
• **OS update options:** Both of the options download the latest macOS updates according to the **OS update frequency.** You can choose to install the updates or notify the user through the App Store that updates are available.

• **OS update frequency:** Determines how frequently Endpoint Management checks and updates the device OS. The default is 7 days.

**Get status for iOS and macOS update actions**

For iOS and macOS, Endpoint Management doesn’t deploy the OS Update policy to devices. Instead, Endpoint Management uses the policy to send these MDM commands to devices:

- Schedule OS Update Scan: Requests that the device performs 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 performs macOS updates, app updates, or both. Thus, the device OS determines when it should download or install 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.
For details such as available OS updates and the last installation attempt, go to the Manage > Devices > Device details (Properties) page.
Samsung SAFE settings

Samsung Enterprise FOTA, also referred to as E-FOTA, lets you determine when devices get updated and the firmware version to use. To use E-FOTA:

1. Create a Samsung MDM License Key device policy with the keys and license information you received from Samsung. For more information, see Samsung MDM license key device policy.
2. Create an OS Update device policy to enable Enterprise FOTA.

- Enable Enterprise FOTA: Set to On.
- Enterprise FOTA License Key: Select the Samsung MDM License Key device policy name.

Windows Desktop and Tablet settings

- Select active hours mode: Select a mode to configure the active hours for performing OS updates. You can specify a range of hours or a start and end time. After you select a mode,
settings appear: **Specify max range for active hours** or **Active hours start** and **Active hours end**. **Not configured** allows Windows to perform 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 initiate 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 a.m. daily. Automatic installation 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 the 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**.

- **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. 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 obtain 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 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 Updates. Default is **Off**.

**Cache size**: The maximum size of the delivery optimization cache. A value of 0 means an unlimited cache. 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**.

**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 attempt 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 the device authenticates to. Selection based on AD DS is for Windows 10, version 1607. Selection based on domain is for Windows 10, version 1511. 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 condi-
tions: 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. Default is 20 GB. A value of 0 means unlimited monthly uploads.

### How Endpoint Management handles approved updates to Windows Desktop and Tablet devices

You can specify whether to install only approved updates. Endpoint Management handles the updates as follows:

- For a security update, such as for Windows Defender definitions, Endpoint Management automatically approves the update and sends an install command to the device during next sync.

- For all other update types, Endpoint Management waits for your approval before sending the install command to the device.

### Prerequisites

- You must upload the Microsoft root certificate to the Endpoint Management server as a server certificate. To get the certificate, go to [https://go.microsoft.com/fwlink/?linkid=747875&clcid=0x409](https://go.microsoft.com/fwlink/?linkid=747875&clcid=0x409).

- 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. Endpoint Management obtains the updates listed in the table from devices.

2. Search for updates with an Approval status of Pending.

3. Click the row for the update 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.

Note: Although the Pending updates table includes add and delete commands, those commands don’t result in any changes to the 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 Endpoint Management to query a device for updates, you must configure and assign to a delivery group at least one OS Update device policy.
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, Endpoint Management saves those updates in its database. To approve any reported updates, edit the policy again.

  Update approval applies only to the policy you are editing. Updates approved in one policy don’t show as approved in another policy. The next time that a device syncs, 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 contains the updates stored in the Endpoint Management database. You must approve updates for each policy.

  During each device sync, 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 update installs, Endpoint Management queries the state of the update until the device reports that the update installed.

- 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 is available. **Windowed** installs an update automatically within the daily maintenance
window specified in the **Start time** and **End time**. **Postpone** allows a user to postpone an update for up to 30 days.

- **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**.

- **Control Enterprise FOTA**: Enables you to control updates to Samsung devices that use the Samsung Enterprise Firmware-Over-the-Air (FOTA) service. For Android Enterprise devices running Samsung Knox 3.0 or later. Default is **Off**.

- **Enterprise FOTA license key**: When **Control Enterprise FOTA** is **On**, **Enterprise FOTA license key** lets you specify the license key to use for Samsung FOTA updates. For Android Enterprise devices running Samsung Knox 3.0 or later. Default is **None**. The key can be set using the **Samsung MDM license key** device policy. See [Samsung MDM license key device policy](#).

**Chrome OS settings**

- **Update enabled**: Specifies whether to update Chrome OS devices automatically to a newly released version of Chrome OS. Default is **Off**.

- **Reboot after update**: Specifies whether to reboot a Chrome OS device the next time that the user signs out after a successful automatic update. Default is **Off**.

- **Target platform version prefix**: If a device is on an older version, this setting specifies the prefix of the target version to update to. For Chrome platform versions, see [https://chromereleases.googleblog.com/](https://chromereleases.googleblog.com/). If a device is already on a version with the given prefix, no update occurs. If the device is on a higher version, it remains on the higher version. Rollback isn’t supported. Default is empty.
Use one of the following version formats:

- """" or unset: Update to latest version available.
- 10323.: Update to any minor version of 10323 (for example, 10323.58.0).
- 10323.58.: Update to any minor version of 10323.58 (for example, 10323.58.0).
- 10323.58.0: Update to this specific version only.

- **Delay update period**: Specifies how long a device can wait before downloading an update. The delay is counted from the time the update first deploys to the server. The device might wait a portion of this time in terms of clock time and the remaining time based on the number of update checks. The maximum duration value is **14** days. Default is **0**.

- **Release channel**: Specifies the Google release channel used to deliver Chrome OS updates. Requires G Suite Chrome configuration.
  - **Delegated**: Means that users can choose the release channel on their devices.
  - **Stable**: The Stable channel is fully tested. By default, Chrome OS updates get distributed over the Stable channel.
  - **Beta**: The Beta channel contains upcoming changes and improvements with low risks.
  - **Dev**: The Dev channel contains the latest features and might be unstable.

**Workspace Hub settings**

You can use the OS Update device policy to specify an update file for Citrix Ready workspace hub devices. When a workspace hub device checks in with the Endpoint Management server, the device downloads the update file and installs it automatically.

- **URL**: The URL where you uploaded the OS update file. First, download the OS update file from the OS vendor and upload it to a share accessible by HTTP or HTTPS. Do not protect the share with any credentials. The update file for a CLASS only applies to devices of the same CLASS.
The URL also must end with the naming used in the OS update file in the format `VERSION-CLASS KERNEL ARCHITECTURE BUILDNUM.lf1`.

When Citrix Ready workspace hub device checks in with the Endpoint Management server, the device downloads the update file and installs it automatically. The installation happens whether the device has a lower or higher OS version that the one being installed.

The policy applies only on devices of the same CLASS as the update file configured in the policy. For example, if the policy has an update file for an NComputing device (NC class), then only the NComputing devices checking in receive the update. If a ViewSonic device (VS class) checks in, Endpoint Management doesn’t apply the update.

- **OS Version:** The OS version in the format `VERSION-CLASS KERNEL ARCHITECTURE BUILDNUM` or `VERSION CLASS Kernel BUILDNUM`.

**Passcode device policy**

November 21, 2019

You create a passcode policy in Endpoint Management based on your organization’s standards. You can require passcodes on users’ devices and can set various formatting and passcode rules. You can create policies for iOS, macOS, Android, Samsung Knox, Android Enterprise, Windows Phone, 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**: In the list, click the minimum passcode length. 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 contain. The default is 0.

- **Passcode security**
  - **Device lock grace period (minutes of inactivity)**: 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 (minutes of 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 fully wiped. The default is Not defined.
• **Policy Settings**
  – Next to **Remove policy**, click either **Select date** or **Duration until removal (in hours)**.
  – If you click **Select date**, click the calendar to select the specific date for removal.
  – If you click **Password required**, next to **Removal password**, type the necessary password.

### 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 you do not enable **Passcode required**, 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**: In the list, click the minimum passcode length. 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 contain. The default is 0.
  - **Passcode security**
    – **Device lock grace period (minutes of inactivity)**: 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 (minutes of 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 locked. The default is Not defined.

- **Delay after failed sign-on attempts, in minutes:** Type the number of minutes to delay before allowing a user to reenter a passcode.

### Policy Settings

- Next to Remove policy, click either Select date or Duration until removal (in hours).
- If you click Select date, click the calendar to select the specific date for removal.
- In the Allow user to remove policy list, click Always, Password required, or Never.
- If you click Password required, next to Removal password, type the necessary password.
- Next to Profile scope, click either User or System. The default is User. This option is available only on macOS 10.7 and later.

### Android settings

- **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, encryption, and Samsung SAFE.
• **Passcode requirements**
  
  – **Minimum length**: In the list, click the minimum passcode length. 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 contain:
    
    * **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**
  
  – **Lock device after (minutes of 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 for the hour or more that encryption takes. If they interrupt the encryption process, they may lose some or all of the data on their devices. After a device is encrypted, the process cannot be reversed except by doing a factory reset, which erases all the data on the device.

• **Samsung SAFE**
As a workaround for disabling face or Iris recognition on Samsung SAFE devices: Create a Restrictions device policy for Samsung SAFE. In the Restrictions policy, turn on **Disable Applications** and add `com.samsung.android.bio.face.service` or `com.samsung.android.server.iris` to the table. Then, deploy the Restrictions policy.

- **Use same passcode across all users**: Select whether to use the same passcode for all users. The default is **Off**. This setting applies only to Samsung SAFE devices and is available regardless of the **Passcode required** setting.
- When you enable **Use same passcode across all users**, type the passcode to be used by all users in the **Passcode** field.
- When you enable **Passcode required**, configure the following Samsung SAFE settings:
  * **Changed characters**: Type the number of characters users must change from their previous passcode. The default is **0**.
  * **Number of times a character can occur**: Type the maximum number of times a character can occur in a passcode. The default is **0**.
  * **Alphabetic sequence length**: Type the maximum length of an alphabetic sequence in a passcode. The default is **0**.
  * **Numeric sequence length**: Type the maximum length of a numeric sequence in a passcode. The default is **0**.
  * **Allow users to make password visible**: Select whether users can make their passcodes visible. The default is **On**.
  * **Configure biometric authentication**: Select whether to enable biometric authentication. The default is **Off**. If you set it to **On**, you can set these options:
    · **Allow fingerprint**: Select to allow users to authenticate using a fingerprint.
    · **Allow iris**: Select to allow users to authenticate using an iris.
  * **Forbidden strings**: You create forbidden strings to prevent users from using insecure strings that are easy to guess like “password”, “pwd”, “welcome”, “123456”, “111111”, and so on. For each string you want to deny, click **Add** and then do the following:
    · **Forbidden strings**: Type the string users may not use.
    · Click **Save** to add the string or click **Cancel** to cancel adding the string.
Samsung Knox settings

**Passcode requirements**

- **Minimum length**: In the list, click the minimum passcode length. The default is 6.
- **Allow users to make password visible**: Select whether to let users make the password visible.
- **Forbidden strings**: You create forbidden strings to prevent users from using insecure strings that are easy to guess like “password”, “pwd”, “welcome”, “123456”, “111111”, and so on. For each string you want to deny, click Add and then do the following:
  - **Forbidden strings**: Type the string users may not use.
  - Click Save to add the string or click Cancel to cancel adding the string.
- **Minimum number of**
  - **Changed characters**: Type the number of characters users must change from their previous passcode. The default is 0.
  - **Symbols**: Type the minimum number of required symbols in a passcode. The default is 0.
- **Maximum number of**
  - **Number of times a character can occur**: Type the maximum number of times a character can occur in a passcode. The default is 0.
  - **Alphabetic sequence length**: Type the maximum length of an alphabetic sequence in a passcode. The default is 0.
  - **Numeric sequence length**: Type the maximum length of a numeric sequence in a passcode. The default is 0.
- **Passcode security**
  - **Lock device after (minutes of inactivity)**: In the list, click the number of seconds a device can be inactive before it is locked. The default is None.
Citrix Endpoint Management

- **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.

- **If the number of failed sign on attempts is exceeded, the device is locked:** In the list, click the number of times a user can fail to sign on successfully after which the device is locked. The default is Not defined.

- **If the number of failed sign on attempts is exceeded, the device is wiped:** In the list, click the number of times a user can fail to sign on successfully, after which the Knox container (along with the Knox data) is wiped from the device. Users need to reinitialize the Knox container after the wiping occurs. The default is Not defined.

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.

For devices running Android 8.0 or later and Samsung Knox 3.0 and later, configure settings for Samsung Knox on the Android Enterprise page. For devices running earlier versions of Android or Samsung Knox, use the Samsung Knox page.
**Note:**
When devices running Samsung Knox 3.0 are enrolled as work profile devices, device passcode settings for Knox 3.0 and later do not apply to the device passcode, even if you configure them.

- **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**.
- **Passcode requirements for device passcode:**
  - **Minimum length:** Specifies the minimum passcode length. The default is 6.
  - **Allow users to make password visible:** 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. Allows users to make the password visible. Default is **Off**.
  - **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**.
  - **Forbidden strings:** 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 strings users can’t use as passcodes. You create forbidden strings to prevent users from using insecure strings that are easy to guess like “password”, “pwd”, “welcome”, “123456”, “111111”, and so on. For each string you want to deny: click **Add**; type the string you don’t want users to use; click **Save** to add the string or click **Cancel** to cancel adding the string.
  - **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 is not 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.
  * **Number of 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 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 (minutes of inactivity) (0-999):** Specifies the number of minutes a device can be inactive before it is locked. The default is None.
  - **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.
  - **Lock the device after (failed sign-on attempts):** 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 times a user can fail to sign on, after which the device is locked. Default is Not defined.

- **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.

- **Passcode requirements for work profile security challenge:**
  - **Minimum length:** Specifies the minimum passcode length. Default is 6.
  - **Allow users to make password visible:** For devices running Knox 3.0 and later that have a valid Knox license key configured. Allows users to make the password visible. Default is Off.
  - **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.

– **Forbidden strings:** For device running Knox 3.0 and later that have a valid Knox license key configured. Specifies strings users can’t use as passcodes. You create forbidden strings to prevent users from using insecure strings that are easy to guess like “password”, “pwd”, “welcome”, “123456”, “111111”, and so on. For each string you want to deny: click Add; type the string you don’t want users to use; click Save to add the string or click Cancel to cancel adding the string.

– **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 is not 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.
  * Number of 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 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 is wiped from the device. Users need to reinitialize the work profile after the wiping occurs. Default is Not defined.
- **Lock container after (minutes of inactivity):** Specifies the number of minutes a device can be inactive before the work profile is locked. The default is **None**.
- **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.
- **Lock the container after (failed sign-on attempts):** For devices running Knox 3.0 and later that have a valid Knox license key configured. Specifies the number of times a user can fail to sign on, after which the device is locked. Default is **Not defined**.

### Windows Phone settings

- **Passcode required:** Select this option to not require a passcode for Windows Phone devices. The default setting is **On**, which requires a passcode. The page collapses and the following options disappear when you disable this setting.
- **Allow simple passcodes:** Select whether to allow simple passcodes. Simple passcodes are a repeated or sequential set of characters. The default is **OFF**.
- **Passcode requirements**
  - **Minimum length:** In the list, click the minimum passcode length. The default is **6**.
  - **Characters required:** In the list, click **Numeric or alphanumerical, Letters only**, or **Numbers only** to configure how passcodes are composed. The default is **Letters only**.
  - **Minimum number of symbols:** In the list, click the number of symbols the passcode must contain. The default is **1**.
• **Passcode security**
  - **Lock device after (minutes of inactivity):** Type the number of minutes a device can be inactive before it is locked. The default is 0.
  - **Passcode expiration in 0-730 days:** 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 (0-50):** 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 before wipe (0-999):** Type the number of times a user can fail to sign on successfully after which corporate data is wiped from the device. The default is 0.

**Windows Desktop/Tablet settings**

- **Passcode security**
  - **Lock device after (minutes of inactivity)(0-999):** Type the number of minutes a device can be inactive before it is locked. The default is 0.
  - **Passcode expiration in 0-730 days:** 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. You must enter a number between 1 and 24 in this field. The default is 0.

- **Passcode requirements**
  - **Minimum length:** In the list, click the minimum passcode length. The default is 6.
Passcode lock grace period device policy

August 26, 2019

The Passcode lock grace period device policy is for Shared iPads. For more information about Shared iPads, see Integrate with Apple Education features.

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

December 17, 2018

You can allow users to connect to the Internet when they are not in range of a WiFi 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
Citrix Endpoint Management

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 remain on by default.

**Power management device policy**

August 26, 2019

The Power management device policy lets you control how Chrome OS devices respond to idle periods when using AC or battery power.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see **Device policies**.

**Chrome OS settings**

The following settings appear for both **AC** and **Battery**.

- **Idle delay**: The length of time without user input before taking the idle action. Specify in minutes. Default for **AC** is 60 minutes. Default for **Battery** is 10 minutes.
- **Idle warning delay**: The length of time without user input before showing a warning dialog. Specify in minutes. Default for **AC** is 58 minutes. Default for **Battery** is 8 minutes. (2 minutes
before the **Idle delay** action starts).

- **Screen dim delay**: The length of time without user input before dimming the screen. Specify in minutes. Default for **AC** is 3 minutes. Default for **Battery** is 1 minute.
- **Screen off delay**: The length of time without user input before turning off the screen. Specify in minutes. Default for **AC** is 10 minutes. Default for **Battery** is 3 minutes.
- **Idle action**: Action to take after reaching the idle delay. Options are **Suspend, Logout, Shut-down,** **Do Nothing**. Default is **Suspend**.

**Profile Removal device policy**

August 26, 2019

You can create an app profile removal device policy in 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**.

**iOS settings**

- **Profile ID**: In the list, click the app profile ID. This field is required.
- **Comment**: Type an optional comment.
macOS settings

- **Profile ID**: In the list, click the app profile ID. This field is required.
- **Deployment scope**: In the list, click either **User** or **System**. The default is **User**. This option is available only on macOS 10.7 and later.
- **Comment**: Type an optional comment.

Provisioning profile device policy

November 18, 2019

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 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 are 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 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 [Create a development provisioning profile](https://developer.apple.com) 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

August 21, 2018

You can remove iOS provisioning profiles with device policies. For more information on provisioning profiles, see **Provisioning profile device policy**.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see **Device policies**.

iOS settings

- **iOS provisioning profile**: In the list, click the provisioning profile you want to remove.
- **Comment**: Optionally, add a comment.

Proxy device policy

November 18, 2019

The Proxy device policy specifies global HTTP proxy settings for supported iOS devices. You can deploy only one global HTTP proxy policy per device.

**Note:**

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 **To place an iOS device in Supervised mode by using the Apple Configurator**.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see **Device policies**.

iOS settings

- **Proxy configuration**: Click **Manual** or **Automatic** for how the proxy will be configured on users’ devices.
If you click Manual, configure these settings:

* **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.
* **Username**: 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 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**
  - Next to **Remove policy**, click either **Select date** or **Duration until removal (in hours)**.
  - If you click **Select date**, click the calendar to select the specific date for removal.
  - If you click **Password required**, next to **Removal password**, type the necessary password.

**Public session device policy**

August 26, 2019

Configure Chrome OS devices to run in a public session that doesn’t require a user to sign on. Instead, a public session prompt appears on the sign on screen.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see **Device policies**.

**Deploy a public session device**

Assign the Public session policy to a specific delivery group rather than the **All Users** group. For information on configuring delivery groups, see **Deploy Resources**. After successfully enrolling the device and signing out, “Public Session” and the configured display name appears on the sign-on screen.

To remove a device from public session mode:

1. Remove the policy from the delivery group.
2. On the **Manage > Devices** page, select the device and then click **Deploy**.

   This action removes the Endpoint Management policies from the device. You can then delete the device from the console.
• Public session
  – Public session enabled: Select whether the public session is enabled or disabled. Requires G Suite Chrome configuration. Default is On.
  – Display name: Type a name to display on the sign-on screen of the device.
  – Session duration in minutes: Type the number of minutes for the session to last. The system signs users out after this amount of time. Default is 60.

• Security
  – Disable Incognito mode: Don’t allow users to browse in Incognito mode. Default is On.
  – Show home button: Allow users to see the home button in their browser. Default is Off.
  – Disable proceeding from the safe browsing warning page: Don’t allow users to proceed to sites that can be harmful. Default is On.
  – Safe browsing mode: Turn on a safe browsing mode that warns users when they’re about to access a potentially harmful site. Default is Off.
  – Disable saving browsing history: Don’t allow the browser to save browsing history or sync tabs from other Chrome OS devices. Default is On.
  – Disable deleting browsing and download history: Don’t allow the user to delete browsing and download history from their session. Users can edit or delete the history database files directly. Default is On.
  – Disable bookmarks bar edit: Don’t allow users to edit the bookmarks you’ve configured. Default is On.
  – External storage accessibility: Select whether users can access external storage devices, such as USB drives. Choose between DEFAULT, READ ONLY, or READ WRITE. Default is DISABLED.
  – Whitelisted websites: Configure a list of websites that users can access. Wildcard expressions are allowed, such as http://*.citrix.com.
  – Blacklisted websites: Configure a list of websites that users can’t access. Wildcard expressions are allowed.

• Content
  – Home page settings: Choose what content users see on the home page. Options are New tab page and Home page URL. Default is New tab page.
  – Pop-up default settings: Select whether pop-ups are allowed. Default is Allow pop-ups.
  – Pop-ups allowed from these sites: If you disallow pop-ups, you can configure specific sites from which to allow pop-ups.
  – Pop-ups not allowed from these sites: If you allow pop-ups, you can configure specific sites from which to block pop-ups.
  – Pages to load on startup: Configure a list of URLs to be loaded when the session begins.

• Bookmarks
  – Enable bookmarks bar: If On, the bookmarks bar is displayed. Default is On.
  – Folder name: Type a name for the bookmarks folder.
- **Bookmark:** Configure a list of bookmarks to appear, including a **Name** and **Bookmark URL**.

- **Chrome apps**
  - **App install allowed:** Select whether users can install apps or not. Options are **Allowed**, **Not allowed**, or **Unspecified**. If you choose **Unspecified**, the device default occurs. Default is **Allowed**.
  - You can also configure a list of apps to specifically allow or disallow.
    * **App name:** Type a name for the app.
    * **App ID:** Type the app ID for the app.
    * **App install allowed:** Select whether this app is **Allowed**, **Not allowed**, or **Unspecified**. Default is **Allowed**.
    * **Installed:** If **On**, the app installs on the device automatically. Default is **Off**.
    * **Pinned:** If **On**, the app is pinned to the task bar. Default is **Off**.
    * **URL:** Type the app URL.
    * **Extension policy:** Type JSON parameters or a URL specific to the app you’re configuring.

**Restrictions device policy**

November 26, 2019

**Note:**
When an upgrade includes new Restrictions device policy settings, you must edit and save the policy. 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 cannot 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 perform the operation or use the feature. For example:

- **Camera:** If **On**, the user can use the camera on their device. If **Off**, the user cannot use the camera on their device.
- **Screenshots:** If **On**, the user can take screenshots on their device. If **Off**, the user cannot take screenshots on their device.

For Windows 10 RS2 Phone: After a Custom XML policy or Restrictions policy that disables Internet
Citrix Endpoint Management

Explorer deploys to the phone, the browser remains enabled. To work around this issue, restart the phone. This issue is a third-party issue.

Note that 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

<table>
<thead>
<tr>
<th>Device Policies</th>
<th>Apps</th>
<th>Media</th>
<th>Actions</th>
<th>Share/Configure</th>
<th>Enrollment Profiles</th>
<th>Delivery Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restrictions Policy</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Policy info</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Platforms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>macOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Android for Work</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Samsung SAFE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Samsung Knox</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Phone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Desktop/Tablet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Mobile/ICE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Some iOS restrictions policy settings apply only to specific versions of iOS, as noted here and in the Endpoint Management console Restrictions policy page.

iOS restrictions policy settings may apply when the device is enrolled in user enrollment mode, unsupervise (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 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 Endpoint Management, the settings apply to the device.
- If an unsupervised iOS 13+ device enrolls in Endpoint Management, the settings don’t apply to the device.
- If an iOS 12 (or lower) device already enrolled in 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 To place an iOS device in Supervised mode by using the Apple Configurator.

<table>
<thead>
<tr>
<th>Setting</th>
<th>User Enrollment</th>
<th>Unsupervised</th>
<th>Supervised</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow hardware controls</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camera</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FaceTime</td>
<td>No</td>
<td>No (new in iOS 13)</td>
<td>Yes</td>
</tr>
<tr>
<td>Screenshots</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow the Classroom app to remotely observe student screens</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow the Classroom app to perform AirPlay and View Screen without prompting</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Photo streams</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Shared photo streams</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Voice dialing</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Siri</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow while device is locked</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Siri profanity filter</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Installing apps</td>
<td>No</td>
<td>No (new in iOS 13)</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow global background fetch while roaming</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Allow apps**

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>iTunes Store</td>
<td>No</td>
<td>No (new in iOS 13)</td>
<td>Yes</td>
</tr>
<tr>
<td>In-app purchases</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>User Enrollment</td>
<td>Unsupervised</td>
<td>Supervised</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Require iTunes password for purchases</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Safari</td>
<td>No</td>
<td>No (new in iOS 13)</td>
<td>Yes</td>
</tr>
<tr>
<td>Autofill</td>
<td>No</td>
<td>No (new in iOS 13)</td>
<td>Yes</td>
</tr>
<tr>
<td>Force fraud warning</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable JavaScript</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Block pop-ups</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Accept cookies</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Network - Allow</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>iCloud actions</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iCloud documents and data</td>
<td>No</td>
<td>No (new in iOS 13)</td>
<td>Yes</td>
</tr>
<tr>
<td>iCloud backup</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iCloud photo keychain</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iCloud photo library</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Security - Force</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted backups</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Limited ad tracking</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Passcode on first AirPlay pairing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Paired Apple Watch to use Wrist Detection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sharing managed documents using AirDrop</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Security - Allow</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accepting untrusted SSL certificates</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>User Enrollment</td>
<td>Unsupervised</td>
<td>Supervised</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------</td>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>Automatic update to certificate trust settings</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Documents from managed apps in unmanaged apps</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Unmanaged apps read managed contacts</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Managed apps write unmanaged contacts</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Documents from unmanaged apps in managed apps</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Diagnostic submission to Apple</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Touch ID to unlock device</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Passbook notifications when locked</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Handoff</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iCloud sync for managed apps</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup for enterprise books</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notes and highlights sync for enterprise books</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Internet results in Spotlight</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enterprise app trust</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Supervised only settings - Allow**
<table>
<thead>
<tr>
<th>Setting</th>
<th>User Enrollment</th>
<th>Unsupervised</th>
<th>Supervised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase all content and settings</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Configuring restrictions</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Podcasts</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Installing configuration profiles</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Fingerprint modification</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Installing apps from device</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Keyboard shortcuts</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Paired Apple watch</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Passcode modification</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Device name modification</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Wallpaper modification</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatically downloading apps</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>AirDrop</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iMessage</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Siri user-generated content</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iBooks</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Removing apps</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Game Center</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Add friends</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Multiplayer gaming</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Modifying account settings</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>User Enrollment</td>
<td>Unsupervised</td>
<td>Supervised</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>-----------------</td>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>Modifying app cellular data settings</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Modifying app cellular data settings</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Modifying Find My Friends settings</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Pairing with non-Configurator hosts</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Predictive keyboards</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Keyboard auto-corrections</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Keyboard spell-check</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Definition lookup</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Single App bundle ID</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>News</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Apple Music service</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iTunes Radio</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Notifications modification</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Restricted App usage</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Diagnostic submission modification</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Bluetooth modification</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow dictation</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Join only WiFi networks installed by a WiFi policy</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>User Enrollment</td>
<td>Unsupervised</td>
<td>Supervised</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>Allow the Classroom app to perform AirPlay and View Screen without prompting</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow the Classroom app to lock to an app and lock the device without prompting</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatically join the Classroom app classes without prompting</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow AirPrint</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow storage of AirPrint credentials in Keychain</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow discovery of AirPrint printers by using iBeacons</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow AirPrint only to destinations with trusted certificates</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Adding VPN configurations</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Modifying cellular plan settings</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Removing system apps</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting up new nearby devices</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow USB restricted mode</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Force delayed software updates</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>User Enrollment</th>
<th>Unsupervised</th>
<th>Supervised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforced software update delay</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Force classroom request permission to leave classes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Force automatic date and time</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Password AutoFill</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Password proximity requests</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Password Sharing</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Security - Show in lock screen

- **Control Center**: Yes
- **Notification**: Yes
- **Today view**: Yes

### Media content - Allow

- **Explicit music, podcasts, and iTunes U material**: No
- **Explicit sexual content in iBooks**: No
- **Ratings region**: No
- **Movies**: No
- **TV Shows**: No
- **Apps**: No

- **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.
  - **Screenshots**: Allow users to take screenshots on their devices.
    - **Allow the Classroom app to remotely observe student screens**: If this restriction
Citrix Endpoint Management

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 perform 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.
- **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.

- **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.
  - **In-app purchases:** Allow users to make in-app purchases.
    - **Require iTunes 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 are not 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**: AirDrop access is a supervised option. Setting this option to On allows supervised devices to use AirDrop to share data and media with nearby iOS devices.

- **Security - Allow**
  - **Accepting untrusted SSL certificates**: Allow users to accept websites’ untrusted SSL certificates.
  - **Automatic update to certificate trust settings**: Allow trusted certificates to be updated automatically.
  - **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 to unlock device**: Allow users to use their fingerprints to unlock their devices.
  - **Passbook notifications when locked**: Allow Passbook 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.
- Internet results in Spotlight: Allow Spotlight to show search results from the Internet as well as 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 as of iOS 12.
- 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 as of iOS 12.

- Supervised only settings - Allow

These settings apply only to supervised devices. For the steps on setting an iOS device to supervised mode, see To place an iOS device in Supervised mode by using the Apple Configurator.

- Erase all content and settings: Allow users to erase all content and settings from their devices.
- Configuring restrictions: Allow users to configure parental controls on their devices.
- 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.
- Fingerprint modification: Allow users to change or delete their Touch ID fingerprint.
- Installing apps from device: Allow users to install apps.
- 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.
- **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.

- **Modifying Find My Friends settings:** Allow users to change their Find My Friends settings.

- **Pairing with non-Configurator hosts:** Allow admin 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 do not want users to be able to look up definitions as they type.

- **Single App bundle ID:** Create a list of apps that are allowed to retain control over the device and prevent interaction with other apps or functions.
  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.
- **iTunes Radio**: Allow users to use iTunes Radio.

- **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.

  **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 proceed, 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 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 is not allowed. The default setting is **On**.

- **Join only WiFi networks installed by a WiFi 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 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 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.

- Enforced software update delay (days): Allows you to specify a 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 automatic date and time:** Allows you to automatically set the date and time on supervised devices. If **On**, device users can't turn off **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 cannot use the AutoFill Passwords or Automatic Strong Passwords features. Default is **On**. Available as of iOS 12.

- **Password proximity requests:** Optional. If disabled, users’ devices don’t request passwords from nearby devices. Default is **On**. Available as of iOS 12.

- **Password Sharing:** Optional. If disabled, users can’t share their passwords using the AirDrop Passwords feature. Default is **On**. Available as of iOS 12.

**Security - Show in lock screen**

- **Control Center:** Allow access to Control Center on the lock screen. 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 obtained. 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 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 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.

### macOS settings

<table>
<thead>
<tr>
<th>Restrictions Policy</th>
<th>Apps</th>
<th>Media</th>
<th>Actions</th>
<th>Sharefile</th>
<th>Enrolment Profiles</th>
<th>Delivery Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Policy Info</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Platforms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>macOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Samsung SAFE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Samsung KNOX</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Phone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Desktop/Tablet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Mobile/CE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 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
· Profiles
· Security & Privacy
· Sharing
· Sound
· Diction & 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**. Repeat this step for each app allowed to launch.
  
  * **Disallowed Folders:** Click **Add**, type the file path to a folder to which you want to restrict user access (for example, /Applications/Utilities), and then click **Save**. Repeat this step for all folders 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 you want users to be able to access.

• **Widgets**

  – **Allow only the following Dashboard widgets to run:** Allow or restrict which Dashboard widgets, such as World Clock or Calculator, users are allowed to run. 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 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 microblogging 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 cannot 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, iTunes, and the App Store. The default is **Off**, which prevents users from using Spotlight Suggestions.

– **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 **Off**, 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](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 Up-
dates. 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.

- **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 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)

**tvOS settings**

- **Security and Media Settings - Allow**
  - **Passcode on first AirPlay pairing:** Require that AirPlay-enabled devices are verified with a one-time onscreen code before they can use AirPlay.
  - **Explicit sexual content in iBooks:** Allow explicit material to be downloaded from iBooks.
  - **Explicit music, podcasts, and iTunes U material:** Allow explicit material on user devices.
  - **In-app purchases:** Allow users to make in-app purchases.
    - *Require iTunes 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.

- **Supervised only settings - Allow**
  - **Device name modification:** Allow users to change the name of their device.
  - **Allow pairing with Apple TV Remote app:** Allow users to pair their device with the Apple TV Remote app.
  - **Siri profanity filter:** 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.
  - **Enable AirPlay:** Allow users to stream content or mirror their iOS device screen on this device.
  - **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.
    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.
If you change this setting to **Only allow some apps:** Before deploying this policy, advise users of devices enrolled using Apple Deployment Program to sign in to their Apple accounts from the Setup Assistant. Otherwise, users might have to disable two-faction authentication on their devices to sign in to their Apple accounts and access allowed apps.

**Android settings**

- **Camera:** Allow users to use the camera on their devices. If **Off**, the camera is disabled. Defaults to **On**.
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.

For devices running Android 8.0 or later and Samsung Knox 3.0 and later, configure settings for Samsung Knox and Samsung SAFE on the Android Enterprise page. For devices running earlier versions of Android or Samsung Knox, use the Samsung Knox and Samsung SAFE pages.

- Allow USB actions
  - Debugging. Allows debugging over USB. Default is Off.
  - File transfer. Allows file transfers over USB. Default is Off.
- Network
– **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**.

– **Android beam.** 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 if **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.** Allows location sharing. For managed profiles, the device owner can override this setting. Default is **Off**.

• **Security**

– **Allow account management.** Allows account to be added to in work profile and managed devices. Default is **Off**.

– **Allow cross profile copy and paste.** Allows or prevents use of the clipboard to copy and paste between apps in the Android Enterprise profile and apps in the personal area. Default is **Off**.

– **Allow Non-Google Play apps.** Allows the installation of apps from stores other than Google Play. 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 use of the status bar.** If set to **On**, this setting enables the status bar on managed devices and dedicated devices (also known as COSU devices). This 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 user control of application settings.** Allows users to uninstall apps, disable apps, clear cache and data, force stop any app, and clear defaults. 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 cannot place work profile app widgets on the device home screen. Default is **Off**.

   * **Apps whose widgets will be allowed.** 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**.

– **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, \texttt{adb shell "pm list packages \(-f\ name"}”, where “name” is part of the package name. For more information, see \url{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, 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 user to configure user credentials: Specify whether users can configure credentials in the managed keystore. Default is On.

- Keep the keyguard from locking the device. If set to On, this setting disables the keyguard on the lock screen on managed devices and dedicated devices (also known as COSU devices). Default is Off.

- Fully Managed Device

  - Allow multiple users. Allows multiple users to use a device (MDM 4.0 and later). Default is On.

  - Allow roaming. Allows users to use cellular data while roaming. The default is OFF, which disables roaming on users’ devices. Default is Off. When this setting is on, these settings are available for Samsung SAFE devices:

    * Data. Allow users to use cellular data for data.
    * Push. Allow users to use cellular data for pushing.
    * Sync. Allow users to use cellular data for syncing.
    * Voice calls. Allow users to use cellular data for voice calls.

  - Allow SMS. Allows users to send and receive SMS messages. Default is Off.

  - Backup. Allows users to back up application and system data on their devices. Default is On.

  - Bluetooth. Allows users to use Bluetooth. Default is On.
Date Time Change. Allows users to change the date and time on their devices. Default is On.

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.

Mass storage. Allows transfer of large data files between users’ devices and a computer over a USB connection. Default is On.

Microphone. Allows users to use the microphone on their devices. Default is On.

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:
  * USB. Allows users to share a mobile data connection with another device using their USB connection.
  * Bluetooth. Allows users to share a mobile data connection with another device using their Bluetooth connection.
  * WiFi. Allows users to share a mobile data connection with another device using their Wi-Fi connection.

WiFi. Allows users to connect to Wi-Fi networks. Default is On. When this setting is on, these settings are available:
  * Direct. Allows users to connect directly to another device through their Wi-Fi connection. For Samsung devices only. For MDM 4.0 and later.
  * State Change. Allows apps to change Wi-Fi connectivity state.

Samsung SAFE: Allow hardware controls

Enable ODE Trusted Boot Verification. Use ODE trusted boot verification to establish a chain of trust from the bootloader to the system image. Default is On.

Allow Emergency Call 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 is in contrast to full disk encryption, which encrypts all data, including settings, application data, downloaded files and applications, media, and other files. Default is On.


DOD boot banner. Displays a DoD approved system use notification message or banner when users’ devices are restarted. Default is Off.

Settings changes. Allows users to change settings on their fully managed devices. Default is On.

Over The Air Upgrade: Allows users’ devices to receive software updates wirelessly (MDM 3.0 and later). Default is On.
- **Background data.** Allows apps to sync data in the background. for fully managed devices. Default is **On**.
- **Clipboard.** Allow users to copy data to the clipboard on their devices.
  - *Clipboard share.* Allow users to share clipboard content between their devices and a computer (MDM 4.0 and later).
- **Home key.** Allows users to use the **Home** key on their fully managed devices. Default is **On**.
- **Mock location.** Allows users to fake their GPS location. For fully managed devices. Default is **On**.
- **NFC.** Allows users to use NFC on their fully managed devices (MDM 3.0 and later). Default is **On**.
- **Power off.** Allows users to turn off their fully managed devices (MDM 3.0 and later). Default is **On**.
- **SD card.** Allows users to use an SD card, if available, with their devices. Default is **On**.
- **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**.
- **Voice dialer.** Allows users to use the voice dialer on their devices (MDM 4.0 and later). Default is **On**.
- **SBeam.** Allows users to share content with others using NFC and Wi-Fi Direct (MDM 4.0 and later). Default is **On**.
- **SVoice.** Allows users to use the intelligent personal assistant and knowledge navigator on their devices (MDM 4.0 and later). Default is **On**.

**Samsung SAFE: Allow apps**

- **Face Recognition:** Allows users to use the face recognition app. Default is **On**.
- **Browser.** Allows users to use the web browser. Default is **On**.
- **Youtube.** Allows users to access YouTube. Default is **On**.
- **Google Play/Marketplace.** Allows users to access Google Play and the Google Apps Marketplace. Default is **On**.
- **Force stop system app.** Allows users to disable pre-installed system apps (MDM 4.0 and later). Default is **On**.

**Samsung SAFE: Network**

- **Incoming Mms.** Allows users to receive MMS messages. Default is **On**.
- **Outgoing Mms.** Allows users to send MMS messages. Default is **On**.
- **Incoming SMS.** Allows users to receive SMS messages. Default is **On**.
- **Outgoing SMS.** Allows users to send SMS messages. Default is **On**.
- **Cellular data.** Allows users to configure mobile networks. Default is **On**.
- **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).
- **Only secure connections.** Allows users to only use secure connections (MDM 4.0 and later). Default is **On**.
- **Audio record.** Allows users to record audio with their devices (MDM 4.0 and later). Default is **On**.
- **Video record.** Allows users to record video with their devices (MDM 4.0 and later). Default is **On**.

**Samsung Knox**

- **Enable Revocation Check.** Enables checking for revoked certificates. Default is **On**.
- **Move Apps To Container.** Allows users to move apps between the Knox container and the personal area on their devices. Default is **On**.
- **Enforce Multifactor Authentication.** Users must use a fingerprint and one other authentication method, such as password or PIN, to open their devices. Default is **On**.
- **Enable TIMA Key store.** 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 **On**.
- **Enforce Auth For Container.** Use a different authentication method from the method used to unlock the device to open the KNOX container. Default is **On**.
- **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 **On**.
- **Use Secure Keypad.** Forces users to use a secure keyboard inside the Knox container. Default is **On**.
- **Authentication Smart Card Browser.** Enables browser authentication on devices equipped with a smart card reader.
- **Enable Samsung DeX.** Enables supported Knox-enabled devices to run in Samsung DeX mode. Requires Samsung Knox 3.1 (minimum version). Default is **On**. For information about Samsung DeX device requirements and setting up Samsung DeX, see How Samsung DeX works.
  - **Allow Ethernet in DeX mode only.** Enables use of Ethernet in Samsung DeX mode. Cellular data, Wi-Fi, and tethering (Wi-Fi, Bluetooth, and USB) are restricted in DeX mode. Default is **On**. When this setting is on, these settings are available:
  - **Upload DeX logo image.** Select this setting to specify a .png image to use as an icon for Samsung DeX.
  - **DeX screen timeout (seconds).** Specify the amount of idle time, in seconds, after which the DeX screen turns off. To disable the timeout, type **0**. Default is **1200** seconds (20 minutes).
Citrix Endpoint Management

- **Add App shortcut in Samsung DeX.** Specify an app package name to add a shortcut for the app to DeX. To look up an app package name, go to Google Play and select the app. The URL includes the package name: https://play.google.com/store/apps/details?id=<package.name>.

- **Remove App shortcut in Samsung DeX.** Specify an app package name to remove a shortcut from DeX. Go to Google Play to look up app package names.

- **App packages to disable in DeX.** Specify a comma-separated list of the app packages that you want to block from Samsung DeX mode. For example: "com.android.chrome", "com.google.android.gm".

**Samsung SAFE settings**

Some options are available only under specific Samsung Mobile Device Management APIs. Those options are marked with the relevant version information.

- **Allow hardware controls**
  - **Enable ODE Trusted Boot Verification:** Use ODE trusted boot verification to establish a chain of trust from the bootloader to the system image.
  - **Allow Development Mode:** Allow users to enable the developer settings on their devices.
  - **Allow Emergency Call Only:** Allow users to enable Emergency Call Only mode on their devices.
  - **Allow Firmware Recovery:** Allow users to recover the firmware on their devices.
  - **Allow Fast Encryption:** Allow encryption of only used memory space. This is in contrast to full disk encryption, which encrypts all data, including settings, application data, downloaded files and applications, media, and other files.
**Citrix Endpoint Management**

- **Common Criteria Mode**: Place device into Common Criteria Mode. The Common Criteria configuration enforces stringent security processes.
- **Factory Reset**: Allow users to do a factory reset on their devices.
- **Date Time Change**: Allow users to change the date and time on their devices.
- **DOD reboot banner**: Display a DoD approved system use notification message or banner when users' devices are restarted.
- **Settings changes**: Allow users to change settings on their devices.
- **Backup**: Allow users to back up application and system data on their devices.
- **Over The Air Upgrade**: Allow users' devices to receive software updates wirelessly (MDM 3.0 and later).
- **Background data**: Allow apps to sync data in the background.
- **Camera**: Allow users to use the camera on their devices.
- **Clipboard**: Allow users to copy data to the clipboard on their devices.
  - **Clipboard share**: Allow users to share clipboard content between their devices and a computer (MDM 4.0 and later).
- **Home key**: Allow users to use the Home key on their devices.
- **Microphone**: Allow users to use the microphone on their devices.
- **Mock location**: Allow users to fake their GPS location.
- **NFC**: Allow users to use NFC on their devices (MDM 3.0 and later).
- **Power off**: Allow users to turn off their devices (MDM 3.0 and later).
- **Screenshot**: Allow users to take screenshots on their devices.
- **SD card**: Allow users to use an SD card, if available, with their devices.
- **Voice Dialer**: Allow users to use the voice dialer on their devices (MDM 4.0 and later).
- **SBeam**: Allow users to share content with others using NFC and Wi-Fi Direct (MDM 4.0 and later).
- **SVoice**: Allow users to use the intelligent personal assistant and knowledge navigator on their devices (MDM 4.0 and later).
- **Allow multiple users**: Allow multiple users to use a device (MDM 4.0 and later). Defaults to Off.

**Allow apps**

- **Browser**: Allow users to use the web browser.
- **Youtube**: Allow users to access YouTube.
- **Google Play/Marketplace**: Allow users to access Google Play and the Google Apps Marketplace.
- **Allow Non-Google Play apps**: Allow users to download apps from sites other than Google Play and the Google Apps Marketplace. If On, a user can use the security settings on their device to trust apps from unknown sources.
- **Stop system app**: Allow users to disable pre-installed system apps (MDM 4.0 and later).
- **Disable applications**: If On, blocks a specified list of apps from running on Samsung SAFE
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, Endpoint Management enables com.example2.

- **Network**
  - **Incoming Mms**: Allow users to receive MMS messages.
  - **Incoming Sms**: Allow users to receive SMS messages.
  - **Outgoing Mms**: Allow users to send MMS messages.
  - **Outgoing Sms**: Allow users send SMS messages.
  - **User Add profiles VPN**:
    - **Bluetooth**: Allow users to use Bluetooth.
      - **Tethering**: Allow users to share a mobile data connection with another device using their Bluetooth connection.
    - **WiFi**: Allow users to connect to Wi-Fi networks.
      - **Tethering**: Allow users to share a mobile data connection with another device using their Wi-Fi connection.
      - **Direct**: Allow users to connect directly to another device through their Wi-Fi connection (MDM 4.0 and later).
      - **State Change**: Allow apps to change Wi-Fi connectivity state.
      - **User Policy Changes**: Allow users to change Wi-Fi policies. If not selected, users can change only the Wi-Fi user name and password. If selected, users can change all Wi-Fi policies.
  - **Tethering**: Allow users to share a mobile data connection with another device.
  - **Cellular data**: Allow users to use their cellular connection for data.
  - **Allow roaming**: Allow users to use cellular data while roaming. The default is OFF, which disables roaming on users’ devices.
  - **Only secure connections**: Allow users to only use secure connections (MDM 4.0 and later).
  - **Android beam**: Allow users to send webpages, photos, videos, or other content from their devices to another device using NFC (MDM 4.0 and later).
  - **Audio record**: Allow users to record audio with their devices (MDM 4.0 and later).
  - **Video record**: Allow users to record video with their devices (MDM 4.0 and later).
  - **Location services**: Allow users to turn on GPS on their devices.
  - **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 USB actions** Allow USB connection between users’ devices and a computer.
  - **Debugging:** Allow debugging over USB.
  - **Host storage:** Allow 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.
  - **Mass storage:** Allow transfer of large data files between users’ devices and a computer over a USB connection.
  - **Kies media player:** Allow users to use the Samsung Kies tool to sync files between their devices and a computer.
  - **Tethering:** Allow users to share a mobile data connection with another device through a USB connection.

### Samsung Knox settings

<table>
<thead>
<tr>
<th>Device Policies</th>
<th>Apps</th>
<th>Media</th>
<th>Actions</th>
<th>ShareFile</th>
<th>Enrollment Profiles</th>
<th>Delivery Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrictions Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Policy Info</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>2 Platforms</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ iOS</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ macOS</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ Samsung SAFE</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ Samsung KNOX</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ Windows Phone</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ Windows Desktop/Tablet</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ Amazon</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ Windows Mobile/CE</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>3 Assignment</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>

### Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

- **Allow use of camera**
- **Enable Revocation Check**
- **Move Apps To Container**
- **Enforce Multifactor Authentication**
- **Enable TIMA Key store**
- **Enforce Auth Per Container**
- **Share List**
- **Enable Audit Log**
- **Use Secure Keypad**
- **Enable Google Apps**

<table>
<thead>
<tr>
<th>Device Policies</th>
<th>Apps</th>
<th>Media</th>
<th>Actions</th>
<th>ShareFile</th>
<th>Enrollment Profiles</th>
<th>Delivery Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrictions Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Policy Info</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>2 Platforms</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ iOS</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ macOS</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ TV OS</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ Android</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ Android Enterprise</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ Samsung SAFE</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□ Samsung KNOX</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>

- **Authentication Smart Card browser**
- **Enable Samsung Dex**

- **Add App shortcut in Samsung Dex**
- **Remove App shortcut in Samsung Dex**

- **App packages to disable in Samsung Dex**
These options are available only under Samsung Knox Premium (minimum version is Knox 2.0).

- **Allow Use of Camera**: Allow users to use the camera on their devices.
- **Allow Revocation Check**: Enable checking for revoked certificates.
- **Move Apps To Container**: Allow users to move apps between the Knox container and the personal area on their devices.
- **Enforce Multifactor Authentication**: Users must use a fingerprint and one other authentication method, such as password or PIN, to open their devices.
- **Enable TIMA Key store**: 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.
- **Enforce Auth For Container**: Use a different authentication method from the method used to unlock the device to open the KNOX container.
- **Share List**: Allow users to share content between apps in the Share Via list.
- **Enable Audit Log**: Enable creation of event audit logs for forensic analysis of a device.
- **Use Secure Keypad**: Force users to use a secure keyboard inside the Knox container.
- **Enable Google Apps**: Allow users to download apps from Google Mobile Services into the Knox container.
- **Authentication Smart Card Browser**: Enable browser authentication on devices equipped with a smart card reader.
- **Enable Samsung DeX**: Enables supported Knox-enabled devices to run in Samsung DeX mode. Requires Samsung Knox 3.1 (minimum version). Default is **On**. For information about Samsung DeX device requirements and setting up Samsung DeX, see [How Samsung DeX works](#).
- **Allow Ethernet in DeX mode only**: Enable use of Ethernet in Samsung DeX mode. Cellular data, Wi-Fi, and tethering (Wi-Fi, Bluetooth, and USB) are restricted in DeX mode.
- **Upload DeX logo image**: Select this setting to specify a .png image to use as an icon for Samsung DeX.
- **DeX screen timeout**: Specify the amount of idle time, in seconds, after which the DeX screen turns off. To disable the timeout, type **0**. Default is **1200** seconds (20 minutes).
- **Add App shortcut in Samsung DeX**: Specify an app package name to add a shortcut for the app to DeX. To look up an app package name, go to Google Play and select the app. The URL includes the package name: [https://play.google.com/store/apps/details?id=package.name](https://play.google.com/store/apps/details?id=package.name).
- **Remove App shortcut in Samsung DeX**: Specify an app package name to remove a shortcut from DeX. Go to Google Play to look up app package names.
- **App packages to disable in DeX**: Specify a comma-separated list of the app packages that you want to block from Samsung DeX mode. For example: "com.android.chrome", "com.google.android.gm".
Windows Phone and Windows Desktop/Tablet settings

- WiFi Settings
  - Allow WiFi: Allow a device to connect to a Wi-Fi network. Windows Phone only.
  - Allow Internet sharing: Allow a device to share its internet connection with other devices by turning it into a Wi-Fi hotspot.
  - Allow auto-connect to WiFi Sense hotspots: Allow a device to connect automatically to Wi-Fi Sense hotspots. Location services must be enabled for this option to work. For more information about Wi-Fi Sense, see the Windows Phone WiFi Sense FAQ.
  - Allow manual configuration: Allow users to manually configure Wi-Fi connections. Windows Phone only.

- Connectivity
  - Allow NFC: Allow device to communicate with an NFC tag or another NFC-enabled transmitting device. Windows Phone only.
  - Allow Bluetooth: Allow device to connect through Bluetooth. Windows Phone only.
  - 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.
  - Allow USB connection: Allow a desktop to access a device’s storage through a USB connection. Windows Phone only.
  - 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.
• **Search:** Windows Phone only.
  – **Allow search to use location:** Allow searches to use the device’s location service.
  – **Filter adult content:** Allow adult content. The default is **Off**, which means adult content is not filtered.
  – **Allow Bing Vision to store images:** Allow Bing Vision to store images captured when performing Bing Vision searches.

• **System**
  – **Allow storage card:** Allow the device to use a storage card.
  – **Telemetry:** In the list, click an option 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 location services:** Allow 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.

• **Security:** Windows Phone only
  – **Allow manual root certificate installation:** Allow users to manually install a root certificate.
  – **Require device encryption:** Require device encryption. After encryption is enabled on a device, it cannot be disabled. The default is **Off**.
  – **Allow copy and paste:** Allow users to copy and paste data on their devices.
  – **Allow screen capture:** Allow users to create screen captures on their devices.
  – **Allow voice recording:** Allow users to use voice recording on their devices.
  – **Allow Save As of Office files:** Allow users to save Office files with Save As.
  – **Allow action center notifications:** Allow Action Center notifications on the device lock screen.
  – **Allow Cortana:** Allow users access to Cortana, the intelligent personal assistant and knowledge navigator.
  – **Allow sync of device settings:** Allow users to sync settings between Windows Phone 8.1 devices when roaming.

• **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 Endpoint Management MDM.
- **Allow sync of device settings**: Allow users to sync settings between Windows 10 devices when roaming.

**Above Lock**: Windows Desktop/Tablet only
- **Allow toasts**: Allow toast notifications on the lock screen. Windows Desktop/Tablet only

**Apps**
- **Allow store access**: Allow users to access the Microsoft Store. Windows Phone only.
- **Allow developer unlock**: Allow users to register their devices with Microsoft and develop or install apps that are not in the Windows Phone app store. Windows Phone only.
- **Allow web browser access**: Allow Internet Explorer on the device. Windows Phone only.
- **Allow appstore auto update**: Allow apps from the app store to automatically update. Windows Desktop/Tablet only.

**Privacy**: Windows Desktop/Tablet only
- **Allow input personalization**: Allows the input personalization service to run, to improve 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**
  - **Non-Amazon Appstore apps**: Allow users to install non-Amazon Appstore apps on their devices.
  - **Social networks**: Allow users to access social networks from their devices.
- **Network**
  - **Bluetooth**: Allow users to use Bluetooth.
  - **WiFi switch**: Allow apps to change Wi-Fi connectivity state.
  - **WiFi settings**: Allow users to change Wi-Fi settings.
  - **Cellular data**: Allow users to use their cellular connection for data.
  - **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.
**Chrome OS settings**

**User policy**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable form autofill</td>
<td>On</td>
</tr>
<tr>
<td>Disable password saving</td>
<td>On</td>
</tr>
<tr>
<td>Disable page translation</td>
<td>On</td>
</tr>
<tr>
<td>Block images</td>
<td>Off</td>
</tr>
<tr>
<td>Disable Incognito mode</td>
<td>Off</td>
</tr>
<tr>
<td>Disable saving browsing history</td>
<td>Off</td>
</tr>
<tr>
<td>Disable deleting browsing and download history</td>
<td>Off</td>
</tr>
<tr>
<td>Disable printing</td>
<td>Off</td>
</tr>
<tr>
<td>Disable proceeding from the safe browsing warning page</td>
<td>Off</td>
</tr>
<tr>
<td>Safe browsing mode</td>
<td>On</td>
</tr>
<tr>
<td>Enable bookmarks bar</td>
<td>On</td>
</tr>
<tr>
<td>Disable bookmarks bar edit</td>
<td>On</td>
</tr>
<tr>
<td>Disable task manager and process</td>
<td>On</td>
</tr>
<tr>
<td>Show home button</td>
<td>On</td>
</tr>
<tr>
<td>External storage accessibility</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

- **Disable form autofill**: Select whether to allow the autofill function of the Chrome browser. If this policy is set to **On**, autofill function is not allowed. Default is **On**.

- **Disable password saving**: Select whether to allow the save password function in the Chrome browser. If this policy is set to **On**, the save password function not allowed. Default is **On**.

- **Disable page translation**: Select whether to allow translation of webpages that are in other languages in the Chrome browser. If this policy is set to **On**, translation of webpages is not allowed.
Default is On.

- **Block images**: Select whether to allow display of images in webpages in the Chrome browser. If this policy is set to On, images in webpages in the Chrome browser are not displayed. Default is Off.

- **Disable Incognito mode**: If On, Chrome OS device users can’t open an Incognito window in Chrome. Requires G Suite Chrome configuration. Default is On.

- **Disable saving browsing history**: If On, users can’t save browsing history, override this setting, or sync tabs from Chrome OS devices. Requires G Suite Chrome configuration. Default is Off.

- **Disable deleting browsing and download history**: If On, users can’t delete browsing or download history from Chrome OS devices. However, even if you prevent users from deleting history from Chrome, users might be able to edit or delete the history database files directly. The browser itself can expire or archive any or all history items at any time. Requires G Suite Chrome configuration. Default is Off.

- **Disable printing**: If On, users can’t print from Google Chrome. Printing is disabled in locations such as the wrench menu, extensions, and Javascript apps. Printing is possible from plugins that bypass Google Chrome to print, such as Flash apps with a Print command in their context menu. Requires G Suite Chrome configuration. Default is Off.

- **Disable proceeding from the safe browsing warning page**: If Off, users can continue from the warning page to visit the potentially malicious site from Chrome OS devices. Requires G Suite Chrome configuration. Default is On.

- **Safe browsing mode**: If Off, Google Safe Browsing mode is never active. Users can’t change or override the “Protect you and your device from dangerous sites” setting in Chrome. Requires G Suite Chrome configuration. Default is On.

- **Enable bookmarks bar**: If On, Chrome displays the bookmarks bar. Requires G Suite Chrome configuration. Default is On.

- **Disable bookmarks bar edit**: If On, users can’t add, update, or delete bookmarks. Requires G Suite Chrome configuration. Default is On.

- **Disable task manager end process**: If On, disables the End Process button in Task Manager. Requires G Suite Chrome configuration. Default is On.

- **Show home button**: If On, Chrome displays the browser home button. Requires G Suite Chrome configuration. Default is On.

- **External storage accessibility**: Controls how users access external storage devices through the file browser. Requires G Suite Chrome configuration. Options:
  - **Disabled**: No access to external storage.
  - **Read only**: Users can have read access external storage only.
- **Write only:** Users can have write access external storage only. Default is **Disabled**.

- **Websites:** Select whether to control access to websites in the Chrome browser using a whitelist or blacklist. If you choose **Whitelist**, you specify a list of allowed URLs. If you choose **Blacklist**, you specify a list of URLs that are exceptions to blacklisted URL specified in Chrome policies in the Google admin console. The most specific filter determines if a URL is blocked or allowed. The whitelist takes precedence over the blacklist. Default is **Blacklist**. After you make a selection, click **Add** to add a list of websites.

- **Extension sources:** Specify the list of URLs that allow users to install extensions, apps, and themes.

### Device policy

<table>
<thead>
<tr>
<th>Restrictions Policy</th>
<th>Device Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Policy Info</td>
<td>Disable Guest user mode</td>
</tr>
<tr>
<td>2 Platforms</td>
<td>Single sign-on IDP redirection</td>
</tr>
<tr>
<td></td>
<td>Enable device state reporting</td>
</tr>
<tr>
<td></td>
<td>Enable recent users reporting</td>
</tr>
<tr>
<td></td>
<td>Single sign-on cookie behavior</td>
</tr>
<tr>
<td></td>
<td>Enable App Runtime for Chrome (ARC)</td>
</tr>
<tr>
<td></td>
<td>Force re-enrollment</td>
</tr>
<tr>
<td></td>
<td>Device Disabled Message</td>
</tr>
<tr>
<td></td>
<td>Sign-in-auto complete domain name</td>
</tr>
<tr>
<td></td>
<td>Device time zone settings</td>
</tr>
<tr>
<td></td>
<td>System time zone</td>
</tr>
</tbody>
</table>

- **Disable Guest user mode:** If **On**, guest users can’t sign on to Chrome OS devices. Requires G Suite Chrome configuration. The default is **Off**.

- **Single sign-on IDP redirection:** If **On**, enables SAML-based single sign-on. Requires G Suite Chrome configuration. The default is **On**.

- **Enable device state reporting:** If **On**, a device reports its current device state, including firmware, Chrome and platform version, and boot mode. Requires G Suite Chrome configuration. Default is **On**.

- **Enable recent users reporting:** If **On**, the device reports a list of users that recently logged on to the device. Users aren’t reported if the device is configured to erase all local user data. Requires
G Suite Chrome configuration. Default is **On**.

- **Single sign-on cookie behavior:** If **On**, transfers cookies set by a SAML IdP to user profiles each time a user signs on with SAML credentials. If **Off**, cookies transfer during the first sign-on only. Requires G Suite Chrome configuration. The default is **On**.

- **Enable App Runtime for Chrome (ARC):** If **On**, allows enrolled Chrome OS device users to run Android apps. Specify ARC apps in the App Restrictions device policy. Requires G Suite Chrome configuration. ARC isn’t available if either Ephemeral mode or multiple sign-on is enabled in the current user session. If **Off**, enterprise Chrome OS device users can’t run Android apps. The default is **On**.

- **Forced re-enrollment:** If set to **On**, forces devices to re-enroll into their previous G Suite domain after a device wipe. Requires G Suite Chrome configuration. Default is **On**.

- **Device Disabled Message:** If the device is disabled for any reason, the user sees the message entered into this text box.

- **Sign-in autocomplete domain name:** If set to a domain name, such as `students.school.edu`, Chrome shows the domain name as an autocomplete option when users sign in. If left blank, Chrome doesn’t show an autocomplete option for the domain name. Requires G Suite Chrome configuration.

- **Device time zone settings:**
  - **System time zone:** Selects the time zone for the Chrome device.
  - **Time zone detection:** Specifies settings used to detect the time zone. Requires G Suite Chrome configuration.
    * **Users decide:** Allows users to configure the policy through standard Date and Time settings on the Chrome OS device.
    * **Disabled:** Denies access to the time zone information.
    * **IP only:** Sets the time zone based on the device IP address.
    * **WiFi access points:** Sets the time zone based on the user’s Wi-Fi connection.
    * **Use Location info:** Sets the time zone by detecting the user’s present location.

- **Users allowed to sign on:** Limits the users who can sign on to Chrome OS devices, based on an email suffix, such as `*@example.com`.

## Roaming device policy

**December 17, 2018**

You can add a device policy in 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](#).
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.

Samsung MDM license key device policy

August 26, 2019

Use the Samsung MDM license key device policy if you have legacy Enterprise Licenses (ELM) and Knox Licenses (KLM). If you have a Knox Platform for Enterprise (KPE) premium license key, use the **Knox Platform for Enterprise device policy** instead. A premium license key is required to create a Knox container.

For the SAFE platform, use the macro to generate the ELM key. Deploy the Samsung Enterprise License Management (ELM) key to a device before you can deploy SAFE policies and restrictions. Endpoint Management also supports the Samsung Enterprise Firmware-Over-The-Air (E-FOTA) service. Endpoint Management supports and extends both Samsung for Enterprise (SAFE) and Samsung Knox policies.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see Device policies.

Samsung SAFE settings

![Samsung MDM License Key Policy](image)
• **ELM License key:** Endpoint Management pre-fills this field with the macro that generates the ELM license key. If the field is blank, type this macro: `${elm.license.key}`

### Configure Samsung E-FOTA settings

Samsung Enterprise FOTA (E-FOTA) lets you determine when devices get updated and the firmware version to use. E-FOTA enables you to test updates before deploying them, to ensure that the updates are compatible with your apps. You can force devices to update with the latest firmware version available, without requiring user interaction.

Samsung supports E-FOTA for Samsung Knox 2.7.1 devices (minimum version) that are running authorized firmware.

To configure an E-FOTA policy:

1. Create a Samsung MDM License Key device policy with the keys and license information you received from Samsung. Endpoint Management then validates and registers the information.

   Type the **ELM License key:** Endpoint Management pre-fills this field with the macro that generates the ELM license key. If the field is blank, type this macro: `${elm.license.key}`

   Type the following information provided by Samsung when you purchased an E-FOTA package:
   - **Enterprise FOTA Customer ID**
   - **Enterprise FOTA license**
   - **Client ID**
   - **Client Secret**

2. Create a Control OS Update device policy.

   - **Enable Enterprise FOTA:** Set to **On**.
   - **Enterprise FOTA License Key:** Select the Samsung MDM License Key policy name that you created in Step 1.

3. Deploy the Control OS Update policy to Secure Hub.
Android Enterprise and Samsung Knox settings

- **Knox License key**: Type the Knox license key that you obtained from Samsung.

SCEP device policy

August 26, 2019

This policy allows you to configure iOS and macOS devices to retrieve a certificate using Simple Certificate Enrollment Protocol (SCEP) from an external SCEP server. If you want to deliver a certificate to the device using SCEP from a PKI that is connected to Endpoint Management, you should 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 may be safe to send the request unencrypted. If, however, the one-time password is allowed to be reused, you should use HTTPS to protect the password. This step is required.

- **Instance name**: Type any string that the SCEP server recognizes. For example, it could 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 a X.500 name represented as an array of Object Identifier (OID) and value. For example, \[
\{ \{ ["C","US"], ["O","Apple Inc."], \ldots, ["1.2.5.3","bar"] \} \]. 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**: In the list, click an alternative name type. The SCEP policy can specify an optional alternative name type that provides 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 should 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)**: In the list, click the key size in bits, either 1024 or 2048. The default is 1024.

- **Use as digital signature**: Specify whether you want the certificate to be used as a digital signature. If someone is using the certificate to verify a digital signature, such as verifying whether a
Certificate was issued by a CA, the SCEP server would verify that the certificate can be used in this manner prior to using the public key to decrypt the hash.

- **Use for key encipherment**: Specify whether you want the certificate to be used for key encipherment. If a server is using the public key in a certificate provided by a client to verify that a piece of data was encrypted using the private key, the server would first check to see whether the certificate can be used for key encipherment. If not, the operation fails.

- **SHA1/MD5 fingerprint (hexadecimal string)**: If your CA uses HTTP, use this field to provide the fingerprint of the CA certificate, which the device uses to confirm authenticity of the CA response during enrollment. You can enter a SHA1 or MD5 fingerprint, or you can select a certificate to import its signature.

### 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 may be safe to send the request unencrypted. If, however, the one-time password is allowed to be reused, you should use HTTPS to protect the password. This step is required.

- **Instance name**: Type any string that the SCEP server recognizes. For example, it could 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 a X.500 name represented as an array of Object Identifier (OID) and value. For example, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, which would translate 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:** In the list, click an alternative name type. The SCEP policy can specify an optional alternative name type that provides 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 should 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.

- **Key size (bits):** In the list, click the key size in bits, either 1024 or 2048. The default is 1024.

- **Use as digital signature:** Specify whether you want the certificate to be used as a digital signature. If someone is using the certificate to verify a digital signature, such as verifying whether a certificate was issued by a CA, the SCEP server would verify that the certificate can be used in this manner prior to using the public key to decrypt the hash.

- **Use for key encipherment:** Specify whether you want the certificate to be used for key encipherment. If a server is using the public key in a certificate provided by a client to verify that a piece of data was encrypted using the private key, the server would first check to see whether the certificate can be used for key encipherment. If not, the operation fails.

- **SHA1/MD5 fingerprint (hexadecimal string):** If your CA uses HTTP, use this field to provide the fingerprint of the CA certificate, which the device uses to confirm authenticity of the CA response during enrollment. You can enter a SHA1 or MD5 fingerprint, or you can select a certificate to import its signature.

---

**Siri and dictation policies**

August 26, 2019

When users ask Siri something or dictate text on managed iOS devices, Apple collects the voice data for purposes of improving Siri. The voice data passes through Apple’s cloud-based services, and therefore exists outside the secure Endpoint Management container. The text that results from dictation, however, remains within the container.

Endpoint Management allows you to block Siri and dictation services, as your security needs require.

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 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:

- 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. For more information, see this Wired article, Apple reveals how long Siri keeps your data.
- 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

December 17, 2018

The SSO account device policy lets you create single sign-on (SSO) accounts in Endpoint Management. Those accounts let users sign on one-time only to access 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 backend.

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)**: In the list, click an optional identity credential that can be used to renew the Kerberos credential without user interaction.
- **Kerberos realm**: Enter the Kerberos realm for this policy. This 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 web site initiates a Kerberos challenge: If that site is not in the URL list, the iOS device does not 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 is not.
    Also, if Kerberos is not activated based on host matching, the URL still falls back to a standard HTTP call. This could 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.
Storage encryption device policy

August 21, 2018

You create storage encryption device policies in Endpoint Management to encrypt internal and external storage, and, depending on the device, to prevent users from using a storage card on their devices.

You can create policies for Samsung SAFE, Windows Phone, and Android Sony devices. 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](#).

**Prerequisites**

For Samsung SAFE devices, make sure the following requirements are met before you configure this policy:

- Set the Screen Lock option on user devices.
- Plug in users devices and charge them to at least 80%.
- Make sure that the devices require a password containing both numbers and letters or symbols.

**Samsung SAFE settings**

- **Encrypt internal storage**: Select whether to encrypt internal storage on users’ devices. Internal storage includes device memory and internal storage. The default is **On**.
- **Encrypt external storage**: Select whether to encrypt external storage on users’ devices. The default is **On**.

**Windows Phone settings**

- **Require device encryption**: Select whether to encrypt users’ devices. The default is **Off**.
- **Disable storage card**: Select whether to prevent users from using a storage card on their devices. The default is **Off**.

**Android Sony settings**

- **Encrypt external storage**: Select whether to encrypt external storage on users’ devices. The device must require a password containing both numbers and letters or symbols. The default is **On**.
Store device policy

August 21, 2018
You can create a policy in Endpoint Management to specify whether devices display an app store webclip 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 webclip appears on user devices. The default is On.

Subscribed calendars device policy

August 21, 2018
You can add a device policy in 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 at www.apple.com/downloads/macosx/calendars.

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.
- Username: 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**.

### Terms and conditions device policy

August 21, 2018

You create terms and conditions device policies in 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 Endpoint Management, they are presented with the terms and 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**.

### Windows Phone and 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**.
**Verified access device policy**

August 26, 2019

On Chrome OS devices, administrators can enable verified access. With verified access enabled, devices cannot access the network unless they are unmodified and are policy-compliant. For more information on Verified Access, see [Enable Verified Access with Chrome devices](#).

You can configure the verified access 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](#).

**Chrome OS settings**

- **User Verified Access**
  - **Enable user verified access:** If enabled, users must comply with the Verified Access requirements to access your network. Requires G Suite Chrome configuration. Default is **On**.
  - **Access Control - Accounts with Full Access:** List of users allowed to call the Verified Access API and receive device IDs. Requires G Suite Chrome configuration.
  - **Access Control - Accounts with Limited Access:** List of users allowed to call the Verified Access API but can't receive device IDs. Requires G Suite Chrome configuration.

- **Device Verified Access**
- **Enable device verified access**: If enabled, devices must comply with the Verified Access requirements to access your network. Requires G Suite Chrome configuration. Default is On.

- **Enable Content Protection**: If enabled, the device can play protected content. Requires G Suite Chrome configuration. Default is On.

- **Access Control - Accounts with Full Access**: List of devices allowed to call the Verified Access API and receive device IDs. Requires G Suite Chrome configuration.

- **Access Control - Accounts with Limited Access**: List of devices allowed to call the Verified Access API but can’t receive device IDs. Requires G Suite Chrome configuration.

## VPN device policy

November 21, 2019

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.

## iOS settings

**To prepare for device upgrades to iOS 12:**

The Citrix VPN connection type in the VPN device policy for iOS doesn’t support iOS 12. Perform 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. Important 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.
Citrix Endpoint Management

- **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. For more information, see the Endpoint Management support article [https://support.citrix.com/article/CTX227708](https://support.citrix.com/article/CTX227708).
    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.
  - **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**.

**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 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.

  - If you enable Password, type an optional authentication password in the Auth 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 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 domains 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 contains 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 **Auth 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 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 domains 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 contains 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 **Auth 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 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 domains 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 contains 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.
Citrix Endpoint Management

- **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 **Auth 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 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.
  - **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 domains 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 contains 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 **Auth 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 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 domains 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 IKEv2 protocols for iOS**

This section includes settings used for the IKEv2, AlwaysOn IKEv2, and AlwaysOn IKEv2 Dual Configuration protocols. For the AlwaysOn IKEv2 Dual Configuration protocol, configure all these settings for both Cellular and Wi-Fi networks.

- **Allow user to disable automatic connection:** For the AlwaysOn protocols. Select whether to allow users to turn off 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.

- **Machine Authentication:** Choose **Shared Secret** or **Certificate** 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**.

- **Extended Authentication Enabled:** Select whether to enable Extended Authentication Protocol (EAP). If you choose **On**, type the **User account** and **Authentication password**.

- **Dead Peer Detection Interval:** Choose how often a peer device is contacted to ensure that the peer device remains 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 NAT keepalive while the device is asleep**: For the AlwaysOn 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 contained 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 contains an empty string, then that string is the default domain. This is how 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 **SHA1-96**.

  - **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.

- **Service Exceptions**: For the AlwaysOn protocols. Service exceptions are system services that are exempt from AlwaysOn 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**


- **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 **Auth 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 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 domains 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.
  - useragent: Associates with this device policy any Citrix Gateway policies that are targeted to VPN plug-in clients. For requests initiated 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-anyconnect/id1135064690, add the app to 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.
- **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 **Auth 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 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**: 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 domains 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 parameter or click **Cancel** to not save the parameter.

**To 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`

The values in step 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**
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 cannot 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 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.
    - 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 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 is not 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 cannot resolve the domain, redirects to a different server, or times out.
  * NeverConnect: The domain never triggers a VPN connection.

- ActionParameters: RequiredDNSServers: For each DNS server IP address to be used for resolving the specified domains, click Add and do the following:
  * DNS Server: Valid only when ActionParameters : DomainAction = ConnectIfNeeded. Type the DNS server to add. This server doesn’t need to be part of the device’s current network configuration. If the DNS server is not reachable, a VPN connection is established in response. This DNS server should 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 doesn’t respond, a VPN connection is established. Valid only when ActionParameters : DomainAction = ConnectIfNeeded.

- OnDemandRules: XML content: Type, or copy and paste, XML configuration on demand rules.
  * Click Check Dictionary to validate the XML code. You see Valid XML in green text below the XML content text box if the XML is valid. If it isn’t valid, you see an error message in orange text describing 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.
      · **Username:** 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**
  - Under Policy Settings, next to Remove policy, select either **Select date** or **Duration until removal (in hours)**.
  - If you select **Select date**, click the calendar to select the specific date for removal.
  - If you select **Password required**, next to Removal password, type the necessary password.

### 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:
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 contains apps.)
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.

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**.
  - 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 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 Auth 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 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 initiate network communication. The default is Off.
    - **Safari domains:** For each Safari domains 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 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 **Auth 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 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 domains 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 **Auth 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 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 domains 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 **Auth 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 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 domains 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.
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 **Auth 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 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 domains 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 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**.

*Click **Save** to save the domain or click **Cancel** to not save the domain.*
– If you enable Password, type an optional authentication password in the Auth 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 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 domains 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:
  – 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 cannot 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. Pos-
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 each domain against which a user device’s search domain list can match that you want to add, 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 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.

- **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 is not 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 cannot resolve the domain, redirects to a different server, or times out.

* NeverConnect: The domain never triggers a VPN connection.

- ActionParameters: RequiredDNSServers: For each DNS server IP address to be used for resolving the specified domains, click Add and do the following:

  * DNS Server: Valid only when ActionParameters : DomainAction = ConnectIfNeeded. Type the DNS server to add. This server doesn’t need to be part of the device’s current network configuration. If the DNS server is not 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 cannot 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, XML configure on demand rules.

  * Click Check Dictionary to validate the XML code. You see Valid XML in green text below the XML content text box if the XML is valid. If it isn’t valid, you see an error message in orange text describing 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.
Android settings

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 initiates 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:
Citrix Endpoint Management

- **Connect**: The client initiates a VPN connection in the untrusted network.
- **Do Nothing**: The client starts a VPN connection in the untrusted network. This option disables 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 Citrix SSO protocol for Android

- **Connection name**: Type a name for the VPN connection. This field is required.
- **Server name or IP address**: Type the FQDN or IP address of the Citrix 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 per-app VPN, all traffic goes through the Citrix VPN tunnel. If you enable per-app VPN, specify the following settings. The default is Off.
  - **Whitelist or Blacklist**: If Whitelist, all apps in the whitelist tunnel through this VPN. If Blacklist, all apps except those apps on the blacklist tunnel through this VPN.
  - **Application List**: Specify the whitelisted or blacklisted apps. Click Add and then type a comma-separated list of app package names.

- **Custom XML**: Click Add and then type custom parameters. Endpoint Management supports these parameters for Citrix VPN:
  - **DisableUserProfiles**: Optional. To enable this parameter, type Yes for the Value. If enabled, Endpoint Management doesn’t display user-added VPN connections and the user cannot 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.

**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](#).

**Samsung SAFE settings**

- **Connection name**: Type a name for the connection.
- **VPN type**: In the list, select the protocol to be used for this connection. The default is **L2TP with pre-shared key**. Possible options are:
  - **L2TP with pre-shared key**: Layer 2 Tunneling Protocol with pre-shared key authentication. This setting is the default.
  - **L2TP with certificate**: Layer 2 Tunneling Protocol with certificate.
  - **PPTP**: Point-to-Point Tunneling.
  - **Enterprise**: Your corporate VPN connection. Applicable to SAFE versions earlier than 2.0.
  - **Generic**: A generic VPN connection. Applicable to SAFE versions 2.0 or higher.

**Configure L2TP with pre-shared key protocol for Samsung SAFE**

- **Host name**: Type the name of the VPN host. This option is required.
- **User name**: Type an optional user name.
- **Password**: Type an optional password.
- **Pre-shared key**: Type the pre-shared key. This option is required.
Configure L2TP with certificate protocol for Samsung SAFE

- **Hostname:** Type the name of the VPN host. This option is required.
- **Username:** Type an optional user name.
- **Password:** Type an optional password.
- **Identity credential:** In the list, select the identity credential to be used. The default is **None**.

Configure PPTP protocol for Samsung SAFE

- **Hostname:** Type the name of the VPN host. This option is required.
- **Username:** Type an optional user name.
- **Password:** Type an optional password.
- **Enable encryption:** Select whether to enable encryption on the VPN connection.

Configure Enterprise protocol for Samsung SAFE

- **Hostname:** Type the name of the VPN host. This option is required.
- **Enable backup server:** Select whether to enable a backup VPN server. If enabled, in **Backup VPN server**, type the FQDN or IP address of the backup VPN server.
- **Enable user authentication:** Select whether to require user authentication. If enabled, configure the following settings:
  - **Username:** Type a user name.
  - **Password:** Type the user password.
- **Group name:** Type an optional group name.
- **Authentication method:** In the list, select the authentication method to be used. Possible options are:
  - **Certificate:** Use certificate authentication. This setting is the default. If selected, in the **Identity credential** list, select the credential to use. The default is **None**.
  - **Pre-shared key:** Use a pre-shared key. If selected, in the **Pre-shared key** field, type the shared secret key.
  - **Hybrid RSA:** Use hybrid authentication using RSA certificates.
  - **EAP MD5:** Authenticate the EAP peer to the EAP server, but does no mutual authentication.
  - **EAP MSCHAPv2:** Use Microsoft's Challenge-Handshake authentication for mutual authentication.
- **CA certificate:** In the list, select the certificate to be used. The default is **None**.
- **Enable default route:** Select whether to enable a default route to the VPN server. The default is **Off**.
- **Enable smartcard authentication:** Select whether to allow users to authenticate by using smart cards. The default is **Off**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
• **Enable mobile option:** Select whether to enable mobile option. The default is Off.

• **Diffie-Hellman group value (key strength):** In the list, select the key strength to be used. The default is 0.

• **Split tunnel type:** In the list, select the type of split tunnel to use. The default is Auto. Possible options are:
  - **Auto:** Split tunneling is used automatically.
  - **Manual:** Split tunneling is used over the IP address and port specified on the VPN server.
  - **Disabled:** Split tunneling is not used.

• **SuiteB type:** In the list, select the level of NSA Suite B encryption to use. The default is **GCM-128**. Possible options are:
  - **GCM-128:** Use 128-bit AES-GCM encryption.
  - **GCM-256:** Use 256-bit AES-GCM encryption.
  - **GMAC-128:** Use 128-bit AES-GMAC encryption.
  - **GMAC-256:** Use 256-bit AES-GMAC encryption.
  - **None:** Use no encryption.

• **Forward 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 generic protocol for Samsung SAFE

• **Host name:** Type the name of the VPN host. This option is required.

• **Enable user authentication:** Select whether to require user authentication. If enabled, in **Password**, type the user password.

• **User name:** Type a user name.

• **Package Name Agent VPN:** The package name, or ID, of the VPN installed on the device; for example, Mocana or Pulse Secure.

• **VPN Connection type:** In the list, select either **IPSEC** or **SSL** for the connection type to be used. The default is **IPSEC**. The following sections describe the configuration settings for each connection type.

### Configure IPSEC connection type settings for Samsung SAFE

• **Identity:** Type an optional identifier for this configuration.

• **IPSec group ID type:** In the list, select the IPsec group ID type to use. The default is **Default**.
  Possible options are:
  - **Default**
  - **IPv4 address**
- Fully qualified domain name (FQDN)
- User FQDN
- IKE key ID

- **IKE version:** In the list, select the Internet Key Exchange version to use. The default is **IKEv1**.
- **Authentication method:** In the list, select the authentication method to be used. The default is **Certificate**. Possible options are:
  - **Certificate:** Use certificate authentication. If selected, in the **Identity credential** list, select the credential to use. The default is **None**.
  - **Pre-shared key:** Use a pre-shared key. If selected, in the **Pre-shared key** field, type the shared secret key.
  - **Hybrid RSA:** Use hybrid authentication using RSA certificates.
  - **EAP MD5:** Authenticate the EAP peer to the EAP server, but does no mutual authentication.
  - **EAP MSCHAPv2:** Use Microsoft’s Challenge-Handshake authentication for mutual authentication.
  - **CAC based Authentication:** Use a Common Access Card (CAC) for authentication.

- **Identity credential:** In the list select the identity credential to use. The default is **None**.
- **CA certificate:** In the list, select the certificate to be used.
- **Enable dead peer detection:** Select whether to contact a peer to ensure that it remains alive. The default is **Off**.
- **Enable default route:** Select whether to enable a default route to the VPN server.
- **Enable mobile option:** Select whether to enable mobile option.
- **ike LifeTime in Minutes:** Type the number of minutes before the VPN connection must be reestablished. The default is 1440 minutes (24 hours).
- **ipsec LifeTime in Minutes:** Type the number of minutes before the VPN connection must be reestablished. The default is 1440 minutes (24 hours).
- **Diffie-Hellman group value (key strength):** In the list, select the key strength to be used. The default is **0**.
- **IKE Phase 1 key exchange mode:** Select either **Main** or **Aggressive** for the IKE Phase 1 negotiation mode. The default is **Main**.
  - **Main:** No information is exposed to potential attackers during negotiation, but is slower than **Aggressive** mode.
  - **Aggressive:** Some information (for example, the identity of the negotiating peers) is exposed to potential attackers during negotiation, but is faster than **Main** mode.
- **Perfect forward secrecy (PFS) value:** Select whether to use PFS to require a new key exchange renegotiating a connection.
- **Split tunnel type:** In the list, select the type of split tunnel to use. Possible options are:
  - **Auto:** Split tunneling is automatically used.
  - **Manual:** Split tunneling is used over the IP address and port specified on the VPN server.
  - **Disabled:** Split tunneling is not used.
• **IPSEC Encryption algorithm:** A VPN configuration that the IPsec protocol uses.
• **IKE Encryption Algorithm:** A VPN configuration that the IPsec protocol uses.
• **IKE Integrity Algorithm:** A VPN configuration that the IPsec protocol uses.
• **Vendor:** A personal profile for generic agents that communicate with the Knox API.
• **Forward 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.
• **Per App VPN:** For each per-app VPN you want to add, click **Add** and do the following:
  – **Per App VPN:** The VPN configuration that the app uses to communicate.
  – Click **Save** to save the per-app VPN or click **Cancel** to not save the per-app VPN.

**Configure SSL connection type settings for Samsung SAFE**

• **Authentication method:** In the list, select the authentication method to be used. The default is **Not Applicable**. Possible options are:
  – **Not Applicable**
  – **Certificate:** Use certificate authentication. If selected, in the **Identity credential** list, select the credential to use. The default is **None**.
  – **CAC based Authentication:** Use a Common Access Card (CAC) for authentication.
• **CA certificate:** In the list, select the certificate to be used.
• **Enable default route:** Select whether to enable a default route to the VPN server.
• **Enable mobile option:** Select whether to enable mobile option.
• **Split tunnel type:** In the list, select the type of split tunnel to use. Possible options are:
  – **Auto:** Split tunneling is automatically used.
  – **Manual:** Split tunneling is used over the IP address and port specified on the VPN server.
  – **Disabled:** Split tunneling is not used.
• **SSL Algorithm:** Type the SSL algorithm to use for client-server negotiation.
• **Vendor:** A personal profile for generic agents that communicate with the Knox API.
• **Forward 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.
• **Per App VPN:** For each per-app VPN you want to add, click **Add** and do the following:
  – **Per App VPN:** The VPN configuration that the app uses to communicate.
  – Click **Save** to save the per-app VPN or click **Cancel** to not save the per-app VPN.
When you configure any policy for Samsung Knox, it applies only inside the Samsung Knox container.

- **VPN Type:** In the list, select the type of VPN connection to configure. The connection can be either **Enterprise** (applicable to Knox versions earlier than 2.0) or **Generic** (applicable to Knox versions 2.0 or higher). The default is **Enterprise**.

The following sections list the configuration options for each of the preceding connection types.

**Configure Enterprise protocol for Samsung Knox**

- **Connection name:** Type a name for the connection. This field is required.
- **Host name:** Type the name of the VPN host. This option is required.
- **Enable backup server:** Select whether to enable a backup VPN server. If enabled, in **Backup VPN server**, type the FQDN or IP address of the backup VPN server.
- **Enable user authentication:** Select whether to require user authentication. If enabled, configure the following settings:
  - **Username:** Type a user name.
  - **Password:** Type the user password.
- **Group name:** Type an optional group name.
- **Authentication method:** In the list, select the authentication method to be used. Possible options are:
  - **Certificate:** Use certificate authentication. For certificate authentication, also select the credential to use from the **Identity credential** list.
Citrix Endpoint Management

- **Pre-shared key**: Use a pre-shared key. If selected, in the **Pre-shared key** field, type the shared secret key.
- **Hybrid RSA**: Use hybrid authentication using RSA certificates.
- **EAP MD5**: Authenticate the EAP peer to the EAP server, but does no mutual authentication.
- **EAP MSCHAPv2**: Use Microsoft’s Challenge-Handshake authentication for mutual authentication.

- **CA certificate**: In the list, select the certificate to be used.
- **Enable default route**: Select whether to enable a default route to the VPN server.
- **Enable smartcard authentication**: Select whether to allow users to authenticate by using smart cards. The default is **Off**.
- **Enable mobile option**: Select whether to enable mobile option.
- **Diffie-Hellman group value (key strength)**: In the list, select the key strength to be used. The default is **0**.
- **Split tunnel type**: In the list, select the type of split tunnel to use. Possible options are:
  - **Auto**: Split tunneling is automatically used.
  - **Manual**: Split tunneling is used over the IP address and port specified on the VPN server.
  - **Disabled**: No split tunneling is used.
- **SuiteB type**: In the list, select the level of NSA Suite B encryption to use. Possible options are:
  - **GCM-128**: Use 128-bit AES-GCM encryption: This setting is the default.
  - **GCM-256**: Use 256-bit AES-GCM encryption.
  - **GMAC-128**: Use 128-bit AES-GMAC encryption.
  - **GMAC-256**: Use 256-bit AES-GMAC encryption.
  - **None**: Use no encryption.
- **Forward routes**: Click **Add** to add any optional forwarding routes if your corporate VPN server supports multiple route tables.

**Configure generic protocol for Samsung Knox**

- **Connection name**: Type a name for the connection. This field is required.
- **Package Name Agent VPN**: The package name, or ID, of the VPN installed on the device; for example, Mocana or Pulse Secure.
- **Host name**: Type the name of the VPN host. This option is required.
- **Enable user authentication**: Select whether to require user authentication. If enabled, configure the following settings:
  - **User name**: Type a user name.
  - **Password**: Type the user password.
- **Identity**: Type an optional identifier for this configuration. Only applies when **Vpn Connection type** = **IPSEC**.
- **Vpn Connection type**: In the list, select either **IPSEC** or **SSL** for the connection type to be used.
The default is IPSEC. The following sections describe the configuration settings for each connection type.

- **Configure IPSEC connection settings**
  - **IPsec group ID type:** In the list, select the IPsec group ID type to use. The default is Default. Possible options are:
    - Default
    - IPv4 address
    - Fully qualified domain name (FQDN)
    - User FQDN
    - IKE key ID
  - **IKE version:** In the list, select the Internet Key Exchange version to use. The default is IKEv1.
  - **Authentication method:** In the list, select the authentication method to be used. The default is Certificate. Possible options are:
    - Certificate: Use certificate authentication. If selected, in the Identity credential list, select the credential to use. The default is None.
    - Pre-shared key: Use a pre-shared key. If selected, in the Pre-shared key field, type the shared secret key.
    - Hybrid RSA: Use hybrid authentication using RSA certificates.
    - EAP MDS: Authenticate the EAP peer to the EAP server, but does no mutual authentication.
    - EAP MSCHAPv2: Use Microsoft’s Challenge-Handshake authentication for mutual authentication.
    - CAC based Authentication: Use a Common Access Card (CAC) for authentication.
  - **CA certificate:** In the list, select the certificate to be used.
  - **Enable dead peer detection:** Select whether to contact a peer to ensure that it remains alive. The default is Off.
  - **Enable default route:** Select whether to enable a default route to the VPN server.
  - **Enable mobile option:** Select whether to enable mobile option.
  - **ike LifeTime in Minutes:** Type the number of minutes before the VPN connection must be reestablished. The default is 1440 minutes (24 hours).
  - **ipsec LifeTime in Minutes:** Type the number of minutes before the VPN connection must be reestablished. The default is 1440 minutes (24 hours).
  - **Diffie-Hellman group value (key strength):** In the list, select the key strength to be used. The default is 0.
  - **IKE Phase 1 key exchange mode:** Select either Main or Aggressive for the IKE Phase 1 negotiation mode. The default is Main.
    - Main: No information is exposed to potential attackers during negotiation, but is slower than Aggressive mode.
- **Aggressive**: Some information (for example, the identity of the negotiating peers) is exposed to potential attackers during negotiation, but is faster than **Main** mode.

- **Perfect forward secrecy (PFS) value**: Select whether to use PFS to require a new key exchange renegotiating a connection.

- **Split tunnel type**: In the list, select the type of split tunnel to use. Possible options are:
  * **Auto**: Split tunneling is automatically used.
  * **Manual**: Split tunneling is used over the IP address and port specified on the VPN server.
  * **Disabled**: Split tunneling is not used.

- **SuiteB Type**: In the list, select the level of NSA Suite B encryption to use. The default is **GCM-128**. Possible options are:
  * **GCM-256**: Use 256-bit AES-GCM encryption.
  * **GMAC-128**: Use 128-bit AES-GMAC encryption.
  * **GMAC-256**: Use 256-bit AES-GMAC encryption.
  * **None**: Use no encryption.

- **IPSEC Encryption algorithm**: VPN configuration that the IPsec protocol uses.

- **IKE Encryption Algorithm**: VPN configuration that the IPsec protocol uses.

- **IKE Integrity Algorithm**: VPN configuration that the IPsec protocol uses.

- **Knox**: Configurations for Samsung Knox only.

- **Vendor**: A personal profile for generic agents that communicate with the Knox API.

- **Forward 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.

- **Per App VPN**: For each per-app VPN you want to add, click **Add** and do the following:
  * **Per App VPN**: The VPN configuration the app uses to communicate.
  * Click **Save** to save the per-app VPN or click **Cancel** to not save the per-app VPN.

• **Configure SSL connection settings**

- **Authentication method**: In the list, click the authentication method to use. Possible options are:
  * **Not Applicable**: No authentication method applies. This setting is the default.
  * **Certificate**: Use certificate authentication. This setting is the default. If selected, in the Identity credential list, select the credential to use. The default is None.
  * **CAC based Authentication**: Use a Common Access Card (CAC) for authentication.

- **CA certificate**: In the list, select the certificate to be used.

- **Enable default route**: Select whether to enable a default route to the VPN server.

- **Enable mobile option**: Select whether to enable mobile option.

- **Split tunnel type**: In the list, select the type of split tunnel to use. Possible options are:
* **Auto:** Split tunneling is automatically used.
* **Manual:** Split tunneling is used over the IP address and port specified.
* **Disabled:** No split tunneling is used.

- **SuiteB Type:** In the list, select the level of NSA Suite B encryption to use. The default is GCM-128. Possible options are:
  * **GCM-128:** Use 128-bit AES-GCM encryption.
  * **GCM-256:** Use 256-bit AES-GCM encryption.
  * **GMAC-128:** Use 128-bit AES-GMAC encryption.
  * **GMAC-256:** Use 256-bit AES-GMAC encryption.
  * **None:** Use no encryption: Type the SSL algorithm to use for client-server negotiation.

- **SSL Algorithm:** Type the SSL algorithm to use for client-server negotiation.
- **Knox:** Configurations for Samsung Knox only.
- **Vendor:** A personal profile for generic agents that communicate with the Knox API.
- **Forward 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.

- **Per App VPN:** For each per-app VPN you want to add, click **Add** and do the following:
  * **Per App VPN:** The VPN configuration the app uses to communicate.
  * Click **Save** to save the per-app VPN or click **Cancel** to not save the per-app VPN.

### Windows Phone settings

![Windows Phone settings](image_url)
These settings are supported only on Window 10 and later supervised phones.

- **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. The following sections describe the settings for each of these options.
- **Configure Native profile type settings:** These settings apply to the VPN built into users’ Windows phones.
  - **VPN server name:** Type the FQDN or IP address for the VPN server. This field is required.
  - **Tunneling protocol:** 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 Microsoft Challenge-Handshake authentication for mutual authentication. This option is not available when you select IKEv2 for the tunnel type. When you choose MSChapV2, an **Automatically use Windows credentials** option appears. The default is Off.
  - **EAP method:** In the list, select the EAP method to be used. The default is TLS. This field is not available when MSChapV2 authentication is enabled. Possible options are:
    - **TLS:** Transport Layer Security
    - **PEAP:** Protected Extensible Authentication Protocol
  - **DNS Suffix:** Type the DNS suffix.
  - **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 Require smart card certificate is enabled.
  - **Remember credential:** Select whether to cache the credential. The default is OFF. When enabled, credentials are cached whenever possible.
  - **Always on VPN:** Select whether the VPN is always on. The default is OFF. When enabled, the VPN connection remains 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 protocol type:** These settings apply to VPN plug-ins obtained from the Win-
Citrix Endpoint Management

dows Store and installed on users’ devices.

- **Server address**: Type the URL, host name, or IP address for the VPN server.
- **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.
- **DNS Suffix**: Type the DNS suffix.
- **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.
- **Remember credential**: Select whether to cache the credential. The default is OFF. When enabled, credentials are cached whenever possible.
- **Always on VPN**: Select whether the VPN is always on. The default is OFF. When enabled, the VPN connection remains on until the user manually disconnects.
- **Bypass For Local**: Type the address and port number to allow local resources to bypass the proxy server.

### Windows Desktop/Tablet settings

![Windows Desktop/Tablet settings](image)

- **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 Microsoft’s Challenge-Handshake authentication for mutual authentication. This option is not 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 is not available when MSChapV2 authentication is enabled. Possible options are:
  * 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 remains 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 obtained 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.
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 remains on until the user manually disconnects.
- **Bypass For Local**: Type the address and port number to allow local resources to bypass the proxy server.

### 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.
• **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.

• **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.
  - 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.
Chrome OS settings

- VPN connection name: Type a user-friendly description of this connection. This setting is required.
- Priority of this network: Type a suggested priority value for this network. Use an integer value.
- Connection type: In the list, select OpenVPN as the connection type.

Selecting OpenVPN reveals more settings that are specific to OpenVPN connections. Scroll to see all settings.
• **Host**: Type the host name or IP address of server the VPN connects to. Required for OpenVPN. The value you type here is the primary host. Optionally, you can configure extra hosts to connect to if the primary host fails to connect.

• **Auto connect**: Select whether the VPN connects to the host automatically. If this setting is set to **ON**, the VPN connects to the host automatically. Default is **OFF**.

• **Port**: Type the host server port number. Default is **1194**.

• **Protocol**: Type the protocol used when communicating with the host server. Default is **UDP**.

• **User authentication type**: In the list, choose the required form of user authentication:
  - **None**: No password or one-time PIN required.
  - **Password**: Password only. You can configure this value or let the user provide it at the time of connection.
  - **Password and OTP**: Password and one-time PIN. You can configure these values or let the user provide it at the time of connection.
  - **OTP**: One-time PIN. You can configure this value or let the user provide it at the time of connection.

• **User name**: Type the user name that is used to connect to the VPN. If not specified, user is
prompted for a user name at time of connection. This value is subject to text string expansions:
- \${LOGIN_ID} expands to the email address of the user before the @ symbol.
- \${LOGIN_EMAIL} - expands to the email address of the user.

- **Password:** Type the password text string that is used to connect to the VPN. If not specified, user is prompted for a password at time of connection.
- **OTP:** Type the one-time PIN text string that is used to connect to the VPN. A password text string. If not specified, user is prompted for a one-time PIN at time of connection.
- **Save credentials:** Select whether user credentials are saved after a connection. If this setting is set to **OFF**, users must enter their credentials each time they connect.
- **Cache credentials in memory:** Select whether user passwords and one-time PINs entered by users are cached in memory on the device. If this setting is set to **ON**, caching is enabled. Default is **OFF**.
- **Auth:** Type the authentication algorithm used to secure the connection. Defaults to **SHA-1**.
- **Authentication retry type:** In the list, select the way the VPN responds when user credentials are not verified. Options are **Fail with error on retry**, **Retry without asking for authentication**, and **Ask again for authentication each time**. Default is **Fail with error on retry**.
- **Cipher:** Type the cipher algorithm used to secure connection. Default is **BF-CBC**.
- **LZO compression:** Select whether to use LZO compression for the VPN. If this setting is set to **ON**, the VPN uses LZO compression. Default is **OFF**.
- **Adaptive compression:** Select whether to use adaptive compression for the VPN. If this setting is set to **ON**, the VPN uses adaptive compression. Default is **OFF**.
• **Extra hosts**: Configure a list of hosts to try, in order, if the device cannot connect to the primary host. Configuring these extra hosts is optional.

  1. Click **Add** to the right of **Host name**.
  2. Type the host name or IP address of server.
  3. Click **Save**.

   Repeat these steps to add more extra hosts.

• **Server poll time-out in seconds**: Type the maximum number of seconds to try to connect to this server before moving on to the next server in the list.

• **Ignore default route**: Select whether the host ignores VPN gateway. By default, the device creates a default route to the gateway address advertised by the VPN server. If this setting is set to ON, split tunneling is allowed. Default is OFF. If the server pushes a redirect-configuration flag to the client, this setting is ignored.

• **Key direction**: Type the key direction text string. The key direction is passed in as “–key-direction”.

• **Peer certificate type**: Type “server” to check the peer certificate type. If this setting is not set, the peer certificate type is not checked.

• **Push peer information**: Select whether peer certificate information is pushed to this host. If this setting is set to **ON**, peer information is pushed. Default is **OFF**.
• **Peer certificate extended key usage**: Type the explicit extended key usage text string, in OID notation, with which the peer certificate must be signed. Optional.

• **Peer certificate key usage**: Add key usage numbers required. These strings are hex encoded numbers.

• **Peer certificate TLS**: Require peer certificate signing based on RFC3280TLS rules. Default is None.

• **Data channel key renegotiation delay in seconds**: Type an integer to indicate the number of seconds to wait before renegotiation a channel key.

• **Bandwidth limit**: Type an integer to indicate the outgoing tunnel bandwidth limit by number of bytes per second.

• **Static challenge**: Type a string used in static challenge responses.

• **TLS auth key contents**: Type the TLS key contents here. If this field is empty, TLS authentication can’t be used.

• **TLS remote connections**: Type an X.509 name or common name to allow connections to only server hosts that share that name.

• **TLS minimum version**: Type the minimum TLS protocol version used by OpenVPN.

• **Verbosity level**: Type an integer for the verbosity level for TLS. If not specified, the verbosity level defaults to OpenVPN’s default.

• **Verbosity hash**: If set, this value is passed as the --verify-hash argument to OpenVPN. The hash specifies the SHA1 fingerprint for the level-1 certificate.

• **Verify host’s X509 name**: Type the host’s X.509 name used for comparison in verifying the name.

• **Verify host’s X509 name type**: Select a type of X.509 name to be verified. Options are name, name-prefix, or subject.

---

**Wallpaper device policy**

December 17, 2018

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. To use different wallpaper 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.
<table>
<thead>
<tr>
<th>Device</th>
<th>Image dimensions in pixels</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 5, 5c, 5s</td>
<td>640 x 1136</td>
</tr>
<tr>
<td>iPhone 6, 6s</td>
<td>750 x 1334</td>
</tr>
<tr>
<td>iPhone 6 Plus</td>
<td>1080 x 1920</td>
</tr>
<tr>
<td>iPad Air, 2</td>
<td>1536 x 2048</td>
</tr>
<tr>
<td>iPad 4, 3</td>
<td>1536 x 2048</td>
</tr>
<tr>
<td>iPad Mini 2, 3</td>
<td>1536 x 2048</td>
</tr>
</tbody>
</table>

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.

**Web content filter device policy**

April 25, 2019

You can filter web content on iOS devices by using the Apple auto-filter function with specific sites that you add to whitelists and blacklists. 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 **To place an iOS device in Supervised mode**.

**Note:**

Android devices don’t support web content filtering.

To add or configure this policy, go to **Configure > Device Policies**. For more information, see **Device policies**.

**iOS settings**

- **Filter type**: In the list, click either **Built-in** or **Plug-in**, 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 or not the auto filter allows access. For each URL you want to add to the whitelist, click **Add** and do the following:
    * Type the URL of the permitted website. You must add `https://` or `http://` before the web address.
    * Click **Save** to save the website to the whitelist or click **Cancel** not to save it.
  - **Blacklisted URLs:** Items in this list are always blocked. For each URL you want to add to the blacklist, click **Add** and do the following:
    * Enter the URL of the website to be blocked. You must add `https://` or `http://` before the web address.
    * Click **Save** to save the website to the blacklist or click **Cancel** not to save it.

- **Bookmark whitelist**
  - **Bookmark Whitelist:** Specifies the sites that users can access. To enable access to web sites, add their URL.
    * **URL:** The URL of each web site that users can access. For example, to enable access to the Secure Hub store, add the Endpoint Management server URL to the **URL** list. You must add `https://` or `http://` 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 web site. For example, type “Google” for the URL `https://google.com`.
    * Click **Save** to save the website to the whitelist 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 plugin 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:** In the list, click an optional identity certificate 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.

### Webclip device policy

August 21, 2018

You can place shortcuts, or webclips, to websites to appear alongside apps on users’ devices. You can specify your own icons to represent the webclips for iOS, macOS, and Android devices; Windows tablet only requires a label and a URL.

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 webclip.
• **URL:** Type the URL associated with the webclip. The URL must begin with a protocol, for example, **https://server**.
• **Removable:** Select whether users can remove the webclip. The default is **Off**.
• **Icon to be updated:** Select the icon to be used for the webclip 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 web page opens in full-screen mode. The default is **Off**.

### macOS settings

• **Label:** Type the label that is to appear with the webclip.
• **URL:** Type the URL associated with the webclip. The URL must begin with a protocol, for example, **https://server**.
• **Icon to be updated:** Select the icon to be used for the webclip by clicking Browse and navigating to the file location.
Android settings

- **Rule**: Select whether this policy adds or removes a webclip. The default is **Add**.
- **Label**: Type the label that is to appear with the webclip.
- **URL**: Type the URL associated with the webclip.
- **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 webclip.
- **URL**: Type the URL associated with the webclip.

WiFi device policy

November 21, 2019

The WiFi device policy lets you manage how users connect their devices to WiFi networks by defining the following items:

- Network names and types
- Authentication and security policies
- Proxy server use
- Other WiFi related details

To add or configure this policy, go to **Configure > Device Policies**. For more information, see [Device policies](https://www.citrix.com).

Prerequisites

Before you create a policy, complete these steps:

- 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.

iOS and tvOS 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.
- **Hidden network (enable if network is open or off)**: Choose whether the network is hidden.
- **Auto Join (automatically join this wireless network)**: Choose whether the network is joined automatically. If a device is already connected to another network, it won’t join this network. The user needs to 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: For the latest release of Windows 10, use of WPA-2 Enterprise requires that you configure SCEP. Endpoint Management can then send the certificate to devices to authenticate to the WiFi server. To configure SCEP, go to Distribution page of Settings > Credential Providers. For more information, see Credential providers.

- Any (Enterprise)

The following sections list the options you configure for each of the preceding connection types.

**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, Any (Enterprise) settings for iOS**

When you choose any of these settings, their settings are listed after Proxy server settings.

- **Protocols, accepted EAP types:** Enable the EAP types you want to support and then configure the associated settings. The default is Off for each of the available EAP type.
- **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.
- **Protocols, EAP-FAST:** 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 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:
  * **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*.

• **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:
    * **Hostname/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 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*. 

© 1999-2019 Citrix Systems, Inc. All rights reserved.
macOS 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**.
- **Hidden network (enable if network is open or off)**: Choose whether the network is hidden.
- **Auto Join (automatically join this wireless network)**: Choose whether the network is joined automatically. If a device is already connected to another network, it won’t join this network. The user needs to 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 you configure for each of the preceding connection types.

**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**

When you choose any of these settings, their settings are listed after Proxy server settings.

- **Protocols, accepted EAP types:** Enable the EAP types you want to support and then configure the associated settings. The default is Off for each of the available EAP type.
- **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.
- **Protocols, EAP-FAST:** 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 Endpoint Management.
      - Provisioning PAC anonymously
- **Authentication:**
  - **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.
    * 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 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.
- Use as a Login Window configuration: Choose whether to use the same credentials entered at the login window to authenticate the user.

- 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:
    * Hostname/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 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.

Android 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 WiFi connection.
  - Open
The following sections list the options 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.

**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.

**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.
- **Hidden network (Enable if network is open or off):** Choose whether the network is hidden.
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 WiFi connection.
  - Open
  - Shared
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

The following sections list the options you configure for each of the preceding connection types. The default is **Open**.

**Open, Shared settings for Android Enterprise**

- **Encryption**: In the list, choose either **Disabled** or **WEP**. The default is **WEP**.
- **Password**: Type an optional password.

**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.
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.
- **Hidden network (Enable if network is open or off):** Choose whether the network is hidden.

Windows Phone 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 WiFi connection.
  - Open
  - WPA Personal
  - WPA-2 Personal
  - WPA-2 Enterprise: For the latest release of Windows 10, use of WPA-2 Enterprise requires that you configure SCEP. SCEP configuration enables Endpoint Management to send the certificate to devices to authenticate to the WiFi server. To configure SCEP, go to Distribution page of Settings > Credential Providers. For more information, see Credential providers.
Citrix Endpoint Management

The following sections list the options you configure for each of the preceding connection types.

**Open settings for Windows Phone**

- **Connect if hidden**: Choose whether to connect when the network is hidden.
- **Connect automatically**: Choose whether to connect to the network automatically.

**WPA Personal, WPA-2 Personal settings for Windows Phone**

- **Encryption**: In the list, choose either AES or TKIP to set the type of encryption. The default is AES.
- **Connect if hidden**: Choose whether to connect when the network is hidden.
- **Connect automatically**: Choose whether to connect to the network automatically.

**WPA-2 Enterprise settings for Windows Phone**

- **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.
- **Connect if hidden**: Choose whether to connect when the network is hidden.
- **Connect automatically**: Choose whether to connect to the network automatically.
- **Push certificate via SCEP**: Choose whether to push the certificate to user devices via Simple Certificate Enrollment Protocol (SCEP).
- **Credential provider for SCEP**: In the list, choose the SCEP credential provider. The default is None.
- **Proxy server settings**
  - **Host name or IP address**: Type the name or IP address of the proxy server.
  - **Port**: Type the port number for the proxy server.
Windows 10 settings

- **Authentication**: In the list, click the type of security to use with the WiFi connection.
  - Open
  - WPA Personal
  - WPA-2 Personal
  - WPA Enterprise
  - WPA-2 Enterprise: For the latest release of Windows 10, use of WPA-2 Enterprise requires that you configure SCEP. SCEP configuration enables Endpoint Management to send the certificate to devices to authenticate to the WiFi server. To configure SCEP, go to **Distribution** page of **Settings > Credential Providers**. For more information, see **Credential providers**.

The following sections list the options you configure for each of the preceding connection types.

**Open settings for Windows 10**

- **Hidden network (Enable if network is open or off)**: 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**

- **Encryption**: In the list, choose either **AES** or **TKIP** to set the type of encryption. The default is **AES**.
- **Hidden network (Enable if network is open or off)**: Choose whether the network is hidden.
- **Connect automatically**: Choose whether to connect to the network automatically.
WPA-2 Enterprise settings for Windows 10

- **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.
- **Connect if hidden:** Choose whether the network is hidden.
- **Connect automatically:** Choose whether to connect to the network automatically.
- **Push certificate via SCEP:** Choose whether to push the certificate to user devices by using Simple Certificate Enrollment Protocol (SCEP).
- **Credential provider for SCEP:** In the list, choose the SCEP credential provider. The default is None.

Chrome OS settings

- **Name:** Type a user-friendly description of this connection. This setting is required.
- **Priority:** Type a suggested priority value for this network. This value can determine which network to connect to when multiple configured networks are available.
- **Allow gateway ARP Polling:** If On, this setting allows ARP messages to be sent to the default gateway to monitor the status of the current connection. Default is On.
- **Auto connect:** If On, devices connect to the network automatically when in range. Default is Off.
• **Hidden SSID:** When set to **On**, the SSID of the network is not broadcast. Default is **Off**.

• **Roam threshold:** Type the roam threshold for this network. The roam threshold is the signal-to-noise value (in dB) below which device attempts to roam to a new network.

• **Select type of security:** Choose the type of security used with this WiFi connection. Options are **None** and **WPA-PSK**. Default is **None**.

### Citrix Ready workspace hub settings

You can connect to 5 GHz WiFi networks if your Citrix Ready workspace hub device is built on the Raspberry Pi 3 Model B+ platform or later. Configure your device to connect to the network:

- **Name:** Type a user-friendly description of this connection. This setting is required.
- **Authentication:** If **Open**, no authentication is required. If **WPA-2 Enterprise**, configure authentication settings for the device. Default is **Open**.
- **EAP Type:** Select an authentication protocol type. If **Automatic**, the workspace hub device automatically determines the authentication protocol. You can also select **PEAP-MSCHAPv2**. Default is **Automatic**.
- **Identity:** Type a user name for authentication.
- **Password:** Type a password for authentication.
- **Anonymous:** Type an 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.

To push the WiFi policy to the device, it must first be connected using Ethernet. After the device reboots, it connects to WiFi automatically.

### Windows Agent device policy

August 26, 2019

Use the Windows Agent device policy to run PowerShell scripts on managed Windows desktops and tablets. You can point to script files uploaded to Endpoint Management as an enterprise app and to other servers that host scripts. For information about adding enterprise apps, see [Add apps](#).

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 returns a result. Based on the result returned, an automated action runs that grants or denies access to an app, marks the device as out of compliance, or has other effects.

To add or configure this policy, go to [Configure > Device Policies](#). For more information, see [Device policies](#).
Windows Desktop and Tablet settings

- **Config name**: Type a descriptive name for your configuration.

- **Task type**: Select *PowerShell*.

- **Select script location**: Select *Uploaded script* for scripts that you have uploaded to Endpoint Management or select *Script location URL* for scripts hosted externally.
  - **Select script**: If you chose *Uploaded script*, select the script to run.
  - **Enter 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. Endpoint Management doesn’t support URLs that deliver scripts as a JavaScript download.

- **Run Schedule**: Select *Run Once* to run the selected script one time or select *Run Frequently* to run the script on a selected schedule.
  - **Scheduling Frequency(hr)**: 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.
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.

```powershell
$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

```json
{
    "firewallEnabled": "true"
}
```
or

```json
{
    "firewallEnabled": "false"
}
```

2. Upload the script to the Endpoint Management console as an enterprise app or host the script at an accessible URL.

3. Configure the Windows Agent device policy as described in this article. Ensure 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 policy result](#). That section shows the specific automated actions created for the example script and Windows Agent device policy.
Windows Hello for Business device policy

August 26, 2019

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 policy. Configure these settings:

**Windows Phone and 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**.
• **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.

**Windows GPO Configuration device policy**

December 4, 2019

The Windows GPO Configuration device policy allows you to:

• Use the Endpoint Management console to import Group Policy Objects (GPOs) and deploy them to Windows 10 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 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 Endpoint Management console.

To create a backup of your GPOs in 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 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.

**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). 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 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.
- 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 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.

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, 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 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 Information Protection device policy

August 26, 2019

Windows Information Protection (WIP), previously known as enterprise data protection (EDP), is a Windows technology that protects against the potential leakage of enterprise data. Data leakage can occur through sharing of enterprise data to non-enterprise protected apps, between apps, or outside of the organization network. For more information, see Protect your enterprise data using Windows Information Protection (WIP) on Microsoft TechNet.

You can create a device policy in Endpoint Management to specify the apps that require Windows Information Protection at the enforcement level you set. The Windows Information Protection policy is for Windows 10 version 1607 and later supervised Phone, Tablet, and Desktop.

Endpoint Management includes some common apps and you can add others. You specify for the policy an enforcement level that affects the user experience. For example, you can:

- Block any inappropriate data sharing.
- Warn about inappropriate data sharing and allow users to override the policy.
- Run WIP silently while logging and permitting inappropriate data sharing.

To exclude apps from Windows Information Protection, define the apps in Microsoft AppLocker XML files and then import those files into Endpoint Management.

To add or configure this policy, go to Configure > Device Policies. For more information, see Device policies.

Windows Phone and Windows Desktop/Tablet settings

- Desktop App (Windows 10 Tablet), Store App (Windows 10 Phone and Tablet): Endpoint Management includes some common apps, as shown in the sample above. You can edit or remove those apps as needed.
To add other apps: In the **Desktop App** or **Store App** table, click **Add** and provide the app information.

**Allowed** apps can read, create, and update enterprise data. **Denied** apps can’t access enterprise data. **Exempt** apps can read enterprise data but can’t create or modify the data.

- **AppLocker XML**: Microsoft provides a list of Microsoft apps that have known compatibility issues with WIP. To exclude those apps from WIP, click **Browse** to upload the list. Endpoint Management combines the uploaded AppLocker XML and the configured desktop and store apps in the policy sent to the device. For more information, see **Recommended deny list for Windows Information Protection**.

- **Enforcement level**: Select an option to specify how you want Windows Information Protection to protect and manage data sharing. Defaults to **Off**.
  - **0-Off**: WIP is off and doesn’t protect or audit your data.
  - **1-Silent**: WIP runs silently, logs inappropriate data sharing, and doesn’t block anything. You can access logs through **Reporting CSP**.
  - **2-Override**: WIP warns users about potentially unsafe data sharing. Users can override warnings and share the data. This mode logs actions, including user overrides, to your audit log.
  - **3-Block**: WIP prevents users from completing potentially unsafe data sharing.

- **Protected domain names**: The domains that your enterprise uses for its user identities. This list of managed identity domains, along with the primary domain, make up the identity of your managing enterprise. The first domain in the list is the primary corporate identity used in the Windows UI. Use “|” to separate list items. For example: `domain1.com | domain2.com`

- **Data recovery certificate**: Click **Browse** and then select a recovery certificate to use for data recovery of encrypted files. This certificate is the same as the data recovery agent (DRA) certificate for the encrypting file system (EFS), only delivered through MDM instead of Group Policy. If a recovery certificate isn’t available, create it. For information, see “Create a data recovery certificate” in this section.

- **Network domain names**: A list of domains that comprise the boundaries of the enterprise. WIP protects all traffic to the fully qualified domains in this list. This setting, with the **IP range** setting, detects whether a network endpoint is enterprise or personal on private networks. Use a comma to separate list items. For example: `corp.example.com,region.example.com`

- **IP range**: A list of the enterprise IPv4 and IPv6 ranges that define the computers in the enterprise network. WIP considers these locations as a safe destination for enterprise data sharing. Use commas to separate list items. For example:
IP ranges list is authoritative: To prevent auto-detection of IP ranges by Windows, change this setting to On. Defaults to Off.

Proxy servers: A list of the proxy servers that the enterprise can use for corporate resources. This setting is required if you use a proxy in your network. Without a proxy server, enterprise resources might be unavailable when a client is behind a proxy. For example, resources might be unavailable from certain Wi-Fi hotspots at hotels and restaurants. Use commas to separate list items. For example:

proxy.example.com:80;157.54.11.118:443

Internal proxy servers: A list of the proxy servers that your devices go through to reach your cloud resources. Using this server type indicates that the cloud resources you’re connecting to are enterprise resources. Don’t include in this list any of the servers in the Proxy servers setting, which are used for non-WIP-protected traffic. Use commas to separate list items. For example:

e.example.internalproxy1.com;10.147.80.50

Cloud resources: A list of cloud resources protected by WIP. For each cloud resource, you can also optionally specify a proxy server in the Proxy servers list to route traffic for this cloud resource. All traffic routed through the Proxy servers is treated as enterprise traffic. Use commas to separate list items. For example:

domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.domain2.com

Set Require protection under lock: Windows 10 Phone only. If On, the Passcode device policy is also required. Otherwise, the Windows Information Protection policy deployment fails. Also, if this policy is On, the setting Require protection under lock appears. Default is Off.

Require protection under lock: Windows 10 Phone only. Specifies whether to encrypt enterprise data using a key that’s protected by an employee PIN on a locked device. Apps can’t read corporate data on a locked device. Defaults to On.

Revoke WIP certificate on unenroll: Specifies whether to revoke local encryption keys from a user device when it’s unenrolled from Windows Information Protection. After the encryption keys are revoked, a user can’t access encrypted corporate data. If Off, the keys aren’t revoked and the user continues to have access to protected files after unenrollment. Defaults to On.

Show overlay icons: Specifies whether to include the Windows Information Protection icon overlay on corporate files in Explorer and enterprise only app tiles in the Start menu.
Citrix Endpoint Management

Defaults to **Off**.

**Create a data recovery certificate**

A data recovery certificate is required to enable the **Windows Information Protection** policy.

1. On the Endpoint Management server, open a command prompt and navigate to a folder (other than Windows\System32) where you want to create a certificate.
2. Run this command:
   ```
   cipher /r:ESFDRA
   ```
3. When prompted, enter a password to protect the private key file.
   The command creates a .cer and a .pfx file.
4. In the Endpoint Management console, go to **Settings > Certificates** and import the .cer file, which applies to both Windows 10 tablets and phones.

**User experience**

When Windows Information Protection is in effect, apps and files include an icon:
If a user copies or saves a protected file to a non-protected location, the following notification appears, depending on the enforcement level configured.

**Deprecated device policies**

December 9, 2019

Note:

Starting the second quarter of 2018, support for Symbian and Windows Mobile/CE devices is no longer available to new customers. For information about the Microsoft product lifecycle, see the Microsoft Support site.
**APN device policy (Windows Mobile/CE)**

You use the Access Point Name (APN) device policy if your organization doesn’t 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.

**Windows Mobile/CE settings**

- **APN**: Type the name of the access point. This name must match an accepted Android APN or the policy fails.
- **Network**: In the list, click the type of network to use. The default is **Built-in office**.
- **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.

**App access device policy (Windows Mobile/CE)**

The app access device policy in Endpoint Management allows you to define a list of apps that meet any of these conditions:

- Required to be installed on the device
- Can be installed on the device
- Must not be installed on the device.

You can then create an automated action to react to the device compliance with that list of apps.

You can only configure one type of access policy at a time. You can add a policy for either a list of required apps, suggested apps, or forbidden apps. You can’t include a mix of required, suggested, or forbidden apps within the same app access policy. If you create a policy for each type of list, we recommend that you name each policy carefully. That practice enables you to know which policy in Endpoint Management applies to which list of apps.

**Mobile/CE settings**

- **Access policy**: Click Required, Suggested, or Forbidden. The default is **Required**.
- To add one or more apps to the list, click Add and then do the following:
  - **App name**: Enter an app name.
  - **App Identifier**: Enter an optional app identifier.
– Click **Save** or **Cancel**.
– Repeat these steps for each app you want to add.

**App inventory device policy (Windows Mobile/CE)**

The App inventory policy lets you collect an inventory of the apps on managed devices. 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 blacklist or whitelist and take action accordingly.

An app appears in a blacklist when the app is forbidden in an app access policy. An app appears in a whitelist when the app is required in an app access policy.

**Windows Mobile/CE settings**

- For each platform you select, leave the default setting or change the setting to **Off**. The default is **On**.

**App uninstall device policy (Windows Mobile/CE)**

The App uninstall policy lets you remove apps from user devices for any number of reasons. It may be that you no longer want to support certain apps. Or perhaps your company wants to replace existing apps with similar apps from different vendors.

The apps are removed when this policy is deployed to user devices. Users receive a prompt to uninstall the app.

**Windows Mobile/CE settings**

- **Apps to uninstall**: For each app you want to add, click **Add** and then do the following:
  - **App name**: In the list, click an existing app 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.

**App tunneling device policy (Windows Mobile/CE)**

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 mobile device app and the app server component.
Any app traffic sent through a tunnel that you define in this policy goes through Endpoint Management before being redirected to the server running the app.

Windows Mobile/CE settings

- **Connection initiated by**: Click Device or Server to specify the source initiating the connection.
- **Protocol**: In the list, click the protocol to use. The default is **Generic TCP**.
- **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**: Specify the time out when you set **Define connection time out** to **On**. The time out is the number of 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.
- **Redirect to Endpoint Management**: In the list, click how the device connects to Endpoint Management. The default is Through app settings.
  - If you select **Using a local alias**, type the alias in **Local alias**. The default is **localhost**.
  - If you select **An IP address range**, type the from IP address in **IP address range from**. Then type the to IP address in **IP address range to**.
- **Client port**: Type the client port number. Usually, this value is the same as for the server port.
- **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.

Connection manager device policy (Windows Mobile/CE)

In Endpoint Management, you can specify the connection settings for apps that connect automatically to the Internet and to private networks. This policy is only available on Windows Pocket PCs.

Windows Mobile/CE settings

- **Note**: *Built-in office* means that all connections are to your company’s intranet. *Built-in Internet*
mean that all connections are to the Internet.

- **Apps that connect to a private network automatically use:** In the list, click either **Built-in office** or **Built-in Internet**. The default is **Built-in office**.

- **Apps that connect to the Internet automatically use:** In the list, click either **Built-in office** or **Built-in Internet**. The default is **Built-in office**.

### Connection scheduling device policy (Windows Mobile/CE)

You create connection scheduling policies to control how and when user devices connect to Endpoint Management. You can specify that users connect their devices manually, that devices stay connected permanently, or that devices connect within a defined time frame.

### Windows Mobile/CE settings

- **Require devices to connect:** Click the option you want to set for this schedule.
  - **Always:** Keep the connection alive permanently. Endpoint Management on the user’s device attempts to reconnect to the Endpoint Management server after a network connection loss. Endpoint Management monitors the connection by transmitting control packets at regular intervals. Citrix recommends this option for optimized security. When you choose **Always**, also use for the device **Tunnel Policy**, the **Define connection time-out** setting to ensure that the connection is not draining battery. By keeping the connection alive, you can push security commands like wipe or lock to the device on-demand. Ensure that you also select the **Deployment Schedule** option **Deploy for always-on connections** in each policy deployed to the device.
  - **Never:** Connect manually. Users must initiate the connection from 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 any new apps or policies.
  - **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: Endpoint Management processes the action on the device the next time that the device connects. When you select this option, the **Connect 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:** When enabled, Endpoint Management on the user’s device attempts to reconnect to the Endpoint Management server after a network connection loss. Endpoint Management 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.
• **Maintain permanent connection during these hours:** Users’ devices must be connected for the defined 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 30 minutes. Thus, if you want a connection between 8:00 AM and 9:00 AM every weekday, click the two squares 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 9:00 AM every weekday.
• A permanent connection between 12:00 AM Saturday and 1:00 AM Sunday.
• At least one connection every weekday between 5:00 AM and 8:00 AM or between 10:00 AM and 11:00 PM.

**Credentials device policy (Windows Mobile/CE)**

You can create credentials device policies in Endpoint Management to enable integrated authentication with your PKI configuration in Endpoint Management. For example, to integrate with a PKI entity, a keystore, a credential provider, or a server certificate. For more information about credentials, see [Certificates and authentication](#).

**Note:**

Before you can create this policy, you need the credential information you plan to use for each platform, plus any certificates and passwords.

**Windows Mobile/CE settings**

• **Store device:** In the list, click the location of the certificate store for the credential. The default is root. Options are:
  – **Privileged execution trust authorities:** Applications signed with a certificate belonging to this store runs with privileged trust level.
  – **Unprivileged execution trust authorities:** Applications signed with a certificate belonging to this store runs with normal trust level.
– **SPC (Software Publisher Certificate)**: The Software Publishing Certificate (SPC) is used for signing .cab files.
– **root**: A certificate store that contains root, or self-signed, certificates.
– **CA**: A certificate store that contains cryptographic information, including intermediary certification authorities.
– **MY**: A certificate store that contains end-user personal certificates.

  • **Credential type**: Certificate is the only credential type for Windows Mobile/CE devices.
  • **The credential file path**: Select the credential file by clicking **Browse** and then navigating to the file’s location.

**Custom XML device policy (Windows Mobile/CE)**

You can create custom XML policies in Endpoint Management to customize the following features:

  • 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

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 Device Management** on the Microsoft Developer Network site.

**Windows Mobile/CE settings**

**XML content**: Type, or cut and paste, the custom XML code you want to add to the policy.

<table>
<thead>
<tr>
<th></th>
<th>After you click <strong>Next</strong>, Endpoint Management checks the XML content syntax. Any syntax errors appear below the content box. Fix any errors before you continue.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>If there are no syntax errors, the <strong>Custom XML Policy</strong> assignment page appears.</td>
</tr>
</tbody>
</table>

**Delete files and folders device policy (Windows Mobile/CE)**

You can create a policy in Endpoint Management to delete specific files or folders from Windows Mobile/CE devices.
Citrix Endpoint Management

Windows Mobile/CE settings

Files and folders to delete: for each file or folder you want to delete, click Add and then do the following:
- Path: Type the path to the file or folder.
- Type: In the list, click File or Folder. The default is File.
- Click Save to save the file or folder, or click Cancel not to save the file or folder.

Delete registry keys and values device policy (Windows Mobile/CE)

You can create a policy in Endpoint Management to delete specific registry keys and values from Windows Mobile/CE devices.

Windows Mobile/CE settings

Registry keys and values to delete: for each registry key and value you want to delete, click Add and then do the following:
1. Key: Type the registry key path. This field is required. The registry key path should either start with HKEY_CLASSES_ROOT\ or HKEY_CURRENT_USER\ or HKEY_LOCAL_MACHINE\ or HKEY_USERS\.
2. Value: Type the value name to be deleted or leave this field blank to delete the entire registry key.
3. Click Save to save the key and value, or click Cancel not to save the key and value.

Files device policy (Windows Mobile/CE)

You can add script files to Endpoint Management that perform certain functions for users. You can add the following file types with this policy:
- Text-based files (.xml, .html, .py, and so on)
- Script files created with MortScript

Windows Mobile/CE settings

- File to be imported: Select the file to import by clicking Browse and navigating to the file location.
- File type: Select either File or Script. When you select Script, Execute immediately appears. Select whether the script is executed when the file is uploaded. The default is Off.
• **Replace macro expressions:** Select whether to replace macro token names in a script with a device or user property. The default is Off.

• **Destination folder:** In the list, select the location in which to store the uploaded file or click Add new to choose an unlisted file location. In addition, you can use any of the following macros as the start of a path identifier:
  - %Flash Storage%
  - %Endpoint Management Folder%
  - %Program Files%
  - %My Documents%
  - %Windows%

• **Destination file name:** Optionally, type a different name for the file if it must be changed before being deployed on a device.

• **Copy file only if different:** In the list, select whether to copy the file if it is different from the existing file. The default is to copy the file only if it is different.

• **Read only file:** Select whether the file is to be read-only. The default is Off.

• **Hidden file:** Select whether the file is not to be shown in the file list. The default is Off.

### Proxy device policy (Windows Mobile/CE)

You can add a device policy in Endpoint Management to specify global HTTP proxy settings for devices running Windows Mobile/CE. You can deploy only one global HTTP proxy policy per device.

### Windows Mobile/CE settings

• **Network:** In the list, click the network type to use. The default is **Built-in office.** Possible options are:
  - User-defined office
  - User-defined Internet
  - Built-in office
  - Built-in Internet

• **Network:** In the list, click the network connection protocol to use. The default is **HTTP.** Possible options are:
  - HTTP
  - WAP
  - Socks 4
  - Socks 5

• **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. The default is **80**.

• **Username:** Type an optional user name to authenticate to the proxy server.

• **Password:** Type an optional password to authenticate to the proxy server.

• **Domain name:** Type an optional domain name.

• **Enable:** Select whether to enable the proxy. The default is **On**.

**Registry device policy (Windows Mobile/CE)**

The Windows Mobile/CE registry stores data about apps, drivers, user preferences, and configuration settings. In Endpoint Management, you can define the registry keys and values that let you administer Windows Mobile/CE devices.

**Windows Mobile/CE settings**

For each registry key or registry key/value pair you want to add, click **Add** and do the following:

• **Registry key path:** Type the full path for the registry key. For example, type `HKEY_LOCAL_MACHINE\Software` to specify the route to the Windows key from the HKEY_LOCAL_MACHINE root key.

• **Registry value name:** Type the name for the registry key value. For example, type `ProgramFilesDir` to add that value name to the registry key path `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion`. If you leave this field blank, it means that you are adding a registry key and not a registry key/value pair.

• **Type:** In the list, click the data type for the value. The default is **DWORD**. Possible options are:
  - **DWORD:** A 32-bit unsigned integer.
  - **String:** Any string.
  - **Extended string:** A string value that can contain environment variables like `%TEMP%` or `%USERPROFILE%`.
  - **Binary:** Any arbitrary binary data.

• **Value:** Type the value associated with Registry value name. For example, to specify the value of `ProgramFilesDir`, type `C:\Program Files`.

• Click **Save** to save the registry key information or click **Cancel** not to save the registry key information.

**Restrictions device policy (Windows Mobile/CE)**

The Restrictions device policy allows or restricts certain features or functionality on user devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and restrictions on the types of apps users can and cannot install. Most of the restriction settings default to **On**, or **allows**.
Tip:
Any option for which you select **On** means that the user can perform the operation or use the feature. For example:

**Camera:** If **On**, the user can use the camera on their device. If **Off**, the user cannot use the camera on their device.

**Windows Mobile/CE settings**

<table>
<thead>
<tr>
<th>Device Policies</th>
<th>Apps</th>
<th>Media</th>
<th>Actions</th>
<th>Shares</th>
<th>Enrollment Policies</th>
<th>Delivery Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrictions Policy</td>
<td>Restrictions Policy</td>
<td>This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Bluetooth/infrared beaming (Obex):** Enable OBEX (OBject EXchange protocol) over Bluetooth or infrared to exchange data between devices.
- **Camera:** Enable the camera on user devices.
- **WiFi switch:** Allow users to switch Wi-Fi networks.
- **Bluetooth:** Enable Bluetooth on users’ devices.

**Roaming device policy (Windows Mobile/CE)**

You can add a device policy in Endpoint Management to configure whether to allow voice and data roaming. When voice roaming is disabled, data roaming is automatically disabled.

**Windows Mobile/CE settings**

- **While roaming**
  - **Use on-demand connection only:** The device only connects to Endpoint Management if users manually trigger the connection on their devices or if a mobile application requests...
a forced connection. For example, such as a push mail request if the Exchange Server has been set accordingly. This option temporarily disables the default device connection schedule policy.

- **Block all cellular connections except the ones managed by Endpoint Management:** Except for the data traffic officially declared in an Endpoint Management application tunnel or other Endpoint Management device management task: No other data is sent or received by the device. For example, this option disables all connections to the Internet through the device’s web browser.

- **Block all cellular connections managed by Endpoint Management:** All application data transiting through an Endpoint Management tunnel is blocked (including Endpoint Management Remote Support). The data traffic related to pure device management, however, is not blocked.

- **Block all cellular connections to Endpoint Management:** Until the device is either re-connected through USB, Wi-Fi, or its default mobile operator cellular network: There is no traffic transiting between the device and Endpoint Management.

- **While domestic roaming**
  - **Ignore domestic roaming:** No data is blocked while users roam domestically.

**WiFi device policy (Windows Mobile/CE)**

Wi-Fi policies let 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 details

**Prerequisites**

Before you create a policy, be sure that you complete these steps:

- 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.
Windows Mobile/CE settings

- **Network name**: Type the SSID that is in the list of available networks on the user device.
- **Device-to-device connection (ad-hoc)**: Allows two devices to connect directly. Default is Off.
- **Network**: Choose whether the device is connected to an external internet source or an Office intranet.
- **Authentication**: In the list, choose the type of security to use with the Wi-Fi connection.
  - Open
  - WPA Personal
  - WPA-2 Personal
  - WPA-2 Enterprise

The following sections list the options you configure for each of the preceding connection types.

Open settings for Windows Mobile/CE

- **Hidden network (Enable if network is open or off)**: Choose whether the network is hidden.
- **Connect automatically**: Choose whether to connect to the network automatically.

WPA Personal, WPA-2 Personal settings for Windows Mobile/CE

- **Encryption**: In the list, choose either AES or TKIP to set the type of encryption. The default is AES.
- **Hidden network (Enable if network is open or off)**: Choose whether the network is hidden.
- **Connect automatically**: Choose whether to connect to the network automatically.

WPA-2 Enterprise settings for Windows Mobile/CE

- **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.
- **Connect if hidden**: Choose whether the network is hidden.
- **Connect automatically**: Choose whether to connect to the network automatically.
- **Push certificate via SCEP**: Choose whether to push the certificate to user devices by using Simple Certificate Enrollment Protocol (SCEP).
• **Credential provider for SCEP:** In the list, choose the SCEP credential provider. The default is **None**.
• **Key provided (automatic):** Choose whether the key is automatically provided. Default is **Off**.
• **Password:** Type the password in this field.
• **Key index:** Choose the key index. Available options are 1, 2, 3, and 4.

**Windows CE certificate device policy (Windows Mobile/CE)**

You can create a device policy in Endpoint Management to create and deliver Windows Mobile/CE certificates from an external PKI to users’ devices.

**Windows CE settings**

• **Credential provider:** In the list, click the credential provider. The default is **None**.
• **Password of generated PKCS#12:** Type the password used to encrypt the credential.
• **Destination folder:** In the list, click the destination folder for the credential or click **Add new** to add a folder not already in the list. The predefined options are:
  - %Flash Storage%
  - %Endpoint Management Folder%
  - %Program Files%
  - %My Documents%
  - %Windows%
• **Destination file name:** Type the name of the credential file.

**Endpoint Management options device policy (Windows Mobile/CE)**

You add an Endpoint Management options policy to configure Secure Hub behavior when connecting to Endpoint Management from Windows Mobile/CE devices.

**Windows Mobile/CE settings**

• **Device agent configuration**
  - **Endpoint Management backup configuration:** In the list, click an option for backing up the Endpoint Management configuration on the users’ devices. The default is **Disabled**. Available options are:
    * Disabled
    * At the first connection after Endpoint Management installation
    * At the first connection after each device reboot
- Connect to the office network
- Connect to the Internet network
- **Connect to the built-in office network**: When set to **On**, Endpoint Management automatically detects the network.
- **Connect to the built-in Internet network**: When set to **On**, Endpoint Management automatically detects the network.
- **Tray bar notification - hide tray bar icon**: Select whether the tray bar icon is hidden or visible. The default is **Off**.
- **Connection time-out(s)**: 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 interval(s)**: Type the length of time in seconds to keep a connection open. The default is 120 seconds.

**Remote support**
- **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**: In the list, click whether to warn the user about a file transfer or whether to ask the user for permission. Available values: **Do not warn the user**, **Warn the user**, and **Ask for user permission**. The default is **Do not warn the user**.

**Endpoint Management uninstall device policy (Windows Mobile/CE)**

You can add a device policy in Endpoint Management to uninstall Endpoint Management from Windows Mobile/CE devices. When deployed, this policy removes Endpoint Management from all devices in the deployment group.

**Windows Mobile/CE settings**

- **Uninstall Endpoint Management from devices**: Select whether to uninstall Endpoint Management from every device to which you deploy this policy. The default is **Off**.

**Add apps**

November 25, 2019

**Important:**

The MDX 10.7.5 release is the final release that supports the wrapping of Citrix mobile productivity apps. You cannot use the MDX Service or the MDX Toolkit 10.7.10 and later to wrap 10.7.5 or later
Citrix Endpoint Management

versions of the Citrix mobile productivity apps. Access mobile productivity apps from the public app stores.

You add apps to Endpoint Management for management. You add the apps to the Endpoint Management console, where you can then arrange the apps in categories and deploy the apps to users.

You can add the following types of apps to Endpoint Management:

- **MDX**: These apps are wrapped with the MDX Service or Toolkit. You deploy MDX apps that you get from internal and public stores.
- **Public App Store**: These apps include free or paid apps available in a public app store, such as iTunes or Google Play. For example, GoToMeeting.
- **Web and Saas**: These apps include apps accessed from an internal network (web apps) or over a public network (SaaS). You can create your own apps, or choose from a set of app connectors for single sign-on authentication to existing Web apps. For example, GoogleApps_SAML.
- **Enterprise**: These apps are native apps that are not wrapped with MDX and do not contain the policies associated with MDX apps.
- **Web Link**: These apps are Web addresses (URLs) to public or private sites, or to web apps that don’t require single sign-on.

**About silent installations**

Citrix supports the silent installation of iOS and Samsung Android apps. Silent installation means that users are not prompted to install apps that you deploy to the device. The apps install silently in the background.

Prerequisites to implement silent installation:

- For iOS apps, put the managed iOS device in supervised mode. For details, see **Import iOS & macOS Profile device policy**.
- For Android apps, enable Samsung for Enterprise (SAFE) or Knox policies on the device.
  
  To do so, you set the Samsung MDM license key device policy to generate Samsung ELM and Knox license keys. For details, see **Samsung MDM license key device policies**.

**How mobile and MDX apps work**

Endpoint Management supports iOS and Android, including Citrix mobile productivity apps, such as Secure Hub, Secure Mail and Secure Web, and the use of MDX policies. Using the Endpoint Management console, you can upload apps and then deliver the apps to user devices. In addition to the Citrix mobile productivity apps, you can add the following types of apps:

- Apps you develop for your users.
• Apps in which you want to allow or restrict device features by using MDX policies.

To distribute Citrix mobile productivity apps, follow these general steps:


2. Upload those files to the Endpoint Management console (Configure > Apps), updating MDX policies as needed.

3. Upload the MDX files to the public app stores. For more information, see Add an MDX app in this article.

   The MDX Toolkit wraps apps for iOS and Android devices with Citrix logic and policies. The tool can securely wrap an app that was created within your organization or an app created outside the company.

**About required and optional apps**

When you add apps to a delivery group, you choose whether they are optional or required. 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.
• As user deletes a required app.
• A Secure Hub update is available.

**Requirements for forced deployment of required apps**

• Secure Hub 10.5.15 for iOS and 10.5.20 for Android (minimum versions)
• MDX Service or MDX Toolkit 10.6 (minimum version)
• Custom server property, `force.server.push.required.app`s

   The forced deployment of required apps is disabled by default. To enable the feature, create a Custom Key server property. Set the Key and Display name to `force.server.push.required.app`s and set the Value to true.

• After you upgrade Endpoint Management and Secure Hub: Users with enrolled devices must sign off and then sign on to Secure Hub, one time, to obtain the required app deployment updates.
**Examples**

The following examples show the sequence of adding the Secure Tasks app to a delivery group and then deploying the delivery group.

**Note:**

Secure Notes and Secure Tasks reached End of Life (EOL) status on December 31, 2018. For details, see [EOL and deprecated apps](#).

After the sample app, Secure Tasks, deploys to the user device, Secure Hub prompts the user to install the app.

**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 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 Endpoint Management console.
3. Use the Endpoint Management console to deploy required apps.
4. The app on the home screen is updated. And, for public store apps, the upgrade starts automatically. Users are not 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 Endpoint Management console to deploy 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 Endpoint Management console.
3. Use the Endpoint Management console to deploy required apps. Or, open the 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 are not prompted for a grace period. (Samsung devices do a silent install.)

Uninstall an app when the app is configured as required

To 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.

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.
How Web and SaaS apps work

Endpoint Management comes with a set of application connectors, which are templates that you can configure for single sign-on to web and SaaS apps. Sometimes you can configure the templates for user account creation and management. Endpoint Management includes Security Assertion Markup Language (SAML) connectors. SAML connectors are used for web applications that support SAML protocol for SSO and user account management. Endpoint Management supports SAML 1.1 and SAML 2.0.

You can also build your own enterprise SAML connectors.

Endpoint Management integration with Citrix Workspace supports mobile SSO. Single sign-on to native SaaS apps is available from iOS and Android devices that are enrolled into MDM. See Configure mobile SSO (preview).

How enterprise apps work

Enterprise apps can reside on Endpoint Management servers or in content delivery network (CDN) locations throughout the world. When a user isn’t located near an Endpoint Management server, enterprise app delivery can take a while. For faster enterprise app downloads, you can use CDN. 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 that’s closest to mobile device users. An edge server caches content from the originating server when mobile devices request apps.
Users can connect to enterprise apps by using Secure Hub. When you add an enterprise app, Endpoint Management creates the app connector for it.

**Deliver enterprise apps from a CDN**

You can deliver enterprise apps from the Citrix Content Delivery Network (CDN) for Enterprise Apps. A CDN refers to a geographically distributed group of servers which work together to securely provide fast delivery of application content. A local server delivers the enterprise apps to mobile devices.

A CDN improves app delivery download times by distributing content geographically closer to the mobile devices by using a nearby CDN distribution point.

CDN support for enterprise apps is available for iOS apps (MDM or MAM enrollment), Android apps (MDM or MAM enrollment), and Windows desktop or tablet apps (MDM enrollment).

**How CDN works**

At the core of the CDN service, servers are linked together with the goal of delivering enterprise 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 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 enterprise 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, Endpoint Management copies the app to the local distribution point. Endpoint Management retains the app there for 24 hours for other local device downloads.

**To get started with CDN delivery of enterprise apps**

As of Endpoint Management release 19.4.1, enterprise app delivery defaults to CDN delivery for all new multitenancy customers. For existing customers from before this release, follow the instructions in this section.

For Enterprise apps already on the Endpoint Management server: Endpoint Management continues to deliver enterprise apps from the server until those apps get reuploaded after you complete the following steps.

1. Enable CDN for your account: In the Endpoint Management console: Go to **Settings > Server Properties**.

2. Search for `app.delivery.cdn` and then click **Edit**.
3. Change the value to **true**.

![Key: app.delivery.cdn
Value: true
Display name: Application Delivery to enable CDN
Description: Application Delivery to enable CDN]

4. In the Endpoint Management console, upload your enterprise apps again:
   a) Go to **Configure > Apps** and filter the app list by **Type (Enterprise)** and **Platform** (iOS, Android, or Windows as applicable).
   b) Select an app, click **Edit**, click **Next**, and click **Upload**.
   c) Repeat the prior step for each enterprise app.

**How the public app store works**

You can configure settings to retrieve app names and descriptions from the Apple App Store. When you retrieve the app information from the store, Endpoint Management overwrites the existing name and description. Manually configure Google Play store app information. See Add a public app store app for more details.

**How web links work**

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. When you finish configuring a web link, the link appears as an icon in the app store. When users log on with Secure Hub, the link appears with the list of available apps and desktops.

**Add an MDX app**

When you receive a wrapped MDX mobile app for an iOS or Android device, you can upload the app to Endpoint Management. After you upload the app, you can configure app details and policy settings. For more information about the app policies that are available for each device platform type, see **MDX Policies at a Glance**. Detailed policy descriptions also in that section.
1. In the Endpoint Management console, click **Configure > Apps**. The **Apps** page appears.

![Apps page](image)

2. Click **Add**. The **Add App** dialog box appears.

![Add App dialog box](image)

3. Click **MDX**. The **MDX App Information** page appears.

4. On the **App Information** pane, type the following information:
   - **Name**: Type a descriptive name for the app. The name appears under **AppName** 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 **Create app categories**.

5. Click **Next**. The **App Platforms** page appears.

6. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.

   When you finish configuring the settings for a platform, see Step 11 for how to set the platform deployment rules.
7. To select an MDX file to upload, click **Upload** and navigate to the file location.

   • If you add an iOS volume purchase B2B app, click **Your application is a volume purchase B2B application?** Then, in the list, click the B2B volume purchase account to use.

   • If you add an Android Enterprise MDX app, 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.

8. Click **Next**. The **App details** page appears. Proceed to step 9 to configure the applicable settings.

9. 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.
- **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 cannot 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**.
- **Prevent app data backup**: Select whether to prevent users from backing up app data. The default is **ON**.
- **Product track**: Specify which product track 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**: Select whether, when the app is installed unmanaged, to prompt users to allow the app to be managed on unsupervised devices. The default is **ON**.
- **App deployed via VP**: Select whether to deploy the app by using volume purchase. If **ON**, and you deploy an MDX version of the app and use volume purchase to deploy the app, 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 such policy areas as Authentication, Device Security, Encryption, App Interaction, and App Restrictions. In the console, each of the policies has a tooltip that describes the policy.

For more information about app policies for MDX apps, see **MDX Policies at a Glance**. That article includes a table showing which policies apply to each platform.

11. Configure the deployment rules. For information, see **Deploy resources**.

12. Expand **Store Configuration**.
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.

- **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 cannot upload a GIF or JPEG image.
- **Allow app ratings**: Select whether to permit a user to rate the app. The default is ON.
- **Allow app comments**: Select whether to permit users to comment about the selected app. The default is ON.

13. Click **Next**. The **Approvals** page appears.
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:** In the list, click an existing workflow 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 Active Directory.
- When the name appears in the field, select the check box 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 check box next to each name you want to remove.

14. Click **Next**. The **Delivery Group Assignment** page appears.

15. 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.

16. 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 **ON**.
   
   • Next to Deployment schedule, click **Now** or **Later**. The default option is **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 **On every connection**.
   
   • Next to **Deploy for always-on connection**, click **ON** or **OFF**. The default option is **OFF**.

      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, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with version 10.18.19 or later
      – Is not recommended for Android, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with before version 10.18.19

© 1999-2019 Citrix Systems, Inc. All rights reserved. 913
The deployment schedule 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 **Save**.

**Create app categories**

When users log on to Secure Hub, they receive a list of the apps, web links, and stores that you set up in Endpoint Management. 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.

You configure categories on the **Apps** page in the Endpoint Management console. Then, 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 Endpoint Management console, click **Configure > Apps**. The **Apps** page appears.
2. Click **Category**. The **Categories** dialog box appears.
3. For each category you want to add, do the following:

- Type the name of the category 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.

4. When you’re done adding categories, close the **Categories** dialog box.

5. On the **Apps** page, you can place an existing app into a new category.

   - Select the app you want to categorize.
   - Click **Edit**. The **App Information** page appears.
   - In the **App category** list, apply the new category by selecting the category check box. Clear the check boxes 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.

Add a public app store app

You can add free or paid apps to Endpoint Management that are available in a public app store, such as iTunes or Google Play.

When you add a paid public app store app for Android Enterprise, you can review the Bulk Purchase licensing status. That status is the total number of licenses available, the number currently in use, and the email address of each user consuming the licenses. The Bulk Purchase plan for Android Enterprise simplifies the process of finding, buying, and distributing apps and other data in bulk for an organization.

Configure app information and choose platforms to deliver the app to:

1. In the Endpoint Management console, click Configure > Apps. The Apps page appears.

2. Click Add. The Add App dialog box appears.
3. Click Public App Store. The **App Information** page appears.

4. 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 Create app categories.

5. Click **Next**. The **App Platforms** page appears.

6. Under **Platforms**, select the platforms you want to add. If you are only configuring for one platform, clear the others.

Next you configure the app settings for each platform. When you finish configuring the settings for a platform, set the platform deployment rules and store configuration.

**Configure app settings for Google Play apps**

**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 whitelists the public Google Play store apps for all Android Enterprise users. 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. Ensure 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**.
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 to 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.
Configure app settings for platforms other than Google Play

1. Type the app name in the search box and click **Search**. Apps matching the search criteria appear. The following figure shows the result of searching for **podio** in apps on iPhone.

![Search Result for podio on iPhone](image)

- To add an Android Enterprise app, type the app name or the package ID in the search box. You can locate the package ID in the Google Play store. The ID can be found 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](https://play.google.com/store/apps/details?id=com.Slack&hl=en_US). Then click **Search**.

The managed Google Play store UI opens the list of apps that match your search criteria. Select an app, and then follow the instructions to approve and save the app.

![Android Enterprise App Search](image)

If you add a previously approved app, click **Select**.
After your app is approved, it appears in the search results on the Endpoint Management console.

2. Click the app you want to add. Then the **App Details** fields pre-populate with information related to the chosen app (including the name, description, version number, and associated image).

3. Configure the settings that apply to the chosen platform:
   - If necessary, change the name and description for the app.
   - **App URL:** Enter a comma-separated list of URLs to launch your apps from the 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 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:** Select whether, when the app is installed unmanaged, to prompt users to allow the app to be managed on unsupervised devices. The default is **OFF**.
- **Force license to association to device:** Select whether to associate an app that has been 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, this field can’t be changed.

**Configure deployment rules**

For information, see [Deploy resources](#).

**Set up store configuration**

1. Expand **Store Configuration**.
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 cannot upload a GIF or JPEG image.
  - **Allow app ratings**: Select whether to permit a user to rate the app. The default is ON.
  - **Allow app comments**: Select whether to permit users to comment about the selected app.

2. Expand **Volume Purchase** or, for Android Enterprise, expand **Bulk Purchase**.

   For Volume Purchase, complete the following steps.
   
   a) In the **Volume purchase license** list, click **Upload a volume purchase license** if you want to enable Endpoint Management to apply a volume purchase license for the app.
   
   b) In the dialog box that appears, import the license.

   For Android Enterprise Bulk Purchase, expand the **Bulk Purchase** section.
The License Assignment table shows the number of licenses in use for the app, out of the total licenses available.

For Android Enterprise, you can select a user and then click **Disassociate** to end their license assignment and free up a license for another user. You can only disassociate the license, however, if the user is not part of a delivery group that contains the specific app.

For Android Enterprise, you can disassociate a license only if the user is not part of a delivery group that contains the specific app.

For iOS, you can disassociate Volume Purchase licenses for an individual user. Doing so ends the license assignments and frees licenses.

3. After you complete the **Volume Purchase** or **Bulk Purchase** settings, click **Next**. The **Approvals** page appears.

   You use workflows when you need approval when creating user accounts. If you don’t need approval workflows, you can skip to the next step.

   Configure these settings to assign or create a workflow:

   - **Workflow to Use:** In the list, click an existing workflow 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
       - 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 Active Directory.
  - When the name appears in the field, select the check box 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 check box next to each name you want to remove.

4. Click **Next**. The **Delivery Group Assignment** page appears.

5. 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.

6. 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 **ON**.
   - Next to **Deployment schedule**, click **Now** or **Later**. The default option is **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 **On every connection**.
   - Next to **Deploy for always-on connection**, click **ON** or **OFF**. The default option is **OFF**.

   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, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with version 10.18.19 or later
   - Is not recommended for Android, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with before version 10.18.19

   The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

7. Click **Save**.
Add a Web or SaaS app

Using the Endpoint Management console, you can give users single sign-on (SSO) authorization to your mobile, enterprise, web, and SaaS apps. If Endpoint Management isn’t Workspace-enabled, you can enable apps for SSO by using application connector templates. If Endpoint Management is Workspace-enabled, see Configure native SaaS apps for single sign-on (preview), after this section.

For a list of connector types available in Endpoint Management, see Application connector types. You can also you build your own connector in Endpoint Management when you add a Web or SaaS app.

If an app is available for SSO only: After you save the settings, the app appears on the Apps tab in the Endpoint Management console.

1. In the Endpoint Management console, click Configure > Apps. The Apps page opens.
2. Click Add. The Add App dialog box appears.
3. Click Web & SaaS. The App Information page appears.
4. 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 you want to use in the **App Connectors** list. The app connector 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 contain 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 Citrix Gateway. Setting this option to **ON** adds the VPN keyword to the app and allows users to connect through Citrix Gateway. The default is **OFF**.
   - **App category**: In the list, click an optional category to apply to the app.
   - **User account provisioning**: Select whether to create user accounts for the application. If you use the Globoforce_SAML connector, you must enable this option to ensure 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: In the list, click the action 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**: In the list, click the user attribute to add to the rule.
    - **Length (characters)**: In the list, click the number 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.
  - **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.

   ![App Information page](image)
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.
- **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 networks to use.

6. Expand **Store Configuration**.

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.
Citrix Endpoint Management

- **App screenshots:** Add screen captures to help classify the app in the app store. The graphic you upload must be a PNG. You cannot upload a GIF or JPEG image.
- **Allow app ratings:** Select whether to permit a user to rate the app. The default is **ON**.
- **Allow app comments:** Select whether to permit users to comment about the selected app. The default is **ON**.

7. Click **Next**. The **Approvals** page appears.

You use workflows when you need approval when creating user accounts. If you don’t need approval workflows, you can skip to Step 8.

Configure these settings if you need to assign or create a workflow:

- **Workflow to Use:** In the list, click an existing workflow 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
  - 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 Active Directory.

- When the name appears in the field, select the check box 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 check box next to each name you want to remove.

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:

    - Next to **Deploy**, click **ON** to schedule deployment or click **OFF** to prevent deployment. The default option is **ON**.

    - Next to **Deployment schedule**, click **Now** or **Later**. The default option is **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 **On every connection**.

    - Next to **Deploy for always-on connection**, click **ON** or **OFF**. The default option is **OFF**.

      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, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with version 10.18.19 or later
      - Is not recommended for Android, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with before version 10.18.19

      The deployment schedule 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**.
Configure mobile SSO (preview)

Endpoint Management integration with Citrix Workspace supports mobile SSO. Single sign-on to native SaaS apps is available from iOS and Android devices that are enrolled into MDM.

This section describes how to configure Endpoint Management and Citrix Gateway to deliver native SaaS apps. With that configuration, Citrix Workspace app provides single sign-on across apps.

Prerequisites:

- Citrix Workspace Premium license
- Your identity provider configured in Citrix Cloud
- The following services configured:
  - Workspace service with Endpoint Management enabled. For information about enabling service integration, see Workspace configuration.
  - Citrix Endpoint Management service
  - Citrix Gateway service
- Citrix Workspace app for iOS
- Citrix Workspace app for Android
- Single sign-on requires that your users manually turn on VPN on Android devices.

The general setup steps described in this section are:

1. Add a native SaaS app.
2. Add device policies.
3. Use Citrix Gateway to configure and publish a native SaaS app.

Add a native SaaS app

To add a native SaaS app to Endpoint Management:

1. In the Endpoint Management console, go to Configure > Add.
2. Click Public App Store.
3. Provide the App Information and then click Next.
4. Complete the Platform pages for the iOS and Android devices you want to support. For help, see Configure app settings for platforms other than Google Play. You also need the package IDs that you copy during this setup when you configure the App attributes device policy for iOS, as described later in this section.
5. Click Next.
6. On the Delivery Group Assignment page, choose delivery groups and then click Save.
Add device policies for iOS

The following device policies are required to support single sign-on to native SSO apps. Be sure to assign each policy to at least one delivery group.

- **App Inventory device policy for iOS**: For help, see [App inventory device policy](#).
- **VPN device policy for iOS**: For help, see the VPN device policy section, [iOS settings](#).

Configure the VPN device policy as follows:

- **Connection name**: Name for the connection.
- **Connection type**: Select *Citrix SSO*.
- **Server name or IP address**: Type `vpn.netscalergateway.net`.
- **User account**: No value required.
- **Authentication type for the connection**: No value required.
- **Auth Password**: No value required.
- **Enable per-app VPN**: Set to *ON*.
- **On-demand match app enabled**: Set to *ON*.
- **Provider type**: Select *Packet tunnel*.
- **Safari domains**: Domains to trigger a per-app VPN connection. Some apps open in WebView and therefore the traffic isn’t tunneled. To enable the traffic to pass through VPN, you must provide a Safari domain. Type `app.netscalergateway.net`.
- **Custom parameters**: Set the *PerAppSplitTunnel* parameter to 1.

- **App attributes device policy for iOS**: Configuring an App attributes device policy for iOS associates an added native SaaS app with the VPN. For help, see [App attributes device policy](#).

Configure the App attributes device policy as follows:

- On the **App Attributes Policy** page, select **Add new**. A blank field appears. Provide the package ID that you noted when adding the app to Endpoint Management.
- Select the newly created VPN from the **Per-app VPN identifier** menu. You provide the package ID and associate it with a VPN so that Endpoint Management uses the associated VPN for requests for that app.

**Add a VPN device policy for Android**

Configure a VPN device policy with the following settings. Be sure to assign the policy to at least one delivery group.

- **Connection name**: Name for the connection.
- **Server name or IP address**: Type `vpn.netscalergateway.net`.
- **Connection type**: Select *Citrix SSO*.
• **Authentication type for the connection:** Default is **Password**. If you don’t provide the VPN credentials, the Citrix VPN app prompts device users for a user name and password.

• **Enable per-app VPN:** Set to **On**.

• **On-demand match app enabled:** Set to **On**. Then, select **Whitelist** or **Blacklist** depending on whether you want to list package names to allow or disallow.

• **App Package Name:** Click **Add** and then type a comma-separated list of app package names.

  **Important:**
  
  For applications that open a Chrome browser for accessing an identity provider URL, add com.android.chrome as a whitelisted application package. Otherwise, the application launch fails. You can also add other browser package names configured as the default browser for the system.

---

**Use Citrix Gateway to configure and publish a native SaaS app**

After you complete the Endpoint Management setup, you then configure and publish the app with Citrix Gateway. For steps to configure and publish a SaaS app using Citrix Gateway, see [Support for Software as a Service apps](#).

When configuring and publishing a SaaS app in Citrix Gateway:

  • Under the **Enhanced security** section, disable the **Enforce policy on mobile device** option.
  
  • Use the same user assignment to publish a SaaS app that you assigned to the VPN device policy in Endpoint Management.

---

**Add an enterprise app**

Enterprise apps in Endpoint Management represent native apps that are not wrapped with the MDX Toolkit and do not contain the policies associated with MDX apps. You can upload an enterprise app on the **Apps** tab in the Endpoint Management console. Enterprise apps support the following platforms (and corresponding file types):

  • iOS (.ipa file)
  
  • Android (.apk file)
  
  • Samsung Knox (.apk file)
  
  • Android Enterprise (.apk file)
  
  • See also: Add Win32 apps as Enterprise apps

Adding apps downloaded from the Google Play store as enterprise apps is not supported. Add apps from the Google Play store as public app store apps instead. See Add a public app store app.

  1. In the Endpoint Management console, click **Configure > Apps**. The **Apps** page opens.
2. Click **Add**. The Add App dialog box appears.

3. Click **Enterprise**. The App Information page appears.

4. 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 Create app categories.

5. Click **Next**. The App Platforms page appears.

6. Under Platforms, select the platforms you want to add. If you are only configuring for one platform, clear the others.

   When you finish configuring the settings for a platform, see Step 10 for how to set the platform deployment rules.

7. For each platform you chose, select the file to upload by clicking **Upload** and navigating to the file location.

   - If you add an Android Enterprise enterprise app, 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.
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.

Enter an email address to get updates about your apps and developer account.
After your application is published, click a private app's icon and click **Select** to open the app information page.

Proceed to Step 9 to configure the settings.

8. Click **Next**. The app information page for the platform appears.

9. 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 cannot 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.
- **Prevent app data backup:** Select whether to prevent the app from backing up data. The default is ON.
- **Force app to be managed:** If you are installing an unmanaged app, select ON if you want users on unsupervised devices to be prompted to allow management of the app. If they accept the prompt, the app is managed.

10. Configure the deployment rules. For information, see [Deploy resources](#).

11. Expand **Store Configuration**.

![Store Configuration](image)

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 cannot upload a GIF or JPEG image.
- **Allow app ratings**: Select whether to permit a user to rate the app. The default is **ON**.
- **Allow app comments**: Select whether to permit users to comment about the selected app. The default is **ON**.

12. Click **Next**. The Approvals page appears.

You use workflows when you need approval when creating user accounts. If you don’t need an approval workflow, you can skip to Step 13.

Configure these settings to assign or create a workflow:

- **Workflow to Use**: In the list, click an existing workflow 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
    * 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 Active Directory.
  - When the name appears in the field, select the check box 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 check box next to each name you want to remove.

13. Click **Next**. The **Delivery Group Assignment** page appears.

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:

   - Next to **Deploy**, click **ON** to schedule deployment or click **OFF** to prevent deployment. The default option is **ON**.
   - Next to **Deployment schedule**, click **Now** or **Later**. The default option is **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 **On every connection**.
   - Next to **Deploy for always-on connection**, click **ON** or **OFF**. The default option is **OFF**.

   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, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with version 10.18.19 or later
   - Is not recommended for Android, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with before version 10.18.19

   The deployment schedule 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 Win32 apps as Enterprise apps

You can upload MSI, APPX, AppxBundle, PS1, or EXE files for Win32 apps to the Endpoint Management console for deployment to managed Windows 10 Desktop and Tablet devices. After you use 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.
Citrix Endpoint Management

- 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. Endpoint Management no longer contains 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.

Requirements

- Windows 10, version 1607 (minimum version)
- Windows 10 Professional or Windows 10 Enterprise
- Standalone Win 32 MSI apps installed with the /quiet option. For this deployment use case, Microsoft doesn’t support MSIs containing multiple apps, nested MSIs, or interactive installation.

Look up metadata

When you add a Win32 app to 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 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 check boxes except for Windows Desktop/Tablet.
4. Configure these settings:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>App name</strong></td>
<td>The name of the app, from the app metadata.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A description for the app.</td>
</tr>
<tr>
<td><strong>App version</strong></td>
<td>The app version number, from the app metadata.</td>
</tr>
<tr>
<td><strong>Minimum OS version</strong></td>
<td>Optional. The oldest operating system version that the device can run to use the app.</td>
</tr>
<tr>
<td><strong>Maximum OS version</strong></td>
<td>Optional. The most recent operating system that the device must run to use the app.</td>
</tr>
<tr>
<td><strong>Excluded devices</strong></td>
<td>Optional. The manufacturer or models of devices that cannot run the app.</td>
</tr>
<tr>
<td><strong>Product Code</strong></td>
<td>The MSI app product code, in UUID format, from the app metadata.</td>
</tr>
<tr>
<td><strong>Installation Context</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Command Line</strong></td>
<td>The command-line options to use when calling MSIEXEC.exe</td>
</tr>
<tr>
<td><strong>Install Command Line</strong></td>
<td>Add command line arguments for installing EXE files silently.</td>
</tr>
<tr>
<td><strong>Uninstall Command Line</strong></td>
<td>Add command line arguments for uninstalling EXE files silently.</td>
</tr>
<tr>
<td><strong>Retry Count</strong></td>
<td>The number of times you can retry a download and installation operation before marking the installation as failed.</td>
</tr>
<tr>
<td><strong>Time Out</strong></td>
<td>The number of minutes that the installation process runs before the installer interprets the installation as failed and no longer monitors the process.</td>
</tr>
<tr>
<td><strong>Retry Interval</strong></td>
<td>The number of minutes between retry operations.</td>
</tr>
</tbody>
</table>

5. Specify deployment rules and store configuration as needed.
6. Click **Next** until you get to the **Summary** page and then click **Save**.

7. Go to **Configure > Delivery Groups** and add the Win32 app as a required app.

8. 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.

**Add a Web link**

In Endpoint Management, you can establish a web address (URL) to a public or private site, or to a web app that doesn’t require single sign-on (SSO).

You can configure web links from the **Apps** tab in the 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 Secure Hub, the link appears with the list of available apps and desktops.

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 Endpoint Management console, click **Configure > Apps**. The **Apps** page appears.
2. Click **Add**. The **Add App** dialog box appears.
3. Click **Web Link**. The **App Information** page appears.

4. 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 may contain 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 Citrix Gateway. Setting this option to **ON** adds the VPN keyword to the app and allows users to connect through Citrix Gateway. The default is **OFF**.
   - **App category**: In the list, click an optional category 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.

5. Expand **Store Configuration**.
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 cannot upload a GIF or JPEG image.
- **Allow app ratings**: Select whether to permit a user to rate the app. The default is **ON**.
- **Allow app comments**: Select whether to permit users to comment about the selected app. The default is **ON**.

6. Click **Next**. The **Delivery Group Assignment** page appears.

7. 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.

8. 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 **ON**.
Next to **Deployment schedule**, click **Now** or **Later**. The default option is **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 **On every connection**.

- Next to **Deploy for always-on connection**, click **ON** or **OFF**. The default option is **OFF**.

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, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with version 10.18.19 or later
- Is not recommended for Android, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with before version 10.18.19

The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for **Deploy for always-on connection**.

9. Click **Save**.

**Enable Microsoft 365 apps**

You can open the MDX container to allow Secure Mail, 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](#).

**Create and manage workflows**

You can use workflows to manage the creation and removal of user accounts. Before you can use a workflow, identify individuals in your organization who have the authority to approve user account requests. Then, you can use the workflow template to create and approve user account requests.

When you set up 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 Endpoint Management:

- In the Workflows page in the 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, you provide a workflow name and then configure the individuals who can approve the user account request.

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 persons by name or email address. When 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 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.

   ![Workflows page](image)

3. Click Add. The Add Workflow page appears.
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 Endpoint Management console. When you click the eye icon to the right of this field, the following dialog box appears.
• **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 Active Directory.

  • When the name appears in the field, select the check box 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 check box next to each name 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, you must create another workflow.
**To view details and delete a workflow**

1. On the **Workflows** page, select a workflow by clicking the row in the table or by selecting the check box next to the workflow.

2. To delete a workflow, click **Delete**. A confirmation dialog box appears. Click **Delete** again. You cannot undo this operation.

**App store and Citrix Secure Hub branding**

You can set how apps appear in the store and add a logo to brand 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 not exceed 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 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.

   ![Client Branding](image.png)

Configure the following settings:
Citrix Endpoint Management

- **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 contain 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**: Select an image or .zip file of images to use for branding by, clicking **Browse** and navigating to the file’s 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**

**Important:**
If Endpoint Management is Workspace-enabled, Citrix Workspace provides access to Virtual Apps and Desktops. The setup in this section doesn’t apply to your site.

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.

1. In the 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.

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
To allow all requests with the URL https://storefront.company.com/Citrix/PNAgent/*, enter this path: /Citrix/PNAgent/*

Endpoint Management blocks all other paths.

4. Click **Test Connection** to verify that Endpoint Management can connect to the specified StoreFront server.

5. Click **Save**.

### App connector types

July 1, 2019

The following table lists the connectors and the types of connectors that are available in Endpoint Management when you add a Web or SaaS app. You can also add a new connector to Endpoint Management when you add a Web or SaaS app.

The table indicates whether the connector supports user account management, which lets you create new accounts automatically or by using a workflow.

<table>
<thead>
<tr>
<th>Connector name</th>
<th>SSO</th>
<th>SAML</th>
<th>Supports user account management</th>
</tr>
</thead>
<tbody>
<tr>
<td>EchoSign_SAML</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Globoforce_SAML</td>
<td></td>
<td></td>
<td>Note: When using this connector, you must enable User Management for Provisioning to ensure seamless SSO integration.</td>
</tr>
<tr>
<td>GoogleApps_SAML</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>GoogleApps_SAML_IDP</td>
<td>Y</td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Lynda_SAML</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Office365_SAML</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Salesforce_SAML</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Salesforce_SAML_SP</td>
<td>Y</td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>SandBox_SAML</td>
<td>Y</td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>SuccessFactors_SAML</td>
<td>Y</td>
<td></td>
<td>Y</td>
</tr>
</tbody>
</table>
Citrix Endpoint Management

<table>
<thead>
<tr>
<th>Connector name</th>
<th>SSO SAML</th>
<th>Supports user account management</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShareFile_SAML*</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>ShareFile_SAML_SP*</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>WebEx_SAML_SP</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

* Not needed if your site is Workspace-enabled.

**Citrix Launcher**

August 26, 2019

Citrix Launcher lets you customize the user experience for Android devices deployed by Endpoint Management. The minimum Android version supported for Secure Hub management of Citrix Launcher is Android 4.0.3. Citrix Launcher and the Launcher Configuration device policy are not compatible with Android Enterprise.

You can add the **Launcher Configuration Policy** to control these Citrix Launcher features:

- Manage 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 enter to exit the launcher.

While Citrix Launcher enables you to apply those device-level restrictions, the launcher grants users built-in access to device settings such as Wi-Fi settings, Bluetooth settings, and device passcode settings. Citrix Launcher isn’t intended as an extra layer of security over what the device platform already provides.

To provide Citrix Launcher to Android devices, follow these general steps.

1. Download the Citrix Launcher app from the [Citrix XenMobile download](#) page for your Endpoint Management edition. The file name is CitrixLauncher.apk. The file is ready for uploading into Endpoint Management and doesn’t require wrapping.

2. Add the device policy **Launcher Configuration Policy**. Go to **Configure > Device Policies**, click **Add**, and in the **Add a New Policy** dialog box, start typing **Launcher**. For more information, see **Launcher Configuration Policy**.
3. Add the Citrix Launcher app to 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 for Citrix Launcher with the following configuration in Configure > Delivery groups.
   - On the Policies page, add the Launcher Configuration Policy.
   - On the Apps page, drag Citrix Launcher to Required Apps.
   - On the Summary page, click Deployment Order and ensure that the Citrix Launcher app precedes the Launcher Configuration policy.
iOS Volume Purchase

December 17, 2019

You can manage iOS app licensing by using Apple iOS volume purchase. The volume purchase solution simplifies the process to find, buy, and distribute apps and other data in bulk for an organization.

With volume purchase, you can use Endpoint Management to distribute public app store apps. Volume purchase is not supported for Citrix mobile productivity apps or for apps wrapped by using the MDX Toolkit. Although you can distribute the Endpoint Management public store apps with volume purchase, the deployment is not optimal. Further enhancements to Endpoint Management and the Secure Hub store are required to address the limitations. For a list of known issues with deploying the Endpoint Management public store apps via volume purchase, see this article in the Citrix knowledge center.

With volume purchase, you can distribute the applicable apps directly to your devices. Or, you assign content to your users by using redeemable codes. You configure settings specific to the iOS volume purchase in Endpoint Management.

Endpoint Management periodically reimports volume purchase licenses from Apple to ensure that the licenses reflect all changes. Such changes include when you manually delete an imported app
from the volume purchase. By default, Endpoint Management refreshes the volume purchase license baseline a minimum of every 720 minutes. You can change the baseline interval through the server property, volume purchase baseline interval (VP_baseline). For information, see Server properties.

This article focuses on using volume purchase with managed licenses, which enables you to use Endpoint Management to distribute apps. If you currently use redemption codes and want to change to managed distribution, see this Apple Support document: Migrate from redemption codes to managed distribution with the Volume Purchase.


After you save these iOS volume purchase settings in Endpoint Management, the purchased apps appear on the Configure > Apps page in the Endpoint Management console.

1. In the Endpoint Management console, click the gear icon in the upper-right corner. The Settings page appears.

2. Click Volume purchase. The Volume purchase configuration page appears.

3. Configure these settings:
   - Store user password in Secure Hub: Select whether to store a user name and password in Secure Hub for Endpoint Management authentication. The default is to store the information by using this secure method.
   - User property for Volume purchase country mapping: Type a code to allow users to download apps from country-specific app stores.

   Endpoint Management uses this mapping to choose the property pool of the volume purchase. For example, if the user property is United States, that user cannot download apps if the volume purchase code for the app is for the United Kingdom. Contact your volume purchase plan administrator for more information about the country mapping code.

4. For each volume purchase account you want to add, click Add. The Add a Volume purchase account dialog box appears.
5. Configure these settings for each account you add:

Note:
If you use Apple Configurator 1, upload a license file: Go to Configure > Apps, go to a platform page, and then expand Volume purchase.

- **Name**: Type the volume purchase account name.
- **Suffix**: Type the suffix to appear with the names of apps obtained through the volume purchase account. For example, if you enter VP, the Secure Mail app appears in the apps list as SecureMail-VP.
- **Company Token**: Copy and paste the volume purchase service token obtained from Apple. To obtain the token: In the Account Summary page of the Apple volume purchase portal, click the Download button to generate and download the volume purchase file. The file contains the service token and other information, like the country code and expiry. Save the file in a secure location.
- **User Login**: Type an optional authorized volume purchase account administrator name used to import custom B2B apps.
- **User Password**: Type the volume purchase account administrator password.
- **App Auto Update**: If On, volume purchase apps automatically update when an update exists on the Apple store. Default is Off.

6. Click **Save** to close the dialog box.
7. Click **Save** to save the Volume purchase configuration.

A message notes that Endpoint Management adds the apps to the list on the **Configure > Apps** page. On that page, notice that the app names from your volume purchase account include the suffix you provided in the preceding configuration.

You can now configure the volume purchase app settings and then tune your delivery group and device policy settings for volume purchase apps. After you complete those configurations, users can enroll their devices. The following notes provide considerations for those processes.

- **When configuring volume purchase app settings (Configure > Apps),** enable **Force license association to device.** An advantage of using Apple volume purchase and Deployment Program with supervised devices: The ability to use Endpoint Management to assign the app at the device (rather than user) level. As a result, you don't have to use an Apple ID device. Also, users don't receive an invitation to join the volume purchase program. Users can also download the apps without signing into their iTunes account.

To view the volume purchase info for that app, expand **Volume purchase.** Notice in the **Volume purchase License Keys** table, the license is associated with a device. If the user removes the token and then imports it again, the word **Hidden** appears instead of the serial number, due to Apple privacy restrictions.

To disassociate a license, click the row for the license and then click **Disassociate.**

If you associate volume purchase licenses with users, Endpoint Management integrates users into your volume purchase account and associates their iTunes ID with the volume purchase account. The iTunes ID of users is never visible to your company or to the Endpoint Management server. Apple transparently creates the association to retain user privacy. You can retire a user from the volume purchase program, to disassociate all licenses from the user account. To retire a user, go to **Manage > Devices.**
Endpoint Management periodically reimports volume purchase licenses from Apple to ensure that the licenses reflect all changes. To force a sync with your volume purchase account, go to Settings > iOS Settings and click Force synchronization.

After you click to confirm the action, Endpoint Management imports the volume purchase information. The import might take several minutes, depending on the number of volume purchase licenses. After the sync completes, Endpoint Management refreshes the iOS Settings page and updates the sync date and time in the new Last Sync Date column.

- When you assign an app to a delivery group, by default Endpoint Management identifies the app as an optional app. To ensure that Endpoint Management deploys an app to devices, go to Configure > Delivery Groups. On the Apps page, move the app to the Required Apps list.

- When an update for a public app store app is available: When volume purchase pushes the app, the app automatically updates on devices. To push an update for Secure Hub, when assigned to device and not to a user, do the following. In Configure > Apps, on a platform page, click Check for Updates and apply the update.

Endpoint Management displays a License Expiration Warning when Apple volume purchase has expired.
Deploy Microsoft Store for Business apps from Endpoint Management

August 26, 2019

Microsoft Store for Business is a location where you can find and distribute free and paid apps in volume for your organization. By connecting Citrix Endpoint Management to Microsoft Store for Business, the Store for Business apps appear in the Endpoint Management Configure > Apps page. You can then deploy those apps to Windows 10 devices.

Endpoint Management supports only online license app management, which is the default licensing model supported by Microsoft Store for Business. This model requires users and devices to connect to Microsoft Store services to acquire an app and its license.

To learn more about Microsoft Store for Business, see the Microsoft documentation at https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview.

Prerequisites to access Microsoft Store for Business apps

- Azure Active Directory
  
  To access Microsoft Store for Business apps, you must first configure Azure Active Directory as an Identity Provider. For information on performing this configuration, see Single sign in with Azure Active Directory.

- Microsoft Store for Business

Connect Endpoint Management to Microsoft Store for Business

1. In the Endpoint Management console Settings page, search for and click the link for Microsoft Store for Business.

2. Configure these settings:

   - **Azure AD configuration**: Select the Azure Active Directory instance you configured as part of the prerequisites.
   - **App Suffix**: Enter a suffix added to all Microsoft Store for Business apps for easy identification.
   - **Localization**: Select the language to use for the app details downloaded from Store for Business to Endpoint Management.
3. Click **Save**. Endpoint Management adds the Microsoft Store for Business apps to the **Configure > Apps** page.

4. To resync the apps later, return to the Microsoft Store for Business settings page and click the **Force Sync** button.
Associate your Microsoft Store for Business account with Endpoint Management

1. Log in to the Microsoft Business Store using the same tenant account that you use to sign in to Azure Active Directory.
2. In the Business Store, choose **Settings > Management tools**.
3. On the **Management tools** page, choose **Add a management tool**.
4. Next, choose the name you specified for the MDM solution (such as Endpoint Management or XenMobile) when configuring Azure Active Directory in the Azure portal.

Sync apps with the Store for Business

By default, Endpoint Management syncs with Microsoft Store for Business every 24 hours. To force a sync, go to **Settings > Microsoft Store for Business** and click **Force sync**.

Assign Store for Business apps to delivery groups

Apps synced from Microsoft Store for Business have the suffix you configured on the **Settings > Microsoft Store for Business** page.
1. To add those apps to delivery groups: Go to **Configure > Delivery Groups**, select a group, click **Edit**, and then click **Apps**. Move the apps to the **Required Apps** list.

2. Go to **Configure > Apps**. Select one or more apps, click **Edit**, and then click **Delivery Group Assignments**.

### Revoke a user license for an app

1. Go to **Configure > Apps**, select the Store for Business app, and then click **Edit**.

2. Under **Platform**, click **Windows Desktop/Tablet**.

3. Scroll down and expand **Microsoft Store for Business**.
Use Citrix Content Collaboration with Endpoint Management

November 21, 2019

Integration of Citrix Content Collaboration with Endpoint Management differs depending on whether your site is Workspace-enabled.

- When using Citrix Workspace and Citrix Workspace app along with the Citrix Content Collaboration service, you deploy Citrix Content Collaboration from Citrix Workspace and your users access Citrix Files from Citrix Workspace. For information, see Deploy and Create or link a Content Collaboration (ShareFile) account to Citrix Cloud.

- If Endpoint Management isn’t Workspace-enabled, Endpoint Management has two options for integrating with Citrix Content Collaboration: Citrix Files and storage zone connectors.

Citrix Files

You can configure Endpoint Management to provide access to your Content Collaboration account. That configuration:

- Gives mobile users access to the full Content Collaboration 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, AD-based user account provisioning, and comprehensive access control policies.
- Provides Content Collaboration configuration, service level monitoring, and license usage monitoring through the Endpoint Management console.

For more information about configuring Endpoint Management for Enterprise accounts, see SAML for single sign-on with Citrix Files.

Storage zone connectors

You can configure Endpoint Management to provide access only to storage zone connectors that you create through the Endpoint Management console. That configuration:
Citrix Endpoint Management

- 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 Citrix Content Collaboration subdomain, provision users to Citrix Files, 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 Endpoint Management console. If you later decide to use the full Citrix Files functionality with Endpoint Management, you can change the configuration in the Endpoint Management console.

For an Endpoint Management integration with storage zone connectors only:

- Citrix Content Collaboration uses your single sign-on configuration to Citrix Gateway to authenticate with storage zones controller.
- 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 Endpoint Management use with storage zone connectors.

Requirements

- Minimum component versions:
  - ShareFile for iOS (MDX) 5.3
  - ShareFile for Android (MDX) 5.3
This article contains instructions for how to configure storage zones controller 5.0

Ensure that the server to run 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 Endpoint Management integration with storage zone connectors only.

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 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 Citrix Gateway as a DMZ proxy for storage zones controller.

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 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 the Citrix Files download page at https://www.citrix.com/downloads/sharefile.html, log on and download the latest storage zones controller installer.
   b) Installing 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 check box for **Launch Storage Zones Controller Configuration Page** and then click **Finish**.

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 proceed 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 secondary storage zones controller to the primary controller.
- Creates a zone and sets the passphrase for it.

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:

```
1 cd c:\pstools
```
3. When prompted, click **Agree** to run the Sysinternals tool.

A PowerShell widow opens.

4. In the PowerShell window, type the following:

```
1   
2   $ Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"
3   $ New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com
4   
```

Where:
**Passphrase:** Is the passphrase 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 Endpoint Management to create storage zone connectors: Complete 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 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 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 Endpoint Management

Before you add storage zone connectors, you configure 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 > Content Collaboration page, the page summarizes the differences between using Endpoint Management for Enterprise accounts and storage zone connectors.

Click Configure Connectors to continue with the configuration steps in this article.

1. In Configure > Content Collaboration, click Manage Storage Zones.
2. In **Manage Storage Zones**, add the connection information.

   ![Manage Storage Zones](image)

   - **Name**: A descriptive name for the storage zone, used to identify the storage zone in 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 Endpoint Management server.
   - **Secure Connection**: If you use SSL for connections to 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. Alternatively, a user account with read and write permissions on the storage zones controllers.

3. Click **Save**.

4. To test the connection, verify that the 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**.
Add a storage zone connector in Endpoint Management

1. Go to **Configure > Content Collaboration** and then click **Add**.

2. On the **Connector Info** page, configure these settings:

   - **Connector Name**: A name that identifies the storage zone connector in 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. Alternatively, you can associate connectors to delivery groups using **Configure > Delivery Groups**.
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 initiates new connections to internal connections on behalf of 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 Endpoint Management. For details, see [To add Citrix Files clients to 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.
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 > Content Collaboration and then click Show filter.
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.
Switch to Enterprise account

After integrating storage zone connectors with Endpoint Management, you can later switch to the full Enterprise feature set. Endpoint Management retains your existing storage zone connector integration settings.

Go to Configure > Content Collaboration, click the Storage Zone Connectors drop-down menu, and then click Configure Content Collaboration.
SmartAccess for HDX apps

November 21, 2019

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. 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 Workspace experience
- 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 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 Endpoint Management

For information about configuring Enterprise accounts, see SAML for single sign-on with Citrix Files.
Export and configure the Endpoint Management server certificate and upload it to the StoreFront store

SmartAccess uses signed and encrypted tags to communicate between the Endpoint Management and StoreFront servers. To enable that communication, you add the Endpoint Management server certificate to the StoreFront store.

For more information about integrating StoreFront and Endpoint Management when Endpoint Management is enabled with domain and certificate-based authentication, see the Support Knowledge Center.

Export the SAML certificate from Endpoint Management

1. In the 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 Endpoint Management server.

3. Ensure 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.

2. When the certificate import wizard appears, click Next.
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.
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**.
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**.
10. Save the certificate.

11. Browse to the certificate and click **Next**.
12. Review your selections and click **Finish**. Click **OK** to dismiss the confirmation window.
13. Locate the certificate in your download directory. Note that the certificate is in CER format.
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 Endpoint Management server certificate on the store:

```
Grant-STSStorePnaSmartAccess -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:
Alternatively, you can run any of these PowerShell commands on the StoreFront server to revoke existing certificates on the StoreFront store:

- **Revoke by name:**

  ```powershell
  $store = Get-STFStoreService -VirtualPath /Citrix/Store
  Revoke-STFStorePnaSmartAccess -StoreService $store -ServerName "My XM Server"
  ```

- **Revoke by thumbprint:**

  ```powershell
  $store = Get-STFStoreService -VirtualPath /Citrix/Store
  Revoke-STFStorePnaSmartAccess -StoreService $store -CertificateThumbprint "[Thumbprint]"
  ```

- **Revoke by server object:**

  ```powershell
  $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 app or apps you want to control access to. Then select **Edit Delivery Group** in the **Actions** pane.
4. On the Access Policy page, select Connections through Citrix Gateway and Connection meeting any of the following.

5. Click Add.

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 Endpoint Management

The SmartAccess policy that you set in the delivery group for an HDX app denies access to a device when the device is out of compliance. Use automated actions to mark the device as out of compliance.
1. From the 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, 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 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 device is marked out of compliance, the HDX apps no longer appear in the Secure Hub store. The user is no longer subscribed to the apps. No notification is sent to the device and nothing in the 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.

This example creates and sends this notification when a device is marked out of compliance: “Device serial number or telephone number no longer complies with the device policy and HDX applications will be blocked.”

Create the notification users see when a device is marked as out of compliance

1. In the 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. When prompted to set up the SMS server first, click **No, set up later**.

5. Configure these settings:
   - **Name**: HDX Application Block
   - **Description**: Agent notification when device is out of compliance
   - **Type**: Ad Hoc Notification
   - **Secure Hub**: Activated
   - **Message**: Device ${firstnonnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked.

6. Click **Save**.

**Create the action that sends the notification when a device is marked out of compliance**

1. From the 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**.

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 as soon as the trigger condition is met.

7. Select the 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 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.

Upgrade MDX or enterprise apps

August 26, 2019

To upgrade an MDX or Enterprise app in Endpoint Management, disable the app in the Endpoint Management console, and then upload the new version of the app.

1. In the Endpoint Management console, click Configure > Apps. The Apps page appears.
2. For managed devices (devices enrolled in Endpoint Management for mobile device management), skip to Step 3. For unmanaged devices (devices enrolled in Endpoint Management for enterprise app management purposes only), do the following:
   • In the Apps table, select the check box next to the app or click the line containing the app you want to update.
• Click **Disable** in the menu that appears.

![Image showing the Apps table with a check box and options for editing and disabling an app]

• Click **Disable** in the confirmation dialog box. **Disabled** appears in the **Disable** column for the app.

![Image showing the Apps table with the disabled status for an app]

**Note:**

Disabling an app puts the app in maintenance mode. While the app is disabled, users cannot reconnect to the app after they log off. Disabling an app is an optional setting, but we recommend disabling the app to avoid issues with app functionality. Issues may result from policy updates, for example, or if users request a download at the same time you are uploading the app to Endpoint Management.

3. In the **Apps** table, click the check box next to the app or click the line containing 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.
Citrix Endpoint Management

- **App category:** Optionally, change the app category.

6. Click **Next.** The first selected platform page appears. Do the following for each selected platform:

- Choose the replacement file you want to upload by clicking **Upload** and navigating to the file location. The app uploads to Endpoint Management.
- Optionally, change the app details and policy settings for the platform.
- 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:

- In the **Apps** table, click to select the app you updated and then in the menu that appears, click **Enable.**
- 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**

November 7, 2019

You add media to Endpoint Management so you can deploy the media to user devices. You can use Endpoint Management to deploy iBooks that you obtain through Apple volume purchase.

After you configure a volume purchase account in Endpoint Management, your purchased and free books appear in **Configure > Media.** From the **Media** pages, you configure iBooks for deployment to iOS devices by choosing delivery groups and specifying deployment rules.

The first time that a user receives an iBook and accepts the volume purchase license, deployed books install on the device. The books appear in the Apple iBook app. You can't disassociate the book license from the user or remove the book from the device. Endpoint Management installs iBooks as required media. If a user deletes an installed book from their device, the book remains in the iBook app, ready for download.

**Prerequisites**

- iOS devices
- Configure iOS volume purchase in Endpoint Management, as described in **iOS Volume Purchase.**

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Configure iBooks

iBooks obtained through volume purchase appear on the **Configure > Media** page.

To configure an iBook for deployment

1. In **Configure > Media**, select an iBook and click **Edit**. The **Book Information** page appears.

   ![Book Information](image)

   The **Name** and **Description** appear only in the Endpoint Management console and logs.

2. In the **iPhone iBook Settings** and **iPad iBook Settings** pages: While you can optionally change the iBook 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 an iBook is purchased through volume purchase.
You can also specify deployment rules or view volume purchase information.

3. Optionally, assign the iBook to delivery groups and set a deployment schedule.

You can also assign iBooks to delivery groups from the **Media** tab for **Configure > Delivery**
Groups. 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, Endpoint Management removes the book from the list. However, the next time Endpoint Management syncs with volume purchase, the book reappears on the list unless it has been removed from volume purchase. Deleting a book from the list doesn’t remove the book from devices.

iBooks appear on user devices as shown in the following example.
Deploy resources

December 13, 2019

Device configuration and management typically involve creating resources (policies, apps, and media) and actions in the Endpoint Management console and then packaging them using delivery groups. The order in which Endpoint Management pushes resources and actions in a delivery group to devices is called the deployment order. This article describes how:

- To add, manage, and deploy delivery groups
- To change the deployment order of resources and actions in delivery groups

Endpoint Management determines deployment order when a user is in multiple delivery groups that have duplicate or conflicting policies.

Delivery groups specify the category of users to whose devices you deploy combinations of policies, apps, media, and actions. 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 what resources and when they get them. You can deploy a delivery group to everyone or to a more narrowly defined group of users. Citrix recommends creating delivery groups before you create device policies.

Deploying to a delivery group means sending a push notification to all users with supported iOS and
Citrix Endpoint Management

Windows devices. Those users must belong to the delivery group to reconnect to Endpoint Management. You can reevaluate the devices and deploy policies, apps, media, and actions that are part of a delivery group.

For Android devices: Citrix recommends that you use Firebase Cloud Messaging (FCM) to control connections from Android, Android Enterprise, and Chrome OS devices to Endpoint Management. For information on using FCM, see Firebase Cloud Messaging.

The default AllUsers delivery group is created when you install and configure Endpoint Management. It contains all local users and Active Directory users. You cannot delete the AllUsers group, but you can disable the group when you do not want to push resources to all users.

Deployment Ordering

Deployment order is the sequence in which Endpoint Management pushes resources to devices. Deployment order is supported only for MDM mode.

When determining deployment order, Endpoint Management applies filters and control criteria, such as deployment rules and deployment schedule, to policies, apps, media, actions, and delivery groups. Before adding delivery groups, consider how the information in this section relates to your deployment goals.

Here's a summary of the main concepts related to deployment order:

- **Deployment order**: The sequence in which Endpoint Management pushes resources (policies, apps, and media) and actions to a device. Deployment order for some policies, such as Terms and Conditions and Software Inventory, has no effect on other resources. The order in which actions are deployed has no effect on other resources, so their position is ignored when Endpoint Management deploys the resources.

- **Deployment rules**: Endpoint Management uses the deployment rules that you specify for 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.

- **Deployment schedule**: 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 immediately, on a particular date and time, or according to deployment conditions.

The following table shows filter and control criteria for the various object and resource types. Deployment rules are based on device properties.
Citrix Endpoint Management

<table>
<thead>
<tr>
<th>Object/Resource</th>
<th>Device platform</th>
<th>Deployment rule</th>
<th>Deployment schedule</th>
<th>User/groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device policy</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>-</td>
</tr>
<tr>
<td>App</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>-</td>
</tr>
<tr>
<td>Media</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>-</td>
</tr>
<tr>
<td>Action</td>
<td>-</td>
<td>Y</td>
<td>Y</td>
<td>-</td>
</tr>
<tr>
<td>Delivery group</td>
<td>-</td>
<td>Y</td>
<td>-</td>
<td>Y</td>
</tr>
</tbody>
</table>

It is likely that, in a typical environment, multiple delivery groups become assigned to a single user, with the following possible results:

- Duplicate objects exist within the delivery groups.
- A specific policy is configured differently in more than one delivery group that is assigned to a user.

When either of those situations occur, Endpoint Management calculates a deployment order for all the objects that it must deliver to a device or act upon. The calculation steps are independent of the device platform.

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) within 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 a user-defined deployment order ahead of resources from delivery groups without one. The rationale for this placement is described after these steps.

   b) As a tie-breaker among delivery groups, order resources from delivery groups by delivery group name. For example, place resources from delivery group A ahead of resources from delivery group B.

   c) While sorting, if a user-defined deployment order is specified for resources of a delivery group, maintain that order. Otherwise, sort the resources within that delivery group by resource name.

   d) If the same resource appears more than once, then remove the duplicate resource.

Resources that have a user-defined order associated with them deploy before resources without a user-defined order. A resource can exist in multiple delivery groups assigned to user. As indicated in
the steps above, the calculation algorithm removes redundant resources and only delivers the first resource in this list. By removing duplicate resources in that way, Endpoint Management enforces the order defined by the Endpoint Management administrator.

For example, suppose that you have two delivery groups as follows:

- Delivery group, Account Managers 1: With unspecified order for resources. Contains the policies WiFi and Passcode.
- Delivery group, Account Managers 2: With specified order for resources. Contains the policies Connection scheduling, Restrictions, Passcode, and WiFi. In this case, you want to deliver the Passcode policy before the WiFi policy.

If the calculation algorithm ordered deployment groups only by name, Endpoint Management would perform the deployment in this order, starting with the delivery group Account Managers 1: WiFi, Passcode, Connection scheduling, and Restrictions. Endpoint Management would ignore Passcode and WiFi, both duplicates, from the Account Managers 2 delivery group.

However, the Account Managers 2 group has an admin-specified deployment order. Therefore, the calculation algorithm places resources from the Account Managers 2 delivery group higher in the list than the resources from the other delivery group. As a result, Endpoint Management deploys the policies in this order: Connection scheduling, Restrictions, Passcode, and WiFi. Endpoint Management ignores the policies WiFi and Passcode from the Account Managers 1 delivery group, because they are duplicates. That algorithm therefore respects the order specified by the Endpoint Management administrator.
To add a delivery group

When you create a delivery group, you specify whether the user assignments are managed in Endpoint Management or in Citrix Cloud. You cannot 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 services include Citrix Virtual Apps and Desktops, Citrix Content Collaboration, or Secure Browser Service. You can only add Active Directory users to these delivery groups.

If you only need mobility management for a delivery group of users and apps, set Manage user assignments to In Endpoint Management. Delivery groups with users managed in Endpoint Management are not visible in Citrix Cloud. Therefore, you cannot use delivery groups managed in Endpoint Management to deliver other services.

Citrix recommends creating delivery groups before you create device policies.

1. In the 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 User Assignments page, specify how to manage the delivery group user assignments.
Important:
You cannot change the Manage user assignments setting after the user group is created.

- **Manage user assignments:**
  - **In Endpoint Management:** Select this option if you plan to create a delivery group for users and apps that only need mobility management. Delivery groups whose user assignments are managed in Endpoint Management are not visible in Citrix Cloud and cannot be used 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 Citrix Content Collaboration.

- **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.
  - 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 check box 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 check box of each of the groups you want to remove.

- **Or/And**: Select whether users can be 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 whom you were not able to authenticate, but you allowed their devices to connect to Endpoint Management anyway.

5. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.

   - In the lists, click options to 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 All.
   - Click New Rule to define the conditions.
   - In the lists, click the conditions, such as Device ownership and BYOD.
   - Click New Rule again to add conditions.

6. Click the Advanced tab to combine the rules with Boolean options. The conditions you chose on the Base tab appear.

7. You can use more advanced Boolean logic to combine, edit, or add rules.

   - Click AND, OR, or NOT.

   - To add the condition to the 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.

   - Click New Rule again if you want to add conditions.

8. Click Next. The Delivery Group Resources page appears. You optionally add policies, apps, or actions for the delivery group here. To skip this step, under Delivery Group, click Summary to see a summary the delivery group configuration.

    To skip a resource, under Resources (optional), click the resource you want to add and follow the steps for that resource.
Citrix Endpoint Management

To add a delivery group (Preview)

The delivery group feature in preview allows you to create delivery groups based on user properties, user domains, and device properties. To request access to this feature, contact your Citrix sales or support representative.

1. In the 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.

---

**Important:**

You cannot change the **Manage user assignments** setting after the user group is created.

- **Manage user assignments:**
  - **In Endpoint Management:** Select this option if you plan to create a delivery group for users and apps that only need mobility management. Delivery groups whose user assignments are managed in Endpoint Management are not visible in Citrix Cloud and cannot be used 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 Citrix Content Collaboration.

- **Group by**:
  - **Users, optionally filtered by devices**: Select this option to configure delivery groups by user groups. You can also filter by device properties.
  - **Devices, optionally filtered by users (Windows Desktop/Tablet only)**: Select this option to configure delivery groups by device properties. You can also filter by user groups. This option is only available for Windows desktops and tablets.

5. If you select **Users, optionally filtered by devices**, configure the following:

   ![User Domain Groups](image)

   - **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.
- 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 check box 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 check box of each of the groups 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 whom you were not able to authenticate, but you allowed their devices to connect to Endpoint Management anyway.

- **Filter by User Properties** and **Filter by Device Properties** (Windows Desktop/Tablet only):
  - Under the **Base** tab click options to 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 **All**.
    * Click **New Rule** to define the conditions.
    * In the lists, click the conditions, such as Device ownership and BYOD.
    * Click **New Rule** again to add conditions.
  - 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**, then click **New Rule**.
    * To add the condition to the 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.

6. **Devices, optionally filtered by users (Windows Desktop/Tablet only)**, configure the deployment rules as described in the previous step. You can also configure filters for user domain membership and user properties as described previously.
7. Click **Next**. The **Delivery Group Resources** page appears. You optionally add policies, apps, or actions for the delivery group here. To skip this step, under **Delivery Group**, click **Summary** to see a summary the delivery group configuration.

To skip a resource, under **Resources (optional)**, click the resource you want to add and follow the steps for that resource.

**To add policies**

1. 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, to limit the list of policies, type a full or partial policy name in the search box, and then click **Search**.
   - Click the policy you want to add and drag it into the box on the right.

   To remove a policy, click the X next to the policy name in the box on the right.
2. Click **Next**. The **Apps** page appears.

**To add apps**

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, to limit the list of apps, type a full or partial app name in the search box, and then click **Search**.
   - Click the app you want to add and drag it 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:

- You upload a new app and mark it as required.
- You mark an existing app as required.
- As user deletes a required app.
- A 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, click the **X** next to the app name in the box on the right.

2. Click **Next**. The **Media** page appears.

### To add media

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, to limit the list of books, type a full or partial book name in the search box, and then click **Search**.
   - Click the book you want to add and drag it into the **Required Books** box.
For books marked as required, users promptly receive updates in situations such as:

- You upload a new book and mark it as required.
- You mark an existing book as required.
- As user deletes a required book.
- A Secure Hub update is available.

To remove a book, click the X next to the book name in the box on the right.

2. Click Next. The Actions page appears.

To add actions

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, to limit the list of actions, type a full or partial action name in the search box, and then click Search.
   - Click the action you want to add and drag it into the box on the right.

To remove an action, click the X next to the action name in the box on the right.
2. Click Next. The **ShareFile** (now called Content Collaboration) page appears.

**To apply the Content Collaboration configuration**

The Content Collaboration page differs depending on whether you configured Endpoint Management (**Configure > Content Collaboration**) for Enterprise accounts or for storage zone connectors.

If you configured Enterprise accounts for use with Endpoint Management: Set **Enable ShareFile** to **ON** to provide the delivery group single sign-on access to Content Collaboration content and data.

If you configured storage zone connectors for use with Endpoint Management, select the storage zone connectors to include in the delivery group.
To select an enrollment profile

- **Enrollment Profile**: Select an Enrollment Profile. To create an enrollment profile, see [Device enrollment limit](#).

- Click **Next**. The **Summary** page appears.
To review configured options and change deployment order

On the Summary page, you can review the options you have 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 reflect the deployment order.

1. Click Back to return to previous pages to make any necessary adjustments to the configuration.

2. Click Deployment Order to view the deployment order or to reorder the deployment order. The Deployment Order dialog box appears.
3. Click a resource and drag it to the location from which you want it deployed. After you change the deployment order, Endpoint Management deploys resources in the list from top to bottom.

4. Click **Save** to save the deployment order.

5. Click **Save** to save the delivery group.

**To 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**.

**To enable and disable the AllUsers delivery group**

AllUsers is the only delivery group that you can enable or disable.

From the **Delivery Groups** page, choose the AllUsers delivery group by selecting the check box 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 only available if AllUsers 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 only available if AllUsers is disabled. **Disabled** disappears from under the **Disabled** heading in the delivery group table.

**To deploy to delivery groups**

Deploying to a delivery group means sending a push notification to all users with iOS, Windows Phone, and Windows tablet devices. Those users must belong to the delivery group to reconnect to Endpoint Management. In that way, you can reevaluate the devices and deploy apps, policies, and actions.

For users with other platform devices: If those devices are already connected to 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.

1. On the **Delivery Groups** page, do one of the following:
   - To deploy to more than one delivery group at a time, select the check boxes next to the groups you want to deploy.
   - To deploy to a single delivery group, either select the check box 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 above or to the right of the delivery group.

Verify that the groups to which you want to deploy apps, policies, and actions are listed and 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 containing the delivery group to display an overlay that indicates **Installed**, **Pending**, and **Failed** deployments.

![Delivery Groups page](image)

**To delete delivery groups**

You cannot delete the AllUsers delivery group, but you can disable the group when you do not want to push resources to all users.

1. On the **Delivery Groups** page, do one of the following:
   - To delete more than one delivery group at a time, select the check boxes next to the groups you want to delete.
   - To delete a single delivery group, either select the check box next to its name or click the line containing its name.
2. Click **Delete**. The **Delete** dialog box appears.

   Depending on how you select a single delivery group, the **Delete** command appears above or to the right of the delivery group.

   **Important:**
   You cannot undo a delete.

3. Click **Delete**.

**To export the Delivery Groups table**

1. Click the **Export** button above the **Delivery Groups** table. 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. You can also cancel the operation.

**Macros**

November 21, 2019

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

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 }
Citrix Endpoint Management

- `{ 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 omit 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 multiple users. The following example shows how to use macros in an 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 ${ firstnonnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked.

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`
- `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

This example shows how to create a notification that includes enrollment URLs for multiple device platforms. The macro for the **Message** is:

```
${enrollment.urls}
```
These examples show how to create messages for notifications that prompt the users to click the enrollment URL for their device platforms:

Example 1:

```plaintext
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}  
- ${
```
Example 2:

1. To enroll an iOS device, click the link `enrollment.ios.url`.
2. To enroll a macOS device, click the link `enrollment.macos.url`.
3. 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 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 Webclip device policy, you can use this macro for the **URL**:

- `${webclips-url}`
Macros to obtain built-in device properties

**Display name:** Device Id
- **Macros:** $device.id

**Display name:** Device IMEI
- **Macros:** $device.imei

**Display name:** OS Family
- **Macros:** $device.OSFamily

**Display name:** Serial Number
- **Macros:** $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 iTunes account
- **Web element:** ACTIVE_ITUNES
- **Macros:** ${ device.ACTIVE_ITUNES }

**Display name:** ActiveSync device known by MSP
- **Web element:** AS_DEVICE_KNOWN_BY_ZMSP
- **Macros:** ${ device.AS_DEVICE_KNOWN_BY_ZMSP }

**Display name:** Administrator disabled
- **Web element:** ADMIN_DISABLED
Citrix Endpoint Management

- **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  
  - **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 DEP activation lock bypass code
• **Web element:** DEP_ACTIVATION_LOCK_BYPASS_CODE
  • **Macros:** ${ device.DEP_ACTIVATION_LOCK_BYPASS_CODE }

  **Display name:** ASM DEP escrow key
  • **Web element:** DEP_ESCROW_KEY
  • **Macros:** ${ device.DEP_ESCROW_KEY }

• **Web element:** ASSET_TAG
  • **Macros:** ${ device.ASSET_TAG }

  **Display name:** Asset tag

• **Web element:** AutoCheckEnabled
  • **Macros:** ${ device.AutoCheckEnabled }

  **Display name:** Automatically check software updates

• **Web element:** BackgroundDownloadEnabled
  • **Macros:** ${ device.BackgroundDownloadEnabled }

  **Display name:** Automatically download software updates in the background

• **Web element:** AutomaticAppInstallationEnabled
  • **Macros:** ${ device.AutomaticAppInstallationEnabled }

  **Display name:** Automatically install app updates

• **Web element:** AutomaticOSInstallationEnabled
  • **Macros:** ${ device.AutomaticOSInstallationEnabled }

  **Display name:** Automatically install OS updates

• **Web element:** AutomaticSecurityUpdatesEnabled
  • **Macros:** ${ device.AutomaticSecurityUpdatesEnabled }

  **Display name:** Automatically install security updates

• **Web element:** AUTOUPDATE_STATUS
  • **Macros:** ${ device.AUTOUPDATE_STATUS }

  **Display name:** Autoupdate Status

• **Web element:** MEMORY_AVAILABLE
  • **Macros:** ${ device.MEMORY_AVAILABLE }

  **Display name:** Available RAM
Display name: Available software updates

- 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 device known by MSP

- Web element: BES_Device_Known_by_ZMSP
Citrix Endpoint Management

- **Macros:** ${ device.BES_DEVICE_KNOWN_BY_ZMSP }

**Display name:** BES PIN

- **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
• **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

• **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

- Web element: CPU_CLOCK_SPEED
- Macros: ${device.CPU_CLOCK_SPEED}

Display name: CPU type

- Web element: CPU_TYPE
Citrix Endpoint Management

- **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
- **Web element:** IsDefaultCatalog
- **Macros:** \${ device.IsDefaultCatalog }

**Display name:** DEP account name
- **Web element:** BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- **Macros:** \${ device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME }

**Display name:** DEP Policy
Citrix Endpoint Management

- **Web element**: WINDOWS_HAS_DEP_POLICY
- **Macros**: ${ device.WINDOWS_HAS_DEP_POLICY }

**Display name**: DEP profile assigned

- **Web element**: PROFILE_ASSIGN_TIME
- **Macros**: ${ device.PROFILE_ASSIGN_TIME }

**Display name**: DEP profile pushed

- **Web element**: PROFILE_PUSH_TIME
- **Macros**: ${ device.PROFILE_PUSH_TIME }

**Display name**: DEP profile removed

- **Web element**: PROFILE_REMOVE_TIME
- **Macros**: ${ device.PROFILE_REMOVE_TIME }

**Display name**: DEP registration by

- **Web element**: DEVICE_ASSIGNED_BY
- **Macros**: ${ device.DEVICE_ASSIGNED_BY }

**Display name**: DEP 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

- **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
- **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

• **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

• **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
- **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 iTunes 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: HTC API version

• **Web element:** HTC_MDM_VERSION

• **Macros:** 
  ```
  \{ device.HTC_MDM_VERSION \}
  ```

Display name: HTC MDM API available

• **Web element:** HTC_MDM

• **Macros:** 
  ```
  \{ device.HTC_MDM \}
  ```

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

• **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
Citrix Endpoint Management

- **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
- **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 }
Citrix Endpoint Management

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
  • 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
  • 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
  • **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 }  

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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
- 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  
  • **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 Compliance  
  • **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?

• **Web element:** WINDOWS_HAS_SAFE_MODE
  
  **Macros:** \$\{ device.WINDOWS_HAS_SAFE_MODE \}  

**Display name:** Samsung Knox API available

• **Web element:** SAMSUNG_KNOX
  
  **Macros:** \$\{ device.SAMSUNG_KNOX \}  

**Display name:** Samsung Knox API version

• **Web element:** SAMSUNG_KNOX_VERSION
  
  **Macros:** \$\{ device.SAMSUNG_KNOX_VERSION \}  

**Display name:** Samsung Knox attestation

• **Web element:** SAMSUNG_KNOX_ATTESTED
  
  **Macros:** \$\{ device.SAMSUNG_KNOX_ATTESTED \}  

**Display name:** Samsung Knox attestation updated date

• **Web element:** SAMSUNG_KNOX_ATT_UPDATED_TIME
  
  **Macros:** \$\{ device.SAMSUNG_KNOX_ATT_UPDATED_TIME \}  

**Display name:** Samsung SAFE API available

• **Web element:** SAMSUNG_MDM
  
  **Macros:** \$\{ device.SAMSUNG_MDM \}  

**Display name:** Samsung SAFE API version

• **Web element:** SAMSUNG_MDM_VERSION
  
  **Macros:** \$\{ device.SAMSUNG_MDM_VERSION \}  

**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
  • 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
**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

- **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**: Sony Enterprise API available

- **Web element**: SONY_MDM
- **Macros**: `${ device.SONY_MDM }`
• **Web element**: SONY_MDM_VERSION
  • **Macros**: ${ device.SONY_MDM_VERSION }

**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
  • **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: $\{ \text{device.UDID} \}$

Display name: User Account Control Status
  • Web element: UAC_STATUS
  • Macros: $\{ \text{device.UAC_STATUS} \}$

Display name: User agent
  • Web element: USER_AGENT
  • Macros: $\{ \text{device.USER_AGENT} \}$

Display name: User defined #1
  • Web element: USER_DEFINED_1
  • Macros: $\{ \text{device.USER_DEFINED_1} \}$

Display name: User defined #2
  • Web element: USER_DEFINED_2
  • Macros: $\{ \text{device.USER_DEFINED_2} \}$

Display name: User defined #3
  • Web element: USER_DEFINED_3
  • Macros: $\{ \text{device.USER_DEFINED_3} \}$

Display name: User language (locale)
  • Web element: USER_LANGUAGE
  • Macros: $\{ \text{device.USER_LANGUAGE} \}$

Display name: Vendor
  • Web element: VENDOR
  • Macros: $\{ \text{device.VENDOR} \}$

Display name: Voice capable
  • Web element: IS_VOICE_CAPABLE
  • Macros: $\{ \text{device.IS_VOICE_CAPABLE} \}$

Display name: Voice roaming allowed
  • Web element: VOICE_ROAMING_ENABLED
Citrix Endpoint Management

- 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
- 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:** Endpoint Management agent ID
- Web element: ENROLLMENT_AGENT_ID
- Macros: \{ device.ENROLLMENT_AGENT_ID \}

**Display name:** Endpoint Management agent revision
- Web element: EW_REVISION
- Macros: \{ device.EW_REVISION \}

**Display name:** 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 obtain built-in user properties**

<table>
<thead>
<tr>
<th>Display name</th>
<th>Macros</th>
</tr>
</thead>
<tbody>
<tr>
<td>domainname</td>
<td>${ user.domainname }</td>
</tr>
<tr>
<td>loginname</td>
<td>${ user.loginnname }</td>
</tr>
<tr>
<td>username</td>
<td>${ user.username }</td>
</tr>
</tbody>
</table>

**Macros for all user properties**

<table>
<thead>
<tr>
<th>Display name</th>
<th>Web element</th>
<th>Macros</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory failed logon tries</td>
<td>badpwdcount</td>
<td>${ user.badpwdcount }</td>
</tr>
<tr>
<td>ActiveSync user email</td>
<td>asuseremail</td>
<td>${ user.asuseremail }</td>
</tr>
<tr>
<td>ASM data source</td>
<td>asmpersonsource</td>
<td>${ user.asmpersonsource }</td>
</tr>
<tr>
<td>ASM Deployment Program account name</td>
<td>asmdepaccount</td>
<td>${ user.asmdepaccount }</td>
</tr>
<tr>
<td>Display name</td>
<td>Web element</td>
<td>Macros</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>ASM managed Apple ID</td>
<td>asmpersonmanagedappleid</td>
<td>${user.asmpersonmanagedappleid}</td>
</tr>
<tr>
<td>ASM passcode type</td>
<td>asmpersonpasscodetype</td>
<td>${user.asmpersonpasscodetype}</td>
</tr>
<tr>
<td>ASM person ID</td>
<td>asmpersonid</td>
<td>${user.asmpersonid}</td>
</tr>
<tr>
<td>ASM person status</td>
<td>asmpersonstatus</td>
<td>${user.asmpersonstatus}</td>
</tr>
<tr>
<td>ASM person title</td>
<td>asmpersontitle</td>
<td>${user.asmpersontitle}</td>
</tr>
<tr>
<td>ASM person unique ID</td>
<td>asmpersonuniqueid</td>
<td>${user.asmpersonuniqueid}</td>
</tr>
<tr>
<td>ASM source system ID</td>
<td>asmpersonsourcesystemid</td>
<td>${user.asmpersonsourcesystemid}</td>
</tr>
<tr>
<td>ASM student grade</td>
<td>asmpersongrade</td>
<td>${user.asmpersongrade}</td>
</tr>
<tr>
<td>BES user email</td>
<td>besuseremail</td>
<td>${user.besuseremail}</td>
</tr>
<tr>
<td>Company</td>
<td>company</td>
<td>${user.company}</td>
</tr>
<tr>
<td>Company name</td>
<td>companyname</td>
<td>${user.companyname}</td>
</tr>
<tr>
<td>Country</td>
<td>c</td>
<td>${user.c}</td>
</tr>
<tr>
<td>Department</td>
<td>department</td>
<td>${user.department}</td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
<td>${user.description}</td>
</tr>
<tr>
<td>Disabled user</td>
<td>disableduser</td>
<td>${user.disableduser}</td>
</tr>
<tr>
<td>Display name</td>
<td>displayname</td>
<td>${user.displayname}</td>
</tr>
<tr>
<td>Distinguished name</td>
<td>distinguishedname</td>
<td>${user.distinguishedname}</td>
</tr>
<tr>
<td>Domain name</td>
<td>domainname</td>
<td>${user.domainname}</td>
</tr>
<tr>
<td>Email</td>
<td>mail</td>
<td>${user.mail}</td>
</tr>
<tr>
<td>Display name</td>
<td>Web element</td>
<td>Macros</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>First name</td>
<td>givenname</td>
<td>${ user.givenname }</td>
</tr>
<tr>
<td>Home address</td>
<td>homestreetaddress</td>
<td>${ user.homestreetaddress }</td>
</tr>
<tr>
<td>Home city</td>
<td>homecity</td>
<td>${ user.homecity }</td>
</tr>
<tr>
<td>Home country</td>
<td>homecountry</td>
<td>${ user.homecountry }</td>
</tr>
<tr>
<td>Home fax</td>
<td>homefax</td>
<td>${ user.homefax }</td>
</tr>
<tr>
<td>Home phone</td>
<td>homephone</td>
<td>${ user.homephone }</td>
</tr>
<tr>
<td>Home state/region</td>
<td>homestate</td>
<td>${ user.homestate }</td>
</tr>
<tr>
<td>Home zip or post code</td>
<td>homezip</td>
<td>${ user.homezip }</td>
</tr>
<tr>
<td>IP phone</td>
<td>ipphone</td>
<td>${ user.ipphone }</td>
</tr>
<tr>
<td>Middle initial</td>
<td>middleinitial</td>
<td>${ user.middleinitial }</td>
</tr>
<tr>
<td>Middle name</td>
<td>middlename</td>
<td>${ user.middlename }</td>
</tr>
<tr>
<td>Mobile</td>
<td>mobile</td>
<td>${ user.mobile }</td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
<td>${ user.cn }</td>
</tr>
<tr>
<td>Office address</td>
<td>physicaldeliveryofficename</td>
<td>${ user.physicaldeliveryofficename }</td>
</tr>
<tr>
<td>Office city</td>
<td>l</td>
<td>${ user.l }</td>
</tr>
<tr>
<td>Office fax number</td>
<td>facsimiletelephonenumber</td>
<td>${ user.facsimiletelephonenumber }</td>
</tr>
<tr>
<td>Office state/province</td>
<td>st</td>
<td>${ user.st }</td>
</tr>
<tr>
<td>Office street address</td>
<td>officestreetaddress</td>
<td>${ user.officestreetaddress }</td>
</tr>
<tr>
<td>Office telephone number</td>
<td>telephonenumber</td>
<td>${ user.telephonenumber }</td>
</tr>
<tr>
<td>Office zip or post code</td>
<td>postalcode</td>
<td>${ user.postalcode }</td>
</tr>
<tr>
<td>P.O. box</td>
<td>postofficebox</td>
<td>${ user.postofficebox }</td>
</tr>
<tr>
<td>Pager</td>
<td>pager</td>
<td>${ user.pager }</td>
</tr>
</tbody>
</table>
### Display name | Web element | Macros
--- | --- | ---
Primary group ID | `primarygroupid` | `{$ user.primarygroupid }`
SAM account | `samaccountname` | `{$ user.samaccountname }`
Street address | `streetaddress` | `{$ user.streetaddress }`
Surname | `sn` | `{$ user.sn }`
Title | `title` | `{$ user.title }`
User logon name | `userprincipalname` | `{$ user.userprincipalname }`

## Automated actions

**November 21, 2019**

You create automated actions in Endpoint Management to program a reaction to events, user or device properties, or 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 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.

For example, suppose that you want to detect an app that you previously blacklisted (for example, “Words with Friends”). You can specify a trigger that sets the user device out of compliance when “Words with Friends” is detected on the device. 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.

In cases in which a user device is put into an out of compliance state, and then the user fixes the device: Configure a policy to deploy a package that resets the device into a compliant state.

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 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 Endpoint Management settings for SMTP and SMS so that Endpoint Management can send the messages. For information, see [Notifications](#). Also, set up any notification templates you plan to use before proceeding. For details, see [Create and update notification templates](#).

To add, edit, and filter automated actions:

1. From the 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 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 an **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. The meaning of each trigger is as follows:

- **Event**: Reacts to a predefined event.
- **Device property**: Checks for a device attribute on the device gathered in MDM mode and reacts to it. For more information, see the [Device property names and values PDF](#).
- **User property**: Reacts to a user attribute, usually from Active Directory.
- **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 performed when the trigger criterion is met. Except for **Send notification**, 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 template using **Notification Template** in **Settings**.

Before you can notify users, you must have configured notification servers in **Settings** for SMTP and SMS so that Endpoint Management can send the messages, see [Notifications](#). Also, set up any notification templates you plan to use before proceeding. For details on setting up notification templates, see [Create and update notification templates](#).

After you select the template, you can preview the notification by clicking **Preview notification message**.
10. In the following fields, set the delay in days, hours, or minutes before performing 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 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**.
   - Device local encryption must be **True**.
   - 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 **Delivery groups to receive app assignment** list.
16. 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 **ON**. If you choose **OFF**, no other options are required.
- Next to **Deployment schedule**, click **Now** or **Later**. The default option is **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 **On every connection**.
- Next to **Deploy for always-on connection**, click **ON** or **OFF**. The default option is **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, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with version 10.18.19 or later
- Is not recommended for Android, Android Enterprise, and Chrome OS to customers who began using Endpoint Management with before version 10.18.19

The deployment schedule 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 in response to all four categories of triggers listed in the Endpoint Management console: event, device property, user property, and installed app name.

**To configure automatic app wipe or app lock**

1. In the Endpoint Management console, click **Configure > Actions**.
2. On the **Actions** page, click **Add**.
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.


For this step, keep the following conditions in mind:

When the trigger type is **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 **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 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 Endpoint Management.

6. Configure 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**.

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 devices out of compliance in Azure AD

When Windows 10 devices joined to Azure AD are marked out of compliance by Endpoint Management, they can also be marked out of compliance in Azure AD. To enable this functionality, add permissions to 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 permissions.

Whenever a Windows 10 Azure AD enrolled device is marked out of compliance by Endpoint Management, it is also marked out of compliance in Azure AD.

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_checkFirewall`. As shown in the following screen, the related Windows Agent device policy defines a config named `cName_checkFirewall`. That config runs the sample script.

![Windows Agent policy configuration](image)

After the script runs on a device, you get the info needed to create an action, as described in Windows Agent device policy.

2. In the 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.

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

November 1, 2019

You can use the Endpoint Management Dashboard and the Endpoint Management Support page to monitor and troubleshoot your Endpoint Management server. Use the Endpoint Management Support page to access support-related information and tools.

In the Endpoint Management console, click the wrench icon in the upper-right corner.

The **Troubleshooting and Support** page appears.

Use the 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 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 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.
  - **Notifications**: Mark the check box 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 Apple volume purchase apps.

With each widget, you can click the individual parts to drill down for more information.

You can also export the information as a .csv file by clicking the **Action** drop-down.
Monitor page for help desk administrators

You can monitor and troubleshoot 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
  - Monitor
The Monitor page gives you a consolidated 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 containing:
  - 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 MAM/MDM managed. The panel also shows the storage encryption status.
  - Running Applications table: Displays the details of the applications currently running on the device.
- 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 Endpoint Management > Manage > Monitor.

Access to Endpoint Management Tools from the console

You can access these Endpoint Management Tools from the Endpoint Management console:

- **Endpoint Management Analyzer** – Identify and triage potential issues with your deployment.
- **APNs Portal** – Submit a request to Citrix to sign an APNs certificate, which you then submit to Apple.
- **Auto Discovery Service** – Request and configure Auto Discovery for Endpoint Management in your domain.
- **Manage Push Notifications** – Manage push notifications for iOS and Windows mobile apps.
- **MDX Service** – Wraps apps that you can then manage by using Endpoint Management.

To access these tools, go to Settings > Endpoint Management Tools. This page is available to users with the Cloud Admin or Customer Admin role.
View and analyze log files in Endpoint Management

1. In the Endpoint Management console, click the wrench icon in the upper-right corner of the console. The Troubleshooting and Support page opens.


3. Select the log you want to view:
• Debug Log Files contain information useful for Citrix Support, such as error messages and server-related actions.
• Admin Audit Log Files contain audit information about activity on the Endpoint Management console.
• User Audit Log Files contain 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.

Endpoint Management uses the log4j syslog appender to send RFC5424 formatted syslog messages. The message data in syslog message is plain text does not have any specific format.

**Connectivity checks**

July 26, 2019

From the Endpoint Management Troubleshooting and Support page, you can check the Endpoint Management connection to Citrix Gateway and to other servers and locations.
Run Endpoint Management connectivity checks

1. In the 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 **Endpoint Management Connectivity Checks**. The **Endpoint Management Connectivity Checks** page appears. If your Endpoint Management environment contains clustered nodes, all nodes are shown.

3. Select the servers you want to include in the connectivity test and then click **Test Connectivity**. The test results page appears.

4. Select a server in the test results table to see detailed results for that server.
Conducting Citrix Gateway Connectivity Checks

1. On the Troubleshooting and Support page, under Diagnostics, click Citrix Gateway Connectivity Checks. The Citrix Gateway Connectivity Checks page appears. The table is empty if there is no connection between Endpoint Management and Citrix Gateway.

2. Click Add. The Add Citrix Gateway Server dialog box appears.
3. In **Citrix Gateway Management IP**, type the management IP address for the server running Citrix Gateway that you want to test.

   If you’re conducting a connectivity check for a Citrix Gateway server that has already been added before, the IP address is provided.

4. Type your administrator credentials for this Citrix Gateway.

   If you’re conducting a connectivity check for a Citrix Gateway server that has already been added before, the user name is provided.

5. Click **Add**. The Citrix Gateway is added to the table on the **Citrix Gateway Connectivity Checks** page.

6. Select the Citrix 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.
You can enable Endpoint Management to use the Mobile Service Provider interface to query BlackBerry and Exchange ActiveSync devices and issue operations.

For example, your organization may have 1,000 users and each user may use one or more devices. After you communicate to every user that he or she must enroll their devices with Endpoint Management for management, the Endpoint Management console indicates the number of devices that users enroll. By configuring this setting, you can determine how many devices connect to Exchange Server. In this way, you can do the following:

- Determine if any users still need to enroll their devices.
- Issue commands to user devices that connect to Exchange Server, such as data wipes.

1. In the 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**.
Reports

November 21, 2019

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 charts 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 have not had any activity for the number of days specified by the 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 Apps**: Failed Deployment - Lists up to 10 apps that have failed to deploy.
- **Blacklisted Apps by Device & User**: Lists blacklisted apps that users have on their devices.

You can export the data in each table in .csv format, which you can open by using programs like Microsoft Excel. You can export the chart for each report in PDF format.

**To generate a report**

1. In the Endpoint Management console, click **Analyze > Reporting**. The **Reporting** page appears.
2. Click the report you want to generate.
To view more details of a report

1. Click areas of the chart to drill down and see more details information.
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.
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.
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 CSV.

Endpoint Management Analyzer

November 21, 2019

Endpoint Management Analyzer is a cloud-based tool that you can use to check the authentication and enrollment setup for Citrix Endpoint Management.

Configure the tool to point to your Endpoint Management server and provide information, such as server deployment type, mobile platform, authentication type, and user credentials. The tool then connects to the server and scans your environment for configuration issues. If Endpoint Management Analyzer discovers issues, the tool provides recommendations to correct the issues.
Key features

• Secure, cloud-based micro-service to troubleshoot issues related to Endpoint Management.
• Recommendations to resolve Endpoint Management configuration issues.
• Reduced support calls and accelerated troubleshooting of Endpoint Management environments.
• Zero-day support for Endpoint Management releases.
• Health check scheduling on a daily or weekly cadence.
• Citrix ADC configuration checks. The Citrix ADC Configuration Report displays a badge notification indicating the number of recommendations.
• Secure Mail autodiscovery service checks.

Prerequisites

<table>
<thead>
<tr>
<th>Product</th>
<th>Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix ADC</td>
<td>10.5 and later</td>
</tr>
<tr>
<td>Client Enrollment Simulation</td>
<td>iOS and Android</td>
</tr>
</tbody>
</table>

Accessing Endpoint Management Analyzer

Use one of the following methods to access Endpoint Management Analyzer:

• In the Endpoint Management console, click the wrench icon in the upper-right corner to open the Troubleshooting and Support page.

• Use your My Citrix credentials to access the tool from https://xmanalyzer.xm.citrix.com/. On the Endpoint Management Analyzer Checks page, click Endpoint Management Environment.
Endpoint Management Analyzer contains the following options:

- **Environment Check**: This option guides you in setting up tests to check your setup. The option provides recommendations and solutions on device, user enrollment, and authentication issues.

- **Gateway Configuration Check**: This option guides you in checking your Citrix ADC configurations for Endpoint Management deployment readiness.

- **Server Connectivity**: This option instructs you to test the connectivity of your servers.

- **Citrix Insight Services**: This option opens Citrix Insight Services to find further issues that the environment check might have missed.

- **Contact Citrix support**: If you are still having issues, you can create a Citrix support case.

The following sections describe each option in more detail.
Performing an environment check

1. Log on to Endpoint Management Analyzer and then click **Endpoint Management Environment**.
2. Click **Add Test Environment**.
3. In the new **Add Test Environment** dialog box, do the following:

   a) Provide a unique name for the test that will help identify the test in the future.
   b) In **FQDN, UPN login, Email or URL Invitation URL**, enter the information that is used to access the server.
   c) In **Instance Name**, if you use a custom instance, provide that value.
   d) In **Choose Platform**, select either **iOS** or **Android** as the platform for testing.
   e) Expand **Advanced Deployment Options** and then in the **Deployment Mode** list, select your deployment mode. The options are:
4. Click **Continue**.

5. On the **Test Options** tab, choose one or more of the following tests and then click **Continue**.

   - **Secure Web Connectivity**: Provide an intranet URL. The tool tests for the reachability of the URL. This test detects if there are any connectivity issues that may potentially occur in Secure Web while trying to reach intranet URLs.

   - **Secure Mail ADS**: Provide a user email ID. Endpoint Management Analyzer uses this ID to test autodiscovery of the Exchange Server in your environment.

   - **ShareFile SSO**: Endpoint Management Analyzer tests if the ShareFile DNS resolution happens successfully. The tool also checks if ShareFile single sign-on (SSO) is compatible with the provided user credentials.

6. On the **User Credentials** tab, depending on your server setup, different Secure Hub user creden-
7. Click **Save & Run** to start the tests.

A progress notification appears. You can leave the progress dialog box open or close the dialog box and the tests continue to run.

Tests that pass appear in green. Tests that fail appear as red.

8. Click the **View Report** icon to see test results.

   - To rerun the same test, click **Run Again**.
   - To download the report, click **Download Report**.
   - To select another Endpoint Management Analyzer option, click **Go To Endpoint Management Analyzer Checks**.
   - To return to the list of tests on the **Environment Lists** page, in the upper-left of the page, click **Environment Check**.

9. On the **Environment List** page, you can copy and edit tests. To do so, select a test, click **More** and then select **Duplicate and Edit**.

A copy of the selected test is created and the **Add Test Environment** dialog box opens, allowing you to modify the new test.
Adding a schedule to environment checks

You can configure tests to run on an automatic schedule with results sent to a list of users you configure.

1. To add a schedule, do one of the following:
   a) On the Environment List page, select the environment for which you want to set up a schedule and then click Add Schedule.
   b) In a test result, click Add Schedule.

2. The Add Schedule window displays a message warning you that Endpoint Management Analyzer saves credentials for running tests on a schedule. Citrix recommends that you use an account with limited access for running scheduled tests. Click I Agree to continue.

3. Enter a Username and Password for running the test.

4. Configure a schedule for the test to run.
a) Select **Daily** or **Weekly**.

b) Select a time of day for the test to run and a time zone.

c) Use the date picker to select a date for the scheduled test to stop running or leave it blank for the test to run indefinitely.

d) Enter a list of email addresses to receive reports, separated by commas.

e) Click **Save**.

5. A clock symbol to the left of your test indicates that a schedule is configured. If you select your test, click **Edit Schedule** to change when the test runs.

![Edit Schedule](image)

- You can change when the test runs.
- You can disable the test, by clicking the switch at the top from **ON** to **OFF**.

**Performing a Citrix ADC check**

1. Log on to Citrix Endpoint Analyzer and then click **Gateway Configuration**. The **Gateway Configuration Check** page appears.
2. Upload the latest ns.conf file from your instance of Citrix Gateway. You can either drag the file into the upload box or click Browse to search and add the ns.conf file. For more information on how you can download the latest ns.conf file, see the Support Knowledge Center.

Note:
Endpoint Management Analyzer does not save the ns.conf file. After the check is complete, you can view and download the report.

3. Click Run Check.

Endpoint Management Analyzer runs two types of configuration checks.

- Essential Checks looks for components that are critical for a successful Endpoint Management deployment.
- Advanced Checks looks for components that are not critical, but are complementary to Endpoint Management deployments.

When the check is complete, the following screen appears:


The Configuration Report page appears.
The notification badge within the Configuration Report indicates the number of recommendations in the Essential Configuration check for Gateway servers configured through the Citrix ADC wizard. The badge also indicates recommendations for user-configured Gateways.

**Note:**

Citrix Gateway Analyzer supports gateway servers configured through the Citrix ADC wizard. Citrix Gateway instances always have the following title convention: _XM_*name*-provided-by-user-when-deploying.

The overall status is a **Success** when the essential configuration checks have passed.

When an Essential Configuration check fails, the Recommendations table lists the **Policy Check**, **Details**, and **Results**.

When an Advanced Configuration check fails, the Recommendations table lists the **Policy**, **Details**, and **Results**. To view the full report details, click **Essential Configuration Checks** and **Advanced Configuration Checks** (or click the expand icon).

On the Configuration Report page, the following options are also available.

- To run another Gateway configuration check, click **Run another test**.
- To download a report of the results, click **Download report and ns.conf file bundle**.
- To view other troubleshooting and analyzing tools, click **Go to Citrix Endpoint Analyzer Checks**.
- To email the report and the ns.conf bundle, next to **Email report and ns.conf bundle**, type one or more email addresses, separated by commas. Click **Send**.

**Known issues**

The following issues are known in the Endpoint Management Analyzer:

- When performing the Secure Web Connectivity checks, typing multiple URLs in the text box is not supported.
The shared devices authentication feature of Secure Hub is not supported.
Secure Web tests only check the connectivity to the URLs entered and not the authentication to the corresponding sites.

REST APIs

August 26, 2019

With the Endpoint Management REST API, you can call services that are exposed through the Endpoint Management console. You can call REST services by using any REST client. The API does not require you to sign on to the Endpoint Management console to call the services.

For the complete current set of available APIs, download the Public API for REST Services PDF.

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 invoke REST API services

You can invoke 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

URL: https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login
Request: { "login":"administrator", "password":"password"}
Method type: POST
Content type: application/json
ActiveSync Gateway

August 26, 2019

ActiveSync is a mobile data synchronization protocol developed by Microsoft. ActiveSync synchronizes data with handheld devices and desktop (or laptop) computers.

You can configure ActiveSync Gateway rules in Endpoint Management. Based on these rules, you can allow or deny devices access to ActiveSync data. For example, if you activate the rule Missing Required Apps, Endpoint Management checks the App Access Policy for required apps and denies access to ActiveSync data if the required apps are missing. For each rule, you can choose either Allow or Deny. The default setting is Allow.

Related information

- Endpoint Management REST API
Citrix Endpoint Management

For more information about the App Access device policy, see App access device policy.

Endpoint Management supports the following rules:

**Anonymous Devices:** Checks if a device is in anonymous mode. This check is available if Endpoint Management can’t re-authenticate the user when a device attempts to reconnect.

**Failed Samsung Knox attestation:** Checks if a device failed a query of the Samsung Knox attestation server.

**Forbidden Apps:** Checks if a device has forbidden apps, as defined in an App Access policy.

**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 and allows or denies connections based on that list. If no rule matches, the default is 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 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, 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 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. That property is usually changed by the automated actions or by a 3rd party leveraging Endpoint Management APIs.

**Revoked Status:** Checks whether the device certificate was 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 a device is still in a managed state, under Endpoint Management control. For example, a device running in MAM mode or an un-enrolled device is not managed.

**Send Android domain users to ActiveSync Gateway:** Click YES to ensure that Endpoint Management sends Android device information to the ActiveSync Gateway.

**To configure the ActiveSync Gateway settings**

1. In the 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.

   ![ActiveSync Gateway Settings]

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 ensure that Endpoint Management sends Android device information to the ActiveSync Gateway.

3. Click **Save**.

**Endpoint Management connector for Exchange ActiveSync**

November 21, 2019

XenMobile Mail Manager is now Endpoint Management connector for Exchange ActiveSync. For details about the Citrix unified portfolio, see the [Citrix product guide](https://www.citrix.com).

The connector extends the capabilities of Endpoint Management in the following ways:
• Dynamic Access Control for Exchange Active Sync (EAS) devices. EAS devices can be automatically allowed or blocked access to Exchange services.
• The ability for Endpoint Management to access EAS device partnership information provided by Exchange.
• The ability for Endpoint Management to perform an EAS Wipe on a mobile device.
• The ability for Endpoint Management to access information about Blackberry devices, and to perform control operations such as Wipe and ResetPassword.

Deprecation of TLS versions

To improve the security of the Citrix Endpoint Management service, Citrix will block any communication over Transport Layer Security (TLS) 1.0 and 1.1, as of March 15, 2019. As a result of its weakening security, TLS 1.0 is being deprecated by the PCI Council and will no longer be supported.

How this impacts you

Older versions of Endpoint Management connector for Exchange ActiveSync support TLS 1.0 only. If you use Endpoint Management connector for Exchange ActiveSync build 10.1.3 or earlier, upgrade to build 10.1.4 or later.

To download the connector, go to the Server Components section under Endpoint Management Server on Citrix.com.

If you use an on-premises Citrix Gateway (formerly, NetScaler Gateway), enable TLS 1.2 on your load balancer service. For information, see https://support.citrix.com/article/CTX247095. Following is a video that shows how to enable TLS 1.2 on Citrix Gateway.

What's new in version 10.1.10

The following issues are fixed in version 10.1.10:

• Customers who experience frequent network issues may 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]

- 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 new connection. [XMHELP-2184, CXM-70836]
- When a configuration change is saved, it is 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 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 new settings. This issue corrects a known issue in version 10.1.8. [CXM-47709, CXM-61330]

- During an upgrade, the existing database configuration was not 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. As of this version, the defaults section always reflects the latest configuration. [CXM-62681]

- Admins can no longer access certain options by pressing Shift when executing 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]
What’s new in earlier versions

The following section lists the new features and fixed issues in earlier versions of Endpoint Management connector for Exchange ActiveSync.

What’s new in version 10.1.8

- It is possible that Exchange will throttle back the Citrix Endpoint Management connector for Exchange ActiveSync service from issuing commands too frequently. This is common in connections to Office 365. The effect of throttling requires that the service pause for a specified period of time 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 are not 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 attempts to initiate a connection up to three times. [CXM-58180]

• To effect policies on Exchange, 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 is not 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. Consequently, a user may 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 ensures 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 performing 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 are not processed, or snapshots are not initiated. 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]

What's new in version 10.1.7

• XenMobile Mail Manager is now Endpoint Management connector for Exchange ActiveSync.
• We have 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 are not in sync with Exchange are detected, their commands may include devices that do not belong to the relevant mailbox. Endpoint Management connector
for Exchange ActiveSync now ensures that commands to Exchange represent only devices that belong to their respective mailboxes. [CXM-54842]

- In some environments, a Microsoft assembly is not available. The required assembly is now explicitly installed with the application. [CXM-55439]
- If Distinguished Names for devices or mailboxes have spaces between the attribute name and the equals, or spaces after the equals and before the value, Endpoint Management connector for Exchange ActiveSync may not properly match a device with its mailbox and vice versa. The result could be that some devices and/or mailboxes are rejected during the snapshot reconciliation. [CXM-56088]

**Note:**

The following What's New sections refer to Endpoint Management connector for Exchange ActiveSync by its former name of XenMobile Mail Manager. The name changed as of version 10.1.7.

**Update in version 10.1.6.20**

An update to 10.1.6 contains the following fix in version 10.1.6.20:

- When device policies that are not in sync with Exchange are detected, their commands may include devices that do not belong to the relevant mailbox. XenMobile Mail Manager now insures 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 contains 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, 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 could result in a truncated dataset. This issue may occur when XenMobile Mail Manager executes a multi-command pipelined script. The upstream command cannot 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 of time. 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 due to 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 a period of time (usually 15 minutes). XenMobile Mail Manager was not 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. Consequently, if permissions were restricted, the behavior could 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]

- Depending on the current workload, when directed to, the XenMobile Mail Manager service may not stop promptly. Therefore, 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 contains the following fixed issues:

- When Exchange is applying throttling to XenMobile Mail Manager activity, there is 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. Additionally, 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 is possible that an insufficient amount of time is allowed to elapsed before executing 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
Citrix Endpoint Management

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 XenMobile Mail Manager uses the identity to query for more data. [CXM-52635]

Known limitation

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 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 all of the policies for those devices of the mailbox to be set. The error reported, which will appear in the XenMobile Mail Manager logs, would look like the following. The example is for the blocked list.

“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 could exceed the limit. Although having that many devices associated with a specific mailbox is rare, it is a possibility. Until XenMobile 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 contains the following fixed issues:

- Due to its weakening security, TLS 1.0 is being deprecated by the PCI Council. Support for TLS 1.1 and 1.2 is added to 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 Exchange fails due to a bad specification: The error message is overridden by an incorrect 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]
- In some cases, 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 XenMobile Mail Manager so we can focus on where we can make the product better.

- **Setting for enabling diagnostics:** An **Enable Diagnostic** check box appears in the Configure console on the **Configuration** dialog box.

![Configuration Dialogue Box](image)

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, XenMobile Mail Manager cannot write to the Commands diagnostics file. When this occurs, the command history is not 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 could be thrown in the Check Health routine. As a result, connections that have experienced an error or have expired might not be purged. Also, 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 is not an accurate message. Instead, the message should indicate that the two sessions that XenMobile Mail Manager normally uses for Exchange communication are in use. [CXM-49994]

**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, 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, 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 cannot 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 XenMobile Mail Manager to restart automatically to provide a clean slate to the system.
• **Microsoft .NET Framework 4.6 prerequisite:** The prerequisite for Microsoft .NET Framework
Citrix Endpoint Management 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 XenMobile Mail Manager deems are not 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 are not recognized. (XMHELP-489)
- Memory management: Better memory management and mitigation. (XMHELP-419)

**Architecture**

The following diagram shows the main components of Endpoint Management connector for Exchange ActiveSync. For a detailed reference architecture diagram, see [Architecture](#).

The three main components are:

- **Exchange ActiveSync Access Control Management:** Communicates with Endpoint Management to retrieve an Exchange ActiveSync policy from 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.
- **Mobile Service Provider**: Provides a web service interface so that Endpoint Management can query Exchange ActiveSync, query Blackberry devices, and issue control operations such as Wipe against ActiveSync and Blackberry devices.

**System requirements and prerequisites**

The following minimum system requirements are required to use Endpoint Management connector for Exchange ActiveSync:

- Blackberry Enterprise Service, version 5 (optional).

Minimum supported versions of Microsoft Exchange Server:

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 Service Pack 3 (support ends January 14, 2020)

**Prerequisites**

- Windows Management Framework must be installed.
  - PowerShell V5, V4, and V3
- 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 are supported. These email clients have been tested by Citrix and performed without errors:

- HTC native email client
- Samsung native email client
- iOS native email client

Exchange: The requirements for 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 execute the following Exchange-specific PowerShell cmdlets.

- For Exchange Server 2010 SP2:
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - 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.

Per the Microsoft TechNet article, about_Remote_Requirements, 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 this blog post, You Don’t Have to Be An Administrator to Run Remote PowerShell Commands.

- 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 is not 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.

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 execute 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, 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 is not 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 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:
   - **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**.

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 perform all the Exchange ActiveSync Access Control functions of the connector for Exchange ActiveSync. Deep snapshots may take longer and are only needed if the Mobile Service Provider is enabled for ActiveSync. This option allows Endpoint Management to query for unmanaged devices.

- Select the Default Access: **Allow**, **Block**, or **Unchanged**. This setting controls how all devices other than those devices identified by explicit 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 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**.
10. On the **Endpoint Management server Service Properties** page, modify the URL string to point to the 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 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** check box is selected, the Endpoint Management Mail Service doesn’t collect policies from Endpoint Management.

11. Click the **Local Rules** tab.

- 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. Therefore, if you are 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 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 perform 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.

13. To configure the Mobile Service Provider, click the **Configure > MSP** tab.

   The Mobile Service Provider is optional. That setting is necessary only if Endpoint Management is also configured to use the Mobile Service Provider interface to query unmanaged devices.

   - Set the Service Transport type as **HTTP** or **HTTPS** for the Mobile Service Provider service.
   - Set the **Service port** (typically 80 or 443) for the Mobile Service Provider service. If you use port 443, the port requires an SSL certificate bound to it in IIS.
   - Set the **Authorization Group** or **User**. This sets the user or set of users who will be able to connect to the Mobile Service Provider service from Endpoint Management.
   - Set whether ActiveSync queries are enabled or not. If ActiveSync queries are enabled for the Endpoint Management server, the Snapshot type for one or more Exchange Servers must be set to **Deep**. That setting might have significant performance costs for taking snapshots.
   - By default, ActiveSync devices that match the regular expression WorxMail* will not be sent to Endpoint Management. To change this behavior, alter the **Filter ActiveSync** field as necessary. Blank means that all devices are forwarded to Endpoint Management.
   - Click **Save**.

14. Optionally, configure one or more instances of BlackBerry Enterprise Server (BES): Click **Add** and then enter the server name of the BES SQL Server.
• 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 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 therefore does not accurately test SQL authentication.

• To support remote Wipe and ResetPassword of BlackBerry devices from Endpoint Management, select the **Enabled** check box.
• 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 are not approved for corporate email use. To comply with this policy, you want to ensure that employees cannot access corporate email from such devices. Endpoint Management connector for Exchange ActiveSync and Endpoint Management work together to enforce such an email policy. Endpoint Management sets the policy for corporate email access. When an unapproved device enrolls with 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. Secure Hub obtains a similar identifier and sends the identifier to 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:
If Endpoint Management sends the connector for Exchange ActiveSync an ActiveSync ID that is different from the ID the device publishes to Exchange, the connector cannot 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 the Samsung SAFE platform, push the device ActiveSync configuration from Endpoint Management.
- On all other Android platforms, push both the TouchDown app and the TouchDown ActiveSync configuration from Endpoint Management.

Note:
DigiCert stopped supporting Android TouchDown on July 2, 2018. Citrix recommends that you use Citrix Secure Mail.

This does not, however, prevent an employee from installing an email client other than TouchDown on an Android device. To guarantee that your corporate email access policy is enforced properly, you can adopt a defensive security stance and configure Endpoint Management connector for Exchange ActiveSync to block emails by setting the static policy to Deny by default. This means that if an employee does configure an email client on an Android device other than TouchDown, and if ActiveSync ID detection does not work properly, the employee is denied corporate email access.

Access control rules

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 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.

Endpoint Management connector for Exchange ActiveSync has three types of rules: local rules, 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 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 upon 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 should be able to add either a normal or regular expression rule. If a major snapshot has not completed, you can only add regular expression rules.

**Endpoint Management server rules**: Endpoint Management server rules are references to an external Endpoint Management server that provides rules about managed devices. The 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 Endpoint Management, such as whether the device is jailbroken or whether the device contains forbidden apps. Endpoint Management evaluates the high-level rules and produces a set of allowed or blocked ActiveSync Device IDs, which are then delivered to 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 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 is not matched by either a local or Endpoint Management server rule will be allowed.
- **Default Access – Block**: Any device that is not matched by either a local or Endpoint Management server rule will be blocked.
- **Default Access - Unchanged**: Any device that is not matched by either a local or 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
- 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 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 encountered, 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. For details, see this Microsoft article.

Analyzing is particularly useful in situations in which multiple rules for the same field have been defined. You can troubleshoot the relationships between rules. You perform 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, and so on.

Rule terminology

- **Overriding rule:** An override occurs when more than a single rule could apply to the same device. Because rules are evaluated by priority in the list, the later rule instance(s) which might apply might never be evaluated.
- **Conflicting rule:** A conflict occurs when more than a single rule could apply to the same device but the access (Allow/Block) does not match. If the conflicting rules are not 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 hence there might be a need to ensure that the two (or more) regular expressions can either be combined into a single regular expression rule, or are not 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
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 one to many ancillary rules. When clicking on 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 will conflict in its access with the primary rule, or the ancillary rule will supplement 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 check box which, when selected, displays only those rules which are conflicts, overrides, redundancies, or supplements.

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. Any time an overridden rule has been highlighted either as a result 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:

In this example, the regular expression rule `WorkMail.*` is the primary rule (indicated by the solid border) and the normal rule `workmailc63313818` 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) due to 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. Prior to clicking either of the rules in a simple example, 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 contains “App” and that the second rule denies all devices with a device ID that contains `Appl`. In addition, even though the second rule denies all devices with a device ID that contains `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:

![Rule Analysis]

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 have applied more than a single regular expression rule to a single matchable field, which could 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 have applied more than a single regular expression rule to a single matchable field, which could mean a redundancy issue or something more serious.

![Rule Analysis]

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 supplement one another will only involve regular expression rules. When rules supplement one another, they are indicated with a yellow overlay. Prior to 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 Endpoint Management connector for Exchange ActiveSync. After clicking the first rule, the dialog box looks as follows:
Citrix Endpoint Management

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.

**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. A number of regular expression rules are included in the list as well, as indicated by the icon.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
How to analyze an override

To see which rule or rules have overridden a particular rule, you click the rule.

**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 rule or 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:
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` contains the user `zentrain01@zenprise.com`, and the Active Directory Group rule `ZenTraining B` also contains 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:
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:
- 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 \texttt{SAM.*} and the regular expression ActiveSync device type rule \texttt{Andro.*}.
- Both of the ancillary rules are bordered with dashes to indicate that they are ancillary.
- Both of the ancillary rules are overlaid with yellow to indicate that they are also applied to the rule field of ActiveSync device type.
- You should ensure in such scenarios that their regular expression rules are not 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 \texttt{touch.*}. Clicking the ancillary rule \texttt{Andro.*} shows a different set of ancillary rules highlighted.
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 prior to being clicked. In the preceding example, the normal ActiveSync device type rule `Android`, was not displayed as an ancillary rule because, from the perspective of the then primary rule (the regular expression `ActiveSync device type rule touch.*`), it was not related to it.

**To configure a normal expression local rule**

1. Click the **Access Rules** tab.
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 below in the list box.
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 SamsungSPhI720 are denied access.
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.
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 below in the list box.
4. Click one of the items in the results list. In this example, SAMSUNGSPHL720 has been selected and appears in the text box adjacent to **Device Type**.
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 SAMSUNGPHL720 to SAMSUNG.*.
   c. Ensure that the regular expression check box is selected.
   d. Click Allow.

To build an access rule

1. Click the **Local Rules** tab.
2. To enter the regular expression, you need to make use of both the Device ID list and the selected item text box.
3. Select the field 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 check box is selected and then click Allow or Deny. In this example, the choice is Allow. The final result is as follows:
To find devices

By selecting the regular expression check box, 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. Ensure that the device match field selector is set to Device ID (the default).
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 check box is selected and then click the magnifying glass icon to display matches as shown in the following figure.
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.
Device monitoring

The Monitor tab in 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.
- Under the MSP tab, click the Info icon for the desired BlackBerry Server.
Troubleshooting and diagnostics

XEndpoint 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

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, whereas the Trace level provides the most detail.

To change the logging level, do the following:

1. In C:\Program Files\Citrix\Citrix Endpoint Management connector, open the nlog.config file.
2. In the <rules> section, change the minlevel parameter to the logging level you prefer. For example:

   ```xml
   <rules>
   <logger name="*" writeTo="file" minlevel="Debug" />
   </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 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 Exchange ActiveSync service cannot access the SQL Server. This may be caused by these issues:
    - The SQL Server service is not running.
Authentication failure.

If Windows Integrated authentication is configured, the user account of the connector for Exchange ActiveSync service must be an allowed SQL logon. The account of the connector for 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.

- The port configured for the Mobile Service Provider (MSP) is not available. A listening port must be selected that is not used by another process on the system.

Endpoint Management cannot connect to the MSP

Check that the MSP service port and transport is properly configured in the **Configure > MSP** tab of the connector for Exchange ActiveSync console. Check that the Authorization Group or User is set properly.

If HTTPS is configured, a valid SSL server certificate must be installed. If IIS is installed, IIS Manager can be used to install the certificate. If IIS is not installed, see [https://msdn.microsoft.com/en-us/library/ms733791.aspx](https://msdn.microsoft.com/en-us/library/ms733791.aspx) for details on installing certificates.

The connector for Exchange ActiveSync contains a utility program to test connectivity to the MSP service. Run the **InstallFolder\MspTestServiceClient.exe** program and set the URL and credentials to a URL and credentials that will be configured in the Endpoint Management and then click **Test Connectivity**. This simulates the web service requests that Endpoint Management issues. If HTTPS is configured, you must specify the actual host name of the server (the name specified in the SSL certificate).

When using **Test Connectivity**, be sure to have at least one ActiveSyncDevice record or the test may fail.
Troubleshooting tools

A set of PowerShell utilities for troubleshooting is available in the Support\PowerShell folder.

A troubleshooting tool performs 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 raw output of all cmdlets to a text file.

Citrix Gateway connector for Exchange ActiveSync

November 21, 2019

XenMobile NetScaler Connector is now Citrix Gateway connector for Exchange ActiveSync. For more detail 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 acting as a reverse proxy for the Exchange ActiveSync protocol. Authorization is controlled by a combination of policies that you define within Endpoint Management and by rules defined locally by Citrix Gateway connector for Exchange ActiveSync.

For more information, see ActiveSync Gateway.
For a detailed reference architecture diagram, see Architecture.

The current release of Citrix Gateway connector for Exchange ActiveSync is version 8.5.3.

**Deprecation of TLS versions**

To improve the security of the Citrix Endpoint Management service, Citrix will block any communication over Transport Layer Security (TLS) 1.0 and 1.1, starting in March 2019. As a result of its weakening security, TLS 1.0 is being deprecated by the PCI Council and will no longer be supported.

**How this impacts you**

Older versions of Citrix Gateway connector for Exchange ActiveSync support TLS 1.0 only. If you use Citrix Gateway connector for Exchange ActiveSync build 8.5.0 or lower, upgrade to build 8.5.1.11 or higher.

To download the connector, go to the Server Components section under Endpoint Management Server on Citrix.com.

If you use an on-premises Citrix Gateway (NetScaler Gateway), enable TLS 1.2 on your load balancer service. For information, see https://support.citrix.com/article/CTX247095. Following is a video that shows how to enable TLS 1.2 on Citrix Gateway.

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 Citrix Gateway connector for Exchange ActiveSync by its former name of XenMobile NetScaler Connector. The name changed as of version 8.5.2.
What’s new in version 8.5.2

- XenMobile NetScaler Connector is now Citrix Gateway connector for Exchange ActiveSync.

The following issues are fixed in this release:

- If more than one criteria is used in defining a policy rule and if one of the criteria involves the user ID, the following issue may occur: If a user has more aliases, the aliases are not 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 XenMobile NetScaler 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, TLS 1.0 is being deprecated by the PCI Council. Support for TLS 1.1 and 1.2 is added to XenMobile NetScaler Connector.

Monitoring Citrix Gateway connector for Exchange ActiveSync

The Citrix Gateway connector for Exchange ActiveSync configuration utility provides detailed logging that you can use to view all traffic passing through your Exchange Server that is either allowed or blocked by Secure Mobile Gateway.

Use the **Log** tab to view the history of the ActiveSync requests forwarded to the connector for Exchange ActiveSync for authorization.

Also, to ensure that the connector for 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 Citrix Gateway connector for Exchange ActiveSync to simulate what ActiveSync traffic will look like in conjunction with your policies. In the connector configuration utility, click the **Simulator** tab. The results show you how your policies will apply according to the rules you have configured.
Choosing filters for the connector for Exchange ActiveSync

The Citrix 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 Endpoint Management. The two options for each filter are **Allow** or **Deny**.

- **Anonymous Devices**: Allows or denies devices that are enrolled in Endpoint Management but the user’s identity is unknown. For example, this could be a user who was enrolled, but the user’s Active Directory password is expired, or a user who enrolled with unknown credentials.
- **Failed Samsung Knox attestation**: Samsung devices have functionality for security and diagnostics. This filter provides confirmation that the device is setup for Knox. For details, see the Endpoint Management article on Samsung Knox.
- **Forbidden Apps**: Allows or denies devices based on the Device List defined by blacklist policies and the presence of blacklisted apps.
- **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 ensures 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 of the other connector filters that have not been selected. For example, Blacklists Apps will be denied (blocked) by the connector, whereas all other filters will be allowed because the Implicit Allow/Deny option is set to **Allow**.
- **Inactive devices**: Creates a Device List of devices that have not communicated with Endpoint Management within a specified period of 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 they should install. The non-suggested apps filter checks the device for apps that are not 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 if the device does or does not meet 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 Endpoint Management database. The Mobile Application Gateway needs to be deployed in a Block Mode.

To configure a connection to Citrix Gateway connector for Exchange ActiveSync

Citrix Gateway connector for Exchange ActiveSync communicates with Endpoint Management and other remote configuration providers through secure web services.

1. In the connector for 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 Endpoint Management server.
3. In **Url**, enter the web address of the Endpoint Management GCS, typically in the format `https://<FQDN>/<instanceName>/services/<MagConfigService>`. The `MagConfigService` name is case-sensitive.
4. In **Password**, enter the password that will be used for basic HTTP authorization with the Endpoint Management server.
5. In **Managing Host**, enter the connector for Exchange ActiveSync server name.
6. In **Baseline Interval**, specify a time period for when a new refreshed dynamic ruleset is pulled from Device Manager.
7. In **Delta interval**, specify a time period for when an update of dynamic rules is pulled.
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 Endpoint Management when a device is blocked. This option is required if you are using the connector rules in any of your 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** check box and then click **Save**.

When you add a new configuration provider, the connector for Exchange ActiveSync automatically creates one or more policies associated with the provider. These policies are defined by a template.
definition contained in config\policyTemplates.xml in the NewPolicyTemplate section. For each Policy element defined within this section, a new policy is created.

The operator may 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) are not modified. Next, add new groups for the provider and update the policy to include the new groups.

**To import a policy from Endpoint Management**

1. In the connector for 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 will be used for basic HTTP authorization with the Endpoint Management server and that has administrative privileges.

3. In **Url**, enter the web address of the 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 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 administrator.

6. When a connection is successfully made, clear the **Disabled** check box 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 Endpoint Management when multiple Forefront Threat Management Gateway (TMG) servers are configured in an array.

After you save the settings, open the GCS.

**Configuring Citrix Gateway connector for Exchange ActiveSync policy mode**

Citrix 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 executes static rules with an implicit deny or block statement at the end. The connector for Exchange ActiveSync blocks devices that are not allowed or permitted via other filter rules.
• **Static Rules: Permit Mode:** This policy mode executes static rules with an implicit permit or allow statement at the end. Devices that are not blocked or denied via other filter rules are allowed through the connector for Exchange ActiveSync.

• **Static + ZDM Rules:** Block Mode. This policy mode executes static rules first, followed by dynamic rules from Endpoint Management with an implicit deny or block statement at the end. Devices are permitted or denied based on defined filters and Device Manager rules. Any devices that do not match on defined filters and rules are blocked.

• **Static + ZDM Rules:** Permit Mode. This policy mode executes static rules first, followed by dynamic rules from Endpoint Management with an implicit permit or allow statement at the end. Devices are permitted or denied based on defined filters and Endpoint Management rules. Any devices that do not match on defined filters and rules are allowed.

The connector for Exchange ActiveSync process permits or blocks for dynamic rules based on unique ActiveSync IDs for iOS and Windows-based mobile devices received from Endpoint Management. Android devices differ in their behavior based on the manufacturer and some do not readily expose a unique ActiveSync ID. To compensate, 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 cannot be differentiated. You can configure the gateway to statically block these devices by ActiveSyncID, if they are known. You can also configure the gateway to block based on device type or user agent.

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 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 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 rules, click the **Simulator** tab. Specify values in the fields. These can also be obtained from the logs. A result message will appear specifying 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. This is commonly found as domain\username as referenced by the server running Endpoint Management connected to Active Directory via LDAP. The Log tab within the connector configuration utility shows the values that are passed through the connector. The values are passed if the value structure needs to be determined or is different.

• **Deviceid (ActiveSyncID):** Also known as the ActiveSyncID of the connected device. This value is commonly found within the specific device properties page in the Endpoint Management console. This value can also be screened from the Log tab in the connector for 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. In most cases, the value specified corresponds to a specific operating system build and version for the mobile device platform.

The connector for 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**.

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** check box.

3. Click **Save**.

   The static rule is now in effect. Additionally, 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 Endpoint Management define dynamic rules and can trigger a dynamic connector for 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:
You must use the Endpoint Management console to configure dynamic rules.

1. In the 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 ensure that Endpoint Management sends Android device information to the Secure Mobile Gateway.

When this option is enabled, Endpoint Management sends Android device information to the connector for Exchange ActiveSync when Endpoint Management does not have the ActiveSync identifier for the Android device user.

To configure custom policies by editing the connector for Exchange ActiveSync XML file

You can view the basic policies in the default configuration on the Policies tab of the connector for Exchange ActiveSync configuration utility. If you want to create custom policies, you can edit the Citrix Gateway connector for Exchange ActiveSync XML configuration file (config\config.xml).

1. Find the PolicyList section in the file and then add a new Policy element.
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.
Citrix Endpoint Management

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 specifies 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 will “pass.” 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**

Additionally, 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.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>In this release, only external XML files are supported.</td>
</tr>
</tbody>
</table>

The default installation implements two XML file in the configuration: allow.xml and deny.xml.

**Configuring Citrix Gateway connector for Exchange ActiveSync**

You can configure Citrix 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 may 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. Endpoint Management can export groups of allowed and blocked devices and users to the connector for Exchange ActiveSync.

Dynamic groups are maintained by an external source called a Gateway Configuration Provider and collected by the connector for Exchange ActiveSync on a periodic basis. 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 may 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 are not 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 Citrix 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 is not always ideal. Every organization that manages IT security may 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 due to the multitude of mobile devices and types, mobile devices per user, and available operating system platforms and apps. In most organizations, the restrictive model will be the most logical choice.

The configuration scenarios that Citrix allows for integrating the connector for Exchange ActiveSync with 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. 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 Citrix Gateway connector for Exchange ActiveSync**

You can use Citrix 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 blacklists or whitelists, and other compliance conditions.
Citrix Endpoint Management

By using the connector for Exchange ActiveSync configuration utility, you can build dynamic and static rules that enforce corporate email policies, allowing 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 and only viewable on managed devices by authorized users.

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 Endpoint Management configuration service and the notification service.

Installing Citrix 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 Endpoint Management.

You can consider installing the connector for Exchange ActiveSync on its own server (separate from Endpoint Management) for the following reasons:

- If your Endpoint Management server is hosted remotely in the cloud (physical location).
- If you do not want the connector for Exchange ActiveSync to be affected by restarts of the Endpoint Management server (availability).
- If you want a server’s system resources to be devoted 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 Endpoint Management. For large numbers of devices (more than 50,000), you may need to provision more cores if you do not have a clustered environment. The memory footprint of the connector is not significant enough to warrant more memory.
Citrix Gateway connector for Exchange ActiveSync system requirements

Citrix Gateway connector for Exchange ActiveSync communicates with NetScaler over an SSL bridge configured on the NetScaler appliance. The bridge enables the appliance to bridge all secure traffic directly to Endpoint Management. The connector for Exchange ActiveSync the following minimum system configuration:

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer and processor</td>
<td>733 MHz Pentium III 733 MHz or higher processor. 2.0 GHz Pentium III or higher processor (recommended)</td>
</tr>
<tr>
<td>NetScaler</td>
<td>NetScaler appliance with software version 10</td>
</tr>
<tr>
<td>Memory</td>
<td>1 GB</td>
</tr>
<tr>
<td>Hard disk</td>
<td>NTFS-formatted local partition with 150 MB of available hard-disk space</td>
</tr>
<tr>
<td>Other devices</td>
<td>Network adapter compatible with the host operating system for communication with the internal network</td>
</tr>
<tr>
<td>Microsoft .NET Framework</td>
<td>Version 8.5.1.11 requires Microsoft .NET Framework 4.5.</td>
</tr>
<tr>
<td>Display</td>
<td>VGA or higher-resolution monitor</td>
</tr>
</tbody>
</table>

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 are supported. Citrix has tested these email clients and the clients have performed without errors:

- HTC native email client
- Samsung native email client
- iOS native email client

Deploying Citrix Gateway connector for Exchange ActiveSync

Citrix Gateway connector for Exchange ActiveSync enables you to use NetScaler to proxy and load balance Endpoint Management server communication with Endpoint Management managed devices. The connector for Exchange ActiveSync communicates periodically with Endpoint Management to synchronize policies. The connector for Exchange ActiveSync and Endpoint Management can be clustered, together or independently, and can be load-balanced by NetScaler.

The connector for Exchange ActiveSync components

- **The connector for Exchange ActiveSync service**: This service provides a REST web service interface that can be invoked by NetScaler to determine if an ActiveSync request from a device is authorized.
- **Endpoint Management configuration service**: This service communicates with Endpoint Management to synchronize Endpoint Management policy changes with the connector for Exchange ActiveSync.
- **Endpoint Management notification service**: This service sends notifications of unauthorized device access to Endpoint Management. In this way, 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 Citrix Gateway connector for Exchange ActiveSync

For Citrix Gateway connector for Exchange ActiveSync to receive requests from NetScaler to authorize ActiveSync traffic, do the following. Specify the port on which the connector for Exchange ActiveSync listens to NetScaler web service calls.

1. From the **Start** menu, select the connector for 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 Endpoint Management (installed on the same server), select port values that do not conflict with 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 Citrix 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 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 Endpoint Management policies, select **Static + ZDM: Permit Mode** or **Static + ZDM: Block Mode**. These policies combine local (or, static) rules with the rules from 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 Endpoint Management

Specify the name and properties of the Endpoint Management server (also known as a Config Provider) that you want to use with Citrix Gateway connector for Exchange ActiveSync and NetScaler.

**Note:**

This task assumes that you have already installed and configured Endpoint Management.

1. In the connector for Exchange ActiveSync configuration utility, click the **Config Providers** tab and then click **Add**.
2. Enter the name and URL of the Endpoint Management server you are using in this deployment. If you have multiple Endpoint Management servers deployed in a multitenant deployment, this name must be unique for each server instance. For example, for **Name**, you could type **CEM**.
3. In **Url**, enter the Web address of the 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 that will be used for basic HTTP authorization with the 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 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 Endpoint Management when a device is blocked. This option is required if you are using Secure Mobile Gateway rules in any of your Endpoint Management Automated Actions.

10. After configuring the server, click **Test Connectivity** to test the connection to Endpoint Management.

11. When connectivity has been established, click **Save**.

---

**Deploying Citrix Gateway connector for Exchange ActiveSync for redundancy and scalability**

If you want to scale your Citrix Gateway connector for Exchange ActiveSync and Endpoint Management deployment, you can install instances of the connector for Exchange ActiveSync on multiple Windows Servers, all pointing to the same Endpoint Management instance. Then you can use NetScaler to load balance the servers.

There are two modes for the connector for Exchange ActiveSync configuration:

- In non-shared mode, each connector for Exchange ActiveSync instance communicates with an Endpoint Management server and keeps its own private copy of the resulting policy. For example, if you had a cluster of Endpoint Management servers, you could run a connector instance on each Endpoint Management server and the connector would get policies from the local Endpoint Management instance.

- In shared mode, one connector for Exchange ActiveSync node is designated the primary node. The connector communicates with Endpoint Management. The resulting configuration is shared among the other nodes either by 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. But the system can tolerate the primary server being down for a few minutes (for example, to restart) because the last known good configuration is cached in the connector process.
Advanced concepts

August 21, 2018

The Endpoint Management Advanced Concepts articles offer a deeper dive into product information about Endpoint Management. The aim is to help reduce deployment time through expert techniques. The articles may cite the technical expert or experts who have authored the content.

For decision points, recommendations, common questions, and use cases for your end-to-end Endpoint Management environment, see Endpoint Management deployment in this section.

For community support forums on Endpoint Management, see Citrix Discussions.

Endpoint Management deployment

November 5, 2018

There’s a lot to consider when you’re planning an Endpoint Management deployment. What devices should you choose? How should you manage them? How do you ensure that your network remains secure while still providing a good user experience? What hardware do you need in place and how do you troubleshoot it? This handbook aims to help answer those questions and more. The articles in this section provide 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 Endpoint Management deployment.

The handbook has three main sections:

- **Assess**: Common use cases and questions to consider when planning your deployment.
- **Design & Configure**: Recommendations for designing and configuring your environment
- **Operate & Monitor**: Ensuring the smooth operation of your running environment.

Assess

As with any deployment, assessing your needs should be your first priority. What is your primary need for 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 Endpoint Management environment? Let’s look at common use cases and questions for you to consider when planning your deployment.

- **Management modes**
- **Device requirements**
Design & 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
- 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 Citrix Gateway and Citrix ADC
- SSO and proxy considerations for MDX apps
- Authentication
- Server properties
- Device and app policies
- User enrollment options

Operate & Monitor

After your Endpoint Management environment is up and running, you’ll want to monitor it to ensure smooth operation. The monitoring section discusses where you can find the various logs and messages Endpoint Management and its components generate, and how to read those logs. This section also includes various common troubleshooting steps you can follow to reduce customer support feedback time.

- App provisioning and deprovisioning
- Dashboard-based operations
- Role-based Access Control and Endpoint Management support
- Systems monitoring
- Citrix support process
Management modes

May 10, 2019

With Endpoint Management, you can choose whether to manage devices, apps, or both.

Endpoint Management uses the following terms for device and app management modes, sometimes also referred to as deployment modes:

- Mobile device management mode (MDM mode)
- Mobile app management mode (MAM mode)
- MDM+MAM mode

To support those management or deployment modes, Endpoint Management has two server modes: MAM and MDM+MAM. When the Endpoint Management server mode is MDM+MAM mode, you can enable users to opt out of MDM enrollment. For more information, see Integrating with Citrix Gateway and Citrix ADC.

Mobile device management (MDM Mode)

With 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. Although app management is not available with MDM mode, you can deliver mobile apps, such as public app store and enterprise apps, in this mode. Following are common use cases for MDM mode:

- MDM is a consideration for corporate-owned devices where device-level management policies or restrictions, such as full wipe, selective wipe, or geo-location are required.
- When customers require management of an actual device, but do not require MDX policies, such as app containerization, controls on app data sharing, or micro VPN.
- 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 Mode)

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 Endpoint Management config-
ured for MAM mode, you can use MDX-enabled mobile apps to provide per-app containerization and control.

By leveraging MDX policies, Endpoint Management provides app-level control over network access (such as micro VPN), app and device interaction, data encryption, and app access.

MAM mode is often suitable for bring-your-own (BYO) devices because, although the device is unmanaged, corporate data remains protected. MDX has more than 50 MAM-only policies that you can set without needing an MDM control or relying on device passcodes for encryption.

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, and secure data storage in Citrix Files. For details, see Mobile productivity apps.

MAM is often suitable for the following examples:

- 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 Mode

MDM+MAM mode provides all feature sets available in the Endpoint Management Enterprise Mobility Management (EMM) solution.

Endpoint Management lets you specify whether users can choose to opt out of device management or whether you require device management. This flexibility is useful for environments that include a mix of use cases. These environments may or may not 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 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, it is likely that users must re-enroll their devices.
Following is a summary of the advantages and disadvantages (along with mitigations) of requiring MDM enrollment in an Endpoint Management Enterprise mode deployment.

**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 Citrix Gateway, Endpoint Management, and per-application time-outs, along with Citrix PIN, provide an extra layer of protection.
- While MDM actions do not apply to the device, some MDX policies are available to deny MAM access. The denial would be 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 holds them responsible if they choose to go out of compliance. Have administrators monitor unmanaged devices.
- Manage application access and security by using application timers. Decreased time-out values increase security, but may affect 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 desired.
- Users are not able to opt out of enrolling their device.
Citrix Endpoint Management

Disadvantages

- Requires all users to enroll with MDM.
- Might decrease adoption for users who object to corporate management of their personal devices.

Mitigation options

- Educate users about what Endpoint Management actually manages on their devices and what information administrators can access.

Device requirements

November 1, 2019

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 numerous. For a list of devices that 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, Endpoint Management functions slightly differently on 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 ensure that they fit the device screen 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 purchase devices that are preconfigured and ready for employees to use. Even when you don’t use these programs, consider whether you want to send invitation links to your users through SMS. You cannot use SMS on tablets.

For more information about enrollment, see User enrollment options.

Security and user experience

November 7, 2019
Security is important to any organization, but you need to strike a balance between security and user experience. On one hand, you may have a very secure environment that is very difficult for users to use. On the other hand, your environment may be so user-friendly that access control is not as strict. The other sections in this virtual handbook cover security features in detail, but the purpose of this article is to give a general overview of the security options available to you and to get you thinking about common security concerns in 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? Will you be using LDAP, certificate-based authentication, or a combination of the two?
- How much time should pass before a user's session 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/or an app-level passcode? How many logon attempts do you want to afford to users? Keep in mind the additional per-app authentication requirements that may be implemented with MAM and how users may perceive them.
- What other restrictions do you want to place on users? Should they be able to access cloud services such as Siri? What can they do with each app you make available to them and what can they not do? Should you deploy corporate WiFi policies to prevent cellular data plans from being eaten up while inside office spaces?

**App vs. Device**

One of the first things you should consider is whether you should only secure certain apps (mobile app management, or MAM) or if you want to manage the entire device (mobile device management or MDM). Most commonly, if you don’t require device-level control, you’ll only need to manage mobile apps, especially if your organization supports Bring Your Own Device (BYOD).

With a MAM-only environment, users can access resources made available to them. MAM policies secure and manage the apps themselves.

MDM allows you to secure an entire device, including the ability to take inventory of all the software on a device and 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 may reduce enrollment rates.

It is possible to have MDM required for some devices and not for others, but keep in mind that this choice may involve setting up two dedicated environments, which requires additional resources and upkeep.
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 big part of the authentication user experience is time-outs. A high security environment may have users log on every time they access the system, but that option may not be ideal for all organizations. For example, having users enter their credentials every time they want to access their email can be very frustrating and may not be necessary.

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 ensure everything functions properly. This information is stored in a generic vault within Secure Hub. If you enable user entropy through the Encrypt Secrets option, Endpoint Management creates a new vault called UserEntropy, and moves the information from the generic vault into this new vault. In order for 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 a number of places. This means, however, that whenever an app requires access to shared data in the UserEntropy vault—which includes passwords, PINs, and certificates—users need to enter a password or PIN.

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 may want this in some situations, but policies may also make a system unusable. For instance, you may want to block access to cloud applications such as Siri or iCloud that have the potential to send sensitive data where you don’t want it going. You can set up a policy to block access to these services, but keep in mind that such a policy may have unintended consequences. The iOS keyboard mic is also reliant on cloud access and you may block access to that feature as well.

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 facilitates application delivery and management. With the increasing adoption of BYOD,
you can typically implement a MAM solution, such as Endpoint Management, to assist with application delivery, software licensing, configuration, and application life cycle management.

With Endpoint Management, you can go a step further to secure these apps by configuring specific MAM policies and VPN settings to prevent data leak and other security threats. Endpoint Management provides organizations with the flexibility to deploy their solution as a MAM-only environment, or to implement Endpoint Management as a unified Endpoint Management Enterprise environment that provides both MDM and MAM functionality within in the same platform.

In addition to the ability to deliver apps to mobile devices, Endpoint Management offers app containerization through MDX technology. MDX secures apps through encryption that is separate from device level encryption; you can wipe or lock the app, and 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 a variety of 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 as well, in some cases. Endpoint Management categorizes these apps as follows:

**Public apps:** These apps include free or paid apps available in a public app store, such as iTunes 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 may use numerous 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, and then wrapping them with the MDX Toolkit for enterprise distribution. If you need to wrap third-party applications, work with your app vendor to obtain the app binaries which you can wrap 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 may 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 Endpoint Management. For example, a healthcare organization may create an in-house app that allows physicians to view patient information on mobile devices. An organization can then use the MDX Service or MDX Toolkit to 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). 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:** These are Citrix-developed apps that are included with the Endpoint Management license. For details, see About mobile productivity apps. Citrix also offers other business-
**ready apps** that ISVs develop by using the Mobile Apps SDK.

**HDX apps:** These 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 Endpoint Management to make the apps available to the enrolled users.

Depending on the type of mobile apps you plan to deploy and manage with Endpoint Management, the underlying configuration and architecture will differ. For example, if multiple groups of users with different level of permissions will consume a single app, you may have to create separate delivery groups to deploy two separate versions of the same app. In addition, you must make sure the user group membership is mutually exclusive to avoid policy mismatches on users’ devices.

You may also want to manage iOS application licensing by using Apple volume purchase. This option will require you to register for the volume purchase program and configure Endpoint Management volume purchase settings in the Endpoint Management console to distribute the apps with the volume purchase licenses. A variety of such use cases makes it important to assess and plan your MAM strategy prior to implementing the Endpoint Management environment. You can start planning your MAM strategy by defining the following:

**Types of apps:** List the different types of apps you plan to support and categorize them, such as public, native, Citrix mobile productivity apps, Web, in-house, ISV apps, and so on. Also, categorize the apps for different device platforms, such as iOS and Android. This categorization will help with aligning different Endpoint Management settings that are required for each type of app. For example, certain apps may not qualify for wrapping, or a few apps may require the use of the Mobile Apps SDK to enable special APIs for interaction with other apps.

**Network requirements:** You need to configure apps with specific network access requirements with the appropriate settings. For example, certain apps may need access to your internal network through VPN. Some apps may require Internet access to route access via the DMZ. In order to allow such apps to connect to the required network, you have to configure various settings accordingly. Defining per-app network requirements help in finalizing your architectural decisions early on, which will streamline the overall implementation process.

**Security requirements:** Defining the security requirements that apply to either individual apps or all the apps is critical. Although settings, such as the MDX policies, apply to individual apps, session and authentication settings apply across all apps, and some apps may have specific encryption, containerization, wrapping, encryption, authentication, geo fencing, passcode or data sharing requirements that you will need to outline in advance to simplify your deployment.

**Deployment requirements:** You may want to use a policy-based deployment to allow only compliant users to download the published apps. For example, you may want certain apps to require that device encryption is enabled or the device is managed, or that the device meets a minimum operating system version. You may also want certain apps to be available only to corporate users. You need to outline such requirements in advance so that you can configure the appropriate deployment rules or actions.
Licensing requirements: You should record app-related licensing requirements. These notes will help you to manage license usage effectively and to decide if you need to configure specific features in Endpoint Management to facilitate licensing. For example, if you deploy an iOS app, irrespective of whether it is a free or a paid app, Apple enforces licensing requirements on the app by making the users sign into their iTunes account. You can register for Apple volume purchase to distribute and manage these apps via Endpoint Management. Volume purchase allows users to download the apps without having to sign into their iTunes account. Additionally, tools, such as Samsung SAFE and Samsung Knox, have special licensing requirements, which you need to complete prior to deploying those features.

Blacklist/whitelist requirements: There may be apps that you do not want users to install or use at all. Creating a blacklist will define an out of compliance event. You can then set up policies to trigger in case such a thing happens. On the other hand, an app may be acceptable for use but may fall under the blacklist for one reason or another. If this is the case, you can add the app to a whitelist 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. This may conflict with your blacklisting strategy.

Apps use case

A healthcare organization plans to deploy 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

- **Secure Hub:** Client used by all mobile devices to communicate with Endpoint Management. IT pushes security settings, configurations, and mobile apps to mobile devices via the Secure Hub client. Android and iOS devices enroll in Endpoint Management through 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.
Citrix Endpoint Management

- **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**: HDX apps are delivered by Citrix Virtual Apps to Citrix workspace.

- **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.

<table>
<thead>
<tr>
<th>App Name</th>
<th>App Type</th>
<th>MDX Wrapping</th>
<th>iOS</th>
<th>Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Mail</td>
<td>Mobile productivity app</td>
<td>No for version 10.4.1 and later</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure Web</td>
<td>Mobile productivity app</td>
<td>No for version 10.4.1 and later</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure Notes</td>
<td>Mobile productivity app</td>
<td>No for version 10.4.1 and later</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note:**

Secure Notes and Secure Tasks reached End of Life (EOL) status on December 31, 2018. For details, see EOL and deprecated apps.
The following tables list specific requirements you can consult when configuring MAM policies in Endpoint Management.

<table>
<thead>
<tr>
<th>App Name</th>
<th>VPN Required</th>
<th>Interaction (with apps outside of container)</th>
<th>Interaction (from apps outside of container)</th>
<th>Device Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Mail</td>
<td>Y</td>
<td>Selectively Allowed</td>
<td>Allowed</td>
<td>Not required</td>
</tr>
<tr>
<td>Secure Web</td>
<td>Y</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Not required</td>
</tr>
<tr>
<td>Secure Notes</td>
<td>Y</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Not required</td>
</tr>
<tr>
<td>Citrix Files</td>
<td>Y</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Not required</td>
</tr>
<tr>
<td>Secure Hub</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>App Name</td>
<td>VPN Required</td>
<td>Interaction (with apps outside of container)</td>
<td>Interaction (from apps outside of container)</td>
<td>Device Encryption</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Citrix Workspace app</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>GoToMeeting</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>SalesForce1</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>RSA SecurID</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Epic Haiku</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Epic Canto</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Epic Rover</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Epic Hyperspace</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Vocera</td>
<td>Y</td>
<td>Disallowed</td>
<td>Disallowed</td>
<td>Not required</td>
</tr>
<tr>
<td>HCMail</td>
<td>Y</td>
<td>Disallowed</td>
<td>Disallowed</td>
<td>Required</td>
</tr>
<tr>
<td>PatientRounding</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>Required</td>
</tr>
<tr>
<td>Outlook Web Access</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>Not required</td>
</tr>
<tr>
<td>SharePoint</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>Not required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>App Name</th>
<th>Proxy Filtering</th>
<th>Licensing</th>
<th>Geo-fencing</th>
<th>Mobile Apps SDK</th>
<th>Minimum Operating System Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Mail</td>
<td>Required</td>
<td>N/A</td>
<td>Selectively Required</td>
<td>N/A</td>
<td>Enforced</td>
</tr>
<tr>
<td>Secure Web</td>
<td>Required</td>
<td>N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Enforced</td>
</tr>
<tr>
<td>Secure Notes</td>
<td>Required</td>
<td>N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Enforced</td>
</tr>
<tr>
<td>Citrix Files</td>
<td>Required</td>
<td>N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Enforced</td>
</tr>
<tr>
<td>Secure Hub</td>
<td>Not required</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Citrix Workspace app</td>
<td>Not required</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
</tbody>
</table>
Citrix Endpoint Management

<table>
<thead>
<tr>
<th>App Name</th>
<th>Proxy Filtering</th>
<th>Licensing</th>
<th>Geo-fencing</th>
<th>Mobile Apps SDK</th>
<th>Minimum Operating System Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoToMeeting</td>
<td>Not required</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>SalesForce1</td>
<td>Not required</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>RSA SecurID</td>
<td>Not required</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Epic Haiku</td>
<td>Not required</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Epic Canto</td>
<td>Not required</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Epic Rover</td>
<td>Not required</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Epic Hyperspace</td>
<td>Not required</td>
<td>N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Vocera</td>
<td>Required</td>
<td>N/A</td>
<td>Required</td>
<td>Required</td>
<td>Enforced</td>
</tr>
<tr>
<td>HCMail</td>
<td>Required</td>
<td>N/A</td>
<td>Required</td>
<td>Required</td>
<td>Enforced</td>
</tr>
<tr>
<td>PatientRounding</td>
<td>Required</td>
<td>N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Outlook Web Access</td>
<td>Required</td>
<td>N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>SharePoint</td>
<td>Required</td>
<td>N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
</tbody>
</table>

**User Communities**

Every organization consists of diverse user communities that operate in different functional roles. These user communities perform different tasks and office functions using various resources that you provide through the users’ mobile devices. Users may work from home or in remote offices using mobile devices that you provide, or using their personal mobile devices, which allows them to access tools that are subject to certain security compliance rules.

As more and more user communities start using mobile devices to either simplify or aid in their job role, Enterprise Mobility Management (EMM) becomes critical to prevent data leak and to enforce an
organization's security restrictions. In order for efficient and more sophisticated mobile device management, you can categorize your user communities. Doing so simplifies the mapping of users to resources and ensures that the right security policies apply to the right 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 multiple 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. A selected set of users receive corporate mobile devices, while others can access limited company resources from their personal devices. In order to enforce the right level of security restrictions and prevent data leak, the organization decided that corporate IT manages each enrolled device, Corporate and Bring Your Own Device (BYOD). Additionally, users can only enroll a single device.

The following section provides an overview of the roles and functions of each subgroup:

**Clinical**

- Nurses
- Physicians (Doctors, Surgeons, and so on)
- Specialists (Dieticians, phlebotomists, 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 performing physician services for patient home visits)
- Research Specialist (Knowledge Workers and Power Users at six Research Institutes performing 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 performing various back office functions including: HR, Payroll, Accounts Payable, Supply Chain Service, and so on)
- Physician Services (Office workers performing a variety of health care 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 performing a variety of non-clinical functions including: Benefits Administration, Clinical Integration, Communications, Compensation & Performance Management, Facility & Property Services, HR Technology Systems, Information Services, Internal Audit & Process Improvement, and so on.)
- Philanthropic Programs (Office and mobile workers that perform 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 Endpoint Management, see Deploy resources.

**Active Directory Organizational Units (OUs) and Groups**

For OU = 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

**Endpoint Management Local Users and Groups**

For Group = Contractors, Users =

- Vendor1
- Vendor2
- Vendor 3
- … Vendor 10
**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**

<table>
<thead>
<tr>
<th>Active Directory Groups</th>
<th>Endpoint Management Delivery Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>XM-Nurses</td>
<td>Clinical-Nurses</td>
</tr>
<tr>
<td>XM-Physicians</td>
<td>Clinical-Physicians</td>
</tr>
<tr>
<td>XM-Specialists</td>
<td>Clinical-Specialists</td>
</tr>
<tr>
<td>XM-Outside Physicians</td>
<td>Clinical-Outside Physicians</td>
</tr>
<tr>
<td>XM-Home Health Services</td>
<td>Clinical-Home Health Services</td>
</tr>
<tr>
<td>XM-Research Specialist</td>
<td>Clinical-Research Specialist</td>
</tr>
<tr>
<td>XM-Education and Training</td>
<td>Clinical-Education and Training</td>
</tr>
<tr>
<td>XM-Shared Services</td>
<td>Non-Clinical-Shared Services</td>
</tr>
<tr>
<td>XM-Physician Services</td>
<td>Non-Clinical-Physician Services</td>
</tr>
<tr>
<td>XM-Support Services</td>
<td>Non-Clinical-Support Services</td>
</tr>
<tr>
<td>XM-Philanthropic Programs</td>
<td>Non-Clinical-Philanthropic Programs</td>
</tr>
</tbody>
</table>

**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.
## Endpoint Management Delivery

<table>
<thead>
<tr>
<th>Groups</th>
<th>Citrix Mobile Apps</th>
<th>Public Mobile Apps</th>
<th>HDX Mobile Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical-Nurses</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Physicians</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Specialists</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Outside Physicians</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Home Health Services</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Research Specialist</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Education and Training</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Non-Clinical-Shared Services</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Non-Clinical-Physician Services</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Non-Clinical-Support Services</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Non-Clinical-Philanthropic Programs</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Contractors</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

## Endpoint Management Delivery

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical-Nurses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Clinical-Physicians</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
## Endpoint Management Delivery Groups

<table>
<thead>
<tr>
<th></th>
<th>Public App: RSA SecurID</th>
<th>Public App: EpicCare Haiku</th>
<th>HDX App: Epic Hyperspace</th>
<th>Passcode Policy</th>
<th>Device Restrictions</th>
<th>Automated Actions</th>
<th>Wi-Fi Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical-Specialists</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Outside Physicians</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Home Health Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Research Specialist</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Education and Training</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Clinical-Shared Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Clinical-Physician Services</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Clinical-Support Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Notes and Considerations
• 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 will have rights to enroll into Endpoint Management.
• 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 Endpoint Management, that user cannot enroll. Likewise, if a user is a member of multiple groups, Endpoint Management will only categorize the user as being in the groups mapped to Endpoint Management.
• In order to make MDM enrollment mandatory, you must set the Enrollment Required option to True in Server Properties in the Endpoint Management console. For details, see Server properties.
• You can delete a user group from an Endpoint Management delivery group by deleting the entry in the SQL Server database, under dbo.userlistgrps.

Caution: Before you perform this action, create a backup of Endpoint Management and the database.

About device ownership in Endpoint Management

You can group users according to the owner of a user device. Device ownership includes corporate-owned devices and user-owned devices, also known as bring your own device (BYOD). You can control how BYOD devices connect to your network in two places in the Endpoint Management console: in Deployment Rules and through Endpoint Management server properties on the Settings page. For details about deployment rules, see Configuring Deployment Rules. For details about server properties, see Server properties.

By setting server properties, you can require all BYOD users to accept corporate management of their devices before they can access apps, or you can give users access to corporate apps without also managing their devices.

When you set the server setting wsapi.mdm.required.flag to true, Endpoint Management manages all BYOD devices, and any user who declines enrollment is denied access to apps. You should consider setting wsapi.mdm.required.flag to true in environments in which enterprise IT teams need high security along with a positive user experience, which comes from enrolling user devices in Endpoint Management.

If you leave wsapi.mdm.required.flag as false, which is the default setting, users can decline enrollment, but may still access apps on their devices through the app store. You should consider setting wsapi.mdm.required.flag to false in environments in which privacy, legal, or regulatory constraints require no device management, only enterprise app management.

Users with devices that 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. The policies, depending on the values you set, require the device to check Endpoint Management routinely to confirm that the apps are still allowed to run.

**Security requirements**

The amount of security considerations when deploying a Endpoint Management environment can quickly become overwhelming. There are many interlocking pieces and settings, that you may not know where to begin or what to choose to ensure 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.

Note that security concerns alone should not dictate your deployment mode choice. It is important to also review the requirements of the use case and decide if you can mitigate security concerns before choosing your deployment mode.

**High:** Using these settings provides an optimal user experience while maintaining a basic level of security acceptable to most organizations.

**Higher:** These settings strike a stronger balance between security and usability.

**Highest:** Following these recommendations will provide a very high level of security at the cost of usability and user adoption.

**Deployment mode security considerations**

The following table specifies the deployment modes for each security level.

<table>
<thead>
<tr>
<th>Security Level</th>
<th>High Security</th>
<th>Higher Security</th>
<th>Highest Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAM and/or MDM</td>
<td>MDM+MAM</td>
<td>MDM+MAM</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**

- Depending on the use case, a MDM-only or MAM-only deployment could meet security requirements and provide a good user experience.
- If there is no need for app containerization, micro VPN or app specific policies, MDM should be sufficient to manage and secure devices.
- For use cases like BYOD in which all business and security requirements may 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. You should enforce MDM enrollment through a server property in the Endpoint Management console.
Citrix Endpoint Management

**Citrix ADC and Citrix Gateway security considerations**

The following table specifies the Citrix ADC and Citrix Gateway recommendations for each security level.

<table>
<thead>
<tr>
<th>High Security</th>
<th>Higher Security</th>
<th>Highest Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix ADC is recommended.</td>
<td>Standard NetScaler for XenMobile wizard configuration with SSL bridge</td>
<td>SSL Offload with end-to-end encryption</td>
</tr>
<tr>
<td>Citrix Gateway is required for MAM and MDM+MAM</td>
<td>if Endpoint Management is in the DMZ; or SSL offload if required to meet security standards when Endpoint Management server is in the internal network.</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**

- Exposing Endpoint Management server to the Internet via NAT or existing third-party proxies/load-balancers could be an option for MDM as long as the SSL traffic terminates on Endpoint Management server, but this choice poses a potential security risk.
- For high security environments, Citrix Gateway with the default Endpoint Management configuration should meet or exceed security requirements.
- For MDM environments with the highest security needs, SSL termination at Citrix Gateway provides the ability 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 Citrix Gateway and Citrix ADC](#).

**Enrollment security considerations**

The following table specifies the Citrix ADC and Citrix Gateway recommendations for each security level.
Citrix Endpoint Management

High Security | Higher Security | Highest Security
--- | --- | ---
Active Directory Group membership only. All users Delivery Group disabled. | Invitation only enrollment mode. Active Directory Group membership only. All users Delivery Group disabled | Enrollment 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 requires disabling the built-in All users Delivery Group.
- You can use enrollment invitations to restrict enrollment to users with an invitation only.
- You can use one-time PIN (OTP) enrollment invites as a two-factor solution and to control the number of devices a user may enroll.
- For environments with the highest security requirements, you can tie enrollment invitations to a device by SN/UDID/EMEI. A two-factor option is also available to require Active Directory password and OTP. (Note that OTP is not supported as an option for Windows devices.)

Device PIN security considerations

The following table specifies the device PIN recommendations for each security level.

| High Security | Higher Security | Highest Security |
--- | --- | ---
Recommended. High security is required for device-level encryption. May be enforced with MDM. Can be set as required for MAM-only by using an MDX policy. | Enforced by using MDM and/or MDX policy. | Enforced by using MDM and MDX policy. MDM Complex passcode policy.

Notes:
- Citrix recommends the use of a device PIN.
- You can enforce a device PIN via an MDM policy.
- You can use an MDX policy to make a device PIN a requirement for using managed apps; for example, for BYOD use cases.
- Citrix recommends combining the MDM and MDX policy options for increased security in

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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 comply with a passcode policy.

**Apps**

November 7, 2019

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 facilitates application delivery and management. With the increasing adoption of BYOD, you can typically implement a MAM solution, such as Endpoint Management. Endpoint Management assists with application delivery, software licensing, configuration, and application life cycle management. You can require or allow users to also opt for MDM management.

With Endpoint Management, you secure apps by configuring MAM policies and VPN settings to prevent data leak and other security threats. Endpoint Management provides organizations with the flexibility to enroll devices as MAM-only or MDM+MAM.

In addition to the ability to deliver apps to mobile devices, Endpoint Management offers app containerization through MDX technology. MDX secures apps through encryption that is separate from device level encryption. You can wipe or lock the app. 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. Endpoint Management categorizes these apps as follows:

- **Public apps:** These apps include free or paid apps available in a public app store, such as iTunes 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 numerous 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, and then wrapping them with the MDX Toolkit for enterprise distribution. To wrap third-party applications, work with your app vendor to obtain 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 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 use the MDX Service or MDX Toolkit to wrap the app to secure patient information and enable VPN access to the patient database.

- **Web and SaaS apps**: These apps include apps accessed from an internal network (web apps) or over a public network (SaaS). 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 Endpoint Management license. For details, see [About mobile productivity 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 Endpoint Management, the underlying configuration might differ. For example, multiple 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. In addition, you must make sure 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 Endpoint Management volume purchase settings in the 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 Endpoint Management environment. You can start planning your MAM strategy by defining the following:

- **Types of apps**: List the different types of apps you plan to support and categorize them, such as public, native, Web, in-house, ISV apps, and so on. Also, categorize the apps for different device platforms, such as iOS and Android. This categorization helps with aligning different 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 the use of the Mobile Apps SDK to enable special APIs for interaction with other apps.

- **Network requirements**: You must configure apps with specific network access requirements with the appropriate settings. For example, certain apps might need access to your internal
network through 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 finalizing 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 encryption, containerization, wrapping, encryption, authentication, geofencing, passcode or data sharing requirements

You must outline those requirements in advance to simplify your deployment. For details on security in 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 device encryption is enabled or 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:** You should record app-related licensing requirements. Your notes will help you to manage license usage effectively and to decide whether to configure specific features in 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 the users sign into their iTunes account. You can register for Apple volume purchase to distribute and manage these apps via Endpoint Management. Volume purchase allows users to download the apps without having to sign into their iTunes account. Also, tools, such as Samsung SAFE and Samsung Knox, have special licensing requirements to complete before deploying those features.

- **Blacklist/whitelist requirements:** You might identify apps that you do not want users to install or use. Creating a blacklist 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 could fall under the blacklist for one reason or another. In that case, you can add the app to a whitelist 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 blacklisting strategy.
Use Case

A healthcare organization plans to deploy 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 Endpoint Management 10.18.14: IT pushes security settings, configurations, and mobile apps to mobile devices via Secure Hub. Android and iOS devices enroll in Endpoint Management through Secure Hub.

For new customers as of Endpoint Management 10.18.14: Secure Hub supports the use of the Workspace apps store. When opening Secure Hub, users no longer see the Secure Hub store. Now, an Add Apps button takes users to the Workspace apps store.

Following is a video that shows an iOS device performing an enrollment to Citrix Endpoint Management using the Citrix Workspace app.

**Citrix Workspace app:** The Citrix Workspace app incorporates existing Citrix Receiver technology, Secure Hub, and other Citrix Workspace client technologies. 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.

**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.

<table>
<thead>
<tr>
<th>App Name</th>
<th>App Type</th>
<th>MDX Wrapping</th>
<th>iOS</th>
<th>Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Mail</td>
<td>Mobile productivity app</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure Web</td>
<td>Mobile productivity app</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Note: Secure Notes reached End of Life (EOL) status on December 31, 2018. For details, see EOL and deprecated apps.

<table>
<thead>
<tr>
<th>Mobile productivity app</th>
<th>Yes</th>
<th>No</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Notes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile productivity app</th>
<th>Yes</th>
<th>No</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Files</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Secure Hub</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Citrix Workspace app</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>GoToMeeting</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Salesforce1</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>RSA SecurID</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Epic Haiku</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Epic Canto</td>
<td>N/A</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Epic Rover</td>
<td>N/A</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Epic Hyperspace</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Vocera</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>HCMail</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>PatientRounding</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Outlook Web Access</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SharePoint</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

The following table lists specific requirements you can consult configuring MAM policies in Endpoint Management.
<table>
<thead>
<tr>
<th>App Name</th>
<th>VPN Required</th>
<th>Interact (with)</th>
<th>Interaction (from)</th>
<th>Device Encryption</th>
<th>Proxy Filtering</th>
<th>Licensing</th>
<th>Minimum Operating System</th>
<th>Mobile Apps</th>
<th>SDK</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Mail</td>
<td>Y</td>
<td>Selectively Allowed</td>
<td>Allowed</td>
<td>Not required</td>
<td>Required N/A</td>
<td>Selectively Required</td>
<td>N/A</td>
<td>Enforced</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Web</td>
<td>Y</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Not required</td>
<td>Required N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Enforced</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Notes</td>
<td>Y</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Not required</td>
<td>Required N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Enforced</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
Secure Notes reached End of Life (EOL) status on December 31, 2018. For details, see EOL and deprecated apps.
<table>
<thead>
<tr>
<th>App Name</th>
<th>VPN Required</th>
<th>Interaction (with apps outside of container)</th>
<th>Interaction (from apps outside of container)</th>
<th>Device Encryption</th>
<th>Proxy Filtering</th>
<th>Geo-fencing</th>
<th>Mobile Apps SDK</th>
<th>Minimum Operating System Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Hub</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Not required</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
</tr>
<tr>
<td>Citrix Workspace app</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Not required</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
</tr>
<tr>
<td>GoToMeeting</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enfored</td>
</tr>
<tr>
<td>SalesForce1</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>RSA SecurID</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Epic Haiku</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Epic Canto</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Epic Rover</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Volume purchase</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Epic HyperSpace</td>
<td>Y</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Vocera</td>
<td>Y</td>
<td>Disallowed</td>
<td>Disallowed</td>
<td>Required</td>
<td>N/A</td>
<td>Required</td>
<td>Required</td>
<td>Enforced</td>
</tr>
<tr>
<td>HCMail</td>
<td>Y</td>
<td>Disallow</td>
<td>Disallow</td>
<td>Required</td>
<td>N/A</td>
<td>Required</td>
<td>Required</td>
<td>Enforced</td>
</tr>
</tbody>
</table>
Citrix Endpoint Management

<table>
<thead>
<tr>
<th>App Name</th>
<th>VPN Required</th>
<th>Interaction (with apps outside of container)</th>
<th>Interaction (from apps outside of container)</th>
<th>Device Encryption</th>
<th>Proxy Filtering</th>
<th>Geo-fencing</th>
<th>Mobile Apps</th>
<th>Minimum Operating System Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>PatientRounding</td>
<td>N/A</td>
<td>N/A</td>
<td>Required</td>
<td>Required</td>
<td>N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>Outlook Web Access</td>
<td>Y</td>
<td>N/A</td>
<td>Not required</td>
<td>Required</td>
<td>N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
<tr>
<td>SharePoint</td>
<td>N/A</td>
<td>N/A</td>
<td>Not required</td>
<td>Required</td>
<td>N/A</td>
<td>Not required</td>
<td>N/A</td>
<td>Not enforced</td>
</tr>
</tbody>
</table>

**User communities**

May 9, 2019

Every organization consists of diverse user communities that operate in different functional roles. These user communities perform 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 allows 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 data leak and to enforce organizational security restrictions. In order for efficient and more sophisticated mobile device management, you can categorize your user communities. Doing so simplifies the mapping of users to resources and ensures that the right security policies apply to the right users.

Categorizing user communities can include 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 Endpoint Management resources.

- **Endpoint Management local users and groups**
For users who don’t have an account in Active Directory, you can create the users as local Endpoint Management users. You can add local users to delivery groups and provision resources to them in the same manner as Active Directory users.

- Endpoint Management delivery groups

If multiple groups of users with different level of permissions are to consume a single app, you might need 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.

**Use case**

This example healthcare organization provides technology resources and access to multiple 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 receive 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 leak, 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, phlebotomists, 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 performing physician services for patient home visits)
- Research Specialist (Knowledge Workers and Power Users at six Research Institutes performing 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 performing various back-office functions including: HR, Payroll, Accounts Payable, Supply Chain Service, and so on)
- Physician Services (Office workers performing various health care 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 performing various non-clinical functions including: Benefits Administration, Clinical Integration, Communications, Compensation & Performance Management, Facility & Property Services, HR Technology Systems, Information Services, Internal Audit & Process Improvement, and so on.)
- Philanthropic Programs (Office and mobile workers that perform 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 Endpoint Management, see Deploy resources in the Endpoint Management product documentation.

**Active Directory Organizational Units (OUs) and Groups**

**For OU =** Endpoint Management Resources

- OU = Clinical; Groups =
Citrix Endpoint Management

- 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

Endpoint Management Local Users and Groups

For Group= Contractors, Users =
• Vendor1
• Vendor2
• Vendor 3
• … Vendor 10

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
### Citrix Endpoint Management

<table>
<thead>
<tr>
<th>Active Directory Groups</th>
<th>Endpoint Management Delivery Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>XM-Nurses</td>
<td>Clinical-Nurses</td>
</tr>
<tr>
<td>XM-Physicians</td>
<td>Clinical-Physicians</td>
</tr>
<tr>
<td>XM-Specialists</td>
<td>Clinical-Specialists</td>
</tr>
<tr>
<td>XM-Outside Physicians</td>
<td>Clinical-Outside Physicians</td>
</tr>
<tr>
<td>XM-Home Health Services</td>
<td>Clinical-Home Health Services</td>
</tr>
<tr>
<td>XM-Research Specialist</td>
<td>Clinical-Research Specialist</td>
</tr>
<tr>
<td>XM-Education and Training</td>
<td>Clinical-Education and Training</td>
</tr>
<tr>
<td>XM-Shared Services</td>
<td>Non-Clinical-Shared Services</td>
</tr>
<tr>
<td>XM-Physician Services</td>
<td>Non-Clinical-Physician Services</td>
</tr>
<tr>
<td>XM-Support Services</td>
<td>Non-Clinical-Support Services</td>
</tr>
<tr>
<td>XM-Philanthropic Programs</td>
<td>Non-Clinical-Philanthropic Programs</td>
</tr>
</tbody>
</table>

### Delivery Group and Resource mapping of apps

<table>
<thead>
<tr>
<th>Secure Mail</th>
<th>Secure Web</th>
<th>Citrix Files</th>
<th>Workspace app</th>
<th>Salesforce</th>
<th>SecurID</th>
<th>EpicCare</th>
<th>Haiku</th>
<th>Hyper-space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical-Nurses</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Physicians</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Specialist</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Outside Physicians</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Home Health Services</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Delivery Group and Resource mapping of MDM Resources

<table>
<thead>
<tr>
<th>Secure Mail</th>
<th>Secure Web</th>
<th>Citrix Files</th>
<th>Workspace app</th>
<th>RSA SecurID</th>
<th>EpicCare Haiku</th>
<th>Epic Hyper-space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical-Research Specialist</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Education and Training</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Non-Clinical-Shared Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Non-Clinical-Physician Services</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Non-Clinical-Support Services</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Non-Clinical-Philanthropic Programs</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Contractors</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Role</td>
<td>MDM: Passcode policy</td>
<td>MDM: Device Restrictions</td>
<td>MDM: Automated Actions</td>
<td>MDM: Wi-Fi policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------</td>
<td>--------------------------</td>
<td>------------------------</td>
<td>-------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Nurses</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Physicians</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Specialists</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Outside Physicians</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Home Health Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Research Specialist</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical-Education and Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Clinical-Shared Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Clinical-Physician Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Clinical-Support Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Clinical-Philanthropic Programs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractors</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes and considerations**

- 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 rights to...
enroll into Endpoint Management.

- 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 Endpoint Management, that user cannot enroll. Likewise, if a user is a member of multiple groups, Endpoint Management only categorizes the user as being in the groups mapped to Endpoint Management.

- To make MDM enrollment mandatory, set the Enrollment Required option to True in Server Properties in the Endpoint Management console. For details, see Server properties.

- To delete a user group from a Endpoint Management delivery group, delete the entry in the SQL Server database, under dbo.userlistgrps.

Caution:
Before you perform this action, create a backup of Endpoint Management and the database.

About device ownership in Endpoint Management

You can group users according to the owner of a user device. Device ownership includes corporate-owned devices and user-owned devices, also known as bring your own device (BYOD). You can control how BYOD devices connect to your network in two places in the Endpoint Management console: in Deployment Rules and through Endpoint Management properties on the Settings page. For details about deployment rules, see Deploy resources. For details about server properties, see Server properties.

By setting server properties, you can require all BYOD users to accept corporate management of their devices before they can access apps. Or, you can give users access to corporate apps without also managing their devices.

When you set the server property wsapi.mdm.required.flag to true, Endpoint Management manages all BYOD devices, and any user who declines enrollment is denied access to apps. Consider setting wsapi.mdm.required.flag to true in environments in which enterprise IT teams need high security plus a positive user experience during enrolling.

If you leave wsapi.mdm.required.flag as false, which is the default setting, users can decline enrollment. However, they can access apps on their devices through the app store. Consider setting wsapi.mdm.required.flag to false in environments in which privacy, legal, or regulatory constraints require no device management, only enterprise app management.

Users with devices that 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. Some policy settings require the device to check Endpoint Management routinely to confirm that the apps are still allowed to run.

**Email strategy**

August 28, 2019

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 Endpoint Management design. 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 may need to use a combination of clients.

The following table outlines design considerations for the different client options available:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Secure Mail</th>
<th>Native (for example, iOS Mail)</th>
<th>Third-party mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Exchange account profiles configured via an MDX policy.</td>
<td>Exchange account profiles configured via an MDM policy. Android support is limited to: SAFE/Knox, HTC, and Android Enterprise. All other clients are considered third-party clients.</td>
<td>Generally requires manual configuration by the user.</td>
</tr>
<tr>
<td>Security</td>
<td>Secure by design, providing the highest security. Uses MDX policies with added data encryption levels. Secure Mail is a fully managed app via an MDX policy. Added layer of authentication with Citrix PIN.</td>
<td>Based on vendor/app feature set. Provides higher security. Uses device encryption settings (with no security via MDX policies). Relies on device-level authentication for access to the app.</td>
<td>Based on vendor/app feature set. Provides high security.</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Integration</td>
<td>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.</td>
<td>Can only interact with other unmanaged (non-MDX) apps by default.</td>
<td>Can only interact with other unmanaged (non-MDX) apps by default.</td>
</tr>
<tr>
<td>Deployment/</td>
<td>You can push Secure Mail through MDM, directly from public app stores. Included with Endpoint Management Advanced and Enterprise licensing.</td>
<td>Client app included with platform operating system. No additional licensing requirements.</td>
<td>Can push via MDM, as an enterprise app or directly from public app stores. Associated licensing model/costs based on app vendor.</td>
</tr>
<tr>
<td>Licensing</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Support**

| Single vendor support for the client and EMM solution (Citrix). Embedded support contact info in Secure Hub/app debug logging capabilities. One client to support. | Vendor defined support (Apple/Google). May need 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 regarding the flow of mail (ActiveSync) traffic in the context of 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, Citrix 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 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 Citrix Gateway (micro VPN and STA)**

This scenario is the default when using the Secure Mail client, due to its micro VPN capabilities. In this case, the Secure Mail client establishes a secure connection to ActiveSync via Citrix Gateway. In essence, you can consider Secure Mail to be the client connecting directly to ActiveSync from the internal network. Citrix customers often standardize on 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 managed (MDX wrapped) apps can use the micro VPN function. Therefore, this scenario does not apply to native clients. Even though it may be possible to wrap third-party clients with the MDX Toolkit, this practice is not common. The use of device-level VPN clients to allow tunneled access for native or third-party clients has proven to be cumbersome and not a viable solution.
**Scenario 3: Cloud-hosted Exchange services**

Cloud-hosted Exchange services, such as Microsoft Office 365, are becoming more popular. In the context of Endpoint Management, this scenario may 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 Secure Mail and other native or third-party clients.

Endpoint Management can add value in three areas for this scenario:

- Client wrapping with MDX policies and app management with Secure Mail
- Client configuration with the use of an MDM policy on supported native email clients
- ActiveSync filtering options with the use of 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 Endpoint Management solution includes two components designed specifically to provide ActiveSync filtering capabilities for native and third-party clients: Citrix Gateway connector for Exchange ActiveSync and Endpoint Management connector for Exchange ActiveSync.

**Citrix Gateway connector for Exchange ActiveSync**

The use of Citrix Gateway connector for Exchange ActiveSync provides ActiveSync filtering at the perimeter, by using Citrix 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 Citrix Gateway and Endpoint Management. When a device communicates with Exchange through the ActiveSync virtual server on the Citrix Gateway, Citrix Gateway performs an HTTP callout to the connector for Exchange ActiveSync service. That service then checks the device status with Endpoint Management. Based on the status of the device, the connector for Exchange ActiveSync replies to Citrix Gateway to either allow or deny the connection. You may 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:

- **Windows Server**: The connector for 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 may configure static
Citrix Endpoint Management

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 Endpoint Management connector for Exchange ActiveSync instead.

- **Citrix Gateway scalability:** Given the requirement to proxy ActiveSync traffic via Citrix Gateway: Proper sizing of the Citrix Gateway instance is critical to support the added workload of all ActiveSync SSL connections.

- **Citrix Gateway Integrated Caching:** The connector for Exchange ActiveSync configuration on the Citrix Gateway uses the Integrated Caching function to cache responses from the connector. As a result of that configuration, Citrix 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 Citrix Gateway Platinum Edition.

- **Custom filtering policies:** You might need to create custom Citrix Gateway policies to restrict certain ActiveSync clients outside of the standard native mobile clients. This configuration requires knowledge on ActiveSync HTTP requests and Citrix Gateway responder policy creation.

- **Secure Mail clients:** Secure Mail has micro VPN capabilities which eliminate the need for filtering at the perimeter. The Secure Mail client would generally be treated as an internal (trusted) ActiveSync client when connected through the Citrix Gateway. If support for both native and third-party (with the connector for Exchange ActiveSync) and Secure Mail clients is required: Citrix recommends that Secure Mail traffic does not flow via the Citrix Gateway virtual server used for the connector. You can accomplish this traffic flow via DNS and keep the connector policy from affecting Secure Mail clients.

For a diagram of Citrix Gateway connector for Exchange ActiveSync in an Endpoint Management deployment, see **Architecture**.

**Endpoint Management connector for Exchange ActiveSync**

Endpoint Management connector for Exchange ActiveSync is an 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 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 Endpoint Management connector for Exchange ActiveSync rule criteria.

Similar to Citrix Gateway connector for Exchange ActiveSync, the connector for Exchange ActiveSync checks the device status with Endpoint Management to filter access based on device compliance. You may 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 Citrix 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 Citrix Gateway connector for Exchange ActiveSync, the connector for Exchange ActiveSync includes filtering rules to evaluate device state. Additionally, 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 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 Endpoint Management to perform an Exchange ActiveSync wipe on a mobile device. The connector for Exchange ActiveSync also allows Endpoint Management to access information about Blackberry devices and to perform other control operations.

For a diagram of Endpoint Management connector for Exchange ActiveSync in an Endpoint Management deployment, see Architecture.

**Email platform decision tree**

The following figure helps you distinguish the pros and cons between using native email or Secure Mail solutions in your Endpoint Management deployment. Each choice allows for associated 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.
What is the best mobile email platform for your situation?

**Citrix Secure Mail**
- Email traffic bypasses Citrix Gateway
- MDX policies secure the app
- Exchange ActiveSync/CAS is exposed to the Internet

**Native email**

**Endpoint Management options and requirements**

**Secure Mail - unrestricted**
- Email traffic is encrypted and secure
- MDX policies secure the app

**Secure Mail – tunneled to the internal network**
- Email traffic leverages Citrix Gateway
- Uses Endpoint Management as a STA server (optional)
- MDX policies secure the app

**Pros for each option**

**Secure Mail - unrestricted**
- Better battery life on device
- Secured with MDX policies
- Supports client certificate authentication for security
- Integration with Citrix mobile productivity apps
- Standard user interface across platforms

**Secure Mail – tunneled to the internal network**
- Better battery life on device (with STA)
- Secured with MDX policies
- Support for client certificates
- Full control of app access
- Integration with Citrix mobile productivity apps
- Exchange ActiveSync/CAS is not exposed to the Internet
- Standard user interface across platforms

**Cons for each option**

**Secure Mail - unrestricted**
- Exchange ActiveSync/CAS exposed to the Internet
- Must account for user adoption

**Secure Mail – tunneled to the internal network**
- Additional overhead to the Citrix Gateway
- Must account for user adoption
- User must have an active session with Secure Hub to receive email updates
- Highly secure
- Requires user education for adoption

**Endpoint Management options and requirements**

**Endpoint Management connector for Exchange ActiveSync**
- Requires existing path to Exchange ActiveSync/Client Access Server (CAS)
- Requires EMDM Mgmt connector for each ActiveSync server

**Citrix Gateway connector for Exchange ActiveSync**
- Can leverage internal-only Exchange access
- Requires Citrix Gateway connector for each ActiveSync server and Citrix Gateway

**Native ActiveSync**
- Existing Exchange ActiveSync/CAS infrastructure
- Exchange ActiveSync/CAS must be externally accessible

**Pros for each option**

**Endpoint Management connector for Exchange ActiveSync**
- Ability to use native mail client
- Supports Microsoft Office 365
- Blacklist/whitelist access policies
- Can perform Exchange ActiveSync/CAS commands (full wipe, reset password, and so on)
- Can connect to BlackBerry BES and perform basic device controls
- Can filter Exchange ActiveSync access to non-EMM-managed devices

**Citrix Gateway connector for Exchange ActiveSync**
- Ability to use devices-native mail client
- Rule-based allow and deny modes
- Users Citrix Gateway as a reverse proxy
- More secure than EMDM Mgmt connector for each ActiveSync and external access to Exchange ActiveSync/CAS

**Native ActiveSync**
- Ability to use native mail client
- Basic Exchange ActiveSync/CAS device management capabilities

**Cons for each option**

**Endpoint Management connector for Exchange ActiveSync**
- Mail client not secured with MDX policies
- Requires Windows Server
- Requires PowerShell to schedule/invoke policies
- Limited control over devices
- May require Touchdown for some Android devices

**Citrix Gateway connector for Exchange ActiveSync**
- Mail client not secured with MDX policies
- Requires Windows Server
- Requires Citrix Gateway
- May require Touchdown for some Android devices

**Native ActiveSync**
- Mail client not secured with MDX policies
- Exposed Exchange ActiveSync/CAS
- Limited control over which devices users can connect

© 1999-2019 Citrix Systems, Inc. All rights reserved.
This article covers what to consider when planning how Endpoint Management is to integrate with your existing network and solutions. For example, if you’re already using Citrix Gateway for Citrix Virtual Apps and Desktops:

- Should you use the existing Citrix Gateway instance or a new, dedicated instance?
- Do you want to integrate with Endpoint Management the HDX apps that are published using StoreFront?
- Do you plan to use Citrix Files with Endpoint Management?
- Do you have a Network Access Control solution that you want to integrate into Endpoint Management?

**Citrix Gateway**

Citrix Gateway is required for Endpoint Management. Citrix Gateway provides a micro VPN path for access to all corporate resources and provides strong multi-factor authentication support.

You can use existing Citrix Gateway instances or set up new ones for Endpoint Management. The following sections note the advantages and disadvantages of using existing or new, dedicated Citrix Gateway instances.

**Shared Citrix Gateway MPX with a Citrix Gateway VIP created for Endpoint Management**

**Advantages:**

- Uses a common Citrix Gateway instance for all Citrix remote connections: Citrix Virtual Apps, full VPN, and clientless VPN.
- Uses the existing Citrix Gateway configurations, such as for certificate authentication and for accessing services like DNS, LDAP, and NTP.
- Uses a single Citrix Gateway platform license.

**Disadvantages:**

- It is more difficult to plan for scale when you handle two very different use cases on the same Citrix Gateway.
- Sometimes you need a specific Citrix Gateway version for a Citrix Virtual Apps use case. That same version might have known issues for Endpoint Management. Or Endpoint Management might have known issues for the Citrix Gateway version.
Citrix Endpoint Management

- If a Citrix Gateway exists, you cannot run the NetScaler for XenMobile wizard a second time to create the Citrix Gateway configuration for Endpoint Management.
- Except when Platinum licenses are used for Citrix Gateway 11.1 or later: User access licenses installed on Citrix Gateway and required for VPN connectivity are pooled. Because those licenses are available to all Citrix Gateway virtual servers, services other than Endpoint Management can potentially consume them.

Dedicated Citrix Gateway VPX/MPX instance

Advantages:

Citrix recommends using a dedicated instance of Citrix Gateway.

- Easier to plan for scale and separates Endpoint Management traffic from a Citrix Gateway instance that might already be resource constrained.
- Avoids issues when Endpoint Management and Citrix Virtual Apps need different Citrix Gateway software versions. The recommendation generally is to use the latest compatible Citrix Gateway version and build for Endpoint Management.
- Allows Endpoint Management configuration of Citrix Gateway through the built-in NetScaler for XenMobile wizard.
- Virtual and physical separation of services.

Disadvantages:

- Requires setup of extra services on Citrix Gateway to support Endpoint Management configuration.
- Requires another Citrix Gateway platform license. License each Citrix Gateway instance for Citrix Gateway.

For information about what to consider when integrating Citrix Gateway and Citrix ADC with each Endpoint Management server mode, see Integrating with Citrix Gateway and Citrix ADC.

StoreFront

If you have a Citrix Virtual Apps and Desktops environment, you can integrate HDX applications with Endpoint Management using StoreFront. When you integrate HDX apps with Endpoint Management:

- The apps are available to users who are enrolled with Endpoint Management.
- The apps display in the app store along with other mobile apps.
- Endpoint Management uses the legacy PNAgent (services) site on StoreFront.
- When the Citrix Workspace app is installed on a device, HDX apps start using that app.
Citrix Endpoint Management

StoreFront has a limitation of one services site per StoreFront instance. Suppose that you have multiple 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 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 Endpoint Management using the same Citrix Gateway.
- Use the same store or create a new one?
- 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 Endpoint Management

Advantages:

- Same store: No additional configuration of StoreFront is required for Endpoint Management, assuming that you use the same Citrix Gateway VIP for HDX access. Suppose that you choose to use the same store and want to direct Citrix Workspace access to a new Citrix Gateway VIP. In that case, add the appropriate Citrix 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 may adversely affect Endpoint Management as well.
- Same StoreFront server: In large environments, consider the additional load from Endpoint Management usage of PNAgent for app enumeration and start-up.

Use a new, dedicated StoreFront instance for integration with Endpoint Management

Advantages:

- New store: Any configuration changes of the StoreFront store for Endpoint Management should not affect existing Virtual Apps and Desktops workloads.
- New StoreFront server: Server configuration changes should not affect Virtual Apps and Desktops workflows. Additionally, load outside of Endpoint Management usage of PNAgent for app enumeration and launch should not affect scalability.

Disadvantages:
Citrix Endpoint Management

- New store: StoreFront store configuration.
- New StoreFront server: Requires new StoreFront installation and configuration.

For more information, see Citrix Virtual Apps and Desktops through the app store.

Citrix Content Collaboration and Citrix Files

Citrix Content Collaboration 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.

Integration of Citrix Content Collaboration with Endpoint Management differs depending on whether your site is Workspace-enabled.

If Endpoint Management is Workspace-enabled

When using Citrix Workspace and Citrix Workspace app along with the Citrix Content Collaboration service, you can:

- Access all of your files from the Files tab in Citrix Workspace.
- View all your Favorites, Personal and Shared Folders, and access your cloud connectors.
- Submit files for Feedback and Approval, view your File Box, manage your Recycle Bin, and edit files.
- For information about Citrix Collaboration features not supported in Workspace, see Deploy and Create or link a Content Collaboration (ShareFile) account to Citrix Cloud.

If Endpoint Management isn’t Workspace-enabled

If Endpoint Management isn’t Workspace-enabled, you integrate Content Collaboration with Endpoint Management. 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 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 Endpoint Management console to configure the integration with Enterprise accounts or storage zone connectors. For more information, see Citrix Files for Endpoint Management.

The following sections note the questions to ask when making design decisions for Citrix Files.

**Integrate with Citrix Files or only storage zone connectors**

**Questions to ask:**

- Do you need 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 Endpoint Management complies with 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.
- Due to storage zone connector communication with internal resources such as file repositories, CIFS shares, and SharePoint: Citrix recommends that storage zones controllers reside in the internal network behind DMZ firewalls and fronted by Citrix Gateway.

**SAML integration with Endpoint Management Enterprise**

**Questions to ask:**
- Is Active Directory authentication required for Citrix Files?
- Does first time use of the Citrix Files app for Endpoint Management require SSO?
- Is there a standard IdP in your current environment?
- How many domains are required to use SAML?
- Are there multiple email aliases for Active Directory users?
- Are there any Active Directory domain migrations in progress or scheduled soon?

**Design decision:**
Endpoint Management Enterprise environments may choose to use SAML as the authentication mechanism for Citrix Files. The authentication options are:
- Use the Endpoint Management server as the Identity Provider (IdP) for SAML
  - This option can provide excellent user experience and automate Citrix Files account creation, as well as enable mobile app SSO features.
    - The Endpoint Management server is enhanced for this process: It does not require the synchronization of 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 may also provide SSO capabilities on the Windows client side. Be sure to evaluate use cases before choosing your Citrix Files SAML IdP.
Additionally, to satisfy both use cases, you can Configure and ADFS and Endpoint Management as a Dual IdP.

Mobile apps

Questions to ask:
- 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 obtain wrapped apps from the Citrix downloads page.
- If security is low and you don’t require containerization, the public Citrix Files application may not be suitable. In an MDM-only environment, you can deliver the MDM version of the Citrix Files app using Endpoint Management in MDM mode.
- For more information, see Apps and Citrix Files for 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 and device security. For information, see Employee Permissions and Managing Devices and Apps.
- Some Citrix Files device security settings and MDX policies control the same features. In those cases, 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 Endpoint Management, the external apps get disabled in Citrix Files. You can configure the apps so that Endpoint Management doesn’t require a PIN/passcode, but the Citrix Files app requires a PIN/passcode.

Standard vs. 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.

Access control

Enterprises can now manage mobile devices inside and outside of networks. Enterprise Mobility Management solutions such as Endpoint Management are great at providing security and controls for mobile devices, independent of location. However, when coupled 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 Endpoint Management device security assessment through your NAC solution. Your NAC solution then can use the Endpoint Management security assessment to facilitate and handle authentication decisions. Citrix has validated NAC integration with Endpoint Management for Cisco Identity Services Engine (ISE) or ForeScout. Citrix doesn’t guarantee integration for other NAC solutions.

Advantages of a NAC solution integration with 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 attempt to connect to your network.
  - Query Endpoint Management for device attributes.
  - Then use that information to determine whether to allow, block, limit, or redirect those devices. Those decisions depend on the security policies 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 Endpoint Management, see Network Access Control.

Integrating with Citrix Gateway and Citrix ADC

July 29, 2019

When integrated with Endpoint Management, Citrix Gateway provides an authentication mechanism for remote device access to the internal network for MAM devices. The integration enables Citrix mo-
Citrix Endpoint Management

Bible productivity apps to connect to corporate servers in the intranet through a micro VPN. Endpoint Management creates a micro VPN from the apps on the device to Citrix Gateway.

Citrix Cloud Operations manages Citrix ADC load balancing.

**Integration requirements for Endpoint Management server modes**

The integration requirements for Citrix Gateway and Citrix ADC differ based on the Endpoint Management server modes: MAM and MDM+MAM, also called ENT (enterprise).

**MAM**

With the Endpoint Management server in MAM mode:

- Citrix Gateway is required. Citrix Gateway provides a micro VPN path for access to all corporate resources and provides strong multifactor authentication support.

**MDM+MAM (ENT)**

With the Endpoint Management server in MDM+MAM mode:

- Citrix Gateway is required. Citrix Gateway provides a micro VPN path for access to all corporate resources and provides strong multifactor authentication support.

- When the Endpoint Management server mode is MDM+MAM and a user opts out of MDM enrollment, devices enroll using the Citrix Gateway FQDN.

**Design Decisions**

The following sections summarize the many design decisions to consider when planning a Citrix Gateway integration with Endpoint Management.

**Certificates**

Decision detail:

- Do you require a higher degree of security for enrollments and access to the Endpoint Management environment?
- Is LDAP not an option?
Citrix Endpoint Management

Design guidance:

The default configuration for Endpoint Management is user name and password authentication. To add another layer of security for enrollment and access to 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 Endpoint Management. Users then enroll using a unique PIN that Endpoint Management generates for them. After a user has access, Endpoint Management creates and deploys the certificate later used to authenticate to the Endpoint Management environment.

Endpoint Management supports Certificate Revocation List (CRL) only for a third party Certificate Authority. If you have a Microsoft CA configured, Endpoint Management uses Citrix Gateway to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the Citrix Gateway Certificate Revocation List (CRL) setting, Enable CRL Auto Refresh. This step ensures that the user of a device in MAM-only mode can’t authenticate using an existing certificate on the device. 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 Citrix Gateway VIPs

Decision detail:

- Do you currently use Citrix Gateway for Citrix Virtual Apps and Desktops?
- Will Endpoint Management use the same Citrix Gateway as Citrix Virtual Apps and Desktops?
- What are the authentication requirements for both traffic flows?

Design guidance:

When your Citrix environment includes Endpoint Management, plus Virtual Apps and Desktops, you can use the same Citrix Gateway virtual server for both. Due to potential versioning conflicts and environment isolation, a dedicated Citrix Gateway is recommended for each Endpoint Management environment.

If you use LDAP authentication, Citrix Workspace and Secure Hub can authenticate to the same Citrix Gateway with no issues. If you use certificate-based authentication, Endpoint Management pushes a certificate in the MDX container and Secure Hub uses the certificate to authenticate with Citrix Gateway. The Workspace app is separate from Secure Hub and can’t use the same certificate as Secure Hub to authenticate to the same Citrix Gateway.

You might consider this work around, which allows you to use the same FQDN for two Citrix Gateway VIPs. You can create two Citrix Gateway VIPs with the same IP address. The one for 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.

Citrix Gateway time-outs

Decision detail:

• How do you want to configure the Citrix Gateway time-outs for Endpoint Management traffic?

Design guidance:

Citrix 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, Citrix Gateway, and for accessing applications while offline.

Enrollment FQDN

Important:

To change the enrollment FQDN requires a new SQL Server database and Endpoint Management server rebuild.

Secure Web traffic

Decision detail:

• Will you restrict Secure Web to internal web browsing only?
• Will you enable Secure Web for both internal and external web browsing?

Design guidance:

If you will use Secure Web for internal web browsing only, Citrix Gateway configuration is straightforward. However, if Secure Web can’t reach all internal sites by default, you might need to configure firewalls and proxy servers.

If you will use 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 Secure Web connections to come back to Citrix Gateway, go through a proxy server, and then go out to Internet. By default, Secure Web access tunnels to the internal network. Secure Web uses a per-application VPN tunnel back to the internal network for all network access and Citrix Gateway uses split tunnel settings.

For a discussion of Secure Web connections, see Configuring User Connections.
Push Notifications for Secure Mail

Decision detail:

- Will you use push notifications?

Design guidance for iOS:

If your Citrix Gateway configuration includes Secure Ticket Authority (STA) and split tunneling is off: Citrix Gateway must allow traffic from Secure Mail to the Citrix listener service URLs. Those URLs are specified in push notifications for Secure Mail for iOS.

Design guidance for Android:

Use Firebase Cloud Messaging (FCM) to control how and when Android devices need to connect to Endpoint Management. With FCM configured, any security action or deploy command triggers a push notification to Secure Hub to prompt the user to reconnect to the Endpoint Management server.

HDX STAs

Decision detail:

- What STAs to use if you will 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 Citrix Content Collaboration

Decision detail:

- Will you use storage zones controller in the environment?
  - What Citrix Files VIP URL will you use?

Design guidance:

If you will include storage zones controller in your environment, ensure 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 Endpoint Management as the SAML IdP?

**Design guidance:**
The recommended best practice is to integrate Citrix Files with Endpoint Management, a simpler alternative to configuring SAML-based federation. 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 Endpoint Management console enables you to perform Citrix Files configuration and to monitor service levels and license usage.

There are two types of Citrix Files clients: Citrix Files for 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 Endpoint Management Clients differ from Citrix Files mobile clients](#).

You can configure Endpoint Management and Citrix Files to use SAML to provide SSO access to:
- Citrix Files mobile apps you wrap with the MDX Service
- Non-wrapped Citrix Files clients, such as the website, Outlook plug-in, or sync clients

If you want to use Endpoint Management as the SAML IdP for Citrix Files, ensure 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, Endpoint Management uses Citrix Gateway to provide secure access to resources outside of the local network. For configuration details, see [ShareConnect](#).

**Enrollment FQDN for each deployment type**
Citrix Endpoint Management

<table>
<thead>
<tr>
<th>Deployment type</th>
<th>Enrollment FQDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDM+MAM with mandatory MDM enrollment</td>
<td>Endpoint Management server FQDN</td>
</tr>
<tr>
<td>MDM+MAM with optional MDM enrollment</td>
<td>Endpoint Management server FQDN or Citrix Gateway FQDN</td>
</tr>
<tr>
<td>MAM-only</td>
<td>Endpoint Management server FQDN</td>
</tr>
<tr>
<td>MAM-only (legacy)</td>
<td>Citrix Gateway FQDN</td>
</tr>
</tbody>
</table>

**Deployment Summary**

Citrix recommends that you use the NetScaler for XenMobile wizard to ensure proper configuration. Be aware that you can use the wizard only one time. If you have multiple Endpoint Management instances, such as for test, development, and production environments, you must configure Citrix Gateway for the additional environments manually. When you have a working environment, take note of the settings before attempting to configure Citrix Gateway manually for Endpoint Management.

The key decision you make when using the wizard is whether to use HTTPS or HTTP for communication to the Endpoint Management server. HTTPS provides secure back-end communication, as traffic between Citrix Gateway and Endpoint Management is encrypted. The re-encryption impacts Endpoint Management server performance. HTTP provides better Endpoint Management server performance. Traffic between Citrix Gateway and Endpoint Management is not encrypted. The following tables show the HTTP and HTTPS port requirements for Citrix Gateway and Endpoint Management server.

**HTTPS**

Citrix typically recommends SSL Bridge for Citrix Gateway MDM virtual server configurations. For Citrix Gateway SSL Offload use with MDM virtual servers, Endpoint Management supports only port 80 as the back-end service.

<table>
<thead>
<tr>
<th>Deployment type</th>
<th>Citrix Gateway load balancing method</th>
<th>SSL re-encryption</th>
<th>Endpoint Management server port</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAM</td>
<td>SSL Offload</td>
<td>Enabled</td>
<td>8443</td>
</tr>
<tr>
<td>MDM+MAM</td>
<td>MDM: SSL Bridge</td>
<td>N/A</td>
<td>443, 8443</td>
</tr>
<tr>
<td>MDM+MAM</td>
<td>MAM: SSL Offload</td>
<td>Enabled</td>
<td>8443</td>
</tr>
</tbody>
</table>
HTTP

<table>
<thead>
<tr>
<th>Deployment type</th>
<th>Citrix Gateway load balancing method</th>
<th>SSL re-encryption</th>
<th>Endpoint Management server port</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAM</td>
<td>SSL Offload</td>
<td>Enabled</td>
<td>8443</td>
</tr>
<tr>
<td>MDM+MAM</td>
<td>MDM: SSL Offload</td>
<td>Not supported</td>
<td>80</td>
</tr>
<tr>
<td>MDM+MAM</td>
<td>MAM: SSL Offload</td>
<td>Enabled</td>
<td>8443</td>
</tr>
</tbody>
</table>

For diagrams of Citrix Gateway in Endpoint Management deployments, see Architecture.

SSO and proxy considerations for MDX apps

September 24, 2019

Endpoint Management integration with Citrix Gateway enables you to provide users with single sign-on (SSO) to all backend HTTP/HTTPS resources. Depending on your SSO authentication requirements, you can configure user connections for an MDX app to use either of these options:

- Secure Browse (Tunneled - Web SSO), which is a type of clientless VPN
- Full VPN Tunnel

Important:

The MDX Toolkit version 18.12.0 release included new policies that combined or replaced older policies.

The Network Access policy combines Network access, Preferred VPN mode, and Permit VPN mode switching. The Exclusion list policy replaces Split tunnel exclusion list. The micro VPN session required policy replaces micro VPN session required. For details, see What’s new in the MDX Toolkit 18.12.0.

Tunneled - Web SSO is the name for Secure Browse in the settings. The behavior is the same.

If Citrix 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 Secure Web. The concepts apply to other MDX apps.

The following flow chart summarizes the decision flow for SSO and user connections.
Citrix Endpoint Management

Citrix Gateway authentication methods

This section provides general information about the authentication methods supported by Citrix Gateway.

SAML authentication

When you configure Citrix Gateway for Security Assertion Markup Language (SAML), users can connect to web apps that support the SAML protocol for single sign-on. Citrix Gateway supports the identity provider (IdP) single sign-on for SAML web apps.

Required configuration:
  • Configure SAML SSO in the Citrix Gateway Traffic profile.
  • Configure the SAML IdP for the requested service.

NTLM authentication

If SSO to web apps is enabled in the session profile, Citrix Gateway performs NTLM authentication automatically.

Required configuration:
  • Enable SSO in the Citrix Gateway Session or Traffic profile.

Kerberos impersonation

Endpoint Management supports Kerberos for Secure Web only. When you configure Citrix Gateway for Kerberos SSO, Citrix Gateway uses impersonation when a user password is available to Citrix Gateway. Impersonation means that Citrix Gateway uses user credentials to get the ticket required to gain access to services, such as Secure Web.

Required configuration:
  • Configure the Citrix Gateway “Worx” Session policy to allow it to identify the Kerberos Realm from your connection.
  • Configure a Kerberos Constrained Delegation (KCD) account on Citrix Gateway. Configure that account with no password and bind it to a traffic policy on your Endpoint Management gateway.
  • For those and other configuration details, see the Citrix blog: WorxWeb and Kerberos Impersonation SSO.
Kerberos Constrained Delegation

Endpoint Management supports Kerberos for Secure Web only. When you configure Citrix Gateway for Kerberos SSO, Citrix Gateway uses constrained delegation when a user password is not available to Citrix Gateway.

With constrained delegation, Citrix Gateway uses a specified administrator account to get tickets on behalf of users and services.

Required configuration:

• Configure a KCD account in Active Directory with the required permissions and a KDC account on Citrix Gateway.
• Enable SSO in the Citrix Gateway Traffic profile.
• Configure the back-end website for Kerberos authentication.
• For those and other configuration details, see the Citrix blog, Configuring Kerberos Single Sign-on for WorxWeb.

Form Fill Authentication

When you configure Citrix 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 Tunneled - Web SSO or Full VPN modes.

Required configuration:

• Configure Form-based SSO in the Citrix Gateway Traffic profile.

Digest HTTP authentication

If you enable SSO to web apps in the session profile, Citrix Gateway performs digest HTTP authentication automatically. This authentication method applies to apps that use Tunneled - Web SSO or Full VPN modes.

Required configuration:

• Enable SSO in the Citrix Gateway Session or Traffic profile.

Basic HTTP authentication

If you enable SSO to web apps in the session profile, Citrix Gateway performs basic HTTP authentication automatically. This authentication method applies to apps that use Tunneled - Web SSO or Full VPN modes.

Required configuration:
Enable SSO in the Citrix Gateway Session or Traffic profile.

**Secure Tunneled - Web SSO, Full VPN Tunnel, or Full VPN Tunnel with PAC**

The following sections describe the user connection types for Secure Web.

**Full VPN Tunnel**

Connections that tunnel to the internal network can use a full VPN tunnel. Use the Secure Web Preferred VPN mode policy to configure full VPN tunnel. Citrix recommends Full VPN tunnel for connections that use client certificates or end-to-end SSL to a resource in the internal network. Full VPN tunnel handles any protocol over TCP. You can use full VPN tunnel with Windows, Mac, iOS, and Android devices.

In Full VPN Tunnel mode, Citrix Gateway does not have visibility inside an HTTPS session.

**Tunneled - Web SSO**

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 Secure Web Preferred VPN mode policy. Citrix recommends Tunneled - Web SSO for connections that require single sign-on (SSO).

In Tunneled - Web SSO mode, Citrix Gateway breaks the HTTPS session into two parts:

- From the client to Citrix Gateway
- From Citrix Gateway to the back-end resource server.

In this manner, Citrix Gateway has full visibility into all transactions between the client and server, enabling it to provide SSO.

You can also configure proxy servers for Secure Web when used in Tunneled - Web SSO mode. For details, see the blog [Endpoint Management WorxWeb Traffic Through Proxy Server in Secure Browse Mode](#).

**Full VPN Tunnel with PAC**

You can use a Proxy Automatic Configuration (PAC) file with a full VPN tunnel deployment for Secure Web on iOS and Android devices. Endpoint Management supports proxy authentication provided by Citrix Gateway. A PAC file contains 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. Secure Web parses PAC
file rules and sends the proxy server information to Citrix Gateway. Citrix Gateway is unaware of the PAC file or proxy server.

For authentication to HTTPS websites: The Secure Web MDX policy, Enable web password caching, enables Secure Web to authenticate and provide SSO to the proxy server through MDX.

**Citrix Gateway Split Tunneling**

When planning your SSO and proxy configuration, you must also decide whether to use Citrix Gateway split tunneling. Citrix recommends that you use Citrix Gateway split tunneling only if needed. This section provides a high-level look at how split tunneling works: Citrix Gateway determines the traffic path based on its routing table. When Citrix Gateway split tunneling is on, Secure Hub distinguishes internal (protected) network traffic from Internet traffic. Secure Hub makes that determination based on the DNS suffix and Intranet applications. Secure Hub then tunnels only the internal network traffic through the VPN tunnel. When Citrix Gateway split tunneling is off, all traffic goes through the VPN tunnel.

- If you prefer to monitor all the traffic due to security considerations, turn off Citrix Gateway split tunneling. As a result, all traffic goes through the VPN tunnel.
- If you use Full VPN Tunnel with PAC, you must disable Citrix Gateway split tunneling. If split tunneling is on and you configure a PAC file, the PAC file rules override the Citrix Gateway split tunneling rules. A proxy server configured in a traffic policy does not override Citrix Gateway split tunneling rules.

By default, the **Network access** policy is set to **Tunneled to the internal network** for Secure Web. With that configuration, MDX apps use Citrix Gateway split tunnel settings. The **Network access** policy default differs for some other Citrix mobile productivity apps.

Citrix 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 Citrix Gateway. Instead, those addresses are sent by using the device internet connection. For more information about reverse split tunneling, see the Citrix Gateway documentation.

Endpoint Management includes a **Reverse split tunnel exclusion list**. To prevent certain websites from tunneling through Citrix Gateway: Add a comma-separated list of fully qualified domain names (FQDN) or DNS suffixes that connect by using the local area network (LAN) instead. This list applies only to Tunneled - Web SSO mode with Citrix Gateway configured for reverse split tunneling.

**Authentication**

April 25, 2019
In an Endpoint Management deployment, several considerations come into play when deciding how to configure authentication. This section will help you understand the various factors that affect authentication by discussing the following:

- The main MDX policies, Endpoint Management client properties and Citrix 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. By reviewing the three recommended configurations, you should gain a greater understanding of the interplay of authentication measures available to you, and how to best deploy your own Endpoint Management environment.

**Authentication Modes**

**Online authentication:** Allows users into the 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.

**Methods of Authentication**

**Single Factor**

**LDAP:** You can configure a connection in Endpoint Management to one or more directories, such as Active Directory that are compliant with the Lightweight Directory Access Protocol (LDAP). This is a commonly used method 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 while still providing the security of complex passwords on enrollment, password expiration, and account lockout.

For more details, see [Domain or domain plus STA](#).

**Client certificate:** Endpoint Management can integrate with industry-standard certificate authorities to use certificates as the sole method of online authentication. 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.
Endpoint Management supports Certificate Revocation List (CRL) only for a third-party Certificate Authority. If you have a Microsoft CA configured, Endpoint Management uses Citrix Gateway to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the Citrix Gateway Certificate Revocation List (CRL) setting, Enable CRL Auto Refresh. This step ensures that the user of a device in MAM-only mode can’t authenticate using an existing certificate on the device; Endpoint Management re-issues 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 if you plan to use certificate-based authentication for users or if you need to use your enterprise Certificate Authority (CA) for issuing device certificates, see Architecture.

Two Factor

**LDAP + Client Certificate:** In the Endpoint Management environment, this configuration is the best combination of security and user experience, with the best SSO possibilities coupled with security provided by two-factor authentication at Citrix Gateway. Using both LDAP and client certificate provides security with both something users know (their Active Directory passwords) and something they have (client certificates on their devices). Secure Mail (and some other Citrix mobile productivity apps) can automatically configure and provide a seamless first-time user experience with client certificate authentication, with a properly configured Exchange client access server environment. For optimal usability, you can combine this option with Citrix PIN and Active Directory password caching.

**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 Involved in 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 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.
If you select Secure offline for the Encryption keys policy, this policy is automatically enabled.

**micro VPN session required:** If **On**, the user must have a connection to the enterprise network and an active session in order to access the app on the device. If **Off**, an active session is not required to access the app on the device. Default is **Off**.

**Maximum offline period (hours):** Defines the maximum period an app can run without reconfirming app entitlement and refreshing policies from Endpoint Management. When you set the Maximum offline period, if Secure Hub for iOS has a valid Citrix Gateway token, the app retrieves new policies for MDX apps from Endpoint Management without any interruption to users. If Secure Hub does not have a valid Citrix Gateway token, users must authenticate through Secure Hub in order for app policies to update. The Citrix Gateway token may become invalid due to a Citrix Gateway session inactivity or a forced session time-out policy. When users sign on to 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)**. Minimum period is 1 hour.

**Background services ticket expiration:** The time period that a background network service ticket remains valid. When Secure Mail connects through Citrix Gateway to an Exchange Server running ActiveSync, Endpoint Management issues a token that Secure Mail uses to connect to the internal Exchange Server. This property setting determines the duration that 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 will discontinue.

**micro VPN session required grace period:** Determines how many minutes a user can use the app offline before the micro VPN session required policy prevents them from further use (until the online session is validated). Default is 0 (no grace period).

For more information about MDX Toolkit authentication policies, see [Endpoint Management MDX Policies for iOS](#) and [Endpoint Management MDX Policies for Android](#).

**Endpoint Management client properties**

**Note:**

Client properties are a global setting that apply to all devices that connect to Endpoint Manage-
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 Endpoint Management console. 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. You should enable this setting if ENABLE_PASSWORD_CACHING is enabled or if Endpoint Management is using certificate authentication.

Possible values: true or false

Default value: false

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 are 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...
Secure Hub to perform 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 will still require 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

### Citrix Gateway Settings

**Session time-out:** If you enable this setting, Citrix Gateway disconnects the session if Citrix Gateway detects no network activity for the specified interval. This setting is enforced for users who connect with the Citrix Gateway Plug-in, Citrix Workspace, 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, Citrix Gateway disconnects the session after the time-out interval elapses no matter what the user is doing. When the time-out interval elapses, there is no action the user can take to prevent the disconnection. This setting is enforced for users who connect with the Citrix Gateway Plug-in, Citrix Workspace, Secure Hub, or through a web browser. If Secure Mail is using STA, a special Citrix Gateway mode, the Forced time-out setting does not apply to Secure Mail sessions. Default is no value, which means sessions will be extended if there's any activity.

For more information about time-out settings in Citrix Gateway, see the Citrix Gateway documentation.

For more information on the scenarios that prompt users to authenticate with 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, by the MDX Service or MDX Toolkit, and in the Endpoint Management console.
### Recommended Configurations

This section gives examples of three Endpoint Management configurations that range from lowest security and optimal user experience, to the highest security and more intrusive user experience. These examples should provide you with helpful reference points to determine where on the scale you want to place your own configuration. Be aware that modifying these settings may require you to alter other settings as well. For instance, the maximum offline period should always be less than the session time-out.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Where to Find the Setting</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session time-out</td>
<td>Citrix Gateway</td>
<td>1440 minutes</td>
</tr>
<tr>
<td>Forced time-out</td>
<td>Citrix Gateway</td>
<td>No value (off)</td>
</tr>
<tr>
<td>Maximum offline period</td>
<td>MDX Policies</td>
<td>72 hours</td>
</tr>
<tr>
<td>Background services ticket</td>
<td>MDX Policies</td>
<td>168 hours (7 days)</td>
</tr>
<tr>
<td>expiration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>micro VPN session required</td>
<td>MDX Policies</td>
<td>Off</td>
</tr>
<tr>
<td>micro VPN session required grace period</td>
<td>MDX Policies</td>
<td>0</td>
</tr>
<tr>
<td>App passcode</td>
<td>MDX Policies</td>
<td>On</td>
</tr>
<tr>
<td>Encrypt secrets using passcode</td>
<td>Endpoint Management client properties</td>
<td>false</td>
</tr>
<tr>
<td>Enable Citrix PIN Authentication</td>
<td>Endpoint Management client properties</td>
<td>false</td>
</tr>
<tr>
<td>PIN Strength Requirement</td>
<td>Endpoint Management client properties</td>
<td>Medium</td>
</tr>
<tr>
<td>PIN Type</td>
<td>Endpoint Management client properties</td>
<td>Numeric</td>
</tr>
<tr>
<td>Enable User Password Caching</td>
<td>Endpoint Management client properties</td>
<td>false</td>
</tr>
<tr>
<td>Inactivity Timer</td>
<td>Endpoint Management client properties</td>
<td>15</td>
</tr>
<tr>
<td>Enable Touch ID Authentication</td>
<td>Endpoint Management client properties</td>
<td>false</td>
</tr>
</tbody>
</table>
### Highest Security

This configuration offers the highest level of security but contains significant usability trade-offs.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Where to Find the Setting</th>
<th>Recommended Setting</th>
<th>Behavior Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session time-out</td>
<td>Citrix Gateway</td>
<td>1440</td>
<td>Users enter their Secure Hub credentials only when online authentication is required—every 24 hours.</td>
</tr>
<tr>
<td>Forced time-out</td>
<td>Citrix Gateway</td>
<td>No value</td>
<td>Sessions will be extended if there's any activity.</td>
</tr>
<tr>
<td>Maximum offline period</td>
<td>MDX Policies</td>
<td>23</td>
<td>Requires policy refresh every day.</td>
</tr>
<tr>
<td>Background services ticket expiration</td>
<td>MDX Policies</td>
<td>72 hours</td>
<td>Time out for STA, which allows for long-lived sessions without a Citrix Gateway session token. In the case of Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop without prompting the user if they don’t open the app before the session expires.</td>
</tr>
<tr>
<td>micro VPN session required</td>
<td>MDX Policies</td>
<td>Off</td>
<td>Ensures a valid network connection and Citrix Gateway session to use apps.</td>
</tr>
<tr>
<td>Feature</td>
<td>Policy</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>micro VPN session required grace period</td>
<td>MDX Policies</td>
<td>0</td>
<td>No grace period (if you enabled micro VPN session required).</td>
</tr>
<tr>
<td>App passcode</td>
<td>MDX Policies</td>
<td>On</td>
<td>Require passcode for application.</td>
</tr>
<tr>
<td>Encrypt secrets using passcode</td>
<td>Endpoint</td>
<td>true</td>
<td>A key derived from user entropy protects the vault.</td>
</tr>
<tr>
<td>Enable Citrix PIN Authentication</td>
<td>Endpoint</td>
<td>true</td>
<td>Enable Citrix PIN for simplified authentication experience.</td>
</tr>
<tr>
<td>PIN Strength Requirement</td>
<td>Endpoint</td>
<td>Strong</td>
<td>High password complexity requirements.</td>
</tr>
<tr>
<td>PIN Type</td>
<td>Endpoint</td>
<td>Alphanumeric</td>
<td>PIN is an alphanumeric sequence.</td>
</tr>
<tr>
<td>Enable Password Caching</td>
<td>Endpoint</td>
<td>false</td>
<td>Active Directory password is not cached and Citrix PIN will be used for offline authentications.</td>
</tr>
<tr>
<td>Inactivity Timer</td>
<td>Endpoint</td>
<td>15</td>
<td>If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.</td>
</tr>
<tr>
<td>Enable Touch ID Authentication</td>
<td>Endpoint</td>
<td>false</td>
<td>Disables Touch ID for offline authentication use cases in iOS.</td>
</tr>
</tbody>
</table>
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, ensuring data security when devices aren’t in use.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Where to Find the Setting</th>
<th>Recommended Setting</th>
<th>Behavior Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session time-out</td>
<td>Citrix Gateway</td>
<td>4320</td>
<td>Users enter their Secure Hub credentials only when online authentication is required - every 3 days</td>
</tr>
<tr>
<td>Forced time-out</td>
<td>Citrix Gateway</td>
<td>No value</td>
<td>Sessions will be extended if there's any activity.</td>
</tr>
<tr>
<td>Maximum offline period</td>
<td>MDX Policies</td>
<td>71</td>
<td>Requires policy refresh every 3 days. The hour difference is to allow for refresh ahead of session time-out.</td>
</tr>
<tr>
<td>Feature</td>
<td>Setting</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Background services ticket expiration</td>
<td>MDX Policies</td>
<td>168 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Time out for STA, which allows for long-lived sessions without a Citrix Gateway session token. In the case of Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop without prompting the user if they don’t open the app before the session expires.</td>
<td></td>
</tr>
<tr>
<td>micro VPN session required</td>
<td>MDX Policies</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensures a valid network connection and Citrix Gateway session to use apps.</td>
<td></td>
</tr>
<tr>
<td>micro VPN session required grace period</td>
<td>MDX Policies</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No grace period (if you enabled micro VPN session required).</td>
<td></td>
</tr>
<tr>
<td>App passcode</td>
<td>MDX Policies</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Require passcode for application.</td>
<td></td>
</tr>
<tr>
<td>Encrypt secrets using passcode</td>
<td>Endpoint Management client properties</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not require user entropy to encrypt the vault.</td>
<td></td>
</tr>
<tr>
<td>Enable Citrix PIN Authentication</td>
<td>Endpoint Management client properties</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable Citrix PIN for simplified authentication experience.</td>
<td></td>
</tr>
<tr>
<td>PIN Strength Requirement</td>
<td>Endpoint Management client properties</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enforces medium password complexity rules.</td>
<td></td>
</tr>
<tr>
<td>PIN Type</td>
<td>Endpoint Management client properties</td>
<td>Numeric</td>
<td>PIN is a numeric sequence.</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------</td>
<td>---------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Enable Password Caching</td>
<td>Endpoint Management client properties</td>
<td>true</td>
<td>The user PIN caches and protects the Active Directory password.</td>
</tr>
<tr>
<td>Inactivity Timer</td>
<td>Endpoint Management client properties</td>
<td>30</td>
<td>If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.</td>
</tr>
<tr>
<td>Enable Touch ID Authentication</td>
<td>Endpoint Management client properties</td>
<td>true</td>
<td>Enables Touch ID for offline authentication use cases in iOS.</td>
</tr>
</tbody>
</table>

**High Security**

This configuration, the most convenient to users, provides base-level security.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Where to Find the Setting</th>
<th>Recommended Setting</th>
<th>Behavior Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session time-out</td>
<td>Citrix Gateway</td>
<td>10080</td>
<td>Users enter their Secure Hub credentials only when online authentication is required - every 7 days</td>
</tr>
<tr>
<td>Forced time-out</td>
<td>Citrix Gateway</td>
<td>No value</td>
<td>Sessions will be extended if there's any activity.</td>
</tr>
<tr>
<td>Feature</td>
<td>Setting</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum offline period</td>
<td>MDX Policies</td>
<td>167</td>
<td>Requires policy refresh every week (every 7 days). The hour difference is to allow for refresh ahead of session time-out.</td>
</tr>
<tr>
<td>Background services ticket expiration</td>
<td>MDX Policies</td>
<td>240</td>
<td>Time out for STA, which allows for long-lived sessions without a Citrix Gateway session token. In the case of Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop without prompting the user if they don’t open the app before the session expires.</td>
</tr>
<tr>
<td>micro VPN session required</td>
<td>MDX Policies</td>
<td>Off</td>
<td>Ensures a valid network connection and Citrix Gateway session to use apps.</td>
</tr>
<tr>
<td>micro VPN session required grace period</td>
<td>MDX Policies</td>
<td>0</td>
<td>No grace period (if you enabled micro VPN session required).</td>
</tr>
<tr>
<td>App passcode</td>
<td>MDX Policies</td>
<td>On</td>
<td>Require passcode for application.</td>
</tr>
<tr>
<td>Encrypt secrets using passcode</td>
<td>Endpoint</td>
<td>false</td>
<td>Do not require user entropy to encrypt the vault.</td>
</tr>
<tr>
<td></td>
<td>Management client properties</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Citrix Endpoint Management

<table>
<thead>
<tr>
<th>Feature</th>
<th>Endpoint Management client properties</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Citrix PIN Authentication</td>
<td></td>
<td>true</td>
<td>Enable Citrix PIN for simplified authentication experience.</td>
</tr>
<tr>
<td>PIN Strength Requirement</td>
<td></td>
<td>Low</td>
<td>No password complexity requirements</td>
</tr>
<tr>
<td>PIN Type</td>
<td></td>
<td>Numeric</td>
<td>PIN is a numeric sequence.</td>
</tr>
<tr>
<td>Enable Password Caching</td>
<td></td>
<td>true</td>
<td>The user PIN caches and protects the Active Directory password.</td>
</tr>
<tr>
<td>Inactivity Timer</td>
<td></td>
<td>90</td>
<td>If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.</td>
</tr>
<tr>
<td>Enable Touch ID Authentication</td>
<td></td>
<td>true</td>
<td>Enables Touch ID for offline authentication use cases in iOS.</td>
</tr>
</tbody>
</table>

#### Using Step-Up Authentication

Some apps may 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 Citrix Gateway appliances).
If a user opens an app that logs on to the alternate Citrix Gateway instance, all other apps will use that Citrix Gateway instance for communicating with the internal network. The session will only switch back to the lower security Citrix Gateway instance when the session times out from the Citrix Gateway instance with enhanced security.

**Using micro VPN session required**

For certain applications, such as Secure Web, you may want to ensure that users run an app only when they have an authenticated session and while the device is connected to a network. This policy enforces that option and allows for a grace period so users can finish their work.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Where to Find the Setting</th>
<th>Recommended Setting</th>
<th>Behavior Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>micro VPN session required</td>
<td>MDX Policies</td>
<td>On</td>
<td>Ensures device is online and has a valid authentication token.</td>
</tr>
<tr>
<td>micro VPN session required grace period</td>
<td>MDX Policies</td>
<td>15</td>
<td>Allows a 15-minute grace period before the user can no longer use apps</td>
</tr>
</tbody>
</table>

**Server properties**

November 21, 2019

Server properties are global properties that apply to operations, users, and devices across an en-
Citrix Endpoint Management

tire 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.

Server Property Definitions

Access all apps in the managed Google Play store

• If true, Endpoint Management makes all apps from the public Google Play store accessible from the managed Google Play store. Setting this property to true whitelists the public Google Play store apps for all Android Enterprise users. Administrators can then use the Restrictions device policy to control access to these apps. Defaults to false.

Add Device Always

• If true, Endpoint Management adds a device to the Endpoint Management console, even if it fails enrollment. As a result, you can see which devices attempted to enroll. Defaults to false.

AG Client Cert Issuing Throttling Interval

• The grace period between generating certificates. This interval prevents Endpoint Management from generating multiple certificates for a device in a short time period. Citrix recommends that you don’t change this value. Defaults to 30 minutes.

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 true, Endpoint Management blocks enrollments for rooted Android devices and jailbroken iOS devices. Recommended setting is true for all security levels. Defaults to true.

Certificate Renewal in Seconds

• The number of seconds before a certificate expires that Endpoint Management starts to renew certificates. For example, if a certificate will expire December 30 and this property is set to 30
days: If the device connects between December 1 and December 30, Endpoint Management attempts to renew the certificate. Defaults to 2592000 seconds (30 days).

Connection Timeout

• The session inactivity timeout, in minutes, after which Endpoint Management closes the TCP connection to a device. The session remains open. Applies to Android and Windows CE devices. Defaults to 5 minutes.

Default deployment channel

• Determines how Endpoint Management deploys a resource to a device: At the user-level (DEFAULT_TO_USER) or device-level. Defaults to DEFAULT_TO_DEVICE.

Disable Hostname Verification

• By default, hostname verification is enabled on outgoing connections except for the Microsoft PKI server. When hostname 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 hostname 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 Endpoint Management
  – The Microsoft CA server is the certificate issuer
  – An internal CA, whose root Endpoint Management doesn’t trust, signed your certificate.

  Defaults to True.

enable.cloud.console.sso

This server property is available only to customers who onboarded before Endpoint Management 19.8.0 (August 1, 2019). New customers sign on to the Citrix Cloud console for SSO access to the Endpoint Management console.
Citrix Endpoint Management

- If **True**, disables direct access to the Endpoint Management console. To access the Endpoint Management console, you sign on to the Citrix Cloud console. Attempts to directly access the Endpoint Management console on port 4443 result in a 404 error.

  By default, `enable.cloud.console.sso` is **False**, which provides direct access to the Endpoint Management console through port 4443. Citrix recommends disabling direct access to the Endpoint Management console.

**Enable Crash Reporting**

- If **true**, Citrix collects crash reports and diagnostics to help troubleshoot issues with Secure Hub for iOS and Android. If **false**, no data is collected. 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 Endpoint Management connections to 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. 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**.

**Enable Notification Trigger**

- Enables or disables Secure Hub client notifications. The value **true** enables notifications. Defaults to **true**.

**Enrollment required**

This property, which applies only when the Endpoint Management server mode is MDM+MAM, specifies whether you require users to enroll in MDM. The property applies to all users and devices for the Endpoint Management instance. Requiring enrollment provides a higher level of security. However, that decision depends on whether you want to require MDM. By default, enrollment is not required.

If **False**, users can decline enrollment, but might still access apps on their devices through the app store. If **True**, any user who declines enrollment is denied access to apps.
Important:
If you change this property after users enroll, the users must re-enroll.

force.server.push.required.apps

- Enables the forced deployment of required apps on Android and iOS devices in situations such as the following:
  - You upload a new app and mark it as required.
  - You mark an existing app as required.
  - As user deletes a required app.
  - A Secure Hub update is available.

Forced deployment of required apps is `false` by default. Create the custom key and set `Value` to `true` to enable forced deployment. During forced deployment, MDX-enabled required apps, including enterprise apps and public app store apps, upgrade immediately. The upgrade occurs even if you configure an MDX policy for an app update grace period and the user chooses to upgrade the app later.

- Key: Custom Key
- Key: `force.server.push.required.apps`
- Value: `false`
- Display Name: `force.server.push.required.apps`
- Description: Force required apps to deploy

Full Pull of ActiveSync Allowed and Denied Users

- The interval in (in seconds) that 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 Endpoint Management. If Endpoint Management has 15 consecutive failed uploads, it disables telemetry. Defaults to `false`.
Inactivity Timeout in Minutes

- The number of minutes after which Endpoint Management logs out an inactive user. The user must have used the Endpoint Management Public API to access the Endpoint Management console or any third-party app. A time-out value of 0 means an inactive user remains logged in. For third-party apps that access the API, remaining logged in is typically necessary. Default is 5.

- If the WebServices timeout type server property is INACTIVITY_TIMEOUT: This property defines the number of minutes after which Endpoint Management logs out an inactive administrator who did the following:
  - Used the Public API for REST Services to access the 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 remains logged in.

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 Endpoint Management. Both properties default to 45 days.

iOS Device Management Enrollment Auto-Install Enabled

- If true, this property reduces the amount of user interaction required during device enrollment. Users must click Root CA install (if needed) and MDM Profile install.

iOS Device Management Enrollment Install Root CA if Required

- The server property ios.mdm.enrollment.installRootCaIfRequired is set to False for all Endpoint Management environments. Endpoint Management uses a publicly trusted certificate chain, thus 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 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 performed. Defaults to SCEP.

iOS Device Management Identity Key Size

- Defines the size of private keys for MDM identities, iOS profile service, and Endpoint Management iOS agent identities. Defaults to 1024.

iOS Device Management Identity Renewal Days

- Specifies the number of days before the certificate expiration that 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, Endpoint Management issues a new certificate. Defaults to 30 days.

iOS MDM APNS Private Key Password

- This property contains the APNs password, which is required for Endpoint Management to push notifications to Apple servers.

Length of Inactivity Before Device IsDisconnected

- Specifies how long a device can remain inactive, including the last authentication, before Endpoint Management disconnects it. Defaults to 7 days.

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 enrollments.

  - 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, with a larger number of threads, such as 6, a volume purchase import results in high CPU usage.

Citrix Gateway (NetScaler) Single Sign-On

- If False, disables the Endpoint Management callback feature during single sign-on from Citrix Gateway to Endpoint Management. If the Citrix Gateway configuration includes a callback URL, Endpoint Management uses the callback feature to verify the Citrix Gateway session ID. Defaults to False.

Number of consecutive failed uploads

- Displays the number of consecutive failures during Customer Experience Improvement Program (CEIP) uploads. Endpoint Management increments the value when an upload fails. After 15 upload failures, Endpoint Management disables CEIP, also called telemetry. For more information, see the server property Identifies if telemetry is enabled or not. 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.

Pull of Incremental Change of Allowed and Denied Users

- The number of seconds that Endpoint Management waits for a response from the domain when executing a PowerShell command to get a delta of ActiveSync devices. Defaults to 60 seconds.

Read Timeout to Microsoft Certification Server

- The number of seconds that Endpoint Management waits for a response from the certificate server when performing 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 Self-Help Portal on port 443 get a 404 error. And, 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 Endpoint Management retains the session log. Defaults to `7`.

Content Collaboration 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 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`. 

© 1999-2019 Citrix Systems, Inc. All rights reserved.
**Static Timeout in Minutes**

- If the **WebServices timeout type** server property is **STATIC_TIMEOUT**: This property defines the number of minutes after which Endpoint Management logs out an administrator after using the following:
  - The Public API for REST Services to access the 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 Secure Hub client messaging. The value **false** enables messaging. Defaults to **true**.

**Trigger Agent Sound Suppression**

- Enables or disables 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. 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**.

**Unauthenticated App Download for Windows Devices**

- Used only for older Secure Hub versions which don’t validate one-time tickets. If **False**, you can download unauthenticated apps from Endpoint Management to Windows devices. Defaults to **False**.

**Use ActiveSync ID to Conduct an ActiveSync Wipe Device**

- If **true**, Endpoint Management connector for Exchange ActiveSync uses the ActiveSync identifier as an argument for the **asWipeDevice** method. Defaults to **false**.
User-Defined Device Properties

- Used for Windows CE devices only. This custom key enables you to obtain properties that you create in the registry of Windows CE devices. After those properties are in the Endpoint Management database, you can create deployment rules based on the value of the properties.
  - Key: Custom Key
  - Key: device.properties.userDefined
  - Value: administrator-defined
  - Display Name: administrator-defined
  - Description: administrator-defined

Users only from Exchange

- If true, disables user authentication for ActiveSync Exchange users. Defaults to false.

VP baseline interval

- The minimum interval that Endpoint Management reimports volume purchase licenses from Apple. Refreshing license information ensures that Endpoint Management reflects all changes, such as when you manually delete an imported app from volume purchase. By default, Endpoint Management refreshes the volume purchase license baseline a minimum of every 720 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 Endpoint Management updated with the changes.
  - The minimum interval between two baselines is 60 minutes. In addition, Endpoint Management performs a delta import every 60 minutes, to capture the changes since the last import. Therefore, 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: Endpoint Management considers a token expired, based on the value of the server property Static Timeout in Minutes.
-- If **INACTIVITY_TIMEOUT**: Endpoint Management considers a token expired, based on the value of the server property **Inactivity Timeout in Minutes**. Defaults to **STATIC_TIMEOUT**.

**Windows Phone MDM Certificate Extended Validity (5y)**

- The validity period of the device certificate issued by MDM for Windows Phone and 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 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**.

**Endpoint Management MDM Self-Help Portal console max inactive interval (minutes)**

- This property name reflects the older Endpoint Management versions. The property controls the Endpoint Management console max inactive interval. That interval is the number of minutes after which Endpoint Management logs an inactive user out of the Endpoint Management console. A time-out of 0 means an inactive user remains logged in. Default is **30**.

**Adding, Editing, or Deleting Server Properties**

In Endpoint Management, you can apply properties to the server.

1. In the 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.

   ![Add New Server Property](image)

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.
Citrix Endpoint Management

- Value: Enter a value depending on the key 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 check box 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.

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 property you want to delete.
Device and app policies

September 26, 2019

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. In the event 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 ensuring 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

Endpoint Management device and app policies address many situations that may pose a security risk, such as the following:

- When users try to access apps and data from untrusted devices and unpredictable locations.
- When users pass data from device to device.
- When an unauthorized user tries to access data.
- When a user who has left the company had used their own device (BYOD).
- When a user misplaces a device.
- When users need to access the network securely at all times.
- When users have their own device managed and you need to separate work data from personal data.
- When a device is idle and requires verification of user credentials again.
Citrix Endpoint Management

- When users copy and paste sensitive content into unprotected email systems.
- When 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:
- At rest
- In transit

**How Endpoint Management protects data at rest**

Data stored on mobile devices is referred to as data at rest. The mobile application management (MAM) capabilities in Endpoint Management enable complete management, security, and control over Citrix mobile productivity apps, MDX-enabled apps, and their associated data. The Mobile Apps SDK, which enables apps for Endpoint Management deployment, leverages Citrix MDX app container technology to separate corporate apps and data from personal apps and data on the user’s mobile device. This allows you to secure any custom developed, third-party, or BYO mobile app with comprehensive policy-based controls.

In addition to an extensive MDX policy library, Endpoint Management also includes app-level encryption. Endpoint Management separately encrypts data stored within any MDX-enabled app without requiring a device PIN code and without requiring that you manage the device to enforce the policy.

Policies and the Mobile Apps SDK enable you to:
- Separate business and personal apps and data in a secure mobile container.
- Secure apps with encryption and other mobile Data Loss Prevention (DLP) technologies.

MDX policies provide many operational controls, so you can enable seamless integration between MDX-wrapped apps, while also controlling all communication. In this way, you can enforce policies, such as ensuring that data only is accessible by MDX-enabled apps.

Beyond device and app policy control, the best way to safeguard data at rest is encryption. Endpoint Management adds a layer of encryption to any data stored in an MDX-enabled app, giving you policy control over features such as public file encryption, private file encryption, and encryption exclusions. The Mobile Apps SDK uses FIPS 140-2 compliant AES 256-bit encryption with keys stored in a protected Citrix Secret Vault.

**How 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 Citrix Gateway.
Consider the situation where an employee wants to access the following resources residing in the secure enterprise network from a mobile device: the corporate email server, an SSL-enabled web application hosted on the corporate intranet, and 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 could infect the entire corporate system. Corporate mobile apps and personal mobile apps are able to coexist on one device.

To offer even stronger levels of security, you can configure MDX-enabled apps with an Alternate Citrix Gateway policy, used for authentication and for micro VPN sessions with an app. You can use an Alternate Citrix Gateway with the micro VPN session required policy to force apps to reauthenticate to the specific gateway. Such gateways would typically have different (higher assurance) authentication requirements and traffic management policies.

In addition to security features, micro VPN also offers data optimization techniques, including compression algorithms to ensure that only minimal data is transferred and that the transfer is done in the quickest time possible, thereby improving user experience, which is a key success factor in mobile project success.

You should reevaluate your device policies periodically, such as in these situations:

- When a new version of Endpoint Management includes new or updated policies due to the release of device operating system updates.
- When you add a new 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 may find differences between iOS, Android, and Windows devices, and even between different manufacturers’ devices running Android.
- To keep Endpoint Management operation in sync with enterprise or industry changes, such as new corporate security policies or compliance regulations.
- When a new version of MDX Service includes new or updated policies.
- When you add or update an app.
- When you need to integrate new workflows for your users as a result of new apps or new requirements.

**App policies and Use case scenarios**

Although you can choose which apps are available through Secure Hub, you might also want to define how those apps interact with Endpoint Management. If you want users to authenticate after a certain time period passes or you want to provide users offline access to their information, you do so through
app policies. The following list includes some of the policies and discusses how you might use them. 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 PIN enabled. This feature ensures use of iOS encryption at the device level and for the MDX container.

  **User example:** Enabling this policy means that the user must set a PIN code on their iOS device before they can access the MDX app.

- **App passcode**
  
  **Why use this policy:** Enable the App passcode policy to have 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 Endpoint Management console. You can set an inactivity timer in Client Properties so that, with continued use, Secure Hub doesn’t prompt the user to authenticate to the managed app again until the timer expires.

  The app passcode differs from a device passcode in that, with a device passcode policy pushed to a device, Secure Hub prompts the user to configure a passcode or PIN, which they must unlock before they can gain access to their device when they turn on the device or when the inactivity timer expires. For more information, see Authentication in 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 so that Endpoint Management prompts the user to connect to the enterprise network or have an active session before using the app.

  **User example:** When a user attempts to open an MDX app that has the micro VPN session required policy enabled, they can’t use the app until they connected to the network using a cellular or Wi-Fi service.

- **Maximum offline period**
  
  **Why use this policy:** Use this policy as an additional security option, to ensure that users can’t run an app offline for long time periods without reconfirming app entitlement and refreshing policies from Endpoint Management.
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 released 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 those who might experience long periods offline when traveling internationally.

  User example: You load a new version of Secure Mail in the app store and then set an app update grace period of 6 hours. All Secure Mail users will see a message asking them to update their Secure Mail app, until the 6 hours expire. When the 6 hours expire, Secure Hub routes users to the app store.

- **Active poll period (minutes)**

  Why use this policy: The active poll period is the interval at which Endpoint Management checks apps for when to perform security actions, such as App Lock and App Wipe.

  User example: If you set the Active poll period policy to 60 minutes, when you send the App Lock command from Endpoint Management to the device, the lock occurs within 60 minutes of when the last poll took place.

Encryption policies

Why use these policies: Endpoint Management includes a secret vault with a strong encryption layer that Secure Hub and other Citrix mobile productivity apps use to persist their sensitive data, such as passwords and encryption keys, on the device without depending on the platform native keystores. As a result, if the device becomes compromised in any way, corporate data remains encrypted in the MDX container and Endpoint Management obfuscates the data before transferring it outside of the container.

User example: If the device owner did not set a device PIN or the device PIN becomes compromised, the corporate data inside the Secure Hub container remains secure.
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 or from pasting data from outside of the container into the containerized apps.

User example: You set an App interaction policy to Restricted, which means a user can copy text from Secure Mail to Secure Web but can’t copy that data to their personal Safari or Chrome browser that is outside the container. In addition, a user can open an attached document from Secure Mail into Citrix Files or QuickEdit but 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. This helps to ensure 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: If you enable the App Restriction policy to block dictation on iOS in an MDX app, the user can't use the dictate function on the iOS keyboard while the MDX app is running. Thus, data 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 remains 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. For the Network access policy, set the Tunneled to the internal network option to automate a micro VPN from the MDX app through the Citrix Gateway to a back-end web service or datastore.

User example: When a user opens an MDX app, such as Secure Web, that has tunneling enabled, the browser opens and launches an intranet site without the user needing to start a VPN. The Secure Web app automatically accesses the internal site using micro VPN technology.
Citrix Endpoint Management

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 contain 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 attempts to use an app outside of the defined radius, the app remains locked and the user cannot 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.

Secure Mail App policies

- Background network services

  Why use this policy: Background network services in Secure Mail leverage Secure Ticket Authority (STA), which is effectively a SOCKS5 proxy to connect through Citrix Gateway. STA supports long-lived connections and provides better battery life compared to micro VPN. Thus, STA is ideal for mail that connects constantly. Citrix recommends that you configure these settings for Secure Mail. The NetScaler for XenMobile wizard automatically sets up STA for Secure Mail.

  User example: When STA isn’t enabled and an Android user opens Secure Mail, they are prompted to open a VPN, which remains open on the device. When STA is enabled and the Android user opens Secure Mail, 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 Secure Mail when the user accesses Secure Mail for the first time. Be aware that 2 weeks of email takes longer to sync than 3 days and prolongs the setup process for the user.

  User example: If the default sync interval is set to 3 days when the user first sets up Secure Mail, they can see any emails in their Inbox that they received from the present to 3 days in the past. If a user wants to see emails that are older than 3 days, they can do a search. Secure Mail then shows the older emails stored on the server. After installing 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 Endpoint Management works with devices. Although many policies are common to all devices, each device has a set of policies 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 articles under Device policies.
**App inventory policy**

**Why use this policy:** Deploy the App inventory policy to a device if you need to see the apps installed by a user. If you don’t deploy the App inventory policy, you can see only the apps that a user installed from the app store and not any personally installed applications. You must use this policy if you want to blacklist 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 Endpoint Management administrators.

**App lock policy**

**Why use this policy:** The App Lock policy, for Android, allows you to blacklist or whitelist apps. For example, by whitelisting 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:** You must use the Connection scheduling policy so that Windows Mobile devices can connect back to Endpoint Management for MDM management, app push, and policy deployment. For Android, Android Enterprise, and Chrome OS devices, use Google Firebase Cloud Messaging (FCM), instead of this policy, to control connections to Endpoint Management. The Scheduling options are as follows:

- **Never:** Connect manually. Users must initiate the connection from 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:** Connects at the designated interval. When this option is in effect and you send a security policy, such as a lock or a wipe, Endpoint Management processes the policy on the device the next time the device connects.

- **Define schedule:** When enabled, Endpoint Management attempts to reconnect the user’s device to the Endpoint Management server after a network connection loss and monitors the connection by transmitting control packets at regular intervals within the timeframe you define.

**User example:** You want to deploy a passcode policy to enrolled devices. The scheduling policy ensures 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 in conjunction with a WiFi policy, the Credentials policy lets you deploy certificates for authentication to internal resources that require certificate authentication.

**User example:** You deploy a WiFi policy that configures a wireless network on the device. The WiFi 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 Endpoint Management, you have two options to deliver Microsoft Exchange ActiveSync email.

- **Secure Mail app:** Deliver email by using the Secure Mail app that you distribute from the public app store or the app store.

- **Native email app:** Use the Exchange policy to enable ActiveSync email for the native email client on the device. With the Exchange policy for native email, 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. Secure Hub then prompts the user to authenticate and 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 Secure Hub. After you deploy this policy and then send a locate command from 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 Endpoint Management Self-Help Portal and choose the locate option to see the location of their device on a map. Note that the user makes the choice to allow 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.

**User example:** When you deploy a passcode policy to a managed device, Secure Hub prompts the user to configure a passcode or PIN, which they must unlock before they can gain access to their device when they turn on the device 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 need to remove that policy from a subset of the users. You can remove the policy for selected users by creating a Profile removal policy and using deployment rules to deploy the Profile removal policy only to specified user names.

  **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 won’t know that camera use is now allowed. 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, from disabling the camera or microphone on a device to enforcing roaming rules and access to third-party services like app stores.

  **User example:** If you deploy a restriction to an iOS device, the user may not be able to access iCloud or the iTunes store.

• **Terms and conditions policy**

  **Why use this policy:** You might need to advise users of the legal implications of having their device managed. In addition, you may want to ensure that users are aware of the security risks when corporate data is pushed to the device. The custom 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 backend systems using older VPN Gateway technology. The policy supports a number of VPN providers, including Cisco AnyConnect, Juniper, as well as 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.

• **Webclip policy**

  **Why use this policy:** Use the Webclip policy if you want to push to devices an icon that opens directly to a website. A webclip contains a link to a website and can include a custom icon. On
a device a webclip looks like an app icon.

**User example:** A user can click on a webclip icon to open an internet site that provides services they need to access. Using a web link is more convenient than needing to open a browser app and type a link address.

- **WiFi policy**

  **Why use this policy:** The WiFi policy lets you deploy WiFi network details, such as the SSID, authentication data, and configuration data, to a managed device.

  **User example:** When you deploy the WiFi policy, the device automatically connects to the WiFi network and authenticates the user so they can gain access to the network.

- **Windows Information Protection policy**

  **Why use this policy:** Use the Windows Information Protection (WIP) policy to protect against the potential leakage of enterprise data. You can specify the apps that require Windows Information Protection at the enforcement level you set. For example, you can block any inappropriate data sharing or warn about inappropriate data sharing and allow users to override the policy. You can run WIP silently while logging and permitting inappropriate data sharing.

  **User example:** Suppose that you configure the WIP policy to block inappropriate data sharing. If a user copies or saves a protected file to a non-protected location, a message similar to the following appears: You can’t place work protected content in this location.

- **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, MDX wrapped apps, Citrix mobile productivity apps, native mobile apps such as .ipa or .apk files, iTunes and Google play apps, web links, and Citrix Virtual Apps published using Citrix StoreFront.

  **User example:** After a user enrolls their device into Endpoint Management, they access the app store through the Citrix Secure Hub app or, if using Citrix workspace, through the workspace. The user can then see all the corporate apps and services available to them. Users can click on an app to install it, access the data, rate and review the app, and download app updates from the app store.

**Client properties**

September 17, 2019
Citrix Endpoint Management

Client properties contain information that is provided directly to Secure Hub on user devices. You can use these properties to configure advanced settings, such as the Citrix PIN. You obtain client properties from Citrix support.

Client properties are subject to change with every release of Secure Hub and occasionally for client apps. For details about more commonly configured client properties, see Client property reference, later in this article.

1. In the 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:** In the list, click the property key that you want to add. **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.

3. Click **Save**.

To edit a client property

1. In the Client Properties table, select the client property you want to edit.
   
   When you select the check box next to a client property, the options menu appears above the client property list. When you click anywhere else in the list, the options menu appears on the right side of the listing.

2. Click **Edit**. The **Edit Client Property** page appears.

   ![Edit Client Property](image)

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 check box next to each property.

2. Click **Delete**. A confirmation dialog box appears. Click **Delete** again.

**Client property reference**

The Endpoint Management predefined client properties and their default settings are as follows.

- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - Display name: MDX Container Self Destruct Period
  - Self-destruct prevents access to 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 does not receive an authentication request to validate the user over a specific length of time. For example, if this property is 30 days and the user doesn't use the apps 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`.
  - 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 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, logs aren't attached. A message indicates that logging is disabled. This setting also prevents you from updating log settings in the Endpoint Management console for Secure Hub and MDX apps.
When this property is set to `true`, 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 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 or not you enable Citrix PIN. If you don’t enable Citrix PIN, users enter their Active Directory password. Endpoint Management supports use of Active Directory passwords with the credential store only for Secure Hub and public store apps. If you use Active Directory passwords with the credential store, Endpoint Management doesn’t support PKI authentication.
- Automatic enrollment in Secure Mail requires that you set this property to `true`.
- 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_NETWORK_EXTENSION**

- This property is deprecated as of November 30, 2018.

**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 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 perform authentication with Endpoint Management.
If ENABLE_PASSCODE_AUTH is true and ENABLE_PASSWORD_CACHING is false, online authentication always prompts for the password because 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, 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, 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.

- Possible values: **true** or **false**
- Default value: **false**

**ENABLE_WORXHOME_CEIP**
- Display name: Enable Worx Home 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 Endpoint Management.

- Value: **true** or **false**
- Default value: **false**

**ENABLE_WORXHOME_GA**
- Display name: Enable Google Analytics in Worx Home
- This property enables or disables the ability to collect data using Google Analytics in Secure Hub. When you change this setting, the new value is set only when the user next logs on to Secure Hub (previously named Worx Home).
- Possible values: true or false
- Default value: true

• 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 Secure Hub to perform 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 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 IT help desk
  - 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 very 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 perform 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
- This property defines the strength of 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, 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:
## Citrix Endpoint Management

### Passcode strength

<table>
<thead>
<tr>
<th>Passcode strength</th>
<th>Rules for numeric passcode type</th>
<th>Allowed</th>
<th>Not allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>All numbers, any sequence allowed</td>
<td>444444, 123456, 654321</td>
<td></td>
</tr>
<tr>
<td>Medium (default setting)</td>
<td>All numbers cannot be the same or consecutive.</td>
<td>444333, 124567, 136790, 555556, 788888</td>
<td>444444, 123456, 654321</td>
</tr>
<tr>
<td>High</td>
<td>Same as for the Medium Passcode strength.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strong</td>
<td>Same as for the Medium Passcode strength.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Rules for alphanumeric passcodes:

<table>
<thead>
<tr>
<th>Passcode strength</th>
<th>Rules for alphanumeric passcode type</th>
<th>Allowed</th>
<th>Not allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Must contain at least one number and one letter</td>
<td>aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa</td>
<td>AAAaaa, aaaaaa, abcdef</td>
</tr>
<tr>
<td>Medium (default setting)</td>
<td>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.</td>
<td>aa11b1, aaa11b, aa11b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~</td>
<td>aaaa11, aa11aa, or aaaa111; abcd12, bcd123, 123abc, xy1234, xyz345, or cba123</td>
</tr>
<tr>
<td>High</td>
<td>Include at least one capital letter and one small letter.</td>
<td>Abcd12, jkrtA2, 23Bc#, AbCd</td>
<td>abcd12, DFGH2</td>
</tr>
</tbody>
</table>
### Passcode strength

Rules for alphanumeric passcode type

<table>
<thead>
<tr>
<th>Allowed</th>
<th>Not allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#</td>
<td>abcd12, Abcd12, dfgh12, jkrtA2</td>
</tr>
</tbody>
</table>

- **PASSCODE_TYPE**
  - **Display name:** PIN Type
  - **Possible values:** Numeric or Alphanumeric
  - **Default value:** Numeric

- **REFRESHINTERVAL**
  - **Display name:** REFRESHINTERVAL
  - **Default value:** 72 hours (3 days)

- **SEND_LDAP_ATTRIBUTES**
  - **For MAM-only deployments of Android, iOS, or macOS devices:** You can configure Endpoint Management so that users who enroll in Secure Hub with email credentials are automatically enrolled in Secure Mail. As a result, users don’t provide extra information or take extra steps to enroll in Secure Mail.
  - **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 name="SEND_LDAP_ATTRIBUTES">
<property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,email=user@site.com\,user@site.com"/>
```

For this property, Endpoint Management treats comma characters as string terminators. Therefore, 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 performing 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 override the default list of domains excluded.
- To configure this global client policy, go to **Settings > Client Properties**, add the custom key **TUNNEL_EXCLUDEDOMAINS**, and set the Value.
- Value: To replace the default list with the domains that you want to exclude from tunneling, type a comma-separated list of domain suffixes. To include all domains in tunneling, type none. Default is:

  ```
  ```

© 1999-2019 Citrix Systems, Inc. All rights reserved.
User enrollment options

November 7, 2019

You can have users enroll their devices in Endpoint Management in several ways. Before considering the specifics, decide if the devices in your environment enroll in MDM+MAM or MAM mode (also known as MAM-only mode). For more information about the management modes, see Management modes.

At the highest level, there are four enrollment options:

- **Enrollment Invitation**: Send an enrollment invitation or invitation link to users.
- **Self-Help Portal**: Set up a portal that users can visit to download Secure Hub and enroll their devices or send themselves an enrollment invitation.
- **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 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 purchase 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, or Android devices. You can also send an installation link through SMTP or SMS to users with iOS, macOS, Android, or Windows devices. For more information, see Enroll devices.

If you choose to use the enrollment invitation method: You can choose from up to seven enrollment modes (depending on platform), and you can use any combination of the modes. You can enable or disable the modes from the Endpoint Management Settings page, and you can select a default from Username + Password, Two Factor, and Username + PIN. For information on each enrollment mode, see Configure enrollment modes.

If you choose certificate-based, consider excluding Username + Password traditional authentication from the allowed options. Username + Password authentication might expose a weak onboarding vector into your environment and potentially void the mandated security quality.

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 cannot be used again. You can use this property to limit the users or devices enrolling to your system.
You can set up Endpoint Management so that iOS users provide credentials during enrollment in one of the following ways:

- Users type their credentials during enrollment.
- Users insert a smart card from a derived credentials provider into a reader attached to their desktop. For information about derived credentials, see Derived credentials.

In the Endpoint Management console, you can also choose the option for Enrollment Profiles. Through that option you can control the number of devices specific users can enroll, based on Active Directory groups. For instance, if you want to allow your Finance division only one device per user, you can configure that scenario through enrollment profiles.

Be aware of the extra costs and pitfalls of certain enrollment options. If you want to send invitations using SMS, you need to set up an extra infrastructure. For more information on this option, see Notifications.

In addition, if you plan to send invitations by email, ensure that users have a way of accessing email outside of Secure Hub. You can use one-time password (OTP) enrollment modes as an alternative to Active Directory passwords for MDM enrollment.

**Self-Help Portal**

Users can request an enrollment invitation through the Self-Help Portal. The default mode is Username + Password, but you can also change that requirement to Two Factor or Username + PIN. For information about setting up the Self-Help Portal, see Configure enrollment modes.

**Manual Enrollment**

With manual enrollment, users connect to Endpoint Management either through autodiscovery or by entering the server information. With autodiscovery, users log on to the server 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 Set up 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 modes. This section discusses the way you reach out to users.

Open Enrollment vs. Selective Invitation

When onboarding users, you can allow enrollment through two basic methods: You can allow open enrollment in which, by default, any user with LDAP credentials and the Endpoint Management environment information can enroll. Or, you can limit the number of users by only allowing users with invitations to enroll. You can also limit open enrollment by 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:

- If you are rolling out a MAM environment, you can easily limit enrollment through Active Directory group membership.
- With an MDM environment, the only way to limit enrollment is to 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 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.
- You also want to keep in mind whether you have user or device licenses. With user licenses, each user can have multiple devices and only one license is consumed. With device licenses, each device enrolled consumes one license.

Selective invitation is typically performed less often because it requires a bit more work than open enrollment. In order 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 invite 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 and SMS messages are a part of the process. You can send emails through the 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. For text messages, you need an SMS server. These servers might be extra costs to consider when making your decision. In addition, before you select a method, consider how you expect new users to access information, like email. If you want all users to access their email through Endpoint Management, sending them an invitation email would be problematic.

You can also send communications by another means outside of Endpoint Management for an open enrollment environment. Be sure to include all the relevant information, such as where users can get the Secure Hub app and what method they use to enroll. If you have discovery turned off, tell users the Endpoint Management server address too. To learn more about discovery, see Set up Endpoint Management AutoDiscovery Service.

App provisioning and deprovisioning

November 7, 2019

Application provisioning revolves around mobile app lifecycle management, which mainly consists of wrapping, configuring, delivering, and managing mobile apps within a Endpoint Management environment. In some instances, developing or modifying application code may also be part of the provisioning process. Endpoint Management is equipped with various tools and processes that you can use for app provisioning.

Before you read this article on app provisioning, it is recommended that you read the articles on 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 may start with a limited number of apps; however, the number of apps you manage could rapidly increase as user adoption rates increase and your environment grows. You should define specific app profiles right from the beginning in order 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: Multiple instances that are deployed for different set 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
- MDX Policies: Wrapped or unwrapped with MDX security policies
- Network Access: Type of access, such as full VPN (Tunneled - Full VPN) or full VPN with single sign-on (Tunneled - Web SSO).

Example:

<table>
<thead>
<tr>
<th>Factor</th>
<th>Secure Mail</th>
<th>Mail</th>
<th>In-House</th>
<th>Epic Rover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>10.1</td>
<td>10.1</td>
<td>X.x</td>
<td>X.x</td>
</tr>
<tr>
<td>Instance</td>
<td>VIP</td>
<td>Physicians</td>
<td>Clinical</td>
<td>Clinical</td>
</tr>
<tr>
<td>Platform</td>
<td>iOS</td>
<td>iOS</td>
<td>iOS</td>
<td>iOS</td>
</tr>
<tr>
<td>Target Users</td>
<td>VIP Users</td>
<td>Physicians</td>
<td>Clinical Users</td>
<td>Clinical Users</td>
</tr>
<tr>
<td>Ownership</td>
<td>IT</td>
<td>IT</td>
<td>Clinical Users</td>
<td>IT</td>
</tr>
<tr>
<td>Type</td>
<td>MDX</td>
<td>MDX</td>
<td>Native</td>
<td>Public</td>
</tr>
<tr>
<td>Upgrade Cycle</td>
<td>Quarterly</td>
<td>Quarterly</td>
<td>Yearly</td>
<td>N/A</td>
</tr>
<tr>
<td>Licensing</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Volume purchase</td>
</tr>
<tr>
<td>MDX Policies</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Network Access</td>
<td>VPN</td>
<td>VPN</td>
<td>VPN</td>
<td>Public</td>
</tr>
</tbody>
</table>

- **App versioning:** Maintaining and tracking app versions is a critical part of the provisioning process. Versioning is usually 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 in order to avoid production impact.

It is also important to evaluate if a specific upgrade is actually required. App upgrades are usually of two types: One is a minor upgrade, such as a fix to a specific bug; the second is a major release, which introduces significant changes and improvements to the app. In either case, you should carefully review the release notes of the app to evaluate if the upgrade is necessary.

- **App signing and wrapping:** With Endpoint Management, you can use MDX policies with managed apps to secure the corporate data through app wrapping. For more information about app wrapping, see **Endpoint Management MDX Service**. The app provisioning process for a wrapped app is significantly different from the provisioning process for a standard non-wrapped app.

- **App security:** You define 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 prior to deploying the apps, which greatly simplifies and expedites app deployment. You may deploy
certain apps differently, or you may need to make architectural changes to your Endpoint Management environment depending on the type of security compliance that the apps require. For example, you may want the device to be encrypted in order to allow the use of a critical business intelligence app, or a certain app may require end-to-end SSL encryption or geo-fencing.

- **App delivery:** 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 without controlling the app apart from enforcing device level restrictions. On the other hand, the MAM mode of delivering apps allows full control over app delivery and over the app itself. Delivering the apps in MAM mode is more suitable in most cases. When you deliver apps in MAM mode, the mobile device must be enrolled either into XME (MDM+MAM) or MAM-only mode.

- **Application maintenance:**
  - Perform an initial audit: You should keep track of the app version that is present in your production environment, as well as the last upgrade cycle. Make note of specific features or bug fixes that required the upgrade to take place.
  - Establish baselines: You should maintain a list of the latest stable release of each app. This app version should be fall back in case unexpected issues occur post upgrade. You should also develop a rollback plan. You should test app upgrades in a test environment prior to your production deployment; if possible, you should 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: This is critical in order to keep up to date with the latest release of the apps. In some cases, an early access release (EAR) build may also be available for testing ahead of time.
  - Devise a strategy to notify users: You should define a strategy to notify users when app upgrades are available. Prepare users with training prior to deployment. You may send multiple notifications prior to updating the apps. Depending on the app, the best notification method might be email notifications or web sites.

App lifecycle management represents the completed lifecycle of an app from its initial deployment through the retirement of the app. The lifecycle of an app can be broken down into these five phases:

1. Requirements for specifications: Start with business case and user requirements.
2. Development: Validate that the app meets business needs.
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

November 1, 2019

You can view information at a glance by accessing your 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 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.
  - **Notifications**: Mark the check box 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 may 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 regarding 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’d like 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 may want to use the **Devices by ActiveSync Gateway Status** and **Devices By Blocked Reason** widgets to determine whether the issue is ActiveSync related.

Reporting

After your environment is setup and users enroll, you can run reports to learn about your deployment. Endpoint Management comes with a number of 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 Endpoint Management support

September 26, 2019

Endpoint Management uses role-based access control (RBAC) to restrict user and group access to Endpoint Management system functions, such as the Endpoint Management console, Self-Help Portal, and public API. This article describes the roles built in to Endpoint Management and includes considerations for deciding on a support model for Endpoint Management that leverages 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 setting, 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 perform 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.

**Device provisioning**

Default access granted:
• Access to the Endpoint Management console to perform basic administration on Windows CE devices: add, change, and remove devices; use the Settings page.

Considerations:
• Applies only to Windows CE devices.

**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 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 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 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 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 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 additional training will they need?

Do you want to give users access to the Endpoint Management Self-Help Portal?
Although some organizations prefer not to grant users access to 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 new role with only the permissions you want to include. You can create as many roles as needed to meet your requirements.

Citrix Support process

March 25, 2019

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 Consulting Services or Citrix Education Services offer help related to product training, advice on product usage, configuration, installation, or environment design and architecture.

Citrix Consulting helps with Citrix product-related projects, including proof of concepts, economic impact assessment, infrastructure health checks, design requirements analysis, architecture design verification, integration, and operational process development.

Citrix Education 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, Citrix Community, and Citrix Support on Twitter 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 Citrix 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. For information on contacting support for Endpoint Management issues, see How to Contact Support.

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 offering and benefits, see Citrix Worldwide Services.

---

**Sending group enrollment invitations in Endpoint Management**

November 21, 2019

Contributed by John Bartel III

You can send enrollment invitations to groups in Endpoint Management. You can send invitations to your nested groups as well. When setting up the group invitation, you can specify one or multiple device platforms. You can also tag devices so that you can, for example, distinguish 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 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 modes and invitations, see User accounts, roles, and enrollment.
General steps

1. Within the 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 multiple 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.
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 authentication you prefer for users.
   • User name + Password
   • High Security
   • Invitation URL
   • Invitation URL + PIN
   • Invitation URL + Password
   • Two Factor
   • User name + PIN
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.
   If you plan to use custom notification templates, you must set up the templates before you configure enrollment modes. For more information about notification templates, see Notifications.
   For these notification templates, use your configured SMTP server setup within 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.

**Solution:** Depending on how large your Active Directory environment is, it could take up to six hours for changes to propagate to all servers. If a user or nested group is removed recently, Endpoint Management may still consider those users as a part of the group.

Therefore, it’s best to wait up to six hours before sending out another group invite to your group.

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

September 20, 2019

Contributed by Vijay Kumar Kunchakuri

To make sure that Secure Mail push notifications work, you must configure Exchange Server for certificate-based authentication. This requirement is especially necessary when Secure Hub is enrolled in Endpoint Management with certificate-based authentication.

You need to 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 Secure Mail push notifications fails and no badge updates occur in Secure Mail.

This article describes the steps to configure certificate-based authentication. The configurations are specifically against the EWS virtual directory on 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

4. Ensure 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** check box.

   b) Under **Client Certificates**, click **Require**. You can set this option to **Accept** if other EWS mail clients connect with user name and password as credentials to authenticate and connect to the Exchange Server.
6. Click Configuration Editor and in the Section drop-down list, navigate to the following section:
   • system.webServer/security/authentication/clientCertificateMappingAuthentication

7. Set the enabled value to True.

8. Click Configuration Editor and in the Section drop-down list, navigate to the following section:
   • 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 may 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.
For more information about troubleshooting Secure Mail issues with iOS push notifications, see this Citrix Support Knowledge Center article.

**Related information**

Push notifications for Secure Mail for iOS

### Configuring an on-premises Device Health Attestation server

November 21, 2019

Contributed by Sanket Mishra

You can enable Device Health Attestation (DHA) for Windows 10 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 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 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 server to server (DHA service and MDM server) and server to client (DHA service and a Windows 10 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 are able to 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 roles** page, select the Device Health Attestation check box.
7. Optional: Click **Add Features** to install other required role services and features.
8. Click **Next**.
9. On the **Select features** 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.
2. Select **Current user** as the store location and click **Next**.
3. Type the password for the private key.

4. Ensure the import option **Include all extended properties** is selected. Click **Next**.

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
      service account holder, select Service account.)
   h) In the Select Computer dialog box, click Finish.
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.
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 available snap-in and add it to selected snap-ins.
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.
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:

```bash
1. mkdir \TrustedTpm
2. expand -F:\* .\TrustedTpm\TrustedTpm.cab .\TrustedTpm
3. cd .\TrustedTpm
4. .\setup.cmd
```

Configure the DHA service

Run this command on the Windows server to configure the DHA service.

Replace the placeholder ReplaceWithThumbprint.

```bash
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:

```bash
$policy = Get-DHASCertificateChainPolicy
$policy.RevocationMode = "NoCheck"
Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

Respond to these prompts, as follows:

```bash
Confirm

Are you sure you want to perform this action?
Performing the operation "Install-DeviceHealthAttestation" on target "[Machine Name]".
```
Adding SSL binding to website 'Default Web Site'.

Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.

Adding web application 'DeviceHealthAttestation' to website 'Default Web Site'.

Adding firewall rule 'Device Health Attestation Service' to allow inbound connections on port(s) '443'.

Setting initial configuration for Device Health Attestation Service.

Registering User Access Logging.
**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 is displayed.

To check whether the DHASActiveSigningCertificate is active, run these commands on the server:

Replace the placeholder ReplaceWithThumbprint and enclose it inside double-quotiation marks as shown.

```
1 Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint" -Force
2
3 Get-DHASActiveEncryptionCertificate
```

If the certificate is active, the thumbprint appears.

To perform a final check, go to this URL:


If the DHA service is running, “Method not allowed” appears.